ITRC
پژوهشگاه ارتباطات و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)

حفاظت از زیر ساخت‌های ملی در برابر

حملات سایبری

مترجم: دکتر احمد صلاحی

حفاظت از زیر ساختهای ملی در برابر

حملات سایبری

تالیف : ادوارد جی روسو
ترجمه: دکتر احمد صلاحی

پژوهشگاه ارتباطات و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)

آراد کتاب

سرشناسه	: آموروسو، ادوارد جی Amoroso Edward G.
عنوان و نام‌پدیدآور	: حفاظت از زیر ساختهای ملی در برابر جملات سایبری/تالیف ادوارد روسو : ترجمه احمد صلاحی
مشخصات نشر	: تهران: آراد کتاب، ۱۳۹۲.
مشخصات ظاهری	: ۳٤۸ ص : مصور ، نمودار.
شابک	: **978-600-186-144-4**
وضعیت فهرست‌نویسی	: فیپا
یادداشت	: عنوان اصلی:
موضوع	: تروریسم رایانه ای—ایالات متحده—پیشگیری.
موضوع	: شبکه های کامپیوتری—تدابیر ایمنی.
موضوع	: جرایم کامپیوتری—ایالات متحده—پیشگیری.
موضوع	: امنیت ملی—ایالات متحده.
شناسه افزوده	: صلاحی ، احمد ، ۱۳۲۵- مترجم.
رده‌بندی کنگره	: H ۷۷۷۳ /۲
رده‌بندی دیویی	: ۳٦۳/۳۲٥۹۰۰٤٦۷۸۰۹۷۳
شماره کتابشناسی ملی	: ۳۳۹۳٥۹۹

حفاظت از زیرساختهای ملی در برابر حملات سایبری

☒ ترجمه : دکتر احمد صلاحی
☒ ناشر: آراد کتاب
☒ نوبت چاپ : اول ۱۳۹۲
☒ تیراژ: ۵۰۰ جلد
☒ چاپ : مدیران
☒ قیمت: ۱۷۵۰۰۰ ریال
☒ شابک: ٤-١٤٤-١٨٦-٦٠٠-٩٧٨
ISBN: 978-600-186-144-4

مرکز پخش و فروش:

آراد کتاب تلفن: ۶۶۴۸۲۲۲۶ – ۶۶۹۷۵۲۸۵ – ۰۹۱۲۳۰۶۲۴۵۸

www.aradbook.com

تقدیر و تشکر

لازم است از تمام کسانی که در ترجمه، تایپ، ویرایش و چاپ این کتاب به من یاری رسانده‌اند؛ تشکر کنم، به خصوص فرزندم، الهه صلاحی که در ویرایش کتاب با من همکاری کرده؛ آقای بذرافشان، مدیر دفتر اسناد و منابع علمی، که در تهیه اصل کتاب و چاپ آن به من یاری رسانده؛ و همچنین، آقای دکتر محمد شهرام معین که راهنمایی‌های لازم را برای بهبود کتاب ارائه کرده است و تیم ویراستاری خانم الهام سادات اختراعی طوسی و آقای سید محمدهادی حیدری تشکر کنم.

احمد صلاحی

آبان ماه ۱۳۹۲

فهرست مطالب

عنوان صفحه

فهرست اشکال

عنوان صفحه

پیشگفتار مؤلف

انسان به جامعه وارد نشده است تا بدتر از آنچه قبلاً بود، شود؛ یا دارای حقوقی کمتر از آنچه قبلاً داشت، گردد؛ بلکه می‌خواست آن حقوق امن‌تر گردد.

Thomas Pain in Common Sense

پیش از اینکه وقت خود را برای مطالعه این کتاب صرف نمایید، لطفاً نکات زیر را مرور کنید. این نکات، مهم‌ترین مطالب فلسفه ابتدایی است که از حفاظت زیرساخت ملی ارائه می‌دهم. با خواندن این نکات، بهتر می‌توانید مطالب کتاب را درک نمایید.

۱. اگر حفاظت‌های ابتدایی امنیتی ارائه نشود، شهروندان ملل آزاد نمی‌توانند امیدی به بیان یا بهره‌مند شدن از آزادی‌شان داشته باشند. امنیت آزادی را سرکوب نمی‌کند بلکه آزادی را ممکن می‌سازد.
۲. در هر کشور مدرن، رایانه‌ها و شبکه‌ها قدرت عناصر زیرساخت حیاتی هستند. در نتیجه، حمله و حمله‌کنندگان سایبری می‌توانند با استفاده از رایانه‌ها و شبکه‌ها به زیرساخت‌هایی که شهروندان به آن متکی هستند، صدمه زده و آن‌ها را خراب کنند.
۳. حفاظت‌های امنیتی، مانند آن‌هایی که در کتاب‌های امنیتی هستند، برای محیط‌هایی با مقیاس کوچک نظیر محیط‌های محاسباتی بنگاه‌های اقتصادی طراحی‌شده‌اند. این حفاظت‌ها قیاسی برای حفاظت زیرساخت‌های پیچیده و عظیم نیستند.

حفاظت‌های سایبری ملی مؤثر، تا حد زیادی با همکاری و هماهنگی بین تجارت، صنعت و سازمان‌های دولتی هدایت می‌شوند. بنابراین، مسائل مدیریتی سازمانی هم به اندازهٔ مسائل فنی برای دفاع ملی مهم هستند.

امنیت یک فرآیند کاهش ریسک است و نه حذف‌کننده آن. بنابراین، باید قدم‌های لازم باید برای کاهش و خطر حمله سایبری به زیرساخت ملی برداشته شود.

خطر فاجعه‌بار حمله سایبری به زیرساخت ملی، در زمان حال، باهر اندازه‌گیری واقعی باید بالا در نظرها گرفته شود. انجام اقدامات کوچک یا انجام ندادن کاری برای کاهش این خطر تصمیم ملی احمقانه‌ای خواهد بود.

فصل‌های این کتاب حول ده اصل پایه‌ای سازمان‌دهی شده است که خطر حمله سایبری به زیرساخت ملی را به طور قابل‌ملاحظه‌ای کاهش می‌دهد. این اصول باتجربه مدیریت امنیت بزرگ‌ترین و پیچیده‌ترین زیرساخت‌ها در جهان؛ سال فراگیری از سازمان‌های دولتی و تجاری مختلف و تعامل با دانشجویان و پژوهشگران دانشگاهی در حوزه امنیت به دست آمده است. این اصول نتیجه تجربه شخصی در مقابله موفق یا ناموفق با دامنه وسیعی از حملات سایبری بوده است، شامل آن‌هایی که هدفشان زیرساخت‌های باارزش بالا بود.

پیاده‌سازی ده اصل این کتاب احتیاج به عزم ملی و تغییر در روش‌هایی دارد که عناصر محاسباتی و شبکه‌ای را در زمینه زیرساخت ملی، طراحی، ساخته و بهره‌برداری کنند.

امیدوارم که پیشنهادها ارائه‌شده در این صفحات، این فرآیند را آسان‌تر نماید

فصل ۱: مقدمه

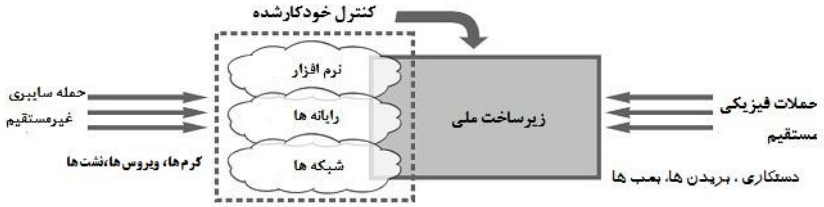
زیرساخت‌های ملی اشاره به سیستم‌های حمایتی ارائه‌دهنده سرویس‌های اساسی و پیچیده برای تمام خدمات با مقیاس وسیع که برای یک ملت کاملاً ضروری هستند دارد. این سرویس‌ها شامل پاسخ در موارد اضطراری، پایگاه‌های داده مجریان قانون (پلیس)، سیستم‌های کنترل نظارت و به دست آوردن داده‌ها (SCADA)، شبکه‌های کنترل نیرو (برق)، سرویس‌های حمایتی نظامی، سیستم‌های سرگرمی مردم (تلویزیون، رادیو)، کاربردهای مالی ارتباطات متحرک و ثابت، خطوط هواپیمایی و ... هستند.

بعضی از سرویس‌های ملی را حکومت فراهم می‌کند؛ اما بیشتر آن‌ها را گروه‌های تجاری، ارائه‌کنندگان سرویس‌های اینترنتی، خطوط هوایی، بانک‌ها و... ارائه می‌نمایند همچنین برخی از سرویس‌هایی که برای قدرت ملی ضروری هستند پشتیبانی زیرساخت‌هایی است که آن‌ها را سازمان‌هایی از دیگر ملت‌ها کنترل می‌نمایند.

می‌نمایند. این به هم وابستگی جهانی با روندی که توماس فرید من از آن به عنوان جهان تخت [۱] یاد می‌کند؛ سازگار است.

زیرساخت‌های ملی به خصوص در ایالات‌متحده امریکا همواره نسبت به حملات فیزیکی نظیر دست‌کاری دستگاه‌ها، بریدن کابل‌ها، بمب‌گذاری در اماکن و دزدی سرمایه‌ها آسیب‌پذیر بوده‌اند. واقعه حمله یازدهم سپتامبر ۲۰۰۱ برجسته‌ترین و آخرین مورد یک حمله عظیم فیزیکی است که هدف آن زیرساخت‌های ملی بود. در چند دهه گذشته، قسمت عمده‌ای از زیرساخت‌های ملی وابسته به نرم‌افزارها، کامپیوترها و شبکه‌ها شده‌اند. این اتکا شامل دسترسی از راه دور به سیستم‌هایی است که سرویس‌های ملی را از طریق معمولاً، اینترنت کنترل می‌نمایند. بنابراین، دشمنان می‌توانند حملات سایبری به زیرساخت‌ها. را با استفاده از کرم‌ها، ویروس‌ها، نشت‌ها و...

شروع نمایند و زیرساخت‌های ملی را از طریق سیستم‌های کنترلی مورد هدف قرار دهند. (به شکل ۱-۱ توجه کنید).



شکل ۱-۱- حملات سایبری و فیزیکی به زیرساخت ملی

یک روش به ظاهر روشن برای مقابله با تهدیدهای سایبری ملی استفاده از تکنیک‌های شناخته‌شده امنیتی کامپیوتری است. در چند دهه اخیر امنیت کامپیوتری به بلوغ قابل‌توجهی رسیده و تخصص قابل‌ملاحظه‌ای در مورد چگونگی حفاظت از نرم‌افزار، کامپیوتر و شبکه به وجود آمده است. در چنین طرح ملی، محافظ‌ها، نظیر؛ دیوارهای آتش، سیستم‌های کشف نفوذ، نرم‌افزار ضد ویروس (ویروس‌کش) کلمه‌های عبور، اسکنرها، دنباله‌های ممیزی و رمزگذاری هستند که باید به طور مستقیم در زیرساخت جاسازی شوند. همان طور که در حال حاضر در محیط‌هایی با مقیاس کوچک‌تر موجود هستند. این سیستم‌های امنیت ملی باید به یک سیستم مدیریت تهدیدات متمرکز وصل شوند و پاسخ به وقایع باید فرآیند آشنایی را که در بنگاه‌ها موجود است طی نماید. همچنین، باید از افرادی که زیرساخت‌های ملی را می‌سازند و اداره می‌نمایند انتظار داشت که برای تضمین تطابق سیاست امنیتی برنامه‌های معمولی نظیر آگاهی کاربران انتهایی، آموزش‌های امنیتی و ممیزی را اجرا کنند. هر ابتکار حفاظتی از زیرساخت‌های ملی که تاکنون پیشنهادشده، راه به ظاهر مستقیمی را طی نموده است. [۲]

با وجود اینکه تکنیک‌های امنیت کامپیوتری به طور قطع برای زیرساخت‌های ملی مفید هستند، بیش‌ترین تجربیات عملی که تاکنون انجام شده است، نشان می‌دهد که این روش‌های معمولی کافی نیست.

دلیل اولیه این موضوع، اندازه، مقیاس و قلمرو ذاتی در زیرساخت‌های پیچیده ملی است.

همان طور که در یک بنگاه به سرمایه قابل مدیریتی جهت پردازش داده‌های امنیتی احتیاج است، در یک شبکه ملی نیز به سیستم غیر معمولی محاسباتی قدرتمندی نیاز است که بتواند حجم عظیمی از اطلاعات را پردازش نماید. چنین حجمی به راحتی از ظرفیت پردازشی و ذخیره‌سازی ابزارهای امنیتی بنگاه‌ها نظیر سیستم‌های مدیریت تهدید تجارتی تجاوز خواهد نمود. متأسفانه، این ناسازگاری با ابتکارات فعلی در صنایع و حکومت جهت کاهش مخارج از طریق استفاده از محصولات تجاری آماده در تضاد خواهد بود.

همچنین، در هنگام وقوع یک فاجعه امنیتی در سیستم‌های تجاری، می‌توان از یک کارشناس امنیتی کمک گرفت؛ درحالی‌که، در زیرساخت‌هایی با مقیاس وسیع ملی، معمولاً به پاسخی احتیاج است که تیمی از متخصصان با دقت با استفاده از فرآیندهای از قبل تعیین‌شده هماهنگ کرده باشند. این تیم متخصصان، معمولاً، به صورت گروه‌ها و سازمان‌های مختلف و در کشورهای گوناگون کار می‌کنند. در بدترین حالات، در صورتی که حکومت‌هایشان آن‌ها را مجبور کنند با یکدیگر همکاری می‌نمایند و برای جلوگیری از عواقب قانونی، آن‌ها تنها مقدار کمی از اطلاعات را تسهیم می‌نمایند. یک مسئله دیگر، پیچیدگی همراه با زیرساخت‌های ملی است که منجر به حالات عجیب و غریب می‌شود؛ که در این حالات، تیم‌های پاسخ گو به شرایط بحرانی درک درست و کاملی از مسئله ندارند و نمی‌دانند که سیستم‌های اساسی چگونه کار می‌کنند. به این دلایل، کوشش‌های به ظاهر راحت جهت به‌کارگیری فرآیندهای امنیت مقیاس کوچک در زیرساخت‌های مقیاس وسیع با شکست مواجه خواهند شد.

(به شکل ۱-۲ توجه کنید).

شکل ۱-۲- اختلاف بین امنیت سایبری مقیاس کوچک و بزرگ

در نتیجه، نوع جدیدی از متدولوژی حفاظتی زیرساخت‌های ملی مورد نیاز است. نوعی که در آن بهترین عناصر موجود تکنیک‌های امنیتی کامپیوتری و شبکه‌ای با چالش‌های پیچیده و منحصربه‌فرد سرویس‌های مقیاس وسیع ملی ترکیب شود.

این کتاب چنین متدولوژی حفاظتی را برای زیرساخت‌های ملی ارائه می‌نماید. بر اساس ربع قرن تجربه عملی طراحی، ساخت و عملیاتی کردن، دریافته‌ام که سیستم‌های امنیت سایبری برای حکومت و بنگاه‌های تجاری و زیرساخت‌های مصرف‌کنندگان بنا شده است و به صورت یک رشته از اصول ارائه می‌شوند که می‌توانند روی سیستم‌های جدید و موجود به کار گرفته شوند.

به علت نیازهای منحصربه‌فرد زیرساخت‌های ملی، به خصوص، اندازه، مقیاس و قلمرو عظیم آن‌ها برخی از زمینه‌های متدولوژی برای متخصصان حوزه امنیت کامپیوتری ناآشنا خواهند بود.

در حقیقت، برخی عناصر این رویکرد، مانند دیدگاه مطلوب ما یعنی "امنیت از طریق ابهام" ممکن است به نظر در تضاد با دیدگاه متداول که چگونه کامپیوترها و شبکه‌ها بایستی حفاظت شوند قرار گیرد.

تهدیدهای سایبری ملی، آسیب‌پذیری‌ها و حملات

امنیت کامپیوتری معمولی بر اساس طبقه‌بندی غالباً تکرار شده تهدیدات امنیتی که شامل محرمانگی، یکپارچگی، دسترس‌پذیری و سرقت می‌باشند بنا شده است.

در وسیع‌ترین حالت، تمام چهار نوع مختلف تهدید در زیرساخت‌های ملی کاربرد دارند و جهت حفاظت‌هایی برای مقابله با موارد زیر به طور مساوی مورد نیاز هستند.

نشت اطلاعات حساس (محرمانگی)، کرم‌هایی که روی عملیات بعضی کاربردهای حیاتی اثر می‌گذارند (یکپارچگی)، باتنت که سیستم‌های مهم را در هم می‌کوبند (دسترس‌پذیری)، شهروندانی که شناسه‌های آن‌ها افشا می‌شود (سرقت) به طور قطع تهدید دسترس‌پذیری به خدمات ملی، با توجه به طبیعت تهدید و رابطه آن با سرمایه‌های ملی، باید مهم تلقی شود؛ بنابراین، باید انتظار توجه مخصوص به تهدید دسترس‌پذیری به زیرساخت‌های ملی را داشته باشیم.

با این حال، عقلانی خواهد بود که تأیید نماییم در متدولوژی حفاظتی زیرساخت‌های ملی، باید هر چهار نوع تهدید امنیتی که در طبقه‌بندی امنیت کامپیوتری وجود دارند، رسیدگی شود.

آسیب‌پذیری‌ها مشکل‌تر از آن هستند که به یک طبقه‌بندی وابسته شوند. روشن است که در زیرساخت‌های ملی باید مسائل به خوبی شناخته‌شده‌ای همانند موارد زیر رسیدگی شود:

دستگاه‌هایی که به طور نامناسب پیکربندی شده‌اند. شبکه‌های محلی که به طور ضعیف طراحی‌شده‌اند. نرم‌افزارهای سیستمی که وصله‌های امنیتی روی آن‌ها نصب نشده است. کد برنامه‌های کاربردی نرم‌افزاری که باگ‌های قابل سو استفاده دارند و کارمندان محلی که ناراضی هستند.

پایه‌یی‌ترین آسیب‌پذیری در زیرساخت‌های ملی پیچیدگی عظیم موجود در سیستم‌های پایه‌ای زیرساخت است. این پیچیدگی چنان فراگیر است که در بسیاری از مواقع، وقایع امنیتی، زمینه‌هایی از عملکرد محاسباتی را آشکار می‌نمایند که قبلاً برای هرکسی حتی برخی مواقع برای طراحان سیستم ناشناخته بوده است.

همچنین، در برخی موارد، راه حل بهینه امنیتی وجود دارد که شامل ساده کردن و پاک کردن زیرساخت‌هایی است که به طور ضعیف فهمیده شده‌اند. این یک خبر بد است؛ زیرا بسیاری از سازمان‌ها، در ساده کردن هر چیزی نالایق و ناتوان هستند. بهترین کاری که برای به دست آوردن یک دیدگاه جامع از آسیب‌پذیری مربوط به زیرساخت ملی می‌توان انجام داد، رسیدگی به نقاط بهره‌برداری نسبی آن‌ها است.

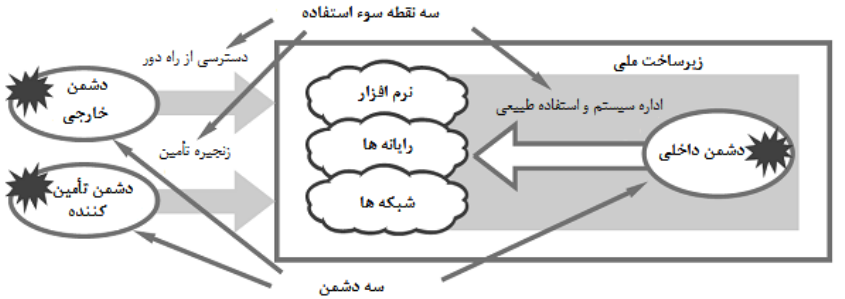
این کار را می‌توان با یک مدل مجرد از امنیت سایبری زیرساخت ملی انجام داد. این مدل شامل سه نوع دشمن بدخواه است که عبارت‌اند از:

- دشمنان خارجی (هکرهای شبکه اینترنت).
- دشمنان داخلی (افراد داخلی مورد اعتماد).
- دشمنان تأمین‌کننده (فروشندگان و شرکا).

با استفاده از این مدل، سه نقطه سو استفاده در زیرساخت ملی ظاهر می‌شود:

- دسترسی از راه دور (اینترنت و دور کاری).
- اداره سیستم و استفاده نرمال و عادی (مدیریت و استفاده از نرم‌افزار، کامپیوترها و شبکه‌ها).
- زنجیره تأمین (خرید اجناس و برون سپاری).

(به شکل ۱-۳ توجه کنید)



شکل ۱-۳- دشمنان و نقاط سواستفاده در زیرساخت ملی

وقتی این سه نقطه سو استفاده و سه نوع دشمن؛ انگیزه‌های ممکن را پیدا کنند؛ یک حمله آزمایشی یا حمله کامل به زیرساخت‌های ملی شروع می‌شود.

پنج انگیزه ممکن برای یک حمله به زیرساخت

- جنگ سایبری حمایت‌شده به وسیله یک کشور: حملات حمایت‌شده و بودجه داده‌شده به وسیله کشورهای دشمن، باید به عنوان قابل‌ملاحظه‌ترین انگیزه بالقوه فرض شوند؛ زیرا شدت قابلیت‌های دشمن و تمایل او به حمله نامحدود است.
- حمله خرابکار: انگیزه خرابکار نیز قابل ملاحظه است؛ زیرا گروه‌هایی که ترور را هدایت می‌کنند، به راحتی می‌توانند قابلیت‌ها و بودجه‌های قابل‌ملاحظه‌ای به دست آورند تا حملات قابل‌ملاحظه‌ای به زیرساخت انجام دهند.
- حملات باانگیزه تجاری: زمانی اتفاق می‌افتد که یک شرکت از حملات سایبری برای به دست آوردن مزیت‌های تجاری استفاده کند. درصورتی‌که شرکت مورد هدف کمپانی تغذیه‌کننده برخی سرمایه‌های ملی باشد. این واقعه، یک حمله به زیرساخت ملی تلقی می‌شود.

- حملات جنایی با اهداف مالی: معمول‌ترین مثال حملات جنایی با اهداف مالی، استفاده مالی گروه‌های جنایتکار از سرقت شناسه‌ها است. موارد دیگری نیز نظیر اخاذی از شرکت‌ها برای اجتناب از حملات سایبری وجود دارد.
- هک کردن: نباید فراموش کرد که بسیاری از حملات را هکرهایی انجام می‌دهند که معمولاً، جوانان شیطانی هستند که سعی می‌کنند شهرتی در جامعه هکرها به دست آورند. این از انگیزه‌های شیطانی خیلی پایین‌تر است و رهبران ملی باید سعی کنند راه‌های بهتری برای استفاده از انرژی‌های بدون حد و مرز جوانان پیدا کنند.

از هر کدام از سه نقطه سواستفاده می‌توان در یک حمله سایبری به زیرساخت‌های ملی استفاده کرد. برای مثال؛ ممکن است یک تأمین‌کننده کد یک اسب تروجان را در داخل جزیی از نرم‌افزار که یک سرمایه ملی را کنترل می‌نماید یا در داخل یک زنجیره تأمین که ضعیف طراحی شده است، قرار دهد و ممکن است یک هکر در اینترنت با بهره‌برداری از یک نقطه دسترسی حفاظت نشده در اینترنت، به داخل یک سرویس آسیب‌پذیر نفوذ نماید. همچنین ممکن است یک عضو داخل سیستم با استفاده از دسترسی مورد اعتماد که برای مدیریت سیستم یا استفاده نرمال از سیستم تعریف شده است، یک حمله ایجاد نماید. شرایط بالقوه‌ای برای یک دشمن خارجی وجود دارد که بتواند با صبر و دقت حساب‌شده نظیر استخدام در یک سازمان حمایت‌کننده زیرساخت و با فرآیند طولانی کیفیت عملکرد مورد اعتماد قرار گیرد. این احتمال وجود دارد که از نوع محدودی از اشتغال به عنوان قسمتی از یک تست و آزمایش برنامه‌ریزی‌شده استفاده شود. اگر کشور و یا گروه‌های تروریستی از حمله حمایت کنند، معمولاً با این شیوه‌ها، عمل می‌نمایند.

در هر نقطه (سوء) استفاده، آسیب‌پذیری که استفاده می‌شود، ممکن است مسئله شناخته‌شده‌ای باشد که در گزارش‌های مشاوره‌ای عمومی معتبر قبلاً گزارش شده است؛

یا مسئله اختصاصی که سازمان محلی آن را پنهان نگه داشته شده است. اولیاء امور باید یک سیستم مشورتی آسیب‌پذیری تفصیلی را جهت عموم ایجاد نمایند؛ مزایای آگاهی رسانی به افراد خوب به مراتب بیشتر از ریسک هشدار به افراد ناباب و بد است. این نتیجه سود و زیان، معمولاً زمانی اتفاق می‌افتد که بسیاری از سازمان‌ها از اطلاعات استفاده می‌نمایند و با اجرای عملیات فوری جلوی حملات را سد می‌نمایند و می‌توانند سود برند. زمانی که آسیب‌پذیری گزارش‌شده منحصربه‌فرد باشد، در آن صورت گزارش مشروح آسیب‌پذیری ممکن است غیرمسئولانه باشد؛ به خصوص اگر فرآیند اطلاع‌رسانی ما را قادر به اصلاح به موقع آسیب‌پذیری نسازد. این یک موضوع اساسی و کلیدی است؛ زیرا بسیاری از اولیاء امور حکومتی قوانین جدیدی را برای گزارش اجباری مورد نظر قرار داده‌اند. اگر اطلاعات به طور مناسبی حفاظت نشود؛ ممکن است گزارش دهی بیشتر باعث صدمه و زیان شود تا موجب سود.

۱-۱- تهدید بات‌نت [۳]

امروزه، شاید موذیانه‌ترین حمله‌ای که وجود دارد، بات‌نت باشد. به طور خلاصه، بات‌نت شامل کنترل از راه دور مجموعه‌ای از کامپیوترهای تسلیم‌شده کاربران انتهایی است که دارای ارتباط باند وسیع به اینترنت هستند. به ماشین‌های کاربران انتهایی کنترل شده بات گفته می‌شود؛ آن‌ها برای حمله به بعضی اهداف که به وسیله کنترل‌کننده بات‌نت مشخص‌شده، برنامه‌ریزی شده‌اند. متوقف کردن این حمله مشکل است؛ زیرا کامپیوتر کاربران به طور غیر کارآمدی اداره می‌شود. همچنین، هنگامی که حمله شروع می‌شود، این حمله از منابعی که در محدوده جغرافیایی، سیاسی با مرزهای ارائه‌دهندگان سرویس متفاوت پخش‌شده‌اند، انجام می‌شود؛ بدتر از آن حالتی است که در آن بات‌ها طوری پروگرام شده‌اند که فرمان حمله را از چند سیستم

کنترل‌کننده می‌گیرند. بنابراین، هر نوع کوششی برای نابود کردن یک کنترل‌کننده باعث توجه بات‌ها به کنترل‌کننده‌های دیگر می‌شود.

پنج موجودی که حمله بات‌نت را تشکیل می‌دهند؛ عبارت‌اند از:

- اپراتور بات‌نت: شخص، گروه و یا کشوری که عملیات بات‌نت را اجرا می‌کند. زمانی که از بات‌نت برای منافع مالی استفاده شود، اپراتور سود می‌برد. ابتکارهای مجریان قانون و مسئولین امنیت سایبری مشخص کرده که شناختن اپراتورهای بات‌نت کار بسیار مشکلی است. مطبوعات به خصوص در مورد گزارش شناسه احتمالی اپراتور بات‌نت ضعیف عمل کرده‌اند. معمولاً، هنگامی که مدارک حمایت‌کننده مختصری وجود دارد، حمایت بعضی را از حمله بات‌نت پیشنهاد می‌نمایند.
- کنترل‌کننده بات‌نت: مجموعه سرورهایی است که کنترل و عملیات بات‌نت را فرماندهی می‌نمایند. معمولاً این سرورها به این منظور، به طور بدخواهانه‌یی تسلیم‌شده‌اند. بسیاری از مواقع صاحبان واقعی سرورهایی که تسلیم‌شده‌اند، حتی نمی‌فهمند که چه اتفاقی افتاده است. نوع فعالیت‌هایی که کنترل‌کننده‌ها آن‌ها را هدایت می‌کنند، شامل، تمام استخدام‌ها، برقرار کردن‌ها، ارتباطات و فعالیت‌های حمله است.

  بات‌نت‌های معمولی تعداد کمی کنترل‌کننده دارند که در سراسر جهان به طریق غیر آشکاری پراکنده‌شده‌اند.
- مجموعه بات‌ها: معمولاً، به کاربران انتهایی یا کامپیوترهای شخصی با ارتباط باند پهن گفته می‌شود که به بد افزار بات‌نت آلوده‌شده‌اند. این کامپیوترها، معمولاً، متعلق به شهروندان معمولی هستند که با آن‌ها کار می‌نمایند و انتقال‌دهنده بی‌اطلاع و ندانسته در یک حمله بات‌نت

می‌باشند. زمانی که بات‌نت شامل مجموعه متمرکزی از کامپیوترهای شخصی در یک ناحیه باشد، ناظرین به اشتباه حمله را به ناحیه ارتباط می‌دهند. استفاده از دستگاه‌های هوشمند موبایل در یک بات‌نت با افزایش ظرفیت پهنای باند از گوشی به شبکه (upstream) و افزایش قدرت پردازشی گوشی‌ها رشد می‌کند.

- پایگاه نرم‌افزارهای بات‌نت: بیشتر بات‌نت ها، شامل سرورهایی هستند که نرم‌افزارهایی را ذخیره می‌کنند که می‌توانند در دوره عمر بات‌نت‌ها استفاده شوند. چنین چیزی را می‌توان معادل انبار مهمات در ارتش فرض کرد. نقاط کنترل‌کننده پایگاه نرم‌افزارهای بات‌نت، خودشان کامپیوترهای تسلیم‌شده‌ای هستند و معمولاً، اپراتورهای این سرورها از این موضوع مطلع نیستند.
- هدف بات‌نت: مکانی است که هدف حمله قرار می‌گیرد؛ معمولاً، یک وب سایت است، ولی می‌تواند هر دستگاه، سیستم و شبکه‌ای که از دید بات‌ها قابل مشاهده است هم باشد. در بسیاری از موارد، بات‌نت ها، وب سایت‌های برجسته و بحث‌برانگیز را هدف قرار می‌دهند؛ زیرا این سایت‌ها به راحتی از اینترنت قابل‌مشاهده هستند و دسترس‌پذیری به چنین سایت‌هایی اهمیت زیادی دارد و باعث افزایش قدرت نفوذ حمله‌کننده می‌گردد. به هر حال، بات‌نت‌ها می‌توانند هر سایت قابل‌مشاهده‌ای را هدف قرار دهند.

بات‌نت‌ها به این صورت عمل می‌کنند: ابتدا کنترولرها طوری برنامه‌ریزی می‌شوند که با یک پروتکل مشخص با بات‌ها ارتباط برقرار نمایند که معمولاً، این پروتکل (IRC) یا گپ رله‌ای اینترنت است. این عمل با قرار دادن بد افزار در کامپیوتر شخصی کاربران انتهایی انجام می‌شود که بات‌ها را تشکیل می‌دهند. چالش بزرگ در این مورد این است که کامپیوترهای شخصی و لپ تاپ‌ها خیلی ضعیف مدیریت می‌شوند. شگفت‌آور است

که در طول زمان، وظیفه مدیریت امنیتی برای کامپیوترهای شخصی به سمت کاربران انتهایی کشانده شده است و این به علت تجربه ضعیف کاربران باعث عدم رضایت عمومی از وظیفه امنیتی شده است. برای مثال زمانی که یک خریدار PC، کامپیوتر جدیدش را به خانه می‌آورد، احتمالاً، این کامپیوتر به وسیله خرده‌فروش کامپیوتر با نرم‌افزارهای امنیتی انباشته است. از این زمان به بعد، وظیفه حفاظت از کامپیوتر به عهده خریدار است؛ که این حفاظت؛ شامل نگهداری و به‌روز کردن دیوار آتش، سیستم کشف نفوذ، ویروس کش، نرم‌افزار ضد هرزنامه و همچنین نصب به‌روز وصله‌های نرم‌افزاری است. زمانی که این کارها درست انجام نشود، کامپیوتر ماشینی خواهد شد آسیب‌پذیر که به راحتی تبدیل به یک بات می‌شود. (غم‌انگیزتر اینکه حتی در مورد ماشین‌هایی که از نظر امنیتی به خوبی مدیریت می‌شوند، طراحان ماهر نرم‌افزارهای بات راهی برای نصب بد افزار در آن‌ها پیدا می‌کنند).

هنگامی که مجموعه‌ای از کامپیوترهای شخصی تسلیم‌شده و به صورت بات در آمدند، حمله کنترل‌کننده‌ها با ارسال یک فرمان به بات‌ها، به نحوی انجام می‌شود که آن‌ها برنامه‌ریزی‌شده‌اند. حمله ممکن است، فوراً، پس از آلوده شدن کامپیوترها (بات‌ها) انجام نشود. در حقیقت، تجربه نشان می‌دهد که بسیاری از بات‌نت‌ها مدت زمان طولانی در حالت خواب به سر می‌برند. با وجود این، در یک ترکیب بات‌نت امکان همه نوع حمله وجود دارد که شامل جلوگیری از سرویس گسترده (DDOS) نیز است. در چنین حالتی، بات‌ها می‌توانند ترافیک ورودی بسیار بیشتر از آنچه دروازه هدف بتواند بپذیرد به سمت آن بفرستند. برای مثال؛ اگر یک دروازه ورودی می‌تواند 1Gbps را بپذیرد و بات‌نت ترافیکی بیشتر از 1Gbps به سمت آن ارسال نماید، در دروازه ورودی صف و ازدحام ایجاد خواهد شد و شرایط جلوگیری از سرویس اتفاق می‌افتد.

(به شکل ۱- ۴ توجه کنید).

شکل ۱-۴- نمونه حمله DDOS از یک بات‌نت

هر مطالعه جدی کنونی امنیت سایبری، باید تهدیدات بی‌نظیری را که بات‌نت‌ها مطرح می‌کنند تأیید نماید. هر سیستم مرتبط با اینترنت نسبت به حملات DDOS که از طریق یک بات‌نت منشأ گرفته، نسبت به قطعی عمده آسیب‌پذیر است. شرایط فیزیکی دلسرد کننده است؛ به این معنی که بات‌نت می‌تواند 500Kbps از ظرفیت خروجی هر بات (که معمولاً، اجازه محاسبات و ارتباطات شبکه‌ای را می‌دهد) دزدیده و تنها با سه بات یک ارتباط T1 هدف را ساقط نماید. با این منطق، از دید نظری ۱۶۰۰۰ بات برای پر کردن یک ارتباط 10Gbps مورد نیاز خواهد بود. به علت اینکه هزاران بات‌نت موجود در اینترنت حداقل دارای همین اندازه (۱۶۰۰۰ یا بیشتر) هستند، تهدید ناشی از بات‌نت آشکار می‌شود. به‌هرحال بسیاری از بات‌نت‌های فعلی نظیر STORM و Conflicker بسیار بزرگ‌تر هستند و از چند میلیون بات تشکیل‌شده‌اند. بنابراین، تهدید نسبت زیرساخت‌های ملی شدید و فوری است.

۱-۲- اجزا متدولوژی امنیت سایبری ملی

متدولوژی پیشنهادی ما برای حفاظت از زیرساخت‌های ملی با ۱۰ اصل طراحی و عملیات پایه‌ای ارائه می‌شود. پیامد استفاده از این اصول به عنوان راهنما برای بهبود

اجزا زیرساخت‌های موجود و ساخت اجزا جدید، رسیدن به نتایج امنیتی مطلوبی است که شامل ریسک کمتر از بات‌نت‌ها خواهد بود. این متدولوژی به هر چهار نوع تهدید امنیتی به زیرساخت‌های ملی اشاره می‌کند. باهر سه نوع دشمن زیرساخت‌های ملی و همچنین، با سه نقطه سو استفاده که در مدل زیرساخت ملی در مورد آن بحث شد، برخورد می‌نماید. از لیست اصول در متدولوژی می‌توانید به عنوان راهنمای باقی‌مانده این فصل و همچنین، به عنوان رئوس مطالب برای فصل‌های باقی‌مانده کتاب استفاده کنید.

- ✓ فصل ۲: فریب دادن- تبلیغ علنی استفاده از فریب دادن برای دشمنان ایجاد شبهه می‌نماید، زیرا آن‌ها نمی‌دانند که مسئله کشف‌شده واقعی است یا یک تله است. روش رایج‌تر استفاده از فریب دادن پنهانی است، که اگر نفوذکننده در تله افتاده باشد، اجازه تجزیه و تحلیل زمان واقعی رفتار دشمن را می‌دهد. برنامه‌های حفاظت از زیرساخت‌های ملی باید شامل استفاده مناسب از فریب دادن، به خصوص کاهش ریسک شرکای بدخواه و تأمین‌کنندگان (تجهیزات) باشد.
- ✓ فصل ۳: جداسازی- امروزه، جدا کردن شبکه، با دیوار آتش انجام می‌شود. برنامه‌های حفاظت زیرساخت‌های ملی احتیاج به سه تغییر مخصوص دارند. زیرساخت‌های ملی باید شامل دیواره‌های آتش مبتنی بر شبکه برای شبکه‌های بک بن با ظرفیت بالا جهت جلوگیری از حملات DDOS و دیوارهای آتش داخلی جهت جدا کردن شبکه داخلی از زیرساخت و کاهش مخاطره و ریسک خرابکاری و بالأخره پیکربندی بهتر ویژگی‌های دیواره آتش برای کاربردهای خاص نظیر پروتکل‌های سیستم‌های کنترل و به دست آوردن داده‌ها (SCADA) باشند.[۴]

- ✓ فصل ۴: تنوع- نگهداری و حفظ تنوع در محصولات، خدمات و فناوری‌های حمایت‌کننده زیرساخت‌های ملی، شانس این را کاهش می‌دهد که از یک ضعف مشترک بتوان استفاده کرد و حملات آبشاری تولید نمود. برنامه وسیعی از خریدهای هماهنگ شده و مدیریت تأمین‌کنندگان برای رسیدن به سطح مطلوبی از تنوع ملی برای تمام سرمایه‌ها مورد نیاز است. این مسئله مشکل است؛ زیرا تمام ابتکارها برای خرید محصولات تکنولوژی اطلاعات که مبتنی بر قیمت محصول باشد، بر اساس کمینه کردن تنوع در زیرساخت‌ها طراحی‌شده‌اند و این در تضاد با به‌کارگیری تنوع در زیرساخت ملی است.
- ✓ فصل ۵: اشتراک- استفاده سازگار از بهترین شیوه‌های عمل امنیتی در اداره زیرساخت‌های ملی تضمین می‌کند که هیچ جزیی از آن به طور ضعیف مدیریت نشده است و کاملاً بدون حفاظ نیست. برنامه‌های ملی انتخاب استانداردها و اعتبارسنجی ممیزی، به خصوص با تأکید بر برنامه‌های یکنواخت ساده‌سازی مورد نیاز است. این برنامه‌ها می‌تواند شهروندان و کاربران انتهایی را شامل شود. هرگز نباید بر سطح بالایی از مراعات کردن امنیتی در محدوده وسیعی از جمعیت تکیه داشته باشد.
- ✓ فصل ۶: عمق- استفاده از دفاع در عمق در زیرساخت‌های ملی، تضمین می‌کند که هیچ سرمایه حیاتی فقط وابسته به یک لایه امنیتی نیست؛ بنابراین، اگر لایه امنیتی شکسته شود، لایه دیگری برای کاهش اثرات حمله وجود دارد. تجزیه و تحلیل‌های ملی برای اطمینان از اینکه تمام سرمایه‌های حیاتی حداقل با دو لایه یا بیشتر حفاظت می‌شوند لازم است.
- ✓ فصل ۷: احتیاط- استفاده از احتیاط شخصی در تسهیم اطلاعات مربوط به سرمایه‌های ملی یک روش عملی است که آن را بسیاری از خبرگان امنیت کامپیوتری به آسانی نمی‌پذیرند؛ زیرا این موضوع در تناقض با

دیدگاه محبوب "امنیت از طریق ابهام" است. حفاظت زیرساخت‌های با مقیاس وسیع نمی‌تواند به خوبی انجام شود، مگر اینکه فرهنگ ملی احتیاط و محرمانه بودن پرورش یابد. بدیهی است که چنین احتیاطی، هرگز، نباید برای پنهان سازی شیوه‌های عمل غیراخلاقی و غیرقانونی به کار گرفته شود.

- ✓ فصل ۸: جمع‌آوری- گردآوری اطلاعات لاگ ممیزی، جزیی لازم از یک طرح امنیتی زیرساخت است. این عمل مسائل محرمانگی، اندازه و مقیاس را ایجاد می‌کند که در کامپیوترهای کوچک و محیط شبکه دیده نمی‌شود. حفاظت زیرساخت‌های ملی به رویکردی برای جمع‌آوری اطلاعات نیاز دارد که شهروندان آن را بپذیرند و بتواند تجزیه و تحلیل امنیتی نیز ارائه دهد.
- ✓ فصل ۹: همبسته سازی- پایه‌یی‌ترین تکنیک تجزیه و تحلیل امنیت سایبری، همبسته سازی است؛ اما روش‌های جدید حمله مثل باتنت‌ها استفاده از آن را برای شاخص‌های مرتبط با حمله به طور فزاینده‌ای پیچیده می‌نماید. همبسته سازی باید در سطح ملی و با استفاده از تمام منابع قابل‌دسترسی، بهترین تکنولوژی و الگوریتم‌های در دسترس انجام شود.

  همبسته سازی اطلاعات در یک حمله باتنت، یکی از کارهای پر چالش در امنیت سایبری است.
- ✓ فصل ۱۰: آگاهی- حفظ آگاهی موقعیتی در حفاظت زیرساخت‌های مقیاس وسیع نسبت به امنیت در کامپیوترها و شبکه‌های سنتی مهم‌تر است؛ زیرا این آگاهی به هماهنگی وجوه زمان واقعی اجزا متعددی از زیرساخت کمک می‌کند. یک برنامه آگاهی موقعیتی ملی باید در سیستم

امنیتی قرار گیرد تا تصمیم سازی مناسب مدیریت برای سرمایه‌های ملی را تضمین نماید.

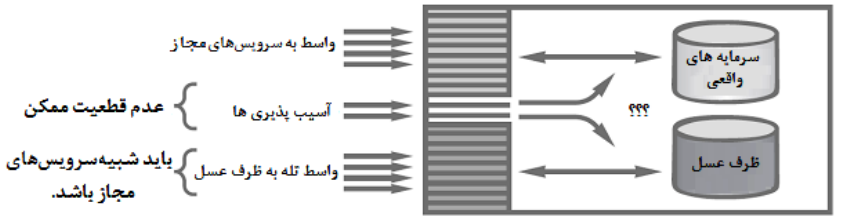
- ✓ فصل ۱۱: واکنش- پاسخ‌گویی به وقایع برای حفاظت از زیرساخت‌های ملی بسیار مشکل است و معمولاً، به علت درگیر شدن وابستگی‌های پیچیده و تعامل بین گروه‌های مختلف تجاری و دولتی اتفاق می‌افتد. پاسخ‌گویی در سطح ملی می‌تواند به بهترین وجه انجام شود که بر نشانه‌های زودهنگام متمرکز باشد نه بر وقایعی که از قبل به سرمایه‌های ملی صدمه زده‌اند.

در ادامه این فصل، در مورد استفاده از هر کدام از اصول فوق در مورد استفاده برای امنیت شبکه‌ها و کامپیوترها و همین طور مزایای مورد انتظار برای حفاظت زیرساخت‌های ملی بحث می‌کنیم.

۱-۲-۱- فریب دادن

اصل فریب دادن شامل ارائه عملکردهای گمراه‌کننده یا اطلاعات اشتباه در زیرساخت‌های ملی به منظور فریب دشمن است. نقشه کار ارائه یک منظر از عملکردهای زیرساخت ملی است که ممکن است شامل سرویس‌ها یا اجزا واسطی باشد که تنها برای وانمود کردن وجود دارند. دانشمندان علم کامپیوتر این عملکرد را ظرف عسل می‌نامند. استفاده از فریب دادن در زیرساخت‌های ملی بسیار فراتر از این دیدگاه متعارف پیش می‌رود. از فریب دادن می‌توان برای حفاظت در مقابل بعضی انواع حملات سایبری استفاده کرد که هیچ نوع روش امنیتی دیگر با آن‌ها مقابله نخواهد کرد، آژانس‌ها مجری قانون سال‌هاست از فریب دادن به طور مؤثری استفاده می‌کنند و با جعل شناسه یک کاربر انتهایی که به آن‌ها گزارش شده است، برای گرفتن مجرمان سایبری اقدام می‌نمایند. با وجود چنین موفقیت روشنی، هنوز جامعه امنیت سایبری باید فریب دادن را به عنوان یک ابزار حفاظتی بپذیرد.

فریب دادن در محاسبات شامل یک لایه از عملکردهای دام گونه و زیرکانه طراحی‌شده‌ای است که به طور راهبردی در واسط‌های داخلی و خارجی برای سرویس‌ها جاسازی شده است. به عبارت ساده‌تر، فریب دادن شامل عملکردهای قلابی جاسازی شده در واسط‌های واقعی می‌باشد. برای مثال؛ یک لینک تله که به طور عمدی روی یک وب سایت جاسازی شده باشد، که باعث هدایت یک نفوذگر به داخل محیطی می‌شود که برای برجسته نمودن رفتار او طراحی شده است. زمانی که فریب دادن آشکار باشد، باعث ایجاد ابهام برای دشمن در استفاده از آسیب‌پذیری‌های واقعی می‌گردد؛ زیرا دشمن گمان می‌کند که این نقطه ورودی یک دام است. زمانی که فریب دادن پنهان باشد، که معمولاً این گونه است، به عنوان پایه‌ای جهت تجزیه و تحلیل فارنسیک زمان واقعی رفتار دشمن به خدمت گرفته می‌شود. در هر کدام از دو حالت، نتیجه یک واسط برای عموم است که شامل سرویس‌های واقعی و تله‌های ظرف عسل عمدی و آسیب‌پذیری قابل سواستفاده غیرقابل اجتنابی هستند که در تمام واسط‌های قابل و بااهمیت وجود دارند. (به شکل ۱-۵ توجه کنید)



شکل ۱-۵- اجزا یک واسط با فریب دادن

تاکنون، فقط تست‌های ناچیزی از فناوری ظرف عسل گزارش‌شده که معمولاً، در قالب فعالیت‌های تحقیقاتی بوده است. هیچ گزارشی در استفاده روزبه‌روز از فریب دادن، به عنوان جزیی ساختاری از برنامه امنیت یک بنگاه اقتصادی حقیقی، ارائه نشده است.

در حقیقت، بیشتر برنامه‌های امنیتی شرکت‌ها و آژانس‌های حکومتی و زیرساخت‌های ملی چنین عملکردی ندارند. دانشمندان علوم کامپیوتر علاقه کمی به این نوع امنیت نشان داده‌اند؛ تعداد کم مقالات و کتبی که در این مبحث وجود دارد، درستی این مطلب را معلوم می‌کند. این عدم علاقه ممکن است ناشی از ناراحتی مرتبط با استفاده از کامپیوتر برای گمراه کردن باشد. یک توضیح دیگر ممکن است به علت غیر کارآمد بودن نسبی فریب دادن در مقابله با تهدید بات‌نت باشد که امروزه، مهم‌ترین مسئله امنیتی در اینترنت است. بدون در نظر گرفتن علت، این تمایل به اجتناب از استفاده از فریب مایه تأسف است؛ زیرا بسیاری از حملات مثل نفوذ زیرکانه افراد مورد اطمینان داخل سازمان و اسب‌های تروجانی که تأمین‌کنندگان به طور بد بدخواهانه‌یی در داخل نرم‌افزارهای تحویلی قرار می‌دهند از راه دیگری نمی‌توانند کشف و رفع گردند.

مستقیم‌ترین سود فریب دادن قادر ساختن تجزیه و تحلیل فارنسیک فعالیت‌های نفوذگر است. با استفاده از ظرف عسل می‌توان بینش منحصر به فردی از روش‌های حمله با مشاهده این که به صورت زمان واقعی چه وقایعی در حال انجام است به دست آورد. واضح است یک چنین فریب دادنی در حالت پنهان و مخفی که برای نفوذگر ناشناخته است به بهترین وضع کار خواهد کرد؛ زیرا اگر نفوذگر پی ببرد که بعضی از نقاط استفاده از آسیب‌پذیری‌ها قلابی است، هیچ سواستفاده‌ای اتفاق نخواهد افتاد. پیشگامان استفاده از ظرف عسل؛ کلیف اِستول، بیل چسویک و لانس اسپیتزنر، قسمت اعظم تجربه‌های گزارش‌شده در فارنسیک زمان واقعی را با استفاده از ظرف عسل ارائه کرده‌اند. آن‌ها همگی معتقدند که سخت‌ترین کار، باورپذیر کردن تله است. گفتنی است که وصل کردن یک ظرف عسل به سرمایه‌های واقعی ایده‌ای وحشتناک است.

یک سود دیگر فریب دادن، معرفی این ایده زیرکانه است که بعضی از آسیب‌پذیری‌ها کشف‌شده ممکن است تله‌هایی باشند که به صورت تعمدی نصب‌شده‌اند. روشن است چنین رویکردی زمانی کارآمد خواهد بود که استفاده از فریب دادن پنهانی نباشد؛ یعنی دشمن باید بداند که فریب دادن یک تکنیک تصویب و پذیرفته شده است که برای

حفاظت به کار می‌رود. بنابراین، مزیت عمده آن این است که راهی که قبلاً یک درِ باز برای نفوذگر بوده است، شناخته‌شده و برای نفوذگر نظیر یک تله به نظر خواهد آمد. یک مفهوم عمیق که شاید برای بحث آزاد مناسب باشد، این است که آیا به کاربردن عبارت تلویحی فریب دادن، ریسک را کاهش خواهد داد. برای مثال؛ ممکن است تأمین‌کنندگان کمتر به پذیرش ریسک جهت تعبیه اسب تروجان تمایل داشته باشند، اگر سازمان‌های خریدار محصول، یک برنامه توسعه و تحقیق جهت آزمایش و وارسی نرم‌افزار در مقابله با این نوع حمله را تبلیغ کنند.

۱-۲-۲- جداسازی

اصل جداسازی شامل اجرای محدودیت‌های سیاست‌های دسترسی روی کاربران و منابع در یک محیط محاسباتی است. محدودیت‌های سیاست‌های دسترسی باعث جداسازی دامنه‌هایی می‌شود که معمول‌ترین مفهوم ساختار امنیتی را دارند و امروزه، از آن‌ها استفاده می‌شود. این خبر خوبی است؛ زیرا ایجاد دامنه‌های جدای مبتنی بر سیاست‌های دسترسی برای حفاظت زیرساخت‌های ملی ضروری است. امروزه، بیشتر شرکت‌ها برای ایجاد خط مرزی امنیتی پیرامون شرکت فرضی خود از دیوار آتش استفاده می‌کنند و تصمیمات دسترسی در مجموعه‌هایی از قواعد مربوطه جاسازی شده‌اند. این استفاده از دیوار آتش شرکت‌ها برای جداسازی با چندین تکنیک دیگر دسترسی تکمیل می‌شود که عبارت‌اند از:

- تأیید هویت و مدیریت شناسه: این روش‌ها برای معتبر سازی و مدیریت شناسه‌هایی به کار گرفته می‌شوند که تصمیمات جداسازی بر روی آن‌ها گرفته شده است. در هر بنگاه اقتصادی به کاربردن این روش‌ها ضروری است؛ اما برای امنیت زیرساخت‌ها نمی‌توان تنها به آن‌ها متکی بود. برای مثال؛ افراد بدخواه داخل سازمان در چنین سیستمی مجاز به استفاده از

منابع خواهند بود. همچنین، تأیید هویت و مدیریت شناسه تأثیری بر حملات خارجی نظیر DDOS نخواهند داشت.

- کنترل‌های دسترسی منطقی: کنترل‌های دسترسی ذاتی موجود در سیستم‌های عامل و کاربردها تا اندازه‌ای جدایی را ایجاد می‌نمایند؛ اما برای سیستم‌هایی که عناصر داخلی تسلیم‌شده دارند، ضعیف هستند. همچنین آسیب‌پذیری‌های اساسی در کاربردها و سیستم‌های عامل، معمولاً می‌توانند برای اختلال در روش‌های کنترل دسترسی به کار گرفته شوند.
- کنترل‌های LAN: لیست‌های کنترل دسترسی در اجزا شبکه‌های محلی می‌توانند جداسازی مبتنی بر اطلاعاتی نظیر آدرس پروتکل اینترنت (IP) یا آدرس کنترل دسترسی رسانه (MAC) را ارائه نمایند. در این مورد آن‌ها خیلی شبیه دیوار آتش هستند؛ اما قلمرو خود را فراتر از یک تکه جدا (LAN) توسعه نمی‌دهند.
- دیوار آتش: دیوارهای آتش، به خصوص برای زیرساخت‌هایی با مقیاس وسیع مفید هستند؛ زیرا یک شبکه را از شبکه دیگر جدا می‌سازند. امروزه، هر ارتباط مبتنی بر اینترنت حتماً با یک نوع از عملکرد دیوار آتش حفاظت می‌شود. این رویکرد به خصوص در اولین سال‌های اینترنت خوب عمل می‌کرد که تعداد ارتباطات اینترنتی به سازمان‌ها کم بود. دیوار آتش، هنوز هم حتی با وجود ارتباطات بیشتر گروه‌ها به اینترنت مفید است. در نتیجه، زیرساخت‌های ملی باید به تداوم استفاده از دیوار آتش برای حفاظت از مرزهای محیطی شناخته‌شده دروازه‌های ورودی به اینترنت ادامه دهند.

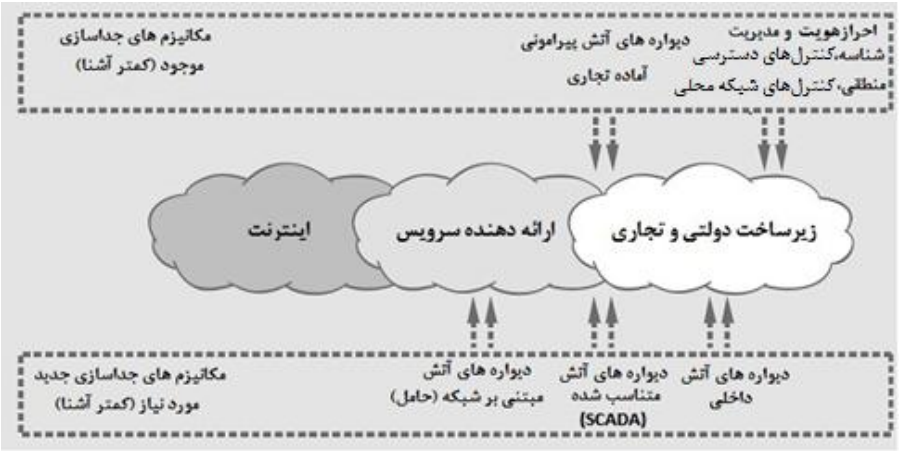
با توجه به مقیاس گسترده و پیچیدگی مرتبط با زیرساخت‌های ملی، سه روش ارتقا مخصوص جداسازی مورد نیاز است که همگی آن‌ها توسعه‌های مفهوم دیوار آتش هستند.

پیشرفت‌های مورد نیاز جداسازی، برای حفاظت از زیرساخت‌های ملی

۱- استفاده از دیوارهای آتش مبتنی بر شبکه قطعاً برای بسیاری از کاربردهای زیرساخت ملی مورد نیاز است، به خصوص کاربردهایی که نسبت به حمله DDOS از اینترنت آسیب‌پذیر هستند. این استفاده از میانجی‌های مبتنی بر شبکه اگر ارائه‌دهنده‌های خدمات در بهره‌برداری از دیوار آتش درگیر باشند، می‌توانند از مزایای بک بن‌های ظرفیت بالای شبکه استفاده کنند.

۲- استفاده از دیوارهای آتش برای جداسازی و ایزوله کردن اجزا زیرساخت از یکدیگر یک تکنیک اجباری برای ساده کردن پیاده‌سازی سیاست‌های کنترل دسترسی یک سازمان است. زمانی که افراد داخل سازمان، مقاصد بد خواهانه‌یی داشته باشند، دیوارهای آتش داخلی ابزارهای سو استفاده آن‌ها را محدود خواهند کرد.

۳- استفاده از دیوارهای آتش آماده تجاری، به خصوص برای کاربردهای SCADA به تنظیم دیوار آتش برای احتیاجات پروتکلی منحصربه‌فرد احتیاج دارد. برای حفاظت از زیرساخت‌های ملی مقاوم‌سازی استفاده از ابزارهای عمومی، تجاری و آماده که برای کار خاصی بهینه نشده‌اند، پذیرفته نمی‌شوند. (به شکل ۱-۶ توجه کنید).



شکل ۱-۶- پیشرفت‌های دیوار آتش برای زیرساخت ملی

با ظهور محاسبات اَبری، بسیاری از مدیران امنیتی بنگاه‌های تجاری و آژانس‌های دولتی به این نتیجه رسیده‌اند که باید مزایای پردازش دیوارهای آتش مبتنی بر شبکه را تأیید نمایند. این روند مقیاس‌پذیر است و با پیچیدگی‌های کنترل ناپذیری که معمولاً، در زیرساخت‌های ملی یافت می‌شود، به خوبی مقابله می‌نماید. امروزه، بسیاری از سرمایه‌های ملی با قرار دادن دیوار آتش در صدها یا هزاران نقطه مناسب و حیاتی امن می‌شوند. این رویکرد مقیاس‌پذیر نیست و ما را به سمت احساس امنیت کاذبی هدایت می‌کند. باید بدانیم که دیوار آتش تنها دستگاهی نیست که مشکل مقیاس‌پذیری دارد. سیستم‌های دیگری نظیر سیستم‌های مقابله بانفوذ IDS، فیلترهای ویروس کش، سیستم‌های مدیریت تهدید و فیلترهای مقابله با امتناع از سرویس نیز برای کار کردن مناسب در زیرساخت ملی احتیاج به رویکردی مبتنی بر شبکه دارند.

مسئله دیگری که در زیرساخت‌های ملی فعلی وجود دارد، نداشتن جدایی نسبی ساختاری به‌کاررفته در یک شبکه داخلی و مورد اعتماد است. بسیاری از مهندسان امنیتی به خوبی می‌دانند که از سیستم‌های بزرگ می‌توان با تقسیم آن‌ها به سیستم‌های

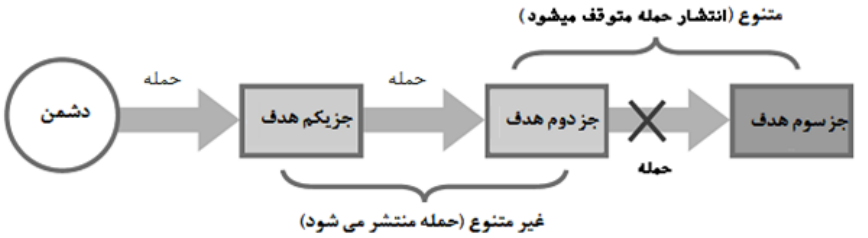
کوچک‌تر حفاظت کرد. دیوارهای آتش و مسیریاب‌های فیلتر کننده بسته می‌توانند برای جداسازی شبکه یک بنگاه تجاری به دامنه‌های قابل مدیریت به‌کاربرده شوند. متأسفانه شیوه عمل فعلی در حفاظت از زیرساخت‌های ملی به ندرت شامل یک رویکرد منضبط برای جداسازی سرمایه‌های داخلی است. این مسئله تأسف‌برانگیز است؛ زیرا به نفوذگر اجازه می‌دهد به چشم‌انداز وسیع‌تری از زیرساخت سازمانی دسترسی داشته باشد. این تهدید زمانی خطرناک‌تر می‌شود که دیوار آتش برای کاربردهایی نظیر SCADA که احتیاج به حمایت پروتکل‌های خاص دارند، بهینه نشده باشد.

۱-۲-۳- تنوع

اصل تنوع شامل انتخاب و استفاده از فناوری‌ها و سیستم‌هایی است که به طور عمدی در راه‌های پایه‌ای و اساسی متفاوت هستند. این تفاوت‌ها می‌تواند شامل منبع فناوری، زبان برنامه‌نویسی، سکوی محاسباتی، محل فیزیکی و فروشنده محصول باشد. برای زیرساخت‌های ملی، تحقق چنین تنوعی احتیاج به یک برنامه هماهنگ خرید دارد که ترکیب مناسبی از فناوری‌ها و فروشندگان را تضمین کند. هدف از واردکردن چنین تفاوت‌هایی، ایجاد عمدی معیار تعامل ناپذیری است که حمله نتواند به راحتی از یک جز به جز دیگر سیستم به صورت آبشاری، با استفاده از یک آسیب‌پذیری مشترک بین اجزا منتقل شود. تحقیقات نشان داده است که حتی در محیط‌های متنوع، ممکن است یک ابزار حمله (مثل کرم یا ویروس) به طور آبشاری منتشر شود؛ اما در صورتی که مشخصات تنوع افزایش یابد، احتمال انتشار کاهش خواهد یافت.

این مفهوم تا اندازه‌ای بحث‌برانگیز است؛ زیرا بسیاری از نظریه‌های علوم کامپیوتری و شیوه‌های عمل فناوری اطلاعات در چند دهه گذشته، متمرکز بر بیشینه کردن تعامل بین فناوری‌ها بوده است و این ممکن است به بیان عدم نسبی توجه به ملاحظات تنوع که در این زمینه‌ها می‌شود، کمک نماید. همان طور که انتشار امراض با تنوع اکوسیستم‌های زیستی کاهش می‌یابد، می‌توان با تنوع فناوری‌ها، اثر حملات سایبری

راهم روی زیرساخت‌های ملی کاهش داد. مسئله‌ای که از یک محدوده زیرساخت شروع می‌شود و هدف آن انتشار خودکار است، تنها با وجود درجه‌ای از تعامل پذیری موفق خواهد بود. اگر فناوری‌ها به اندازه کافی گوناگون باشند، انتشار حمله کاهش‌یافته و یا حتی متوقف خواهد شد؛ بنابراین مدیران سرمایه‌های ملی مجبورند برای تحقق منافع امنیتی، به ابزارهای ایجاد تنوع توجه کنند. (به شکل ۱-۷ توجه کنید).



شکل ۱-۷- واردکردن تنوع در زیرساخت ملی

پیاده‌سازی تنوع در زیرساخت‌های ملی به چند دلیل مشکل است. اول اینکه باید تأیید کرد چشم‌انداز تجاری سیستم‌عامل کامپیوترهای شخصی تنها به وسیله یک شرکت عمده تجاری در بیشتر محیط‌های بنگاه‌های تجاری و دولتی مورد تسلط قرار گرفته است (میکروسافت). احتمالاً، این وضع در آینده نزدیک نیز تغییر نخواهد کرد. بنابراین، ابتکارات امنیتی زیرساخت ملی، باید اکو تنوع را در چشم‌انداز کامپیوترهای شخصی بپذیرند. مشخصات نرم‌افزارهای سیستم‌عامل سرورهای کامپیوتری از نظر تنوع کمی بهتر است، اما تعداد محدودی از آن‌ها در دسترس است. امروزه، سیستم‌عامل در گوشی‌های موبایل تنوع قابل‌توجهی را ارائه می‌کند؛ کمکی نمی‌توان کرد، جز انتظار دیدن روندی به سمت یکپارچه شدن بیشتر.

ثانیاً، تنوع باهدفی که در بیشتر سازمان‌ها برای ساده نمودن رابطه بین تأمین کنندگان و فروشندگان وجود دارد در تضاد است. یعنی اگر یک تکنولوژی مشترک در

سراسر سازمان به کار گرفته شود مخارج روزانه نگهداری، مدیریت و آموزش، کمینه خواهد شد. همچنین، با خرید به صورت عمده از یک فروشنده شرایط خرید بهتری دریافت خواهید داشت. در مقابل، استفاده از تنوع باعث کاهش میزان سرویس می‌شود که در سازمان ارائه می‌گردد. برای مثال؛ فرض کنید که یک ارائه‌دهنده سرویس‌های اینترنتی خدمات شبکه‌ای امن و قابل‌اعتمادی را به یک سازمان پیشنهاد می‌دهد. شاید قابلیت اعتماد حتی با معیارهای دسترس‌پذیری کمّی قابل‌ملاحظه‌ای اندازه‌گیری شود. اگر سازمان متعهد به ایجاد تنوع باشد، ممکن است از یک ارائه‌دهنده سرویس با سطح پایین‌تری از قابلیت اطمینان نیز استفاده کند.

با وجود این اشکالات، تنوع، منافع بی‌چون و چرایی را برای زیرساخت‌های با مقیاس وسیع همراه خواهد داشت. بنابراین، یکی از چالش‌های عمده در حفاظت از زیر ساخت‌های ملی شامل راه‌هایی برای یافتن محصولات و سرویس‌هایی با تنوع فناوری، بدون افزایش مخارج و از دست دادن ارجحیت‌های کسب‌وکار با فروشندگان است.

۱-۲-۴- ثبات

- اصل ثبات شامل توجه یکنواخت به بهترین شیوه‌های عمل امنیتی در سراسر اجزا زیرساخت‌های ملی است. مشخص کردن اینکه کدام شیوه‌های عمل مربوط به چه سرمایه ملی است، احتیاج به ترکیبی از دانش محلی در مورد آن سرمایه و همین طور دانش با قلمرو وسیع‌تری از آسیب‌پذیری‌های امنیتی در حفاظت زیرساخت‌های عمومی دارد. بنابراین؛ کامل‌ترین رویکرد برای ثبات، استفاده از استانداردهایی مانند کنترل‌های Sarbanes-Oxley در ایالات‌متحده امریکا است که باسیاست محلی امنیتی میزان شده و با مأموریت‌های آن سازمان ترکیب شده باشد. این ترکیب، سازمان‌هایی را که مسئولیت طراحی و عملیات زیرساخت‌های ملی را به عهده‌دارند، متعهد می‌کند که سیاست امنیتی محلی نیز داشته باشند.

تعجب‌آور است که امروزه، بعضی گروه‌های بزرگ چنین سیاست‌های امنیتی ندارند.

بهترین شیوه‌های عملی که مربوط به زیرساخت‌های ملی هستند؛ شامل متدولوژی‌های چرخه عمر نرم‌افزارهای به خوبی تعریف‌شده، تفکیک کنترل‌های کارها در اداره سیستم، مدیریت تهدید تمام اطلاعات امنیتی جمع‌آوری شده، آموزش‌های آگاهی امنیتی برای تمام مدیران سیستم، پیکربندی عملیاتی و تنظیمات عملیاتی برای مدیریت زیرساخت‌ها و استفاده از ابزارهای امنیتی نرم‌افزاری برای اطمینان از مدیریت یکپارچه مناسب هستند. بیشتر متخصصان امنیتی در مورد بهترین شیوه‌های عمل که باید در مجموعه عمومی نیازهای امنیتی قرار گیرد، توافق دارند. به عنوان گواه، این‌ها هسته عمومی شیوه‌های عمل در هر استاندارد امنیتی هستند. بنابراین، توجه به ثبات که یکی از اصول توصیه‌شده ما است، یکی از اصولی است که کمتر بحث‌برانگیز است.

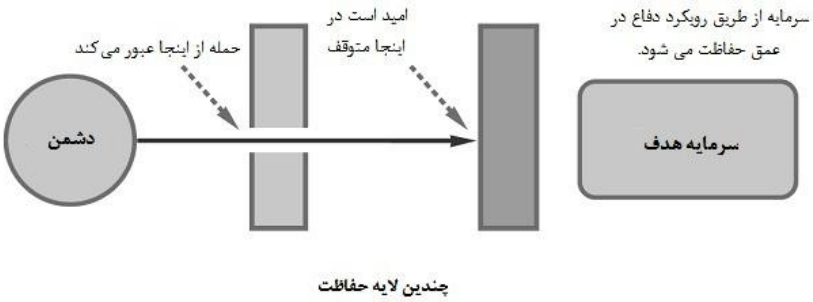
بزرگ‌ترین چالش در اجرای بهترین شیوه‌های عمل ثبات در سراسر زیرساخت شامل ممیزی است. یک فرآیند معمولی ممیزی را باید شخص سوم مستقلی انجام دهد که بتواند با تجزیه و تحلیل زیرساخت مورد هدف، سازگاری با استانداردهای مطلوب را مشخص نماید. معمولاً نتیجه ممیزی یک نمره یا امتیاز عددی است که به صورت وسیع گزارش می‌شود و از آن برای تصمیم‌گیری‌های مدیریتی استفاده می‌کنند. در ایالات‌متحده امریکا، آژانس‌های حکومتی فدرال در مقابل یک استاندارد امنیت سایبری ممیزی می‌شوند. این استاندارد FISMA یا قانون مدیریت امنیت اطلاعات فدرال نامیده می‌شود. ممیزی ما را به سمت پوشش اصلاح‌شده بهترین شیوه‌های عمل هدایت می‌کند، ولی، معمولاً مشکلاتی نیز دارد. برای مثال؛ بسیاری از عملیات ممیزی به صورت ضعیف انجام می‌شود که باعث گیجی، سردرگمی و گرفتن تصمیمات نامناسب مدیریتی می‌گردد. همچنین با تأکید بر رتبه‌بندی عددی، بسیاری از آژانس‌ها به جای تمرکز بر شیوه‌های عمل خوب مدیریتی، به رتبه‌بندی خود توجه می‌کنند.

امروزه، سازمان‌های مسئول حفاظت از زیرساخت‌های ملی، از انواع مختلفی از ممیزی‌های امنیتی بهره می‌گیرند. ساده کردن این استانداردها خوب است. به موارد دیگری نیز باید توجه شود که شامل بهبود انواع آموزش‌های عمومی است که باید برای مدیران امنیتی ارائه شود و همین طور شیوه‌های عمل قبلی در حفاظت از زیرساخت‌های ملی در استانداردهای عمومی ممیزی، باید مورد توجه قرار گیرد. آشکارترین ملاحظات عملی جهت زیرساخت‌های ملی، توافق ملی در مورد این است که استانداردهایی را باید برای تعیین صلاحیت محافظت از دارایی‌های ملی به کاربرد. به دست آوردن یک توافق وسیع در بین تمام شرکای ملی مشکل است. مسئله دیگر، اشتراک در پیکربندی عملیاتی زیرساخت‌های ملی است. احتمالاً اگر یک عنصر داخلی تسلیم‌شده بخواهد با یک پیکربندی ناجور نصب‌شده به مقاصد بد خواهانه خود برسد، این اشتراک در پیکربندی عملیاتی زیرساخت‌های ملی باعث کاهش شانس او می‌گردد.

۱-۲-۵- عمق

اصل "عمق" شامل استفاده از چندین لایه امنیتی محافظ برای حفاظت از سرمایه‌های زیرساخت ملی است. این لایه‌ها، سرمایه‌ها را از حملات داخلی و خارجی با رویکرد شناخته‌شده دفاع در عمق حفظ می‌کنند. وجود چندین لایه امنیتی شانس این را افزایش می‌دهد که حداقل یکی از لایه‌ها در مقابل حمله مؤثر باشد بنابراین، ریسک حمله کاهش می‌یابد. از دیدگاه مهندسی سنتی، این وضعیت تا حدودی ناقص به نظر می‌رسد. برای مثال؛ مهندسان عمران، هرگز، با طراحی یک سازه که در آن چندین ستون معیوب برای نگهداری بار طراحی‌شده‌اند، به امید اینکه یکی از ستون‌ها بار را نگاه می‌دارد، راحت نخواهند بود. متأسفانه، متخصصان امنیت سایبری انتخاب دیگری به جز اتکا به این مفهوم معیوب ندارند و شاید این به علت عدم بلوغ نسبی امنیت به عنوان یک رشته مهندسی باشد.

شاید بپرسید که چرا عمق، چنین نیاز مهمی است؛ زیرا امروزه، که اجزا زیر ساخت‌های ملی به وسیله نرم‌افزار کنترل می‌شوند؛ وضعیت کنونی مهندسی نرم‌افزار، وضعیتی ناپیمودنی و گرداب مانند است. در مقایسه با دیگر انواع مهندسی، مهندسی نرم‌افزار تنها موردی است که خلق محصولاتی را با علم به معیوب بودن آن‌ها می‌پذیرد. نتیجه اینکه تمام نرم‌افزارهای معیوب دارای آسیب‌پذیری قابل سو استفاده هستند؛ بنابراین، ایده ایجاد چندین لایه دفاع امنیتی اجتناب‌ناپذیر است. گفتنی است که درجه تنوع در این لایه‌ها اثر مستقیم در کارایی آن‌ها خواهد داشت. (به شکل ۱-۸ توجه کنید).



شکل ۱-۸- امنیت زیرساخت ملی از طریق دفاع در عمق

برای بیشینه کردن سودمندی لایه‌های دفاعی در زیرساخت‌های ملی، توصیه می‌شود ترکیبی از کنترل‌های عملکردی و رویه‌ای گنجانیده شود. برای مثال، اولین لایه معمول دفاع، نصب یک مکانیسم کنترل دسترسی برای پذیرش کامپیوترها و دستگاه‌ها در شبکه‌های محلی است که این می‌تواند شامل کنترل‌های مسیریاب در یک شبکه کوچک یا قواعد دسترسی دیوار آتش در یک بنگاه تجاری باشد. در هر یک از دو حالت فوق آشکار است که اولین خط دفاع عملکردی می‌باشد. به همین ترتیب یک انتخاب خوب برای دومین لایه دفاع ممکن است شامل یک گزینه رویه‌ای مثل به‌کارگیری

پویش برای مشخص نمودن این باشد که آیا دستگاه‌های نامناسب از لایه اول دفاع، عبور کرده‌اند. چنین تنوعی، شانس این را افزایش خواهد داد که علت شکست در یک لایه احتمالاً باعث شکست مشابهی در یک لایه دیگر نشود.

یک پیچیدگی بزرگ در حفاظت زیرساخت‌های ملی این است که بسیاری از لایه‌های دفاعی وجود یک محیط پیرامون شبکه‌ای تعریف‌شده را فرض می‌کنند. برای مثال؛ وجود بسیاری از عیوب در امنیت بنگاه اقتصادی که به وسیله ممیزین یافت می‌شوند، با شناخت اینکه نفوذگران باید از این پیرامون و محیط به بنگاه تجارتی نفوذ کنند تا بتوانند از این عیوب و ضعف‌ها استفاده کنند، کاهش می‌یابد. متأسفانه، برای بسیاری از سرمایه‌های ملی یافتن یک محیط و پیرامون دیگر ممکن نیست. برای مثال؛ نمی‌توان سرمایه‌های یک کشور را در محدوده مرزهای جغرافیایی و سیاسی آن تعریف کرد. مدیران امنیتی باید در شناسایی کنترل‌هایی که دارای معنی برای سرمایه‌های پیچیده هستند و خواص آن‌ها معمولاً آشکار نیست، خلاقیت نشان دهند. ممکن است کنترل‌های معنی‌دار، غلط فهمیده شوند؛ چندین لایه دفاع، برای حفاظت به غلط به کار گرفته‌شده و برخی از سرمایه‌های اصلی بدون لایه‌های دفاعی رها شوند.

۱-۲-۶- احتیاط

اصل احتیاط مربوط به افراد و گروه‌هایی است که برای پنهان کردن اطلاعات حساس زیرساخت‌های ملی تصمیمات مهمی می‌گیرند. این عمل با ترکیب برنامه‌های حفاظت اطلاعات اجباری رسمی با رفتارهای احتیاطی غیررسمی انجام می‌شود. برنامه‌های رسمی اجباری سال‌هاست که در حکومت فدرال امریکا اجرامی شود، جایی که در آن مدارک طبقه‌بندی شده و سیاست‌ها بر اساس گواهی عدم سوپیشینه‌ای اجرا می‌شود که به افراد اعطا می‌گردد. در محیط‌های حساس و شدید نظیر محفظه‌های فوق مخفی در سازمان‌های اطلاعاتی، نقض سیاست‌های دسترسی می‌تواند به عنوان جاسوسی

تعبیر شود. با تمام عواقب جنایی که در پی خواهد داشت. به این دلیل افشا و نقض‌های عمده اطلاعات طبقه‌بندی شده حکومتی زیاد معمول نیست.

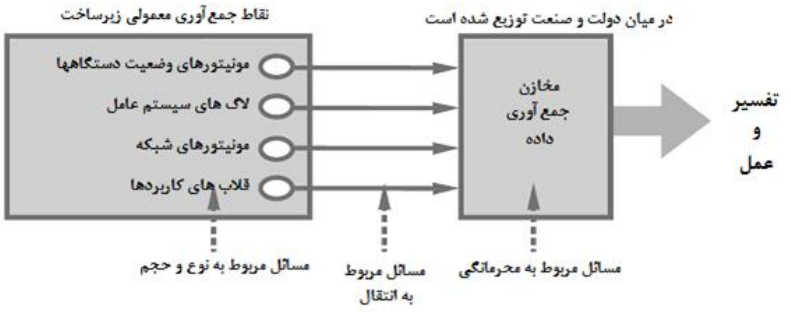
برنامه‌های حفاظت اطلاعات، در محیط‌های تجاری پذیرش وسیع‌تری می‌یابد؛ زیرا در چنین محیط‌هایی نیاز فزاینده‌ای به حفاظت اطلاعات شناسایی پرسنلی (PII) نظیر شماره‌های کارت‌های اعتباری وجود دارد. کارمندان شرکت‌ها در تمام دنیا اهمیت پنهان نمودن بعضی از جنبه‌های فعالیت‌های شرکت‌هایشان را درک کرده‌اند و این برای حفاظت زیرساخت‌های ملی نشانه سالمی است. در حقیقت برنامه‌های احتیاط، برای حفاظت زیرساخت‌های ملی، نیاز به اجرای ترکیبی از اجرای سیاست‌های امنیتی حکومت‌ها، شرکت‌ها و نشانه‌گذاری اطلاعات سفارشی دارد که برای سرمایه‌های ملی طراحی‌شده‌اند. سیاست احتیاطی، به عنوان یک لایه حفاظتی برای جلوگیری از این عمل می‌کنند که اطلاعات مربوط به زیرساخت‌های ملی در اختیار افرادی که هیچ احتیاجی به دانستن آن‌ها ندارندقرارنگیرد.

مفهوم "امنیت از طریق ابهام" سدی در مقابل به‌کارگیری احتیاط توصیه‌شده ما است. متخصصان امنیت، به خصوص رمزنگاران، مدت‌هاست که شکایت دارند و معتقدند که ابهام رویکرد حفاظتی پذیرفتنی نیست. آن‌ها به درستی به مسائل ناشی از امن کردن یک سیستم با سعی در پنهان نمودن جزییات زمینه‌ای آن اشاره می‌کنند. به طور اجتناب‌ناپذیری، دشمن رموز طراحی پنهان‌شده را کشف خواهد کرد و حفاظت امنیتی از بین خواهد رفت. به این دلیل در امنیت کامپیوتری معمولی به درستی به رویکردی باز در نرم‌افزار، طراحی و الگوریتم‌ها فرمان داده می‌شود. مزیت این رویکرد باز، بازبینی اجتماعی است که همراه با تبلیغ گسترده خواهد آمد. برای مثال؛ بدون مقدار قابل‌ملاحظه‌ای از بازبینی شدید یک نرم‌افزار، احتمال درست بودن آن پایین خواهد بود. بنابراین، استدلال امنیت کامپیوتری معمولی در مقابل شعار "امنیت از طریق ابهام" در بسیاری از موارد تا حد زیادی معتبر خواهد بود.

در هر حال، هر مدیری که مسئول حفاظت زیرساخت‌های مقیاس وسیع و ارزشمند باشد، خواهد گفت که احتیاط و ابهام اجزا ضروری یک برنامه حفاظتی هستند. پنهان کردن جزییات در مورد فناوری به‌کاررفته، نرم‌افزار استفاده‌شده، سیستم‌های خریداری شده و پیکربندی و تنظیمات به جلوگیری و کند شدن بعضی از انواع حمله کمک خواهد کرد. هکرها، معمولاً، با ادعای کشف این نوع اطلاعات در مورد یک شرکت و تبلیغ ضعف‌های آن، عملاً به نفع تیم امنیتی شرکت‌ها کار می‌کنند. آن‌ها معتقدند که چنین تبلیغاتی برای باانگیزه نمودن یک تیم امنیتی برای یافتن یک راه حل لازم است؛ اما چنین نیست. برنامه‌های مربوط به احتیاط و ابهام مناسب برای اطلاعات زیرساخت‌ها ضروری هستند و باید در سطحی ملی هماهنگ گردند.

۱-۲-۷- جمع‌آوری

اصل جمع‌آوری شامل گردآوری خودکار اطلاعات، به وسیله سیستم‌هایی است که در زیرساخت ملی وجود دارند و می‌توانند برای تجزیه و تحلیل امنیتی به کار گرفته شوند چنین جمع‌آوری معمولاً، به صورت بی‌درنگ انجام می‌شود و شامل قرار دادن کاوشگرها و قلاب‌هایی در برنامه‌های کاربردی، نرم‌افزارهای سیستم، عناصر شبکه و دستگاه‌های سخت‌افزاری جهت جمع‌آوری اطلاعات مورد نظر است.



شکل ۱-۹- جمع‌آوری اطلاعات امنیتی مرتبط با زیرساخت ملی

استفاده از دنباله‌های ممیزی در امنیت کامپیوتری مقیاس کوچک مثالی از یک شیوه عمل جمع‌آوری بلندمدت است که سودمندی آن در میان متخصصان کمتر بحث‌برانگیز بوده است. دستگاه‌های امنیتی مثل دیوار آتش، فایل‌های لاگ تولید می‌نمایند و سیستم‌هایی که ادعا می‌شود درجه‌ای از سودمندی امنیتی را دارند نیز به عنوان خروجی، دنباله ممیزی تولید می‌کنند. این شیوه عمل چنان متداول است که نوع جدیدی از محصول به نام SIMS یا سیستم مدیریت اطلاعات امنیتی برای پردازش تمام این داده‌ها توسعه یافته است.

چالش اصلی عملیاتی در راه‌اندازی نوع درستی از فرآیند جمع‌آوری برای کامپیوترها و شبکه‌ها عبارت‌اند از:

- ✓ اول: در مورد این که چه نوع اطلاعاتی باید جمع‌آوری شود تصمیم گرفته شود. اگر تصمیم درستی گرفته شود، اطلاعات جمع‌آوری شده، دقیقاً، داده‌هایی مورد نیاز برای تجزیه و تحلیل امنیتی است.
- ✓ دوم: در مورد اینکه چه مقدار اطلاعات عملاً باید گردآوری شود تصمیم گرفته شود. که می‌تواند شامل استفاده از عملکردهای سیستم‌های موجود مثل فعال‌سازی تولید خودکار آمار در یک مسیریاب باشد؛ یا معرفی نوع

جدیدی از توابع که به طور عمدی اطلاعات مورد نظر را جمع‌آوری می‌کنند باشد.

پس از اینکه این ملاحظات به کار گرفته شدند، مکانیسم‌های مناسبی برای جمع‌آوری داده‌ها از زیرساخت ملی می‌تواند در ساختار امنیتی جاسازی شود.

(به شکل ۱-۹ توجه کنید).

چالش‌های فنی و عملیاتی با جمع‌آوری لاگ‌ها و دنباله‌های ممیزی در حفاظت از سرمایه‌های ملی تشدید می‌شود. از آنجا که زیرساخت ملی خیلی پیچیده است، تعیین اینکه چه نوع اطلاعاتی باید جمع‌آوری شود، دشوار است. با جمع‌آوری اطلاعات فرصت‌های زیادی برای نفوذ به محرمانگی افراد و گروه‌های یک ملت ایجاد می‌شود. بنابراین، هر ابتکار برای حفاظت از زیرساخت‌ها با جمع‌آوری داده‌ها، باید شامل حداقل ترتیباتی جهت معین کردن سیاست‌های محرمانگی باشد. به طور مشابه حجم داده‌های جمع‌آوری شده از زیرساخت‌های بزرگ می‌تواند از حدود عملی تجاوز نماید. سیستم‌های جمع‌آوری ارتباطی راه دور که برای حفاظت یکپارچگی بک بن شرکت‌های ارائه‌دهنده خدمات طراحی‌شده‌اند، می‌توانند به راحتی چندین ترابایت داده را در هر ساعت از پردازش تولید نمایند.

در هر دو حالت، تخصص‌های فنی و عملیاتی باید برای اطمینان از این که داده‌های مناسب به مقدار مناسب جمع‌آوری می‌شوند به کار گرفته شوند. خوشبختانه، تمام الگوریتم‌های حفاظت امنیت به اطلاعات کاوشی و عمیق از نوعی که ممکن است مسائل محرمانگی و حجمی تولید کنند احتیاجی ندارند. در عوض، چالش‌ها زمانی ایجاد می‌شود که جمع‌آوری داده‌ها بدون تجزیه و تحلیل مقدماتی مناسب انجام شده باشد که باعث جمع‌آوری داده‌ها بیش از حد مورد نیاز می‌شود و می‌تواند منجر به مشکلات حفظ حریم خصوصی در بعضی مخازن جمع‌آوری ملی شود؛ بنابراین، به برنامه‌ریزی مخصوصی که راهبرد ملی جمع‌آوری داده‌ها باشد و با رهنمودهای سیاستی و قانونی معمولی در مورد اینکه چه کسی، تحت چه شرایطی، چه داده‌هایی را می‌تواند

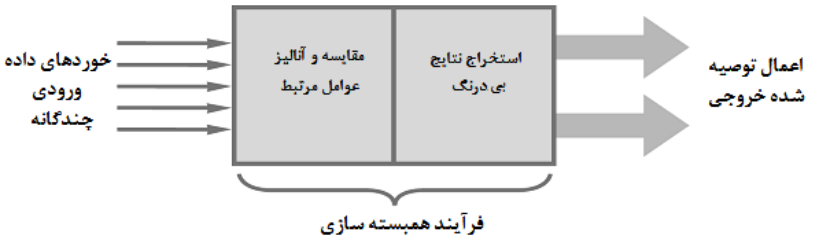
جمع‌آوری کند نیاز است. همان طور که در بالا پیشنهاد شد، این شیوه عمل باید به کمک نیازهای تجزیه و تحلیل امنیتی هدایت شود.

۱-۲-۸- همبسته سازی

اصل همبسته سازی، نوع خاصی از تجزیه و تحلیل است که می‌تواند روی فاکتورهای مربوط به حفاظت از زیرساخت ملی اعمال شود. هدف از همبسته سازی شناسایی این است که آیا ممکن است شاخص‌های مرتبط با امنیت از این تجزیه و تحلیل به دست آیند. برای مثال؛ اگر برخی از سرمایه‌های محاسباتی ملی کند عمل کنند، فاکتورهای دیگر نظیر شبکه‌های وسیع و محلی را برای یک رابطه همبسته سازی احتمالی امتحان می‌کنند؛ این شبکه‌ها می‌توانند برای ترافیکی که طبیعت حمله‌ای داشته باشد، تجزیه و تحلیل شوند. همچنین، برای مشخص کردن اینکه سرمایه‌های مشابه محاسباتی نیز مسائل عملکردی مشابهی را تجربه می‌کنند، آن‌ها را نیز امتحان می‌کنند. همچنین، تمام نرم‌افزارها و خدمات جاسازی‌شده در سرمایه ملی را نیز برای آسیب‌پذیری‌های شناخته‌شده، مورد تجزیه و تحلیل قرار می‌دهند. در هر حالت، منظور از همبسته سازی، ترکیب کردن و مقایسه فاکتورها برای کمک به بیان یک مسئله امنیتی است. تجزیه و تحلیل‌های مبتنی بر مقایسه برای زیرساخت‌های ملی، به علت پیچیدگی آن‌ها، ضروری به نظر می‌رسد.

جالب است بدانید که تاکنون، در هر ابتکار عمده به‌کاررفته در جهت حفاظت از زیرساخت‌های ملی عمده، یک مرکز ادغام برای همبسته سازی بی‌درنگ داده‌ها گنجانیده شده است. مرکز ادغام، یک مرکز عملیات امنیت با ابزارهایی برای جمع‌آوری و تجزیه و تحلیل منابع چندگانه داده‌های ورودی است. غیرمعمول نیست که چنین مرکزی صفحات نمایشگر بزرگ رنگارنگ داشته باشد. با اینکه چنین ادغام اتوماتیکی امیدوار کننده است، در بهترین شیوه عمل همبسته سازی برای حفاظت زیرساخت‌های ملی به قضاوت انسانی در تجزیه و تحلیل‌ها احتیاج است. بنابراین، بدون توجه به اینکه

آیا منابع به طور متمرکز در یک محل فیزیکی هستند یا خیر، واقعیت این است که انسان احتیاج به در نظر گرفته شدن در پردازش‌ها را دارد.
(به شکل ۱-۱۰ توجه کنید).



شکل ۱-۱۰- رویکرد همبسته سازی سطح بالای زیرساخت ملی

مراکز ادغام و فرآیندهای مربوطه و الگوریتم‌های همبسته سازی، اجرایشان حتی در محیط‌های با مقیاس کوچک نیز بسیار دشوار است. بات‌نت‌ها شامل استفاده سیستم‌های منبعی هستند که به طور تصادفی انتخاب‌شده‌اند؛ بنابراین، با استفاده از همبسته سازی نمی‌توان تعیین کرد که کجا و چرا حمله اتفاق می‌افتد. در حقیقت، همبسته سازی اطلاعات جغرافیایی با منبع فعالیت‌های بات‌نت ها، حتی باعث نتیجه‌گیری غلط در مورد این می‌شود که چه کسی به چه کسی حمله کرده است. تیم‌های امنیتی، ساعت‌های طولانی را صرف جمع‌آوری اطلاعات در مورد بات‌نت‌ها کرده‌اند تا بتوانند منبع آن را بیابند و در بهترین حالت می‌توانند اطلاعاتی را در مورد کنترل‌کننده‌های بات‌نت و پایگاه‌های نرم‌افزار بات‌نت‌ها به دست آورند. در انتها، متوجه می‌شوند که روش‌های فعلی همبسته سازی، ناقص هستند. امروزه، برای بهبود قابلیت‌های همبسته سازی فعلی برای حفاظت از زیرساخت‌های ملی نیاز است که در چند مرحله این کار انجام شود.

سه مرحله برای بهبود قابلیت‌های فعلی همبسته سازی

۱- علوم کامپیوتری عملی در مورد الگوریتم‌های همبسته سازی احتیاج به تحقیق بیشتری دارند. در علوم کامپیوتری دانشگاهی و دپارتمان‌های ریاضی کاربردی توجه کمی به همبسته سازی چند متغیره داده‌های امنیتی بی‌درنگ شده است؛ که این می‌تواند با تأکید بیشتر حکومت بر ارائه کمک‌هزینه تحصیلی و تخصیص بودجه تغییر کند.

۲- توانایی برای شناسایی فیدهای داده قابل‌اعتماد، احتیاج به بهبود بیشتری دارد. توجه زیادی به جمع‌آوری تک کاره فیدهای داده داوطلبانه انجام‌شده که باعث پیچیده شدن توانایی تجزیه و تحلیل برای انجام همبسته سازی معنی‌دار می‌گردد.

۳- باید به طراحی و عملیات یک مرکز ادغام در سطح ملی توجه جدی شود و ساز و کارهایی برای کنار گذاشتن مسائل بودجه‌ای و سیاسی شناسایی شود تا بتوان این هدف مهم را به انجام رساند.

۱-۲-۹- آگاهی

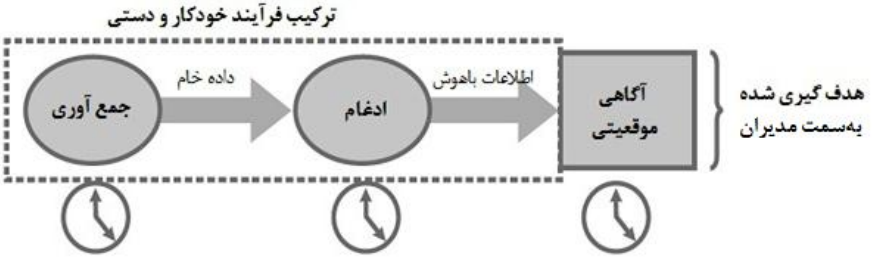
- ✓ بر اساس اصل آگاهی، یک سازمان در زمان بی‌درنگ و در همه زمان‌ها اختلاف بین حالت مشاهده‌شده و حالت طبیعی را در زیرساخت ملی تشخیص می‌دهد. این وضعیت می‌تواند شامل ریسک‌ها، آسیب‌پذیری‌ها و رفتار زیرساخت مورد هدف باشد. در اینجا رفتار به مخلوطی از فعالیت کاربر، پردازش سیستم، ترافیک شبکه و انجام محاسباتی در نرم‌افزار، کامپیوترها و سیستم‌هایی اشاره دارد که زیرساخت را تشکیل می‌دهند. معنی و مفهوم این است که سازمان به نحوی می‌تواند وضعیت داده‌شده را به عنوان وضعیت طبیعی یا غیرطبیعی مشخص نماید. همچنین،

سازمان باید بتواند اختلاف بین دو حالت رفتاری را کشف و اندازه‌گیری کند. در چنین تعیین کردنی تجزیه و تحلیل همبسته سازی ذاتی است، اما چالش واقعی کمتر مربوط به الگوریتم‌ها و بیشتر مربوط به فرآیندهایی است که باید برای اطمینان از آگاهی موقعیتی در هر ساعت و هر روز سر جایشان باشند. برای مثال؛ اگر یک آسیب‌پذیری جدید مطرح شود که روی زیرساخت محلی تأثیرگذار است، این دانش بایستی کسب و در تصمیمات مدیریتی فوراً تأثیرگذار گردد.

معمولاً نمی‌توان مدیران زیرساخت‌های ملی را در مورد اینکه آگاهی از وضعیت مهم است متقاعد کرد. موضوع مهم این است که چگونه می‌توانیم به این هدف (آگاهی موقعیتی) برسیم. آگاهی بی‌درنگ و زمان واقعی احتیاج به توجه و مراقبت دارد که به ندرت در امنیت کامپیوتری یافت می‌شود. ابتدا باید داده‌ها جمع‌آوری شده و به طور پیوسته به داخل مرکز ادغام وارد شوند تا همبسته سازی انجام گیرد. نتایج همبسته سازی باید یک نمایش پایه‌ای از رفتارها باشد، به نحوی که اختلافات اندازه‌گیری شوند. این کار آسان به نظر می‌رسد؛ زیرا بسیاری از وضعیت‌های عجیب و غریب قادر به تقلید رفتار نرمال (زمانی که آن واقعاً یک مسئله است) یا یک مسئله (زمانی که واقعاً چیزی نیست) می‌باشند. با وجود این، حفاظت از زیرساخت ملی نیاز دارد که مدیران سرمایه‌ها ساز و کارهای محلی مربوطه‌ای را ایجاد نمایند تا قادر باشند حالت امنیت را در تمام زمان‌ها به طور دقیق توضیح دهند. این به آن‌ها اجازه می‌دهد تصمیمات مدیریتی مناسبی در مورد امنیت بگیرند. (به شکل ۱-۱۱ توجه کنید).

جالب است بدانید که امروزه، آگاهی موقعیتی به عنوان یک جز عمده از معادله امنیتی کامپیوتری در نظر گرفته نمی‌شود. این مفهوم در امنیت با مقیاس کوچک نظیر شبکه‌های خانگی، نقش اساسی بازی نمی‌کند، زیرا هنگامی که پایه محاسباتی که باید از آن حفاظت شود، به اندازه کافی ساده باشد، فقط مشخص کردن وضعیت بی‌درنگ آن

لازم نیست. به طریقی مشابه، زمانی که یک مدیر امنیتی برای یک بنگاه اقتصادی کوچک کنترل‌های امنیتی برقرار می‌کند، آگاهی موقعیتی بالاترین ارجحیت را ندارند.



شکل ۱-۱۱- جریان فرایند آگاهی موقعیتی بی‌درنگ

معمولاً، نزدیک‌ترین چیزی که می‌توان انتظار داشت که درجه‌ای از آگاهی بی‌درنگ را برای یک سیستم کوچک ایجاد نماید مرور گاه به گاه فایل‌های لاگ سیستم است. بنابراین، گذر از حفاظت یک سیستم کوچک به زیرساخت با مقیاس وسیع، احتیاج به توجه جدیدی به آگاهی موقعیتی دارد که به خوبی توسعه نیافته است.

گفتنی است مفهوم عمومی "آگاهی کاربر" در امنیت، اصلی نیست که در اینجا مشخص شود. درست است که داشتن دانش امنیتی به کاربران کمک می‌کند، با وجود این هر برنامه حرفه‌ای طراحی‌شده برای امنیت زیرساخت‌های ملی، باید در نظر داشته باشد که درصد بالایی از کاربران انتهایی در صورتی که به آن‌ها اجازه داده شود همیشه انواع اشتباهی از تصمیمات امنیتی را خواهند گرفت. بنابراین، حفاظت زیرساخت‌های ملی، هرگز، نباید متکی بر تصمیم‌گیری کاربران انتهایی از طریق برنامه‌های آگاهی رسانی باشد.

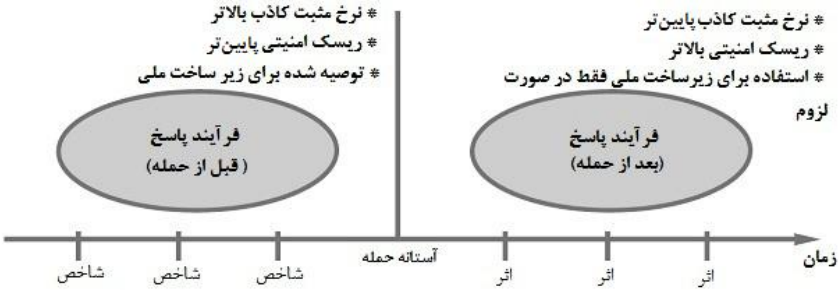
پیشرفت دیگر که برای آگاهی موقعیتی لازم است، ارتقاء رویکرد گزارش دهی متریک‌های امنیتی است. جامعه اطلاعاتی غیر سایبری، کار بزرگی جهت توسعه ابزارهای ارائه خلاصه روزانه اطلاعات به مقامات ارشد حکومتی انجام داده است؛ اما جامعه امنیت سایبری به ندرت این روش را در نظر گرفته است. در واقع برای اینکه آگاهی موقعیتی یک جز ساختاری از زیرساخت ملی شود، متریک‌های معتبری که

وضعیت را به طور دقیق نشان می‌دهند، باید توسعه یابند و این کارها باید به صورت گزارش‌های منظم مناسبی از اطلاعات تدوین شوند، به نحوی که مقامات عالی‌رتبه بتوانند از آن‌ها برای تعیین وضعیت امنیتی استفاده نمایند. می‌توان انتظار داشت که اطلاعات امنیت سایبری از یک نقطه مرکزی مثل مرکز ادغام جریان پیدا کنند، اما این یک الزام نیست.

۱-۲-۱۰- واکنش

بر اساس اصل واکنش، باید اطمینان باشد که فرآیندهایی آماده هستند تا به شاخص‌های امنیتی در دسترس واکنش نشان دهند. عمدتاً، این شاخص‌ها باید از لایه آگاهی موقعیتی به داخل فرآیند واکنش جریان یابند. واکنش زیرساخت ملی باید بر شاخص‌ها تاکید کند نه بر وقایع. در بسیاری از کاربردهای فعلی امنیت کامپیوتری، تیم واکنش به وقایع امنیتی، منتظر اتفاق افتادن مسائل جدی هستند که معمولاً، شامل شکایت کاربران، ضعیف اجراشدن برنامه‌های کاربردی و کارکرد کند شبکه است. زمانی که چنین اتفاقاتی بیفتد، تیم واکنش وارد عمل می‌شود، حتی اگر بازی امنیتی را قبلاً باخته باشد. برای خدمات ضروری زیرساخت‌های ملی، این ایده منطقی نیست که منتظر بمانیم تا سرویس تنزل یابد و سپس، واکنش نشان دهیم. یک تغییر مرتبط با واکنش اضافی برای حفاظت از زیرساخت‌های ملی این است که در مفهوم بدخیم "مثبت کاذب" باید تجدیدنظر شود. در محیط‌های مقیاس کوچک فعلی، یک هدف عمده تیم امنیت کامپیوتری، کمینه کردن تعداد شروع مواردی از واکنش است که فقط در انتها معلوم می‌شود، چیزی اشتباه نیست. رسیدن به این هدف ساده است، تنها می‌توان صبر کرد تا فاجعه‌ای اتفاق بیفتد که در آن هیچ تردیدی نباشد و سپس، واکنش شروع شود واضح است که برای زیرساخت‌های ملی روش بالا پذیرفتنی نیست. واکنش باید شاخص‌ها را تعقیب نماید و مفهوم کمینه کردن "مثبت کاذب" نباید جزیی از این رویکرد باشد. تنها متریک کمّی که باید در واکنش‌های در سطح ملی کمینه گردد، ریسک است.

(به شکل ۱-۱۲ توجه کنید)



شکل ۱-۱۲- رویکرد واکنش امنیتی زیرساخت ملی

چالشی که باید در ایجاد عمل واکنش در حفاظت سرمایه‌های ملی در نظر گرفته شود، شاخص‌هایی هستند که مدت‌ها قبل از آن که آثار زیان‌بار دیده شوند ظاهر می‌شوند. این موضوع نشان می‌دهد که برای حفاظت از زیرساخت باید آگاهی موقعیتی دقیقی داشت که در آن خدمات خیلی بیشتری از آثار قابل‌مشاهده‌ای؛ نظیر، مشکل کاربران، ساقط شدن شبکه، یا دسترس ناپذیر شدن لحاظ شده باشد. شاخص‌های زیرکانه باید با دقت تجزیه و تحلیل شوند؛ زیرا چالش با "مثبت کاذب" ظاهر می‌شود. زمانی که تیم‌های واکنش با در نظر گرفتن چنین شاخص‌هایی موافقت می‌نمایند، احتمال اینکه این شاخص‌ها بی‌خطر باشند، بیشتر می‌شود. یک راز بزرگ برای نشان دادن واکنش مناسب نسبت به وقایعی که برای زیرساخت‌های ملی رخ می‌دهد، این است که نرخ "مثبت کاذب" بالاتر، علامت خوبی است.

گفتنی است که اصول جمع‌آوری، همبسته سازی، آگاهی و واکنش، همگی، با پیاده‌سازی یک مرکز ملی ادغام سازگار هستند. معمولاً فعالیت‌های واکنشی به بی‌درنگ بودن، مرکز عملیات حاضر در همه جا برای هماهنگ کردن فعالیت‌ها، تماس با افراد کلیدی، جمع‌آوری داده‌هایی که در دسترس قرار می‌گیرند و مستند کردن پیشرفت در فعالیت‌های واکنشی وابسته هستند. به این ترتیب واکنش در سطح ملی به امنیت

سایبری باید شامل یک مرکز ملی متمرکز باشد. ایجاد چنین امکاناتی، باید محور هر برنامه حفاظت از زیرساخت ملی باشد تمام سازمان‌هایی که مسئولیتی برای خدمات ملی را بر عهده‌دارند باید در آن شرکت فعال داشته باشند.

۱-۳- اجرای اصول به صورت ملی

در به‌کارگیری این مجموعه کامل اصول امنیتی در عمل، برای حفاظت از زیرساخت‌های ملی، برخی ملاحظات اجرای عملی ظاهر می‌شود:

- کمیسیون‌ها و گروه‌ها: در طی سال‌ها، برای حفاظت از زیرساخت‌های ملی کمیسیون‌ها و گروه‌های متعددی ایجاد شده است. بیشترین آن‌ها اثر جزیی مثبتی روی امنیت زیرساخت داشته‌اند، اما هیچ‌کدام اثر کافی برای کاهش ریسک ملی فعلی به میزان قابل پذیرش نداشته‌اند. این کمیسیون‌ها و گروه‌ها به جای اینکه ابزاری برای حل مسئله امنیت سایبری باشند، پایان و فرجام آن هستند. زمانی که چنین اتفاقی می‌افتد، احتمال موفقیتشان به طور قابل‌ملاحظه‌ای کاهش می‌یابد. کمیسیون‌ها و گروه‌های آینده باید این موضوع را در نظر بگیرند.
- تسهیم اطلاعات: تاکنون به تسهیم اطلاعات بین حکومت و صنایع توجه زیادی شده است؛ ظاهراً به این علت که هر دو طرف از این موضوع استفاده زیادی می‌برند. البته اجرای یک برنامه جامع تسهیم اطلاعات ساده نیست؛ زیرا زمانی که سازمان‌ها در حال جنگیدن با یک آسیب‌پذیری هستند، ترجیح می‌دهند کمتر در صحنه دیده شوند.

همچنین، ممکن است برخی سازمان‌ها، حکومت‌ها و شرکت‌های تجاری قسمتی از اطلاعات را داشته باشند که بتوان با آن یک حمله سایبری را حل نمود و ریسک را کاهش داد که معمولاً، با شیوه‌های عمل سازگار

نیست. بنابراین، انگیزه یک بنگاه تجاری برای اینکه اطلاعات مربوط به یک آسیب‌پذیری واقعه را با حکومت تسهیم نماید کم است و چیز مهمی از این تسهیم به دست نخواهد آمد.

- همکاری‌های بین‌المللی: ابتکارات ملی که متمرکز بر ایجاد قانون‌گذاری امنیت سایبری حکومت‌ها باشد، باید با تأیید بر جهانی بودن اینترنت انجام شود، همین طور سرویس‌های مشترک مثل سیستم‌های اسم دامنه (DNS) که همه آن‌ها سرمایه‌های ملی و جهانی هستند، به یکدیگر وابسته‌اند. بنابراین، هر برنامه حفاظت از زیرساخت‌های ملی، باید شامل مقرراتی برای همکاری بین‌المللی باشد. چنین همکاری‌هایی، توافقاتی را بین شرکت‌کنندگان ایجاب می‌کند و تا زمانی تداوم می‌یابد که هر کدام از شرکا منافع آن را دریافت می‌نمایند.
- هزینه‌های تکنیکی و عملیاتی: برای اجرای اصولی که در بالا بیان شد، حکومت‌ها و محیط‌های تجاری باید مقدار قابل‌ملاحظه‌ای از هزینه‌های فنی و عملیاتی را بپردازند. با اینکه وسوسه‌انگیز است که فرض کنیم که تهیه‌کنندگان زیرساخت‌های ملی این هزینه‌ها را به راحتی با بودجه‌های معمولی تجاری جذب خواهند کرد، ولی این موضوع در گذشته اتفاق نیفتاده است. در عوض تاکید باید بر اساس پاداش و مشوق‌ها برای سازمان‌هایی باشد که تصمیم به اجرای این اصول گرفته‌اند. این نکته اهمیت حیاتی دارد؛ زیرا بر اساس این روش، بهترین استفاده ممکن از بودجه دولتی، به ابتکاراتی کمک می‌کند که به امن کردن سرمایه‌های ملی کمک خواهند کرد.

در فصل بعدی، حجم بزرگی از بحث‌های ما فنی است و به برنامه و سیاست نپرداخته‌ایم؛ نه به علت اینکه آن‌ها اهمیت کمی دارند؛ بلکه می‌خواهیم نگرانی‌ها را کنار گذاشته و به شرح مفصل "چه" باید کرد، بپردازیم.

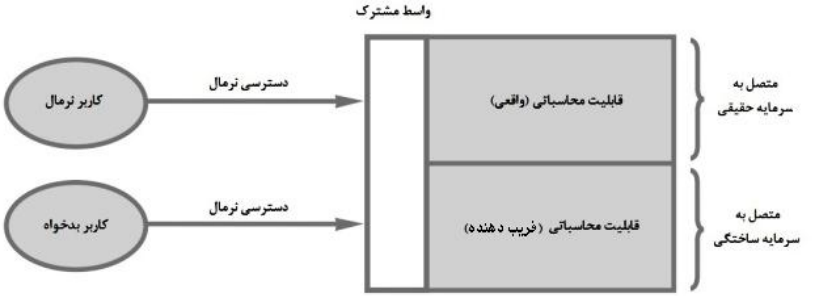
فصل۲: فریب دادن

یک شبکه بسازید و آن را به شدت کنترل کنید؛ در آن شبکه یک سیستم تولید قرار دهید و سپس، تمام فعالیت‌هایی را که در آن شبکه اتفاق میفتد نظارت، ضبط و تجزیه و تحلیل کنید. به علت اینکه این یک شبکه تولید نیست؛ بلکه یک شبکه عسل است، به هر ترافیکی در آن می‌توان سوظن و شک داشت. پروژه شبکه عسل.[۵]

استفاده از فریب دادن در محاسبات با گمراه کردن عمدی دشمن با ایجاد یک جز سیستم انجام می‌شود که به نظر می‌رسد این جز واقعی باشد؛ اما در حقیقت یک تله است. بعضی مواقع به این جز سیستم ظرف عسل گفته می‌شود و معمولاً، می‌تواند در سیستم محاسباتی و شبکه‌ای جاسازی‌شده و به صورت یک سرمایه فیزیکی برای گول زدن مهاجم طراحی شده باشد. در هر دو حالت، یک واسط مشترک به دشمنی ارائه می‌شود که ممکن است تصور کند به سرمایه واقعی متصل می‌شود، اما ندانسته به قابلیت فریب‌دهنده‌ای دسترسی یافته که به یک سرمایه غیرواقعی وصل است. در یک سیستم فریب‌دهنده که خوب طراحی‌شده، نباید تمایز بین قابلیت‌های واقعی و تله برای نفوذگر معلوم باشد. (به شکل ۲-۱ توجه کنید).

منظور از فریب دادن، بالا بردن و تقویت امنیت است؛ بنابراین در زمینه زیرساخت ملی، می‌توان از آن برای حفاظت با مقیاس وسیع سرمایه‌ها استفاده کرد. دلیل اینکه فریب دادن موفق عمل می‌نماید این است که به انجام هر کدام از چهار هدف امنیتی زیر یا تمام آن‌ها کمک می‌کند:

- توجه: می‌تواند توجه دشمن را از سرمایه واقعی به سمت سرمایه ساختگی منحرف کند.
- انرژی: وقت باارزش و انرژی دشمن روی یک هدف ساختگی تلف می‌شود.



شکل ۲-۱- استفاده از فریب دادن در محاسبات

- عدم یقین: حول صحت یک آسیب‌پذیری کشف‌شده ایجاد عدم یقین می‌نماید.
- تجزیه و تحلیل: برای تجزیه و تحلیل بی‌درنگ رفتار دشمن پایه و اساس ایجاد می‌کند.

برای کسانی که تا به حال از ظرف عسل در یک شبکه استفاده کرده‌اند حقیقت اینکه فریب دادن توجه دشمن را منحرف کرده و انرژی و وقت او را صرف می‌نماید، مفهومی آشنا است؛ تا زمانی که تله به طور مناسبی نصب شده باشد و ظرف عسل به اندازه کافی واقعی به نظر برسد، دشمنان ممکن است وقت، توجه و انرژی خود را به چیزی معطوف کنند که از نظر حمله بدون ارزش است. آن‌ها ممکن است در قابلیت تله یک بمب زمانی قرار دهند؛ چون معتقدند که ممکن است این تله برای هدف قرار دادن بعدی سرمایه‌های واقعی به کار رود. روشن است که یک ظرف عسل این‌گونه عمل نمی‌کند؛ اما این نوع فریب دادن وسیله بازدارنده قدرتمندی است؛ زیرا می‌تواند با گول زدن دشمن یک حمله کامپیوتری را برای دوره زمانی طولانی خنثی نماید.

تا امروز به طور ضعیفی در مورد اینکه؛ ممکن است فریب دادن عدم یقین حول صحت آسیب‌پذیری کشف‌شده ایجاد کند کاوش شده است. اگر یک نفوذگر به طور اجتناب‌ناپذیری به داخل یک سوراخ امنیتی قابل سو استفاده بیفتد، بد نیست او را به این باور هدایت کنم که این سوراخ امنیتی یک تله است؛ بنابراین، تحت شرایط درست،

نفوذگر از ترس اینکه ممکن است این آسیب‌پذیری به طور عمدی جاسازی شده باشد، گزینه عدم استفاده از آسیب‌پذیری را انتخاب می‌کند. در بسیاری از محیط‌ها، جاسازی فریب، کاری مشکل است، ولی فریب دادن مفهوم قدرتمندی دارد؛ زیرا به مدیران امنیتی اجازه خنثی کردن آسیب‌پذیری‌های موجود را می‌دهد، بدون اینکه این آسیب‌پذیری‌ها را بشناسند. این مفهوم به قدر کافی مهم است و باید آن را تکرار کنیم: استفاده از فریب دادن در محیط‌های محاسباتی به مدیران امنیتی سیستم اجازه می‌دهد تا ریسک آسیب‌پذیری‌هایی را که ممکن است حتی از وجود آن‌ها بی‌اطلاع باشند، کاهش دهند.

این حقیقت که تجزیه و تحلیل می‌تواند بی‌درنگ روی ظرف عسل انجام شود، در محیط‌ها و اجتماعات محاسباتی امروزه به خوبی شناخته شده است. شاید به آن علت که بهترین شیوه عملی که به طور وسیعی پذیرفته‌شده، این است که مدیران امنیتی باید سعی کنند رفتار نفوذگرانی را که کشف‌شده‌اند مشاهده نمایند. برای مثال؛ بیشتر سیستم‌های کشف نفوذ که سیستم‌های مدیریت تهدید انتهایی دارند، برای حمایت از چنین هدفی طراحی‌شده‌اند. در بهترین حالت تجزیه و تحلیل فارنسیک جمع‌آوری شده در هنگام فریب دادن به اندازه کافی مشروح خواهد بود تا بتوان دشمن را تشخیص داد و او را از نظر قانونی تعقیب کرد. در بیشتر موارد معمولی، معمولاً، ردگیری دقیق تا شناسایی منشأ انسانی مسئله، به ندرت انجام می‌شود.

خوشبختانه، با توجه به این حقیقت که نفوذگران، همیشه، طراحان و اپراتورهای سرمایه‌های ملی را به صورت افراد نامرتب در کار و ناکارآمد در آموزش و نالایق در علمشان در نظر می‌گیرند به موفقیت تله‌های فریب‌دهنده کمک می‌شود. این نظر فوق‌العاده منفی از افرادی که زیرساخت‌های ملی را اداره می‌کنند هسته اعتقادی هر انجمن هکری در جهان است که در برخی محیط‌ها مسلماً توجیه‌پذیر است. جالب اینجاست که این انتظار پایین، عنصر مهمی در کمک به عملی‌تر شدن فریب پنهانی است، زیرا ظروف عسل همیشه تقلید محیط مدیریت شده کاملی نیستند. در عوض

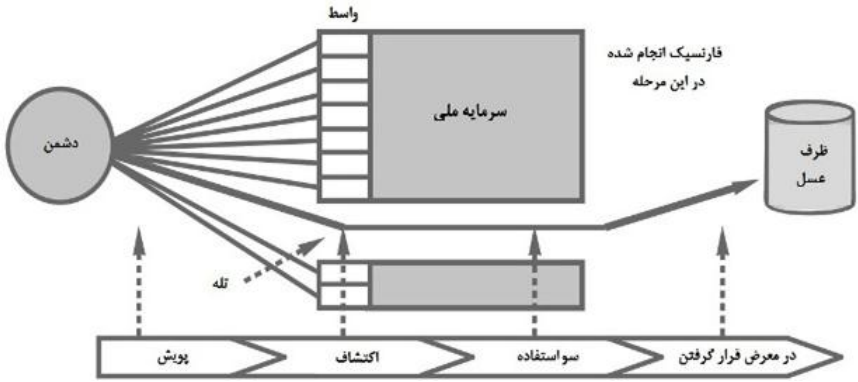
دشمنان عموماً می‌توانند به این طرز تفکر که محیط سیستمی‌ای را که یافته‌اند به گونه‌ای ضعیف مدیریت می‌شود هدایت نمود و این به طراحان فریب کمک می‌کند.

مورد کمتر شناخته‌شده از فریبی که به صورت علنی تبلیغ می‌شود، متکی بر این است که دشمن معتقد شود که طراحان و اداره‌کنندگان سرمایه‌های ملی به اندازه کافی برای جاسازی یک تله باورپذیر در سرمایه‌های ملی لیاقت دارند. این نگرش یک مانع را در پیش رو دارد، زیرا اجتماع هکرها برای باور اینکه شخصی که مرتبط با یک سازمان بزرگ است، به اندازه کافی ماهر و لایق باشد که بتواند یک برنامه پیچیده فریب محاسباتی را مدیریت نماید احتیاج به دیدن دلایل قانع‌کننده‌ای دارند. این خیلی بد است؛ زیرا استفاده آشکار فریب، مزایای بزرگی به همراه خواهد داشت که در ادامه به طور مشروح آن‌ها را بیان خواهیم کرد. روانشناسی فهمیدن و مدیریت کردن نظریات دشمن کار آسانی نیست. این مسئله نرم، باید قسمتی از معادله حفاظت از زیرساخت ملی گردد و آشکار خواهد بود که به مجموعه جدیدی از مهارت‌ها در میان کارشناسان امنیتی نیازمی باشد.

معمولی‌ترین اجرای فریب شامل جاسازی نقاط ورودی قلابی حمله؛ مثل؛ پرت‌های باز سرویس است که ممکن است دشمنان انتظار دیدن آن‌ها را در یک سیستم نرمال داشته باشند. امید است که دشمن با کشف (احتمالاً از طریق اسکنر) و وصل شدن به این پرت‌های باز سرویس به ظرف عسل هدایت شود. همان طور که در بالا اشاره شد، ایجاد احساس واقعی بودن در ظرف عسل آسان نیست؛ اما گزینه‌های طراحی متعددی وجود دارد. یک رویکرد شامل هدایت اتصالات ورودی باز به سیستم‌های ساختگی است، که به طور فیزیکی جدا هستند و از سرمایه‌های واقعی ایزوله می‌باشند و این اجازه کپی کردن به صورت بلند کردن چنگالی قابلیت‌های واقعی (شاید با داده‌های حساس بهداشتی شده) به یک نقطه ایزوله و امن جایی را می‌دهد که هیچ صدمه واقعی را نمی‌توان انجام داد. به یاد بیاورید که اگر فریب دادن به صورت علنی تبلیغ شود، احتمال

اینکه دشمن زحمت حمله را به خود ندهد، افزایش می‌یابد. مسلماً این بسط سناریوهای ممکن است که ارزش تذکر دارد.

با این همه، باید در نظر بگیریم که ممکن است دشمن نقاط ورودی فریب را بیابد؛ فکر کند که آن‌ها واقعی هستند و تصمیم به انجام و ادامه حمله بگیرد. اگر فریب بعدی به صورت مناسبی مدیریت شود، دشمن باید به مسیر کنترل شده‌ای هدایت شود که چهار مرحله متمایز حمله هستند؛ اسکن (پویش)، اکتشاف، بهره‌برداری و در معرض قرار گرفتن. (به شکل ۲-۲ توجه کنید)



شکل ۲-۲- مراحل فریب دادن برای حفاظت زیرساخت ملی

در طی مرحله پویش اولیه، دشمن با هر ابزاری در جستجوی نقاط ورودی قابل سواستفاده است. در این مرحله، فرض بر این است که واسط سرویس شامل قابلیت تله باشد؛ مثل لینک‌های ساختگی روی وب سایت‌های پروکسی شده که به سمت یک ظرف عسل برای جمع‌آوری اطلاعات هدایت می‌شوند. به هر حال گفتنی است که فرآیند جستجو، همیشه، به این دلیل نیست که دشمن مشغول استفاده از شبکه است. ممکن است دشمن در جستجوی نقاط ورودی قابل‌استفاده در قراردادها، فرآیندها،

کابینت‌های قفل شده و گاوصندوق‌ها؛ یا ایجاد روابطی با کارمندان زیرساخت ملی باشد. حتی می‌توان انتظار داشت که ترکیبی از جستجوهای محاسباتی و غیر محاسباتی را برای کسب اطلاعاتی در مورد نقاط ورودی قابل بهره‌برداری به کاربر که مطابق آن فریب باید طراحی شود به کار گرفته شود.

در فاز اکتشاف، دشمن یک نقطه ورودی قابل بهره‌برداری می‌یابد که ممکن است واقعی یا قلابی باشد. اگر آسیب‌پذیری واقعی باشد، می‌توان امیدوار بود که امنیت انتهایی خوبی بر قرار است تا از فجایع زیرساختی اجتناب شود. به هر حال، تصمیم نفوذگر در مورد اینکه از آسیب‌پذیری کشف‌شده واقعی یا قلابی استفاده نماید، یک نقطه تریگر مهم است. سیستم‌های امنیتی زیرساخت خوب احتیاج دارند این نقطه بهره‌برداری را به یک سیستم مدیریت تهدید وصل کنند که بلیط یک مزاحمت امنیتی را باز کند؛ و یا یک هشدار به مدیریت امنیتی بدهد که به مفهوم این باشد که یک نفوذگر یا شروع به حمله کرده یا در تله یک طعمه فریب‌دهنده افتاده است. واضح است که چنین هشدارهایی نباید به نفوذگر علامت دهد که یک تله وجود دارد.

در مرحله سواستفاده، دشمن از آسیب‌پذیری کشف‌شده به هر منظوری استفاده می‌کند. اگر آسیب‌پذیری واقعی باشد، باعث سناریوی نقض امنیتی زیرساخت می‌شود. اگر آسیب‌پذیری تله باشد، کارایی آن مستقیماً مرتبط با واقعی نمایی ظرف عسل است. برای هر دو نوع فریب، علنی و پنهانی، در مرحله ابتدایی داده‌ها برای تجزیه و تحلیل فارنسیک در دسترس قرار می‌گیرند. یکی از ملاحظات و مفروضات طراحی، این است که هرگز نباید سرمایه واقعی در اثر قرار دادن تله در خطر نقض امنیتی قرار گیرد؛ زیرا این باعث می‌گردد که قابلیت‌های فریب‌دهنده در جزیره‌های محاسباتی اجرا شوند که به صورت عملکردی از سرمایه‌ای حقیقی جدا هستند. طی مرحله، در معرض فریب قرار گرفتن، می‌توانید رفتار دشمن را مشاهده کنید. ظروف عسل باید نظارت کافی بر نمایش تکنیک، منظور و شناسه دشمن داشته باشند. معمولاً، در طی این مرحله است که تصمیمات مدیریتی گرفته می‌شود، در مورد اینکه آیا اعمال واکنشی و پاسخگویی موجه

است؟ در همین مرحله است که به عمل بی‌درنگ و زمان واقعی نیاز است تا فریب به نظر واقعی برسد. همان طور که در بالا بیان کردیم مزیت بالایی که ایجاد می‌شود، انتظار کم دشمن در مورد لیاقت و کفایت مدیریتی سیستم، به خصوص در مورد تیم و گروه زیرساخت است که اجازه می‌دهد گروه امنیتی به بهانه راه‌اندازی ضعیف، شکاف‌های عملکردی خود را بپوشاند.

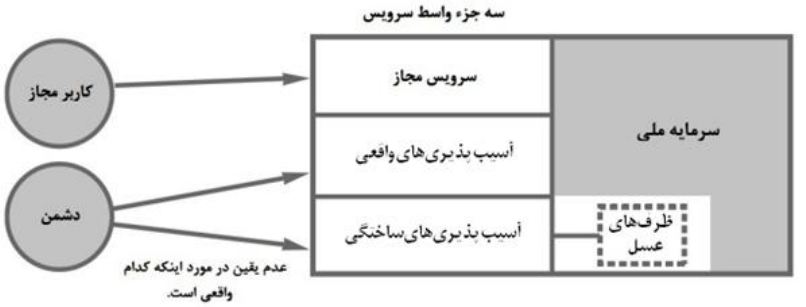
هر کدام از چهار مرحله فریب دادن مسائل قانونی و اجتماعی قابل‌ملاحظه‌ای را به دنبال دارند؛ بنابراین، هر برنامه حفاظت از زیرساخت ملی باید شرکایی از جامعه قانونی ملی را برای مشخص کردن اینکه چه چیزهایی پذیرفتنی است، در خود داشته باشد. برای مثال؛ تفاوت بین یک تله غیرفعال و یک گول زننده فعال بسیار ظریف است و باید پیش از به‌کارگیری عملی آن در زیرساخت، وضعیت آن روشن شود. از دیدگاه اجتماعی می‌توان امید داشت پذیرشی که برای استفاده از فریب برای گرفتن پرسه‌زن‌های بی‌درنگ در محیط اینترنت وجود دارد را بتوان برای گرفتن دشمنانی که زیرساخت‌های ملی را هدف قرار می‌دهند، جهت امنیت فضای سایبری تعمیم داد.

۲-۱- مرحله پویش (اسکن)

در این مرحله، فرض بر این است که دشمن هر چیزی را که در دسترس است برای یافتن نقطه سواستفاده جهت حمله به زیرساخت ملی پویش می‌نماید. این پویش می‌تواند شامل جستجوهای بی‌درنگ و بر خط برای اطلاعات مبتنی بر وب، پویش شبکه برای مشخص کردن قابل‌دسترس بودن پرت‌ها و حتی جستجوی غیر بر خط مدارک برای اطلاعات مورد نظر باشد. فریب دادن می‌تواند جهت منحرف کردن این تلاش‌های پویشی از طریق ایجاد نقاط ورودی قلابی به آسیب‌پذیری‌های جاسازی‌شده به کار رود. برای مقابله با موارد غیر بر خط، فریب دادن را می‌توان به حالات غیر محاسباتی نظیر باز گذاشتن عمدی در کابینت یا گاوصندوقی تعمیم داد که در حالت معمولی باید قفل

باشد و مدارک ساختگی در آن قرار داده شده است تا افراد داخل سازمان بدخواه را گول بزند.

هدف طراحی فریب در هنگام پویش در دسترس قرار دادن واسطی با سه جز متمایز است: سرویس‌های مجاز، آسیب‌پذیری‌های واقعی و آسیب‌پذیری‌های ساختگی. در جهان کامل، هیچ‌گونه آسیب‌پذیری موجود نخواهد بود و تنها سرویس‌های مجاز وجود دارند. متأسفانه به علت پیچیدگی بسیار بالای مرتبط با سرویس‌های زیرساخت ملی انتظار عدم وجود آسیب‌پذیری، غیر واقعی است، بنابراین آسیب‌پذیری‌های واقعی، همیشه، به شکل خاصی حضور خواهند داشت. زمانی که فریب دادن به کار گرفته می‌شود، این آسیب‌پذیری‌های حقیقی با انواع قلابی آن جمع شده و باید از یکدیگر غیرقابل تمایز باشند. بنابراین، زمانی که واسط سرمایه‌های ملی با فریب ارائه شوند دشمن سه جز را می‌بینند. (به شکل ۲-۳ توجه کنید).



شکل ۲-۳- واسط خدمات سرمایه‌های ملی با فریب دادن

آسیب‌پذیری‌های ساختگی، معمولاً، بر اساس انواع معمول مسائلی که در نرم‌افزارها یافته می‌شوند، جاسازی می‌گردند. این یکی از موارد معدودی است که در آن نقاط ضعف و عیوب مهندسی نرم‌افزار عملاً می‌تواند مورد استفاده خوب برای امنیت قرار گیرد. می‌توان مواردی را تصور کرد که آسیب‌پذیری‌های جدید را کشف و سریعاً از آن‌ها

به عنوان تله در سیستم‌هایی استفاده می‌شود که احتیاج به حفاظت دارند. به حال سوراخ‌های جاسازی‌شده همیشه نباید بر اساس چنین باگ‌های نرم‌افزاری قابل‌استفاده یا عدم پیکربندی‌های درست سیستم بنا گذاشته شوند. در برخی موارد، آن‌ها می‌توانند متناظر با قابلیت‌هایی با مدیریت مناسب باشند؛ اما ممکن است این موارد را برای استفاده‌های محلی نپذیرند.

ظروف عسل می‌توانند در داخل وب سایت‌ها ساخته شوند.

یک مثال خوب از یک تله که بر اساس یک قابلیت مدیریت شده مناسب پایه‌گذاری شده است برگ‌های بی‌قاعده در یک وب سایت می‌باشد که به صورت آشکار تقاضای نشت اطلاعات می‌نمایند و این بعضی مواقع در برخی بلوگ‌های بحث‌برانگیزتر یافت می‌شود. اگر به آن‌ها پذیرش سیاستی و قانونی داده شود، این لینک‌ها در اینترانت‌های پروکسی شده محلی به یک سایت ظرف عسل جمع‌آوری اطلاعات وصل می‌شوند. اگر افراد داخل سازمان بخواهند اطلاعات را به طور مستقیم از طریق این لینک به سایت‌های به ظاهر معتبر در اینترنت نشت نمایند، اطلاعاتشان که در اثر فریب خوردن نشت کرده‌اند، به یک تیم امنیتی سازمان نشت می‌شود. این مورد را تنها زمانی می‌توان به کاربرد که الزامات قانونی و سیاستی آن رعایت شده باشد؛ این مثال احتمالات مختلف رانشان می‌دهد.

یک هدف برجسته فریب دادن، مشاهده دشمن در حین عمل است. این عمل با گردآوری زمان واقعی داده‌ها در مورد فعالیت‌های نفوذگر همراه با تجزیه و تحلیل مستدل منظور او انجام می‌شود. برای مثال؛ اگر یک نفوذگر، در حال حدس زدن کلمه‌های عبور به صورت تکراری برای دسترسی به یک سیستم ظرف عسل باشد، ممکن است مدیریت در زمان واقعی تصمیم به واگذاری دسترسی به او بگیرد. چالش بزرگ، خودکار کردن و اتوماسیون چنین تصمیم‌گیری‌هایی برای پاسخ‌گویی است که در

حال حاضر کاملاً شناخته‌نشده و بسیار کم در برنامه‌های تحقیقاتی امنیت گنجانده شده است. این خیلی بد است؛ زیرا چنین حالاتی می‌تواند باعث چالش شود و نهایتا، مهارت‌های یک مدیر امنیتی خوب را بهبود بخشد. حتی می‌توان تصور کرد که گروه‌های ملی مسابقاتی را بین نفوذگرها و مدیران امنیتی به صورت زنده برگزار کنند که در آن نفوذگرها و مدیران امنیتی با یکدیگر در حال جنگ باشند، جنگی به صورت زمان واقعی در یک ظرف عسل ساختگی.

۲-۲- پرت‌های عمداً باز

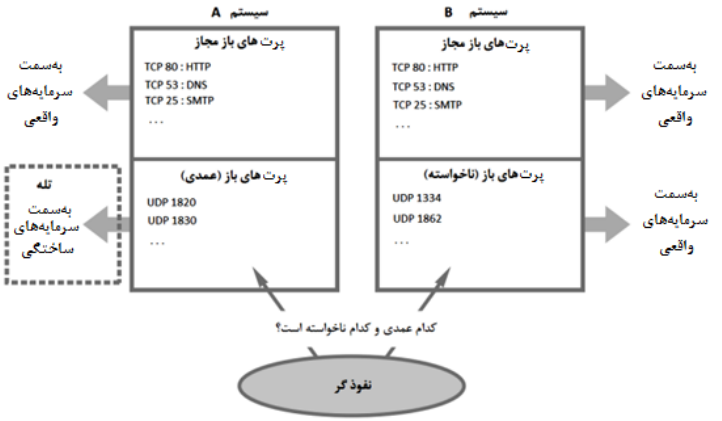
نفوذگران به طور منظم در اینترنت جستجو می‌کنند، تا سرورهایی را بیابند که به آن‌ها اجازه اتصال برای استفاده از سرویس‌های ورودی قابل بهره‌برداری خود را می‌دهند. این سرویس‌ها، معمولاً، قابل سو استفاده هستند، زیرا ضعف‌هایی مثل شرایط سرریز با فر رادارند و می‌توان از آن‌ها برای به دست آوردن دسترسی با ارجحیت استفاده کرد. زمانی که دسترسی با ارجحیت امکان‌پذیر شود، نفوذگر می‌تواند وظایف مدیر سیستم را انجام دهد؛ این وظایف می‌توانند نظیر؛ تغییر فایل‌های سیستم، نصب بد افزارها و دزدی اطلاعات حساس باشند. تمام مدیران خوب سیستم اهمیت محکم کردن سرورها را با غیرفعال کردن تمام سرویس‌های غیر لازم و قابل سواستفاده درک می‌کنند. مسئله این است که محکم کردن، فرآیند پیچیده‌ای است که حتی می‌تواند در محیط‌هایی که سیستم عامل اختصاصی و غیر شفاف دارند، بسیار پیچیده‌تر هم باشد. تعجب‌آور است که بسیاری از فروشندگان نرم‌افزار و سرورها هنوز محصولاتشان را با پیکربندی که در آن‌ها بسیاری از سرویس‌ها به صورت پیش‌فرض فعال می‌باشند تحویل می‌دهند. سر راست‌ترین شیوه بین تمام شیوه‌های عمل فریب دادن محاسباتی، جاسازی عمدی پرت‌های سرویس باز در واسط سرور به اینترنت است.

پرت‌های عمداً باز به قابلیت ظرف عسل در پشت سیستم وصل می‌شوند که خود به سیستم‌های نظارتی جهت مشاهده و تجزیه و تحلیل متصل هستند. نتیجه اینکه

سرورها به دشمنان زیرساخت‌های ملی سه منظره متفاوت از پرت‌های سرویس باز را ارائه می‌دهند:

- پرت‌های باز معتبری که می‌توان انتظار داشت نظیر پرت‌های HTTP، DNS و SMTP.
- پرت‌های بازی که سهواً بازمانده‌اند و ممکن است متناظر با نرم‌افزارهای قابل سو استفاده باشند.
- پرت‌های بازی که عمداً جاسازی‌شده‌اند و به سرمایه‌های ساختگی در یک ظرف عسل وصل هستند.

تا زمانی‌که دشمن درک کند که فریب دادن می‌تواند به‌طور بالقوه استفاده شده باشد،در او مقداری تردید در مورد اینکه کدام پرت‌هاعمداً وکدام سهواً باز هستند وجود خواهد داشت. (به شکل ۲-۴ توجه کنید).

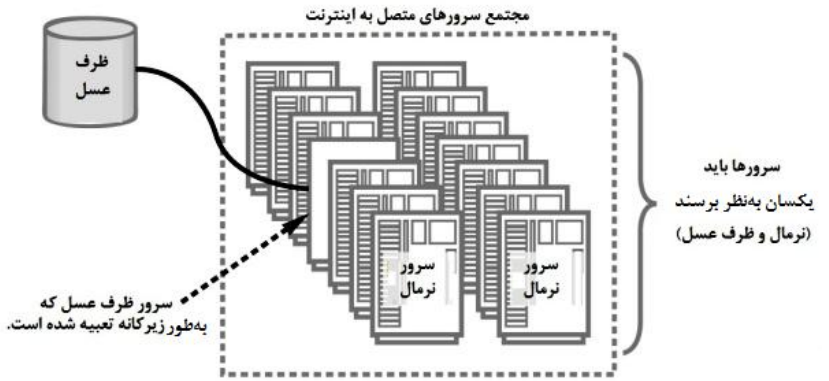


شکل ۲-۴- استفاده از فریب با پرت‌های باز برای سرمایه‌های ساختگی

مدیران امنیتی که از اسکنرهای پرت به عنوان قسمتی از یک برنامه معمولی حفاظت شبکه شرکت یا بنگاه تجاری استفاده می‌کنند، از فریب دادن، به طور نادرست

استفاده می‌کنند. چیزی که اتفاق میفتد، این است که اسکنر، تعدادی پرت باز را پیدا می‌کند که عمداً به عنوان تله جا سازی شده‌اند و باعث تولید گزارشاتی می‌شود که باعث برجسته شدن آسیب‌پذیری‌های فرض شده برای مدیران، کاربران و ممیزین می‌گردد، برای جلوگیری از افشا و در معرض دید قرار گرفتن، می‌توان قسمتی از خروجی را به طور دستی برید؛ اما ممکن است یک بنگاه تجاری بزرگ، به علت عظیم بودن خروجی، نتواند این کار را انجام دهد. متأسفانه راه‌حل‌هایی برای حل ناسازگاری بین استفاده مجاز از اسکنر پرت و استفاده عمدی از پرت‌های باز به عنوان تله به آسانی مشخص نمی‌شود و این یک زمینه دیگر تحقیق و توسعه در محاسبات فریب دادن است.

یک ملاحظه دیگر در استفاده عمدی از پرت‌های باز، این است که بایستی به نرم‌افزارهای عقبه سیستم توجه کرد تا اطمینان حاصل شود که سرمایه‌های واقعی نمی‌توانند مورد سواستفاده قرار گیرند. تعجب‌آور نیست که تکنیک‌های عملی برای انجام این عمل به خوبی شناخته‌شده نیست. برای مثال؛ اگر نرم‌افزار فریب دادن عقبه سیستم به پرت‌های عمداً بازی وصل شوند که با سرمایه‌های معتبر در منابع سهیم هستند، می‌توانند آثار جانبی منفی به وجود بیاورند. امروزه، تنها رویکرد عاقلانه قرار داشتن پرت‌های عمداً باز روی سرورهای ساختگی است که ظروف عسل با هیچ‌گونه منابع معتبر هستند. این سرورها باید به طور زیرکانه‌ای در مجموعه سرورهایی جاسازی شوند که نرمال و طبیعی به نظر بیایند و به سرمایه‌های جداگانه ظرف عسل متصل باشند. این روش، احتمال آثار جانبی منفی را روی سرورهای معمولی کاهش می‌دهد.
(به شکل ۲-۵ توجه کنید).



شکل ۲-۵- تعبیه سرور ظرف عسل در داخل یک مجموعه سرور معمولی

در عمل چالش واقعی در استفاده از فریب دادن در پرت‌های باز، ایجاد قابلیت‌های متصل به پرتی است که به قدر کافی معتبر است و می‌تواند دشمن خبره را گول بزند. در همان حال، به طور مناسبی از سرویس‌های معتبر جدا باشند، طوری که دشمن نتواند با استفاده از ظرف عسل حمله‌اش را پیش ببرد.از آنجا که علم کامپیوتر کمک پایه‌ای زیادی در این رابطه ارائه نمی‌کند، ابتکارات حفاظت زیرساخت‌های ملی باید شامل برنامه‌های فوری باشد که موجب تحقیق، توسعه و جلو راندن این تکنیک‌ها می‌شود.

۲-۳- مرحله اکتشاف

مرحله اکتشاف، مرحله‌ای است که در آن دشمن طعمه امنیتی را که در تله جاسازی شده است، یافته و آن را می‌پذیرد. دو هدف امنیتی که در این مرحله مورد نظر است؛ عبارتند از:

نفوذگر باور کند که آسیب‌پذیری واقعی می‌تواند ساختگی باشد و آسیب‌پذیری ساختگی می‌تواند واقعی باشد. اولین هدف با ساختن یک برنامه فریب دادن انجام می‌شود

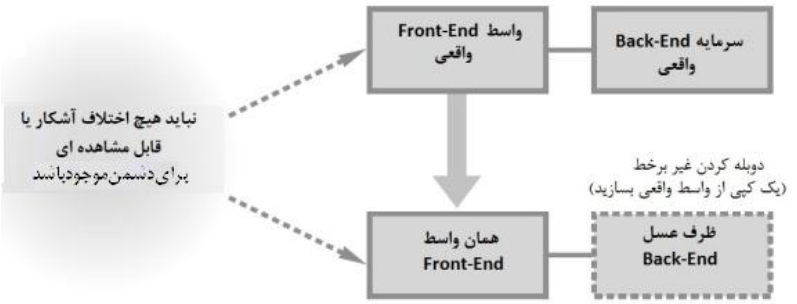
که به خوبی تثبیت‌شده و آشکارا شناخته شده باشد. تکنیک‌های ویژه برای انجام آن شامل موارد زیر است:

- تحقیقات حمایت‌شده: استفاده از فریب دادن در زیرساخت‌های ملی می‌تواند به صورت عمومی با حمایت باز و بودجه گذاری تحقیقات طبقه‌بندی نشده و کارهای توسعه‌ای در این زمینه فرض و پذیرفته شود.
- مطالعات موردی چاپ‌شده: انتشارات باز و علنی مطالعات موردی نشان می‌دهد که از فریب دادن به طور مؤثری برای حفاظت از زیرساخت‌های ملی استفاده شده است و با این شیوه، احتمال اینکه دشمن یک آسیب‌پذیری یافته شده را عمدی فرض نماید، افزایش می‌یابد.
- درخواست‌های باز و علنی: درخواست برای اطلاعات (RFI) و درخواست برای پیشنهاد (RFP) را باید مسئولان حفاظت از زیرساخت‌های ملی به صورت باز و علنی صادر کنند. به آن معنی که تخصیص بودجه باید به سمت پروژه‌های امنیتی جهت داده شود که از روش‌های فریب دادن استفاده می‌نمایند.

تردید و شک دشمن پیش از استفاده از آسیب‌پذیری واقعی، فقط زمانی افزایش می‌یابد که استفاده از فریب دادن به نظر یک احتمال واقعی بیاید. برای مثال؛ اعلام ساده اینکه از فریب دادن استفاده شده است، بدون سعی و تلاش صادقانه برای به‌کارگیری واقعی چنین فریب‌هایی در زیرساخت ملی یک هدف تو خالی خواهد بود. درست مانند این است که تابلوی علامت حفاظت از منزل را در یک چشم‌انداز قرار دهیم، بدون اینکه سیستم امنیتی واقعی در آن نصب کنیم. برای اینکه تبلیغات علنی فریب دادن مؤثر باشد، تیم حفاظت زیرساخت ملی باید به طور کامل به انجام عملی کارهای مهندسی پیاده‌سازی و عملیات فریب دادن متعهد شوند.

هدف دوم از واقعی به نظر رسیدن آسیب‌پذیری‌های ساختگی برای متخصصان امنیت کامپیوتری، استفاده از ظرف عسل است. از تکنیک دوبله سازی، معمولاً، در

طراحی ظرف عسل استفاده می‌شود، جایی که یک سیستم ساختگی کپی کامل یک سیستم واقعی است، بدون اینکه به سرمایه واقعی متصل باشد که حفاظت می‌شود. این عمل، معمولاً، با دوبله کردن واسط ورودی به یک سیستم واقعی و قرار دادن سیستم دوبله و ظرف عسل در پشت آن انجام می‌شود. دوبله کردن، میزان واقعی به نظر رسیدن را به شدت افزایش می‌دهد و اجرای آن آسان است. (به شکل ۲-۶ توجه کنید).



شکل ۲-۶ دوبله کردن در طراحی ظرف عسل

همان طور که در بالا پیشنهاد شد، مزیت دوبله کردن در طراحی ظرف عسل عبارت از بیشینه کردن اصالت است. برای مثال؛ اگر یک آسیب‌پذیری واقعی در برخی سرورهای ورودی یافت شود، می‌توان از آن به عنوان مرحله ورودی سرور در پیکربندی گمراه‌کننده آینده استفاده کرد. برنامه‌های حفاظت از زیرساخت‌های ملی باید راه‌های مؤثری جهت مرتبط نمودن فرآیند کشف آسیب‌پذیری‌ها به طراحی ظرف عسل بیابند. بنابراین، زمانی که یک آسیب‌پذیری جالب‌توجه یافته شد، از این آسیب‌پذیری باید در مرحله ورودی تله گمراه‌کننده بعدی استفاده شود.

۲-۴- مستندات و مدارک گمراه‌کننده

ایجاد مدارک فریب‌دهنده و قرار دادن آن‌ها در محل‌های خاص، مثالی از یک روش حقه زدن به دشمن در هنگام کشف است. این تکنیک که می‌تواند به صورت الکترونیکی یا دستی انجام شود، به طور مخصوص برای کشف حضور یک عنصر داخلی بدخواه، مفید است و تنها تحت دو شرط مؤثر خواهد بود:

- محتوا: مدارک ساختگی باید شامل اطلاعاتی باشد که به طور متقاعد کننده‌ای واقعی به نظر برسند. دوبله کردن یک مدرک واقعی با تغییراتی در حساس‌ترین اجزا آن، یک راه سر راست برای انجام آن است.
- حفاظت: قرار دادن مدرک ساختگی باید شامل حفاظت‌های کافی باشد تا مدارک واقعی به نظر برسند. اگر رویکرد حفاظت ضعیف باشد، باعث سوظن فوری خواهد شد. خرابکاری را می‌توان با حفاظت از مدارک ساختگی در محیطی کشف نمود که شخصی به جز عوامل داخلی مورد اعتماد نمی‌توانند به آن دسترسی داشته باشند.

مراحل یک رویکرد گویا برای حفاظت از زیرساخت ملی:

اول، یک مدرک با اطلاعاتی ایجاد شود که به یک سرمایه ساختگی، مخصوصاً تولیدشده مثل یک شماره تلفن، آدرس یک محل فیزیکی و یک سرور اشاره دارد، ایجاد. این اطلاعات، هرگز، نباید واقعی باشد؛ ولی باید به نظر واقعی برسد. سپس، مدرک در محلی که به شدت حفاظت می‌شود؛ مثل یک گاوصندوق یا کامپیوتر مطمئن ذخیره شود (کامپیوتر یا فیزیکی). فرض کنید که در شرایط نرمال مدارک در محل قفل شده و مطمئن خود به صورت بی‌استفاده باقی خواهند ماند؛ زیرا هیچ استفاده حقیقی برای هیچ کس نخواهد داشت. در نهایت، این سرمایه ساختگی مخصوصاً تولیدشده، به دقت

از نظر هر تلاشی جهت نقض امنیتی نظارت می‌شود، اگر کسی این مدرک را بیابد و آن را بردارد، می‌توان نتیجه گرفت که آن عنصر داخل سازمان قابل‌اعتماد نیست.

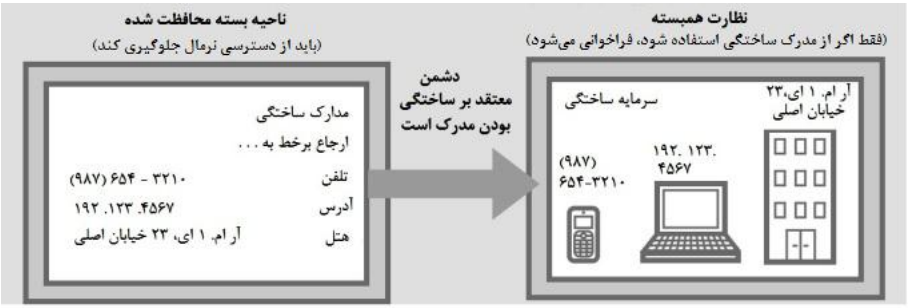
قدم‌های جاسازی یک مدرک ساختگی

برای جاسازی مؤثر یک مدرک ساختگی، باید نکات زیر را در نظر داشت:

۱- یک فایل ایجاد کنید با دستورالعمل‌هایی که به نظر می‌آید اطلاعات فوق‌العاده حساسی را می‌توان از آن به‌دست آورد. این فایل می‌تواند شامل یک شماره تلفن، آدرس اینترنتی یک سرور و شاید اتاقی دریک هتل باشد.

۲- محتویات فایل را رمزنگاری کرده و آن را در یک سرور ذخیره کنید (یا چاپ‌شده آن را در گاوصندوق قرار دهید و آن را قفل کنید) به طوری که فرض شود که از دسترس داخل و خارج حفظ شده است.

۳- امکانات نظارتی روی سرور یا گاوصندوق را بدون محدودیت زمانی فعال کنید. در حقیقت، نظارت ممکن است تا بی‌نهایت ادامه یابد؛ چون ممکن است انتظار داشت که رفتاری مرتبط و همبسته با این سرمایه‌های ذخیره‌شده، تحت نظارت مشاهده نشود. (به شکل ۲-۷ توجه کنید).



شکل ۲-۷- جاسازی یک مدرک ساختگی در یک محیط محاصره‌شده

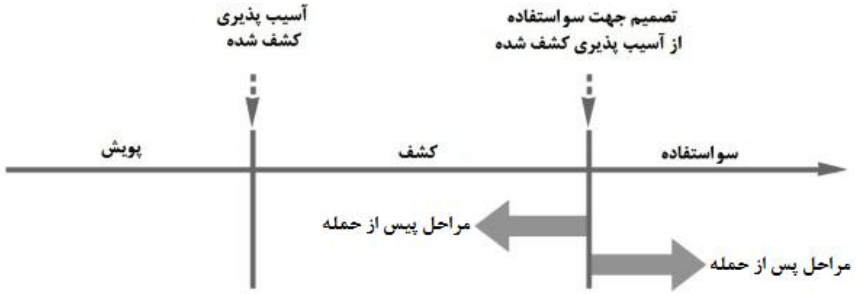
باید آشکار باشد که طرحی که به طور مثال در شکل ۲-۷ نشان داده شده است، برای یک مدرک الکترونیکی که با رمزنگاری و کنترل دسترسی حفاظت‌شده، به همان خوبی یک مستند و مدرک کاغذی حفاظت می‌شود که در یک گاوصندوق قفل شده قرار داشته باشد. در هر دو حالت، باید انتظار داشت که هیچ‌کسی این مراجع ساختگی را به هم همبسته ننماید. اگر معلوم شود که نظارت به نحو مرتبطی دسترسی به این سرمایه ساختگی را نشان می‌دهد، باید فرض کرد که محاصره حفاظت‌شده مورد نقض امنیتی قرار گرفته است. (نظارت اتاق‌های هتل ممکن است به پشتیبانی تدارکاتی پیچیده‌ای؛ نظیر؛ استفاده از دوربین‌های مخفی احتیاج داشته باشد.) به هر صورت، این سرمایه‌ها سکویی را برای تجزیه و تحلیل‌های بعدی فعالیت‌های سواستفاده دشمن ایجاد می‌کنند.

۲-۵- مرحله سو استفاده

مرحله سوم در چرخه فریب دادن برای دشمن، شامل سواستفاده از یک آسیب‌پذیری کشف شده است. این یک قدم کلیدی در فرآیند تصمیم‌گیری برای یک دشمن می‌باشد؛ زیرا، معمولاً، اولین مرحله‌ای است که در آن قواعد سیاستی یا حتی قوانین شکسته و نقض می‌شود. هنگامی‌که نفوذگران شروع به ایجاد یک حمله سایبری می‌کنند، قدم‌های ابتدایی مربوط به تهیه مقدمات را برداشته و معمولاً، قواعد سیاست‌های امنیتی یا قانون را نقض نمی‌نمایند. برخی مواقع، متخصصان امنیتی از این فعالیت‌های ابتدایی به عنوان فعالیت‌های رادار پایین یاد می‌کنند؛ اگر این فعالیت‌ها کشف شوند، با کلمات نشانه و هشدار به آن‌ها اشاره می‌شود. مشخص کردن این که آیا باید نسبت به نشانه‌ها و هشدارها واکنشی نشان داد، خود یک چالش است؛ زیرا پاسخ به آن‌ها احتیاج به زمان و انرژی دارد. اگر سابقه تیم امنیتی دربرگیرنده بسیاری از عملیات واکنش به نشانه‌ها و هشدارها باشد، که معمولاً، بیشتر آن‌ها مثبت کاذب هستند، سازمان برای کاهش نقطه تریگر واکنش وسوسه می‌شود. این یک نظر و ایده بد برای

زیرساخت‌های ملی است؛ زیرا شانس اینکه یک واقعه حقیقی اتفاق بیفتد، به سرعت زیاد می‌شود.

بنابراین، در حفاظت از زیرساخت‌های ملی باید ذهن را از سعی در کاهش واکنش‌ها به نشانه‌ها و هشدارهای مربوط به مثبت‌های کاذب دور کرد. هدف باید مقابله با تمام مواردی باشد که در آن‌ها اعمال نشانه‌ها و هشدارها به نظر می‌رسد که در حال ایجاد آستانه لازم برای شروع سواستفاده هستند. این مسئله به خصوص مهم است؛ زیرا این آستانه‌ها، علائم اولین مرحله‌ای است که در آن اگر سرمایه‌های واقعی مورد هدف باشند، ممکن است صدمه ببینند. (به شکل ۲-۸ توجه کنید).



شکل ۲-۸- مراحل قبل و بعد از حمله در مرحله سواستفاده

نیاز کلیدی در این نقطه تصمیم‌گیری، عبارت از این است که هر بهره‌گیری از سرمایه ساختگی نباید باعث مسائلی مربوط به افشا، یکپارچگی، دزدی یا دسترس‌پذیری در سرمایه واقعی شود. هنگامی که این سرمایه‌ها تا حد ممکن جدا باشند، انجام چنین عدم تداخلی بین سرمایه‌های ساختگی و واقعی بسیار ساده است. جدایی فیزیکی سرمایه‌ها آسان است. برای مثال؛ یک کاربرد نرم‌افزاری با داده‌های حقیقی رامی توان، باقراردادن آن‌ها در سرورهای مختلف یا حتی شبکه‌های متفاوت از یک کاربرد ساختگی با داده‌های قلابی جدا نمود. این همان روشی است که بسیاری از ظروف عسل بر اساس

آن عمل می‌کنند و ریسک تداخل در آن، معمولاً، پایین است. در محیطی که تسهیم منابع بین سرمایه‌های حقیقی و قلابی وجود داشته، رسیدن به عدم تداخل چالش برانگیزتر خواهد بود. برای رسیدن به هدف عدم تداخل، طراح فریب باید خلاقیت داشته باشد. برای مثال؛ اگر برخی فرآیندهای تجاری در هردو قابلیت‌های حقیقی و قلابی به اشتراک گذارده شوند، مجریان فریب باید دقت کنند که تضمین شود سیستم واقعی به هیچ وجه تضعیف نمی‌شود.

تحقیقات مختصری در این زمینه به خصوص در مورد تهدیدات دسترس‌پذیری انجام شده است. برای مثال؛ اجازه دادن به یک دشمن بدخواه برای اجرا برنامه‌ها روی یک سیستم زنده و معتبر، فرصت‌هایی را برای فرسایش منابع به صورت بدخواهانه ایجاد می‌نماید. هر حال، رویکرد عمومی دارای وعده‌های قابل‌توجهی است و سزاوار توجه بیشتری می‌باشد. ممکن است سیستم‌های کشف نفوذ و پاسخ به حوادث در هنگام سواستفاده، فریب داده شوند و باور کنند که قابلیت تله یک قابلیت واقعی است. سال‌ها است که طراحان فریب در شرکت‌ها با این مسئله مقابله نموده‌اند. آن‌ها باید با تیم‌های امنیتی طوری هماهنگ باشند که تضمین شود فعالیت آن‌ها باعث ایجاد آلارم‌های کاذب نشود و این کار می‌تواند از راه‌های مختلفی انجام شود:

- هماهنگی فرآیند: در این مرحله، تیم ظرف عسل فعالیت‌های خود را از پیش با تیم‌های امنیت زیرساخت هماهنگ می‌کند. عیب این مسئله برجسته شدن فریب است و ممکن است باعث تخریب شفافیت‌های پنهان شود، به خصوص اگر فریب جهت کشف کارمندان داخلی بدخواه طراحی شده باشد.
- ایزوله کردن تله: برای مطمئن شدن از این است که سیستم امنیتی مثل پروب‌های کشف نفوذ در مسیرهای فریب نیستند. در این حالت، تجزیه و تحلیل ساختاری مداوم لازم است تا اطمینان ایجاد شود که این شرایط در طول چرخه سیستم باقی می‌مانند.

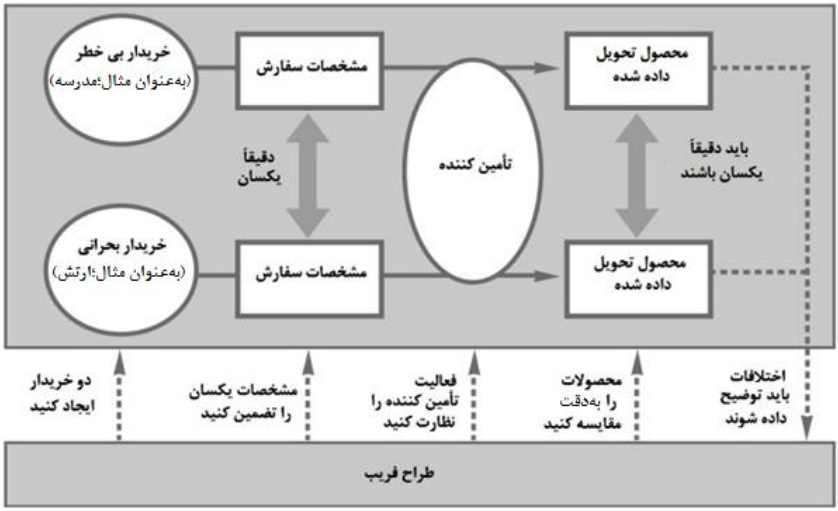
- کارمند داخلی در داخل سیستم: اگر تیم امنیتی شامل بعضی کارمندان داخلی مورد اعتماد باشد که درگیر فعالیت‌های واکنش و پاسخ هستند، در این صورت آن‌ها می‌توانند با اطمینان از اینکه واکنش‌هایشان ضایع کردن زمان و منابع نیست به فعالیت‌هایشان ادامه دهند؛ در حالتی که کارمند داخل تیم یک تصمیم گیر باشد، کار به بهترین وجه انجام خواهد شد.
- کمک‌هزینه اضافی فرآیند: در صورت وجود کمک‌هزینه، فعالیت‌های کشف و واکنشی مجاز به ادامه خواهند بود. اگر فرض شود که فریب دادن است و باید کاملاً از تمام کارمندان داخلی پنهان نگه داشته شود و انجام آن توصیه می‌شود.

مرحله سواستفاده، خطرناک‌ترین قسمت چرخه عمر فریب دادن است؛ زیرا شامل فعالیت‌های بدخواهانه واقعی دشمن است. اگر این مرحله به دقت مدیریت شود، تیم‌های زیرساخت باید فهمیدن و احترام به زیان‌های حقیقی بالقوه را یاد بگیرند.

۲-۶- حقه‌های خرید

یک راه برای فهمیدن رفتار دشمن، مقایسه آن در محیط‌های مختلف است. برای مثال؛ یک طراح فریب دو درخواست مجزای خرید یک کالا یا سرویس داده‌شده را تهیه نماید. یک درخواست برای یک کاربرد بی‌خطر، غیر بحرانی و غیر حساس و دیگری برای کاربردی آشکارا حساس و از نظر ملی بحرانی خواهد بود. در هر دو حالت، دقیقاً باید همان محصول یا سرویس را درخواست کرد؛ اما زمانی که محصول یا سرویس درخواست شده به کاربرد خود تحویل می‌شود، امتحانات مشروحی برای شناسایی اختلافات باید شروع شود. هر اختلاف یافته شده بین دو محصول دریافت شده را هر یک از دو خریدار

که به صورت عمدی جاسازی‌شده‌اند، به عنوان یک exploit بالقوه تلقی می‌کنند (به شکل ۲-۹ توجه کنید).



شکل ۲-۹- استفاده از فریب دادن در مقابل تأمین‌کنندگان بدخواه

فریب توضیح داده‌شده در بالا زمانی مؤثر است که قابلیت فارنسیک برای مقایسه دو محصول وجود داشته باشد. برای هر محصول یا سرویس، این می‌تواند شامل مقایسه اندازه نسبی نرم‌افزار، عملکرد سیستم، مستندات محصول، قابلیت سرویس یا حمایت فنی از محصول باشد. حتی می‌توان سطح دومی از فریب را با استفاده از مهندسی اجتماعی تصور کرد که در آن درخواست هیجان‌آوری از تأمین‌کننده‌ای برای ارائه سیستم پشتیبانی اضطراری مستند نشده‌ای انجام شود که معمولاً، از نوع مدیریت از راه دور است. اگر هر کدام از محصولات تحویل‌شده برای مدیریت از راه دور راه‌اندازی شود، مدیر سرمایه‌های ملی باید بداند که اشکالی در کار است.

چرخه عمر خرید و تدارکات یکی از دست کم گرفته‌ترین اجزا در حفاظت از زیرساخت‌های ملی از منظر و نگاه حمله می‌باشد. معمولاً تیم‌های امنیتی روی انتخاب، تست، نصب و قابلیت‌های بهره‌برداری تمرکز می‌کنند و عملیات اجرایی خریداری را به عهده تیم زنجیره تأمین می‌گذارند. این یک اشتباه بزرگ است و دشمنان این نکته را به خوبی می‌دانند. بنابراین، ابتکارات حفاظت از زیرساخت ملی باید به فرآیند خرید و تدارکات توسعه یابد؛ استفاده زیرکانه از فریب دادن ابزار قدرتمندی در این مورد است.

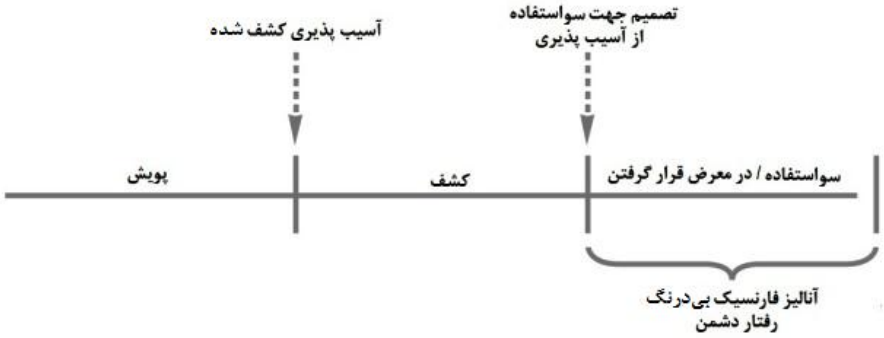
۲-۷- مرحله (در معرض قرار گرفتن) ظاهر شدن

آخرین مرحله در چرخه فریب دادن، شامل ظاهر شدن رفتار دشمن در مقابل اپراتور فریب است. احتمالاً، در این مرحله دشمن در قابلیت تله قرار دارد و متقاعد شده است که تمام سیستم‌ها و سرمایه‌ها واقعی هستند. همه گونه احتمال جهت اینکه عمل هک دشمن چگونه جلو خواهد رفت وجود دارد که، این می‌تواند بارشی ناگهانی از فعالیت‌های شدید در یک زمان کوتاه یا فرآیندی آهسته و طولانی از عملیات کوتاه و آهسته باشد. بنابراین؛ تیم فریب باید بردبار و صبور باشد. هم چنین، در این مرحله ممکن است دشمن استفاده از تکنیک‌های معروف هک کردن و ابزارهای آن را به کاربرد؛ یا از تکنیک‌هایی استفاده کند که تیم امنیتی پیش از آن ندیده است.

(به شکل ۲-۱۰ توجه کنید).

در این مرحله، چالش این است که در فریب دادن باید یک پنجره برای مشاهده فعالیت‌های نفوذگر ایجاد نمود؛ در همان حال باید این مشاهده پنهان بماند. باید یک واسط راحت برای تیم فریب ایجاد شود تا داده‌ها را جمع‌آوری کند. در همان حال، راهی را ارائه نماید برای فرمان‌های صادره برای تغییراتی که باید به صورت بی‌درنگ و در زمان واقعی اجرا شوند. متأسفانه، تعداد کمی از محصولات تجاری وجود دارند که برای

حمایت از این ویژگی‌ها طراحی‌شده‌اند. الزامات عملکردی خاص برای نظارت محیط در طول مرحله ظاهر شدن دشمن در عملیات فریب شامل موارد زیر است:



شکل ۲-۱۰- مرحله ظاهر شدن دشمن در هنگام فریب

- جزییات کافی: محیط نظارت باید جزییات کافی به اپراتور فریب ارائه دهد تا او بتواند تعیین نماید که چه چیزی باید انجام شود. برای مثال؛ لاگ‌های ممیزی به شدت رمز شده با فرمت ساده و مختصر بافاصله‌هایی در بعضی قسمت‌ها بهترین رویکرد نیستند. واسط مدیریتی معمولی به سیستم‌عامل (معمولاً از طریق واسط فرمان‌ها) معمولاً، مطلوب‌ترین رویکرد است. نباید نمایشگرهای فانتزی و رنگارنگ برای عمل نظارت انتظار داشت؛ زیرا بیشتر تحلیل گران امنیتی راحتی کار با یک واسط مختصر و ساده خط فرمان را ترجیح می‌دهند.
- کاوشگر یا پروب‌های پنهان: نظارت در این مرحله از فریب دادن تنها هنگامی مؤثر است که کاملاً پنهان باشد. اگر دشمن متوجه شود که کسی او را تماشا می‌کند، فوراً رفتارش را تغییر می‌دهد. کارهای ساده‌ای؛ نظیر؛ لیست کردن فشرده فرآیندهایی که به وسیله تیم فریب شروع می‌شود

باید پیاده‌سازی شود. هنر ایجاد قابلیت‌های واقعی برای پنهان کردن پروب‌ها احتیاج به حمایت و پرورش در جامعه امنیتی دارد.

- مشاهده زمان واقعی یا بی‌درنگ: اپراتور فریب باید دسترسی به اطلاعات مربوط به رفتار ظاهرشده دشمن در حین انجام آن را داشته باشد. درجه بی‌درنگ و زمان واقعی بودن برای چنین نظارتی (برای مثال؛ فوری بودن، در چند ثانیه، چند دقیقه) بستگی به شرایط محلی دارد. در بسیاری از موارد این مشاهده از طریق دیدن لاگ‌های سیستم به سادگی انجام می‌شود؛ اما ابزارهای پیشرفته‌تری لازم است تا اطلاعات مربوط به رفتار یک نفوذگر را ثبت و ذخیره نماید.

همان طور که در بالا پیشنهاد شد، در تمام موارد نظارت بر فریب، هدف کلیدی طراحی باید اطمینان از ایجاد محیطی باشد که دشمن بتواند آن را باور کند. نباید هیچ فرآیند مشکوک و غیرقابل توضیحی وجود داشته باشد که به نفوذگر علامت دهد سیستم در حال لاگ گرفتن است. لاگ‌های قلابی ممیزی راه خوبی برای ایجاد این باور هستند. اگر یک ظرف عسل با استفاده از یک سیستم‌عامل با لاگ ممیزی نرمال توسعه یابد می‌توان این سیستم لاگ گیری را فعال کرد. یک دشمن خوب این سیستم لاگ گیری را غیرفعال خواهد کرد. ایده این است که نظارت پنهان را زیر سیستم لاگ گیری نرمال قرار دهیم و این همان قابلیتی است که دشمن نمی‌تواند آن را غیرفعال نماید.

۲-۸- واسطهای بین انسان‌ها و کامپیوترها

معمولاً جمع‌آوری شواهد فارنسیک در هنگام تجزیه و تحلیل رفتار نفوذگر در ظرف عسل متکی بر فهمیدن این است که چگونه سیستم‌ها، پروتکل‌ها و خدمات تعامل می‌نمایند. این نوع ارتباطات می‌تواند در چهارراه مختلف انجام شود: انسان به انسان، انسان به کامپیوتر، کامپیوتر به انسان و کامپیوتر به کامپیوتر. اگر منظور از اولین کلمه

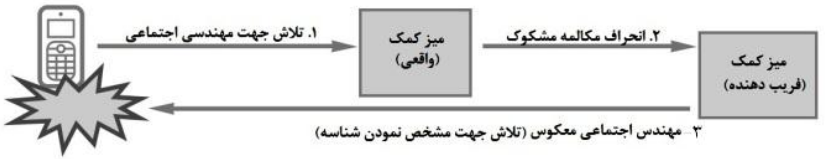
(انسان یا کامپیوتر) نفوذگر و دومین کلمه مدیر ظرف عسل باشد، می‌توانیم تمایز منطقی را ایجاد کنیم.

اول: باید آشکار باشد که در یک حمله خودکار شده مثل یک باتنت بر اساس بعضی مشاهدات ذهنی قابلیت‌های ظرف عسل، رفتار بی‌درنگ سیستم حمله تغییر نخواهد کرد. تفسیر نتایج حمله باتنت به آسانی روی تفکر اپراتور باتنت اثر می‌گذارد؛ اما تأثیری بر قابلیت‌های بی‌درنگ ندارد به این ترتیب، قدرتمندترین حالات در تجزیه و تحلیل فارنسیک زمان واقعی و بی‌درنگ رفتار یک ظرف عسل در مواردی است که تعاملات بین انسان به انسان و انسان به کامپیوتر با یک نفوذگر انجام می‌گیرد. بگذارید هر کدام را به نوبه خود امتحان کنیم.

معمول‌ترین تعامل بین انسان به انسان در زیرساخت ملی شامل میز کمک[۱] یا قابلیت حمایت از مراقبت و پشتیبانی مشتریان است که رویکرد حمله متناظر با آن شامل مهندسی اجتماعی چنین فعالیتی می‌شود. وضعیت فعلی، پیشرفته‌ترین فناوری مقابله با این آسیب‌پذیری، آموزش اپراتورها و پرسنل مراقبت و پشتیبانی مشتریان است تا بتوانند تلاش‌های مهندسی اجتماعی را کشف و آن‌ها را به تیم امنیتی گزارش کنند. اما فریب دادن یک گزینه جالب‌تر را ارائه می‌کند، اگر احتمال تلاش برای استفاده از مهندسی اجتماعی بالا باشد، یک رویکرد پیشرفته برای حفاظت ممکن است گول زدن دشمن طوری باشد که او باور کند موفق شده است؛ این کار می‌تواند به آسانی از طریق آموزش اپراتورها به منتقل کردن تلاش‌های مهندسی اجتماعی به میز کمک قلابی مخصوصی انجام شود که برای این منظور ایجاد شده است. اپراتورها در این میزهای کمک ساختگی با تکنیک‌های معکوس مهندسی اجتماعی، حمله‌کنندگان را وادار به افشا شناسه و انگیزه‌شان می‌کنند. (به شکل ۲-۱۱ توجه کنید).

---

[۱] helpdesk



شکل ۲-۱۱- بهره‌برداری فریب‌دهنده از واسط انسان به انسان

معمول‌ترین تعامل بین انسان و کامپیوتر، زمانی اتفاق می‌افتد که نفوذگر سعی در به دست آوردن دسترسی غیرمجاز از طریق یک سری از فرمان‌های زنده و تعاملی می‌کند. نفوذگرها را باید طوری هدایت کنیم که باور کنند فعالیتشان باعث درخواست سرویس‌هایی در سیستم مورد هدف شده است؛ مانند آنچه در انواع معمول هک کردن سیستم‌های عامل اتفاق میفتد. برای مثال؛ تلاش نفوذگر ممکن است برای اجرای متوالی برخی فرمان‌ها و عملیات در سیستم تله باشد. اگر تیم امنیتی متوجه این قصد و منظور شود و بتواند به سرعت فرمان یا عمل مورد نظر نفوذگر را به طور عمدی اجرا کند، این تعامل حیله گرانه باعث می‌شود دشمن متخصص متوجه شود که پیکربندی سیستم هدف در حال تغییراست که واضح است که طبیعی نیست.

۲-۹- برنامه فریب ملی

امیدواریم که نوعی برنامه فریب ملی ایجاد شود که بر اساس مجموعه‌ای از تله‌ها، به صورت راهبردی در اجزا زیرساخت ملی جاسازی‌شده‌اند عمل نماید و با شبکه‌ای به یک مرکز تجزیه و تحلیل فریب متصل گردند. چنین رویکردی غیر محتمل است؛ زیرا فریب به عنوان رویکردی امنیتی به طور ضعیفی درک شده است و مدیران زیرساخت ملی، هنوز، برای اجازه دادن به نصب تله در سیستم‌های تولید مردد هستند. این تله‌ها اگر بد عمل کنند یا آن طور که تبلیغ‌شده عمل ننمایند، باعث حقه زدن به کاربران مجاز شده و عملیات طبیعی سیستم را مشکل خواهند کرد. هر ارزیابی واقعی از

شیوه‌های عمل فناوری امنیتی و اطلاعاتی فعلی پیشنهاد می‌کندکه امروزه، قبول فریب برای حفاظت از زیرساخت ملی به طور وسیعی پذیرفته نخواهد شد. در نتیجه، بهتر است برنامه‌های فریب ملی با توجه به مفروضات زیر طراحی شوند:

- استفاده از برخی زیرساخت‌های برگزیده: باید فرض کرد که برخی از اجزا زیرساخت، تله‌های فریب دارند و دیگران فاقد آن هستند. در زمان فعلی، هنوز، تیم‌های امنیت زیرساخت با مفاهیم فعلی ابتدایی امنیت کامپیوتری دست به گریبان هستند و ایده این که آنان با نصب تله موافقت کنند، واقع بینانه نیست. به این ترتیب، هر برنامه فریب ملی باید فرض کند که تمام اجزا از ظرف عسل به شیوه یکسان استفاده نخواهند کرد.
- به اشتراک‌گذاری نتایج و بینش‌ها: برنامه‌های فریب ملی می‌تواند و باید شامل مکانیزم و سازوکاری جهت به اشتراک‌گذاری نتایج و بینش‌های به دست آمده، از طریق استفاده عملیاتی از تله‌ها و ظروف عسل باشند. بینش‌های به دست آمده با تجزیه و تحلیل فارنسیک رفتار دشمن می‌تواند به صورت ساختار یافته به اشتراک گذارده شود.
- استفاده مجدد از ابزارها و روش‌ها: می‌توان از برنامه‌های فریب ملی به عنوان ابزاری برای در دسترس سازی نرم‌افزارهای ظرف عسل و تله در جهت به‌کارگیری بهره گرفت. در برخی موارد، ابزارهای فریب و روش‌هایی که در یک حوزه زیرساخت کار کنند، می‌توانند در محل‌های دیگر نیز مورد استفاده مجدد قرار گیرند.

متداول‌ترین انتقاد از فریب دادن در امنیت زیرساخت‌های ملی با مقیاس وسیع این است که ابزارهای خودکار شده نظیر بات‌نت به وسیله قابلیت تله تحت تأثیر قرار نمی‌گیرند. بات‌نت‌ها حمله به زیرساخت ملی را به صورت خودکار و کور، بدون توجه به اینکه هدف واقعی یا ساختگی است، انجام می‌دهند؛ اما احتمال دارد که قابلیت تله بعضی آثار مثبت را داشته باشد. برای مثال؛ ممکن است موجب هماهنگی ملی تعداد

زیادی نقاط انتهایی ساختگی شوند که آماده و موافق با پذیرش نرم‌افزار بات‌نت هستند. اگر این نقاط انتهایی به طور مناسبی طراحی‌شده باشند، می‌توان تصور کرد که آن‌ها به طور عمدی جهت آشفته کردن ارتباطات بات‌نت طراحی‌شده‌اند و شاید این عمل باهدف قرار دادن کنترل‌کننده‌های بات‌نت انجام شود. اغلب، به این رویکرد به عنوان tarpit اشاره می‌شود و این متد برای کاهش مؤثر بودن بات‌نت کاملاً جالب است.

فصل ۳: جداسازی

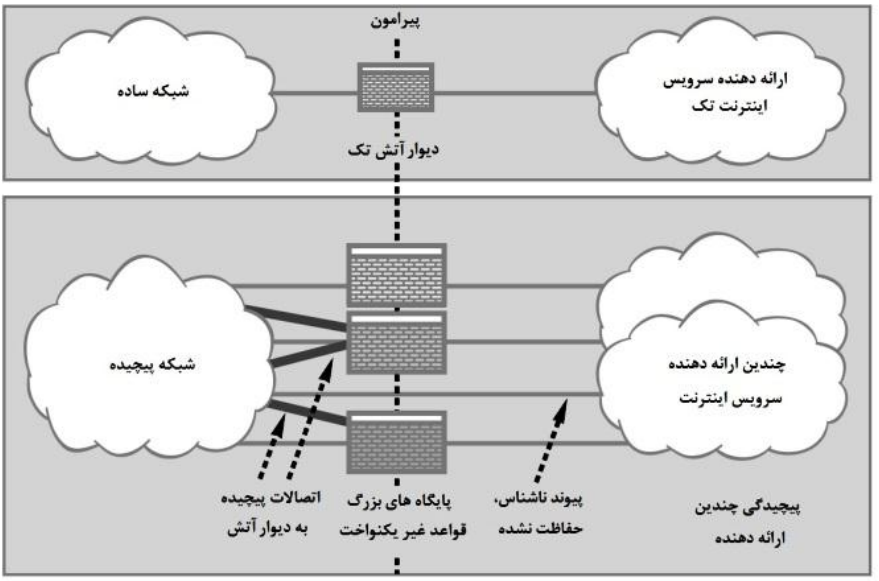
یکی از محدودیت‌های دیوارهای آتش این است که آن‌ها می‌توانند فقط به خوبی کنترل‌های دسترسی و فیلترهایشان باشند و ممکن است در کشف بسته‌های خرابکارانه موفق نشوند. در برخی موارد، ممکن است کلاً دور زده شوند. برای مثال؛ اگر یک کامپیوتر در پشت دیوار آتشی باشد که یک پورت ارتباط تلفنی دارد، که خیلی معمول است، نفوذگر می‌تواند با شماره‌گیری تلفنی به ماشین دسترسی یابد.Dorothy Denning [6]

شاید معمول‌ترین رویکرد حفاظت در حوزه امنیت کامپیوتری، جداسازی سرمایه‌های شبکه از نفوذگران بدخواه با استفاده از دیوار آتش باشد. امروزه، نوعی از دیوار آتش را در اطراف تقریباً هر کامپیوتر، کاربرد، سیستم و شبکه‌ای در دنیا خواهید یافت. دیوار آتش به عنوان محور در قابلیت‌های امنیتی بیشتر سازمان‌ها که شامل عناصر دیگری جهت، فیلتر ضد ویروس و حتی مدیریت شناسه است عمل می‌نماید. صنعت عظیم دیوار آتش برای حمایت از چنین به‌کارگیری قابل‌ملاحظه‌ای به وجود آمده و برای سال‌های متوالی بجز تداوم رشد کاری انجام نداده است.

با وجود این پذیرش گسترده، دیوار آتش به عنوان سازوکار جداسازی برای زیرساخت‌های با مقیاس وسیع با درجه محدودی عمل نموده است. شبکه‌ها و سیستم‌های مرتبط با سرمایه‌های زیرساخت‌های ملی با بسیاری از نقاط مختلف ورودی برای نفوذگران از طریق فراهم‌کنندگان سرویس‌های اینترنتی مختلف تمایل به پیچیده بودن دارند. همچنین، الزامات و نیازهای اتصال برای شبکه‌های پیچیده، باعث ایجاد مجموعه‌های بزرگی از قوانین که اجازه دسترسی به انواع مختلفی از سرویس‌ها و آدرس‌های منابع را می‌دهند شده است. از این بدتر، معمولاً، پیچیدگی شبکه‌های با

مقیاس وسیع، باعث ایجاد نقاط ورودی حفاظت نشده و ناشناس به داخل و خارج سازمان می‌شود (به شکل ۳-۱ توجه کنید).

همان طور که در زیر بیان کرده‌ایم، استفاده از دیوارهای آتش، در حفاظت سرمایه‌های ملی، به نقش خود ادامه خواهند داد. برای مثال؛ فیلتر بسته‌های خروجی، به طور بسیار مؤثری در پیرامون فرضی سازمان عمل خواهد کرد. به طور مشابه، زمانی که دو سازمان یا بیشتر ارتباطی را به اشتراک می‌گذارند، نقاط انتهایی اتصال، طبیعی‌ترین محل برای قرار دادن فیلتر است، به خصوص اگر اتصالات سوئیچ مداری به‌کاررفته باشند.



شکل ۳-۱- دیوار آتش در شبکه‌های ساده و پیچیده

برای رسیدن به جداسازی بهینه در حفاظت از سرمایه‌های زیرساخت ملی، رعایت سه رویکرد جدید برای دیوار آتش الزامی است:

- جداسازی مبتنی بر شبکه: از آنجا که تعریف دقیق پیرامون هر جز پیچیده زیرساخت ملی مشکل است، باید از متدهای جداسازی مثل دیوارهای آتش مبتنی بر شبکه استفاده کرد. چنین قابلیت مبتنی بر اَبر، اجازه ترسیم دقیق‌تر نگرشی از فعالیت‌های خروجی و ورودی سازمان را می‌دهد. همچنین، محیط غنی‌تری را برای فیلتر کردن حملات ظرفیت بالا مهیا می‌نماید. برای مثال، فیلتر کردن حملات امتناع از سرویس که هدف آن زیرساخت است، می‌تواند با انواع مخصوصی از دیوارهای آتش فیلتر کننده مبتنی بر اَبر که به طور راهبردی در شبکه قرار داده‌شده‌اند، متوقف گردند.
- جداسازی داخل: حفاظت در زیرساخت ملی نیاز به برنامه‌ای دارد که سرمایه‌های داخلی را از دیوارهای آتشی که به صورت راهبردی در شبکه قرارگرفته‌اند، جداسازی کند. این نوع جداسازی سرمایه‌های داخلی با استفاده از دیوار آتش یا سازوکارهای دیگر (مثل کنترل دسترسی در سیستم‌های عامل) معمولاً، در بیشتر محیط‌های زیرساختی موجود نیست، به جای آن، این ایده هنوز وجود دارد که افراد داخلی باید دسترسی نامحدودی به منابع داخلی داشته باشند و دیوارهای آتش محیطی، باید منابع سیستم را از دسترسی خارجی غیرقابل‌اعتماد حفظ کنند. این مدل در محیط‌های زیرساخت پیچیده تأثیری ندارد؛ زیرا به آسانی می‌توان عوامل داخلی را جاسازی نمود یا از پیرامون شبکه‌های پیچیده به داخل آن نفوذ کرد.
- جداسازی متناسب شده: استفاده از پروتکل‌های مخصوص در مدیریت زیرساخت ملی، به خصوص در کنترل نظارت و به دست آوردن داده‌ها (SCADA)، متناسب کردن دیوارهای آتش برای انجام پروتکل‌ها و خدمات منحصربه‌فرد، از الزامات است. این یک چالش است؛ زیرا

دیوارهای آتش تجاری برای استفاده عمومی در یک بازار وسیع طرح‌شده‌اند و متناسب کردن آن‌ها به سعی و تلاش متمرکز بیشتری نیاز دارد. نتیجه عملیات دقیق‌تر دیوارهای آتش برای فعال‌سازی کاربردهای SCADAبه تعداد زیادی از پرت‌های سرویس باز احتیاج ندارد.

ممکن است خواننده‌ها با شنیدن طنزی که امروزه در مورد اتصالات شبکه و جداسازی امنیتی وجود دارد، متعجب شوند. بیست سال پیش، مشکل اصلی در شبکه‌های کامپیوتری تعامل بین سیستم‌ها بود. متصل ساختن دو کامپیوتر از طریق شبکه یک چالش قابل ملاحظه بود؛ چالشی که دانشمندان علوم کامپیوتر برای غلبه بر آن سخت کارکردند. در برخی موارد، باید پروژه‌های بزرگی شروع می‌شد که هدف آن‌ها وصل کردن سیستم‌ها از طریق شبکه به یکدیگر بود. چالشی که امروزه با آن مقابله می‌نماییم، مربوط به اتصال سیستم‌ها نیست؛ بلکه مربوط به جداسازی آن‌ها است. این از حضور فراگیر پروتکل اینترنت یا IP ناشی می‌شود که تقریباً هر سیستمی را روی کره زمین قادر می‌سازد تا با تلاش جزیی به دیگر سیستم‌ها وصل شود. در گذشته، نمی‌دانستیم که چگونه سیستم‌ها را به هم وصل کنیم، امروزه، نمی‌دانیم چگونه آن‌ها را جدا نماییم.

۳-۱- جداسازی چیست؟

در زمینه حفاظت از زیرساخت ملی، جداسازی به عنوان تکنیکی در نظر گرفته می‌شود که یکی از اهداف امنیتی زیر را انجام می‌دهد:

- جداسازی دشمن: هدف اول جداسازی، شامل جداسازی یک سرمایه از دسترسی دشمن جهت کاهش مخاطرات حمله مستقیم است. هر نوع پیاده‌سازی، باید باعث شود تا نفوذگر هیچ وسیله مستقیمی برای دسترسی به سرمایه‌های ملی نداشته باشد.

- توزیع اجزا: دومین هدف جداسازی، شامل جدا کردن ساختاری اجزا در یک زیرساخت جهت توزیع ریسک نقض امنیتی است. نباید به نقض امنیتی در یک ناحیه از زیرساخت اجازه انتشار مستقیم داده شود.

محدودیت‌های دسترسی، را می‌توان از طریق ابزارهای عملکردی یا فیزیکی به دست آورد هر کدام از این رویکردها باعث جداسازی می‌شود. چاره‌های عملکردی شامل نرم‌افزار، کامپیوتر و شبکه است؛ در صورتی که، وسایل فیزیکی شامل جداسازی‌های محسوس مثل قفل، گاوصندوق و کابینت‌ها هستند. بیشتر محدودیت‌های دسترسی مرتبط با جداسازی را باید با تمرکز بر عوامل داخلی یا تهدید خارجی طراحی کرد. رابطه بین گزینه‌های مختلف جداسازی را با سه فاکتور اولیه می‌توان امتحان کرد که درگیر استفاده از جداسازی در حفاظت از زیرساخت هستند.

یک طبقه‌بندی کاری از تکنیک‌های جداسازی

سه فاکتور اولیه درگیر در استفاده از جداسازی برای حفاظت از زیرساخت شامل منبع تهدید (عوامل داخلی یا خارجی)، هدف کنترل امنیت (دشمن یا سرمایه) و رویکرد استفاده‌شده در کنترل امنیت (عملکردی یا فیزیکی) هستند. می‌توانیم با استفاده از این سه فاکتور طبقه‌بندی جداسازی که در مقایسه و تضاد بین گزینه‌های مختلف برای جداسازی زیرساخت از دشمن را ایجاد نماییم. (به شکل ۳-۲ توجه کنید).

مثال	رویکرد	هدف	تهدید	
کنترل دسترسی اینترنت	عملکردی	دشمن	کارمند داخلی	تکنیک های عملکردی دشمن
دیواره آتش بسمت اینترنت	عملکردی	دشمن	فرد خارجی	
جدایی کاربرد	عملکردی	سرمایه	کارمند داخلی	تکنیک های عملکردی سرمایه
توزیع کاربرد	عملکردی	سرمایه	فرد خارجی	
محفظه بندی پروژه	فیزیکی	دشمن	کارمند داخلی	تکنیک های فیزیکی دشمن و سرمایه
کلاس بندی اطلاعات	فیزیکی	دشمن	فرد خارجی	
تنوع شبکه داخلی	فیزیکی	سرمایه	کارمند داخلی	
توزیع میزبان فیزیکی	فیزیکی	سرمایه	فرد خارجی	

شکل ۳-۲- طبقه‌بندی تکنیک‌های جداسازی

اولین ستون در طبقه‌بندی نشان می‌دهد که کنترل‌های جداسازی، متمرکز بر دور نگه‌داشتن دو عامل داخلی و خارجی از بعضی سرمایه‌ها هستند. اختلاف کلیدی این است که عوامل داخلی (کارمندان) بیشتر مورد اعتمادند و فرصت‌های بیشتری برای به دست آوردن انواعی از دسترسی را دارند. ستون دوم نشان می‌دهد که کنترل‌های جداسازی متمرکز بر دور نگه‌داشتن دشمن از بعضی سرمایه‌ها یا جداسازی ذاتی بعضی از اجزا سرمایه واقعی، احتمالاً از طریق توزیع کردن آن‌ها هستند. ستون سوم مشخص می‌نماید که آیا رویکرد جداسازی از عملکردهای محاسباتی استفاده می‌کند؛ و یا به جای آن متکی بر نوعی کنترل فیزیکی یا محسوس است.

از دو سطر اول این طبقه‌بندی آشکار است که کنترل‌های دسترسی داخلی یک وسیله عملکردی را نشان می‌دهند که می‌توانند برای جداسازی دشمنان داخلی از سرمایه‌ها به‌کار روند. دیوارهای آتش اینترنت هم تقریباً همان کار را در مورد دشمنان خارجی انجام می‌دهند. این دیوارهای آتش، ممکن است همان دستگاه‌های سنتی باشند که در بنگاه‌های تجاری یافت می‌شوند، یا دستگاه‌های مخصوص فیلتر کردن که در

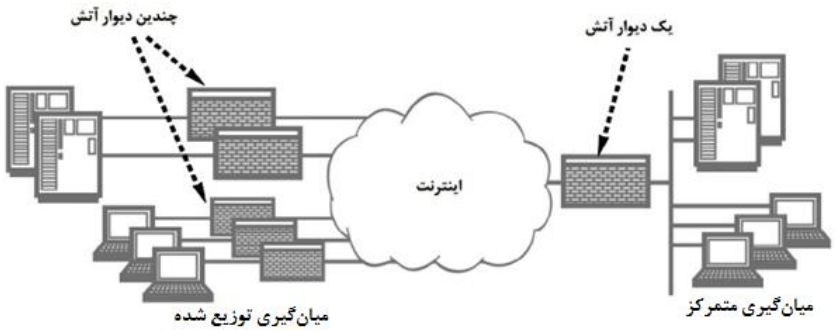
شبکه جهت جلوگیری و خفه کردن حملات حجمی به کار می‌روند. سطرهای سوم و چهارم نشان می‌دهد که جداسازی منطقی یک کاربرد، روش خوبی برای پیچیده کردن یک حمله توسط عوامل و کارمندان داخلی است. این عمل به طور قابل‌مقایسه‌ای برای عوامل خارجی به وسیله توزیع کاربرد در تمام میزبان‌های مختلفی که با اینترنت سروکاردارند انجام شود. آخرین چهار سطر در شکل ۳-۲، راه‌های مختلفی را نشان می‌دهند که با استفاده از آن‌ها می‌توان از ابزارهای فیزیکی برای حفاظت از زیرساخت بهره برد. دامنه این راه‌ها از جدا نگه‌داشتن پروژه‌ها و افراد از سرمایه‌ها تا حفظ تنوع و توزیع سرمایه‌های زیرساخت تغییر می‌کند. بخش زیر شرح مفصل‌تری را از این عناصر طبقه‌بندی جداسازی ارائه می‌کند.

۳-۲- جداسازی عملکردی

معمول‌ترین روش جداسازی عملکردی یک دشمن از هر سرمایه محاسباتی را می‌توان با استفاده از مکانیسم کنترل دسترسی با تأیید هویت و مدیریت شناسه لازم به دست آورد. کنترل‌های دسترسی مشخص می‌کنند که کدام کاربر می‌تواند کدام عمل را روی چه موجودی انجام دهد. قوانین دسترسی در سیاست‌های امنیتی باید از پیش مشخص‌شده باشند. برای مثال؛ این قوانین باید مشخص کنند که کدام کاربران می‌توانند به کاربرد مشخصی دسترسی داشته باشند؛ واضح است که تأیید اعتبار شناسه کاربر باید دقیق باشد. در برخی موارد، قواعد سیاست امنیتی باید پویاتر باشند. مثلاً؛ در این مورد که آیا باید نوع جدیدی از ترافیک جریانی اجازه و حق دخول به نقاط ورودی اینترنت را داشته باشد. این ممکن است با تجزیه و تحلیل زمان واقعی و بی‌درنگ جریان ترافیک شبکه تعیین شود.

سیاست دسترسی، باید در هر سازمان مقرری خاص را برای هر کاربر که تقاضای انجام عملی را روی موجودات سیستم‌هایش انجام می‌دهد تعیین کند. سیاست‌های دیوار آتش متداول‌ترین مثال از این نوع هستند، برای مثال؛ کاربرانی که سعی در ارتباط

با یک سرور وب داشته باشند، ممکن است تحت اعمال سیاست‌های کنترل دسترسی قرارگیرندکه باید مشخص نماید آن‌ها مجاز به این دسترسی هستند. به طور مشابه، آدرس‌های IP بعضی سازمان‌ها ممکن است به داخل قواعد دیوار آتش برده شود تا اجازه دسترسی به سیستم‌های معینی داده شود. مسئله عمده‌ای که در عمل با دیوارهای آتش اتفاق میفتد این است که پایگاه قواعد دیوار آتش می‌تواند به اندازه بسیار بزرگی مثلاً چند هزار قاعده رشد نماید. نتیجه این عمل پیچیدگی و توان بالقوه جهت خطا خواهد بود. در ابتکارات زیرساخت‌های ملی، باید پاداش‌ها و مشوق‌هایی برای سازمان‌هایی که پایگاه‌های قواعد خود را به اندازه کافی کوچک نگه می‌دارند در نظر گرفته شود. برخی از سازمان‌ها، برای این منظور از ابزارهای بهینه‌سازی استفاده کرده‌اند و باید استفاده از این شیوه عمل برای سرمایه‌های ملی توصیه شود.



شکل ۳-۳- میان‌گیری توزیع‌شده در مقابل متمرکز

زمانی که سعی داریم عملکرد دشمن را از هر گونه سرمایه زیرساخت ملی جداسازی کنیم، می‌توانیم دو دسته وسیع امنیتی را تعقیب کنیم. اولین دسته؛ شامل توزیع مسئولیت میان‌گیر دسترسی به صاحبان اجزا سرمایه‌های کوچک‌تر مثل

کامپیوترهای شخصی یا شبکه‌های کوچک است. دومین دسته، شامل به‌کارگیری یک مکانیزم میان‌گیر مرکزی که از طریق آن تصمیمات کنترل دسترسی گرفته می‌شود.
(به شکل ۳-۳ توجه کنید).

امروزه، رویکرد توزیع‌شده درخواست قابل‌ملاحظه‌ای در جوامع اینترنتی جهانی دارد. این روش از مسئله اعتماد داشتن به یک موجود بزرگ با تصمیمات میان‌گیری اجتناب می‌کند. این روش به موجودات تجاری اجازه می‌دهد تا برای ابزارهای امنیتی خود به مقیاس وسیع برای کاربران انتهایی بازاریابی نمایند. در این روش سیاست، کنترل دسترسی نزدیک به سرمایه قرار می‌گیرد و باعث می‌شود که احتمال اینکه سیاست امنیتی مناسبی اتخاذ شود، افزایش یابد. توزیع جهانی شدید واگذاری مسئولیت امنیتی کامپیوتر به صاحبان کامپیوترهای شخصی منازل، مثالی از این رویکرد است. کاربران باید در مورد چگونگی حفاظت از سرمایه‌هایشان، به جای این که متکی بر یک قدرت مرکزی باشند، خود تصمیم بگیرند.

متأسفانه، رویکرد توزیع‌شده منجر به نتایج ضعیفی شده است. بیشتر کاربران انتهایی برای گرفتن تصمیمات امنیتی مناسب، صلاحیت ندارند. حتی اگر درصد بالایی از آن‌ها تصمیماتی عالی بگیرند و کسانی باشند که آسیب‌پذیری‌های جدی ایجاد نمی‌کنند و کل طرح را مواجهه با ریسک نمی‌نمایند. برای مثال؛ بات‌نت‌ها، کامپیوترهای کاربران انتهایی را که ضعیف مدیریت می‌شوند، با ارتباطات باند پهن شکار می‌کنند. زمانی که یک کامپیوتر شخصی خانگی با بد افزار آلوده شد، هیچ قدرت مرکزی برای پاک‌سازی وجود ندارد. این بی‌قدرتی مرکزی در اینترنت، باعث ایجاد مخاطرات امنیتی عظیم می‌شود. روشن است که هرگز، نمی‌توان اینترنت را دوباره طراحی کرد تا شامل کنترل مرکزی گردد.

به هر حال، برای زیرساخت‌های ملی این امکان برای کنترل‌های بیشتر مرکزی وجود دارد. در این مورد، اعتقاد بر این است که اتکا بیشتر به حفاظت مرکزی مخصوصاً در مورد ارائه‌دهندگان شبکه، باعث بهبود روش‌های حفاظت سرمایه‌های ملی می‌گردد.

این به آن معنا نیست که حفاظت توزیع‌شده مورد نیاز نیست. در حقیقت، در بیشتر محیط‌ها نصب کردن هر دوی امکانات امنیتی توزیع‌شده و مرکزی به طریقی ماهرانه، برای جلوگیری از حمله به زیرساخت‌های ملی مورد نیاز است.

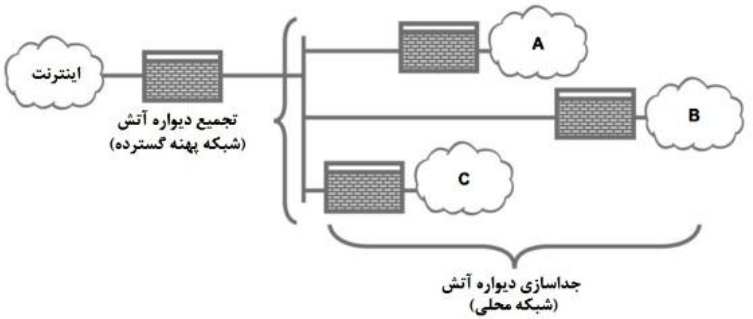
۳-۳- دیوارهای آتش زیرساخت ملی

متداول‌ترین کاربرد یک دیوار آتش، قرار گرفتن آن بین یک سیستم، یا یک بنگاه تجاری، یا یک شبکه غیرقابل‌اعتماد مثل اینترنت است که باید از آن حفاظت شود. برای حفاظت از سرمایه ملی این دو امکان باید فوراً ایجاد:

- پوشش: دیوار آتش ممکن است تمام مسیرهای بین سرمایه ملی را که باید از آن حفاظت شود و شبکه غیرقابل‌اعتمادی مثل اینترنت را پوشش ندهد، با توجه به پیچیدگی بیشتر زیرساخت‌های ملی این یک مورد محتمل است.
- دقت: دیوار آتش ممکن است مجبور شود که اجازه دسترسی به سرمایه‌های ملی را به نحوی که باعث ارائه دسترسی غیر عمدی و غیرمجاز به بعضی سرمایه‌های حفاظت شده می‌شود بدهد. این حالت، در محیط‌های با مقیاس وسیع معمول است؛ به خاطر اینکه پروتکل‌های مخصوص مانند آنچه در سیستم‌های SCADA وجود دارد، به ندرت به کمک دیوارهای آتش تجاری حمایت می‌شوند. در نتیجه، اپراتور دیوار آتش با رها کردن برخی پرت‌ها به صورت کاملاً باز برای ترافیک ورودی، این نقیصه را جبران می‌کند.

برای مقابله با این چالش‌ها، طراحی زیرساخت امنیت ملی احتیاج دارد که با جاگذاری ماهرانه قابلیت‌های جداسازی اطمینان ایجاد کند که تمام ترافیک مربوطه از میان‌گیر (دیوار آتش) می‌گذرد و در زمانی که اجازه دسترسی به سرمایه خاصی داده

شد، هیچ اثر جانبی خاصی اتفاق نخواهد افتاد؛ دو روش مؤثر تجمیع حفاظت‌ها در شبکه‌های گسترده (WAN) و تفکیک و جداسازی محافظت‌ها در شبکه‌های محلی (LAN) است. (به شکل ۳-۴ توجه کنید).



شکل ۳-۴- دیوار آتش تجمیع کننده WAN و دیوار آتش تفکیک‌کننده LAN

تجمیع قابلیت‌های دیوار آتش در یک دروازه ورودی و خروجی تعریف‌شده برای مدیران امنیتی بنگاه‌ها ناشناخته نیست و به اطمینان از پوشش ارتباطات غیرقابل‌اعتماد در محیط‌های پیچیده‌تر کمک می‌کند. همچنین، وسیله‌ای برای تمرکز روی بهترین منابع، ابزارها و کارمندان را در یک مجموعه امنیتی مجتمع شده ارائه می‌کند. تفکیک و جداسازی در یک شبکه محلی هم شناخته شده است؛ اگر چه شاید کمتر به آن عمل می‌شود؛ مثلاً؛ در کاهش احتمال اینکه دسترسی خارجی به سیستم A دارای اثر جانبی ارائه دسترسی خارجی به سیستم B باشد، مؤثر است. در ضمن، احتیاج به مدیریت دستگاه‌های بیشتری دارد و معمولاً، مخارج بیشتری را در پی خواهد داشت. به هر حال، در هر دو این روش‌ها، قرار دادن دیوار آتش متمرکز و توزیع‌شده در زیرساخت ملی مهم هستند.

یک چالش عمده در زیرساخت ملی که باید برای تمام سرمایه‌های ملی در سال‌های آینده حتمی فرض شود افزایش شدید در ارتباطات بی‌سیم است. امروزه،

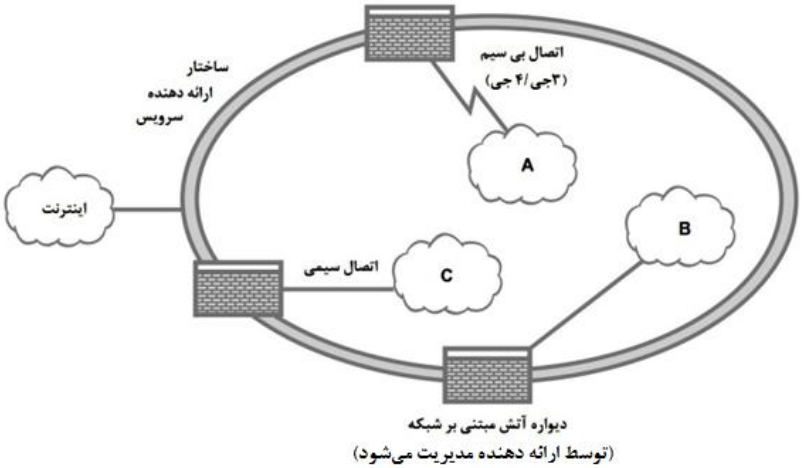
بیشتر کارگران و کارمندان بنگاه‌های تجاری نوعی از دستگاه‌های هوشمند را که در همه جا به اینترنت وصل می‌شوند، با خود حمل می‌کنند. چنین دستگاه‌های هوشمندی مانند کامپیوترهایی هستند که دارای مرورگر، دسترسی به پست الکترونیکی و شبکه‌های خصوصی مجازی (VPN) هستند و می‌توانند از کاربردهایی حمایت کنند که ممکن است در پشت دیوار آتش باشند. به این ترتیب، احتمال اینکه اجزا زیرساخت بتوانند به راحتی دروازه‌های دیوار آتش را دور بزنند، به میزان زیادی افزایش یافته است. شاید نتیجه چنین ارتباطات بی سیمی با به‌کارگیری نسل چهارم موبایل (4G) این باشد که تمام اجزا زیرساخت برای اطمینان از امنیت به نوعی از ابزار مشترک احتیاج دارند.

ممکن است توزیع وسیع امنیت در دستگاه‌های نقاط انتهایی بی‌سیم هوشمند، برای تمام علت‌هایی که قبلاً به آن‌ها اشاره شد، بهترین گزینه نباشد. توزیع عظیم مسئولیت‌های امنیتی به تمام صاحبان دستگاه‌های هوشمند مورد نیاز است. از طرف تمام صاحبان دستگاه‌های هوشمند، مراقبت و احتیاط نیز لازم است که این انتظار معقولی نیست. رویکرد دیگر، شناسایی یک زیرساخت انتقال مشترک برای اجرای سیاست‌های مطلوب است که؛ ممکن است از طریق حامل‌های شبکه به بهترین نحو انجام شود. ارائه‌دهندگان سرویس‌های شبکه ارجحیت‌های چندی را در رابطه با امنیت متمرکز ارائه می‌کنند:

- دیدگاه: ارائه‌کننده سرویس شبکه دیدگاه وسیعی دارد که شامل تمام مشتریان، نقاط مشابه و دروازه‌ها را شامل می‌شود بنابراین، اگر واقعه‌ای در اینترنت اتفاق بیفتد ارائه‌کننده سرویس آثار آن را مشاهده خواهد کرد.
- عملیات: ارائه‌دهندگان سرویس می‌توانند از بروز شدن پوشش امضاها، وصله‌های نرم‌افزاری و روش‌های جدید امنیتی مطمئن شوند؛ بر خلاف تقریباً بیشتر کاربران انتهایی که قادر به بروز نگه‌داشتن نرم‌افزارهای امنیتی خود نیستند.

- سرمایه‌گذاری: بر خلاف بیشتر کاربران انتهایی که احتمالاً امکانات مالی کافی برای نصب چندین نوع مختلف از ابزارهای مختلف یا حتی افزونه امنیتی را ندارند؛ ارائه‌کنندگان سرویس معمولاً، می‌توانند از یک مورد کسب‌وکار برای چنین سرمایه‌گذاری حمایت کنند.

به این دلایل تصویر و منظر آینده قابلیت دیوار آتش برای زیرساخت ملی احتمالاً شامل یک نقطه تجمع جدید یعنی مفهومی از اجرای دیوار آتش مبتنی بر شبکه در ابر Cloud خواهد بود. (به شکل ۳-۵ توجه کنید).



شکل ۳-۵- دیوار آتش مبتنی بر شبکه حامل محور.

در حفاظت از زیرساخت ملی، استفاده از دیوارهای آتش مبتنی بر شبکه که در دستگاه‌های ارائه‌کنندگان سرویس جاسازی‌شده‌اند، احتیاج به مشارکت جدیدی بین حامل‌ها و گروه‌های کاربران انتهایی دارد. متأسفانه، بیشتر موافقت‌های سرویس (SLA) مخابراتی فعلی با این مفهوم سازگار نیستند و به جای اینکه بر اجرای سیاست‌ها تأکید کنند، بر مسائل و موضوعاتی نظیر گم شدن و تأخیر بسته‌ها تأکید می‌کنند. امروزه این

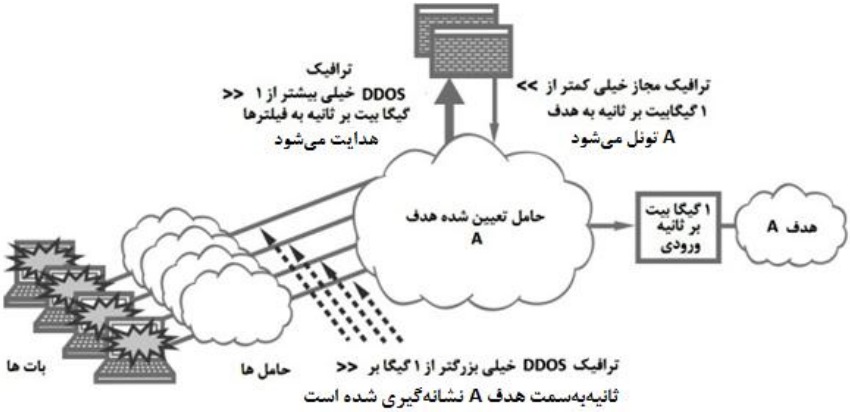
امر باعث موارد متعددی از حملات به ارائه‌کنندگان سرویس‌های زیرساخت ملی شده است و ارائه‌دهندگان سرویس در هنگام حادثه حمله هیچ حمایتی نکرده؛ یا مقدار ناچیزی حمایت ارائه داده‌اند. آشکار است که برای حفاظت از سرمایه‌های ملی این وضعیت باید تغییر کند.

۳-۴- فیلتر کردن DDOS

یک کاربرد عمده مفهوم دیوار آتش مبتنی بر شبکه شامل یک نوع خاص از دستگاه‌های میان‌گیر جاسازی‌شده در شبکه‌های WAN برای خفه کردن حملات جلوگیری از سرویس توزیع‌شده یا DDOS است. برای شبکه‌های مدرن، به‌کارگیری این دستگاه که به طور ناپخته‌ای به آن فیلتر DDOS گفته می‌شود، با توجه به خطر بزرگ حملات DDOS که از بات‌نت‌ها ناشی می‌شود، ضروری است. با توجه به فیزیک ظرفیت ورودی شبکه، سعی در فیلتر کردن حملات DDOS در لبه ورودی بنگاه‌های تجاری عاقلانه نیست. برای مثال؛ اگر یک بنگاه تجاری یک لینک ارتباطی با ظرفیت 1Gbps به شبکه اینترنت داشته باشد، هر حمله بات‌نتی با حجم ورودی به این لینک که بیشتر از 1Gbpsباشد، باعث در هم شکستن این ارتباط خواهد شد.

راه حل این مسئله حجمی، جابه‌جا کردن محل فیلتر به نقاط بالاتر سلسله‌مراتب شبکه است. زیرساخت حامل معمولاً، بهترین گزینه در دسترس را ارائه می‌کند. افزایش حجمی ترافیک ورودی باعث می‌گردد که این ترافیک به صورت بی‌درنگ به سمت فیلتر DDOSتغییر جهت دهد تا در آنجا ترافیکی که از بات‌نت‌ها منشأ گرفته‌اند، از ترافیک معتبر جدا شوند. معمولاً، الگوریتم‌های اجرای چنین فیلتری بر اساس نوع ترافیک فرستاده‌شده، اندازه نسبی ترافیک و هرگونه نشانه دیگری که اشاره به ترافیک با طبیعت حمله دارد، عمل می‌کنند. زمانی که ترافیک فیلتر شد، ترافیک باقیمانده به مبادی ورودی فرستاده می‌شود. نتیجه مانند یک دریچه اطمینان بزرگ یا یک جذب‌کننده

ضربه در شبکه‌های با پهنه وسیع و تنها زمانی عمل می‌نماید که حمله‌ای جهت یک بنگاه تجاری در کار باشد (به شکل ۳-۶ توجه کنید).



شکل ۳-۶- فیلتر کردن حملات DDOS ورودی روی سرمایه‌های مورد هدف

تجزیه و تحلیل کمی مرتبط با حفاظت از زیرساخت ملی در مقابل حملات DDOS آزار دهنده است. برای مثال؛ اگر فرض کنیم بات‌ها می‌توانند به راحتی از هر کامپیوتر آلوده‌شده بدون اینکه صاحبش بداند 500kbps از پهنای باند وسیع خروجی‌اش را به سرقت ببرند، تنها به سه بات برای در هم شکستن یک ارتباط با خط (1.5Mbps)T1 نیاز خواهد بود. اگر این استدلال را به کاربریم، یک شبکه بات‌نت با ۱۶۰۰۰ بات برای در هم شکستن یک ارتباط 10Gbps کافی خواهد بود. با وجود بات‌نت‌های مشهوری مانند Storm (طوفان) و Conflicker که بعضی خبرگان معتقدند بین ۲ تا ۳ میلیون بات در اختیاردارند، ضرورت مرتبط با استقرار فیلترهای DDOS را نمی‌توان نادیده گرفت. یک پیامد این مسئله این است که ابتکارات حفاظت از زیرساخت‌های ملی باید فیلتر DDOS را به نحوی در نظر بگیرند تا ریسک حملات DDOS به سرمایه‌های ملی را کاهش دهند.

مسئله جدی ای که باید به آن پرداخته شود، این است که حملات فعلیDDOS به زیرساخت‌ها شامل رویکرد معروف به "تقویت کردن" نیز است. حملات DDOS جدید با شناخت و در نظر گرفتن این حقیقت طراحی‌شده‌اند که فیلترهای DDOS برای کشف جریان بزرگی از ترافیک غیرعادی ورودی در شبکه وجود دارند بنابراین، دشمن برای اجتناب از فیلتر شدن روی ترافیک ورودی در زیرساخت حامل، از دو ابتکار طراحی استفاده می‌نماید. اول؛ آن‌ها ترافیک حملات DDOS را طوری طراحی می‌کنند که رفتار نرمال و طبیعی سیستم را تقلید نماید و معمولاً، تعاملاتی را با سیستم هدف ایجاد می‌نمایند که به نظر کاملاً معتبر است. دوم؛ حمله خود را طوری طراحی می‌کنند که شامل مقدار کوچکی از ترافیک ورودی باشد که از بعضی از خصوصیات منحصربه‌فرد نرم‌افزار در سیستم هدف استفاده می‌کند تا حجم عظیمی از ترافیک خروجی در سیستم هدف ایجاد شود. نتیجه رشته ورودی کوچک‌تر و کمتر معلومی است که بعداً باعث تولید ترافیک خروجی بزرگ‌تری می‌گردد که می‌تواند باعث شرایط DDOS شود.

چالش بزرگ فیلتر کردن حملات DDOS

چالش بزرگ در مورد حملات فعلی DDOS این است که تنها راه برای اجتناب از مسئله‌ای که قبلاً ذکر شد از طریق تغییرات غیر جزیی در زیرساخت سیستم مورد هدف می‌باشد. لازم است دو تغییر غیر جزیی مهم در اینجا گفته شوند:

۱- تأیید هویت قوی‌تر پرس و جو و تعاملات ورودی از کاربران ضروری است. برای سایت‌های تجارت الکترونیکی که برای جلب کاربران از اینترنت طراحی‌شده‌اند و رویه‌های آن‌ها برای عدم ترساندن و فرار مشتریان کمینه شده‌اند، این موضوع مطلوب نیست.

۲- برای کمینه کردن آثار تقویت‌کنندگی، برخی سیستم‌های هدف باید مراقبت‌های زیادی برای تجزیه و تحلیل رفتار کاربرهایی که از طریق اینترنت

مشاهده می‌شوند انجام دهند تا مشخص گردد که آیا پرس و جوهای کوچک می‌توانند پاسخ‌های بسیار بزرگ‌تری را تولید کنند. این امر، به ویژه برای خدمات عمومی به اشتراک گذاشته‌شده نظیر سیستم نام دامنه (DNS)که کاملاً نسبت به حملات تقویت‌کنندگی آسیب‌پذیر هستند، مهم است.

این ملاحظات فنی باید در ابتکارات حفاظت از زیرساخت‌های ملی مدرن گنجانده شود.

۳-۵- معماری جداسازی SCADA

بسیاری از سیستم‌های زیرساخت‌های حیاتی ملی قابلیت کنترل نظارت و به دست آوردن داده (SCADA) را دارند. این سیستم‌ها را می‌توان به عنوان مجموعه‌ای از نرم‌افزارها، کامپیوترها و شبکه‌ها در نظر گرفت، که هماهنگی از راه دور سیستم‌های کنترل برای زیرساخت‌های ملموس نظیر سیستم‌های تولید برق، کارخانه‌های شیمیایی، تجهیزات تولید، سیستم‌های حمل‌ونقل را انجام می‌دهند.

ساختار کلی سیستم‌هایSCADA شامل اجزا زیر می‌باشند:

- واسط انسان و ماشین (HMI): واسط بین اپراتور انسان و دستورات و فرمان‌های مربوط به سیستم SCADA
- واحد ترمینال اصلی (MTU): در یک معماری Client Server این ترمینال به عنوان Client عمل کرده و داده‌های محلی را جمع‌آوری و جهت ترمینال سرور در دوردست می‌فرستد.
- واحد ترمینال دوردست (RTU): در ساختار Client-Server، این ترمینال به صورت Server عمل کرده؛ داده‌های رسیده از ترمینال‌های دوردست را جمع‌آوری می‌کند و پس از پردازش، سیگنال‌های کنترلی را ایجاد می‌نماید و به سیستم‌های کنترلی میدانی می‌فرستند.

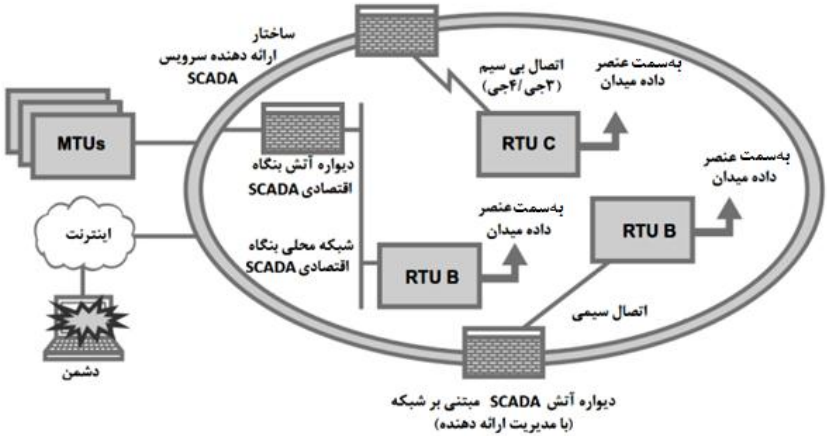
- سیستم‌های کنترلی میدانی: سیستم‌هایی هستند که دارای واسط مستقیم به عناصر تولید یا دریافت‌کننده داده‌های میدانی؛ نظیر؛ حسگرها، پمپ‌ها و سوئیچ‌ها هستند.

مسئله اولیه جدایی امنیتی در ساختار سیستم‌های SCADA، عبارت است از دسترسی از راه دور یک MTU به یک RTU داده‌شده که باید بر اساس یک سیاست کنترل دسترسی به نحو مناسبی میان‌گیری شود؛ بنابراین، استفاده از دیوارهای آتش بین MTUها و RTUها در معماری سیستم‌های SCADA ضروری است. این جداسازی باید در هر ارتباط با شبکه‌های غیرقابل‌اعتماد نظیر ارتباط اینترنت به RTU سیاست‌های امنیتی را اعمال نماید. اگر این نوع حفاظت موجود نباشد، خطر آشکاری پدید خواهد آمد که دشمن بتواند با دسترسی از راه دور باعث تغییر یا تأثیر بر عملیات یک سیستم کنترل میدانی شود.

همان طور که می‌توان انتظار داشت تمام اشکالات در ارتباط با به‌کارگیری و استقرار مقیاس وسیع دیوار آتش در سیستم‌های SCADA نیز وجود دارد. مسائل مربوط به پوشش و دقت باید در نظر گرفته شود. همچنین، باید احتمال این را در نظر گرفت که هر کدام از اجزا باید با کانال‌های ناشناخته و غیر مصوب ارتباط مستقیم یا بی‌سیم به اینترنت داشته باشند. این به آن معنی است که حفاظت از RTU از دسترسی غیرمجاز نیاز به ترکیبی از دیوارهای آتش محلی تفکیک‌کننده و دیوارهای آتش جمع کننده در سطح بنگاه تجاری و دیوارهای آتش مبتنی بر شبکه‌های حامل دارد (به شکل ۳-۷ توجه کنید).

بزرگ‌ترین مسئله برای امنیت جداسازی SCADA، این است که بیشتر سیستم‌های الکترومکانیکی مربوطه، در محیطی جدا از محیط‌های محاسباتی و شبکه‌ای متداول طراحی‌شده و تکامل‌یافته‌اند. تنها متون کمی به طور مشروح و زیرکانه معماری سیستم‌های SCADA را تشریح می‌نمایند. در حقیقت، دانشمندان کامپیوتری به راحتی می‌توانند بدون اینکه در مرض کوچک‌ترین مسائل محیطی SCADA قرار

گیرند، برنامه‌های پیشرفته خود را کامل کنند. در بسیاری از محیط‌های SCADA، ارتباطات کامپیوتری بین سیستم‌های مهم و شبکه‌های کنترل آن‌ها به صورت تک کاره انجام‌شده و این بیشتر به خاطر ایجاد راحتی کار مثل دسترسی از راه دور بود. به این دلیل احتمال اینکه آخرین سازوکارهای امنیتی جهت حفاظت از سیستم‌های SCADA در مقابل حملات سایبری در سیستم قرار گیرد، کم بود.



شکل ۳-۷- معماری توصیه‌شده دیوارهای آتش سیستم SCADA

مشکل دیگری که در استفاده از دیوار آتش در سیستم‌های SCADA ظاهر می‌شود، این است که معمولاً، دیوارهای آتش تجاری پروتکل‌های SCADA را حمایت نمی‌کنند. زمانی که چنین اتفاقی میفتد، اپراتور دیوار آتش باید بررسی کند که چه پرتی برای استفاده پروتکل، مورد نیاز است؛ این پرت‌ها باید باز شوند. زمان طولانی است که کارشناسان امنیتی می‌دانند که آسیب‌پذیری‌های بزرگ در یک شبکه، به خاطر باز گذاشتن سهوی پرت‌هایی است که از طریق آن‌ها حمله انجام می‌شود. بدیهی است ابتکارات حفاظت از زیرساخت‌های ملی باید انواع جدیدی از قابلیت‌های دیوار آتش را

تشویق و فعال کند؛ مانند؛ پروکسی‌های مخصوص که بتوانند در معماری SCADA جاسازی شوند و قابلیت‌های فعلی را بهبود بخشند.

۳-۶- جداسازی فیزیکی

یکی از روش‌های جداسازی که به ظاهر آشکار است؛ اما کمتر در امنیت کامپیوتری ارائه‌شده، جداسازی فیزیکی یک شبکه از دیگر شبکه‌ها است. می‌توان انتظار داشت که چیزی ساده‌تر از جداسازی یک شبکه از هر محیط غیرقابل‌اعتماد دیگر نباشد و این فقط با قطع تمام ارتباطات ورودی و خروجی انجام می‌شود. این فرآیند به نام فاصله هوایی شناخته‌شده و بزرگ‌ترین مزیت آن این است که به دستگاه خاص، نرم‌افزار و یا سیستمی احتیاج ندارد و فقط برای جدا کردن شبکه بنگاه تجاری از اینترنت و اجزا یک شبکه از یکدیگر به کار می‌رود.

مشکل جداسازی فیزیکی به عنوان یک تکنیک امنیتی این است که با افزایش پیچیدگی در برخی سیستم‌ها یا شبکه‌هایی که باید ایزوله شوند، احتمال اینکه یک ارتباط خارجی غیرمجاز ناشناخته ایجاد شود، افزایش می‌یابد. به عنوان مثال؛ معمولاً، یک شرکت کوچک با یک شبکه محلی (LAN) نسبتاً کوچک می‌تواند از اینکه ارتباطات خارجی‌اش به اینترنت کاملاً شناخته‌شده هستند و به طور مناسبی حفاظت می‌شوند، مطمئن باشد. درحالی‌که، شرکت رشد می‌کند و دفاتر شعبه‌هایش را با دستگاه‌ها، افراد و لوازم مختلفی مجهز می‌کند؛ احتمال اینکه ارتباطات خارجی ناشناخته‌ای ایجاد شود، بالا خواهد رفت و جداسازی فیزیکی شبکه مشکل‌تر خواهد شد.

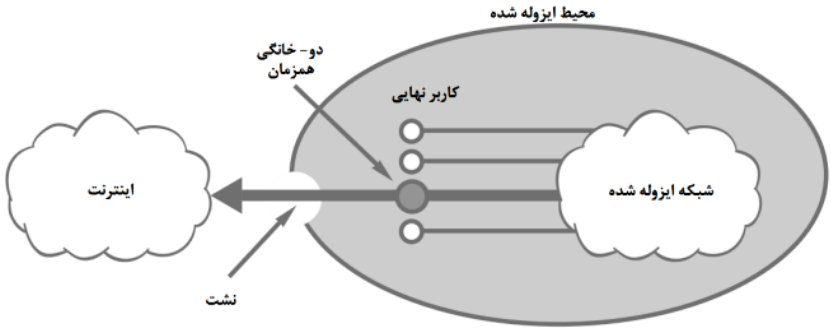
بنابراین، چگونه می‌توان شبکه‌ای ایجاد نمود که بافاصله هوایی جدا شده است؟ پاسخ در اصول اساسی زیر نهفته است:

- سیاست روشن: اگر شبکه‌ای به صورت فیزیکی ایزوله باشد، باید سیاست روشنی داشته باشد، در مورد اینکه کدام ارتباطات شبکه‌ای قابل‌قبول و

کدام غیرقابل‌قبول است بنابراین، سازمان‌ها نیاز به بررسی سیاست استقراریافته‌ای خواهند داشت که به عنوان قسمتی از فرآیند ایجاد ارتباط شبکه عمل کند.

- پویش و اسکن مرز شبکه: شبکه‌های ایزوله شده باید مرزهای قابل‌شناسایی داشته باشند. گرچه داشتن مرزهای تعریف‌شده می‌تواند با تعبیه دیوار آتش در شبکه‌های ایزوله شده پیچیده شود، یک برنامه پویش مرزها به شناسایی نشت کمک خواهد کرد.
- پیامدهای نقض سیاست: اگر نقض سیاست اتفاق بیفتد عواقب آن باید به روشنی استقرار یافته باشد. شبکه‌های حکومتی در ارتش و جوامع اطلاعاتی ایالات‌متحده امریکا مثل SIPRNet و Intelink؛ با قوانینی حفاظت می‌شوند که چگونگی استفاده افراد از این شبکه‌های طبقه‌بندی شده را مشخص می‌کنند. پیامدهای نقض این سیاست‌ها خوشایند نیست.
- گزینه‌های معقول: معمولاً، به علت اینکه کسی احتیاج به برقراری نوعی ارتباط با محیط خارجی دارد، نشت‌هایی معمولاً در شبکه ایزوله شده اتفاق می‌افتد. اگر یک اتصال شبکه‌ای وسیله مناسبی برای رسیدن به این منظور نباشد، سازمان باید گزینه معقول دیگری را ارائه نماید.

شاید بزرگ‌ترین تهدید به ایزولاسیون فیزیکی شبکه شامل دو خانه‌ای بودن یک سیستم به هر دو شبکه بنگاه تجاری و یک شبکه خارجی مثل اینترنت باشد. چنین دوخانگی زمانی که کاربر انتهایی با بهره‌گیری از یک سیستم، دسترسی به هر دو شبکه ایزوله شده و اینترنت را انجام می‌دهد، به آسانی می‌تواند به وجود آید. از آنجایی که کامپیوترهای Laptop شروع به داشتن امکانات دسترسی بی‌سیم 3G در داخل خود کرده‌اند، احتمال دو خانه‌ای شدن افزایش یافته است. بدون در نظر گرفتن روش، اگر هر نوع اتصالی به طور همزمان به هر دو سیستم فعال شود، در این صورت کاربر انتهایی یک پل غیر عمدی ایجاد کرده است. (به شکل ۳-۸ توجه کنید).



شکل ۳-۸- پل زدن یک شبکه ایزوله شده توسط کاربر دو خانه

گفتنی است که پل اشاره‌شده در بالا لزوماً نباید به طور همزمان برقرار شود. اگر یک سیستم به یک شبکه وصل شود و به نوعی بد افزار آلوده شود، می‌تواند پس از آن به شبکه‌های دیگر وصل گردد و بد افزار را پخش نماید. به این دلیل، دستگاه‌های Laptop و گوشی‌های موبایل نیاز به داشتن نوعی حفاظت در خوددارند تا این مسئله کمینه گردد. متأسفانه فناوری روز برای جلوگیری از بار شدن بد افزار در سیستم‌ها ضعیف است.

روشی آشنا برای جلوگیری از ایجاد پل بین شبکه‌ها؛ اعمال سیاست سخت‌گیرانه‌ای روی دستگاه‌های کاربر انتهایی است که می‌تواند برای دسترسی به سیستم‌های ایزوله بکار روند که ممکن است شامل جلوگیری از وصل شدن به اینترنت برخی لپ‌تاپ‌ها، کامپیوترهای شخصی و گوشی‌های موبایل باشد. این دستگاه‌ها باید فقط برای استفاده در شبکه ایزوله شده بکار روند. این روش، قطعاً خطر را کاهش می‌دهد؛ اما جایگزینی پر هزینه است. برای سیستم‌های حیاتی، به خصوص آن‌هایی که کاربردهای ایمنی و مرگ و زندگی دارند، اگر چنین تفکیکی عملی باشد احتمالاً، هزینه‌های اضافی نیز دارد. به هر صورت، تحقیقات اضافی در سیستم‌های چند حالته ضروری است؛ و برای حفاظت از

زیرساخت‌های ملی توصیه می‌شود زیرا که اطمینان از اجتناب از دو خانه شدن را بین شبکه‌ها ایجاد می‌کند.

۳-۷- جداسازی کارمندان و عوامل داخلی

مقابله با تهدید عوامل داخلی در حفاظت از زیرساخت ملی مشکل است؛ زیرا به دست آوردن موقعیت‌های مورد اعتماد برای دشمنان مصمم، در گروه‌های مسئول حفاظت از سرمایه‌های ملی نسبتاً آسان است. چون شرکت‌ها به شراکت، خرید و برون سپاری در بین مرزهای سیاسی خود ادامه می‌دهند، مقابله با این تهدید مشکل‌تر هم شده است؛ بنابراین، سهولتی که با آن دشمن در یک کشور می‌تواند به سیستم‌های زیرساختی مورد اعتماد و داخلی یک کشور دیگر دسترسی یابد، هم در حال رشد و هم نگران کننده است.

به طور سنتی، دولت‌ها با این چالش از طریق بررسی سخت‌گیرانه الزامات و سوابق هر شخصی که دسترسی به سیستم‌های حساس حکومتی را لازم داشته باشد، برخورد نموده‌اند. این شیوه عمل در بسیاری از محیط‌های تدارکاتی حکومتی تداوم دارد، به ویژه آن‌هایی که شامل اطلاعات نظامی و یا اطلاعاتی هستند.

مشکل این است که زیرساخت ملی شامل سیستم‌های بسیار دیگری به غیر از سیستم‌های حساس حکومتی است. این زیرساخت‌ها شامل سیستم‌های SCADA، شبکه‌های مخابراتی، زیرساخت حمل‌ونقل، شبکه‌های مالی و مانند آن‌ها می‌باشد. اگر نگوییم، هرگز، به ندرت در این محیط‌های تجاری نوعی کنترل برای مقابله با جمع‌آوری داده‌های غیرمجاز، دسترسی نامناسب به سوابق مشتریان یا دسترسی اداری به کاربردهای حیاتی توسط کارمندان داخلی الزاماتی جاسازی شده است. در عوض، معمولاً، به کارمندان اجازه دسترسی به اینترنت داخلی شرکت اعطاء شده است و هر چیزی را می‌توانند به دست آورند.

روش‌هایی برای کاهش خطر دسترسی غیرمجاز کارمندان داخلی وجود دارد که می‌تواند در طراحی و بهره‌برداری عملیات زیرساخت ملی جاسازی شوند. این روش‌ها شامل موارد زیر است:

- دیوار آتش داخلی: دیوارهای آتش که اجزا سرمایه‌های ملی را از هم جدا می‌کنند، می‌توانند خطر دسترسی کارمندان داخلی را کاهش دهند. برای مثال؛ یک کارمند با حق دسترسی به جز A، برای دسترسی به جز B، باید تعامل موفقیت‌آمیزی با یک دیوار آتش داشته باشد. تقریباً، هر روشی برای جداسازی کارمندان داخلی از سرمایه‌ها، نوعی از دیوار آتش را دارد. این روش‌ها، می‌توانند به صورت یک دیوار آتش کاملاً پیکربندی شده باشند و یا یک روتر فیلتر کننده بسته‌ها؛ با وجود این روش جداسازی کارمندان داخلی از سرمایه‌ها با استفاده از دیوار آتش باید یک کنترل فراگیر در زیرساخت ملی شود.
- ظروف عسل فریب‌دهنده: همان طور که در بخش دوم بحث شد، ظروف عسل داخلی می‌توانند به شناسایی کارمندان داخلی بدخواه کمک کنند. اگر فریب دادن به صورت علنی تبلیغ شده باشد، کارمندان داخلی بدخواه در فعالیت‌های خرابکارانه خود تردید می‌کنند. اگر فریب دادن پنهانی باشد، ممکن است اپراتورها نقض امنیتی بدخواهانه را مشاهده کرده و منبع داخلی آن را شناسایی کنند.
- اجرای اجباری نشانه‌گذاری داده‌ها: بسیاری از سازمان‌ها با مسئولیت‌هایی در زیرساخت ملی، به طور مناسبی اطلاعات خود را نشانه‌گذاری نمی‌کنند. هر شرکت یا آژانس دولتی باید شناسایی، تعریف و اجرا کردن یک نشانه‌گذاری داده‌ای که به راحتی قابل مشاهده باشد را بر روی تمام اطلاعات خود که می‌توانند مورد سواستفاده قرار گیرند، قرار دهد. بدون چنین نشانه‌گذاری، احتمال اینکه اطلاعات اختصاصی به طور غیر عمد در

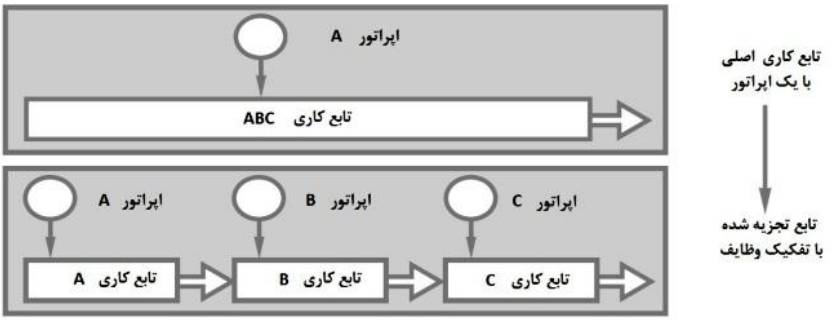
دسترس دشمن گذاشته شود، افزایش می‌یابد. اخیراً، برخی از شرکت‌ها شروع به استفاده از نشانه‌گذاری داده‌های مرتبط با اطلاعات شناسایی افراد نموده‌اند. (PII).

- سیستم‌های حفاظت (جلوگیری از) نشت داده‌ها (DLP): روش‌هایی برای بوکشی ترافیک دروازه‌ها، برای شناسایی داده‌های حساس یا نامناسب متداول شده است. ابزارهایی که به نام سیستم‌های DLP نامیده می‌شوند، به طور متداول در شرکت‌ها و آژانس‌ها بکار گرفته می‌شوند و در بهترین حالت، حفاظت ضعیفی در مقابل تهدید ناشی از کارمند داخلی ارائه می‌دهند، اما آن‌ها به شناسایی نشت نادرست نیز کمک می‌کنند. زمانی که این سیستم‌ها بکار گرفته شوند، می‌توانند آماری را ارائه دهند، از اینکه کارمندان داخلی کجا و چگونه با استفاده از سیستم‌های شرکت، اطلاعات را نشت می‌نمایند. هیچ کارمند داخلی آگاهی، هرگز، به کمک یک ابزار نشت داده گرفتار نشده است. نشت با شبکه‌ها و کامپیوترهایی انجام می‌شود که شرکت آن‌ها را ارائه نکرده است.

یکی از کنترل‌های مؤثرتر در مقابل تهدیدات ناشی از کارمندان داخلی شامل یک شیوه عمل روزمره است که می‌تواند در تمام عملیات مختلف یک سازمان تعبیه شود؛ این روش به نام تفکیک وظایف شناخته شده است که باید برای کسانی که در ایالات‌متحده امریکا به الزامات Sarbanes-Oxley پرداخته‌اند، آشنا باشد. محققان امنیتی مفهوم جداسازی وظایف مربوطه را که در مدل تمامیت کلارک ویلسون معرفی شده است، می‌شناسند. در هر دو مورد توابع کاری بحرانی تجزیه‌شده به طوری که تکمیل شدن کار احتیاج به چندین فرد که بایستی درگیر باشند خواهد داشت. برای مثال؛ اگر یک کار مالی احتیاج به دو نوع فعالیت برای تکمیل شدن دارد، سپس نیاز تفکیک وظایف، این اطمینان را ایجاد می‌کند که هیچ فردی، هرگز، نمی‌تواند هر دو عمل را به تنهایی انجام دهد.

با ایجاد اطمینان از اینکه افراد متعددی درگیر یک کار بحرانی و حساس هستند، امکان اینکه یک کارمند داخلی بتواند مرتکب خرابکاری شود، به مقدار زیادی کاهش می‌یابد؛ در این صورت هنوز، چند نفر می‌توانند تبانی کرده و یک حمله داخلی ایجاد کنند؛ اما در بیشتر موارد، این عمل مشکل‌تر و احتمال آن کمتر است. باسیاست‌های تقسیم وظایف پیچیده‌تر، می‌توان خطر ایجاد خرابکاری توسط چند نفر را کاهش داد، با استفاده از کنترل‌های معماری امنیتی که احتمالاً مبتنی بر دیوار آتش نصب‌شده داخلی است. در حقیقت، برای کارهای جداسازی مبتنی بر شبکه، استفاده از دیوار آتش داخلی، سر راست‌ترین روش پیاده‌سازی است.

به طور کلی، مفهوم تفکیک وظایف را از طریق یک تابع کار ABC، با یک اپراتور تنهای A، و یا به کمک یک سری از تکه‌های کار و همچنین، با کمک چند اپراتور می‌توان نشان داد. این شمای کلی بیشتر موارد تفکیک وظایف را بدون در نظر گرفتن انگیزه و مشروح پیاده‌سازی حمایت می‌کند. تفکیک وظایف، یک لایه حفاظتی و دیوار آتش داخلی یک تفکیک وظایف سر راست ایجاد می‌نمایند. (به شکل ۳-۹ توجه کنید).



شکل ۳-۹- تجزیه توابع کاری برای تفکیک وظایف

ایده شکستن توابع کار به اجزا آن جدید نیست. سال‌های طولانی، مدیران، توابع کاری را به وظایف کوچک‌تری تجزیه کرده‌اند و این نشان می‌دهد که خط مونتاژ از کجا نشأت گرفته است. متأسفانه، بیشتر تلاش‌ها برای تجزیه تابع کار باعث افزایش بوروکراسی و کاهش رضایت کارگر (و کاربر انتهایی) شده است. تصویر کلیشه‌ای از ادارات دولتی این است که در آن مشتریان باید برای هر عملی مقابل میزی بایستند، سپس جلوی میز دیگری برای کار دیگری و تا پایان کارشان به همین ترتیب ادامه دهند. این فرآیند آزار دهنده است و امکان خرابکاری در آن بسیار کم است.

چالش برای حفاظت از زیرساخت ملی، یکپارچه کردن سیاست‌های تفکیک وظایف در تمام جنبه‌های مدیریت سرمایه‌های حیاتی و عملیاتی است؛ به طوری که با کمترین افزایش بوروکراسی انجام شود. این کار به خصوص برای سازمان‌های دولتی مشکل خواهد بود که همواره، تمایل به پرورش و در برگرفتن فرآیندهای بوروکراسی جدید را دارند.

۳-۸- جداسازی سرمایه

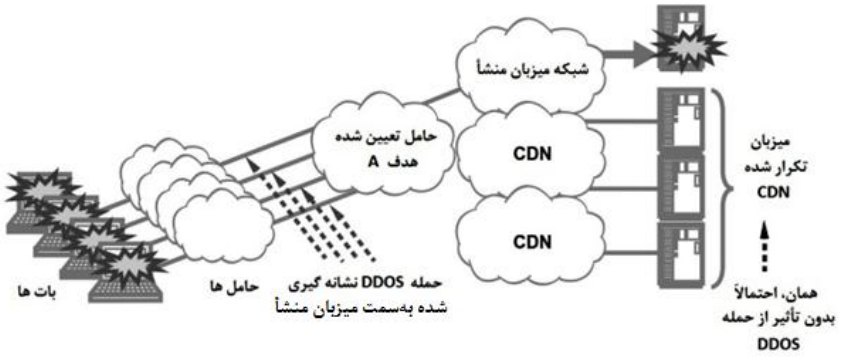
جداسازی سرمایه؛ شامل؛ توزیع، تکثیر، تجزیه و تفکیک سرمایه‌های ملی برای کاهش خطر یک سازش امنیتی ایزوله است. هر کدام از روش‌های جداسازی می‌تواند به صورت زیر تعریف شود.

- توزیع: شامل ایجاد قابلیت استفاده از چندین جز همکار می‌باشد که با یکدیگر به عنوان یک سیستم توزیع‌شده کار می‌کنند. مزیت امنیتی این سیستم در آن است که اگر سیستم توزیع‌شده به طور مناسبی طراحی شده باشد، ممکن است یک یا بیشتر اجزا آن دچار سازش یا شکست امنیتی شوند، بدون اینکه عملکرد کل سیستم دچار شکست شود.
- تکثیر: شامل کپی کردن سرمایه‌ها در سراسر اجزا غیر هم جنس است، طوری که اگر یک دارایی شکسته شود، نسخه‌های کپی شده، هنوز، در

دسترس باشند. به این ترتیب، سیستم‌های پایگاه داده برای سال‌های متمادی حفاظت‌شده‌اند. آشکار است که برای کاهش ریسک، نباید هیچ سرمایه ملی بدون درجه‌ای از تکثیر وجود داشته باشد.

- تجزیه: شکستن سرمایه‌های پیچیده به اجزای فردی است؛ به طوری که سازش امنیتی ایزوله یکی از اجزا با احتمال کمتری کل سرمایه را با شکست مواجه کند. برای مثال؛ یک روش کلی پیاده‌سازی فرآیند پیچیده تجاری، معمولاً، شامل درجه‌ای از شکستن کل فرآیند به قسمت‌های کوچک‌تر است.
- تفکیک: جداسازی منطقی سرمایه‌ها از طریق کنترل‌های دسترسی خاص، نشانه‌گذاری داده‌ها و اجرای سیاست‌ها می‌باشد. متأسفانه، سیستم‌های عامل، کنترل‌های ضعیفی در این رابطه ارائه می‌دهند که بیشتر به علت به‌کارگیری گسترده کامپیوترهای تک کار بره در چند دهه گذشته است. سازمان‌ها جداسازی منطقی داده‌ها را با تلاش بر حفظ آن‌ها در کامپیوترهای شخصی و لپ تاپ‌های متفاوت پیاده‌سازی می‌کنند که این یک روش پیاده‌سازی ضعیف است.

هر کدام از این روش‌ها در مدیریت زیرساخت‌های مدرن متداول است. برای مثال؛ شبکه‌های توزیع محتوا (CDN) که به ندرت به خاطر داشتن اثر مثبت روی امنیت زیرساخت به ندرت به آن‌ها اشاره می‌شود. میزبانی توزیع، تکرار و تکثیر که در شبکه‌های توزیع محتوا وجود دارد تکنیک‌های قدرتمندی برای کاهش ریسک و خطر هستند. برای مثال؛ کامل کردن حملات DDOS برعلیه محتواهای به میزبانیCDN نسبت به محتویاتی که فقط در میزبان منشأ هستند، مشکل‌تر است. (به شکل ۳-۱۰ توجه کنید).



شکل ۳-۱۰- کاهش خطر DDOSاز طریق محتوای CDN میزبان

مهم است تأکید شود که استفاده ازCDN ، قطعاً، حفاظت در مقابل حملات DDOS را تضمین نمی‌کند؛ اما تکثیر و توزیع ذاتی درCDN باعث مشکل‌تر شدن اجرای حمله خواهد شد. با داشتن اشاره‌گری از سیستم نام دامنه DNS به سرمایه‌های توزیع‌شده CDN، محتوا طبیعتاً قوی‌تر می‌شود. طراحان زیرساخت ملی و اپراتورها مجبورند تضمین کنند که میزبانی CDN حداقل برای تمام محتواهای مهم و حیاتی، به خصوص محتویات چندرسانه‌ای (بار کردن و دانلود جریانی پیش‌رونده) و هر نوع از نرم‌افزارهای حیاتی لحاظ شده است.

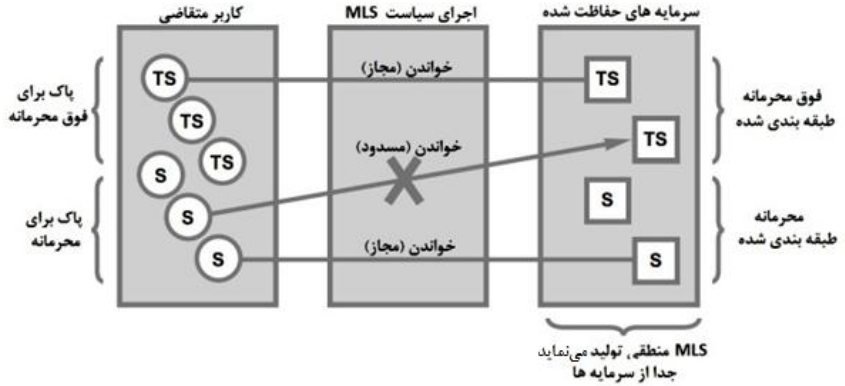
هرروز، تعبیه سرویس‌های چندرسانه‌ای در زیرساخت ملی متداول‌تر و مهم‌تر می‌شود. در گذشته نزدیک، ایده ارائه ویدیو از طریق اینترنت یک کنجکاوی ناچیز بود. آشکار است که ازدیاد محتوای ویدیویی در سایت‌هایی نظیر YouTube.com، این سرویس‌ها را جز سرویس‌های جریان اصلی درآورده است. سرمایه‌های ملی که متکی بر سرویس‌های و یدیویی هستند، باید جهت تقویت خود از سرویس‌های CDN استفاده کنند. حفاظت‌های اضافی از محتوا در مقابل حملات DDOS از طریق ارائه‌دهندگان خدمات زیربنایی نیز توصیه می‌شود.

۳-۹- امنیت چند سطحی.(MLS)

روشی که برای جداسازی منطقی سرمایه‌هایی که در جوامع امنیتی کامپیوتری، بین سال‌های ۱۹۸۰ و ۱۹۹۰، محبوبیت داشت، به نام امنیت چند سطحی شناخته می‌شود (MLS). در طی آن سال‌ها، سیستم‌عامل MLS، کاربردهای زیادی را به بازار جامعه امنیتی عرضه کرد. یک پیاده‌سازی معمولی MLS؛ شامل تعبیه کنترل‌های دسترسی اجباری و قلاب‌های دنباله ممیزی در هسته سیستم‌عامل بود. برای اطمینان از اینکه اجزا مورد اعتماد هسته سیستم‌عامل درست هستند یا، درست به نظر می‌رسند، از روش‌های تضمین‌شده استفاده می‌شد. امروزه به دلایل بیشتر اقتصادی، سیستم‌های MLS دیگر در دسترس نیستند بجز در بیشتر کاربردهای طبقه‌بندی شده و محرمانه دولتی.

ایده پنهان در MLS این است که می‌توان با برچسب‌گذاری فایل‌ها و دیرکتوری‌های سیستم کامپیوتر با طبقه‌بندی‌های معنی‌دار و همچنین، با برچسب‌گذاری کاربران سیستم بر اساس پاک بودن سوابق آن‌ها سیاست امنیت شناخته‌شده‌ای را اجرا نمود. این طرح که بیشتر انگیزه آن مبتنی بر روش‌های کاغذی استفاده‌شده در دولت جهت حفاظت اطلاعات بود، بر اساس سیاست‌های جداسازی منطقی بین بعضی سرمایه‌ها و بعضی کاربران ایجاد شده بود. برای مثال؛ فایل‌هایی را که با علامت "Secret" نشانه‌گذاری شده بودند، تنها کاربرانی می‌توانستند بخوانند که سوابق گزینشی و اجازه خاصی داشتند؛ کاربرانی که سوابق گزینشی آن‌ها در سطح "Topsecret" نبود، اجازه خواندن چنین فایل‌هایی را نداشتند.

(به شکل ۳-۱۱ توجه کنید).



شکل ۳-۱۱- استفاده از جدایی منطقی MLS برای حفاظت از سرمایه‌ها

نتیجه، یک سیاست اجباری برای درخواست کاربران و حفاظت از سرمایه‌ها بود. چندین مدل رفتار سیستم‌های کامپیوتری با چنین قابلیت‌های MLS در سال‌های اولیه امنیت کامپیوتری توسعه پیدا کرد. مدل‌های افشا Bell-Padilla و تمامیت Biba مثال‌های برجسته آن هستند. هر کدام از این مدل‌ها، قوانین سیاست‌های تصریح‌شده‌ای است که به برخی خواص امنیتی مطلوب کمک خواهد کرد؛ قطعاً، مشکلاتی نیز وجود دارد، به خصوص اگر شبکه به سیستم‌های امن ایزوله شده اضافه شود. متأسفانه، تحقیق و توسعه در مورد MLS به طور مرموزی در اواسط دهه ۱۹۹۰ از بین رفت که شاید به علت کشش اقتصادی وب سراسری جهان (WWW) بود. متأسفانه، قابلیت‌های ذاتی در مدل جداسازی MLS در چشم‌انداز زیرساخت ملی کنونی نیز باارزش است. علاقه مجددی به سیستم‌هایMLS به شدت تشویق و توصیه می‌شود تا حفاظت سرمایه‌های ملی را بهبود بخشد.

پیاده‌سازی یک برنامه جداسازی ملی

پیاده‌سازی یک برنامه جداسازی ملی شامل بازبینی و تأیید درستی برخی اهداف طراحی در آژانس‌های دولتی و شرکت‌هایی با مسئولیت در زیرساخت ملی است. این اهداف مرتبط با اجرای سیاست‌ها بین کاربران متقاضی و سرمایه‌های حفاظت‌شده ملی بوده و شامل موارد زیر است:

- جداسازی اینترنت: برخی از سرمایه‌های حیاتی ملی نباید به آسانی از طریق اینترنت قابل‌دسترسی باشند. سیستم‌های کنترل نیروگاه اتمی کاندید خوبی برای جداسازی از اینترنت هستند. وجود برنامه‌های رسمی ملی برای معتبر سازی چنین جداسازی ایده خوبی است. اگر این برنامه به تغییراتی در شیوه‌های عمل تجاری نیاز نداشته باشند، به کمک و راهنمایی برای انتقال از اتصال باز اینترنتی به چیز دیگری که خصوصی‌تر است، مورد نیاز خواهد بود.
- دیوارهای آتش مبتنی بر شبکه: سیستم‌های زیرساخت ملی باید تشویق شوند که از دیوارهای آتش مبتنی بر شبکه استفاده کنند. ترجیحاً دیوارهای آتشی که به وسیله یک گروه مرکزی مدیریت می‌شوند، در این صورت احتمال اینکه امضاها بروز نگه داشته شوند و سیستم‌های امنیتی به طور مناسبی بر اساس ۲۴/۷ عمل نمایند، افزایش می‌یابد. استفاده از امنیت مبتنی بر شبکه، به خصوص برنامه‌های خرید و تدارکات دولتی باید به صورت معمول در هر قرارداد با ارائه‌دهندگان سرویس‌های اینترنتی گنجانده شود.
- حفاظت از DDOS: تمامی شبکه‌های مرتبط با سرمایه‌های ملی، پیش از اینکه حمله‌ای اتفاق بیفتد، باید نوعی حفاظت در مقابل حملات DDOS داشته باشند. این حفاظت باید در شبکه‌های ظرفیت بالای زیرساخت

تعبیه شده باشد تا باعث شود که مهاجمانی که حمله سایبری مبتنی بر ظرفیت بالا را در نظر می‌گیرند، کار برایشان سخت شود. اگر برخی سازمان‌ها؛ نظیر؛ آژانس‌های دولتی طرح حفاظت DDOS مناسبی نداشته باشند، مثل این است که آن‌ها هیچ برنامه بازیافت از فاجعه ندارند.

- جداسازی داخلی: محیط‌های زیرساخت ملی حیاتی باید نوعی مشوق برای پیاده‌سازی سیاست جداسازی داخلی جهت جلوگیری از خرابکاری داشته باشند. الزامات Sarbanes-Oxley در ایالات‌متحده امریکا سعی در اجرای چنین جداسازی برای سیستم‌های مالی داشته‌اند. از آنجا که بحث در مورد اینکه این یک ابتکار موفق آمیز بوده است یا خیر، ادامه دارد. داشتن نوعی برنامه برای زیرساخت ملی، ارزش لحاظ کردن را خواهد داشت. اعتبارسنجی مورد نیاز خواهد بود تا دیوارهای آتشی که وجود دارند، بتوانند دامنه حفاظتی را در اطراف سرمایه‌های حیاتی ایجاد کنند.
- تنظیم الزامات و نیازها: برای فروشندگان دیوارهای آتش باید مشوق‌هایی در نظر گرفته شود که ساخت سیستم‌های مناسب و مخصوص مانند دیوار آتش برای محیط‌های SCADA را در نظر بگیرند. این کار، به شدت به مدیران امنیتی نیاز دارد تا در چنین موقعیت‌هایی پیکربندی شبکه‌هایشان را در موقعیت باز کاهش دهند.

بدیهی است، هنگامی که یک برنامه ملی در جای خود قرار بگیرد، در نظر گرفتن چگونگی جداسازی سرمایه‌ها بین کشورهای همکار مختلف، یک توسعه منطقی آن خواهد بود. که با توجه به پیچیدگی و مشکل ایجاد یک سیاست اجرایی اعتبارسنجی شده در یک ملت، این هدف دورتری خواهد بود.

فصل ٤: تنوع

به کامپیوترها همان طور نگاه می‌کنیم که پزشکان به بیمارانی که اشکالات ژنتیکی دارند، همه این بیماران مستعد ابتلا به اختلالات مشابهی هستند.

مایک ریتر استاد مهندسی برق و کامپیوتر و علوم کامپیوتر در دانشگاه کارنگی-ملون.

ساخت متنوع‌تر زیرساخت ملی برای ایجاد انعطاف‌پذیری بیشتر در مقابل حملات سایبری رویکرد خیلی معقولی به نظر می‌رسد. برای مثال؛ از سال‌ها پیش، دانشمندان علوم طبیعی پی برده‌اند که یک اکوسیستم متنوع، همیشه، انعطاف‌پذیری بیشتری در مقابل امراض نسبت به اکوسیستم بدون تنوع دارد. زمانی که یک جنگل دارای یک نوع درخت است احتمال دارد که یک مرض تنها بتواند کل اکوسیستم را نابود کند.

این وضعیت حتی در کسب‌وکار هم رخ می‌دهد. برای مثال؛ بعضی خطوط هوایی تصمیم گرفته‌اند که از یک مدل هواپیما استفاده کنند. این باعث کاهش هزینه‌های نگهداری و آموزش می‌شود؛ اما مخاطرات جدی‌ای را در صورتی که این نوع هواپیماها به عللی زمین‌گیر شوند (مثل عیب طراحی) ایجاد می‌نماید. شرکت هواپیمایی تعطیل خواهد شد- خطری که با رویکرد تنوع می‌توان از آن جلوگیری کرد.

می‌توان استدلال کرد که فرآیند امن کردن هر مجموعه از سرمایه‌های ملی، همیشه، باید نوعی راهبرد تنوع داشته باشد و به تمام کاربردها، نرم‌افزارها، کامپیوترها، شبکه‌ها و سیستم‌ها گسترش یابد. متأسفانه، به استثناء الزامات جغرافیایی روی مسیرهای شبکه و مرکز داده، تنوع، معمولاً، در الزامات حفاظت از زیرساخت گنجانده نشده است. در حقیقت، محققان علوم کامپیوتری به خوبی به مبحث معرفی عمدی تنوع

برای افزایش امنیت در زیرساخت ملی توجه نکرده‌اند. اخیراً، بعضی پژوهشگران منافع تنوع در پیاده‌سازی نرم‌افزار را بررسی کرده‌اند.

تنوع در زیرساخت‌های ملی؛ شامل؛ قرار دادن تفاوت‌های عمدی در داخل سیستم‌ها است. تفاوت‌های مرتبط، منبع فروشنده، رویکرد به‌کارگیری، اتصال به شبکه، استانداردهای مورد هدف، زبان برنامه‌نویسی، سیستم‌عامل، پایه کاربرد، نسخه نرم‌افزار و ... را شامل می‌شود. دو سیستم متنوع در نظر گرفته می‌شوند اگر ویژگی‌های کلیدی آن‌ها متفاوت باشند در غیر این صورت، غیر متنوع خواهند بود. (به شکل ۴-۱ توجه کنید).

سیستم	منبع فروشنده	رویکرد به‌کارگیری	اتصال شبکه	استانداردهای مورد هدف	زبان برنامه نویسی	سیستم عامل	ویژگی ها
A	شرکت X	آماده مصرف	IP	IP sec	C++	ویندوز	A و B متنوع هستند
B	شرکت Y	مشتری	TDM	هیچ	جاوا	یونیکس	
C	شرکت Z	مشتری	TDM	هیچ	جاوا	یونیکس	B و C غیر متنوع هستند

شکل ۴-۱- اجزا متنوع و غیر متنوع از طریق تفاوت ویژگی‌ها

متأسفانه، دشمن در مورد هر یک از ویژگی‌های مرتبط با سیستم هدف، فرض‌هایی دارد. در صورت نداشتن تنوع، دشمن فرضیات درستی را در مورد هر کدام از ویژگی‌ها خواهد داشت. برای مثال؛ اگر دشمن فرض کند که مجموعه‌هایی از کامپیوترها سیستم عامل میکروسافت دارند و حمله‌ای را انجام دهد، اگر سرمایه‌های ملی در خطر، از این نوع سیستم عامل استفاده کرده باشند، نتایج ایجادشده می‌تواند قابل ملاحظه باشد. در صورتی که تنوع وجود داشته باشد، برای دشمن ایجاد حمله‌ای که بیشترین اثر را داشته باشد، بسیار مشکل خواهد بود. این امر، به ویژه در حملاتی بسیار مؤثر است که جهت انتشار خودکار طراحی‌شده‌اند. سرانجام حمله به نقطه‌ای می‌رسد که دیگر نمی‌تواند خود را در سیستم هدف کپی کرده و از دور اجرا نماید و فرآیند انتشار متوقف می‌شود.

پس چرا به تنوع در حفاظت از زیرساخت‌های ملی، کم توجه شده است؟ برای درک این مطلب، ابتدا باید هدف نزدیک به وسواس اجرای مجموعه‌ای از استانداردهای رایجی را تشخیص دهیم که مجامع امنیتی و فناوری اطلاعات برای رسیدن به آن‌ها تلاش کرده‌اند. در هر زمینه محاسباتی مجموعه‌ای از استانداردها و شیوه‌های عمل ممیزی تعریف‌شده‌اند که سازمان‌های قدرتمندی از آن‌ها حمایت می‌کنند. در ایالات‌متحده امریکا، استاندارد Sarbanes-Oxley تأثیر عمیقی بر عملیات شرکت‌های بزرگ در کشور داشته و منجر به رویکردهای مشترکی برای عملیات سیستم‌های مالی شده است. همان طور که در فصل بعد بحث خواهد شد، اشتراک تا حدودی در تقابل با تنوع است.

این تمرکز بر حفظ محیط‌های عملیاتی استاندارد و مشترک نباید باعث تعجب گردد. به عنوان مثال، ظهور اینترنت، با پذیرش مشترک یک مجموعه پروتکل (TCP/IP) به تحرک درآمده است. حتی ارائه خدمات اینترنتی؛ نظیر؛ وب سایت‌ها و سرورهای پست الکترونیکی برای پیروی از تخصیص پرت‌های مشترک به توافق بین مدیران سیستم‌ها نیاز دارند. اگر هر مدیر تصمیم به تخصیص شماره پرت‌های تصادفی به سرویس‌های اینترنتی خود بگیرد، هرج‌ومرج پیش خواهد آمد؛ کاربران انتهایی به آسانی نخواهند توانست نیازهای خود را تعیین کنند و اینترنت یک محیط آشفته خواهد شد. (این مسئله، گستره وسیعی از حملات را پیچیده‌تر خواهد کرد)؛ بنابراین، نتیجه توافقی عمومی بر پیکربندی محاسباتی مشترک خواهد بود.

برای بیشتر مدیران سیستم‌ها، یکی دیگر از انگیزه‌های کلیدی برای جلوگیری از تنوع هزینه‌های آن است. تیم‌های معمولی مدیریت شبکه و محاسبات، برنامه‌هایی ایجاد کرده‌اند که متمرکز بر حذف تفاوت‌ها در سیستم‌های بنگاه اقتصادی برای کاهش هزینه‌های عملیاتی است. روشن است که سیستم‌های غیر متنوع فناوری اطلاعات، به‌کارگیری سکوها، تربیت کاربران انتهایی، شیوه‌های عمل مدیریت و مستندسازی سیستم‌ها را تسهیل می‌نمایند. برای این دلایل مرتبط با هزینه، در بیشتر محیط‌های

فعلی زیرساخت ملی، ایجاد تنوع یک هدف برجسته نیست. در نتیجه، یک زیرساخت امنیت کمتری خواهد داشت. در حال حاضر، مسئله تنوع با اشتراک و صرفه‌جویی در هزینه در حال رقابت است.

۴-۱- تنوع و انتشار کرم

خود انتشار دهندگی یک کرم کامپیوتری مثال خوبی از یک نوع حمله است که عمل کردن مناسب آن بر محیط هدف غیر متنوع متکی می‌باشد. پاراگراف زیر نشان می‌دهد که یک حمله می‌تواند بسیار ساده باشد.

عملکرد کرم در سه قدم آسان

عملکرد یک کرم کامپیوتری معمولی کاملاً سرراست است؛ فقط سه قدم و می‌تواند با جملات شبه کد ساده زیر بیان شود:

برنامه: کرم

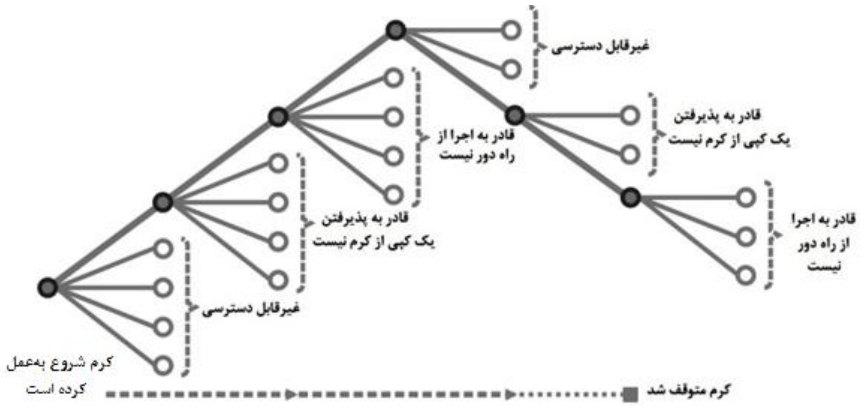
شروع

- قدم اول: یک سیستم هدف در شبکه برای انتشار برنامه کرم پیدا کنید.
- قدم دوم: برنامه کرم را در سیستم هدف کپی کنید.
- قدم سوم: برنامه کرم را در سیستم هدف از دور اجرا کنید.
- قدم‌های ۱ تا ۳ را تکرار کنید.

همان طور که می‌بینید، برنامه کرم متکی بر توانایی یافتن سیستم‌های متداول، در دسترس و قابل تعامل در شبکه‌هایی است که یک کپی از برنامه کرم را پذیرفته و اجرا می‌کنند. در روزهای ابتدایی اینترنت، این عمل با بررسی یک فایل محلی انجام می‌شد که دارای لیست تمام سیستم‌های قابل‌دسترس بود. امروزه آن را با ایجاد دسته‌هایی از

آدرس‌های پروتکل اینترنت انجام می‌دهند. همچنین، در روزهای اولیه، به علت اینکه دیوار آتش هنوز اختراع نشده بود، کپی و اجرا کردن برنامه‌ها از یک سیستم به سیستم دیگر آسان بود.

همه امیدوار بودند و گمان می‌کردند که به‌کارگیری جهانی دیوار آتش می‌تواند دشمن را برای ایجاد کرم‌ها متوقف کند؛ ولی متأسفانه این‌طور نشد. در عوض، آسیب‌پذیری‌ها یا خدماتی که از طریق دیوار آتش باز بودند، مبنای استفاده کرم‌ها قرار گرفتند نداشتن تنوع در برپا کردن و راه‌اندازی چنین سیستم‌هایی معمول است؛ زیرا اگر کرم در یک محیط متنوع عمل نماید و نتواند سیستم‌هایی را پیدا کند که یک یا چند تا از این معیارها را رعایت می‌کنند، انتشار آن سریع‌تر متوقف خواهد شد. عمل فوق را می‌توان در یک نمودار ساده دسترس‌پذیری نشان داد که در آن برای یک کرم نقطه شروع انتشارش تا نقطه پایان را که در آن فعالیتش به علت وجود تنوع متوقف می‌شود، نشان می‌دهد. آنجا که کرم سعی در انتشار دارد، ویژگی‌های تنوع، توانایی او را در یافتن سیستم‌های قابل‌دسترسی که بتوانند خود را در آن‌ها کپی کرده و از دور آن‌ها را اجرا کنند، کاهش می‌دهد. (به شکل ۴-۲ توجه کنید).



شکل ۴-۲- کاهش فعالیت‌های کرم از طریق تنوع

بدیهی است که سر انجام انتشار تمام کرم‌ها، صرف‌نظر از درجه تنوع موجود در شبکه، متوقف می‌شود. مزیت امنیتی که با تنوع می‌توان به دست آورد، این است که انتشار کرم احتمالاً سریع‌تر و شاید بدون دخالت آسان متوقف خواهد شد. نتایج تجربی در مجامع امنیتی جهانی که با کرم‌هایی نظیر SQL/Slammer، Blaster Worms Of 2003 و Sasser Worm 2004 مقابله می‌کردند، پیشنهاد می‌کند که برای متوقف کردن عملیات بدخواهانه به دخالت قابل ملاحظه انسان نیاز است. در ساعات اولیه انتشار کرم SOL/Slammer، بیشتر پاسخ‌های تماس حوادث امنیتی مربوط به افرادی بود که برای کشف اینکه چکار باید بکنند، تلاش می‌کردند. سرانجام، مؤثرترین راه حل قرار دادن شبکه‌های محلی در موقعیتی بود که بتوانند ورود ترافیک متجاوز را متوقف کنند. پس از پایان این حادثه، میلیون‌ها ساعت از کار در سراسر جهان صرف کار روی این مسئله شده بود. با افزایش تنوع، می‌توان انتظار داشت که مخارج پاسخگویی مرتبط با مقابله با کرم‌ها در سراسر جهان کاهش یابد.

چالش واقعی این است که اینترنت، شبکه‌ها و سیستم‌هایی که شرکت‌ها و آژانس‌هایی که مسئول زیرساخت ملی هستند، آن‌ها را اداره می‌کنند متنوع نیستند و بحث‌های کمی در مورد تغییر این وضعیت در جریان است. همان طور که قبلاً اشاره کردیم، این عدم تنوع بیشتر به خاطر بیشینه کردن هدف تعامل پذیری است. در مجامع محاسباتی وسیع‌تر، بعضی موارد استثنا نیز وجود دارد؛ مثل؛ سیستم‌های مبتنی بر مدیریت حقوق دیجیتال (DRM) که تمایل به محدود کردن اجرای بعضی کاربردهای محتوایی به برخی دستگاه‌های خاص نظیر IPod و IPone دارند. به هر حال، روند رایج به سمت محاسبات تعامل پذیر بازتر است. این به آن معنی است که برای اجزای زیرساخت ملی که باید در مقابل حملات خودکار مثل حمله کرم‌ها انعطاف‌پذیر باشند، تا زمانی که محیط شبکه غیر متنوع است، این تهدید باقی می‌ماند.

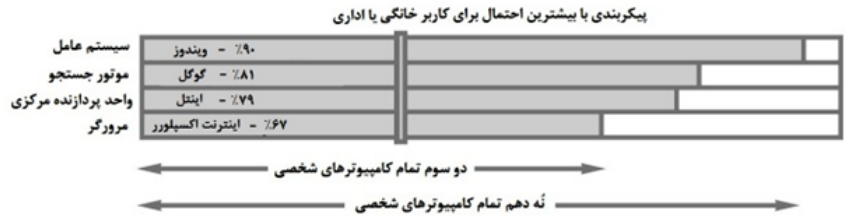
۴-۲- تنوع سیستم کامپیوتری رومیزی

کاربران معمولی کامپیوتر در خانه یا اداره، از یک سیستم عامل تجاری استفاده می‌کنند که روی یک سکوی پردازنده استاندارد اجرا می‌شود و از یک یا چند مرورگر محبوب جهت جستجو روی یکی از موتورهای جستجوی متداول استفاده می‌کنند. در روزهای ابتدایی کامپیوتر و محاسبات، بسیاری از کاربران از سیستم‌های کامپیوتر خانگی و اختصاصی استفاده می‌کردند که روی آن‌ها انواع نرم افزارهایی که ممکن بود به صورت محلی شناخته شوند نصب شده بود.

امروزه، پیکربندی با بیش‌ترین احتمال سیستم عامل مبتنی بر ویندوز روی یک سکوی اینتل با مرورگر اینترنت اکسپلورر است که برای جستجوها از گوگل استفاده می‌شود. می‌توانیم با اطمینان بگوییم که تقریباً تمام برآوردهای فعلی سهم بازار، سیستم‌های فوق را به عنوان محصولات غالب در زمینه مربوطه خودشان لیست می‌کنند. قطعاً، سکوها و خدمات رقیب از Apple و دیگران تهاجماتی را در بازار شروع کرده‌اند؛ ولی هنوز در بسیاری از محیط‌های دولتی و تجاری پیکربندی برای کامپیوترهای رومیزی هنوز با احتمال بالایی قابل پیش‌بینی است. (به شکل ۴-۳ توجه کنید).

وضعیت این چند شرکت غالب (نظیر میکروسافت، گوگل، اینتل و ...)، مسلماً باعث ایجاد نتایج مثبت شده است. برای مثال، باعث درک مشترک عمیق‌تری از محاسبات در بین افراد در سراسر دنیا شده است. مردم مختلف از فرهنگ‌های متفاوت در جهان، می‌توانند تجربیات، توصیه‌ها و پیشنهادات کاربردی‌شان را در مورد سیستم‌های عامل، موتورهای جستجو، پردازشگرها و مرورگرها به اشتراک بگذارند. موقعیت غالب این محصولات، با ایجاد بازارهای هدف مشترک و جذاب به توسعه صنعت نرم‌افزار کمک می‌کند. توسعه‌دهندگان نرم‌افزار و سخت‌افزار خیلی دوست دارند که پیکربندی سکوی غالب را داشته باشند؛ زیرا با استفاده بیشینه از محصولاتشان سود بالقوه‌شان افزایش

خواهد یافت؛ بنابراین محاسبات، به خاطر این اشتراک، سخت‌افزار و نرم‌افزار به جلو حرکت کرده است.



شکل ۴-۳- پیکربندی معمولی کامپیوترهای شخصی که نداشتن تنوع را نشان می‌دهند

از چشم‌انداز زیرساخت‌های ملی، اشکال این است که دشمنان حملات را آسان‌تر با برد و پیامدهای قابل‌ملاحظه‌تر ایجاد می‌نمایند. درست مثل بازی دومینو، زمانی که دومینو به صورت یکنواخت طراحی‌شده و قرار گرفته باشد، به بهترین نحو عمل می‌کند؛ یک زیرساخت مشترک را نیز می‌توان با یک فشار ساده و یکنواخت راحت‌تر سرنگون کرد. در برخی موارد، آثار حمله قابل ملاحظه است؛ برای مثال؛ شرکت میکروسافت بازار سیستم عامل کامپیوترهای شخصی رومیزی را تسخیر کرده است؛ یک حمله مبتنی بر ویندوز که خوب طراحی شده باشد، می‌تواند تا ۹۰ درصد کامپیوترهای رومیزی را مورد هدف قرار دهد.

به احتمال زیاد، ایجاد باتنت به علت نداشتن تنوع پیکربندی کامپیوتر شخصی بسیار آسان‌تر می‌شود. هنگامی که یک اپراتور باتنت، طراحی مفهومی باتنت جدیدی را انجام می‌دهد مهم‌ترین ملاحظات طراحی شامل برد است. یعنی اپراتور باتنت در جستجوی ایجاد بد افزاری است که با احتمال بالا به طور موفقیت‌آمیزی تعداد زیادی از کامپیوترهای شخصی هدف را آلوده کند. به این ترتیب، عدم تنوع پیکربندی کاربران انتهایی نقش مهمی برای اجرای اهداف اپراتور باتنت ایفا می‌کند. اگر این همراه با شیوه عمل ضعیف مدیریت سیستم‌های بیشتر کامپیوترهای شخصی باشد، می‌تواند نابود

کننده باشد. بدتر از همه اینکه، بسیاری از مدیران امنیتی در کسب‌وکار و دولت این خطر را نمی‌فهمند و به ندرت مشکل ناشی از یک مجموعه جهانی از کامپیوترهای شخصی کاربران انتهایی غیر متنوع را که به وسیله کاربران خانگی و اداری سیستم‌هایشان را بد مدیریت می‌کنند، درک می‌کنند.

در واکنش به این تهدید، حفاظت از زیرساخت ملی نیاز به معرفی و ورود هماهنگ و عمدی تنوع به محیط محاسباتی جهانی کامپیوترهای رومیزی دارد. آشکار است که توجه بنگاه‌های تجاری نسبت به افراد در خانه متفاوت است، اما در هر دو مورد اصول یکسانی بکار گرفته می‌شوند. اگر سرمایه‌های محاسباتی کامپیوترهای رومیزی که می‌توانند به سرمایه‌های ملی دسترسی داشته باشند، خیلی مقاوم و انعطاف‌پذیر باشند، تنوع این کامپیوترهای رومیزی ارزش توجه را خواهد داشت. بارزترین چالش به بازار مصرف‌کنندگان کامپیوترهای شخصی برمی‌گردد؛ یعنی دلیل اینکه چرا مصرف‌کنندگان از یک سکوی مشابه استفاده می‌کنند؛ و آن را ترجیح می‌دهند و برای خرید انتخاب می‌کنند. برای مثال؛ اگر شرکت‌های میکروسافت و اینتل ارزش‌هایی را در محصولات خود ارائه نمی‌کردند، مردم محصولات دیگری را می‌خریدند. بنابراین، بزرگ‌ترین مانع همان عدم تنوع در ارائه محصولاتی است که مردم علاقه به استفاده از آن‌ها دارند، شاید رسیدن به این هدف از طریق عناصر تنوعی که در اساس فروشندگان موجود است، به دست آید.

ملاحظات تنوع کامپیوترهای رومیزی

مسائل اضافی که در مورد برنامه تنوع کامپیوترهای رومیزی وجود به می‌آید؛ شامل موارد زیر است:

- هزینه‌های سکو: با وارد شدن چندین سکوی متنوع به محیط‌های محاسباتی، مخارج مرتبط با سخت‌افزار و نرم‌افزار افزایش می‌یابد. این توجیه متداولی است که مدیران فناوری اطلاعات برای اجتناب از ابتکارات ایجاد تنوع از آن بهره می‌گیرند. خرید حجم بیشتری از یک محصول خاص، باعث کاهش قیمت یک واحد آن خواهد شد. ورود رقابت در عرصه خرید و تدارکات کامپیوترهای شخصی، افزایش هزینه‌ها را تا حدی کاهش می‌دهد.
- قابلیت تعامل کاربردها: سکوهای متعدد و متنوع، اهداف سازمانی را برای تضمین تعامل مشترک برنامه‌های کاربردی کلیدی در سراسر سکوها پیچیده خواهد کرد. این را می‌توان با تلاش بر تطبیق دادن سکوهای کامپیوتری رومیزی به احتیاجات محلی خود، مدیریت کرد؛ این فرآیند جزیی و کم اهمیت نیست. خوشبختانه، بیشتر کاربردهای مبتنی بر وب در سکوهای متنوع شبیه هم رفتار می‌کنند.
- پشتیبانی و آموزش: سکوهای متعدد و متنوع فرآیندهای پشتیبانی و آموزش را با اضافه کردن مجموعه جدیدی از نگرانی‌های فروشندگان پیچیده خواهند کرد؛ اثر یک سکو مانند Mac OSرا در محیط سنتی ویندوز در سیستم‌ها وارد و معرفی کنیم؛ بسیاری از مصرف‌کنندگان باهر دو سکو راحت هستند. به خصوص جوان ترها که تمایل بیشتری به انتخاب‌های متنوع دارند؛ مشکل آن طور که به نظر می‌رسد، شدید نخواهد بود.

برای حفاظت از زیرساخت ملی، ابتکارهای تنوع کامپیوترهای رومیزی شانس زیادی برای موفقیت خواهند داشت، اگر بر وجود اختلافات آژانس‌ها، شرکت‌ها و بنگاه‌های تجاری تمرکز شود. در یک بنگاه تجاری، می‌توان برای مخلوط کردن سکوهای کامپیوترهای رومیزی پاداش‌ها و مشوق‌هایی قرار داده شود. که از نظر طراحی و به‌کارگیری بات‌نت موارد فوق سودمندی محدودی خواهند داشت. مزیت واقعی از تنوع در کامپیوترهای شخصی حاصل می‌شود که ارتباطات باند پهن دارند و مصرف‌کنندگان در سراسر جهان از آن استفاده می‌کنند. متأسفانه، این مسئله‌ای نیست که به راحتی بتواند به وسیله ابتکاری در کشوری مانند ایالات‌متحده امریکا، کنترل شود.

جالب توجه است که یک مشکل مرتبط دیگر ظاهراً دزدی گسترده نرم‌افزار است که می‌توان آن را در برخی نقاط دنیا یافت. دزدی نرم‌افزار در کامپیوترهای رومیزی، مشکل به‌روز کردن‌های امنیتی آن‌ها را نیز ایجاد می‌کند. برای کامپیوترهای شخصی که نرم‌افزارهای غیرمجاز دارند، حفاظت امنیتی مناسب آن‌ها از طریق وصله‌های نرم‌افزاری مشکل خواهد بود. زمانی که چندین میلیون کامپیوتر در این وضعیت هستند، مسئله غیر متنوع بودن بسیار جدی خواهد شد.

۴-۳- پارادوکس (تناقض) تنوع محاسبات اَبری

معرفی یک مدل ساده از سیستم‌های رایانه‌ای رومیزی، به فهم بهتر اینکه چگونه می‌توان به اهداف تنوع رسید، کمک می‌کند. این مدل، یک طیف خطی از گزینه‌هایی است که در آن درجه‌ای که سیستم‌ها متنوع یا غیر متنوع هستند را نمایش می‌دهد. به این ترتیب، برای یک محیط داده‌شده، شناسایی دو سر طیف آسان است. در یک طرف طیف، گزینه عدم تنوع کامل وجود دارد که در آن هر کامپیوتر رومیزی در سازمان یا بنگاه تجاری یا گروه عیناً مثل هم است و در طرف دیگر طیف، گزینه تنوع کامل است که در آن در سراسر سازمان یا شرکت، هیچ دو سیستم کامپیوتر رومیزی مثل هم

نیستند. در وسط طیف، انواع معمولی تنظیمات قرار می‌گیرد که در آن درجه کمی از تنوع همراه با یک سیستم غالب آشکار وجود دارد.

این مدل طیف مفید است؛ زیرا پیشنهاد ما را در مورد امنیت زیرساخت اساسی در کامپیوترهای شخصی نشان می‌دهد؛ یعنی همان طور که تنوع افزایش می‌یابد، اجرای حملات به کامپیوترهای رومیزی شامل استفاده از کرم‌ها برای ایجاد شرایط امتناع از سرویس محلی مشکل‌تر خواهد شد؛ همچنین، ایجاد و استفاده از بات‌نت نیز مشکل‌تر می‌شود؛ اما این کار سودمندی نسبتاً کمتری خواهد داشت. (به شکل ۴-۴ توجه کنید).

شکل ۴-۴- طیف گزینه‌های تنوع در کامپیوترهای رومیزی

در حقیقت، نقض امنیتی یکنواخت رایانه‌های رومیزی متنوع، مشکل‌تر است؛ زیرا آن‌ها به عنوان یک گروه به حملات مقیاس‌پذیر و خود انتشاردهنده کمتر رسانا خواهند بود. برای مثال؛ اگر نیمی از کامپیوترهای شخصی یک شرکت، سیستم عامل ویندوز و نیم دیگر Mac OS داشته باشند، آشکار است که این برای یک حمله خود انتشاردهنده چالش بیشتری ایجاد خواهد کرد. بنابراین، میزان تنوع و سختی حمله با یکدیگر همبستگی دارند. یک چالش در مقابل این نظر این است که به طور مناسبی انتخاب بهینه‌ای در کاهش خطر حمله به کامپیوترهای رومیزی را مشخص نمی‌کند. یعنی اگر همه رایانه‌های رومیزی را از محیط هدف حذف کنیم، خطر حمله به سیستم‌هایی که دیگر وجود ندارند، هم وجود نخواهد داشت. این یک طیف جدید تنوع در مقابل مشکل

حمله را پیشنهاد می‌نماید (مسلماً به صورت نظری و تئوری). (به شکل ۴-۵ توجه کنید).

شکل ۴-۵- تنوع و مشکل بودن حمله با گزینه حذف

این نشان می‌دهد که گزینه نهایی (البته غیرممکن) برای امن‌تر ساختن رایانه‌های رومیزی ممکن است شامل حذف آن‌ها باشد. بدیهی است که این یک هدف عملی نیست، اما اهداف امنیتی کامپیوترها، از طریق جملات روشنی مهار می‌شوند که شرایط ایده آل امنیتی را معین می‌کنند. با اینکه ساختار فعلی محاسباتی شرکت‌ها و خانه‌ها گزینه نداشتن کامپیوترهای رومیزی را دربر نمی‌گیرد، خوانندگان کتاب که مسن‌تر هستند، روزهایی را به خاطر می‌آورند که رایانه‌های رومیزی وجود نداشت. در آن روزها، مردم برای دسترسی به اطلاعات از ترمینال‌های کامپیوترهای بزرگ mainframe استفاده می‌کردند و در یک چنین سیستم‌هایی، منافع امنیتی موجود بود. در چنین سیستم‌هایی احتیاجی به وصله‌های نرم‌افزاری کاربران و همین طور سکویی برای اینکه کاربران انتهایی هدف بد افزار قرار گیرند موجود نبود. یک طنز بزرگ در به‌کارگیری رایانه‌های رومیزی برای هر مرد یا زن و یا بچه روی کره زمین این ست که بیشتر مردم احتیاجی به چنین قدرت محاسباتی ندارند. احتمالاً، برای بیشتر مردم یک صفحه‌کلید، نمایشگر و یک موس کافی است تا بتوانند با اینترنت همه جا به کاربردهای ساکن شبکه دسترسی یابند.

در محاسبات مدرن، نزدیک‌ترین چیز به این آرایش، محاسبات مجازی شده مبتنی بر اَبر است. در چنین آرایشی، قدرت محاسباتی و هوش کاربردها به مجموعه سرورهای پیچیده مرکزی منتقل می‌شوند؛ که از طریق مشتری‌هایی با نیاز محاسباتی سبک قابل‌دسترسی هستند. در حقیقت، در چنین محیط‌های اَبری، گوشی‌های موبایل دستی مانند یک رایانه رومیزی عمل می‌کنند. بنابراین، باملاحظه شکل ۴-۵ می‌توان فرض کرد که با حذف رایانه‌های رومیزی غیر متنوع، محاسبات ابری منافع امنیتی قابل‌ملاحظه‌ای را در محیط ایجاد خواهند کرد. در صورتی که، زیرساخت‌هایی که از کاربردهای ابری حمایت می‌کنند، به طور مناسبی امن شوند، به علت اصولی که قبلاً در این کتاب توضیح داده شد، این موضوع درست خواهد بود. اگر این‌طور نباشد، آسیب‌پذیری‌های ناشی از عدم تنوع را به آسانی از رایانه‌های رومیزی به سرورها منتقل خواهیم کرد.

۴-۴- تنوع فناوری شبکه

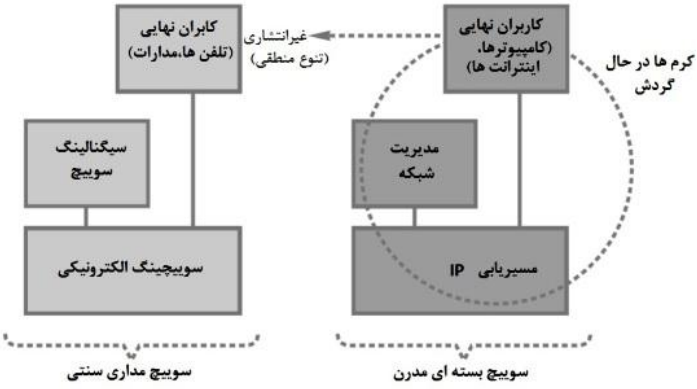
سیستم‌های شبکه‌های مخابراتی مدرن می‌توانند از دو چشم‌انداز دیده شوند که دو نوع فناوری پایه‌ای را شامل می‌شود.

- سوئیچ مداری: فناوری سیستم‌های قدیمی، سوئیچ مداری می‌باشد و از سرویس سنتی تلفن‌های ساده، سرویس‌های صدا و داده حمایت می‌کند. شبکه تلفن سوئیچ شده عمومی یا PSTN، مهم‌ترین مثال از به‌کارگیری فناوری سوئیچ مداری است.
- سوئیچ بسته‌ای: این سیستم‌های مدرن‌تر سوئیچ بسته‌ای را شامل می‌شود که پروتکل اینترنت (IP) و سرویس‌های مرتبط صدا و داده و چند رسانه‌ای را حمایت می‌کنند. همچنین، اینترنت به عنوان آشکارترین مثال از سوئیچ بسته‌ای است، شبکه سیگنالینگ کنترل‌کننده شبکه‌های PSTN نیز خود یک سیستم سوئیچ بسته‌ای است.

در بیشتر قسمت‌ها، تنوع منطقی و فیزیکی، به طور طبیعی بین این دو نوع از سرویس وجود دارد که تا حد زیادی به خاطر قابلیت تعامل فناوری است. بیشتر دستگاه‌ها، نرم‌افزارها، فرآیندها و زیرساخت‌های این سرویس‌ها متفاوت هستند. بسته‌ها نمی‌توانند به طور تصادفی یا عمدی در مدارها نشت کنند.

از نظر شبکه‌سازی، اگر یک واقعه امنیتی در یکی از این فناوری‌ها اتفاق بیفتد معمولاً اثری در دیگری نخواهد داشت. برای مثال؛ اگر یک کرم شبکه در اینترنت رها شود، همان طور که جامعه جهانی در چارچوب زمانی ۲۰۰۴-۲۰۰۳ به طور شدیدی تجربه کرده است، احتمال اینکه این مشکل روی سرویس‌های داده و صدای شبکه‌های سنتی تسهیم زمانی (TDM) اثر بگذارد، ناچیز است. چنین تنوع فناوری برای حفاظت از زیرساخت ملی استفاده قابل ملاحظه دارد؛ زیرا برای یک حمله مثل یک کرم بسیار مشکل‌تر می‌شود از فناوری‌هایی که به طور منطقی جدا هستند عبور نماید.

(به شکل ۴-۶ توجه کنید).

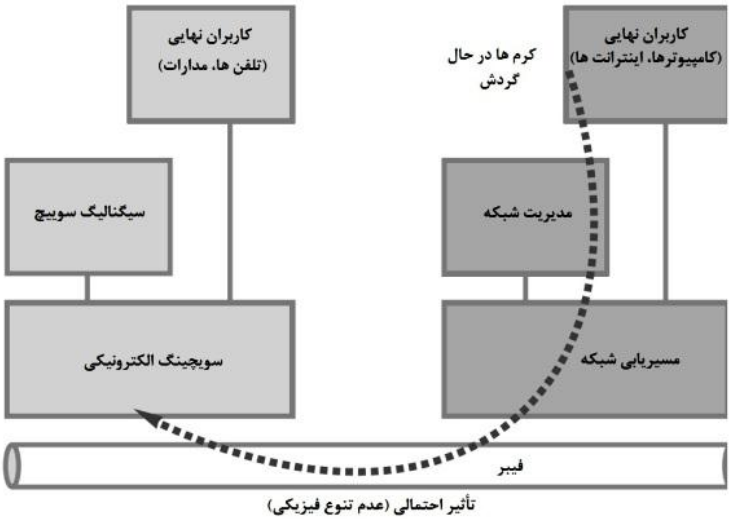


شکل ۴-۶- منفعت عدم انتشار کرم، ناشی از شبکه‌های مخابراتی متنوع

حتی با تنوع منطقی ذاتی در این فناوری‌های مختلف در نتیجه‌گیری باید دقت کرد. برای مثال؛ یک نگاه دقیق‌تر به مخابرات متنوع، این حقیقت را نشان میدهدکه

ممکن است از لایه‌های پایین‌تر شبکه انتقال به طور مشترک استفاده شود. برای مثال؛ بسیاری از شرکت‌های مخابراتی از شبکه فیبر نوری هم برای ارائه سرویس‌های سوئیچ مداری و هم برای سرویس‌های مبتنی بر IP استفاده می‌کنند. از آنجا که حامل‌های مختلف با استفاده از قانون حق راه، از مسیرهای یکسان برای مسیر سازی فیبر نوری استفاده می‌کنند، بسیاری از محل‌ها؛ مانند؛ تونل‌ها، پل‌ها و اتوبان‌های عمده برای نصب فیبر نوری مورد استفاده قرار می‌گیرد و در صورتی که یک فاجعه با یک حمله تروریستی هدفمند اتفاق بیفتد، می‌تواند روی شبکه‌هایی که برای کار با حامل‌های متنوع طراحی‌شده‌اند، تأثیر بگذارد.

شراکت در استفاده از فیبر نوری و مسیرهای با حق راه، از نظر پیاده‌سازی عملیاتی و هزینه معقول است ولی باید از شراکتی بودن زیرساخت آگاه بود؛ زیرا این اشتراکی بودن، الگوی تنوع را تغییر می‌دهد. اتکا بر یک راهبرد چند فروشنده‌ای، تنوع را پیچیده خواهد کرد و در ضمن، از نظر تئوری برای حملات مبتنی بر IP حملاتی را ممکن می‌سازد که تولید امتناع از سرویس گسترده (DDOS) می‌کنند که پیامدهای منفی روی انتقال‌هایی که مبتنی بر IP نیستند به خاطر حجم ترافیک ایجادشده توسط DDOS خواهد داشت. تا کنون، در محیط‌های فعلی چنین اتفاقی نیفتاده است، اما به علت اینکه از بیشتر شبکه‌های فیبر نوری به صورت اشتراکی استفاده می‌شود، باید به آن توجه کرد. (به شکل ۴-۷ توجه کنید).



شکل ۴-۷- توانایی بالقوه برای انتشار اثر ضربه در طول فیبری که به صورت مشترک از آن استفاده می‌شود

یک سناریوی محتمل‌تر این است که در یک فناوری سرویس ملی نظیر خدمات بی‌سیم 2G و 3G برای شهروندان و کسب‌وکار، می‌توان مشکلات امنیتی ناشی از حملات مبتنی بر سوئیچ بسته‌ای یا سوئیچ مداری را دید. برای مثال؛ از آنجا که یک زیرساخت بی‌سیم حامل معمولی، دارای هر دو هسته سوئیچ بسته‌ای و سوئیچ مداری است، حمله در هر کدام از این دو حوزه می‌تواند مشکلاتی را ایجاد کند. مرورگری اینترنت و پیغام‌رسانی چندرسانه‌ای می‌توانند در سیستم‌های سرور و دروازه‌های این نوع سرویس‌ها مورد حمله قرار گیرند. به طور مشابه، خدمات صوتی می‌تواند در مراکز سوئیچینگ موبایل که از این قابلیت حمایت می‌کنند، مورد حمله قرار گیرند. بنابراین، با اینکه اطمینان از درجه‌ای از تنوع در وابسته بودن این فناوری‌ها ممکن است یک هدف باشد، ممکن است رسیدن به این هدف، امکان‌پذیر نباشد.

از نظر حفاظت از زیرساخت ملی، بیشینه کردن تنوع به خفه کردن حملات با مقیاس وسیع کمک خواهد کرد، اما باید کل معماری و ساختار را از نزدیک بررسی کرد. در بسیاری از موارد، بررسی عمیق‌تر آشکار خواهد کرد که زیرساختی که به عنوان متنوع تبلیغ‌شده اجزایی دارد که متنوع نیستند؛ همیشه، در زیرساخت‌های غیر متنوع کاهش خطرات به اندازه کافی انجام نمی‌شود، طراحان باید برای بررسی و چک کردن وقت بگذارند. زمانی که این کار انجام شود، تنوع فناوری شبکه یک ابزار عالی برای کاهش خطر باقی می‌ماند. برای مثال؛ بسیاری از افسران امنیتی گزارش می‌دهند که خدمات صوتی سوئیچ مداری، معمولاً، در مقابل کرم‌ها، بات‌نت‌ها و ویروس‌های اینترنتی سلامت خود را حفظ می‌کنند.

۴-۵- تنوع فیزیکی

الزامات تنوع فیزیکی در طراحی زیرساخت محاسباتی شاید شناخته‌ترین آن‌ها در میان تمام مسائل مرتبط با تنوع باشد. همه سرمایه‌های محاسباتی یا شبکه‌ای که به عنوان یک جز ضروری یک عملکرد یا تابع حیاتی خدمت می‌کنند، باید توزیع فیزیکی داشته باشد باشند تا بتوانند زمان بقای خود را افزایش دهند. این رویکرد از مجامعی که بازیافت از فجایع را مدیریت می‌کنند، نشأت گرفته است و تأکید اولیه آن بر فجایع طبیعی نظیر طوفان‌ها و آتش‌سوزی بوده است. با رشد تهدیدات امنیتی، مدیران زیرساخت ارزش ارائه درجه‌ای از تنوع فیزیکی را دریافته‌اند. برای مثال؛ تنوع فیزیکی، متکی بودن تنها به یک شبکه توزیع برق را کاهش می‌دهد. این شبکه، هدف باارزشی برای حمله سایبری دشمن است. تنوع فیزیکی، همچنین، خطر حمله فیزیکی یا حمله به ساختمان را به علت وجود امکانات متعدد به میزان زیادی کاهش می‌دهد.

این مسائل و مشکلات بحث‌برانگیز نیستند. در حقیقت، برای سال‌های متمادی، پروژه‌های خرید و تدارکات برای سیستم‌های سرمایه‌های ملی در هر دو مورد دولت و

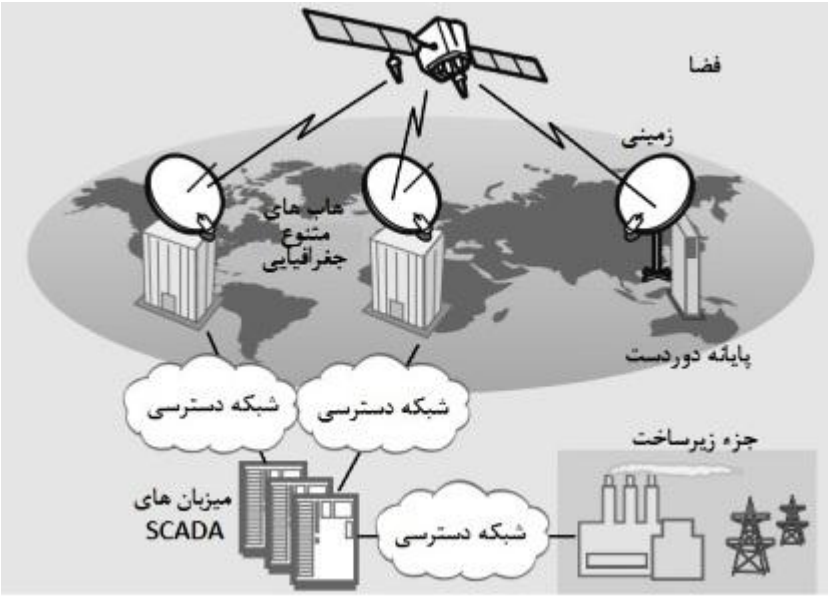
صنعت به طور معمول تقاضای مورد ملاحظه قرار گرفتن مشکلات تنوع فیزیکی زیر را داشته‌اند:

- تنوع مرکز پشتیبان: اگر هر مرکز عمده برای مدیریت سیستم، شبکه یا کاربرد در یک جز زیرساخت گنجانیده شود نیاز خواهد بود که یک مرکز پشتیبان را در یک محل متمایز فیزیکی دیگر مشخص کنیم. اگر این روش به طور مناسبی به کار گرفته شود، اطمینان از اینکه دو مرکز (اصلی و پشتیبان) در دو قسمت متفاوت شبکه باشند، ایجاد می‌شود و کمتر کسی با این رویکرد، بحث و جدال خواهد داشت.
- تنوع تأمین‌کننده یا فروشنده: بسیاری از سازمان‌ها، تأکید دارند که باید درجه‌ای از تنوع در ترکیب تأمین‌کنندگان و فروشندگان اجزا زیرساخت‌های حیاتی وجود داشته باشد و این باعث کاهش احتمال اینکه یک شرکت تأمین‌کننده تأثیر زیادی در تمامیت زیرساخت داشته باشد می‌گردد. در ضمن، احتمال مسائل آبشاری را که ممکن است با بعضی عناصر معمولی نظیر روتین‌های نرم‌افزاری و کتابخانه‌های جاسازی‌شده در سبد محصولات یک فروشنده مربوط باشند را کاهش می‌دهد.
- تنوع مسیر شبکه: زمانی که زیرساخت شبکه برای حمایت از زیرساخت ملی استقرار یافت، غیرمعمول نخواهد بود که از تأمین‌کننده یا تأمین‌کنندگان درجه‌ای از تنوع مسیر شبکه را درخواست کنیم. این موضوع به کاهش احتمال مسائل بدخواهانه‌ای که بر ارتباطات تأثیر می‌گذارند کمک خواهد کرد. همان طور که در بالا اشاره شد، استفاده مشترک از پل‌ها، تونل‌ها و اتوبان‌ها برای پیاده‌سازی محیط فیزیکی شبکه که از فروشندگان مختلف تهیه‌شده باشند، واقعی بودن تنوع مسیرها را پیچیده می‌کند.

دستیابی به تنوع فیزیکی از طریق خدمات داده ماهواره

یک مثال خوب از کاربردی که اصول تنوع فیزیکی را نشان می‌دهد، ارائه برخی از انواع سیستم‌های SCADA است که از IP روی ماهواره (IPOS) استفاده می‌نمایند؛ در جایی که ساخت شبکه‌های زمینی مشکل باشد، خدمات داده‌ای ماهواره به طور سنتی مزیت زیادی در توانایی عملکرد قوی از طریق امواج رادیویی در سراسر نقاط جهان را دارند. معمولاً، در چنین مناطقی پوشش بی‌سیم تجاری کمتر فراگیراست؛ یا حتی کاملاً در دسترس نیست. بعضی کاربردهای SCADA از این ویژگی قوی مخابراتی در سیستم‌های ماهواره‌ای به عنوان یک مزیت جهت ارتباط پایانه‌های کاربران دوردست با سیستم میزبان SCADA استفاده می‌نمایند، گرچه نیاز به درجه‌ای از تنوع هنوز باقی می‌ماند. همان‌طورکه قبلاً گفته شد بیشتر این تأکید بر تنوع با نگرانی‌های ناشی از فجایع طبیعی و فیزیکی مرتبط بوده است؛ ولی یک منفعت امنیت سایبری نیز به طور روشن وجود دارد.

معمولاً، برپا کردن سیستم‌های SCADA با ماهواره شامل کاربران انتهایی مرتبط است که از طریق IPOSبه مجموعه فیزیکی متنوعی از هاب‌ها متصل می‌شوند و این هاب‌ها به صورت گسترده‌ای به میزبان‌های SCADA وصل می‌گردند. دشمنی که بخواهد به این هاب‌ها حمله کند، باید از ابزارهای منطقی یا الکترونیکی استفاده نماید و به تلاش‌های زیاد تدارکاتی نیاز دارد، به خصوص اگر هاب‌ها در نقاط مختلفی در دنیا نصب‌شده باشند. برای مثال؛ شرکت هیوز در زمینه بازاریابی این نوع محیط‌ها برای مشتریان SCADA بسیار فعال بوده است. پیکربندی دسترسی از راه دور توصیه‌شده برای کنترل سیستم‌های SCADA متنوع در شکل ۴-۸ نشان داده شده است.



شکل ۴-۸- هاب‌های متنوع در پیکربندی ماهواره‌ای SCADA

مزایای هاب‌های متنوع آشکار است. اگر یکی از آن‌ها به طور مستقیم مورد حمله فیزیکی یا منطقی قرار گیرد و امنیت آن نقض شود، میزبان‌های SCADA هنوز به وسیله کاربران انتهایی قابل‌دسترسی خواهند بود. همچنین، حملات به اجزا زیرساخت‌های محلی که عملیات SCADA به آن وابسته است، مثل نیروی برق دارای اثر آبشاری نخواهند بود. چنین رویکردی، تنها زمانی مؤثر خواهد بود که تمام اجزا متنوع در یک سطح سرویس مشترک عمل نمایند. برای مثال، اگر یک ارائه‌دهنده سرویس، سرویس‌های امن، با قابلیت اتکا بالا یا سابقه انطباق با توافق سطح سرویس تبلیغ‌شده (SLA)، را پیشنهاد می‌نماید، ایده خوبی نخواهد بود که ارائه‌دهنده دیگر با انطباق SLA ضعیف را وارد نماییم؛ زیرا معقول نیست برای سیستمی که باکیفیت بالا عمل می‌کند برای تنوع یک رقیب سطح پایین با عملکرد ضعیف بسازیم. به‌هرحال، این

مفهوم عمومی تنوع رله باید بین کاربران و میزبان‌های حیاتی در داخل تمام سیستم‌های زیرساخت ملی تعبیه شود.

۴-۶- برنامه تنوع ملی

توسعه یک برنامه تنوع ملی به هماهنگی بین شرکت‌ها و آژانس‌های دولتی در موارد زیر نیاز دارد:

- تجزیه و تحلیل مسیر بحرانی: برای شناسایی برخی مسیرهای بحرانی، باید تجزیه و تحلیل اجزا زیرساخت ملی که برای سرویس‌های ضروری مورد نیاز است، انجام شود.
- برای مثال؛ اگر یک گروه نظامی، برای کامل کردن بعضی مأموریت‌های تدارکاتی به یک مسیر بحرانی متکی باشد، باید اطمینان یافت که این مسیر بحرانی به وسیله فروشندگان، تأمین‌کنندگان، تیم‌های حمایتی و فناوری حمایت می‌شود.
- مدل‌سازی آبشاری: برای شناسایی شرایط در اجزا زیرساخت ملی، به یک تجزیه و تحلیل مشابه نیاز است که در آن اثر آبشاری به علت وجود عدم تنوع امکان‌پذیر باشد. اگر تمام رایانه‌های شخصی یک سازمان پیکربندی یکسان داشته باشند، یک خطر جدی ایجاد خواهد شد. مسلماً، ممکن است سازمان پذیرش ریسک را انتخاب کند؛ اما این انتخاب باید صریحاً پس از بررسی امنیتی صورت گیرد.
- نظم و انضباط تدارکاتی: باید در انتخاب و خرید فناوری به وسیله سازمان‌های مسئول زیرساخت‌های حیاتی درجه‌ای از الزامات و نیازهای تنوع گنجانیده شود. این مسئله عموماً به صورت طبیعی در بیشتر سازمان‌های بزرگ اتفاق می‌افتد؛ بنابراین، ضرورت ممکن است شدید نباشد؛ اما منافع امنیتی در آن آشکار است.

تصمیم بین دو گزینه ارائه پاداش و مشوق برای تنوع، در مقابل یک رویکرد سخت‌گیرانه‌تر برای ارائه مدارک و شواهد به‌کارگیری درصدی از تنوع در هر سیستم، باید به کمک محیط و فرهنگ محلی گرفته شود. محیط تهدید در آرایش و تنظیمات ارتشی به طور قابل‌ملاحظه‌ای متفاوت از آن چیزی است که در ارتباطات و انتقال می‌توان یافت؛ بنابراین، محتاطانه خواهد بود که این تصمیم‌گیری‌ها به صورت محلی انجام شود.

فصل ۵: اشتراک

تنها سیستم امن واقعی، سیستمی است که خاموش شده باشد؛ در داخل بلوکی سیمانی در اتاقی پوشیده از سرب و مهر و موم شده با نگهبانان مسلح قرار داده شود و حتی پس از آن هم، من شک و تردیدهای خود را (در مورد امن بودن آن) خواهم داشت.

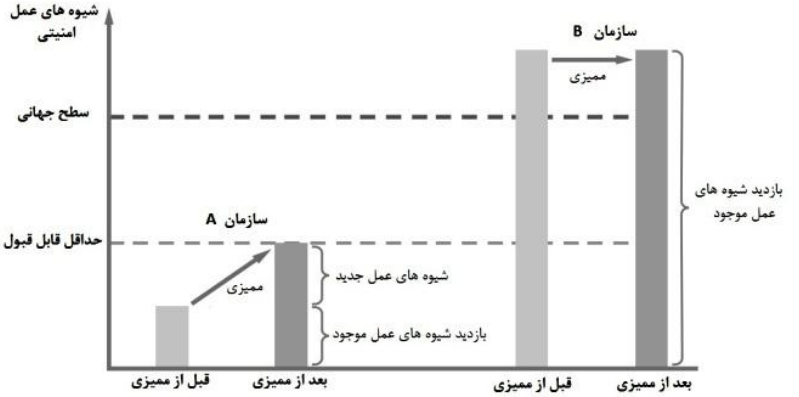
اوژن اسپافورد، مدیر اجرایی مرکز آموزش و تحقیقات در تضمین اطلاعات و امنیت (CERIAS) در دانشگاه Purdue.

ما پیشنهاد خود را در فصل پیش برای دارا بودن تنوع در سیستم‌های زیرساخت ملی مشخص کردیم. اکنون می‌توانیم در مورد یک نیاز به ظاهر متناقض دیگر در سیستم‌های زیرساخت بحث نماییم که نشان‌دهنده درجه‌ای از "اشتراک" است. به خصوص، برخی از ویژگی‌های امنیتی مطلوب در تمام زمینه‌های زیرساخت ملی برای تضمین حداکثر انعطاف‌پذیری در مقابل حمله سایبری باید موجود باشد. هر کسی که در حوزه امنیت کار کرده است، این جمله را می‌فهمد و احتمالاً، به صورت اصولی با آن موافق است. معمولاً، به مجموعه‌ای از ویژگی‌های امنیتی مطلوب به صورت جمعی به عنوان بهترین شیوه‌های عمل امنیتی گفته می‌شود. مثال؛ بهترین شیوه‌های عمل شامل موارد اسکن منظم سیستم‌ها، تست نفوذ از شبکه به طور منظم، برنامه‌های آگاه‌سازی امنیتی، بررسی مدیریت تمامیت و یکپارچگی در سرورها می‌تواند باشد.

زمانی که بهترین شیوه‌های عمل امنیتی شناسایی و اندازه پذیر شد، این شیوه‌های عمل می‌توانند پایه چیزی گردند که به عنوان استاندارد امنیتی شناخته می‌شود. یک استاندارد امنیتی، پایه و اساس فرایندی به نام ممیزی امنیتی است که در آن یک شخص سوم ناظر بی‌طرف بر اساس مدارک و شواهد، معین می‌کند که آیا الزامات

موجود در استاندارد رعایت شده است، یا خیر. مسئله کلیدی برای حفاظت از زیرساخت‌های ملی این است که بهترین شیوه‌های عمل، استانداردها و ممیزی، پایین‌ترین سطح مجاز امنیتی را برای تمام سازمان‌های مربوطه ایجاد کند.

(به شکل ۵-۱ توجه کنید).



شکل ۵-۱ ممیزی‌های امنیتی روشن و گویا برای دو سازمان

سازمان‌هایی که از نظر امنیتی زیر مینیمم سطح بهترین شیوه‌های عمل امنیتی قابل‌قبول قرار گیرند. ممیزی استانداردهای امنیتی برای آن‌ها شیوه‌های عمل جدیدی را علاوه بر بازبینی شیوه‌های عمل موجودشان پیدا می‌کند. اثر مطلوب این است که حالت قبل از ممیزی به حالت‌های بهبودیافته پس از ممیزی برای تمام شیوه‌های عمل انتقال یابد. همیشه، این اتفاق نخواهد افتاد، به خصوص برای سازمان‌هایی که محیط ضعیف برای ورود و معرفی شیوه‌های عمل جدید امنیتی دارند. ولی برای آن‌ها ورود به شیوه‌های عمل جدید می‌تواند یک هدف باشد. برای سازمان‌هایی که از قبل در سطح بالاتری ازمینیمم سطح قابل‌قبول و حتی با ویژگی‌هایی در سطح جهانی قرار دارند، ممیزی بندرت شیوه‌های عمل جدیدی را معرفی خواهد کرد، اما به جای آن شیوه‌های

عمل موجود بازبینی می‌شوند. اثر مطلوب این است که این شیوه‌های عمل به تدریج تقویت خواهند شد؛ اما این روش ممکن است، همیشه، به صورت کامل مؤثر نباشد.

به خصوص اگر ممیزها با ویژگی‌های امنیتی که امروزه در سطح جهانی برقرار است، کمتر آشنا باشند، برخی از استانداردهای متداول بهترین شیوه عمل مرتبط با امنیت را که می‌توان در محیط‌های زیرساخت ملی یافت، در ادامه آمده است.

استانداردهای بهترین شیوه‌های عمل متداول مرتبط با امنیت

- مدیریت امنیت اطلاعات فدرال (FISMA): FISMAاستانداردهای حداقلی بهترین شیوه‌های عمل امنیت را در محیط‌های دولت فدرال امریکا برقرار می‌کند. قانون اجرای آن را در سازمان‌های دولت فدرال اجباری کرده است و سالانه یک نمره حرفی را به هر آژانس دولت فدرال اختصاص می‌دهد.

  وزارت‌های دفاع، تجارت، کار، حمل‌ونقل، کشور، دارایی، امور سربازان قدیمی و کشاورزی؛ همین طور کمسیون تنظیم مقررات اتمی، در سال ۲۰۰۷، نمره F از FISMA گرفتند.
- قانون انتقال‌پذیری و پاسخگویی بیمه بهداشتی (HIPAA): عنوان پاراگراف II در HIPAA شامل استانداردهای توصیه‌شده برای کنترل‌های امنیت و حریم خصوصی در رسیدگی به اطلاعات مرتبط با سلامت شهروندان آمریکایی است. این استاندارد با قانون‌گذاری کنگره امریکا لازم‌الاجرا است.
- استاندارد امنیت داده‌های صنعت کارت‌های اعتباری (PCIDSS): این استاندارد توسط شورای امنیتی PCIکه شرکت‌های عمده کارت‌های اعتباری مثل Visa ® Card، Discover ® Card، AmericanExpress ® و

Master Card ®را در بر می‌گیرد، توسعه یافته است و الزاماتی برای رمزگذاری داده‌های حساس مشتریان دارد.

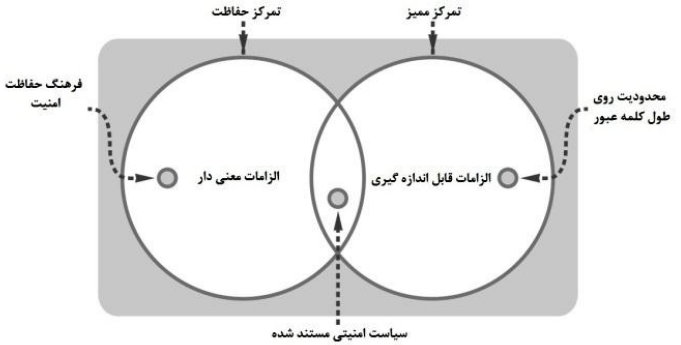
- استاندارد ISO/IEC27000(ISO27K): سازمان بین‌المللی استاندارد (ISO) و کمسیون بین‌المللی الکتروتکنیک یک استاندارد امنیتی بریتانیایی را که با کد BS-7799شناخته می‌شد، تکمیل کرده و به مجموعه شناخته‌شده‌ای از بهترین شیوه‌های عمل امنیتی قابل ممیزی تبدیل کردند. بعضی متخصصان امنیتی معتقدند که مجموعه استانداردهای امنیتی ISO27K جهانی‌ترین، مورد توافق‌ترین و بهترین شیوه‌های عمل امنیتی هستند.

تمام استانداردها، زیرمجموعه بزرگی از الزامات امنیتی و عملکردی هستند که به‌طور یکسان عمل می‌کنند. به عنوان مثال؛ هر کدام از استانداردها نیاز به سیاست‌ها و رویه‌های دقیقاً مستند شده، تأیید هویت و کنترل‌های تأیید هویت، سیستم‌های جمع‌آوری داده و رمزگذاری تعبیه‌شده در سیستم‌ها را دارند. هر استاندارد نیاز به نظارت مدیریت، نظارت‌های امنیتی جاری دارد، نمرات تطابق امنیتی که ممیزین معینی آن را صادر می‌کنند و اگر بهترین شیوه‌های عمل رعایت نشده باشد، مجازات‌ها و تنبیهات مالی به دنبال دارد.

با چنین افزونگی در استانداردهای امنیتی و رعایت کردن آن‌ها، می‌توان حدس زد که اصل اشتراک در حفاظت زیرساخت ملی رعایت شده است. برای مثال؛ ممکن است برخی از سازمان‌ها نیاز به نشان دادن رعایت ده‌ها استاندارد مختلف امنیتی داشته باشند. می‌توان انتظار داشت که چنین توجه شدید و متمرکزی در زمینه امنیت، منجر به یک رویکرد تا حد زیادی مشترک به امنیت در سراسر جهان شود. متأسفانه، اعتقاد بر این است که با وجود ممیزی قابل‌توجه و رعایت کردن استانداردها در سراسر جهان، بیشتر این فعالیت‌ها به نوعی از اشتراک امنیتی که تفاوت مثبتی برای حفاظت

زیرساخت‌های ملی ایجاد کند، نمی‌پردازند. در عوض این فعالیت‌ها تمایل دارند بر روی نیازهایی تمرکز کنند که باارزش هستند؛ اما حیاتی‌ترین مسایل را دربر نمی‌گیرند. در حقیقت، بیشتر این شیوه‌های عملی که در طبقه‌بندی فناوری‌های روز امنیتی موجودند، بسیار بالاتر از سطوح مینیمم که در بیشتر ممیزی‌ها به آن‌ها اشاره می‌شود، قرار دارند.

مشکل ممیزی از تفاوت‌های ذاتی بین بهترین شیوه‌های عمل امنیتی معنی‌دار و قابل اندازه‌گیری نشأت می‌گیرد مانند این لطیفه قدیمی که مردی به دنبال پول گمشده‌اش در تقاطع خیابان‌های چهل و دوم و هشتم می‌گشت. عابری از او می‌پرسد: "آیا پول خود را در این نقطه گم کرده‌ای؟ مرد نگاهی کرده و می‌گوید: پول در تقاطع خیابان‌های چهل و یک و دهم گمشده؛ ولی چون اینجا روشن‌تر است، اینجا را می‌گردم". ممیزی امنیتی بهترین شیوه‌های عمل، معمولاً، نظیر لطیفه بالا است. تنها شیوه‌های عملی که می‌توانند ممیزی شوند؛ آن‌هایی هستند که در آن‌ها روشنایی خوب است و معیارهای قابل اندازه‌گیری را می‌توان برقرار کرد؛ ولی چنین معیارهایی، همیشه، معنی‌دار نیستند. (به شکل ۵-۲ توجه کنید).



شکل ۵-۲- رابطه بین نیازهای معنی‌دار و قابل اندازه‌گیری

مثالی از الزامات که در شکل ۵-۲ نشان داده شده است، اشاره به انواعی از نیازها دارد که احتمالاً، در هر طبقه‌بندی گنجانده می‌شوند. می‌توان به راحتی نیاز قابل

اندازه‌گیری را روی کلمه عبور تحمیل کرد؛ گرچه، معمولاً، این محدودیت کمتر مفید است و قابل اندازه‌گیری است؛ اما معنی‌دار نیست. در مقابل، می‌توان موجود بودن فرهنگ قوی امنیتی را در یک محیط بسیار مهم دانست؛ در صورتی که آن فرهنگ معنی‌دار باشد؛ اما اندازه‌گیری آن تقریباً غیرممکن است. سیاست امنیتی نیز وجود دارد که می‌تواند هم معنی‌دار و هم قابل اندازه‌گیری باشد و نشان می‌دهد که بعضی از الزامات در هر دو طبقه از قرار می‌گیرند.

۵-۱- بهترین شیوه‌های عمل معنی‌دار برای حفاظت از زیرساخت

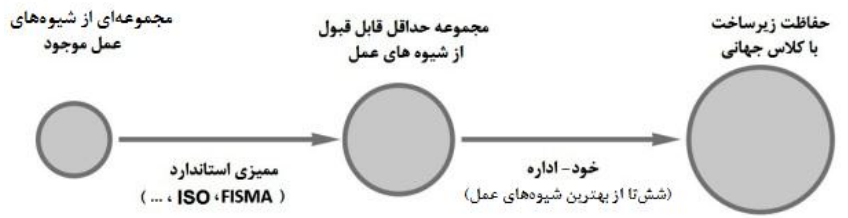
توانایی ممیزی بهترین شیوه‌های عمل، تأثیر آن‌ها را در مفید بودن در حفاظت از زیرساخت معین نمی‌کند و این یک پیامد تحریک‌آمیز است. در حقیقت، انگیزه اصلی برای حفاظت مناسب از زیرساخت نباید نمره ممیزی به دست آمده باشد، بلکه انگیزه باید مبتنی بر موفقیت و اقتصاد باشد. واقعیت این است که اگر شرکت‌ها، آژانس‌ها و گروه‌های با مسئولیت حفاظت از زیرساخت از بهترین توصیه‌های در دسترس برای بهترین شیوه‌های عمل امنیتی پیروی نکنند، شکست خواهند خورد. متأسفانه، بهترین توصیه‌ها از استانداردهای امنیتی و مجامع ممیزی نمی‌آید، بلکه از تجربه‌های عملی نشأت می‌گیرد.

اگر با این نظر موافق نیستید، لطفاً در نظر بگیرید که برای چند دهه استانداردهای امنیتی به وسیله گروه‌های قوی و معتبر حمایت‌شده‌اند. همچنین، ممیزین امنیتی باده‌ها سال تجربه، تجزیه و تحلیل‌های سختی را انجام داده و نمرات عدم موفقیت و شکست ناراحت‌کننده‌ای را برای تیم‌های امنیتی در سراسر جهان صادر نموده‌اند. برای مثال؛ در اشاره قبلی به FISMA نمرات ردی برای آژانس‌های مهم و برجسته دولتی در ایالات‌متحده امریکا ارائه دادیم. در دهه‌های گذشته با وجود تمام فعالیت‌ها و گزارش‌ها، تغییر مهمی در روش‌های امن کردن سیستم‌های کامپیوتری و شبکه‌ها و سیستم‌ها

انجام نشده است. در حقیقت، می‌توان ادعا کرد که امروزه، زیرساخت‌های ملی نسبت به حملات آسیب‌پذیرتر از بیست سال گذشته هستند؛ بنابراین، چطور می‌توان تصور کرد که استانداردهای دقیق‌تر امنیتی و فرایندهای ممیزی می‌توانند این روند را تغییر دهند؟

بر اساس تجربه نویسنده این کتاب که مدیریت امنیتی اجزا عمده زیرساخت‌های حیاتی را برای سال‌های طولانی تجربه کرده است جواب سئوال فوق در یک متدولوژی دو مرحله‌ای قرار دارد.

- گام اول ممیزی استاندارد: قدم اول معمولی و مطابق رویه مرسوم است و در آن توصیه می‌شود که هر سازمان برای اطمینان از اینکه هیچ گروهی زیر آستانه مینیمم قابل‌قبول عمل نکند، تحت یک ممیزی استاندارد واقع شود. بسیاری از سازمان‌ها ادعا می‌کنند که این مرحله در حال انجام است، اما هدف به دست آوردن یک نمره مطلوب به جای رد شدن است. بنابراین، حتی اگر یک شرکت یا آژانس تحت یک ممیزی در حال انجام است، باید نمره قبولی را در ممیزی کسب کند. هر کدام از استانداردهای ممیزی عمده که در بالا ذکر شدند، احتمالاً قابل‌قبول است و همه آن‌ها ما را به سمت شیوه‌های عمل مینیمم یکسانی هدایت می‌کنند.
- گام دوم تمرکز در سطح جهانی: مرحله دوم شامل تمرکز شدیدتر روی مجموعه‌ای از شیوه‌های عمل معنی‌دار حفاظت از زیرساخت ملی است. این شیوه‌های عمل بیشتر از تجربه گرفته‌شده‌اند. آن‌ها با مطالب موجود در این کتاب سازگار هستند و فقط در قسمت‌هایی از بیشتر استانداردهای ممیزی امنیتی موجود، وجود دارند. بزرگ‌ترین موفقیت از اداره کردن این تمرکز جدید در سازمان نشأت می‌گیرد؛ زیرا اندازه‌گیری و ممیزی این شیوه‌های عمل آسان نیست. (به شکل ۵-۳ توجه کنید).



شکل ۵-۳- متدولوژی رسیدن به شیوه‌های عمل حفاظت از زیرساخت در سطح جهانی

برای گام اول مسئله مهم این است که صدمه ممیزی بیشتر از منافعش نباشد. برای مثال؛ فرض کنید به یک مدیر سیستم لایق و قابل‌اعتماد مسئولیت یک دسته از کارها در جزیی از زیرساخت واگذار شده باشد و او در طول مدت طولانی مسئولیت بدون هیچ مشکلی نتایج عالی امنیتی را کسب کند. این یک حالت عادی است، به‌خصوص در شرکت‌ها و آژانس‌هایی که مدیریت سیستم را جدی می‌گیرند. متأسفانه، یک ممیز امنیتی به چنین ترتیبات مدیریتی با وحشت نگاه می‌کند و آن را نقض آشکار حداقل امتیاز و تفکیک وظایف و چیزهای شبیه به این می‌پندارد.

در ایالات‌متحده آمریکا، اگر قسمتی که مدیریت می‌شود، یک واحد مالی در یک شرکت بخش عمومی باشد. نقض قانون Sarbanes-Oxley در مورد الزام تفکیک وظایف خواهد بود. ممیز، معمولاً، نیاز دارد که یک مدیر لایق با فرآیندی دیوان‌سالار که تیمی از پرسنل بالقوه پایین‌تر است جانشین شود که هر کدام فقط قسمتی از کل کار را می‌بینند. در این صورت، مشکل نخواهد بود که اجزا ضعیف‌تر مدیریت شده و کمتر امن باشند. این بدترین حالت در ممیزی است و نباید از آن در حفاظت از زیرساخت ملی استفاده کرد.

در گام دوم؛ بهترین شیوه‌های عمل معنی‌دار مخصوص آورده شده است که برای حفاظت از زیرساخت ملی جمعاً شش مورد می‌شود. این شش مورد بهترین شیوه‌های عمل با فرآیندهای ممیزی فعلی و استانداردها در تناقض نیستند؛ اما قطعاً برای ممیزی

آسان کاربردها طراحی نشده‌اند و برای مثال ارزیابی اینکه چیزی "مناسب" است یا "ساده" مشکل می‌باشد. با این حال، توصیه اکید ما دقت در اطمینان از اشتراک در سراسر زیرساخت است. با این شش شیوه عمل منافع قابل‌ملاحظه‌ای به دست خواهد آمد.

شش مورد از بهترین شیوه‌های عمل برای حفاظت از زیرساخت ملی

- شیوه عمل ۱. سیاست امنیتی مناسب و مرتبط با محل: هر سازمانی که مسئولیت طراحی یا عملیات زیرساخت ملی به او محول شده باشد، باید سیاست امنیتی داشته باشد که برای محیط و مأموریت سازمان مناسب باشد. بنابراین، باید از سازمان‌های مختلف انتظار سیاست‌های امنیتی متفاوتی را داشت. خوشبختانه، نیاز به سیاست امنیتی تا حد زیادی با بیشتر استانداردها سازگار است و یکی از شیوه‌های عملی آسان است که باید درک شود.
- شیوه عمل ۲. فرهنگ‌سازمانی حفاظت از امنیت: سازمان‌هایی که مسئولیت زیرساخت ملی به آن‌ها محول شده است، باید فرهنگ حفاظت از امنیت را توسعه و پرورش دهند. این فرهنگ باید در سازمان نفوذ کرده و شایع شود؛ همچنین، باید مشوق‌های بزرگ برای رفتار مثبت و نتایج وخیم برای رفتار منفی داشته باشند. امروزه، هیچ استاندارد امنیتی متقاضی توجه فرهنگی به امنیت نیست؛ زیرا نمی‌توان آن را اندازه‌گیری کرد.
- شیوه عمل ۳. تعهد به ساده‌سازی زیرساخت: به علت اینکه پیچیدگی علت اولیه مشکلات امنیتی در بیشتر محیط‌های با مقیاس وسیع است، تعهد به ساده‌سازی زیرساخت برای اطمینان از امنیت مناسب حیاتی است؛ تعیین آنچه "ساده سازی" معنی می‌دهد، یک مفهوم ذهنی و محلی

است که به ویژگی‌های محیط مورد هدف بستگی دارد. امروزه، هیچ استاندارد امنیتی تقاضای ساده‌سازی زیرساخت را نمی‌کند.

- شیوه عمل ۴. اعطای گواهینامه و برنامه‌های آموزشی برای تصمیم سازان: باید یک برنامه آموزش امنیتی و اعطای گواهینامه حرفه‌ای برای تصمیم سازان و کسانی که مسئولیت پیاده‌سازی زیرساخت ملی به آن‌ها محول شده است، وجود داشته باشد. در حالت مطلوب، این برنامه نباید کاربران انتهایی را شامل شود؛ چون احتمال پوشش مناسب را به شدت کاهش می‌دهد.
- شیوه عمل ۵. مسیر شغلی و ساختار پاداش برای تیم‌های امنیتی: کسانی که متصدی امنیت در محیط‌های زیرساخت ملی هستند، باید مسیرهای شغلی روشن و پاداش‌های مناسب در مسیر حرفه‌ای خود داشته باشند. در صورت عدم وجود این پاداش‌ها، کارهای مهم امنیتی به وسیله افرادی که تربیت‌نشده‌اند یا دارای انگیزه ضعیف هستند، انجام خواهد شد. این نیاز، معمولاً در سازمان‌های بزرگ‌تر معنی‌دارتر خواهد بود.
- شیوه عمل ۶. شواهد شیوه‌های عمل امنیتی مسئولانه گذشته: همان‌گونه که بسیاری از صنعتگران دوره‌های کارآموزی را برای فراگیری و نشان دادن مهارت‌های مناسب می‌گذرانند، سازمان‌ها نیز باید دوره‌ای را بگذرانند تا پیش از اینکه مسئولیت حفاظت از زیرساخت ملی به آن‌ها محول شود، مهارت‌های مناسب را کسب کنند. تعجب‌آور است که ممیزی‌های امنیتی موجود، معمولاً، شامل بررسی دقیق شیوه‌های عمل امنیتی گذشته در مقابله با حملات سایبری زنده نیستند.

خوانندگانی که با استانداردها و ممیزی آشنا هستند، فوراً چالش‌هایی با مفاهیم ذهنی را که در پاراگراف قبلی معرفی شدند، خواهند شناخت. تنها راهی که می‌تواند به طور مناسب به کار گرفته شود این است که مدیران امنیتی منظور و قصد نیازها را درک

کنند و سپس، صادقانه برنامه حمایتی را به طور خود اداره‌ای انجام دهند. این برای اطمینان شخص ثالث بهینه نیست، اما تنها راه معقولی است که می‌توان با آن به بهترین شیوه‌های عمل امنیتی در کلاس جهانی رسید.

۵-۲- سیاست امنیتی مناسب و مرتبط محلی

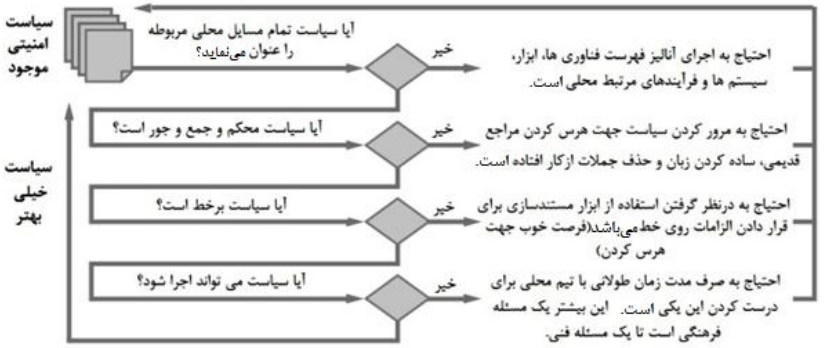
هر سازمان تجاری یا دولتی که اکنون مشغول توسعه و مدیریت زیرساخت ملی است، قبلاً نوعی سیاست امنیتی داشته است. بنابراین، طرح این سئوال که آیا یک سیاست امنیتی باید، توسعه یابد بی‌مورد است؛ هر سازمان برای خود یک سیاست امنیتی دارد. در عوض سئوال واقعی برای بیشتر سازمان‌هایی که نقشی در زیرساخت ملی دارند، این است که چگونه سیاست‌های خود را برای محیط محلی مناسب و مرتبط سازند. به خصوص چهار نوع از ملاحظات پایه‌ای سیاست امنیتی برای حفاظت زیرساخت ملی توصیه می‌شود.

- قابلیت اجرا: نوشتن بیشتر سیاست‌های امنیتی آسان است؛ ولی اجرای آن‌ها آسان نیست بنابراین، سازمان‌ها باید زمان زیادی صرف مسئله قابل‌اجرا بودن سیاست امنیتی کنند. محیط تهدید محلی باید در نظر گرفته شود؛ زیرا کارمندان برخی از شرکت‌ها و آژانس‌ها نسبت به افراد دیگر بیشتر متمایل به پیروی کردن از قوانین و سیاست‌های امنیتی هستند. با این حال یک سیاست وقتی باارزش است که اجرا شود بنابراین؛ هر سازمان باید بتواند راهبرد اجرا کردن سیاست‌های خود را به طور صریح بیان کند.
- کوچک‌سازی: بیشتر سیاست‌های امنیتی بیش از حد بزرگ و پیچیده هستند. اگر یک تمرین برای تیم زیرساخت ملی سالم‌ترین تمرین باشد، همانا رفتن و مرور داخل زبان سیاست امنیتی موجود و هرس کردن

مراجع قدیمی، جملات از رده خارج و منسوخ و مثال‌های کهنه است. نباید از سیاست‌های امنیتی بیش از حد بزرگ و پیچیده با جزییات زیاد استفاده شود. یک مسئله کلیدی، جهتی است که سیاست امنیتی به آن سو می‌رود؛ یعنی یا راکد است و یا در حال بزرگ‌تر شدن و پیچیده‌تر شدن (ناسالم)؛ یا اینکه در حال کوچک‌تر و فشرده‌تر شدن است. (سالم).

- بر خط بودن: زبان سیاست برای اینکه واقعاً در محیط‌های زیرساخت ملی مفید باشد، باید بر خط و بی‌درنگ و قابل جستجو باشد. تیم‌ها باید بتوانند الزامات مربوطه را به آسانی بیابند و جملات مربوطه را بریده و به داخل مستندات و مدارک پروژه و فرایند خود بچسبانند. از زمان چاپ و توزیع سیاست‌های امنیتی با جلدهای فانتزی مدت‌ها گذشته است.
- فراگیر بودن: سیاست امنیتی باید تمام عناصر محاسباتی و شبکه‌ای را در محیط زیرساخت ملی محلی در بر گیرد که تنها با تجزیه و تحلیل می‌تواند مشخص شود. متأسفانه، این تجزیه و تحلیل می‌تواند تا اندازه‌ای وقت‌گیر و کند باشد. بی‌دقتی باعث به وجود آمدن یک سیاست بسیار پیچیده می‌گردد. برای نوشتن سیاست فراگیری که بیش از حد پیچیده نباشد، مهارت قابل‌ملاحظه‌ای لازم است.

این چهار نیاز سیاست امنیتی برای گروه‌هایی که مسئولیت زیرساخت ملی به آن‌ها محول شده است، می‌تواند تحت یک تجزیه و تحلیل ساده تصمیم‌گیری قرار گیرد که به مشخص کردن اینکه سیاست امنیتی محلی مرتبط و مناسب برای مأموریت سازمان می‌باشد، کمک می‌کند؛ این فرآیند تصمیم سازی در شکل ۵-۴ نشان داده شده است.



شکل ۵-۴- فرآیند تصمیم برای تجزیه و تحلیل سیاست امنیتی

گفتنی است، همان طور که در فصل بعد خواهیم دید، فرهنگ محیط محلی می‌تواند روی توسعه سیاست امنیتی اثر داشته باشد. در محیطی که تغییر فناوری چندان چشمگیر نیست و مهارت‌های عملیاتی به بلوغ رسیده‌اند؛ مثل؛ تلفن سوئیچ مداری سنتی، زبان سیاست می‌تواند کمتر به جزییات بپردازد و برای شناسایی رویه‌های غیرمنتظره‌ای به کار رود که ممکن است برای امنیت لازم باشند.

در محیطی که تغییر فناوری چشمگیر است و مهارت‌های عملیاتی به طور دائم در حال تغییر هستند؛ مثل؛ تلفن بی‌سیم، ممکن است زبان سیاست خاص تر هم باشد. در هر حالت، مسئله این نیست که آیا سیاست بعضی عناصر مورد نیاز را دارد یا نه؟ سیاست باید از نظر محلی مرتبط و مناسب باشد.

۵-۳- فرهنگ حفاظت از امنیت

دومین شیوه عمل معمول توصیه‌شده ما ایجاد فرهنگ‌سازمانی حفاظت از امنیت است. زمانی که یک سازمان فرهنگ حفاظت از امنیت را داشته باشد، به دو دلیل، توان بالقوه برای بهره‌برداری بدخواهانه از آسیب‌پذیری‌ها به میزان زیادی کاهش می‌یابد:

اول: احتمال اینکه خود آسیب‌پذیری موجود باشد، کاهش می‌یابد؛ زیرا سعی و کوشش برای تصمیم‌گیری امن‌تر افزایش می‌یابد.

دوم: مراقبت و هوشیاری بی‌درنگ و زمان واقعی در یک چنین فرهنگی از سواستفاده از آسیب‌پذیری‌ها جلوگیری خواهد کرد. بارها هوشیاری انسان در یک فرهنگ امنیتی، مؤثر بودن خود را در کمک به جلوگیری از حملات بدخواهانه نشان داده است.

(خوانندگان به خاطر می‌آورند که تنها اقدامات مؤثر امنیتی که در ۱۱سپتامبر ۲۰۰۱ انجام شد، آن‌هایی بودند که به وسیله انسان‌ها آغاز شدند).

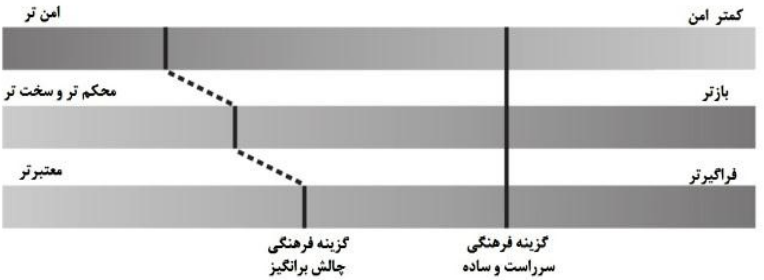
برای مشخص کردن اینکه یک سازمان فرهنگ حفاظت از امنیت دارد؛ به امکانات محلی سازمان بروید و با دقت بررسی کنید که از ورود غیرمجاز به ساختمان‌ها چگونه پاسداری می‌شود. اگر از یک در الکترونیکی برای تأیید هویت ورود استفاده می‌شد و پشت آن یک نگهبان هر بازدیده کننده‌ای را با چشم بررسی می‌کرد، در آن صورت، احتمال اینکه فرهنگ حفاظت از امنیت وجود داشته باشد، خیلی زیاد است. ولی اگر شخص مقابل شما، در را باز نگه دارد، برای اینکه شما بدون اینکه به خود زحمت نشان دادن کارت معتبر ورودی خود را بدهید وارد شوند یا بدتر اینکه در باز نگه داشته شده باشد، فرهنگ حاکم فرهنگ باز است. یک فرهنگ امنیتی، قطعاً، دلالت بر اینکه همه چیز کاملاً امن است، نمی‌کند، اما وجود چنین فرهنگی در حفاظت از سرمایه‌های ملی ضروری است.

متأسفانه، بسیاری از ما تمایل به یکسان تصور کردن فرهنگ‌سازمانی امنیت با یک محیط سخت و خشن، اقتدارگرا پارانویید و شاید حتی نظامی داریم. همچنین، یک فرهنگ امنیتی، معمولاً، مدیرانی دارد که از ریسک کردن دوری می‌کنند و از رسانه‌ها فاصله می‌گیرند، دسترسی ارتباطی از راه دور را دوست ندارند و با فناوری‌های جدید مثل شبکه‌های اجتماعی راحت نیستند. برای مثال؛ می‌توان یک محیط بدون فرهنگ امنیتی را با یک محیط جوان، پویا، خلاق، باز و تساوی گرا، یکسان در نظر گرفت. در

چنین فرهنگی، مدیران، معمولاً، با ریسک کردن راحت هستند، در صحبت کردن در مورد کارشان با خارجی‌ها باز هستند؛ عاشق فناوری‌های جدید هستند و از ارتباطات راه دور حمایت می‌کنند.

واقعیت این است که هیچ‌کدام از دو کلیشه فوق دقیق نیست؛ بلکه چالش در ارتقا فرهنگ امنیت عبارت از ترکیب بهترین عناصر هر کدام از دو رویکرد مدیریت بدون استفاده از ضعف‌های آن‌ها است. هدف، پرورش ویژگی‌های مثبت محیطی است، طوری که از سرمایه‌های ملی به نحو بارزی حفاظت شود. یعنی، هر محیط محلی باید راهی برای انطباق ویژگی‌های خود با آنچه در مأموریتشان به آن اشاره‌شده، داشته باشد. برای مثال؛ هیچ گروهی مایل نیست که از آن‌ها به عنوان گروهی بسته و پارانویید یاد شود. اما ممکن است یک گروه اطلاعاتی نظامی گزینه دیگری نداشته باشد. همین طور هیچ گروهی نمی‌خواهد به عنوان بی بند و بار در امنیت به آن‌ها اشاره شود. اما برخی سازمان‌های خلاق نظیر برخی دانشگاه‌ها و کالج‌ها این تصمیم را به صراحت و روشنی اتخاذ کرده‌اند.

به این ترتیب، سازمان‌ها باید برای توسعه فرهنگ مناسب خود طیفی از گزینه‌ها را در نظر بگیرند. این طیف نشان می‌دهد رابطه‌ای معکوس بین استحکام سازمانی و امنیت وجود دارد. همین‌طورآسان است هر چیزی را سخت بگیریم و امیدوار باشیم که فرهنگ افزایش امنیت توسعه خواهد یافت. با این حال، چالش در شکستن این رابطه است که اجازه دادن به انجام فعالیت‌های باز و خلاقی که در همان حال در آن‌ها نقض امنیتی انجام نشود، امکان‌پذیر باشد؛ در برخی زمینه‌ها، محیط امن‌تر و در دیگر موارد کمتر امن می‌شود. چنین هدف فرهنگی ترکیب‌شده‌ای را باید به عنوان نیاز مشترک برای کلیه گروه‌های درگیر در سرمایه‌های ملی در نظر گرفت (به شکل ۵-۵ توجه کنید).



شکل ۵-۵- طیف گزینه‌های امنیتی فرهنگ‌سازمانی

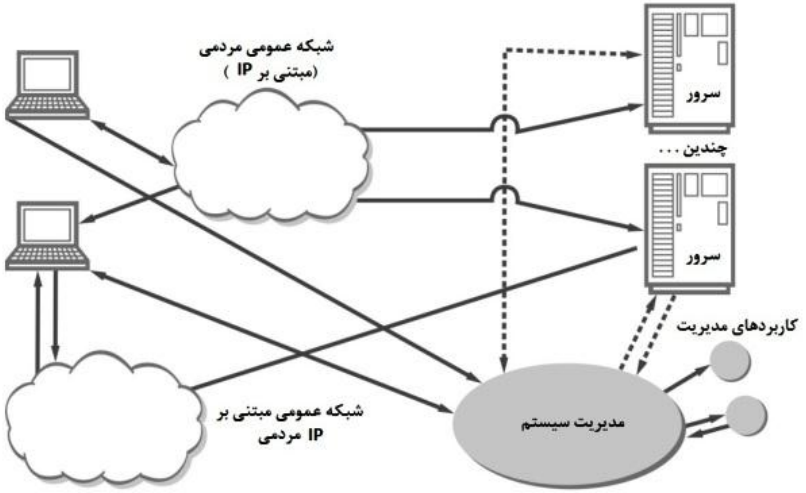
بنابراین، سئوال واضحی که ممکن است از دیدگاه حفاظت از زیرساخت ملی پرسیده شود، این است که چرا به بالاترین سطح فرهنگ امنیتی در تمام موارد، بدون توجه به اهداف فرهنگی نظیر باز بودن، خلاق بودن و موافق تعامل عمومی بودن، نیاز نیست؟ به عنوان مثال؛ ارتش ایالات‌متحده امریکا، ممکن است نمونه‌ای از سطح سخت فرهنگی تعهد به امنیت را نشان دهد. همان طور که در بالا بحث شد، یک پاسخ این است که لزوم برقرار کردن یک فرهنگ در سازمان کاری مشکل است. ممکن است جنبه‌های خاصی از فرهنگ؛ نظیر؛ سیاست قوی، اجرای سخت و ... مورد نیاز باشد؛ اما به وجود یک فرهنگ آسان نیاز است. با این حال، برخی استانداردهای امنیتی برای زیرساخت ملی مورد نیاز است، استانداردهایی که تنها می‌توانند در محیط‌هایی رعایت شوند که فرهنگ حفاظت امنیتی در آن‌ها موجود است. این کار، وضعیت ناراحت‌کننده‌ای را می‌طلبد که در آن مدیران محلی باید صادقانه برای ایجاد فرهنگ مناسب کار کنند و در برخی موارد، ممکن است به چند دهه از توجه احتیاج داشته باشند.

یک عنصر مهم از فرهنگ امنیتی، نمادگرایی است که مدیریت می‌تواند با رفتار خود آن را ایجاد کند. هنگامی که به مدیران ارشد اجازه عبورهایی داده می‌شود که نقض سیاست‌های امنیتی است، این یک خطای جدی است؛ زیرا اهداف فرهنگی را

تضعیف می‌کند. متأسفانه، ارشدترین مدیران همیشه، از کارمندان امنیتی ارشدتر هستند و در این شیوه عمل معافیت مدیران ارشد متداول است. شاید عمده درخواست‌های زیرساخت ملی از سازمان‌ها شامل سئوالاتی در مورد شیوه عمل مدیران ارشد آن‌ها باشد، پیش از اینکه قراردادهایی جهت اجرا به آن سازمان‌ها واگذار شود. ممکن است به تیم‌های امنیتی سلاح بیشتری برای متوقف ساختن این معافیت‌ها بدهد.

۵-۴- ساده‌سازی زیرساخت

سومین شیوه عمل مشترک که توصیه می‌کنیم؛ تعهد صریح سازمان به ساده‌سازی زیرساخت است. از نظر ما، برای ساده‌سازی در زمینه زیرساخت، باید از زبان ذهنی استفاده کرد. زیرساخت ساده‌تر فهمش آسان‌تر، کمتر دست و پاگیر و کارآمدی بیشتری دارد. به این ترتیب، اندازه‌گیری ابتکارات ساده‌سازی ذهنی و موضوعی، با استفاده از متریک‌های کمی خیلی مشکل‌تر خواهد بود. برای نشان دادن فرآیند ساده‌سازی، نگاهی به نوعی شما تیک درهم‌ریخته مهندسی می‌اندازیم که ممکن است از آن برای توصیف زیرساخت شبکه استفاده شود. نمودار در شکل ۵-۶ نشان داده شده است و از مدارک طراحی تعبیه‌شده در یک پروژه زیرساخت گرفته‌شده که اخیراً، نویسنده کتاب درگیر آن بوده است.



شکل ۵-۶- نمونه نمودار مهندسی به‌هم‌ریخته

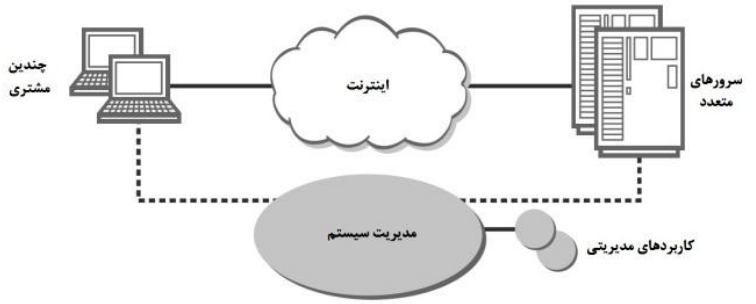
این دیاگرام از انواع مسائلی رنج می‌برد که در طراحی و عملیات زیرساخت ملی می‌توان یافت.

- عدم عمومیت: سیستم‌های موجود در دیاگرام به حالتی عمومی مشاهده نمی‌شوند. به جای اینکه یک جز را تعمیم داده و برای نشان کل اجزا یکسان به کار ببریم، یک چیز چندین بار در مکان‌های متفاوت در دیاگرام نشان داده شده است؛ برای مثال سرور.
- مبهم کردن چیزهای آشکار: واسط‌های موجود در دیاگرام به صورت واضح نشان داده نشده‌اند. خطوط در سراسر شکل پخش‌شده‌اند و واسط‌های ساده مبهم شده‌اند تا از آنچه که عملاً یک اتصال آشکار است، جلوگیری کنند.
- جریانی از طراحی آگاهانه: دیاگرام محصول اولین پیش‌نویس جریان فکری آگاهانه بوده و طرحی نیست که به دقت برنامه‌ریزی‌شده باشد.

اغلب زیرساخت‌ها بدون اینکه کسی برای بررسی و تجدیدنظر روی آن‌ها وقت بگذارد، در اولین پیش‌نویس قرار می‌گیرند.

- عدم یکنواختی: به اشیا به طور یکنواخت اشاره نشده است، ارجاعات به یک شبکه مبتنی بر IP، مختصری متفاوت هستند و در حقیقت، باید به اینترنت ارجاع داده شود.

اگر مقداری ساده‌سازی منطقی در طراحی نمودار درهم‌ریخته نشان داده‌شده در بالا، همراه با دقت برای هر عنصری که ذکر شد، به کار ببریم، محصول معادل عملکردی حاصل، فهمش بسیار آسان‌تر می‌شود. نمودار بهبودیافته‌تر نیاز به بازگشت به عقب و تأیید این را دارد که واقعاً همان عملکرد را بیان می‌کند. در حقیقت، نمودار جدید همان کار را انجام می‌دهد. (به شکل ۵-۷ توجه کنید).



شکل ۵-۷- نمودار مهندسی ساده‌شده

تجزیه و تحلیل اینکه چگونه یک نمودار به‌هم‌ریخته را ساده کرده و تبدیل به چیزی کنیم که به آسانی قابل‌درک باشد، برخی از تکنیک‌هایی را برجسته می‌کند که می‌تواند برای ساده‌سازی محیط یک جز زیرساخت ملی مفید باشد.

چگونه می‌توان محیط یک زیرساخت ملی پیچیده را ساده نمود

- کاهش اندازه: نمودار دوم کوچک‌تر از نمودار اول است. ارتباط این عمل به زیرساخت ملی باید آشکار باشد. ساده‌سازی باید شامل کاهش اندازه باشد. کد کمتر، واسط‌های کمتر، عملکرد کاهش‌یافته، همگی اهداف ساده‌سازی سالمی هستند که به طور قطعی امنیت را بهبود می‌بخشند. در حقیقت، یک نیاز زیرساخت ملی باید ارائه مدارک و شواهد قابل نشان دادنی باشد، از حذف نرم‌افزارها یا ابتکاراتی که کاهش را باعث می‌شوند. تنها قطعه امن واقعی، کدی است که حذف کرده‌اید.
- تعمیم مفاهیم: نمودار دوم، مفاهیم را نسبت به نمودار اول، به طور مؤثرتری، تعمیم می‌دهد، این موضوع باید در زیرساخت ملی نیز درست باشد. به جای مدیریت ده‌ها، صدها و هزاران حالت خاص، مؤثرتر است که یک راهبرد تعمیم برنامه‌ریزی‌شده داشته باشیم که اجازه مدیریت ساده‌تری را می‌دهد. بدیهی است که این موضوع نیاز به تعادل و توازن با نیازهای تنوع محلی دارد.
- واسط‌های تمیزتر: شاید آشکارترین اختلاف بین دو نمودار این باشد که نمودار دوم نمایش تمیزتری از واسط‌ها را ارائه می‌دهد. از آنجا که زیرساخت ملی واسط‌های پیچیده‌ای بین سیستم‌ها دارد، باید ابتکاراتی برای ساده‌سازی این واسط‌ها موجود باشد تا موجب امنیت بهینه سرمایه‌های ملی شود.
- برجسته کردن و تأکید بر الگوها: دیاگرام دوم، الگوهای عملکردی و جریان داده را به طوری آشکار نشان می‌دهد و باعث می‌گردد هر تغییری که ممکن است در معماری و ساختار داده شود، ساده گردد. زیرساخت

باید به نحوی طراحی شود که الگوهای مهم در پردازش یا داده‌ها را برجسته نماید.

- کاهش درهم ریختگی: نمودار اول تا آنجا که می‌شود تصور کرد درهم‌ریخته است که این، معمولاً، نشان‌دهنده جریانی از فرآیند طراحی آگاهانه است. اغلب مواقع، زیرساخت ملی نیز همین طور تحول می‌یابد. اول یک سیستم در جای خود قرار می‌گیرد و سپس، یکی دیگر؛ سپس، آن‌ها به چیزهای دیگر وصل می‌شوند و فرآیند ادامه می‌یابد. نتیجه از نظر امنیتی بهینه نیست.

اگر فرآیند ممیزی این اهداف ذهنی و موضوعی رام شدنی نباشد، چالش آور است. اما این موضوع اهمیت تلاش برای رسیدن به هر هدف در زیرساخت ملی را کاهش نمی‌دهد. می‌توان استدلال کرد که ساده‌سازی زیرساخت در حقیقت تنها هدف مهم در حفاظت از سرمایه‌های ملی است. روشن است که مدیران امنیتی روح خویشاوندی با بیشتر مدیران فناوری اطلاعات پیدا خواهند کرد. البته یک مدیر ارشد اطلاعاتی به ندرت می‌داند که چگونه ساده‌سازی و کاهش زیرساخت را مدیریت کند. یک نشانه خوب از اینکه یک سازمان محلی در حال تلاش برای ساده‌سازی است این است که در حال انجام ابتکارات متمرکزی برای کاهش یا حذف کاربردهای نرم‌افزاری باشد.

۵-۵- صدور گواهینامه و آموزش

چهارمین شیوه عمل مشترک توصیه‌شده، برنامه‌های آموزش و صدور گواهینامه برای تصمیم گیران کلیدی است. در حال حاضر بیشتر ابتکارات آموزش‌های امنیتی کامپیوتر تمایل به تمرکز تدریس آگاهی به کاربران انتهایی در مورد انتخاب مناسب کلمه عبور، ذخیره‌سازی داده‌ها، به‌کارگیری و رفتار با دستگاه‌ها و ... دارند. این طرح‌های آگاهی رسانی از این اعتقاد مشترک ناشی می‌شود که سیستم‌های رایانه‌ای و شبکه‌ای اگر کاربران انتهایی وقت بگذارند و یاد بگیرند و قوانین سیاست‌های امنیتی را پیروی

کنند، باید به طور کامل امن شوند. وضعیت یادآور پزشکانی است که بیماران خود را به خاطر بیماری‌شان سرزنش می‌کنند.

ممیزین امنیتی عموماً با نظر مسئول بودن کاربران انتهایی موافق‌اند و اغلب، بررسی‌های نقطه‌ای را در محیط‌های هدف انجام می‌دهند. این بررسی‌های نقطه‌ای شامل امتحانات کوتاهی از افراد تصادفی در مورد دانش و تفسیر آن‌ها از سیاست امنیتی محلی است. وقتی درصد بالایی از افراد، به علت ندانستن بعضی قواعد امنیتی، نمره بدی می‌گیرند، تیم‌های امنیتی مجبور می‌شوند که برنامه آگاهی رسانی را با نصب پوستر، نمایش ویدیو، تست‌های اجباری و حتی مجازات هایی برای نادانی کاربر انتهایی بیشتر کنند.

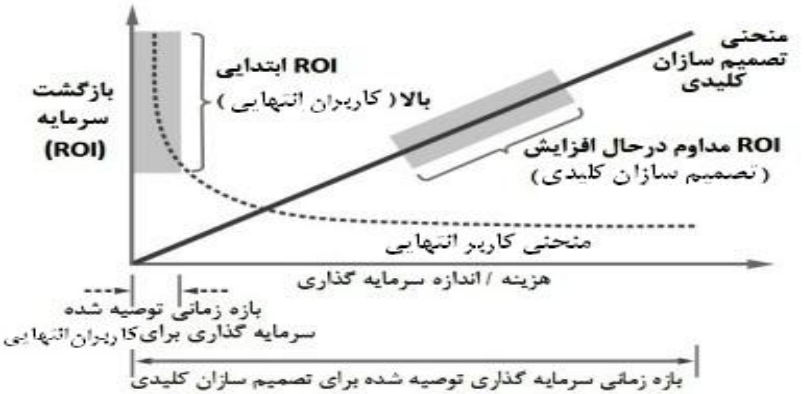
بر اساس چند دهه تجربه در اجرای این نوع ممیزی‌ها، حمایت آن‌ها و همچنین، در معرض این ممیزی‌ها قرار گرفتن، نتیجه‌ای که اینجا گرفته می‌شود این است که کاربران انتهایی، هرگز، به آگاهی صد درصدی امنیتی نمی‌رسند. آموزش امنیتی برای کاربران انتهایی ضرری ندارد؛ زیرا هر کسی باید از خطرات هر عملی که انجام می‌دهد و می‌تواند در محیط محلی باعث صدمه امنیتی شود، آگاه باشد. برای مثال؛ اگر اطلاعات با مالکیت اختصاصی در اختیار کاربران نهایی قرار بگیرد، آن‌ها باید بفهمند که اگر این اطلاعات را در اختیار افراد غیرمجاز قرار دهند، برایشان پیامدهایی خواهد داشت.

یک هدف عملی‌تر برای حفاظت از زیرساخت ملی، تمرکز بر بهبود صلاحیت و لیاقت امنیتی تصمیم سازان به جای کاربران انتهایی است. تمایز اینجا زیرکانه و اساسی است. تصمیم سازان کلیدی در محیط‌های زیرساخت ملی افراد زیر هستند:

- مدیران ارشد: افرادی هستند که ارجحیت‌های عملیاتی و مالی را برقرار می‌کنند که بر زیرساخت ملی اثر می‌گذارد. آن‌ها ارشدترین مدیران در یک سازمان یا افرادی با بالاترین درجه در ارتش هستند.

- طراحان و توسعه‌دهندگان: طراحان شبکه، سیستم و کاربردها، توسعه‌دهندگانی هستند که معین می‌کنند چه ویژگی‌های امنیتی و عملکردی در سیستم باید موجود باشد تا مردم از آن‌ها استفاده کنند آن‌ها، معمولاً، در گروه فناوری اطلاعات کار می‌کنند.
- مدیران: مدیران سیستم و شبکه هستند که وظایف روزبه‌روز نگهداری و فعال بودن سیستمی را که مردم از آن استفاده می‌کنند، به عهده‌دارند. در بسیاری از موارد، این افراد آموزش‌های کمی دیده‌اند و کمتر از معمول حقوق می‌گیرند.
- اعضای تیم امنیت: این کارکنان امنیتی، مسئولیت سیستم‌های سازمانی را به عهده‌دارند که حفاظت از سرمایه‌ها را انجام می‌دهند. تعداد فزاینده‌ای از سازمان‌ها، زمینه‌هایی از این کار را برون سپاری می‌کنند. تا زمانی که ترتیبات به خوبی مدیریت شده و هماهنگ باشند، هیچ ایرادی به این کار نیست.

این چهار نوع تصمیم سازان کلیدی، افرادی هستند که می‌توانند تفاوت اساسی در امنیت یک سازمان ایجاد کنند و برای آن‌ها پوشش صد درصدی، هدفی آسان است. ضرری ندارد که اندازه جمعیت تصمیم سازان کلیدی در یک شرکت خیلی کمتر از کل افراد سازمان باشد و آن‌ها باید به بهترین وجه آموزش‌دیده باشند و اهمیت امنیت را بفهمند. از چشم‌انداز سرمایه‌گذاری، بازده سرمایه‌گذاری روی آموزش برای کاربران انتهایی و تصمیم سازان کاملاً متفاوت به نظر می‌رسد. (به شکل ۵-۸ توجه کنید).



شکل ۵-۸- گرایش‌های بازده سرمایه‌گذاری (ROI) برای آموزش امنیت

پیامی که در منحنی‌های ROI در شکل ۵-۸ نشان داده شده است، این است که سرمایه‌گذاری ابتدایی مختصری در اخذ گواهینامه امنیتی و آموزش کاربران انتهایی تولید بازدهی ابتدایی معقولی می‌نماید؛ ولی این بازدهی به سرعت تقلیل می‌یابد؛ زیرا در یک محیط معمولی این بیشترین کاری است که یک کاربر انتهایی می‌تواند انجام دهد. در حقیقت، در محیط‌های با بهترین طراحی، وظیفه کاربران انتهایی برای گرفتن تصمیمات امنیتی خودمختارانه مینیمم شده است. برای تصمیم سازان کلیدی، ROI مداوم، به طور ثابت، در چرخه عمر سرمایه‌گذاری در حال افزایش است. برخلاف کاربران انتهایی، تصمیم سازان کلیدی می‌توانند به طور مداوم دانش امنیتی افزایش‌یافته خود را به طور معنی‌دار و مقیاس‌پذیر در زیرساخت به کاربرند.

به طور مختصر، توصیه می‌کنیم که از یک رویکرد دو قسمتی برای گواهی امنیتی و آموزش در محیط زیرساخت ملی استفاده کنید.

- تصمیم سازان کلیدی: تمرکز روی ارائه مداوم برنامه‌هایی برای اخذ گواهی امنیتی و آموزش به تصمیم سازان کلیدی است. با تمرکز روی

تصمیم سازان کلیدی، بازدهی سرمایه سازگار، روبه افزایش و مقیاس‌پذیر خواهد بود.

- کاربران انتهایی: ایجاد فعالیت‌های کم هزینه و با بازدهی بالا برای گواهی دادن و آموزش مکمل کاربران انتهایی. سیستم‌ها باید طوری طراحی شوند که تصمیماتی را که کاربران انتهایی برای امنیت می‌گیرند، مینیمم گردانند.

صدور گواهی‌های خاص و برنامه‌های آموزشی برای یک محیط باید به طور محلی تعین شود و به طور مناسبی بکار گرفته شود. ایجاد یا یافتن برنامه‌های بالا، سخت نیست؛ اما اگر بدون دقت برنامه‌ریزی شود، به طور غلط بکار گرفته خواهند شد. گواهی‌های امنیتی معروف نظیر متخصصان امنیت سیستم‌های اطلاعاتی گواهی شده (CISSP) برای مدیران سیستم و شبکه بسیار عالی هستند؛ اما برای کاربران انتهایی ضرورتی ندارند به طریقی مشابه، برنامه‌های آگاهی رسانی برای انتخاب کلمه‌های عبور خوب برای کاربران انتهایی خوب است، اما فقط مدیران سیستم را ناراحت می‌کند.

۵-۶- مسیر شغلی و ساختار پاداش

پنجمین شیوه عمل مشترک توصیه‌شده ما شامل ایجاد و استقرار مسیرهای شغلی و ساختارهای پاداش برای افراد حرفه‌ای در زمینه امنیت است. تعجب‌آور نیست که سازمان‌هایی که مسئولیت زیرساخت ملی به آن‌ها محول شده است، باید برای کارمندان امنیتی خود فرم مشترکی از مسیر شغلی و ساختار پاداش را مشخص کنند. این مسئله مخصوصاً مهم است؛ زیرا برای انجام وظایف امنیتی به طور مناسب، درجه‌ای از سابقه کار و طول عمر لازم است. بیشتر مواقع، کارهای مهم امنیت سایبری را کارمندانی انجام می‌دهند که در حرفه امنیتی تازه‌کار هستند و حقوق مناسبی برای کارشان دریافت نمی‌کنند.

رفع این مشکل ممکن است واضح باشد، اما هیچ استاندارد امنیتی برای ممیزی آن در نظر گرفته نشده است. عناصری که به طور معمول باید در محیط زیرساخت ملی موجود باشند؛ شامل موارد زیر است:

حقوق‌های جذاب: سازمان‌های زیرساختی باید ساختار حقوقی را نشان دهند که مهارت‌های مخصوصی را که در ارتباط با امنیت سایبری می‌باشد در آن در نظر گرفته شده باشد. حقوق‌ها باید بالاتر از میانگین در صنعت باشد، متریکی که می‌تواند به طور کمی ممیزی شود. (تعجب‌آور است که من، هرگز، ممیزی حقوق کارمندان امنیتی را به عنوان قسمتی از تلاش فراوان ممیزها ندیده‌ام).

مسیرهای شغلی: برای پیشرفت شغلی، ارتقا و افزایش حقوق، باید فرصت‌هایی در سازمان‌های زیرساخت موجود باشد. شاید بیشتر از هر زمینه دیگر مرتبط با شبکه و فناوری اطلاعات مهندسان امنیتی زیرساخت ملی نیازمند سال‌ها تجربه هستند تا بتوانند تصمیم‌گیری‌ها و قضاوت‌های مناسبی را اتخاذ کنند. اگر به مشکلات شغلی آن‌ها توجه نشود، احتمال اینکه سازمان بهترین نیروهای امنیتی را حفظ کند، کم خواهد بود.

مدیران ارشد: برای مدیران ارشد در سازمان‌های زیرساخت بسیار مطلوب و مناسب است که سهمی در مجامع امنیتی داشته باشند. این قطعاً به تصمیم‌گیری در سطوح بالا کمک می‌کند؛ اما مهم‌تر از آن، نشانه‌ای برای کارمندان امنیتی خواهد بود که رسیدن به سطوح بالای مدیریت از طریق بخش امنیت نیز قابل‌دسترسی است.

این ویژگی‌های سازمانی مرتبط با شغل بندرت در زمینه اینکه امنیت مناسبی در سازمان استقرار دارد بحث می‌کند. ممیزین هیچ‌گاه در مورد این مسائل بحث نمی‌کنند. این مایه تأسف است؛ زیرا حقوق خوب و مسیر شغلی برای کارمندان امنیتی ارتباط بیشتری با وضعیت امنیتی کلی یک سازمان دارند تا جزییات بی‌اهمیتی از قبیل طول کلمه عبور، طول فاصله زمانی بین دو تلاش ورود ناموفق به سیستم و دیگر چیزهایی که معمولاً در استانداردهای امنیتی یافت می‌شوند.

این نکته نیز گفتنی است که شرکت‌ها و آژانس‌ها نباید به جذب و استخدام افرادی اقدام کنند که در شکستن قوانین مربوط به رایانه‌ها و شبکه‌ها سابقه‌دارند. هک کردن، در تجسم ابتدایی خود یادگرفتن و به اشتراک گذاشتن بود. زمانی که هکرها این دیدگاه را نشان می‌دهند، می‌توان آن‌ها را جذب سازمان کرد تا مولد باشند. مسیر شغلی و پاداش برای این افراد به ندرت ارتقا و پول است، بلکه دسترسی روز به بیشترین و آخرین نوع فناوری‌ها می‌باشد.

۵-۷- سابقه شیوه عمل امنیتی مسئولانه

ششمین شیوه عمل مشترک که به شما توصیه می‌کنیم، شامل دو عمل مخصوص است:

اول: هر شرکت یا آژانسی که برای زیرساخت ملی کار می‌کند، باید شیوه عمل گذشته خود در حوادث زنده امنیتی را نشان دهد.

دوم: شرکت‌ها و آژانس‌ها باید جهت مدیریت بایگانی حوادث زنده، شامل پایگاه داده‌ای از فاکتورهای کلیدی، علل ریشه‌ای و آموزش‌های امنیتی از وقایع، کار بهتری انجام دهند.

این دو عمل به ظاهر واضح، هرگز، به طور صریح انجام نمی‌شوند و بیشتر شرکت‌ها و آژانس‌ها حتی مستندات رسمی حوادث امنیتی گذشته را نگاه نمی‌دارند.

خوشبختانه، اکثر درخواست‌ها برای کارهای پروژه‌ای زیرساخت ملی، الزاماتی را شامل می‌شود که شیوه‌های عمل مهندسی پروژه‌های قبلی را که برای بهبود مسائل امنیتی خواهد بود نشان دهند. زمانی که یک آژانس حکومت فدرال برای کار فنی و مهندسی قراردادی می‌بندد، در قسمت‌هایی از قرارداد، اطلاعاتی در مورد پروژه‌های قبلی، فعالیت‌های مشابه و فهرست مشتریان مرجع در خواست شده است. این شیوه عمل مناسب و باارزش است، گرچه ممکن است بیشتر به عنوان نوعی کلی از کار جمع‌آوری اطلاعات تلقی شود.

امروزه این شیوه عمل برای امنیت از درخواست‌هایی برای اطلاعاتی در مورد سیاست‌های امنیتی، عناصر ساختار امنیتی و حتی تکنیک‌های خاص مثل رمزگذاری استفاده می‌کند. چنین درخواست‌هایی مهم هستند و برای پروژه حفاظت از زیرساخت ملی باید در نظر گرفته شوند. در چنین تحقیقاتی به اندازه کافی وارد جزییات نمی‌شوند. مخصوصاً هر سازمانی که درخواستی در مورد زیرساخت ملی دارد، باید مدارکی از شیوه‌های عمل گذشته‌اش، در موارد زیر، ارائه دهد:

- سوابق آسیب: سازمان باید بتواند مدارک و شواهدی از حوادث امنیتی در گذشته را ارائه کند که باعث صدمات بدخواهانه واقعی به برخی سرمایه‌های باارزش شده است. ممکن است ارائه این مدارک منطقی به نظر نرسد. اما در واقع، هیچ سازمانی نمی‌تواند بدون اینکه درگذشته با حوادث واقعی سروکار داشته باشد، ادعا کند که در امن ساختن زیرساخت‌های عظیم مهارت دارد. گروه‌هایی که آماده ارائه توضیحات این حوادث گذشته هستند، معمولاً، در فرآیندهای امنیتی فعلی خود بلوغ بیشتری دارند.
- جلوگیری از حوادث در گذشته (پیشگیری): به طور مشابه؛ سازمان باید بتواند شواهدی ارائه دهد که از حوادث جلوگیری کرده است. این کار سخت‌تر از آن است که بتوان فکرش را کرد؛ زیرا در بسیاری از موارد حفاظت‌های امنیتی دارای اثر جلوگیری کننده هستند که به راحتی قابل مشخص کردن و اندازه‌گیری نیستند. بنابراین، تنها سازمان‌های امنیتی واقعاً ماهر می‌توانند شواهد یک عمل عمدی را که باعث جلوگیری از موفقیت حمله شده است، ارائه نمایند. استقرار یک فیلتر شبکه بی‌درنگ خیلی جلوتر از یک حمله DDOS، می‌توان مثال خوبی باشد. اگر از فیلتر کردن برای متوقف کردن تلاش برای حمله استفاده شود، این نشان‌دهنده قضاوت عالی درباره ارجحیت‌های سازمان در مورد امنیت می‌باشد.

- پاسخ در گذشته: رایج‌ترین جز تجربه امنیتی است که گروه‌ها می‌توانند به عمل واکنشی خود اشاره کنند که در هنگام حملات از طریق کرم‌ها، ویروس‌ها و دیگر حملات از آن‌ها بهره برده‌اند.

این الزامات باید در هر درخواست پروژه رسمی در نظر گرفته شود و به آن‌ها ارجحیت‌های بالایی اختصاص یابد. الزامات کمی می‌توانند به طور مناسبی توانایی یک سازمان را برای مقابله با شرایط امنیتی در آینده، نظیر؛ تجربه آن‌ها در مقابله با شرایط مشابه درگذشته، برجسته نماید.

۵-۸- برنامه اشتراک ملی

چالش در ایجاد یک برنامه ملی جدید برای مطمئن شدن از اشتراک با شیوه‌های عمل امنیتی مطابق با آخرین فناوری‌های روز در حفاظت از زیرساخت ملی، شامل چند نگرانی مختلف متعادل‌کننده زیر است:

- مجموعه‌هایی از استانداردهای موجود: بیشتر سازمان‌ها از تعداد زیادی استانداردها و ممیزی‌هایی که باید پوشش دهند، ناامید هستند. پیامد این است که از ایجاد یک استاندارد امنیتی ملی جدید که متناسب با شش شیوه عملی باشد که در این فصل توضیح داده شد، به خوبی استقبال نخواهد شد.
- لبه پایینی در مقابله لبه بالایی (کلاس جهانی): همان طور که قبلاً بحث شد، استانداردهای امنیتی فعلی و ممیزی‌های موجود بیشتر متمرکز بر ایجاد یک لبه پایینی مشترک امنیت به جای فشار آوردن برای رسیدن به کلاس جهانی وضعیت امنیت هستند.
- هیئت امنا و کمیسیون‌های موجود: این عرصه از پیش با کمیسیون‌های ملی، گروه‌های کاری و هیئت‌های امنایی که از رهبران تجاری و دولتی

تشکیل‌شده‌اند، پر شده است. این گروه‌ها برای ایجاد مجموعه‌ای از توصیه‌ها برای امنیت زیرساخت کار می‌کنند. بعید به نظر می‌رسد که آن‌ها از بین بروند و در هر برنامه پیاده‌سازی باید نقش آن‌ها در نظر گرفته شود.

با اینکه این‌ها ممکن است استانداردهای رسمی با فرآیندهای ممیزی مرتبط با خود نباشند. سازمان‌هایی که در این رابطه تحت تأثیر قرار می‌گیرند، ممکن است فشار مرور و بررسی این کارها را احساس کنند تا بتوانند درجه‌ای از پذیرش را نشان دهند حتی اگر با آن‌ها انطباق نداشته باشند. راه حل ایجاد توازن میان این نگرانی‌ها، در رویکردهای مختلف پیاده‌سازی و اشاراتی قراردادکه مبتنی بر تجارب قبلی با چند استاندارد و الزامات آن‌ها؛ نظیر؛ کتاب‌های زرد، کتاب‌های قرمز و سری امنیتی "Security Rainbow series" در سال ۱۹۸۰ است. در مرحله اول، دولت‌ها باید یک استاندارد تنها را برای تمام ممیزی‌های امنیتی دولتی و تجاری بپذیرند. تا زمانی که این تنها یک استاندارد باشد، مهم نیست که کدام یک از استانداردهای ممیزی انتخاب شده باشد. تمام درخواست‌های بعدی دولتی و قراردادها باید تقاضای انطباق با این استاندارد را داشته باشند. موجودیت‌های تجاری نیز ممکن است به تدریج نسبت به این استاندارد میل نمایند.

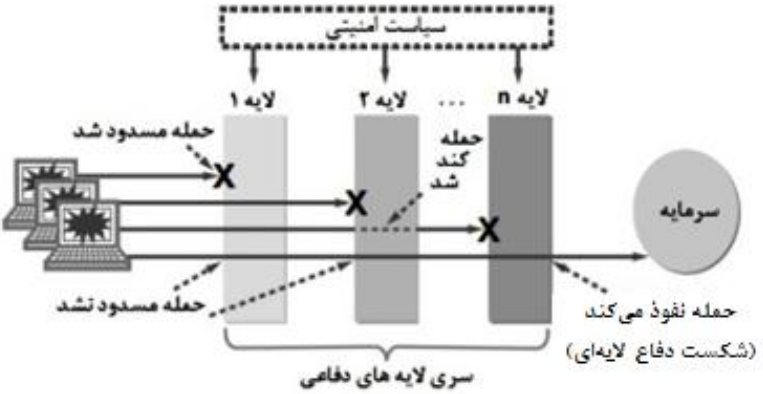
دوم: شیوه‌های عمل در سطح جهانی که در اینجا توضیح داده شد، باید در تمام درخواست‌های دولتی و قراردادها به عنوان نیازهای عملکردی با شرکت‌ها و آژانس‌ها تعبیه شود؛ این باعث جلوگیری از مسائل انطباق ممیزی شده و اجزا امنیتی را به طبقه‌بندی عملکردی در راستای عملکرد، قدرت پردازشی، قدرت ذخیره‌سازی و شبکه‌ای خود سوق خواهد داد. آژانس‌های دولتی می‌توانند با دادن پاداش و ارائه مشوق‌ها برای گنجانیدن این شرایط در معاملات خصوصی بین شرکت‌ها، مکمل این عمل باشند.

فصل ٦: عمق

استراتژی امنیتی عمومی دفاع در عمق بر اساس مشاهداتی است که هر لایه حفاظتی در هر زمان می‌تواند شکسته شود. لذا، دفاع در عمق شامل قرار دادن چندین لایه دفاعی برای بالا بردن احتمال این است که حمله متوقف یا حداقل کند شود. این احتمال وابسته به کیفیت و ویژگی‌های نسبی لایه‌های مختلف دفاعی می‌باشد. مسائل هزینه و تجربه کاربر انتهایی، محدودیت‌هایی در مورد اینکه لایه‌های مختلف چقدر در عمل قوی باشند ایجاد می‌کند. بیشتر کارشناسان امنیتی راهبرد دفاع در عمق را می‌شناسند، اما متأسفانه شواهدی بر استفاده از آن در محیط‌های زیرساخت ملی وجود ندارد. این خیلی بد است؛ زیرا حفاظت از زیرساخت ملی به طور طبیعی به چندین لایه از دفاع نیاز دارد.

شمای کلی مرتبط با لایه‌های دفاعی عبارت از مجموعه‌ای از عناصر حفاظتی است که بین سرمایه و دشمن قرارگرفته‌اند. واضح است که این آرایش دفاعی زمانی بهترین خواهد بود که عناصر دفاعی به صورت سری باشند و برای دسترسی به منبع حفاظت‌شده، باید به طور موفقیت‌آمیزی از کلیه عناصر دفاعی عبور کرد. با این حال، بیشتر مواقع لایه‌بندی چندان کارآمد نیست و ممکن است دارای ترکیبات و آرایش‌های مختلفی از عناصر دفاعی بین سرمایه و دشمن باشد. در چنین مواقعی، اهداف راهبردی باید کشف و حذف مسیرهای دسترسی تک لایه‌ای به سرمایه‌ها باشد و بدیهی است که باید از حالاتی که لایه‌ها در تناقض با یکدیگر هستند، اجتناب شود. برای زیرساخت ملی، هدف، قرار دادن چند لایه امنیتی در مقابل سرویس‌ها ضروری است.

(به شکل ۶-۱ توجه کنید).



شکل ۶-۱- شمای عمومی دفاع در عمق

منظور امنیتی برای هر سری از لایه‌ها، اجرای سیاست‌های امنیتی در تمام مسیرهای دسترسی ممکن به سرمایه‌های هدف است؛ بنابراین، اگر هر سرمایه تنها از طریق یک نقطه ورودی قابل‌دسترسی باشد، لایه‌ها نیاز به اجرای سیاست در همان نقطه ورودی را دارند. اگر سرمایه به طور گسترده‌ای از نقاط ورودی مختلفی قابل‌دسترسی باشد، دفاع لایه‌ای نیاز به اجرای سیاست در تمام این نقاط دارد. اگر تمام لایه‌ها تلاش حمله به سرمایه حفاظت‌شده را متوقف یا به اندازه کافی تضعیف ننمایند، روش‌های دفاع در عمق شکست‌خورده و باعث نقض امنیتی به وسیله دشمن شده است. زمانی که یک حمله کشف می‌شود، نسبتاً آسان است که مشخص کنیم یک شکست دفاعی اتفاق افتاده است؛ با این حال، زمانی که یک حمله بدون توجه ادامه می‌یابد یا هنگامی‌که تجزیه و تحلیل ادله و شواهد بعد از یک حمله نمی‌تواند نقطه بهره‌برداری شده توسط حمله‌کننده را مشخص کند، ممکن است سوراخ‌های لایه‌های دفاعی به طور نامحدودی باقی بمانند.

گاهی اوقات، کاربران مورد اعتماد و کارمندان داخلی شرکت یا آژانس یا شرکا، پیاده‌سازی‌های دفاع در عمق را به طور نامناسب یا حتی بدخواهانه‌ای دور می‌زنند. به عنوان مثال؛ یک سازمان زیرساخت برای اطمینان از اینکه نفوذگران نتوانند سرمایه‌اش را از محیط خارجی نظیر اینترنت مورد نقض امنیتی قرار دهند، ممکن است لایه‌های مختلفی از قابلیت‌های امنیتی ایجاد کند. با این حال، اگر کارمندان داخلی بدخواه بتوانند به طور مستقیم بر سرمایه دسترسی یابند، می‌توانند باعث نقض امنیتی شوند و در این صورت، مشکلاتی به وجود خواهد آمد. برای اطمینان از اینکه دفاع در عمق واقعاً سرمایه‌ها را احاطه کرده است، باید دقت، نظم و انضباط شدیدی در داخل سازمان و در ارتباط با خارج از طریق اینترنت ایجاد شود. برای حفاظت از سرمایه‌ها در مقابل عناصر خودی احتیاج به کنترل‌های عملکردی اضافی در شبکه محلی سازمان است.

در برخی مواقع، راهبردهای دفاع در عمق شامل مفهوم آشنای ارتشی ایجاد یک لایه حفاظتی کند کننده نفوذگر می‌باشد. معلوم شده است که جلوی ورودی را گرفتن قیاس مناسبی برای امنیت سایبری نیست. روش‌های امنیت سایبری تمایل به باینری بودن در عملکرد خوددارند، یعنی حفاظت یا کار خواهد کرد یا خیر. در مورد اینکه یک رویکرد چه مدت حمله‌کنندگان را معطل خواهد کرد، بحث‌هایی وجود دارد. مثل انتخاب این است که طول کلید رمزنگاری تا چه مدتی می‌تواند اثر خود را داشته باشد و معتبر باقی بماند. به طور مشابه، معمولاً، با حملات شبکه با گلوگاه گیری یا محدود کردن نرخ ترافیک مجاز برای ورود به محیط سرمایه هدف، برخورد می‌شود. این رویکردها ممکن است تا حدی مؤثر باشند؛ اما استثنا هستند و توصیه می‌شود که معماری امنیت سایبری برای زیرساخت‌های ملی به عناصری متکی نباشد که اثرات جزیی روی یک حمله خاص دارند.

۶-۱- تأثیر دفاع در عمق

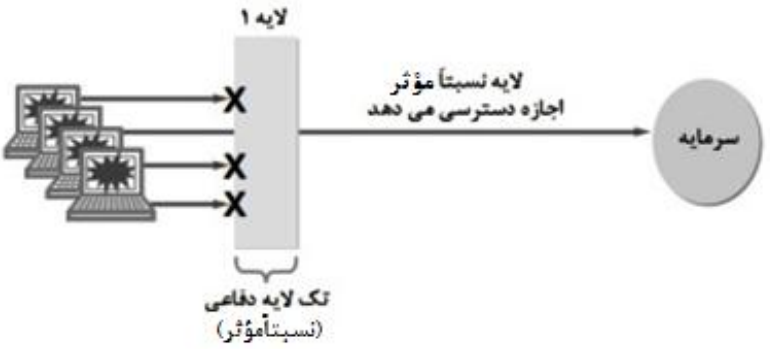
دانشگاهیان به طور رسمی مؤثر بودن مجموعه‌ای از لایه‌های دفاعی را با احتمالات ریاضی مدل می‌کنند. چنین رویکردی مستلزم اندازه‌گیری کمّی وابستگی‌های نسبی بین لایه‌ها و همچنین، احتمال مؤثر بودن هر لایه داده شده است. متأسفانه، در هر محیطی که ساده و کم اهمیت نباشد، هر دوی این تخمین‌ها بیش از یک حدس توسط یک دانشگاهی نخواهد بود. به عنوان مثال؛ می‌دانیم که موفقیت کنترل‌های دسترسی برای کاربردهای سازمان وابسته به موفقیت تأیید هویت قوی برای دسترسی از راه دور است. تلاش برای تعیین کمی دقیق این وابستگی برای تجزیه و تحلیل احتمالاتی، اتلاف وقت است و به تخمینی بهتر از حدس یک متخصص منتج نمی‌شود.

بنابراین، از دیدگاه عملی و در چهارچوب حفاظت واقعی زیرساخت ملی، متخصصان باید تعیین مؤثر بودن یک طرح در عمق را حدس بزنند. که از آن به عنوان استدلال ذهنی غیررسمی مبتنی بر شاخص‌های امنیتی مربوطه یاد می‌شود، اما هنوز هم در حد یک حدس است. فاکتورهای مربوطه برای تخمین مؤثر بودن یک لایه شامل موارد زیر است:

- تجربه عملی: به طور قطع تجربه عملی و نتایج گذشته یک روش امنیتی خاص را می‌توان تجزیه و تحلیل کرد. اگر این روش به معنی واقعی کلمه انجام شود، خطرناک است؛ زیرا ممکن است بسیاری از حملات دیده نشوند و درست باشند و دفاع آسیب‌پذیر برای مدتی قبل از حمله خواب باشد.
- تجزیه و تحلیل مهندسی: مهندسان مجرب امنیتی از دانش و تخصص خود برای ارائه یک قضاوت عالی در مورد اینکه یک لایه خاص مؤثر است، استفاده می‌کنند. باید از فروشندگان و بازاریاب‌ها در این فرآیند اجتناب

کرد؛ زیرا آن‌ها همواره قابلیت‌های محصولات و خدمات خود را تحریف می‌کنند.

- مطالعات موردی استفاده: اضافه کردن دقت بیشتر به تجزیه و تحلیل مهندسی، ایده خوبی است و متدولوژی آشنای مورد استفاده، مخصوصاً برای لایه‌های امنیتی مناسب می‌باشد. که خود می‌تواند یک فرم از تست باشد.
- تست و شبیه‌سازی: تست عملی یک لایه در حالت کنترل شده، اطلاعات خوبی در مورد مؤثر بودن آن ارائه می‌دهد. در مواردی که در آن‌ها یک لایه دفاعی در مقابل چیزهایی که به آسانی تست نمی‌شوند، عمل حفاظت را انجام می‌دهد، مثل یک حمله امتناع از سرویس گسترده، شبیه‌سازی ایده خوبی است.



شکل ۶-۲- تک لایه حفاظتی نسبتاً موثر

برای نشان دادن این رویکرد، با یک وضعیت ساده که در شکل ۶-۲ نشان داده شده است شروع می‌کنیم. مخصوصاً، تنها یک لایه حفاظتی نشان داده‌شده و تخمین زده می‌شود که دارای اثر متوسطی باشد. می‌توانیم فرض کنیم که برخی از زیر مجموعه‌ها از فاکتورهایی که در بالا شرح داده شدند، جهت این تصمیم مورد استفاده قرارگرفته‌اند. شاید بعضی از تیم‌های کارشناسان، حفاظت را تجزیه و تحلیل کرده؛ نگاهی به مؤثر بودن سیستم‌های با وضعیت مشابه انداخته و یک سری از تست‌ها و شبیه‌سازی‌ها را انجام داده باشند. به هر صورت، فرض کنیم که آن‌ها تصمیم گرفته باشند یک حفاظت خاص را که در مقابل برخی انواع حملات در یک محیط تهدید محلی حادث می‌شود، بکار گیرند که تأثیر متوسطی داشته دارد.

تعیین اینکه این لایه تنها "نسبتاً" مؤثر است، در اکثر موارد بیشتر از یک حدس ذهنی نیست. با این حال، این بخش مهمی از اطلاعات برای حفاظت از زیرساخت ملی است؛ زیرا پیامد آن این است که حفاظت در تمام موارد مؤثر نخواهد بود؛ یعنی متخصصان مشخص کرده‌اند که برخی از انواع حملات حفاظت را دور زده یا آن را خواهند شکست؛ بنابراین سرمایه را در دسترس نفوذگر بدخواه قرار خواهند داد. در نتیجه، هنگامی‌که یک لایه حفاظتی خاص، تمام حملات شناخته‌شده را پوشش نمی‌دهد، می‌توانیم به نتایج زیر برسیم:

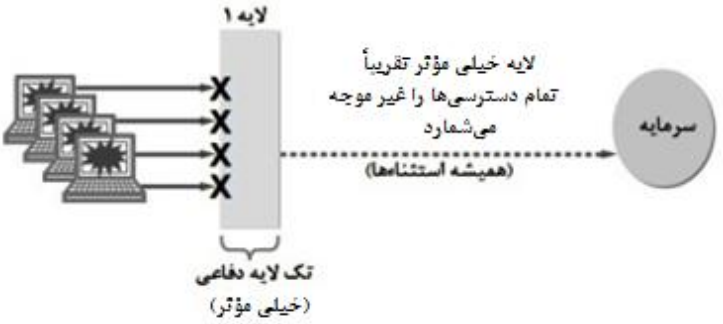
- معایب: حفاظت ممکن است معیوب باشد. این عیب می‌تواند یک مسئله جزیی نظیر وجود یک باگ نرم‌افزاری ناشناس باشد که اجازه انجام بعضی حملات را می‌دهد؛ یا یک عیب بزرگ با پیامدهای عمده. در هر دو حالت، عیوب حفاظتی نیاز به تعمیر و رفع شدن دارند و یک لایه حفاظتی مکمل، باید آثار مخرب آن‌ها را کاهش دهد.
- مناسب بودن: ممکن است حفاظت برای محیط هدف مناسب نباشد برای مثال؛ ممکن است این حفاظت به منظور جلوگیری از وقوع حوادث A و B در محیط خاصی باشد؛ درحالی‌که ، تهدید واقعی در حادثه C اتفاق

بیفتد. معمولاً، چنین سناریوهایی در پاسخ و واکنش به یک واقعه یافت می‌شود، زمانی که رویدادهایی اتفاق بیفتد و حفاظت‌های فرض شده به دلیل عدم تطابق و تناسب اثر کمی داشته باشند، می‌توان با تغییر لایه و لایه مکمل آن را تعمیر و اصلاح کرد.

اگر دشمن از وضعیتی اطلاع داشته باشد که لایه‌ای معیوب یا نامناسب است وضعیت بدتر خواهد شد. بدون در نظر گرفتن استدلال کلی هکرها، که معتقدند مشکلات یک روش حفاظتی باید دیده‌شده و گزارش شوند. واقعیت این است که در دسترس قرار دادن این اطلاعات بیشتر باعث صدمه و آسیب به سیستم می‌شود تا به نفع آن. بدیهی است، اگر سازمانی در اصلاح و تعمیر مشکلات امنیتی خود که پیامدهای وسیعی دارد، سهل‌انگار باشد پذیرفتنی است. اما روش اخاذی از آن‌ها برای اقدام فوری نیز، همیشه، به نفع همه نیست. برای مثال؛ هکری که به طور مؤثری آسیب‌پذیری‌های تلفن موبایل را بدون اینکه اول به ارائه‌دهنده سرویس هشدار دهد در معرض دید قرار می‌دهد، از نظر خدمات مخابراتی ضروری گناهکار شناخته می‌شود زیرا ممکن است جان انسان‌ها را به خطر بیندازد.

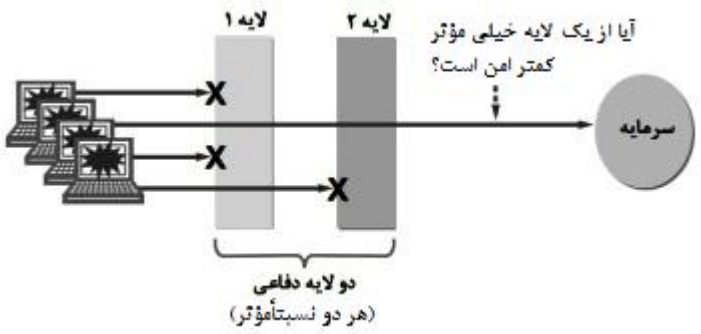
فرض کنید یک سازمان بسیار پرتلاش است و سعی می‌کند که حفاظت نسبتاً مؤثری را بهبود بخشد، نتیجه اینکه تخمین جدید کار آیی لایه حفاظتی ممکن است بسیار مؤثر شود. برای مثال؛ فرض کنید که تیم محلی به این نتیجه رسیده باشد که سیستم فعلی نسبتاً مؤثر است و باید با محصولی جانشین شود که فروشنده از آن حمایت می‌کند. در بیشتر حالات، سیستم جدید به صورت سیستم "بسیار مؤثر" دیده می‌شود (با این اخطار که هیچ سیستم جلوگیری از نفوذی، هرگز، مطابق آنچه که باید کار کند، عمل نمی‌کند). نتیجه نهایی این است که لایه حفاظتی از نسبتاً مؤثر به بسیار مؤثر بهبود می‌یابد. واضح است که حتی در محیط حفاظتی بسیار مؤثر نیز شرایط استثنایی وجود دارد که ممکن است در آن شرایط حفاظت شکست بخورد.

(به شکل ۶-۴ توجه کنید).



شکل ۶-۴- حفاظت تک لایه‌ای خیلی مؤثر

به هر حال اصلاح یک لایه، تنها گزینه در دسترس نیست. گزینه جایگزین این است که لایه حفاظتی حفظ شود و با یک لایه حفاظتی مکمل دیگر تقویت گردد. این روش مزایایی دارد که شامل کاهش هزینه و خطر برداشتن یک لایه حفاظتی و جانشین کردن لایه جدید به جای آن می‌باشد. اضافه کردن یک لایه مکمل حفاظتی به لایه قبلی، نسبتاً مؤثر بوده و باعث می‌شود اثر مجموعه وسیع‌تری از حملات روی سیستم کاهش یابد. این روش، نوعی از محاسبات را به مدیر امنیتی معرفی می‌کند که بر تصمیمات آن‌ها در مورد اینکه آیا تعدادی از حفاظت‌های نسبتاً مؤثر نسبت به تعداد کمتری از حفاظت‌های خیلی مؤثر بهتر یا بدتر است تأثیر می‌گذارد. (به شکل ۶-۴ توجه کنید).



شکل ۶-۴- حفاظت با چندین لایه نسبتاً مؤثر

پاسخ به اینکه آیا چند لایه نسبتاً مؤثر بهتر از تعداد کمتری از لایه‌های بسیار مؤثر عمل می‌کنند، بستگی به جمع ملاحظات خواهد داشت. یعنی اگر دو حفاظت نسبتاً موثر مکمل یکدیگر بوده و ضعف‌های یکدیگر را برطرف کنند، ترکیب حفاظتی آن‌ها کاملاً خوب خواهد بود. از سوی دیگر، اگر چند حفاظت نسبتاً مؤثر ضعف‌های مشابهی داشته باشند، ضعف در حفاظت جمعی آن‌ها نیز باقی خواهد ماند. در عمل، مدیران امنیتی معمولاً باید به دنبال مجموعه متنوعی از حفاظت‌ها باشند، به طوری که این مجموعه تا حد ممکن قوی بوده و ضعف‌ها را متعادل نماید. برای زیرساخت‌های ملی لایه‌های حفاظت؛ شامل؛ تأیید هویت، حفاظت از بد افزار، کنترل دسترسی، رمزنگاری و کشف نفوذ است.

۶-۲- تأیید هویت لایه‌ای

بیشتر تیم‌های فناوری اطلاعات و امنیت در دولت و صنعت متعهد شده‌اند که تعداد کلمه‌های عبور، عبارات عبور، توکن‌های دستی، گواهینامه‌ها، سیستم‌های بیومتریک و دیگر توکن‌های اعتباری را که در محیطشان وجود دارند، کاهش دهند. این طرح‌ها، معمولاً، با اشتیاق زیادی در میان کاربران انتهایی مواجه می‌شوند؛ زیرا باعث زیرساختی ساده‌تر و تمیزتر شده و کاربران انتهایی باید چیزهای بسیار کمتری را به خاطر بسپارند یا بنویسند. نمی‌توان انکار کرد که چنین ساده‌سازی اثر مفیدی روی کل امنیت خواهد داشت. با این دلایل، پیشنهادات متعددی برای ایجاد سیستم‌های تأیید هویت ملی که به وسیله دولت اداره می‌شود، داده‌شده که تمام شهروندان را شامل خواهد شد.

معمولاً، از ابتکارات تک امضایی SSO برای انجام هدف ساده‌سازی تأیید هویت استفاده می‌شود. SSO با استفاده از یک سیستم تنها، برای شناسایی مشترک و تأیید هویت تمام کاربردهای مرتبط به کار می‌رود. این سیستم مشترک، در یک فرآیند مدیریت شناسه جاسازی می‌شود، به طوری که شناسه‌های گزارش‌شده می‌توانند به طور یکنواخت مدیریت شده و حفظ شوند. از دیدگاه امنیتی، ساده‌سازی ذاتی در SSO مطلوب است؛ زیرا احتمال خطایی را که نتیجه وجود چند سیستم پیچیده اجازه دهنده ورود به سیستم هستند کاهش می‌دهد. بنابراین، استفاده از مدیریت شناسه مشترک مخصوصاً در محیط بنگاه‌های تجاری از منظر امنیتی مطلوب است.

اگر در ساده‌سازی فرآیند تأیید هویت زیاده‌روی شود، مشکلاتی در محیط‌های زیرساخت ملی به وجود می‌آید. حتی ثابت‌قدم‌ترین مدافعان SSO باید بپذیرند که برای بعضی کاربردها، مجموعه متنوعی از چالش‌های تأیید هویتی که به نحو مناسبی مدیریت و طراحی‌شده‌اند و متکی به فاکتورهای اثبات جداگانه‌ای هستند، امن‌تر از

سیستم قابل‌مقایسه SSO خواهد بود. قطعاً، مجموعه متنوعی از مراحل تأیید هویت برای کاربران انتهایی کمتر راحت است، ولی اگر به طور صحیح اجرا شوند، امن‌تر خواهند بود؛ زیرا چنین طرحی از سناریوی کابوس مانندی جلوگیری می‌کند که در آن دشمن با یک ورود تنها به سیستم، دسترسی مشترکی به چند سیستم زیرساخت ملی را خواهد یافت. سناریوی حمله چنان برای زیرساخت ملی مؤثر است که توجه خاصی را ایجاب می‌کند.

سازمان‌ها می‌توانند برای مدیریت زیرساخت ملی، برای هدف ایجاد توازن بین خطرات و منافع SSO، تمام کاربردهای مناسب سازمانی؛ نظیر؛ ایمیل کسب‌وکار، کاربردهای روتین و دسترسی از راه دور را به طور قابل قبولی نگهدارند. تا زمانی که هیچ‌کدام از سرمایه‌های ملی را نتوان با دسترسی SSO به طور مستقیم مورد نقض امنیتی قرارداد، SSO خوب خواهد بود. شرکت‌ها و آژانس‌هایی که مسئولیت زیرساخت ملی به آن‌ها محول شده باشد، می‌توانند و باید به سمت طرح SSO با مدیریت شناسه متناظر حرکت کنند. برای تأیید هویت کاربران انتهایی، استفاده از خدمات و کاربردهای زیرساخت حیاتی یک طرح دفاع در عمق پیچیده‌تر، اکیداً، توصیه می‌شود.

فاکتورهای یک سیستم دسترسی SSO زیرساخت ملی موفق

سرویس‌های زیرساخت ملی حیاتی احتیاج به طرح دفاع در عمقی دارند که با ملاحظات زیر توسعه‌یافته باشند:

- تنوع با یک ثبت‌نام تنها: سیستم‌های تأیید هویت، باید برای حفاظت از سرمایه‌های ملی از طرح SSO ای استفاده کنند که متفاوت از طرحی می‌باشد که برای دسترسی در بنگاه‌های تجاری بکار می‌روند. این ایجاب می‌کند که بین SSO بنگاه‌های تجاری و سیستم تأیید هویت زیرساخت ملی فناوری، فروشنده و فرآیند مدیریت جداگانه‌ای مورد نظر قرار گیرد.

هدف این ست که اطمینان حاصل شود که نقص و عیب در یک سیستم تأیید هویت در دیگری موجود نباشد.

- تنوع فاکتورهای اثبات: به طریقی مشابه فاکتورهای اثبات آشنا نظیر.
  «چیزی که می‌دانید».
  «چیزی که دارید».
  «چیزی که با خود دارید. (بیومتریک)».
  «جایی که در آن هستید».

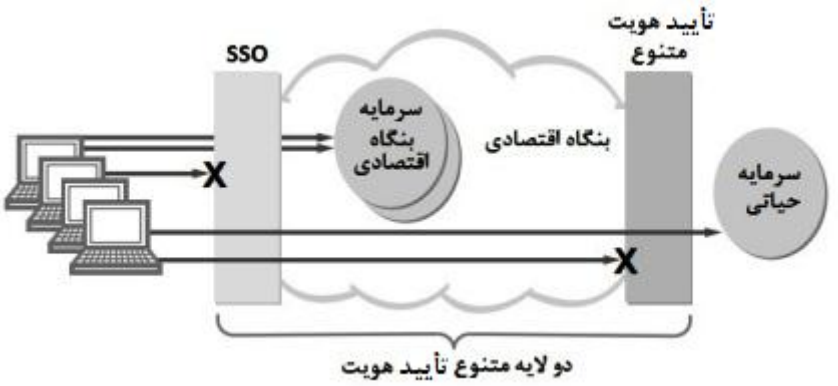
باید در سرمایه‌های ملی متنوع‌تر نسبت به فاکتورهای اثبات در SSO باشند. این ایجاب می‌کند که نباید به کارمندان تنها یک تأیید هویت کننده دستی داده شود که بتوانند از آن برای دسترسی به ایمیل و دیگر اجزا عملیاتی زیرساخت حیاتی استفاده کنند.

- تأکید بر امنیت: با اینکه تأکید بر قابل استفاده بودن ابتکارات SSO بنگاه‌های تجاری قابل‌قبول است ولی در حفاظت از زیرساخت‌های ملی باید تأکید مستقیماً به سمت امنیت برگردانده شود. تنها مسائل مربوط به کاربر انتهایی آن‌هایی هستند که برای کاهش خطا، استفاده کردن را تسهیل می‌کنند. سهولت استفاده تا هنگامی‌که طرح تأیید هویت رفتارهای بدی نظیر اشتراک در تو کن یا نوشتن کلمه عبور در یک جا را به دنبال نمی‌کشد، نباید یک هدف عمده باشد.

یک طرح دفاع در عمق برای سازمان‌های زیرساخت ملی باید شامل SSO برای کاربردها و دسترسی در سطح بنگاه‌های تجاری و در پی آن فرآیند تأیید هویت متنوع برای تمام سرمایه‌های ملی باشد. در نتیجه، کاربران انتهایی پیش از به دست آوردن دسترسی به سرمایه‌های حیاتی، به دو بار تأیید هویت احتیاج خواهند داشت. به این ترتیب، نفوذگران مجبور می‌شوند برای به دست آوردن دسترسی بدخواهانه به سرمایه

هدف دو سیستم تأیید هویت را بشکنند. احتمالاً، کاربران انتهایی این فرآیند را دوست ندارند؛ زیرا هزینه‌ها بالاتر هستند اما افزایش امنیت ارزش آن را دارد.

(به شکل ۶-۵ توجه کنید).

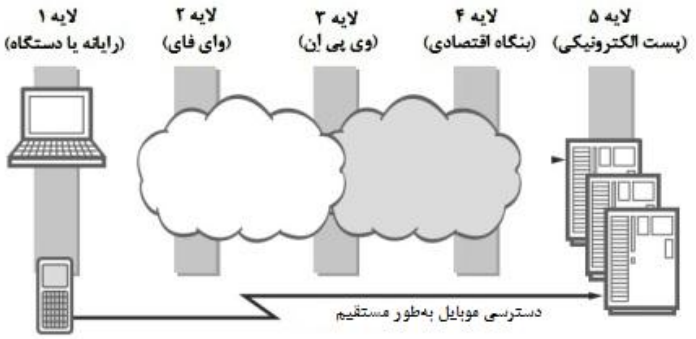


شکل ۶-۵- طراحی برای نشان دادن دو لایه از تأیید هویت کاربر انتهایی

برای چند سرمایه ملی حیاتی در محیط زیرساخت، راهبرد دفاع در عمق باید شامل تنوع بیشینه برای هر سرمایه باشد. یعنی مشخصات محاسباتی عمومی و منبع قابلیت تأیید هویت باید متنوع باشند. همچنین، فاکتورهایی که برای برقراری اثبات شناسه برای سرمایه‌های حیاتی به کار می‌روند، باید از کلمه عبور ساده، قوی‌تر باشند، دستگاه‌های تأیید هویت دستی یا بیومتریک توصیه می‌شوند. زیرساخت‌های اساسی باید با بیشترین دقت و صحت اداره شوند. برای جلوگیری از مهندسی اجتماعی، رویه‌های اداری به دست آوردن یک توکن تأیید هویت، بازگرداندن دسترسی زمانی که توکن یا کلمه عبور از دست می‌رود و کمک به کاربران انتهایی هنگامی‌که سردرگم هستند، باید با دقت طراحی شود. در سطح ملی، این موضوع احتیاجی به تست مکرر دارد.

یک موضوع جدید کلیدی برای تأیید هویت بنگاه‌های تجاری، درجه‌ای است که دسترسی با تلفن همراه به زیرساخت به طور بالقوه می‌تواند وضعیت امنیتی را تغییر دهد. برای مثال؛ فرض کنید که بیشتر سازمان‌ها راه طولانی را جهت اطمینان از اینکه چند لایه تأیید هویت بین کاربران از راه دور و کاربردهای حساس نظیر، ایمیل بنگاه تجاری وجود دارد طی می‌کند، در حقیقت، بیشتر مردم زمانی که سعی می‌کنند ایمیل سازمانی‌شان را از راه دور با لپ‌تاپ به دست بیاورند مراحلی را تجربه می‌کنند که در ادامه آورده شده است:

مثال زیر اهمیت شناخت روند تکنولوژی را نشان می‌دهند که در آن ابتکارات حفاظت از زیرساخت ملی برجسته شده است. برای یک بنگاه تجاری، با ظهور دسترسی موبایل به زیرساخت‌های حامل بی‌سیم مفهوم قدیمی محیط حفاظت‌شده سازمان ناپدید می‌شود. هنوز هم می‌توان ساختارهایی را یافت که در آن کاربران دسترسی موبایل خود را به بنگاه تجاری طوری متصل می‌نمایند که این اتصال از طریق دیوار آتش به کاربرد مورد هدف برقرار شود، اما احتمالاً، این شیوه عمل در آینده افول خواهد کرد (به شکل ۶-۶ توجه کنید).



شکل ۶-۶- گزینه‌های تأیید هویت شامل دسترسی گوشی تلفن به صورت مستقیم

حفاظت چند لایه‌ای: پنج مرحله برای دسترسی ایمیل از راه دور

یک کاربر از راه دور برای دسترسی به ایمیل سازمانی خود احتیاج به گذراندن مراحل زیر دارد:

- لایه ۱ تأیید هویت: ابتدا کاربر باید به کامپیوتر وارد شود. احتمالاً این عمل با استفاده از یک کلمه عبوری انجام می‌شود که قسمت فناوری اطلاعات یا گروه امنیت سازمان تعیین کرده‌اند.
- لایه ۲ تأیید هویت: کاربر باید به وای فای محلی یا شبکه دسترسی باند پهن وارد شود. گاهی اوقات، این عمل رایگان است و گاهی احتیاج به کارت اعتباری دارد که می‌تواند به عنوان گام شناسایی اضافی در نظر گرفته شود.
- لایه ۳ تأیید هویت: کاربر باید به سرور دسترسی از راه دور وارد شود، احتمالاً، با یک شبکه خصوصی مجازی وی‌پی‌ان این عمل را انجام خواهد دارد. بیشتر مواقع، شرکت‌ها و آژانس‌ها برای تأیید هویت دسترسی به وی‌پی‌ان، احتیاج به شماره شناسه فردی پین، کلمه عبور و یا توکن دستی دارند.
- لایه ۴ تأیید هویت: کاربر باید احتمالاً با نوعی از کلمه عبور دامنه‌ای وارد شبکه بنگاه تجاری شود. این ورود، احتمالاً، به وسیله گروه فناوری اطلاعات یا امنیت محلی کنترل می‌شود.
- لایه ۵ تأیید هویت: سرانجام کاربر باید وارد کاربرد ایمیل مخصوصی گردد که بنگاه تجاری استفاده می‌کند. برخی مواقع، این عمل احتیاج به یک کلمه عبور دیگر دارد؛ اما معمولاً فقط به دسترسی نیاز است.

به ظاهر، به نظر می‌رسد که این مراحل، نهایت تأیید هویت لایه‌ای است که کمتر از ۵ لایه نخواهد داشت! مشکل این است که بسیاری از سازمان‌ها به کارمندان خود

وسایلی ارائه می‌نمایند که بتوانند به کاربردهایی نظیر ایمیل با یک دستگاه دستی از راه دور دسترسی یابند. در نظر بگیرید، در این حالت، بیشتر مردم هنگامی‌که سعی در به دست آوردن ایمیل سازمانی خود به وسیله یک گوشی همراه دارند، تجربه‌ای به صورت زیر خواهند داشت:

- لایه ۱ تأیید هویت: کاربر باید به سادگی به گوشی موبایل وارد شود. روی آیکون ایمیل کلیک کند سپس، ایمیل را بخواند یا آن را تولید کند.

روشن است که این یک لایه تأیید هویت برای گوشی موبایل است و نشان می‌دهد که کاربران می‌توانند راه‌های راحت‌تری را برای دور زدن لایه‌های تأیید هویت بیابند.

برای کاربردهایی نظیر ایمیل بنگاه تجاری، ممکن است این نوع دور زدن‌های راحت، کاملاً خوب باشد. در واقع، برای ایمیل بنگاه تجاری، مخصوصاً انتظار اینکه کارمندان در محیط‌های زیرساخت ملی اجازه دسترسی به گوشی موبایل را نداشته باشند، غیرمنطقی است. برای کاربردهای حساس‌تر زیرساخت ملی، مانند آن‌هایی که ارائه‌دهنده یا کنترل‌کننده سیستم‌های حیاتی هستند، پیش از اینکه اجازه راه‌های جایگزین با گوشی موبایل داده شود، به یک تجزیه و تحلیل تهدید نیاز است. اطلاعات طبقه‌بندی شده، مثال دیگری از سرمایه‌ها می‌باشد که بدون دور زدن دسترسی با گوشی موبایل، احتیاج به چندین لایه تأیید هویت دارد. این نوع از الزامات، باید راه خود را به داخل هر نوع قرارداد حمایتی زیرساخت ملی پیدا کنند.

۶-۳- حفاظت لایه دار در مقابل ویروس ایمیل و هرزنامه

محیط‌های تجاری به طور فزاینده‌ای به راه‌حل‌های مجازی شده در اَبر برای فیلتر کردن ویروس‌های ایمیل و هرزنامه‌ها در دروازه‌های و رودی‌شان روی آورده‌اند. این تصمیم به سازمان اجازه می‌دهد که فیلترها را از دروازه‌هایشان بردارند و به سادگی کاری را که این فیلترها انجام می‌دادند، حذف کنند. این تصمیم سالم کننده‌ای خواهد

بود؛ زیرا یک اصل امنیتی عمومی این است که باید حملات را تا حد ممکن نزدیک منبعشان متوقف کرد. شبکه قطعاً نزدیک‌تر به منبع حمله است، تا نقطه ورودی مقصد حمله، بنابراین، فیلتر کردن مجازی مطلوب است. برای حامل‌ها نیز این مفیدتر است؛ زیرا باعث کاهش داده‌های آشغال شناور در زیرساخت شبکه می‌گردد و حامل‌ها وظیفه خود را با بهره‌وری بالاتری در حمایت سرویس‌های ملی انجام می‌دهند.

مدیران محیط‌های تجاری تشخیص داده‌اند که نقاط انتهایی محاسباتی آن‌ها نمی‌توانند فقط متکی بر پردازش در ابر یا دروازه‌ها باشند. به این ترتیب، آخرین و به‌روزترین شیوه عمل حفاظت در مقابل ویروس و هرزنامه؛ شامل؛ به‌کارگیری دفاع در عمق فیلترها برای هر لپ‌تاپ، نوت بوک، کامپیوتر شخصی و سرورهای یک بنگاه است. این رویکرد، زمانی که تهدید ویروس‌ها و هرزنامه‌ها در حال افزایش است، به دستگاه‌های دستی موبایل راه پیدا می‌کند. به این ترتیب، یک ویروس خاص یا هرزنامه‌ای که از منبع بدخواهی فرستاده می‌شود، باید از میان حداقل دو لایه فیلتر، راهی را برای رسیدن به هدف مورد نظر خود بیاید. (به شکل ۶-۷ توجه کنید).

شکل ۶-۷- معماری نمونه برای فیلتر لایه‌ای ایمیل

این ترتیب فیلتر ابری که در بیشتر شرکت‌ها یافت می‌شود، از نظر سازمان‌های مسئول زیرساخت ملی نیز پذیرفته می‌گردد. توصیه می‌شود که، برای بیشتر کاربردهای

حیاتی، رویکرد دفاع در عمق شامل هر دو روش در اَبر و پردازش پیرامونی باشد. همچنین، برای مدیران کلیدی در این شرکت‌ها و آژانس‌ها که ممکن است دشمن مستقیماً آن‌ها را هدف قرار دهد، گذاردن فیلترهای اضافی روی کامپیوتر رومیزی و یا کاربردها معقول است. تجربه عملی نشان می‌دهد که هرزنامه برای مدیریت سرمایه‌های ملی بیشتر یک مزاحمت است، تا یک تهدید قابل ملاحظه بنابراین، احتمال اینکه حمله‌کننده از هرزنامه برای ایجاد وقفه در خدمات ملی استفاده کند، محدود است. همچنین، نرم‌افزارهای ضد ویروس (ویروس کش) در سال‌های اخیر کم اهمیت شده‌اند و این به علت تهدیدات نرم‌افزاری مانند بات‌های به خوبی کد شده که به آسانی با نرم‌افزارهای ضد ویروس قابل کشف نیستند می‌باشد. پژوهش در زمینه روش‌های بهتر برای تشخیص وجود بد افزارها باید به عنوان یک اولویت ملی فوری در نظر گرفته شود.

۶-۴- کنترل‌های دسترسی لایه‌ای

کنترل‌های دسترسی مشخص می‌کنند که چه کسانی می‌توانند تحت چه شرایطی به چه منابعی دسترسی داشته باشند. آن‌ها متداول‌ترین و به بلوغ رسیده‌ترین روش‌های حفاظت امنیتی هستند که قدمت آن‌ها به اولین کامپیوترهای الکترونیکی بر می‌گردد. اگر برخی از سرمایه‌ها به وسیله یک مجموعه تنها از کنترل‌های دسترسی حفاظت شوند، این شبیه یک قفل ترکیبی ساده است که برای حفاظت از یک سرمایه فیزیکی بکار گرفته می‌شود. به این معنا که اگر شخصی ترکیب صحیح را بداند، به او اجازه دسترس داده می‌شود. کنترل‌های دسترسی متداول؛ شامل؛ لیست‌های کنترل‌های دسترس (ACLs) در سیستم عامل مبتنی بر ویندوز و بردارهای اجازه دسترسی در سیستم‌های عامل مبتنی بر یونیکس هستند. این لیست‌ها به صورت ساختار داده نرم‌افزاری پیاده‌سازی شده‌اند و دسترسی را بر اساس برخی سیاست‌های تعریف‌شده مشخص می‌نمایند.

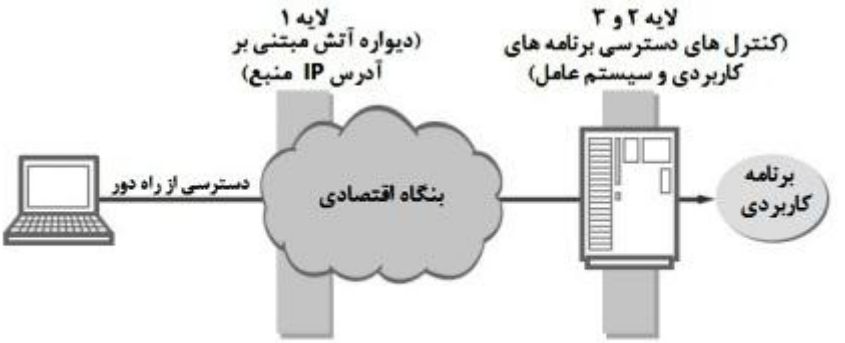
یک رویکرد استفاده از دفاع در عمق برای حفاظت کاربردهای نرم‌افزاری؛ شامل؛ تعبیه یک نوع کنترل دسترسی در محیط کاربرد و سپس، میزبانی کاربرد روی سیستم عاملی است که از نوع متفاوتی از کنترل دسترسی استفاده می‌کند. در یک چنین ترتیبی، دسترسی به کاربرد موقعی می‌تواند به دست آید که مذاکرات موفقیت‌آمیزی با لایه‌های زیر انجام شود:

- لایه ۱ کنترل دسترسی: باید به کاربر اجازه ورود به سیستم عامل از طریق کنترل‌های دسترسی سیستم عامل داده شود؛ که این ممکن است UNIX permission و یا WindowsACLs و یا چیزهای شبیه آن‌ها باشد.
- لایه ۲ کنترل دسترسی: باید از طریق کنترل‌های دسترسی کاربرد به کاربر اجازه ورود به کاربرد داده شود. احتمالاً این یک کلمه عبور جاسازی‌شده در محیط کاربرد است و صاحب کاربرد آن را کنترل می‌کند.

در مواردی که به سیستم عامل و کاربرد از راه دور نمی‌توان رسید، این دو لایه را می‌توان با کنترل‌های متنوع اضافی؛ نظیر دسترسی محافظت‌شده به ساختمان‌های فیزیکی و یا مراکز داده قفل شده، تقویت کرد؛ یعنی، دسترسی به برنامه‌های کاربردی ابتدا نیاز به به دست آوردن دسترسی فیزیکی به کنسول دارد، پیش از اینکه بتوان تلاشی برای دسترسی به سیستم عامل و کاربرد را انجام داد. این دو لایه تأیید هویت مهم هستند و باید در هر محیط زیرساخت ملی تست شوند، مخصوصاً، در سیستم‌هایی که در آن‌ها از کنترل نظارت و جمع‌آوری داده (SCADA) استفاده می‌شود، جایی که تکنیک‌های امنیت کامپیوتری دارای سابقه کوتاه مدت تری هستند. به هر حال، به علت اینکه افراد داخلی احتمالاً هر دو نوع کلمه عبور را می‌دانند، این لایه‌ها به متوقف کردن خرابکاری‌های کارمندان داخلی کمکی نخواهد کرد.

در مواردی که دسترسی از راه دور مجاز است، استفاده از دیوار آتش رایج‌ترین روش برای اطمینان از رعایت سیاست‌های امنیتی برای کسانی است که مجاز به

دسترسی هستند. چنین سیاستی، همیشه، مبتنی بر آدرس پروتکل اینترنت (IP) منبع طرف درخواست کننده است. این قوی‌ترین روش کنترل دسترسی نیست؛ زیرا به سادگی می‌توان آدرس IP را جعل کرد. همچنین، برای نگهداری چنین طرحی باید یک بوروکراسی پیچیده و مستعد خطا، استقرار یابد که درخواست‌های دسترسی را پذیرش و نگهداری نماید. زمانی که این طرح همراه با لایه‌های کنترل دسترسی اضافی سیستم عامل و کنترل دسترسی برنامه‌های کاربردی استفاده شود، ممکن است در برخی محیط‌ها قابل‌قبول باشد (به شکل ۶-۸ توجه کنید).



شکل ۶-۸- سه لایه حفاظت با استفاده از دیوار آتش و کنترل‌های دسترسی

برای حفاظت از زیرساخت ملی، باید سرمایه‌های حیاتی را با لایه‌های زیادی از کنترل دسترسی پوشش داد. در مورد تأیید هویت، اگر خدمات ملی حیاتی در خطر باشد، مسئله راحتی کاربر انتهایی باید با ارجحیت پایین‌تری مورد نظر قرار گیرد. برخی ابتکارات عمومی برای حفاظت از زیرساخت ملی با کنترل‌های دسترسی لایه‌ای شامل موارد زیر است:

- دیوارهای آتش مبتنی بر شبکه: استفاده از دیوارهای آتش ابری یک لایه پوششی کنترل اضافی را ارائه می‌دهد. این روش به عنوان مکمل کنترل‌های موجود بنگاه‌ها مفید است، مخصوصاً، سیستم دیوار آتش مبتنی بر حامل نسبت به سیستم‌های دیوار آتش مبتنی بر میزبان و سیستم‌های مرتبطی که در بنگاه‌های تجاری بکار می‌روند، متفاوت است.
- دیوارهای آتش داخلی: این دیوارهای آتش لایه دیگری از حفاظت در داخل بنگاه تجاری برای اطمینان از اینکه افراد با دسترسی به منبع X فقط به آن منبع دسترسی می‌یابند و لا غیر را ایجاد می‌کنند. معمولاً، روترها می‌توانند قابلیت ساده فیلتر کردن بسته‌ها را به عنوان قسمتی از مجموعه پردازشی بومی خود ارائه دهند که باعث سادگی ساختار و کمینه شدن هزینه می‌گردد.
- امنیت فیزیکی: امنیت عالی دسترسی به ساختمان‌ها و امکانات یک لایه محسوس اضافی از حفاظت را ایجاد می‌کند و برای ابتکارات حفاظت از زیرساخت‌های ملی ضروری است. این حفاظت باید با انتخاب مناسب کاربردها و سیستم‌های مناسبی تکمیل گردد که هرگز، نتوان از راه دور و حتی در طول یک شبکه محلی LAN به آن‌ها دسترسی یافت.

هنگامی‌که چند سیستم کنترل دسترسی استقراریافته‌اند، در صورتی که توابع مدیریتی اساسی باتیمی انجام شود که از مجموعه‌ای از ابزارهای مشترک استفاده می‌نمایند؛ منافع لایه‌بندی کاهش می‌یابد. زمانی که این شامل یک مرکز عملیات امنیتی باشد، که حفاظت‌شده و با دقت مدیریت می‌شود، وضعیت پذیرفتنی است. اما اگر مدیریت تک کاره بوده و به طور ضعیفی کنترل شود، لایه‌بندی ممکن است به وسیله حمله‌کننده‌ای که با موفقیت به سیستم مدیریت نفوذ می‌نماید تضعیف شود.

۶-۵- رمزگذاری لایه‌ای

رمزگذاری، کنترل امنیت شناخته‌شده و مؤثری برای حفاظت اطلاعات است.

ریاضیدانان و دانشمندان کامپیوتری، صدها طبقه‌بندی مختلف برای دسته‌بندی سیستم‌های رمزگذاری متقارن و یا با کلید عمومی ایجاد نموده‌اند. روش‌های خاصی که برای حفاظت از زیرساخت ملی مفید هستند، در زیر نشان داده شده است.

پنج روش رمزگذاری برای حفاظت از زیرساخت ملی:

- ذخیره‌سازی درگوشی‌های موبایل: تلفن‌های هوشمند موبایل و لپ‌تاپ‌ها باید رمزگذاری بومی برای حفاظت در مقابل از دست دادن و سرقت اطلاعات داشته باشند تا در آن‌ها نقض امنیتی در مورد اطلاعات موجود انجام نشود. رمزگذاری، هرگز، کامل نخواهد بود، اما باید حفاظت مفیدی در میدان کار ایجاد کند. چند فروشنده این نوع رمزگذاری را به صورت خدمات افزودنی ارائه می‌دهند. اما سرانجام رمزگذاری یک تابع بومی در داخل تمام گوشی‌های موبایل و لپ‌تاپ‌ها خواهد شد.
- انتقال شبکه: هرگونه اطلاعات حساس در داخل یک بنگاه تجاری و بین شرکای معلوم و شناخته‌شده که انتقال داده می‌شود، باید رمزگذاری شود. ابزارهای سنتی برای چنین رمزگذاری به صورت متقارن بوده و در دستگاه‌های سخت‌افزاری تعبیه‌شده‌اند. اخیراً، روش‌های رمزگذاری بیشتر مبتنی بر نرم‌افزار و شامل کلید عمومی بوده و با ابزارهای زیرساخت کلید عمومی PKI حمایت می‌شوند. وقتی انتقال داده در شبکه به صورت تک کاره انجام می‌شود، فرض بر این است که رمزگذاری با کلید مشترک بین سازمان‌ها به علت پیچیدگی وجود ندارد. این رمزگذاری، ترافیک شبکه را

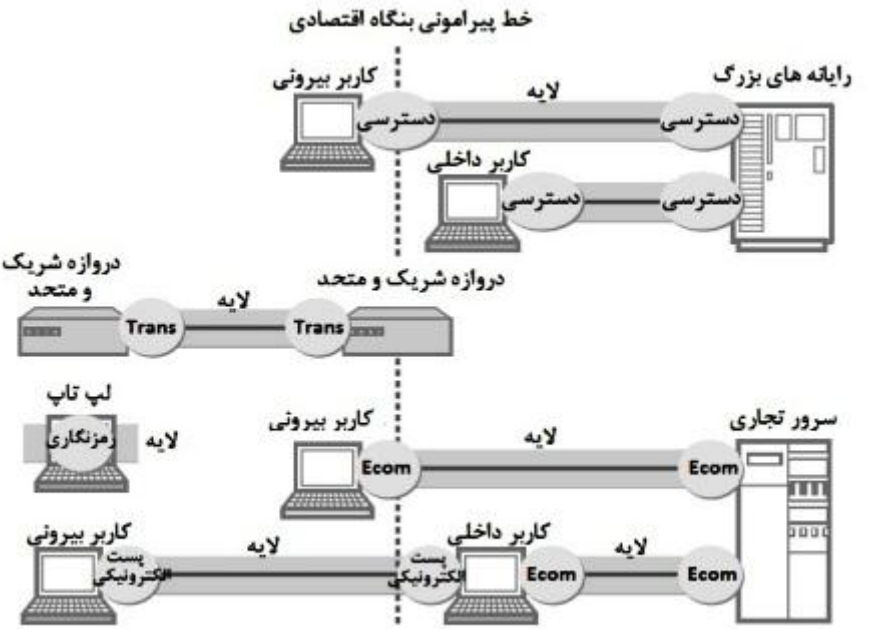
بدون هماهنگی‌های قبلی مشکل می‌سازد. زیرا کلیدهای مشترک باید قبلاً توزیع شده باشند.

- تجارت امن: اگر سازمانی خدمات تجارت الکترونیکی را روی اینترنت ارائه می‌کند، استفاده از پروتکل‌هایی نظیر SSL یا لایه سو کت امن که در آن روش‌های رمزگذاری استفاده می‌شود، باید مورد نظر قرار گیرد، در این پروتکل روش رمزگذاری مبتنی بر کلید عمومی است.
- تقویت برنامه‌های کاربردی: پذیرایی ایمیل بارزترین برنامه کاربردی است که می‌تواند خواص پنهان‌کاری و تأیید هویت را از طریق استفاده از رمزگذاری معرفی کند. همان طور که در بالا اشاره شد، امروزه، متحدشدن سازمان‌ها برای استفاده از روش رمزگذاری مناسب ایمیل که همیشه، مبتنی بر کلید عمومی باشد، در مقیاس وسیع انجام نشده است.
- ذخیره‌سازی داده‌ها در رایانه‌های بزرگ و سرورها: در سال‌های اخیر، رمزگذاری روی‌داده‌های موجود در سرورها و رایانه‌های بزرگ مورد توجه قابل‌ملاحظه‌ای بوده است؛ اما این توجه شدید را باید با شک و تردید مورد نظر قرارداد. داده‌های ساکن با رمزگذاری به طور ضعیفی حفاظت می‌شوند؛ زیرا سیستم‌های مدیریت کلید مربوطه که معمولاً، نیاز به عمر طولانی دارند، دارای آسیب‌پذیری‌های آشکاری می‌باشند. در بدترین حالت، مدیریت کلید آشفته، می‌تواند داده‌ها را کمتر امن کند. توجه داشته باشید که تلفن‌های هوشمند و لپ‌تاپ‌ها نسبت به سرورها، به علت اینکه در حالت حرکت هستند، متفاوت عمل می‌کنند.

خوشبختانه، در بیشتر قسمت‌ها، پنج روش رمزگذاری دارای تضاد نیستند و می‌توان از آن‌ها به صورت ترکیبی و هماهنگ استفاده کرد، بدون اینکه مشکلات بزرگ اداری یا عملکردی داشته باشیم. تا زمانی که ابزارهای اداری حمایت‌کننده به خوبی کار کنند، کاملاً، خوب خواهد بود که اطلاعات را چند بار رمزگذاری کنیم. به این ترتیب، به

راحتی می‌توان سناریوهایی را تصور کرد که در آن‌ها تمام پنج روش استقرار دارند و پنج لایه مختلف حفاظت اطلاعات را ارائه می‌دهند. معمولاً، تمام آن‌ها در یک سری کامل قرار ندارند، اما می‌توانند در یک محیط زیرساخت استقرار داشته و امنیت لایه‌ای را ارائه دهند (به شکل ۶-۹ توجه کنید).

متأسفانه، هر کدام از روش‌ها نیاز به مدیریت کاربران و سیستم مدیریت کلید خوددارند که باعث ایجاد یک تصویر نامتجانس از رمزگذاری در سراسر شرکت می‌گردد و می‌تواند به صورت ترتیب پراکنده‌ای در شکل ۶-۹ دیده شود. این کار باعث افزایش پیچیدگی می‌گردد که خود باعث افزایش احتمال خطا و نقض امنیتی مخصوصاً در زیرساخت‌های اساسی است. با وجود مواردی که در بالا توضیح داده شد؛ باید استفاده از رمزنگاری در حفاظت از زیرساخت‌های ملی تشویق شود، حتی اگر لایه‌ها به صورت بهینه هماهنگ نشده باشند.



شکل ۶-۹- لایه‌های چندگانه رمزگذاری

۶-۶- کشف نفوذ لایه‌ای

کشف نفوذ زمانی به عنوان امیددهنده‌ترین روش امنیتی مقیاس وسیع در نظر گرفته می‌شد. حتی نام تحریک‌کننده و امیدوارکننده "کشف نفوذ" یک فناوری قدرتمند را نشان می‌دهد که می‌تواند در یک محیط برای هشدار دادن به تیم‌های امنیتی زمانی که وقوع یک نفوذ نزدیک باشد قرار داده شود. با اینکه به این هدف نرسیده‌اند؛ کشف نفوذ ابزارهای مفیدی برای کشف شاخص‌هایی از رفتار بالقوه آسیب‌زننده‌ای را ارائه می‌دهد. برخی مواقع، این شاخص‌ها برای نشان دادن هشدارهای زودهنگام بکار

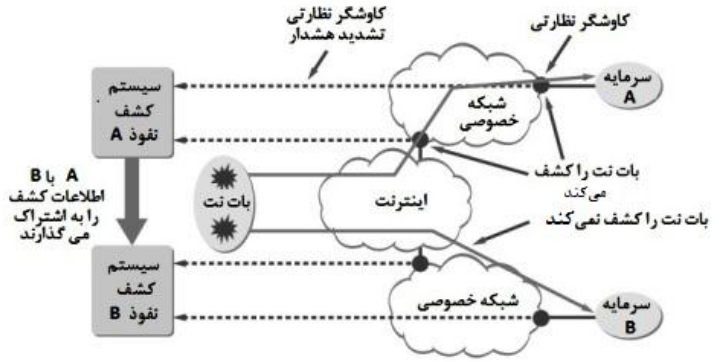
می‌روند، اما در بیشتر مواقع، جهت همبسته شدن با انواع دیگری از اطلاعات در دسترس در زمان وقوع یک حادثه به کار می‌روند.

به علت اینکه کشف نفوذ، معمولاً، به صورت غیر بر خط انجام می‌شود، بنابراین، تحت نظر چند لایه از نظارت قرار دارد. بدیهی است که اگر کشف نفوذ شامل یک واکنش فعال نیز باشد، جمعاً به آن کشف و جلوگیری از نفوذ گفته می‌شود؛ در آن صورت، ترتیبات پیچیده‌تر خواهد بود، اما در حال حاضر، به تجزیه و تحلیل راهبردها برای نظارت غیرفعال و غیر بر خط حملات می‌پردازیم. بیشتر سازمان‌ها این کار را با استفاده از سیستم‌های تجاری انجام می‌دهند که شامل سه جز است؛ این اجزا عبارت‌اند از مانیتورها که در نقاط راهبردی برای جمع‌آوری اطلاعات قرار داده می‌شوند، سیستم‌های انتقال که اطلاعات هشدارها را به نقطه مرکزی منتقل می‌کنند و یک عملگر نظارت‌کننده مرکزی که داده‌های ورودی را پردازش کرده و نوعی خلاصه از همبسته کردن اطلاعات ورودی را به صورت هشدار به یک کنسول ارائه می‌کند. زمانی که این نوع سیستم کشف نفوذ در سازمان در جای خود قرار می‌گیرد، می‌توان آن را به صورت لایه صریحی از حفاظت در نظر گرفت. در حقیقت، بسیاری از ممیزین، هنگامی که برخی از حفاظت‌ها ضعف‌هایی را نشان می‌دهند، سیستم کشف نفوذ را به عنوان کنترل کننده مکمل می‌پذیرند.

می‌توان یک لایه جایگزین کشف نفوذ را تصور کرد که در سطح گسترده‌تری قرار داده شده است و شاید به وسیله بعضی گروه‌های دولتی و صنعتی هماهنگ می‌شود. اجزای سیستم کشف نفوذ یکسان هستند اما تفاوت‌های آن با سیستم کشف نفوذ بنگاه‌های تجاری شامل قرار دادن مانیتورهای بسیار متنوع، امضاهای مختلف حملات و پایگاه گسترده‌ای از داده‌ها است که بتوان با آن‌ها عمل همبسته‌سازی را انجام داد. مشکل این لایه جایگزین، این است که حفاظت احتمالاً شامل مسیرهایی از شبکه خواهد بود که بیشتر آن‌ها، از آنچه در محیط‌های بنگاه‌های تجاری خاص وجود دارد، جدا هستند. برای مثال؛ نفوذی که هدفش برخی آژانس‌های دولتی است، با یک سیستم

کشف نفوذی که در یک بنگاه تجاری جداگانه دیگر قرار دارد، کشف نخواهد شد. با این حال، سه فرصت خاص برای سیستم‌های متفاوت کشف نفوذ برای ارائه حفاظت لایه‌ای وجود دارد:

- کشف داخل باند: اگر دو سیستم کشف نفوذ، هر دو، نظارت دسترسی بر یک جریان حمله یا حمله مرتبطی را داشته باشند. هردو، فرصت کشف حمله را خواهند داشت، اگر یکی از دو سیستم در کشف حمله شکست بخورد، ممکن است دیگری موفق به کشف حمله شود و این اساس دفاع در عمق است، اما این روش، زمانی مؤثر خواهد بود که فرآیندهای واکنش و پاسخ برای هر دو یا چند سیستم هماهنگ باشند.
- همبسته سازی خارج باند: در طی یک حادثه، اپراتورهای سیستم‌های کشف نفوذ از اطلاعاتی که دیگر اپراتورها در اختیارشان می‌گذارند، سود می‌برند. این اطلاعات می‌تواند مربوط به منابع، روش‌ها و تکنیک‌هایی باشد که حمله‌کننده از آن استفاده می‌کند. اگر این اطلاعات بی‌درنگ در اختیار اپراتورهاقرار گیرد، به بهترین نحو می‌توان از آن استفاده کرد.
- اشتراک‌گذاری امضا: حالت خاصی از این همبسته سازی، شامل، اشتراک‌گذاری امضای حملات خاص و واردکردن این امضاها به سیستم‌هایی است که دیگر اپراتورها آن را اداره می‌کنند. برای مثال، سازمان‌های ارتشی، امضاهایی را توسعه می‌دهند که می‌توانند با گروه‌های صنعتی برای بهبود امنیتشان به اشتراک گذارده شوند.



شکل ۶-۱۰- به اشتراک‌گذاری اطلاعات کشف نفوذ بین سیستم‌ها

در هر کدام از این موارد، سیستم‌های کشف نفوذ متنوع را می‌توان به عنوان ارائه‌دهنده دفاع در عمق برای سرمایه‌های مورد هدف در نظر گرفت. نتیجه، مجموعه‌های هماهنگ شده‌ای از لایه‌های کشف نفوذ است که به حفاظت از زیرساخت ملی کمک می‌کنند. این هماهنگی، معمولاً، نیاز به اشتراک‌گذاری اطلاعات بین مراکز تجزیه و تحلیل و نظارت مختلف دارد. یعنی؛ اگر یک سیستم کشف نفوذ شرایط حمله‌ای نظیر بات‌نت را متوجه شود، می‌تواند اطلاعات این حمله را با سیستم‌های دیگری به اشتراک بگذارد که ممکن است آن‌ها شرایط حمله را کشف نکرده باشند.

(به شکل ۶-۱۰ توجه کنید).

قطعاً، ایده سیستم‌های کشف نفوذ هماهنگ شده، یک ایده جدید نیست. برای مثال، گروه‌ها و کمیسیون‌های امنیت سایبری دولتی، برای سال‌ها، از مفهوم به اشتراک‌گذاری امضا حملات بین دولت و صنعت دفاع کرده‌اند. به هر دلیل، چنین هماهنگی به ندرت اتفاق افتاده است، اما برای حفاظت از زیرساخت ملی، رسیدن به توان کامل بالقوه برای چنین هماهنگی باید تشویق و به آن پاداش داده شود.

برنامه ملی دفاع در عمق

ایجاد یک برنامه هماهنگ دفاع در عمق با استفاده از چندین لایه امنیتی برای زیرساخت ملی می‌تواند فقط با تجزیه و تحلیل ساختاری دقیق تمام سرمایه‌ها و سیستم‌های حفاظتی تضمین شود. تجزیه و تحلیل ساختاری باید منتج به یک نگاشت شود که احتمالاً، با یک ماتریس نمایش داده می‌شود، جایی که در آن هر سرمایه ملی با چند لایه مشخص امنیتی حفاظت شده است. زمانی که این عمل انجام شد، محاسبات ساده‌ای برای تعیین سختی نفوذ با لایه‌های مختلف انجام می‌شود. این کار از آنچه به نظر می‌رسد، آسان‌تر است، برخی از ملاحظات عملی‌تر که در چنین روش عملی ظاهر می‌شوند؛ عبارت‌اند از:

- شناسایی سرمایه‌ها: این یک قدم لازم برای چندین اصل حفاظت از زیرساخت ملی است؛ نظیر؛ فریب دادن که قبلاً توصیه‌شده بودند. این شناسایی، به خصوص برای دفاع در عمق مهم است زیرا تجزیه و تحلیل مؤثر بودن دفاع در عمق تنها می‌تواند از طریق سرمایه‌های شناسایی‌شده به طور خاص اندازه‌گیری شود.
- برآورد ذهنی: در این مرحله، چالش‌های ذاتی به صورت مشروح توضیح داده می‌شود. برخی قراردادها می‌توانند به کارشناسان امنیتی کمک کنند که به برآورد مشترک مؤثر بودن، برسند. در دهه ۱۹۸۰، وزارت دفاع ایالات‌متحده آمریکا مجموعه معیارهایی را که به طور غیررسمی کتاب نارنجی نامیده می‌شود، برای اندازه‌گیری کارآمدی امنیت در سیستم ایجاد کرد. شاید برخی از عناصر این رویکرد، بتوانند معیاری برای ارائه کمک در برآورد ذهنی مؤثر بودن یک لایه معرفی شوند.
- اخذ اطلاعات اختصاصی: اگر در شرکت یا آژانسی سیستم دفاعی برای برخی سرویس‌های ملی ضروری، استقرار یافته است. بدست آوردن اطلاعات مربوط به این سیستم‌های دفاعی برای تجزیه و تحلیل گسترده آن‌ها مشکل

است. هدف باید نشان دادن ارزش برای سازمان‌هایی باشد که این اطلاعات را به صورت مشروح به اشتراک می‌گذارند (اطلاعات دفاعی) حتی اگر این خبر خوبی نباشد.

- شناسایی تمام مسیرهای ممکن دسترسی: شاید سخت‌ترین قسمت هر تمرین امنیت سایبری، شامل تلاش برای تعیین وسایل دسترسی به برخی اهداف باشد. اگر این کار به طور مناسبی انجام نشود، راهبرد دفاع در عمق از هم پاشیده خواهد شد؛ بنابراین، این گام مهم نیاز به توجه ویژه دارد.

این ملاحظات چالش‌های قابل‌ملاحظه‌ای را معرفی می‌کند. بیشتر تیم‌های امنیتی، حتی در محیط‌های با مقیاس وسیع، به ندرت وارد تمرین‌های محلی برای شناسایی شرایط دفاع در عمق می‌شوند. در نتیجه، بیشتر تیم‌های حفاظت از زیرساخت ملی باید برای اولین بار تمرین یافتن مسیرهای ممکن به سرمایه‌های هدف را در چهارچوب یک برنامه ملی انجام دهند.

فصل ۷: احتیاط

روح انگلیسی در راه به میخانه گفت: "رمزنگاری با کلید عمومی؟ شما خیلی بیشتر از ما با آن کار انجام دادید". اعترافی ظاهراً تصادفی که در تقابل با طفره رفتن مؤدبانه‌ای که فرم استاندارد الیس برای پاسخگویی بود. استیون لوی[۱۰]

باوری که در جامعه هکرها وجود دارد، این است که همه اطلاعات باید آزاد باشد و هر کسی که سعی دارد، جریان آزاد اطلاعات را متوقف کند، شیطان است. مشکل این دیدگاه این است که پیشنهاد می‌کند داده‌های حساس شخصی را باید در معرض دید جهانیان قرارداد. این دیدگاه افراطی را هکرها اصلاح کردند و به صورت زیر درآمد:

تمام اطلاعات مرتبط با سازمان‌ها و به خصوص دولت باید آزاد باشد، اما اطلاعات خصوصی افراد، هرگز، نباید افشا شود، زیرا سازمان‌های بزرگ هم از افراد تشکیل‌شده‌اند، و هکرها تقریباً به صورت جهانی علاقه‌مند به حفظ حقوق افراد هستند این دیدگاه از اطلاعات، یک منشور را برای جامعه هکرها ایجاد می‌کند که در آن هر چیزی که باعث تنزل حقوق افراد شود را در معرض دید عمومی قرار می‌دهند.

نتیجه، ایجاد یک فرهنگ هکری است که در آن در معرض دید قرار دادن اطلاعات اختصاصی دولتی و یا متعلق به صنعت در مجله‌های هکرها، وب سایت‌ها و کنفرانس‌ها و در سراسر اینترنت قابل‌قبول فرض می‌شود. هکرها ادعا می‌کنند که گزارش آسیب‌پذیری‌های ملی و تجاری یک خدمت مفید عمومی است که باعث سریع‌تر شدن رفع عیوب امنیتی می‌شود؛ این قطعاً، نشت اطلاعات اختصاصی را که هیچ ربطی به آسیب‌پذیری‌ها ندارد توجیح نمی‌کند. بدون در نظر گرفتن انگیزه، در واقع، اگر هکرها اطلاعات اختصاصی شرکت‌ها و آژانس‌ها را کشف کنند، قطعاً، به صورت گسترده‌ای افشا خواهند کرد. بدتر از آن، این است که تروریست‌ها و جنگجویان اطلاعاتی نیز، برای

مقاصد بدخواهانه خود، نیز به این اطلاعات علاقمند هستند و به ندرت مقاصد خود را به صورت علنی اعلام می‌کنند.

در نتیجه، ابتکارات حفاظت از زیرساخت ملی باید شامل وسایلی برای حفاظت و جلوگیری از نشت اطلاعات حساس باشد. در وهله اول، بهترین رویکرد دوری جستن از آسیب‌پذیری‌ها است؛ زیرا این اطلاعات خواهان زیاد دارند و برای افشا عمومی ارزشمند هستند. با این حال، زیرساخت ملی طیف وسیعی از اطلاعاتی را دارد که دامنه آن از داده‌های بی‌ضرر و شایعات تا داده‌های حساس حیاتی در مورد زیرساخت تغییر می‌کند. این طیف، به برنامه حفاظتی سفارشی و مشتری‌پسندی نیاز دارد که در درجه اول متمرکز بر حیاتی‌ترین اطلاعات باشد. هر پیاده‌سازی عملی باید شامل کنترل‌های امنیتی عملکردی اجباری باشد؛ همچنین، افرادی که این اطلاعات مهم را در اختیاردارند، باید احتیاط کنند. کنترل‌های اجباری باید به صورت مرکزی پیاده‌سازی شوند؛ اما احتیاط باید در فرهنگ محلی تعبیه شود و به صورت توزیع‌شده و فردی رعایت گردد.

۷-۱- پایه محاسباتی مورد اعتماد

جامعه امنیت کامپیوتری، به شناسایی اهمیت احتیاط انسان در معماری ساختی که در سال ۱۹۸۰ به عنوان پایه محاسباتی مورد اعتماد (TCB) معرفی شده است، به بیشترین حد نزدیک گردیده است. تعریف TCB مجموعه سخت‌افزار، نرم‌افزار، فرآیندها و افرادی هستند که عمل و تصمیم‌گیری صحیح آن‌ها برای امنیت کلی سیستم ضروری است. در یک سیستم‌عامل، شامل، فایل‌های سیستم و فرآیندها در هسته سیستم‌عامل می‌شود. در یک سازمان، شامل مدیران امنیتی می‌گردد که بهره‌برداری از سیستم‌های حفاظتی حیاتی را انجام می‌دهند. همچنین، برای یک سازمان، همه سازه‌ها برای مدیریت و ذخیره اطلاعات شناسایی پرسنل (PII) در مورد کارمندان و مشتریان را

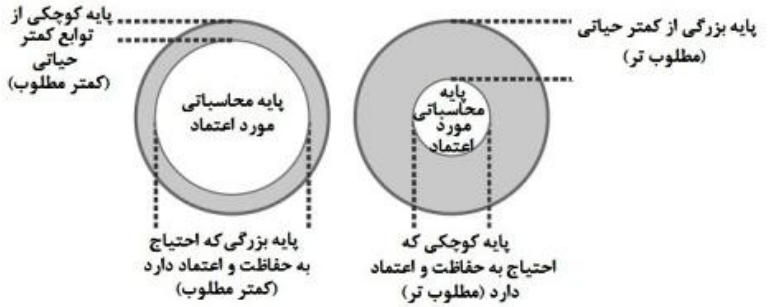
شامل می‌شود. نامزدهای بیرون بردن از لیست TCB، شامل هر چیزی است که نقص، خراب شدن و افشا عمومی آن مشکل آبشاری یا قابل ملاحظه‌ای را ایجاد نخواهد کرد. در زیرساخت‌های مدرن، TCB، به سیستم‌ها، شبکه‌های شرکا و گروه‌های تأمین‌کننده نیز توسعه می‌یابد که تا حد زیادی حفاظت از سرمایه‌های TCB را پیچیده‌تر می‌کند؛ زیرا مرزهای پیرامونی TCB را به محیطی توسعه می‌دهد که کنترل آن مشکل‌تر است.

هدف اولیه هر برنامه احتیاط در حفاظت از زیرساخت ملی، باید اطمینان از این باشد که اطلاعات در مورد عملکرد TCB، عملیات و فرآیندها، در اختیار دید افرادی قرار می‌گیرد که شناخته‌شده و از افشا شدن آن اطلاعات جلوگیری می‌کنند. چنین برنامه‌ای دو جز متمایز را با یکدیگر ترکیب خواهد کرد:

- کنترل‌های اجباری: مکانیزم‌های عملکردی و رویه‌ای هستند که برای اطمینان از این بکار می‌روند که اطلاعات از دسترسی غیرمجاز حفاظت شود، به جز مدیران کلیدی در داخل TCB، هیچ فرد دیگری نباید بتواند کنترل‌های اجباری را دور بزند که معمولاً، شامل دیوارهای آتش، سیستم‌های کشف نفوذ و ظروف عسل هستند.
- سیاست احتیاطی: توصیه‌ها و رهنمودهایی است که یک سازمان برای حفاظت از اطلاعات، به خصوص در مورد TCB، ارائه می‌دهد. معمولاً، احتیاط با نگرانی‌های عملی هدایت می‌شود. هیچ مکانیزم عملی نمی‌تواند مسائلی را کنترل کند که مردم به طور غیررسمی به همکاران و مشتریانشان می‌گویند. تنها راه برای اطمینان از حفاظت، رعایت رهنمودهای احتیاطی است که به وسیله فرهنگ محلی فراهم شده است و می‌تواند با مجازات‌های شدید برای کسانی که آشکارا روح حفاظت اطلاعات مرتبط با TCB را نقض می‌نمایند، تکمیل شود.

همان طور که انتظار می‌رود، حفاظت TCB زمانی در آسان‌ترین وضع قرار دارد که اندازه و پیچیدگی آن کمینه باشد. برای مثال؛ داشتن تعداد کمی افراد که برای حفاظت

از امنیت بتوان به آن‌ها اعتماد کرد، بهتر از داشتن بسیاری از افراد و گروه‌های مختلف است. به طور مشابه؛ از دیدگاه امنیتی، داشتن سیستم‌های با پیچیدگی کمتر که شخص بتواند به آن‌ها اعتماد کند، برای سازمان بهتر است. بنابراین، کمینه کردن TCB یک هدف عالی است، گرچه این موضوع نادیده گرفته می‌شود. در اغلب موارد، شیوه‌های عمل امنیتی، شامل؛ واردکردن برخی سیستم‌های امنیتی جدید است که بزرگ و پیچیده هستند و نیاز به اطمینان کامل دارند. (به شکل ۷-۱ توجه کنید).



شکل ۷-۱- مشکلات مقایسه اندازه در یک پایگاه محاسباتی مورد اعتماد

بنابراین، یکی از ملاحظات عمده در حفاظت از زیرساخت ملی، چگونگی مدیریت، ارتقا و اطمینان از احتیاط مناسب نیروی انسانی حول اطلاعات حیاتی مرتبط با سرمایه‌های TC است. این امر، مستلزم استقرار سیاست‌ها، رویه‌ها و حتی کنترل‌های کارکردی است که برای کمک به انجام شدن چنین احتیاط‌هایی لازم است. پیش از افشا شدن هرگونه اطلاعات مرتبط با TCB که می‌تواند آثار بدی روی امنیت برخی سرمایه‌های ملی بگذارد، انواع سئوالات زیر مورد نظر قرار گیرد:

- کمک: آیا این اطلاعات می‌تواند به دشمن کمک کند که به برخی از جنبه‌های زیرساخت ملی حمله کند؟ برای مثال؛ اگر تروریست‌ها و جنگجویان اطلاعاتی که کشوری از آن‌ها حمایت می‌کند این اطلاعات را داشته باشند؛ می‌توانند مبارزه بدخواهانه‌ای را بر علیه سرویس‌هایی نظیر اورژانس ۹۱۱ شروع نمایند؟
- رفع عیب‌ها: آیا افشای اطلاعات کمکی به شناسایی و رفع عیب امنیتی به صورت مؤثرتر و در زمان کوتاه‌تر خواهد کرد؟ برای مثال؛ آیا افشا اطلاعات به کسی اطلاعاتی خواهد داد که بتواند زمان لازم برای رفع عیب و مشکل را کاهش دهد؟
- حدود: آیا افشای اطلاعات می‌تواند محدود به کسانی باشد که در موقعیت طراحی رفع عیب هستند؟ به طور خاص‌تر، آیا می‌توان اطلاعات را به طور بی سروصدا و در خلوت به گروهی مثل فروشندگان یا ارائه‌دهندگان سرویس که می‌توانند مستقیماً مسئله را حل کنند، ارائه داد.
- قانونی بودن: آیا افشای اطلاعات در محیط محلی یک نیاز قانونی و قراردادی است؟ آیا افشای اطلاعات به برخی دلایل دیگر انجام می‌شود؟ آیا این دلایل دیگر، می‌تواند ارتقا شخصی یا خشم پایمال‌شده نسبت به سازمان به علت حرکت کند آن باشد؟

- آسیب: آیا کسی یا گروهی از افراد از حفاظت و عدم افشای این اطلاعات صدمه و آسیب می‌بینند؟
- نیاز: آیا دیگران برای حفاظت سیستم و زیرساخت خود به این اطلاعات نیاز دارند؟

همان طور که گفته شد، احتیاط و صلاح‌دید مناسب افراد در تفسیر این سئوالات، همراه با تصمیم سازی بعدی برای حفاظت از سرمایه‌های ملی، حیاتی است. در بسیاری از موارد، دولت و سازمان‌ها، اطلاعات مرتبط با بعضی سرویس‌ها و اجزا زیرساخت ملی را درخواست می‌کنند، به خصوص اگر این اطلاعات مربوط به برخی پایگاه‌های محاسباتی مورد اعتماد باشد. تا زمانی که هدف به اشتراک‌گذاری معقول و متمرکز بر بهبود وضعیت باشد، این عمل خوب است. زمانی که دولت یا گروه‌ها، این اطلاعات را برای اهداف نامشخصی (در بدترین حالت، به منظور قدرت، غیبت و شایعات بی‌اساس) درخواست کنند، به اشتراک‌گذاری توصیه نمی‌شود.

در هر صورت، با وجود فرآیندهای امنیتی، ساختارها و سیستم‌هایی که برای حفاظت از سرمایه‌ها استقراریافته‌اند، انسان‌ها یک حلقه حیاتی در زنجیره حفاظت باقی خواهند ماند. در حقیقت، در بسیاری از محیط‌ها، ممکن است انسان‌ها ضعیف‌ترین حلقه زنجیر باشند. به همین دلیل، محتاط بودن در به اشتراک‌گذاری اطلاعات اصل مهمی است.

۷-۲- امنیت از طریق ابهام

مفهوم بسیار بدخیم و ضعیف فهمیده شده امنیت از طریق ابهام، سدی در مقابل احتیاط و صلاح‌دید مناسب است. از هر کارشناس امنیتی بپرسید که در مورد این مفهوم چه فکر می‌کند، این پاسخ محتاطانه را به خصوص از رمزنگاران دریافت می‌کنید که پنهان کردن عمدی اطلاعات برای اطمینان از امنیت، مؤثر نخواهد بود. ادعای آن‌ها

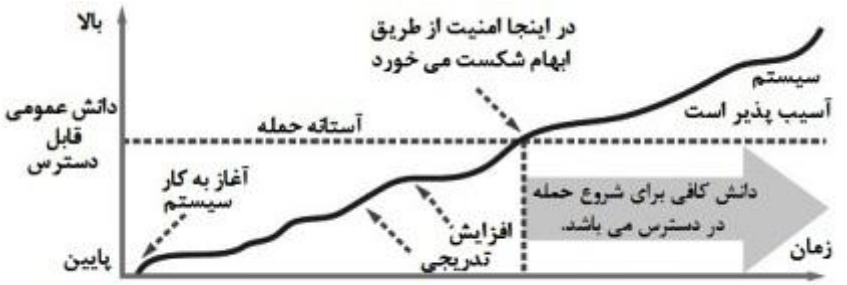
این است که هر کسی سعی در پنهان کردن جزییات طراحی، پیاده‌سازی و یا عملیات را داشته باشد، فقط سعی در پوشاندن عیوب دارد. همچنین، تمام اطلاعات راه خود را به سمت عموم پیدا می‌کنند و تمام وابستگی‌های مربوط به سرکوب اطلاعات سرانجام فرو خواهند ریخت. در دو سناریوی زیرمیتوان قابل اعتراض‌ترین کاربردهای امنیت از طریق ابهام را توضیح داد:

- پنهان کردن درازمدت آسیب‌پذیری ها: اپراتورهای یک سیستم برای امن کردن سیستم، به جای اینکه رویکرد مطلوب تری را انتخاب کنند که در آن آسیب‌پذیری‌ها رفع شود، عیوب قابل سواستفاده خود را می‌پوشانند.
- توقیف اطلاعات به صورت درازمدت: زمانی اتفاق می‌افتد که اپراتورهای یک سیستم هدف، به طور عمدی اطلاعات عمومی سیستم را توقیف می‌کنند تا دشمنان، هکرها و اشخاص ثالث نتوانند به راحتی عیوب سیستم را کشف کنند.

در هر کدام از سناریوهای بالا کنترل اولیه، شامل پنهان کردن اطلاعات است. بیشتر افراد معتقدند که این روش قابل‌اعتماد و درازمدت نیست؛ زیرا اطلاعات توقیف شده سرانجام عمومی خواهند شد. وضعیت می‌تواند به صورت خط زمان دانش نشان داده شود که در نقطه‌ای از زمان اطلاعات سیستم شروع به عمومی شدن می‌کند. با گذشت زمان، افزایش تدریجی در دانش عمومی قابل‌دسترس سیستم اتفاق می‌افتد. اگر این افزایش به نقطه‌ای برسد که اطلاعات کافی برای استفاده از آسیب‌پذیری در دسترس باشد، طرح امنیت از طریق ابهام شکست خورده است. بدیهی است، وقایع مخربی؛ نظیر؛ اطلاعیه‌های هکرها، می‌تواند باعث افزایش ناگهانی دانش عمومی شود. (به شکل ۷-۲ توجه کنید).

امنیت از طریق ابهام برای حفاظت درازمدت به عنوان کنترل اولیه توصیه نمی‌شود، ولی در بسیاری از موارد به عنوان کنترل‌کننده مکمل عالی باقی می‌ماند و در کوتاه مدت به عنوان یک نیاز ضروری برای بسیاری از انواع مشکلات امنیتی در

زیرساخت خواهد بود. به عنوان مثال؛ هیچ کس دلیل قانع‌کننده‌ای برای عمومی کردن اطلاعات ساختار امنیتی یک سازمان ندارد. تا زمانی که طراحی امنیتی تحت نظر متخصصان امنیتی محلی قرار دارد، بهتر است اطلاعات آن عمومی نشود. بدیهی است که هیچ کس نباید امنیت از طریق ابهام را به عنوان کنترل اولیه توصیه کند و از آن برای پنهان کردن عیوب استفاده نماید؛ اما چنین احتیاطی، کار را برای حمله دشمن مشکل می‌کند و ممکن است فرق بین موفقیت و شکست یک حمله توسط دشمن باشد.

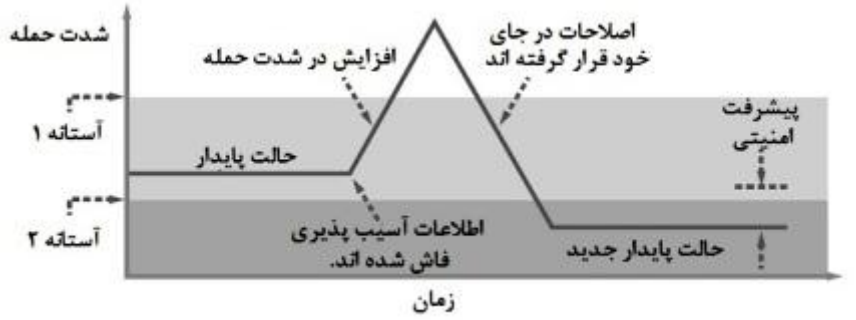


شکل ۷-۲- چرخه عمر دانش برای امنیت از طریق ابهام

به همین ترتیب، اگر عیب قابل سواستفاده‌یی کشف شود که نیاز به توجه فوری داشته باشد، بدترین چیزی که می‌تواند اتفاق بیفتد، اشتراک‌گذاری اطلاعات آن به صورت وسیع خواهد بود. شاید با فرستادن اطلاعات به اینترنت، چنین اتفاقی بیفتد، به علت نگرانی‌های ناشی از روابط عمومی، تهدیدات نزدیک و نگرانی‌های قانونی، واکنش و پاسخ محلی تحریف‌شده خواهد بود. اگر عیوب سیستم با دقت تجزیه و تحلیل شوند و در توسعه‌های مناسب و بعدی چرخه عمر عملیات، جاسازی و تعبیه شوند، راه‌حل‌های فنی مهندسی بسیار بهبود یافته‌تر خواهند بود. همچنین، فرض کنید برای تضمین عملکرد مناسب برخی سیستم‌ها، امنیت کافی وجود داشته باشد و هر آسیب‌پذیری که ممکن است موجود باشد باندازه کافی مهم باشد به طوری که فناوری را به طور معقولی

قابل اتکا ناید، در چنین سیستمی، اگر یک آسیب‌پذیری شدید یافت شود، حالت ثابت جدید می‌تواند به حالت ریسک بالای غیرقابل‌قبول پرش نماید و یکپارچگی و قابل اعتماد بودن عملیات در معرض خطر قرار گیرد. این سیستم، به سادگی، حتی برای زمان کوتاه، برای سرویس‌های ضروری ملی پذیرفته نمی‌شود.

اغلب، استدلال آشنای هکرها، این است که با معرض دید قرار دادن آسیب‌پذیری ها، محل به سرعت تعمیر و آسیب‌پذیری رفع خواهد شد. همچنین، زمانی که در سیستم اصلی رفع عیب جاسازی شود، یکپارچگی سیستم افزایش می‌یابد؛ زیرا عیوب موجود رفع شده‌اند. این یک استدلال قوی و درست است. مسئله این است که در زمانی که آسیب‌پذیری رفع نشده، خطر از یک آستانه قابل گذشت برای سرویس‌های ضروری بالاتر خواهد رفت و باید از آن اجتناب کرد. زمانی که باید یک سرویس ضروری مستقر باشد، معمولاً، منطق سرد جایی نخواهد داشت؛ زیرا یک بیمار حمله قلبی باید کمک دریافت کند و یک مستأجر در داخل شهر، باید برق و گرما دریافت نماید؛ یا اپراتورهای کارخانه برق اتمی، باید بتوانند از شرایط اضطراری خطرناک که می‌توانند فجایع سلامتی جدی‌ای را ایجاد کنند، اجتناب نمایند. (به شکل ۷-۳ توجه کنید).



شکل ۷-۳- چرخه عمر افشا آسیب‌پذیری

بدون در نظر گرفتن شدت حملات، حالت پایدار خاص و آستانه‌های قابل‌قبول، افرادی که مسئولیت حفظ اطلاعات آسیب‌پذیری‌ها را دارند، لازم است که احتیاط مناسب را جهت اطمینان از سطحی از ابهام برای سیستم‌هایشان بنمایند. بدون چنین احتیاط و ابهامی، احتمال اینکه شدت حملات از سطح مطلوبی تجاوز نماید، زیاد خواهد بود و منجر به مسائل جدی خواهد شد. به طور کلی، شیوه عمل باید اجتناب از افشای عمومی آسیب‌پذیری‌ها باشد، تا زمانی که رفع عیب مسئولانه‌ای استقرار یابد. این نشان می‌دهد که افشای اطلاعات آسیب‌پذیری‌ها باید کمینه گردد و منحصر و محدود به کسانی شود که در موقعیت طراحی و جاسازی راه‌حل‌های مناسب هستند.

۷-۳- اشتراک‌گذاری اطلاعات

اطلاعات حساس به طرق مختلف می‌توانند افشا شوند؛ نشت عمدی اطلاعات، اظهارنظرهای پراکنده، دزدی اسناد و افشا توسط هکرها. هر کدام از این اتفاقات می‌تواند برای تیم امنیتی تکان دهنده باشد و به باعث ایجاد احساس کلی ناخرسندی مخصوصاً در محیط زیرساخت ملی شود. یک مسیر اضافی برای افشا اطلاعات حساس؛ شامل؛ به اشتراک‌گذاری عمدی اطلاعات با برخی گروه‌های معتبر و کنترل شده است. درحالی‌که، این یک رویداد قابل پیش‌بینی است و دریافت‌کنندگان این اطلاعات، معمولاً، خیلی خوشحال خواهند شد، گروهی که عمل به اشتراک‌گذاری را انجام می‌دهند، به ندرت، با کل این فرآیند احساس رضایت می‌نمایند.

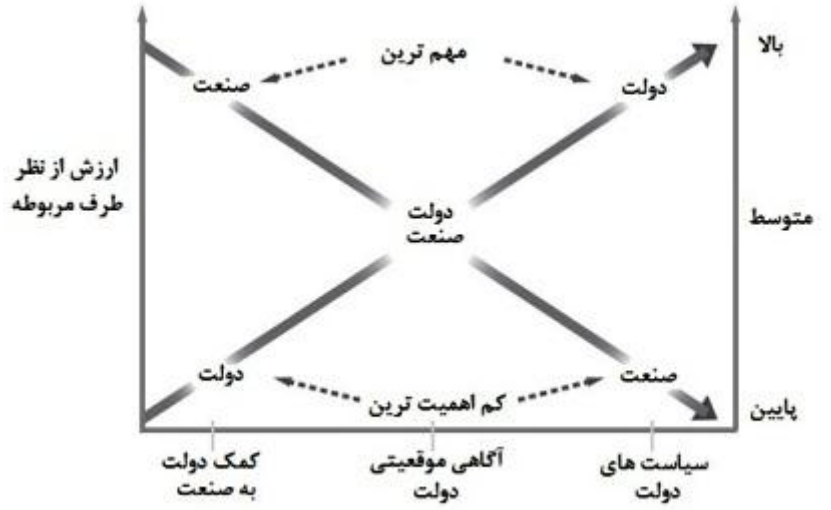
آژانس‌های دولتی در ارتقا به اشتراک‌گذاری اطلاعات از همه تهاجمی‌تر هستند. بدیهی است اگر الزامات قانونی گزارش داده‌ها را دیکته نماید، جایی برای بحث وجود ندارد. برای مثال؛ گروه‌های مجری قانون (پلیس) و تنظیم‌کننده‌های قوانین دولت فدرال (امریکا) به طور منظم این اطلاعات را درخواست می‌کنند. این عمل تحت شرایط شدیداً کنترل شده‌ای انجام می‌شود و هرگز، باعث افشای اطلاعات مرتبط با آسیب‌پذیری‌ها به

دشمن نمی‌شود. با این حال، آژانس‌های دولتی برای امنیت سایبری، از صنایع درخواست می‌کنند اطلاعات حساس را به دلایل زیر به اشتراک بگذارند:

- کمک دولت به صنعت: در تئوری، امضاهای حملات و داده‌های امنیتی مربوطه، تا زمانی که دولت کاملاً از آسیب‌پذیری هایی که ممکن است در زیرساخت‌های تجاری موجود باشد آگاه است، می‌تواند از طریق دولت به صنایع داده شود. و این نیاز به اشتراک‌گذاری اطلاعات از صنایع به دولت دارد.
- آگاهی موقعیتی دولت: برای دولت‌ها، ارزیابی مناسب ریسک امنیت سایبری در سطح ملی به اشتراک‌گذاری اطلاعات از صنعت به دولت را نیاز خواهد داشت.
- سیاست‌ها: گروه‌های دولتی طبیعتاً سیاسی هستند و اطلاعات حساسی را که صنایع ارائه می‌کنند؛ به عنوان نوعی از "ارز قدرت" جهت فشار برای اهداف سیاسی در داخل دولت استفاده می‌کنند. این نکته، به ندرت، بیان می‌شود؛ اما هیچ مسئول دولتی صحت و اعتبار آن را انکار نمی‌کند.

به اشتراک‌گذاری اطلاعات بین دولت و صنعت نتایج نقطه‌ای برای هر دو طرف ایجاد خواهد کرد. برای مثال؛ ایده ارائه کمک امنیت سایبری مستقیم از دولت به صنعت بیشتر نظری است. برای امضای حملات به آسانی می‌توان سناریوهای معتبری را تصور کرد که ممکن است برای گروه‌های ارتشی و اطلاعاتی شناخته‌شده باشند، اما تحقق چنین حمله‌ای به ندرت دیده شده است. به طریقی مشابه، ایده اینکه دولت با استفاده از اطلاعات به اشتراک گذاشته‌شده یک دیدگاه جمعی از خطرات و ریسک‌های امنیت سایبری ایجاد کند، به نظر عالی می‌آید، ولی هرگز، در راه‌های عمومی انجام نشده است. در مقابل، برای بیشتر ابتکارات به اشتراک‌گذاری اطلاعات، اهداف سیاسی، محرک اصلی بوده است که به بیان شور و شوقی کمک می‌کند که در دولت برای انجام این فعالیت وجود دارد. این مسئله شرم‌آور است؛ زیرا از میان تمام انگیزه‌ها، این یکی

برای اپراتور به اشتراک گذارنده داده‌ها کم اهمیت‌ترین می‌باشد. در حقیقت، به نظر می‌رسد که یک رابطه معکوس بین اندازه ارزش مربوطه برای به اشتراک گذارندگان و دریافت‌کنندگان اطلاعات وجود دارد. (به شکل ۷-۴ توجه کنید).



شکل ۷-۴- ارزش معکوس به اشتراک‌گذاری اطلاعات برای دولت و صنعت

رابطه در شکل ۷-۴، نشان می‌دهد که دولت در درجه اول با اطلاعات، در جستجوی قدرت سیاسی است؛ صنعت در این مورد کم‌ترین توجه را دارد و در جایی که صنعت بیشترین سود را از کمک دولت می‌برد، دولت در ضعیف‌ترین موقعیت برای کمک است. دولت و صنعت هر دو معتقدند که برای دولت مهم است که آگاهی موقعیتی از آسیب‌پذیری‌ها را حفظ نماید؛ ولی هیچ‌کدام این موضوع را هدف اصلی خود نمی‌دانند. این رابطه معکوس است که کمک می‌کند بفهمیم چرا ابتکارات به اشتراک‌گذاری

اطلاعات به ندرت مؤثر بوده است. بدون اینکه در مورد مواردی صحبت کنیم که اطلاعاتی که با دولت به اشتراک گذارده شده است، به طور نامرتبی بکار گرفته‌شده اندو شاید حتی اطلاعات به مطبوعات نشت کرده و فقط باعث بدتر شدن کار گردیده است.

در اینجا، توصیه این است که هر انرژی قابل صرف کردنی که در این زمینه موجود است، باید تا حدودی بر مسطح کردن این دو منحنی متمرکز باشد. دولت باید کمتر بر سیاست متمرکز و صنعت باید کمتر نگران گرفتن چیزی در مقابل به اشتراک گذاشتن اطلاعات باشد. نتیجه نهایی این است که اهداف به اشتراک‌گذاری شده باید به طور طبیعی همگرا به سمت اهداف آگاهی موقعیتی توافق شده باشند که گرچه مهم است؛ قطعاً چنان مهم نیست که اجازه دهد تمام توجهات در بحث‌های امنیت سایبری به این مسئله برده شود.

۷-۴- شناسایی اطلاعات

فعالیت‌های اکتشافی شناسایی که دشمن انجام می‌دهد، وسیله دیگری است که می‌تواند اطلاعات حساس را افشا کند. مهم است که تشخیص دهیم، حملات به زیرساخت ملی، همیشه، با برخی از انواع شناسایی همراه است. این شناسایی می‌تواند از راه‌های زیر انجام شود:

- دسترسی از راه دور از طریق اینترنت.
- از طریق کارمندان داخلی که از نظر امنیتی تسلیم‌شده‌اند؛ در سازمان جاسازی‌شده‌اند و به داده‌های حیاتی محلی دسترسی دارند.
- از طریق روش‌های مهندسی اجتماعی.
- از طریق دزدی عمدی، هک از راه دور، خرابکاری آرام و ...

با وجود روش‌ها و دیدگاه‌ها، شناسایی، برای برنامه‌ریزی و آماده شدن برای حمله به زیرساخت بکار گرفته می‌شود.

سطوح برنامه‌ریزی شناسایی

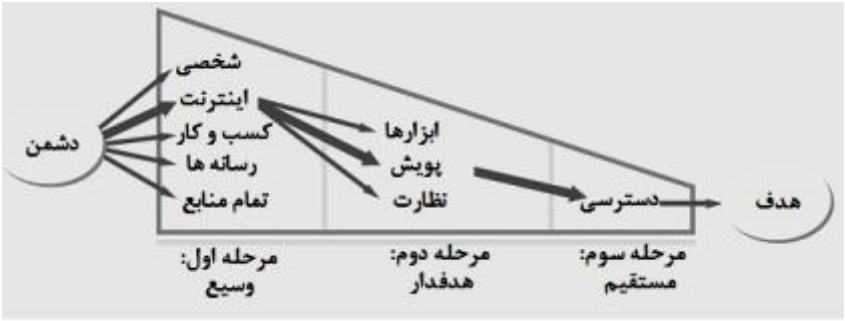
در بیشترین موارد برنامه‌ریزی حملات سایبری، سه سطح از شناسایی در نظر گرفته می‌شود:

۱- اولین سطح شناسایی شامل؛ مجموعه گسترده، با دستیابی وسیع از منابع ممکن مختلف است که می‌تواند شامل جستجوهای وب، تماس‌های شخصی و تعاملات کسب و کاری باشد.

۲- دومین سطح شناسایی؛ شامل؛ مجموعه مورد هدف است که در آن، معمولاً، از امکانات خودکار برای کمک استفاده می‌کنند. پویش (اسکن) شبکه، متداول‌ترین حمایت عملکردی برای سطح دوم شناسایی است.

۳- سطح سوم؛ شامل؛ دسترسی مستقیم به هدف است. یک هک موفق برای نفوذ به برخی سیستم‌ها و به دنبال آن جمع‌آوری داده‌های مورد نظر، مثال خوبی از شناسایی سطح سوم است.

سناریوی ممکن دیگر؛ شامل رشته‌ای از هر سه فاز با یکدیگر است که ممکن است شامل یک شناسایی گسترده باشد جایی که یافتن چیزی در اینترنت باعث شروع فوری شناسایی‌های هدف‌دار بیشتری می‌گردد که می‌توانند شامل فعالیت‌های پویش برای یافتن چیزهایی باشد که می‌توانند برای دسترسی مستقیم به هدف در فاز سوم مورد استفاده قرار گیرند. (به شکل ۷-۵ توجه کنید).



شکل ۷-۵- سه مرحله شناسایی برای امنیت سایبری

این مدل سه مرحله‌ای نشان می‌دهد که در هر مرحله که دشمن در حال جمع‌آوری اطلاعات است، مهندسان امنیتی فرصت دارند در اطلاعات ابهام به وجود آورند. هدف از ایجاد ابهام، سعی در جلوگیری از افشای اطلاعات از طریق فعالیت‌های شناسایی است. انواع خاصی از اطلاعات زیرساخت ملی مرتبط با امنیت وجود دارد که باید در آن‌ها ابهام سازی کرد؛ این اطلاعات عبارت‌اند از:

- ویژگی‌ها: این اطلاعات به ویژگی‌های ظاهراً غیرامنیتی، عملکردها، مشخصات محاسباتی، شبکه‌ای، کاربردها و نرم‌افزارهای مرتبط با زیرساخت ملی مربوط می‌شوند. این اطلاعات می‌تواند مربوط به نوع تجهیزات، اسم فروشنده، اندازه، ظرفیت و عملکردهای پشتیبانی شده باشد. به علت اینکه این اطلاعات زمینه را برای حملات خاصی فراهم می‌نماید، دشمنان به دنبال این اطلاعات هستند.
- حفاظت: این نوع از اطلاعات مربوط به حفاظت امنیتی یک سرمایه ملی است. دامنه این اطلاعات از پیکربندی فنی یا داده‌های تنظیمات در مورد یک سیستم تا اطلاعات تماس‌های غیر فنی برای کارمندان کلیدی اداره‌کننده امنیت تغییر می‌کند. ارزش این اطلاعات آشکار است. زمانی که این اطلاعات به دست دشمن بیفتد، می‌تواند یک نقشه راه برای انواع

مقابله‌هایی را ارائه کند که باید در برنامه‌ریزی موفق یک حمله در نظر گرفت.

- آسیب‌پذیری‌ها: است این اطلاعات مربوط به سوراخ‌های قابل سواستفاده در زیرساخت ملی است. دامنه این اطلاعات می‌تواند از اشکالات نرم‌افزاری شناخته‌شده در سیستم‌های عامل تجاری تا آسیب‌پذیری‌های جدی در برخی از سرمایه‌های ملی تغییر کند. دشمنان از هر منبع ممکن در جستجوی این اطلاعات خواهند بود. این منابع می‌توانند تیم اداره‌کننده زیرساخت ملی، فروشندگان خدمات یا فناوری مرتبط و حتی عموم مردم باشند. جامعه هکرها منبعی غنی از اطلاعات آسیب‌پذیری‌ها مخصوصاً اطلاعات مرتبط با زیرساخت ملی را در اختیاردارند.

در این سه ویژگی، بیشتر اطلاعات مربوط به آسیب‌پذیری هایی است که یک دشمن تمایل دارد آن‌ها را در اختیار داشته باشد. برای مثال؛ اگر به قسمت کتب فنی یک فروشگاه کتاب بروید، می‌توانید کتب ضخیمی را بیابید که در آن‌ها وقایع و تاریخچه سوراخ‌های قابل سواستفاده در هر فناوری شرح داده شده است. بنابراین، پنهان کردن اطلاعات آسیب‌پذیری‌ها بسیار مشکل است. این موضوع نباید اپراتورهای زیرساخت ملی را دلسرد کند. هنگامی که یک مسئله جدی کشف می‌شود که می‌تواند سرویس‌های ضروری را تنزل دهد، تنها عمل مسئولانه حرکت به سمت نوعی مرمت و اصلاح با کمک طرف‌های مسئول است. پیش از اینکه اطلاعات آسیب‌پذیری با بقیه دنیا که بدیهی است شامل دشمنان نیز می‌شود، به اشتراک گذارده شود.

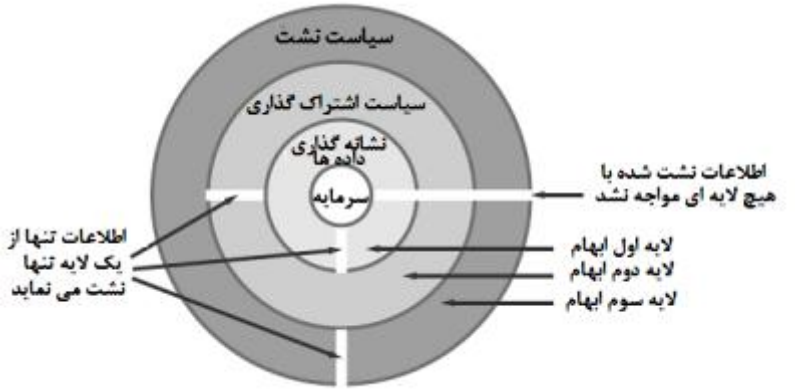
۷-۵- لایه‌های ابهام

یک رویکرد مفهومی به مدیریت احتیاط در حفاظت از اطلاعات زیرساخت ملی شامل لایه‌های ابهام است. این لایه‌ها برای کاهش احتمال افشا اطلاعات حیاتی به افراد

غیرمجاز در نظر گرفته می‌شوند. روش‌های واردکردن لایه‌های ابهام از احتیاط عاقلانه انسانی تا فرآیندهای ساختار یافته تر برای کنترل جریان اطلاعات تغییر می‌کند که اگر به طور مناسبی طراحی شوند، زمانی لایه‌های ابهام افشای غیرمجاز را ممکن می‌سازند که چند روش مختلف ابهام به نحوی دور زده شوند. به این ترتیب، لایه‌های ابهام را می‌توان مواردی از دفاع در عمق در نظر گرفت.

در بهترین حالت، لایه‌های ابهام پوششی متنوع، مکمل و کارآمد در اطراف اطلاعات سرمایه ملی ارائه می‌دهند. به این معنا که یک سرمایه ممکن است با لایه‌ای از ابهام حفاظت شود که شامل نشانه‌گذاری داده‌ها باشد تا به افراد، تعهد آن‌ها به احتیاط را یادآوری کند. لایه دوم ابهام ممکن است شامل نوعی فرمان و تعهد باشد که هیچ اطلاعات فنی در مورد شبکه‌های محلی، نرم‌افزارها یا سکوهای محاسباتی نباید خارج از تیم مدیران مورد اعتماد به اشتراک گذارده شود. لایه سوم ابهام ممکن است شامل فرمانی باشد که اگر به نحوی اطلاعات حیاتی زیرساخت به خارج نشت کرد، سازمان هرگز نباید در هیچ جنبه نشت به صورت عمومی توضیح دهد.

این سه لایه مکمل هم هستند و در مورد اینکه افراد باید چگونه با احتیاط عمل کنند و چه اطلاعاتی می‌تواند به اشتراک گذارده شود، رهنمودهایی ارائه می‌کند. به این ترتیب، این سه لایه ابهام می‌تواند به عنوان وسیله احتیاطی مؤثری برای حفاظت از سرمایه‌ها در نظر گرفته شود (به شکل ۷-۶ توجه کنید).



شکل ۷-۶- لایه‌های ابهام برای حفاظت از اطلاعات سرمایه

نشت اطلاعات از میان لایه‌های ابهام ممکن است راه به بیرون بیابد و یا با یک یا چند لایه ابهام مواجه شود. برای مثال؛ در شکل ۷-۶ نشت اطلاعات که با هیچ لایه‌ای مواجه نمی‌شود ممکن است شامل کسی باشد که با نادیده گرفتن نشانه‌گذاری داده‌ها از نظر احتیاطی ضعیف عمل می‌کند (از طریق لایه اول)، سیاست‌های به اشتراک‌گذاری اطلاعات را نقض می‌نماید (از طریق لایه دوم) و از سیاست‌هایی در مورد افشا اطلاعات بعد از وقوع یک حادثه آگاه نیست (از طریق لایه سوم). این اثر عنصر انسانی در استفاده از احتیاط برای حفاظت از اطلاعات زیرساخت حیاتی را نشان می‌دهد، نمونه‌های دیگری از لایه‌های ابهام در حفاظت از زیرساخت ملی عبارت‌اند از:

- صحبت عمومی: ممکن است سیاستی بکار گرفته شود که به طور عمدی هر شخص مسئولی را در زیرساخت ملی، از صحبت کردن بدون آمادگی و برنامه‌ریزی صریح روابط عمومی منع کند.
- سایت خارجی مصوب: ممکن است یک مکانیزم فراگیر مثل یک وب سایت، به طور ثابت جهت ارائه اطلاعات زیرساخت مصوب شده سازمانی

برقرار گردد تا اطلاعاتی را که ممکن است به وسیله موجودیت‌ها و افراد خارج سازمان مورد درخواست باشد، به آن‌ها ارائه کند.

- جستجو برای نشت: ممکن است موتورهای جستجویی با استفاده از روش‌های هک کردن اخلاقی برای مشخص کردن درجه و قلمرو اطلاعات نامناسب که قبلاً در وب سایت‌ها و حافظه‌های کشه محل یابی شده‌اند به کار گرفته شوند. این را می‌توان با ابزارهای مدرن حفاظت نشت داده (DLP) تکمیل کرد.

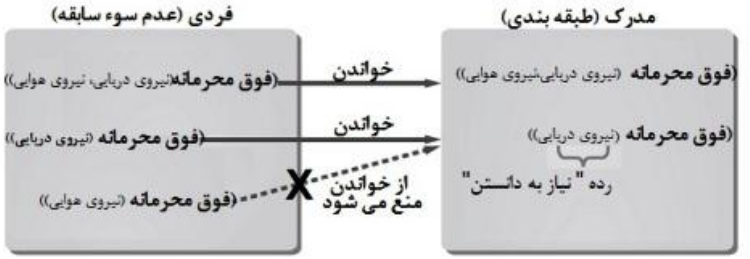
همان طور که در بالا پیشنهاد شد، منظور از کنترل‌های احتیاطی، توقیف اطلاعات برای پنهان کردن بی‌کفایتی یا رفتار نامناسب نیست، هدف کنترل مسئولانه نوعی از اطلاعات است که ممکن است در دسترس دشمن بدخواه قرار.

۷-۶- محفظه‌های سازمانی

یک روش حفاظت از اطلاعات که دولت فدرال ایالات‌متحده امریکا، به طور موفقیت‌آمیزی به خصوص در ارتش و مجامع اطلاعاتی، بکار گرفته است؛ محفظه بندی افراد و اطلاعات می‌باشد. این محفظه‌ها می‌توانند به عنوان گروه‌هایی در نظر گرفته شوند که برای آن‌ها برخی مجموعه‌هایی از قوانین سیاستی به طور یکنواخت بکار گرفته می‌شوند. در مورد افراد به طور معمول از طریق بررسی سوابقشان چک می‌شوند تا میزان قابل‌اعتماد بودنشان تعیین شود. سپس، به آن‌ها گواهی پاکی امنیتی معینی داده می‌شود. در مورد اطلاعات به طریق مشابهی، تجزیه و تحلیل می‌شوند تا سطح بحرانی بودن آن‌ها تعیین شود؛ سپس، طبقه‌بندی امنیتی خاصی برای آن‌ها تعیین می‌گردد.

جزییات چگونگی اعطای گواهی پاکی امنیتی و طبقه‌بندی امنیتی خارج از قلمرو این کتاب است، اما مفهوم کلیدی آن این است که آن‌ها بعضی مفاهیم سلسله مراتبی (برای مثال؛ خیلی سری، سری، محرمانه، طبقه‌بندی نشده) را با یک مفهوم متناظر دسته‌بندی "نیاز به دانستن" (برای مثال؛ در نیروی دریایی و هوایی) ترکیب می‌کنند.

حاصل‌ضرب، مجموعه‌هایی از اطلاعات طبقه‌بندی شده با مجموعه افرادی است که دارای گواهی پاکی امنیتی برای دسترسی به آن اطلاعات هستند را یک محفظه‌ی امنیتی می‌نامند. قوانین سیاستی برای دسترسی به داده‌ها مثل مدارک طبقه‌بندی شده از یک محفظه می‌تواند سپس پیاده‌سازی شود. (به شکل ۷-۷ توجه کنید).



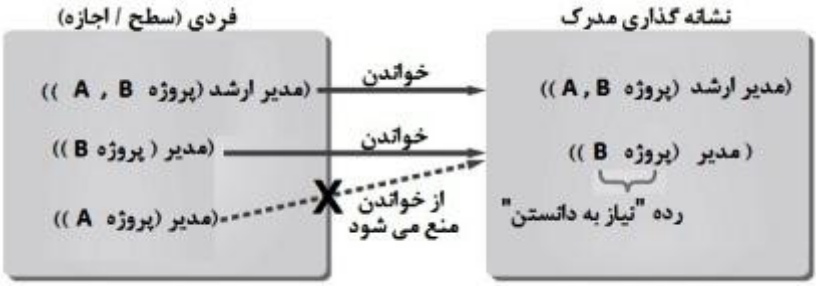
شکل ۷-۷ استفاده از پاکی امنیتی و طبقه‌بندی اطلاعات، برای کنترل افشای اطلاعات

مثال‌های شکل ۷-۷ موارد زیر را نشان می‌دهند:

فردی با گواهی پاکی امنیتی، برای دسترسی به اطلاعات فوق سری در دسته‌های نیروی دریایی و نیروی هوایی به طور موفقیت‌آمیزی مدرکی را در همان سطح و دسته طبقه‌بندی شده می‌خواند. همچنین، فردی که برای مدارک فوق محرمانه در دسته نیروی دریایی گواهی امنیتی دارد، مدرکی را که در همان سطح و دسته قرار دارد، به طور موفقی می‌خواند. از سوی دیگر، فردی که گواهی پاکی امنیتی برای دسترسی به مدارک با سطح فوق سری در دسته نیروی هوایی دارد، از دسترسی به مدارکی که دسته‌بندی آن "فقط نیروی دریایی" است، منع می‌شود. این نوع رویکرد، به ویژه در محیط‌های عملی دولتی غالب است؛ زیرا نشت اطلاعات می‌تواند به عنوان نقض قوانین

دولت فدرال تفسیر شود. در شدیدترین حالت، نقض قانون می‌تواند به عنوان جاسوسی با تمام مجازات‌های مرتبط با آن که از چنین عملی ناشی می‌شود، تفسیر شود. نتیجه، ایجاد محیط رشد یافته‌ای است که برای کاهش احتمال اینکه اطلاعات مرتبط با امنیت ملی نشت کند، در بیشتر محیط‌های دولتی وجود دارد.

بدیهی است که حفاظت از سرویس‌های ملی تنها وظیفه دولت نیست؛ بنابراین، صنعت نیز احتیاج به رویکرد متناظری برای کنترل دسترسی مبتنی بر سیاست دارد. خوشبختانه، ترجمه محفظه‌های دولتی به محیط شرکت‌ها نسبتاً ساده است. گواهی پاکی امنیتی و سطوح طبقه‌بندی می‌تواند به سطوح سازمانی مبتنی بر شرکت‌ها مثل ناظر و مدیر ارشد نگاشت شود. دسته‌بندی می‌تواند به پروژه‌های خاص در یک شرکت نگاشت شود؛ بنابراین، یک محفظه در یک شرکت ممکن است متناظر با سطح مدیر ارشد، در داخل بعضی پروژه‌های A و B باشد. (به شکل ۷-۸ توجه کنید).



شکل ۷-۸- مثالی از نگاشت تجاری گواهی پاکی امنیتی و طبقه‌بندی‌ها

حرف آخر در مورد محفظه بندی این است که باید بتواند محیطی فراهم کند که در حول آن بتوان به اطلاعات دسترسی یافت و تصمیمات محتاطانه‌ای گرفت. در بیشتر مواقع، در محیط‌های امروزی امنیت کامپیوتری، هدف زمینه‌ای بسیاری از پروژه‌ها و در مدیریت بسیاری از سیستم‌های حیاتی، اجتناب از استفاده از اطلاعات مرزی است و این

هدف به خاطر منافع ناشی از باز بودن و به اشتراک‌گذاری می‌باشد. این مفاهیم برای بسیاری از انواع استانداردها، اطلاعات، داده‌ها، نرم‌افزارها و خدمات با ارزش هستند. اما متأسفانه، باز بودن و به اشتراک‌گذاری، همیشه، با حفاظت از اطلاعات مرتبط با امنیت مربوط به زیرساخت ملی سازگار نیستند.

۷-۷- برنامه احتیاط ملی

برای پیاده‌سازی یک برنامه ملی ابهام اطلاعات و احتیاط به چند وظیفه مدیریتی و مهندسی امنیتی نیاز است:

- تعریف TCB: مقامات ملی مناسب، باید تلاش‌هایی در جهت هدایت فعالیت‌های تعریف پایگاه محاسباتی مورد اعتماد در سراسر کشور انجام دهند؛ این عمل می‌تواند مشکل باشد؛ لازمه این کار، هماهنگی بین دولت و صنعت است؛ اما سازه حاصل به هدایت تصمیمات مدیریت امنیت کمک خواهد کرد.
- کاهش تأکید بر به اشتراک‌گذاری اطلاعات: دولت باید فوراً تأکید بر تقاضای خود را که اطلاعات باید به وسیله صنایع به اشتراک گذارده شوند را کاهش دهد. هر ابتکار به اشتراک‌گذاری اطلاعات که چنین تأکیدی را حفظ می‌کند، باید متمرکز بر ارائه اطلاعات حالت وضعیت به دولت باشد.
- همزیستی با جامعه هکرها: جامعه ملی زیرساخت در دولت و صنعت از ایجاد روحیه همکاری با صنعت هک سود خواهند برد. این همکاری، می‌تواند از طریق حمایت مالی گروه‌های هکر و فوروم‌های مربوطه توسط دولت باشد و می‌تواند به طور صریح‌تر؛ شامل؛ ارائه کارهای عملی به آن‌ها در برنامه‌های واقعی باشد.

- مدل لایه‌ای ابهام: یک لایه ابهام ملی برای هدایت تصمیمات در مورد احتیاط انسانی باید در حفاظت از اطلاعات حساس مرتبط با زیرساخت ملی استقرار یابد.
- مدل‌های حفاظت از اطلاعات تجاری: در سازمان‌ها جهت به‌کارگیری درجه‌ای از کنترل دسترسی مبتنی بر سیاست نظیر آنچه در مدل ارتش بکار می‌رود، باید مشوق‌ها و پاداش‌هایی در نظر گرفته شود.

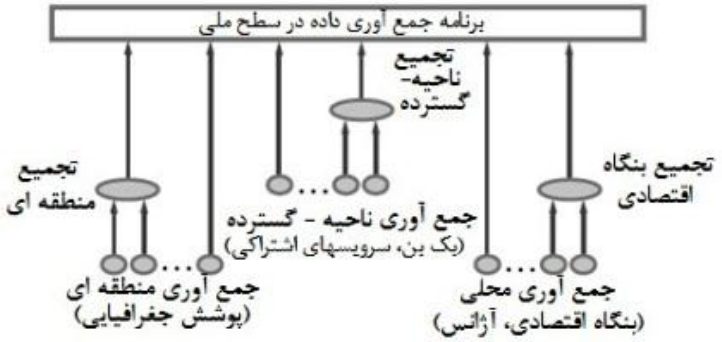
قطعاً، برای افزایش احتمال اینکه این کارها موفق باشند، باید فرهنگ احتیاط نیروی انسانی در حول اطلاعات حساس ایجاد شود. مدیران ارشد باید این فرهنگ را با دور نزدن کنترل‌های اختیاری تقویت کنند. برای مثال؛ تمام مدارک، حتی آن‌هایی که مدیران ارشد تولید می‌کنند، باید به طور مناسبی نشانه‌گذاری شوند. اگر نقض احتیاط اطلاعات پایه‌ای رخ داد، عواقب آن بدون در نظر گرفتن موقعیت یا سطح سازمانی باید اعمال شود.

فصل ۸: جمع‌آوری

مهم است که درک روشنی از چیزی که به دنبال آن هستید و رویدادهایی که به آن علاقه‌مندید داشته باشید؛ زیرا هر چیزی را نمی‌توانید جمع‌آوری و یا کشف کنید استفان نورث کات[۱۱] .

یک اصل پایه‌ای امنیت کامپیوتری، مشاهده سخت کوشانه و مداوم رفتار محاسباتی و شبکه‌ای است که می‌تواند فعالیت‌های بدخواهانه را برجسته کند. این موضوع زمانی به بهترین نحو عمل می‌کند که ناظر یک قاب خوب مرجع برای چیزی که رفتار نرمال و طبیعی را تشکیل می‌دهد، داشته باشد. سپس، ازالگوریتم‌ها و قضاوت انسانی برای مقایسه مشخصات با مشاهدات برای شناسایی فعالیت‌هایی که ممکن است مشکوک باشند بکار گرفته شوند. این تجزیه و تحلیل می‌تواند برای قسمت‌بندی فعالیت‌های مشکوک به دسته‌بندی بی‌خطر و بدخواهانه استفاده شود. تمام این پردازش‌ها و تجزیه و تحلیل‌ها می‌تواند تنها در زمینه یک برنامه موجود جمع‌آوری داده‌ها انجام شود.

در سطح ملی، داده‌های مرتبط با امنیت باید اول در سطح محلی و ناحیه‌ای به وسیله مدیران سپس، زیرمجموعه‌ای از آن‌ها جهت گردآوری وسیع‌تر در داخل یک سیستم جمع‌آوری ملی انتخاب شوند. در برخی حالات، جمع‌آوری محلی و ناحیه‌ای می‌تواند مستقیماً به برنامه‌های ملی وصل شود. نقاط جمع‌آوری با مقیاس وسیع‌تر در شبکه‌های WAN که شاید به وسیله حامل‌ها یا آژانس‌های دولتی اداره، می‌شوند می‌توانند در داخل طرح جمع‌آوری داده‌ها جاسازی‌شده و با موجودیت‌های گردآوری داده محلی، ناحیه‌ای ترکیب شوند. (به شکل ۸-۱ توجه کنید).



شکل ۸-۱- جمع‌آوری داده‌های محلی، ناحیه‌ای و ملی با تجمیع

امروزه، چنین فرآیند جمع‌آوری ملی، به صورت سازماندهی‌شده، وجود ندارد. ساخت چنین مجموعه‌ای به اراده قابل‌ملاحظه‌ای احتیاج دارد. از دیدگاه فنی، هر نقطه جمع‌آوری احتیاج به تصمیم‌گیری در مورد این دارد که کدام داده باید جمع‌آوری شود؛ برای جمع‌آوری از چه روش‌هایی باید استفاده شود و چگونه باید از این داده‌ها استفاده و حفاظت گردد. برای هر سازمان جمع‌آوری هرگونه داده‌هایی، بدون پاسخ‌های مشخص به این سئوالات ساده، کار معقول و منطقی نیست. جمع‌آوری نامناسب داده که در آن هیچ توجیه روشنی برای این گردآوری وجود ندارد، می‌تواند منجر به مشکلات جدی قانونی، سیاسی و یا حتی مسائل عملیاتی برای سازمانی که مسئول حفاظت برخی از سرمایه‌های ملی است، گردد.

به عنوان مثال، در گذشته، بسیاری از گروه‌های دولتی کارهای وحشتناکی در مورد حفاظت از داده‌هایی که گردآوری شده بود، انجام داده‌اند. برای مثال؛ چند سال پیش، اطلاعات حساسی از یک شرکت شیمیایی در نیویورک جمع‌آوری شده بود که در وب سایت یک آژانس دولتی منتشر شد. این اطلاعات را گزارشگرها جمع کرده و به صورت یک مقاله در روزنامه شهر نیویورک چاپ کردند. این مقاله شامل نقشه‌هایی بود که

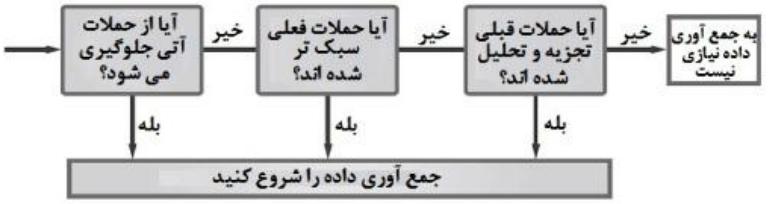
نشان می‌داد چه نوع مواد شیمیایی خطرناکی دقیقاً در کدام نقاط موجودند، همین طور پیامدهای آن‌ها را در سلامتی و بهداشت یادآوری می‌کرد. بدیهی است که تروریست‌ها به این نوع اطلاعات علاقه زیادی دارند. انتشار این اطلاعات می‌تواند تأثیر منفی روی عملیات کسب‌وکار، اعتبار و شهرت این شرکت‌ها داشته باشد.

در هر دو سطح محلی و ملی، تصمیم‌گیری در مورد جمع‌آوری اطلاعات برای زیرساخت‌های ملی باید بر پایه سه هدف امنیتی زیر باشد:

- جلوگیری از حمله: آیا گردآوری داده‌ها در حال حاضر، یا در آینده، به توقف یک حمله کمک خواهد کرد؟ یعنی گیرنده داده‌های جمع‌آوری شده، باید نقش خود را در متوقف کردن حمله توجیه کند. اگر گیرنده داده‌ها، اجزایی از زیرساخت حیاتی شبکه‌های اصلی نظیر بک بن شبکه را مدیریت می‌نماید که می‌توانند برای خفه کردن و متوقف نمودن حمله مؤثر باشند، توجیه بدیهی می‌باشد. ولی اگر گیرنده یک آژانس دولتی باشد، توجیه مشکل‌تر می‌شود.
- کاهش اثر حمله: آیا داده‌های جمع‌آوری شده به واکنش به یک حمله در حال انجام کمک می‌کند؟ یعنی گیرنده داده‌ها باید بتواند آنچه را که در حال اتفاق افتادن است تفسیر کندو به یک راه حل برسد. برای مثال؛ یکی از مرتبط‌ترین پرسش‌ها در مورد حمله در حال انجام این است که حمله تا چه حد ممکن است گسترده باشد؟ جمع‌آوری اطلاعات وسیعی می‌تواند به پاسخگویی به این سئوال کمک کند.
- تجزیه و تحلیل حمله: آیا داده‌های جمع‌آوری شده می‌تواند به تجزیه و تحلیل ادله قانونی (فارنسیک) یک حمله بعد از اینکه حمله اتفاق افتاد، کمک نماید. این یک هدف مهم است، اما می‌تواند به راحتی مورد سواستفاده قرار گیرد؛ زیرا جمع‌آوری هر نوع داده قابل‌دسترسی را توجیه می‌کند.

تجزیه و تحلیل‌کننده‌های ادله قانونی (فارنسیک) مدعی هستند که در صورت وجود حجم زیادی از داده‌ها، کار آن‌ها آسان‌تر می‌شود؛ بنابراین، باید مراقب بود جمع‌آوری داده نامناسبی فقط به خاطر اینکه ممکن است یک تجزیه و تحلیل‌کننده اطلاعات ادعا کند که به اطلاعات احتیاج دارد اتفاق نیفتد.

این سه مورد الزامات باید قلمرو، پوشش و درجه جزییات مرتبط با برنامه جمع‌آوری داده را برای هر جز زیرساخت ملی هدایت کند. در حقیقت، آن‌ها یک قالب مناسب ارائه می‌دهند، برای مشخص کردن اینکه چه نوع داده‌ای باید جمع‌آوری شود. در سطوح محلی، ناحیه‌ای، منطقه وسیع و ملی، جمع‌آوری داده‌ها تنها زمانی باید پیش رود که بتوان جواب‌های مثبتی به این سئوالات داد. (به شکل ۸-۲ توجه کنید).



شکل ۸-۲- قالب تجزیه و تحلیل تصمیمات مبتنی بر توجیه برای جمع‌آوری داده‌ها

تصمیم برای توقف جمع‌آوری داده‌ها ممکن است در میان سخت‌ترین تصمیم‌ها برای هر سازمان به خصوص یک آژانس دولتی باشد. یکی از بزرگ‌ترین بدیهیات برای امنیت کامپیوتر دولتی این بوده است که همیشه، داده بیشتر، بهتر است. به خصوص، اگر مسیری برای جمع‌آوری داده وجود داشته باشد. در واقع، جمع‌آوری نامناسب داده‌ها می‌تواند زیرساخت ملی را تضعیف کند.

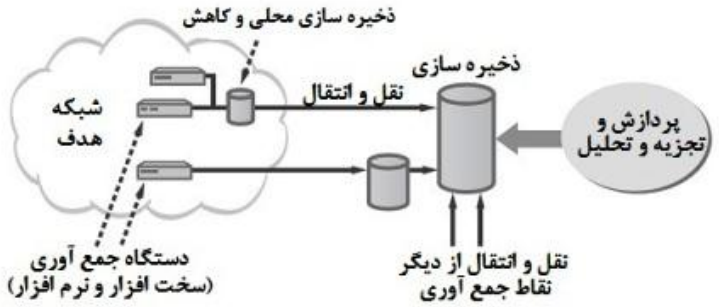
۸-۱- جمع‌آوری داده‌های شبکه

شاید مفیدترین داده‌ها برای جمع‌آوری در زیرساخت ملی متاداده‌های شبکه هستند. همچنین، به عنوان netflow نیز به آن‌ها اشاره می‌شود. متاداده‌ها بسیاری از جزییات امنیتی را در مورد فعالیت‌های شبکه ارائه می‌دهند. در محیط پروتکل‌های TCP/IP، متاداده‌ها به تجزیه و تحلیل‌کننده امنیتی اجازه می‌دهند که آدرس منبع، آدرس مقصد، پرت منبع، پرت مقصد، نوع پروتکل و انواع پرچم‌های موجود در سرآیند را در یک جلسه خاص شناسایی کنند. چنین اطلاعاتی به امنیت نیز مربوط می‌شوند؛ زیرا پایه‌ای برای هر فعالیت تجزیه و تحلیل هستند. یک مقایسه غیر فنی عبارت از این است که متاداده‌ها شبیه اطلاعاتی هستند که کارگران پستی می‌توانند روی پاکت‌های پستی ببینند، در هنگامی که آن‌ها را پردازش می‌کنند. اندازه، وزن، رنگ، بافت و اطلاعات آدرس روی پاکت‌ها و بسته‌بندی‌ها آشکار است، درحالی‌که، اطلاعات داخل آن‌ها معلوم نیست.

جمع‌آوری متاداده‌ها شامل قرار دادن دستگاه‌ها و نرم‌افزارهایی است که برای تولید رکوردهای متاداده در داخل شبکه مورد استفاده قرار می‌گیرند. این رکوردها، جمع‌آوری و ذخیره‌سازی می‌شوند تا دوباره، تجزیه و تحلیل شوند. بدیهی است، برای اینکه جمع‌آوری متاداده‌ها عملی باشد، ملاحظات عملکردی زیادی انجام می‌شود. باید توجیه قانونی برای جمع‌آوری داده‌ها وجود داشته باشد؛ همچنین، باید ظرفیت ذخیره‌سازی کافی برای نگهداری داده‌های جمع‌آوری شده وجود داشته باشد و سرانجام تجزیه و تحلیلگرها با قابلیت‌های مناسب برای اینکه تفسیرها به طور مؤثر و کارآمدی در مورد داده‌ها انجام شود بایستی وجود داشته باشند. شاید مهم‌ترین چیزی که باید در نظر بگیرید، ملاحظه این است که آیا قابلیت جمع‌آوری داده‌ها به اندازه کافی قدرتمند است که بتواند از عهده ظرفیت پهنای باند شبکه مورد هدف برآید.

(به شکل ۸-۳ توجه کنید).

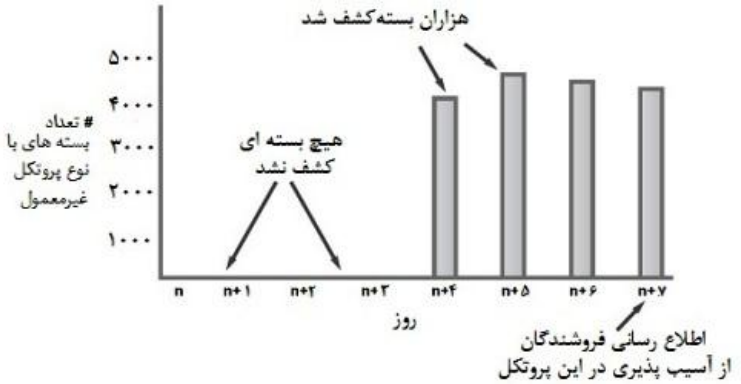
یک مسئله در مورد رویکرد جمع‌آوری در موارد مقیاس خیلی وسیع، این است که بسیاری از سیستم‌های جمع‌آوری متاداده‌ها در زیرساخت شبکه‌های حامل در اوایل این قرن جهت بیرون کشیدن داده‌های امنیتی از بک بون شبکه 10Gpbs بکار گرفته شده‌اند. چالش این است که حامل‌های بک بن شروع به رشد نموده‌اند و ظرفیت آن‌ها به 40 تا 100Gpbs رسیده است. در صورتی که سیستم‌های جمع‌آوری با نرخ متناسبی افزایش نیابند، توانایی گردآوری متاداده‌ها ده برابر کاهش می‌یابد.



شکل ۸-۳- شما تیک عمومی جمع‌آوری داده‌ها

راه‌حلی که بسیاری از تحلیلگران امنیتی، برای مقابله با افزایش ظرفیت شبکه، بکار می‌برند، نمونه‌برداری از داده‌ها است. این روش؛ شامل؛ نمونه‌برداری از داده‌ها در فواصل زمانی از پیش تعیین شده است، طوری که جریان ورودی داده‌ها با توانایی پردازش همسان گردد. معمولاً، داده‌های نمونه‌برداری شده برای تجزیه و تحلیل وسیع فعالیت‌های شبکه پذیرفته می‌شوند؛ اما برای فارنسیک با جزییات مشروح، به اندازه متاداده‌های نمونه‌برداری نشده مؤثر نیستند. در یک محیط نمونه‌برداری نشده، تحلیلگر می‌تواند ناهنجاری کوچکی را در حجم عظیمی از داده کشف کند. این ملاحظات طراحی، در فرآیند جمع‌آوری کلی تأثیر خواهد داشت.

به عنوان مثال؛ چند سال پیش، متاداده‌های نمونه‌برداری نشده در یک شبکه بک‌بن IP به تحلیلگر اجازه می‌داد که در یک محیط حامل جهانی تعداد کمی بسته را از یک پروتکل غیرمعمول کشف کند. سال ها، بسته‌هایی از این نوع در شبکه بک بن دیده نشده بودند؛ بنابراین، این یک ناهنجاری آشکار بود که باید بررسی می‌شد. بسته‌های مشکوک از این واقعه غیرمعمول جمع‌آوری شد و برای چهار روز مورد نظارت قرار گرفت، تا اینکه یک فروشنده کلیدی دستگاه‌ها با شرکت حامل تماس گرفت و یک عیب امنیتی جدی را در سیستم‌عامل خود گزارش داد. جالب است که نرم‌افزارهای استفاده کننده از این آسیب‌پذیری ترافیکی، دقیقاً، همین پروتکل را می‌فرستادند؛ بنابراین، نقطه جمع‌آوری، شواهد فعالیتی را در شبکه کشف کرده بود که مرتبط با مسئله امنیتی بود که هنوز گزارش نشده بود. (به شکل ۸-۴ توجه کنید).



شکل ۸-۴- سیستم جمع‌آوری، شواهدی از آسیب‌پذیری را قبل از مطلع شدن را کشف می‌نماید

در شرایط عادی، هیچ موردی از این بسته پروتکل در حامل بک بن مشاهده نشده بود. زمانی که این پروتکل به طور ناگهانی و غیرعادی مشاهده شد، هیچ راه توجیه ساده‌ای برای تعیین علت آن وجود نداشت، جز اینکه یک نوع ناهنجاری اتفاق افتاده

است. هنگامی که فروشنده‌ای مشکل را در مورد این پروتکل گزارش داد، تحلیلگران توانستند اطلاعات را کنار هم قرار دهند و بفهمند که چرا این ناهنجاری اتفاق افتاده است. این مثال؛ اهمیت یکپارچه کردن تمام اطلاعات منابع را در یک محیط جمع‌آوری داده نشان می‌دهد. حفاظت از زیرساخت ملی باید دارای این نوع جمع‌آوری و تجزیه و تحلیل مربوطه باشد تا بتواند به صورت مؤثر از خدمات ضروری حفاظت کند.

۸-۲- جمع‌آوری داده‌های سیستم

ابتکارات حفاظت از زیرساخت ملی، به طور سنتی، شامل تمهیداتی برای جمع‌آوری داده‌ها از کامپیوترهای خیلی بزرگ، سرورها و کامپیوترهای شخصی نمی‌باشد. توجیه حذف چنین قابلیتی بر اساس موضوعات مقیاس و اندازه که به طور ذاتی در حجم عظیمی از داده قرار دارد که باید از کامپیوترها گرفته و پردازش شوند، می‌باشد. چنین سیستم‌هایی، داده‌های مرتبط با امنیت چندانی ارائه نخواهند داد. ملاحظه‌ای که باید در نظر گرفته شود، توان بالقوه برای سواستفاده از داده‌های حریم خصوصی است؛ این مسئله برای شهروندان بیشتر کشورها مهم است. تا امروز، برای حفاظت از زیرساخت ملی هیچ برنامه جدی‌ای پیشنهاد نشده است.

با توجه به موضوعات مقیاس و اندازه، زیرساخت محاسباتی لازم برای جمع‌آوری داده از کامپیوترهای بسیار بزرگ، سرورها و کامپیوترهای شخصی که بخشی از خدمات زیرساخت ملی تلقی شود، باید خیلی پیچیده باشد. بر اساس دانسته‌های مورخان محاسباتی بی‌سابقه نیست که الزامات پیچیده برای یک نسل کامپیوتر، ویژگی عادی در نسل‌های بعدی آن گردد. همچنین، رویکرد تاکتیکی شناسایی زیرمجموعه‌ای از کامپیوترهای مرتبط قابل کار در سطح ملی امکان‌پذیر است. به عنوان مثال؛ مجموعه کامپیوترهای خیلی بزرگ، سرورها و کامپیوترهایی را که می‌توان در شرکت‌ها و آژانس‌هایی که مسئول اداره زیرساخت ملی هستند به عنوان هدف جهت جمع‌آوری داده‌ها قرارداد و این چالش را می‌توان کنترل کرد.

آیا کامپیوترهای خیلی بزرگ، سرورها وکامپیوترهای شخصی، اطلاعات امنیتی مناسبی را برای حفاظت از زیرساخت ملی ارائه می‌کنند؟ بسیاری از وقایع بحرانی به بهترین نحو توسط جمع‌آوری داده‌های آن‌ها شناسایی شده است. لاگ‌های سیستم عامل، خلاصه رویدادهای کامپیوترهای خیلی بزرگ و رکوردهای تاریخچه کامپیوترهای شخصی شواهد عالی را در مورد فعالیت‌های بدخواهانه‌ای که ممکن است در حال انجام باشد، ارائه می‌کنند. متریک‌های اندازه‌گیری مهندسی نظیر استفاده از حافظه و بار پردازشی می‌توانند علائم ارزشمندی از موضوعات امنیتی ارائه دهند. برای مثال؛ زمانی که یک سرور افزایش استفاده از پردازنده را به عنوان نتیجه یک حمله نشان می‌دهد، وجود این حالت را به آسانی می‌توان با ابزارهای نظارتی جاسازی‌شده در سیستم‌عامل کامپیوتر شناسایی کرد.

با وجود دیوارهای آتش، سیستم‌های کشف نفوذ و دیگر ابزارهای امنیتی، نظارت بر سیستم‌های حفاظت از زیرساخت ملی مهم است؛ زیرا معمولاً نظارت تنها عملکردی است که یک واقعه امنیتی در حال انجام را نشان می‌دهد. در نتیجه، ابتکارات حفاظت از زیرساخت ملی باید تمهیداتی برای جمع‌آوری و پردازش داده‌های حاصل از کامپیوترهای خیلی بزرگ، سرورها و کامپیوترهای شخصی داشته باشند. این داده‌ها باید انتخاب، جمع‌آوری و با حفاظت مناسبی انتقال و در محیطی که اندازه آن مناسب حجم عظیمی از داده است، ذخیره و به صورت بی‌درنگ و زمان واقعی پردازش شوند. کادر زیر چهار نوع خاص از اطلاعاتی را لیست می‌نماید که باید جمع‌آوری شوند.

بالاترین چهار زمینه جمع‌آوری داده

- بهره‌برداری: یکی از متریک‌های مهم در تعیین اینکه آیا حمله‌ای در حال انجام است، مشخصات بهره‌برداری از سرورها در محیط محلی می‌باشد. مدیران سرمایه‌های ملی باید سرورهایی را شناسایی کنند که مناسب

نظارت هستند و برای جمع‌آوری داده‌ها برنامه مرتبطی را تجهیز نمایند. برای این کار، به همکاری بین دولت و صنعت و همچنین، گنجانیدن الزامات عملکردی مناسب در قراردادهای حمایت از زیرساخت نیازاست.

- میزان استفاده: برای برقرار کردن حفاظت از زیرساخت، شناسایی الگوهای میزان استفاده در کامپیوترهای خیلی بزرگ، سرورها و کامپیوترهای شخصی در یک کشور (ملت) خاص مهم هستند.
- کاربردها: جمع‌آوری داده‌هایی در مورد برنامه‌های کاربردی ساکن در یک سیستم زیرساخت، به اطلاعات مفیدی در مورد حملات سایبری ممکن اشاره می‌کند. یک متریک اندازه‌گیری رایج عبارت از لیست ۱۰ کاربرد اولی است که معمولاً، بیشتر از همه استفاده می‌شوند. اگر ترکیب آن‌ها (لیست ده‌تایی) تغییر کند، نشانه یک حمله است. سیستم‌های دروازه شبکه و پروکسی‌های آن‌ها، نامزدهای عالی برای جمع‌آوری این نوع داده‌ها برای یک بنگاه تجاری هستند. حامل‌ها نیز می‌توانند این نوع داده را برای WAN (شبکه‌های پهنه گسترده) یا یک ناحیه خاص ارائه دهند.
- قطع شدن سرویس: اطلاعات مربوط به قطع شدن برای امنیت مهم است؛ زیرا وقایعی که به نظر بی‌خطر می‌رسند، ممکن است قسمتی از یک حمله سایبری باشند و برای مدیران سیستم غیرمعمول نیست که از این، امکان چشم‌پوشی کنند؛ بنابراین جمع‌آوری داده‌ها در مورد قطع شدن مهم است. به عنوان مثال؛ تجزیه و تحلیل علل ریشه‌ای پس از قطع شدن‌های جدی باید به عنوان اطلاعات مهم برای جمع‌آوری و تجزیه و تحلیل در نظر گرفته شوند.

در تعبیه داده‌های مدیریت سیستم در زیرساخت امنیت سایبری، دو روش مفید هستند. اول؛ برای شناسایی سیستم‌هایی که در یک محیط خاص حیاتی فرض می‌شوند،

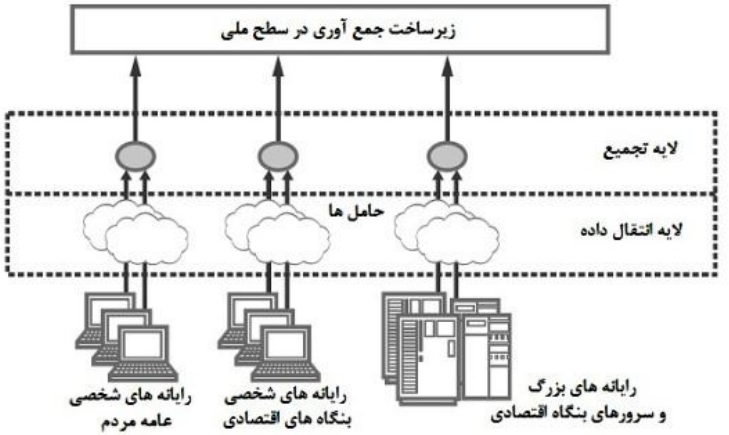
فرآیندی مورد نیاز است. این فرآیند، ممکن است نیاز به تجزیه و تحلیل مهندسی در سراسر زیرساخت صنعتی و دولتی مربوطه داشته باشد تا بتواند تعیین کند که یک سیستم خاص در مسیر بحرانی برخی سرویس‌های ملی قرار دارد. با روشی دیگر، در مورد حیاتی بودن سیستم‌ها می‌توان با جمع‌آوری اطلاعات از هر سیستمی که در مجموعه در دسترس است، تصمیم گرفت. دوم؛ برای آن دسته از سیستم‌هایی که ارزش جمع‌آوری اطلاعات را دارند، باید یک فرآیند تجهیز یا استفاده مجدد از امکانات جمع‌آوری داده شناسایی شود. این فرآیند می‌تواند استفاده از دنباله‌های ممیزی سیستم‌عامل یا نصب نوعی برنامه‌های لاگ کردن در سطح کاربردها باشد.

بدون در نظر گرفتن این رویکرد، داده‌ها باید از کامپیوترهای هدف مورد نظر در طول رسانه شبکه به نقاط مختلف جمع‌آوری داده‌ها جریان داشته باشند. شبکه‌های محلی و سازمانی باید پیش از به اشتراک‌گذاری داده با خارج، قابلیت جمع‌آوری اطلاعات برای سازمان خود را ایجاد نمایند. می‌توان انتظار داشت که حامل‌های شبکه به راحتی نقش ارائه‌کنندگان خدمات انواع مختلف جمع‌آوری داده را ایفا کنند. یعنی؛ مشتریان DSL و خدمات کابلی می‌توانند با توجه به مشوق‌های مناسب با جمع‌آوری داده‌های مربوط به وجود بد افزار، ویروس‌ها و دیگر نرم‌افزارهای نقض‌کننده امنیت موافقت نمایند. می‌توان از رمزگذاری برای حفاظت از داده‌های محرمانه در حال عبور یا در حال ذخیره شدن استفاده کرد.

باید برای تمرکز بر جمع‌آوری داده‌های مورد علاقه از سیستم‌های خاص و محدود کردن داده‌ها تنها به آن‌هایی که می‌توانند مفید باشند، نوعی از فیلتر یا کاهش‌دهنده داده‌ها را ایجاد کرد. برای مثال؛ اگر ملتی سعی در جمع‌آوری داده‌های مرتبط با امنیت از صدها، هزاران یا میلیون‌ها کامپیوتر شخصی در هر روز نماید، نتیجه، جریانی از داده‌ها در محدوده اندازه چندین ترابایت خواهد بود. پایگاه‌های داده تجاری برای ذخیره‌سازی این حجم داده کافی نیستند؛ بنابراین، پایگاه‌های داده سفارشی نیاز است.

در نهایت، حجمی از داده‌های جمع‌آوری شده در دسترس سیستم‌های پردازش و تفسیر امنیتی قرار می‌گیرند و از نتیجه کار آن‌ها برای اهداف زیرساخت ملی استفاده می‌شود.

برای جمع‌آوری اطلاعات، می‌توان ساختارهای خلاقانه‌تری؛ نظیر؛ نقطه به نقطه را تصور کرد؛ اما رویکرد با جمع‌آوری متمرکز، احتمال بیشتری برای پیاده‌سازی دارد؛. این رویکرد جمع‌آوری متمرکز با استقرار یک مرکز عملیات امنیت ملی کاملاً سازگارتر است. (به شکل ۸-۵ توجه کنید).



شکل ۸-۵- جمع‌آوری داده از کامپیوترهای خیلی بزرگ، سرورها و کامپیوترهای شخصی

برای مثال؛ هر سازمان بزرگ یا آژانس دولتی به طور منظم نرم‌افزار مدیریت یکپارچگی؛ نظیر قابلیت Tripwire را در کامپیوترهای بزرگ یا سرورهای خود تعبیه می‌کند. همچنین، تقریباً تمام سازمان‌ها و آژانس‌ها از عوامل نرم‌افزاری در کامپیوترهای شخصی برای جمع‌آوری داده‌های مرتبط با امنیت و مدیریت استفاده می‌کنند. (ممکن است اپراتورهای باتنت نیز ایده جمع‌آوری داده‌ها از تعداد عظیمی از کامپیوترهای

کاربران انتهایی را به منظور یک حمله، کامل کرده باشند.) ایده توسعه این طرح کلی به حفاظت خیرخواهانه زیرساخت ملی به نظر ساده و آسان می‌رسد.

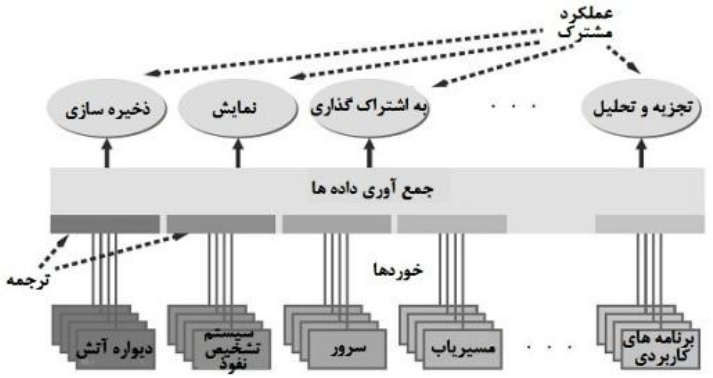
چالش این نوع طرح‌ها در این است که می‌توانند مورد سواستفاده قرار گیرند. دانشمندان کامپیوتری از اجرای یک برنامه با ارجحیت بالا در سیستمشان ناراحت خواهند بود. شهروندان در مقابل این ایده که یک ناظر ناشناس داده‌ها را از سیستم آن‌ها به یک مرکز جمع‌آوری داده‌ها ببرد و احتمالاً اصول حفظ حریم خصوصی آن‌ها را نقض نماید، مقاومت می‌کنند. هر دو این نگرانی‌ها به‌جاهستند و باید در مورد آن‌ها بحث کرد. اگر دولت با تجار و شهروندان به یک مصالحه قابل‌قبول برسند، می‌تواند یک سیستم مناسب ملی طراحی کند. چنین مصالحه‌ای، حداقل باید شواهد قابل‌مشاهده‌ای داشته باشد، در مورد اینکه کامپیوترهای خیلی بزرگ، سرورها و کامپیوترهای شخصی تنها اطلاعات مرتبط امنیتی را که بدون زیان است ارائه می‌دهند؛ نظیر؛ داده‌های اسکن، حالت امنیتی و کشف بد افزارهای مبتنی بر امضا. هر چیزی بانفوذ بیشتر که اجازه دسترسی یا اجرا از راه دور از یک ایستگاه مرکزی را بدهد، پذیرفته نمی‌شود، حتی اگر سازمان‌ها این کار را به طور منظم با پایگاه داده کارمندان خود انجام دهند.

احتمال دیگر؛ ممکن است، نوعی از فعالیت‌های جمع‌آوری داده که اساس حمایت شهروندان و توسط خود شهروندان برای کامپیوترهای شخصی و سرورها در نظر گرفته می‌شود باشد، شرکت‌کنندگان برای ارائه اطلاعات امنیتی به داشتن یک سیستم توزیع‌شده عظیم از نقاط توافق کنند. چنین سیستمی با پیرامون سیاسی یا جغرافیایی یک ملت منطبق نیست و بسیاری از شهروندان بر اساس اصولی از شرکت در آن اجتناب می‌کنند. تعداد کمی از شرکت‌کنندگان در شبکه‌های با عضویت عظیم که برای توزیع موزیک و ویدئو هستند، در مورد پیامدهای حریم خصوصی ناشی از اجرای چنین نرم‌افزارهایی روی کامپیوترشان که معمولاً سئوال برانگیز و غیرقانونی است، شکایت می‌کنند. آن‌ها، معمولاً، از گرفتن محتواهای مجانی لذت می‌برند. این ایده که یک سازه شبیه به این می‌تواند برای کمک به امن کردن زیرساخت ملی بکار رود، نیاز به نشان

دادن نوعی سود و منفعت به شرکت‌کنندگان خود دارد که ممکن است مقدور نباشد؛ اما از دیدگاه امنیتی، این تلاش باارزش است، زیرا داده‌های جمع‌آوری شده از به‌کارگیری گسترده کامپیوترها در سراسر یک کشور داده‌شده، پنجره ارزشمند و بی‌بدیلی از وضعیت امنیتی زیرساخت ملی را ارائه می‌کند.

۸-۳- اطلاعات امنیتی و مدیریت رویداد

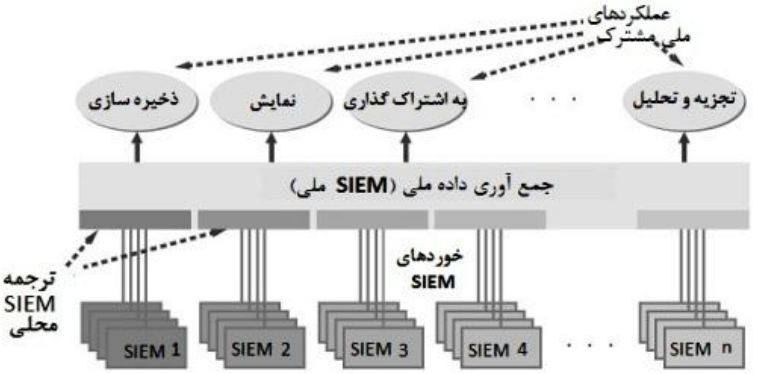
فرآیند تجمیع داده‌های سیستمی از منابع گوناگون، به منظور حفاظت، در مجامع امنیت کامپیوتری با عنوان اطلاعات امنیتی و مدیریت رویداد یا (SIEM) شناخته می‌شود. امروزه، ابزارهای SIEM را که مجموعه وسیعی از فناوری‌ها را دارند می‌توان از فروشندگان مختلفی خرید. این مجموعه، شامل؛ دیوارهای آتش، سیستم‌های کشف نفوذ (IDS)، سرورها، روترها و کاربردها است. تقریباً، تمام بنگاه‌های تجاری و آژانس‌های دولتی به نوعی از SIEM استفاده می‌کنند. می‌توان قابلیت توسعه‌یافته‌ای برای SIEM تصور کرد که جمع‌آوری اطلاعات امنیتی از سرورها، کامپیوترهای بزرگ و کامپیوترهای شخصی را نیز به عهده گیرد. (به شکل ۸-۶ توجه کنید).



شکل ۸-۶- ساختار عمومی SIEM

سیستم‌های SIEM دارای عملکردهای ترجمه کننده برای گرفتن خروجی‌های اختصاصی، لاگ‌ها و رشته‌های هشدار از فروشندگان مختلف و تبدیل آن‌ها به یک فرمت مشترک هستند. با این فرمت جمع‌آوری مشترک، می‌توان مجموعه‌ای از کارهای مشترک را انجام داد که شامل؛ ذخیره‌سازی، نمایش، اشتراک‌گذاری و تجزیه و تحلیل داده‌ها است. حفاظت از زیرساخت ملی، باید ابزارهای منطقی برای تفسیر داده‌های SIEM که از اجزا زیرساخت به دست می‌آید داشته باشد، زیرا بسیاری از سازمان‌ها از قبل سیستم SIEM را مستقر کرده‌اند تا داده‌های جمع‌آوری شده محلی آن‌ها را پردازش کند. به علت این حقیقت که بیشتر به‌کارگیری‌های موجود SIEM در شرکت‌ها و آژانس‌های دولتی متقابلاً سازگار هستند، تفسیر داده‌های SIEM که از منابع مختلف جمع‌آوری شده‌اند، پیچیده هستند. مشکل بحرانی دیگر، تمایل نداشتن بیشتر مدیران امنیتی برای تجهیز اتصال بی‌درنگ سیستم SIEM خود به سیستم جمع‌آوری ملی است. مشکل بعد، این است که در حال حاضر، ارائه‌دهندگان سرویس، داده‌های خروجی مشتریان مصرف‌کننده خود را به سیستم‌های محلی SIEM نمی‌خورانند.

به هر حال، تصور ساختار یک سیستم ملی جمع‌آوری داده با استفاده از قابلیت SIEM سخت نیست. هر سیستم SIEM به طور عملکردی می‌تواند برای جمع‌آوری، فیلتر کردن و پردازش داده‌های جمع‌آوری شده محلی استقرار یابد و داده‌های خروجی آن برای به اشتراک‌گذاری در سطح ملی در نظر گرفته شوند. این داده‌های فیلتر شده می‌توانند به صورت رمزگذاری شده از طریق شبکه به نقطه تجمیع که خود دارای قابلیت SIEM است، فرستاده شوند. در نهایت، عملکرد SIEM در سطح ملی استقراریافته و داده‌های رسیده از نواحی و نقاط تجمیع محلی و سازمان‌ها پردازش می‌شوند. در این نوع ساختار، سیستم‌های SIEM محلی می‌توانند به عنوان منابع داده فرض شوند، همان طور که دیوارهای آتش، سیستم‌های کشف نفوذ و شبیه به آن‌ها در محیط محلی SIEM در نظر گرفته می‌شوند (به شکل ۸-۷ توجه کنید).



شکل ۸-۷- ساختار عمومی SIEM ملی

متأسفانه، بیشتر مدیران زیرساخت‌های محلی با ساختاری که در شکل ۸-۷ نشان داده شده است، به چند دلیل موافقت نمی‌کنند. اول: آشکار است که برای استقرار این ساختار، هزینه‌هایی وجود دارد و معمولاً، این بودجه‌ها به وسیله گروه‌های دولتی در دسترس قرار نگرفته است. ثانیاً: ممکن است قابلیت SIEM جاسازی‌شده، مشکلات عملکردی در محیط محلی ایجاد کند و با قلاب‌های SIEM که در سیستم تعبیه می‌شود، می‌تواند استفاده از پردازنده را در سیستم افزایش دهد؛ مخصوصاً در نقاط دروازه با داده‌هایی که ممکن است از نقاط جمع‌آوری وارد آن‌ها شوند، می‌توانند محیط شبکه را پر ازدحام و مسدود کنند.

مسئله بحرانی‌تری که در ایده به‌کارگیری SIEM در مقیاس ملی وجود دارد، این است که بیشتر مدیران امنیتی سازمان‌ها و آژانس‌های دولتی هرگز با این ایده موافق نیستند که داده‌های حساس امنیتی از محل سازمانشان بیرون برده شود. ارائه‌دهنده خدمات امنیتی مدیریت شده، باید داده‌های امنیتی را در یک مکان دور بپذیرد و پردازش نماید. این یک ترتیب خصوصی بین کسب‌وکار و تأمین‌کننده سرویس امنیتی است. تجزیه و تحلیل داده‌ها فقط برای سودرسانی مستقیم به محیط منشأ آن انجام

می‌شود. همچنین، توافقنامه سطح خدمات را که معمولاً، شرایط تعامل را مشخص می‌کند، فقط سازمان یا آژانس متقاضی خدمات می‌تواند فسخ کند. هیچ راه حل خوبی برای پیاده‌سازی SIEM ملی وجود ندارد، جز جمع‌آوری داده به صورت ملی که منجر به امنیت ملی بهتری می‌گردد و برای همه سودمند خواهد بود.

۸-۴- روند در مقیاس وسیع

اساسی‌ترین روش پردازشی که برای داده‌های جمع‌آوری شده از سراسر زیرساخت ملی بکار می‌رود، شناسایی روندها است. در بسیاری از موارد، این روندها در داده‌های جمع‌آوری شده دیده می‌شود. نظیر؛ روند افزایش حجم داده‌های جمع‌آوری شده یا بسته‌های تحویل داده‌شده به شبکه. با این حال، ممکن است در موارد دیگر روندها خیلی آشکار نباشند. به عنوان مثال، زمانی که فرآیند جمع‌آوری و سیستم‌های نظارتی تغییراتی را تجربه می‌کنند، ممکن است شناسایی روند ساده نباشد. اگر شبکه تحت نظارتی در حال رشد، اما سیستم جمع‌آوری داده‌ها خوب عمل نکند، ممکن است داده‌های حساس از دست بروند به طریقی مشابه؛ اگر تغییراتی در سیستم‌های اساسی جمع‌آوری داده‌ها انجام شود که ممکن است این تغییر، اضافه کردن فناوری جدید و فروشنده دستگاه‌های دیگری باشد؛ این تغییر می‌تواند در روندی که احتمالاً قابل مشاهده است، تأثیر بگذارد.

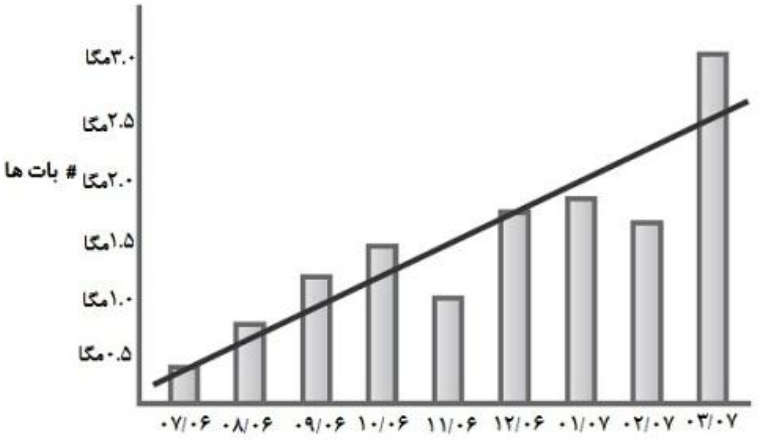
در ساده‌ترین سطح، یک روند شامل برخی ویژگی‌های کمی مانند بالا رفتن (رشد)، پایین رفتن (کاهش)، ماندن در همان سطح (تسطیح) و یا هیچ‌کدام (غیرقابل‌پیش‌بینی) می‌باشد. برای مثال؛ زمانی که داده‌ها بالا پایین می‌روند، گرفتن نتیجه آسان نیست؛ اما خود تغییر داده‌ها می‌تواند نتیجه مهم و مفیدی باشد. شاید رایج‌ترین سئوالی که مدیران زیرساخت در مورد امنیت می‌پرسند، این است که آیا حملات در قسمتی از زیرساخت، افزایش و یا کاهش‌یافته؛ یا به همان مقدار سابق باقیمانده است؟ مدیران

اجرایی و نمایندگان مجلس ملی به این سئوال در مورد روند حملات علاقه دارند. فقط با توجه به محتوای داده‌های جمع‌آوری می‌توان به آن جواب دقیقی داد.

به عنوان مثال؛ در طول یک دوره نه ماهه از ژوئن ۲۰۰۶ تا مارس ۲۰۰۷ یک سیستم جمع‌آوری پایدار که در بک بن ارائه‌دهنده خدمات جهانی تعبیه شده بود، افزایشی در رفتار، سازگار با بات‌های بدخواه را کشف کرد. همان طور که در بخش یکم توضیح داده شد، یک بات تکه‌ای از نرم‌افزار است که در یک کامپیوتر شخصی تعبیه شده است و معمولاً، با ارتباط باند وسیع به شبکه وصل می‌شود؛ و نرم‌افزار تعبیه‌شده با اهداف بدخواهانه و سئوال برانگیر در داخل آن قرار می‌گیرد. از بات‌ها ممکن است برای حمله به بعضی اهداف، یا فرستادن هرزنامه، یا دزدیدن اطلاعات شخصی استفاده شود. کشف رفتار بات ها، با جمع‌آوری اطلاعات ترافیکی، به منظور شناسایی ارتباطات بین تعدادی کامپیوترهای شخصی کاربران انتهایی و تعداد کمتری سرور روی اینترنت به دست می‌آید.

با جمع‌آوری شواهد از رفتار بات‌ها و پردازش نتایج در یک هیستوگرام ساده، رشد بات‌ها به وضوح دیده می‌شود و بر اساس آن مدیریت محلی تصمیم می‌گیرد.

(به شکل ۸-۸ توجه کنید).



شکل ۸-۸- روند رشد رفتار بات‌نت در طول دوره ۹ ماهه (۲۰۰۷-۲۰۰۶)

بیشتر مدیرانی که به آن‌ها روند رشد مطابق شکل ۸-۸ نشان داده شده است، نتیجه‌گیری کرده‌اند که بات‌ها تهدید فزاینده‌ای را در طی این دوره زمانی نشان می‌دهند. با این حال، پیش از اینکه نتیجه واقعی گرفته شود، حفاظت مناسب زیرساخت ملی نیاز به تجزیه و تحلیل دقیق‌تر دارد. در زیر برخی از ملاحظات عملی پایه‌ای که تحلیلگران امنیتی، پیش از اینکه به روند هر چارت جمع‌آوری داده اعتماد کنند باید در نظر بگیرند، در زیر آورده شده است:

- زمینه جمع‌آوری: تعجب‌آور است که داده‌های روند مانند آنچه در شکل ۸-۸ نشان داده شده است، معمولاً، در چهارچوب یک ساختار جمع‌آوری که ممکن است تغییر کند ارائه می‌شود. برای مثال، اگر یک سیستم جمع‌آوری داده برای بات‌ها از طریق بهبود الگوریتم و یا پوشش کامل‌تر، به طور دقیق‌تری عمل کند، رشدی که ممکن است در بات‌ها مشاهده می‌شود، به سادگی استفاده مؤثرتر از ابزارهای کشف بات را منعکس می‌کند.

- داده‌های داوطلبانه: داده‌هایی است که سازمان‌های دولتی و تجاری جهت اخذ نتیجه در مورد روندهای رایج، داوطلبانه در اختیار دیگران می‌گذارند. این‌گونه نتیجه‌گیری‌ها خطرناک است؛ زیرا هیچ کنترل ضعیفی در مورد چگونگی جمع‌آوری و مدیریت این اطلاعات وجود ندارد. ممکن است که داده‌ها نادرست بوده؛ یا دست‌کاری شده باشند و با مقاصد بدخواهانه و شیطانی به طور داوطلبانه داده‌شده باشند.
- پوشش مناسب: میزان پوششی از محیط که داده‌ها از آن جمع‌آوری می‌شوند، در معتبر بودن یک روند مشاهده‌شده تأثیر خواهد گذاشت. برای مثال؛ یک سازمان کوچک با یک ارتباط اینترنت، با استفاده از داده‌های این ارتباط در مورد روندهای ترافیک شبکه نتیجه‌گیری کند. قطعاً، دیدگاه این شرکت کوچک نسبت به یک شرکت حامل جهانی در مورد روند ترافیک کمتر جذاب خواهد بود.

تفسیر داده‌هایی که مدیران زیرساخت ملی جمع‌آوری می‌کنند، اهمیت اخذ یک رویکرد به بلوغ رسیده را با توجه به موارد فوق برجسته می‌کند. این مسئله‌ی به‌خصوص بسیار مهم است؛ زیرا اطلاعات مربوط به روند، اختصاص دادن منابع حیاتی و بودجه را به دنبال دارد. برای مثال؛ متخصصان در سطح ملی، باتجربه امنیتی به موارد متعددی اشاره می‌کنند که در آن‌ها نوعی از روند برای تخصیص بودجه به یک ابتکار و فعالیت برای پیشبرد موردشان مؤثر بوده است؛ (مانند؛ جنجال کرم‌ها).

برای مثال؛ گزارش شده است که کرم Conficker، نوعی از حمله جاسازی‌شده را داشت که باید در تاریخ اول آوریل سال ۲۰۰۹ اتفاق می‌افتاد. Conficker، مهم بود و هنوز هم مهم است؛ زیرا عملیات آن دربرگیرنده چند میلیون بات است. Conficker، را در مجامع امنیتی به عنوان یک بات‌نت قدرتمند می‌شناسند. بیشتر کارشناسان امنیتی می‌دانند که در کد برنامه Conficker چیزی که باعث به وجود آمدن واقعه‌ای در تاریخ معینی شود، وجود ندارد. اما تاریخ و زمان حمله پیش‌بینی‌شده وسیله راحت، رایج و

متداولی برای جلب توجه است. حفاظت از زیرساخت ملی به شدت خواهان رویکرد پخته‌تری برای تفسیر بخش عمومی از داده‌های جمع‌آوری شده است.

۸-۵- ردیابی یک کرم

جمع‌آوری داده‌ها وسیله‌ی عالی برای ردیابی یک کرم است. یک کرم برنامه‌ای است که سه کار مهم انجام می‌دهد:

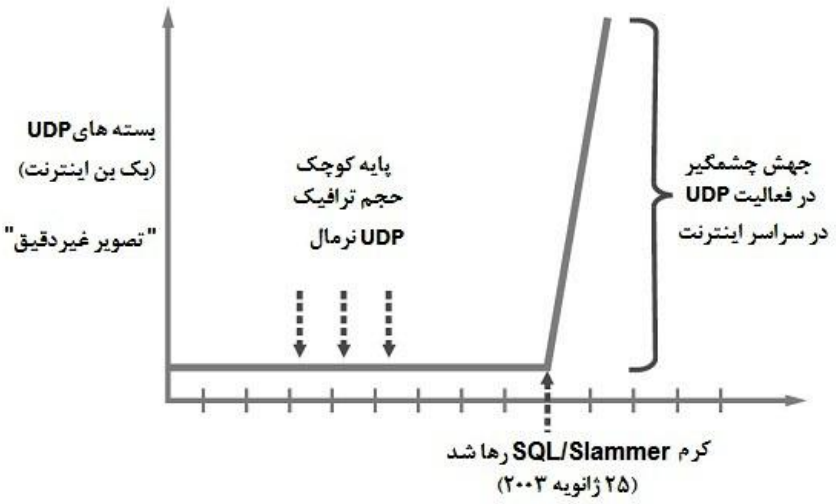
۱- در شبکه، کامپیوترهایی را پیدا می‌کند که می‌توانند یک کپی از برنامه کرم را بپذیرند.
۲- یک کپی از برنامه خودش را به کامپیوتری که درشبکه شناسایی کرده است، می‌فرستد.
۳- کپی راه دور خود را در کامپیوتر هدف از راه دور اجرا می‌کند و واکنش زنجیره‌ای را شروع می‌نماید که در آن شناسایی، کپی کردن و اجرای از راه دور کپی برنامه به طور نامحدود و بی‌پایانی ادامه خواهد داشت.

با جمع‌آوری متاداده‌های شبکه، در همان حال که انتشار کرم در حال انجام است، تحلیلگران امنیتی عموماً می‌توانند تعیین کنند که کرم چکار انجام می‌دهد و این واقعه چقدر جدی است. در بهترین حالات، جمع‌آوری متاداده‌ها حتی اشاراتی را که می‌توانند جهت توقف کرم از گسترش بیشتر مورد استفاده قرار گیرند ارائه می‌کنند که بدیهی است که این برای امنیت زیرساخت ملی جذاب است.

در سال‌های ۲۰۰۳ و ۲۰۰۴، اینترنت تعداد زیادی از وقایع مرتبط با کرم‌ها را به طور غیرمعمولی تجربه کرد. این عمدتاً به علت فرآیندهای ضعیفی بود که در آن زمان برای وصله زدن نرم‌افزارهای سیستم‌عامل و نرم‌افزارهای سطح کاربرد وجود داشت. مسئله وصله زنی، برای هر دو نوع سیستم، سیستم‌های سازمانی و کاربران خانگی با ارتباط باند وسیع به شبکه درست بود. در این دوره زمانی، کرم‌ها یکی پس از دیگری در

سراسر اینترنت می‌خروشیدند و بیشتر ناظران این وقایع را بیشتر خود به خودی در نظر می‌گرفتند. همه گمان می‌کردند که کرم‌ها در چند دقیقه گسترش می‌یابند و جمع‌آوری داده‌ها بی‌فایده است. اگر قرار بود یک کرم کامپیوتر شما را آلوده کند، به زودی کامپیوتر را آلوده می‌کرد و نمی‌توانستید از پیش، هیچ کاری برای توقف این واقعه انجام دهید.

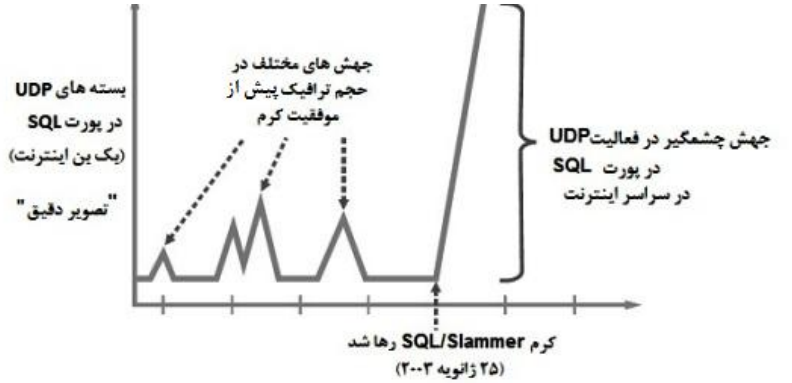
واقعیت وضعیت زیرکانه‌تر بود. برای مثال؛ کرم SQL/Slammer در ژانویه ۲۰۰۳، یکی از کرم‌هایی بود که تأثیر خود به خودی روی ترافیک داشت. دقایقی که در طی آن به نظر می‌رسید که کرم به طور قابل‌ملاحظه‌ای گسترش یافته است. بسته‌های ترافیک UDP یا پروتکل دیتا گرام کاربران از مقدار کم و قابل پیش‌بینی با حجم ناهنجاری کم به طور ناگهانی به حجم بالایی افزایش یافت. در نگاه اول، اتفاق به گونه‌ای بود که باعث هیچ اخطاری نمی‌شد و هیچ زمانی برای آماده سازی و واکنش به حادثه موجود نبود. (به شکل ۸-۹ توجه کنید).



شکل ۸-۹- تصویر غیر دقیقی از ترافیک UDP از کرم SQL/Slammer (با اجازه از Dave Gross و Brian Rexroad)

به علت وجود کرم SQL/Slammer حجم بسته‌ها، به طور ناگهانی و بدون هشدار افزایش یافت. با امتحان دقیق‌تر می‌توان بسته‌های UDP را یافت که منجر به این واقعه شده و با خود نشانه‌ها و هشدارهایی از نظر امنیتی حمل می‌کردند. در اوایل ژانویه ۲۰۰۳، حجم بسته‌های UDP برای پرت‌های SQLخاص، که به وسیله کرم استفاده می‌شد، رفتار ناهنجاری را نشان دادند. در دوم ژانویه ۲۰۰۳، اولین افزایش ناگهانی بسته‌های UDP اتفاق افتاد و سه هفته بعدی رفتار غیرعادی مشابهی را به دنبال داشت. با مطالعه ترافیک در این دوره زمانی پیش از حمله، می‌توان به طور قطعی نتیجه‌گیری کرد که این افزایش‌های ناگهانی، تلاش‌های اولیه برای تولید کرم بوده‌اند، ولی هیچ کس نمی‌تواند تغییر جدی را در رفتار UDP در اینترنت پیشنهاد کند.

(به شکل ۸-۱۰ توجه کنید).



شکل ۸-۱۰ تصویر ریز و دقیق افزایش ترافیک ناشی از کرم SQL/Slammer (با اجازه از Dave Gross و Brian Rexroad)

بررسی دقیق و مشروح رفتار UDP در درگاه‌های ورودی SQL، پیش از اینکه کرم SQL/Slammer به هدفش برسد، می‌توانست اطلاعات باارزشی به مهندسان امنیتی بدهد. به خصوص اینکه آسیب‌پذیری که کرم SQL/Slammer از آن سواستفاده می‌کرد، در آن زمان شناخته شده بود؛ گرچه بیشتر مدیران امنیتی در نصب وصله نرم‌افزاری آن سهل‌انگاری کرده بودند. اگر در آن زمان اطلاعات شکل ۸-۱۰ به طور گسترده‌ای منتشر شده بود، هر کسی که به اندازه کافی عاقل بود، این وصله را نصب می‌کرد و از صدمات کرم SQL/Slammer در امان می‌ماند. از دیدگاه حفاظت از زیرساخت ملی پیامدهای این وضعیت باید آشکار باشد.

۸-۶- برنامه جمع‌آوری ملی

پیاده‌سازی یک برنامه جمع‌آوری داده ملی برای امنیت زیرساخت نیاز به ترکیبی از ابتکارات گسترده دسترسی عمومی دارد، پیش از اینکه سازه‌ها با مقیاس وسیع استقرار یابند. شهروندان و جامعه کسب‌وکار باید هدف، استفاده، کاربری و

کنترل‌های مرتبط با سیستم جمع‌آوری را به طور کامل درک کنند. مکانیزم‌هایی برای جلوگیری از سواستفاده از داده‌های جمع‌آوری شده مربوط به حریم خصوصی باید بالاترین ارجحیت بحث‌های تعبیه‌شده در هر ساختار پیشنهاد شده را داشته باشد. خصوصیات اینکه چه چیزهایی در این بحث‌ها باید تأثیر بگذارند، خارج از محدوده این کتاب است. هیچ برنامه جمع‌آوری ملی نمی‌تواند بدون انجام این قدم موفق باشد.

هنگامی‌که پذیرش عمومی برای ایجاد یک برنامه جمع‌آوری داده ملی به دست آمد، موضوعات فنی و ساختاری زیر باید در نظر گرفته شود؛

- منابع داده‌ها: از نظر ملی باید توجه شود که کدام منابع داده‌ای برای امنیت اطلاعات در عملیات جمع‌آوری گسترده با ارزش تلقی می‌شوند. آشکار است که مهم‌ترین این منابع کامپیوترهای بزرگ و سرورهای مهم سازمان‌ها و آژانس‌هایی می‌باشند که مسئول حفاظت از زیرساخت هستند. به سختی می‌توان کامپیوترهای شخصی را که متعلق به کاربران انتهایی بوده و شهروندان خصوصی از آن‌ها استفاده می‌کنند، جز منابع مهم داده در نظر گرفت.
- حفاظت از جابه‌جایی و انتقال داده‌ها: داده‌های جمع‌آوری شده مرتبط با امنیت از منابع شناسایی‌شده احتیاج به انتقال و جابه‌جایی از طریق شبکه‌های مناسب با رمزنگاری کافی دارند. ملاحظات در مورد اندازه می‌تواند محدودیت‌هایی را روی حجم اطلاعاتی اعمال نماید که آن اطلاعات از یک منبع خاص به دست می‌آید.
- ملاحظات ذخیره‌سازی: بدیهی است که حجم اطلاعات جمع‌آوری شده قابل‌کنترل است، اما اشتها برای دریافت داده‌های تحلیلگران امنیتی نامحدود است؛ بنابراین، فشار برای ماکسیمم کردن مقدار اطلاعات و

همین طور افزایش طول زمانی که داده‌ها برای تجزیه و تحلیل در دسترس باشند، وجود دارد.

- تأکید بر کاهش داده‌ها: در همه ابتکارات ملی برای جمع‌آوری داده‌ها زمان و انرژی باید به سمت کاهش حجم داده بکار گرفته شود. بدیهی است ممکن است که یک روش جمع‌آوری داده به طور غیر عمد اطلاعات بیشتری ازآنچه مورد نیاز است جمع‌آوری کند و یا اطلاعاتی را که هیچ ارتباطی به چالش امنیتی ندارند گرد آورد.

هر یک از این موضوعات به خصوص در موارد اندازه و مقیاس، چالش فنی را نشان می‌دهند؛ ولی می‌توان با مهندسی مناسب، آن‌ها را در یک سیستم معقول ترکیب کرد. رویکرد کلی از روش اصلاح گام به گام سودمند خواهد برد، این رویکرد ابتدا با یک زیرمجموعه قابل‌کنترلی از منابع داده‌ای شروع می‌کند، به تدریج با گذشت زمان این مجموعه بزرگ‌تر می‌گردد.

فصل ۹: همبسته سازی

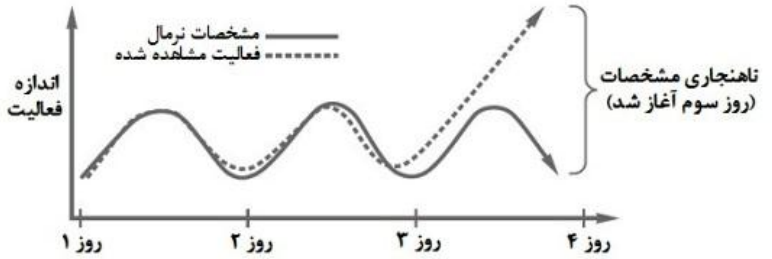
یک استفاده‌ی از کشف ناهنجاری این است که می‌تواند حملات پیش‌بینی‌نشده را کشف کند و محدودیت آن این است که به سختی می‌تواند رفتار نرمال را از رفتار غیر نرمال تشخیص دهد. دو روتی دنینگ[۱۲].

کارشناسان امنیت کامپیوتری و شبکه، همبسته سازی را به عنوان یک روش تحلیلی قدرتمند در دسترس، برای بررسی تهدیدات می‌شناسند. برای مثال؛ سیستم‌های کشف نفوذ، فقط هنگامی مفید هستند که رشته‌های هشدار که از امضاها یا پردازش های مبتنی بر مشخصات نتیجه می‌شود را بتوان با داده‌های زمینه های دیگر همبسته نمود. زمانی که به هشدارها به صورت ایزوله نگاه کنیم، استفاده محدودی دارند. این محدودیت در پردازش هشدارها، مستقیماً مربوط به پیچیدگی محیط مورد هدف می‌باشد، یعنی تصمیم گیران در محیط‌های پیچیده نسبت به محیط‌های محدودتر بیشتر متکی بر همبسته سازی داده‌های جمع‌آوری شده هستند. بنابراین، حفاظت مناسب زیرساخت ملی بسیار وابسته به برنامه هماهنگ شده‌ای است که اطلاعات تمام منابع در دسترس را همبسته سازی می‌نماید.

از دیدگاه بنیادی، چهار روش تحلیلی متمایز برای همبسته سازی اطلاعات امنیتی در دسترس هستند. همبسته سازی مبتنی بر مشخصات، همبسته سازی مبتنی بر امضا، همبسته سازی مبتنی بر دامنه و مبتنی بر زمان.

- همبسته سازی مبتنی بر مشخصات: شامل مقایسه مشخصات نرمال و طبیعی فعالیت‌های هدف با الگوهای فعالیت‌های مشاهده شده است. اگر تفاوت اساسی بین مشخصات طبیعی و مشخصات مشاهده‌شده وجود داشت، یک نفوذ احتمالی را نشان می‌داد. بدیهی است، حالت‌های بسیاری

وجود دارد که در آن فعالیت‌های مشاهده‌شده طبیعی نیستند؛ ولی این حالت‌ها، نفوذی را نشان نمی‌دهند. برای مثال، وب سایت‌هایی که در حال اجرا و یا حمایت تعاملات مخصوص با زمان محدود هستند، افزایش ناگهانی ترافیک را در دوره‌های زمانی محدود خواهند دید که با الگوی طبیعی ترافیک آن‌ها مطابقت ندارد. با این حال، از دیدگاه امنیتی ناهنجاری‌های همراه با مشخصات فعالیت مهم هستند.
(به شکل ۹-۱ توجه کنید).

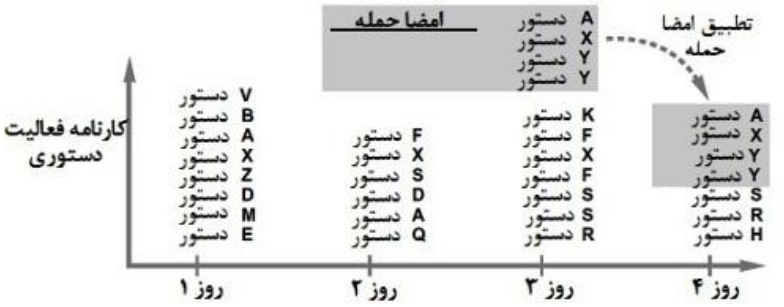


شکل ۹-۱- ناهنجاری فعالیت مبتنی بر مشخصات

- همبسته سازی مبتنی بر امضا: مقایسه یک الگوی امضا مربوط به برخی شرایط بدخواهانه شناخته‌شده با فعالیت‌های مشاهده شده است. اگر این دو مطابقت داشته باشند، اطمینان بالایی برای در جریان بودن یک نفوذ وجود دارد. چالش زمانی ایجاد می‌شود که فعالیت مشاهده شده مشخصاتی را با یک امضا به صورت مشترک داشته؛ ولی به صورت دقیق مطابقت نداشته باشند در اینجا به سعی و کوشش تیم امنیتی برای متمرکز باقی ماندن نیاز است. بیشترین الگوهای همبستگی مبتنی بر امضا دنباله‌ای از رویدادها هستند، مثل فرمان‌هایی که به صورت امضا گسسته تعریف

شده‌اند و با لاگ فعالیت‌های مشاهده شده مقایسه می‌شوند برای مثال؛ نرم‌افزار ویروس کش، الگوریتم‌های ضد هرزنامه و سیستم‌های کشف نفوذ، همگی، به این ترتیب عمل می‌کنند.

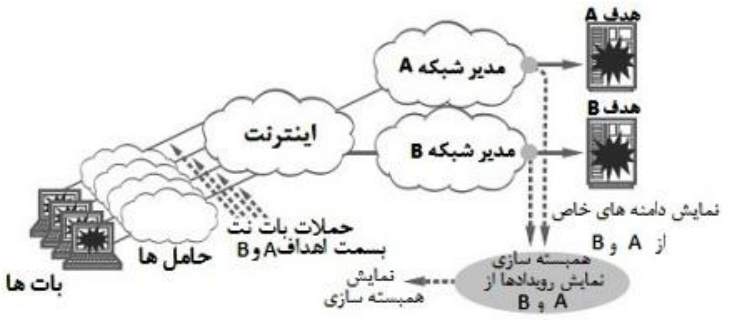
(به شکل ۹-۲ توجه کنید).



شکل ۹-۲- مطابقت فعالیت مبتنی بر امضا

- همبسته سازی مبتنی بر دامنه: مقایسه داده‌های یک دامنه با داده‌های جمع‌آوری شده در یک زمینه کاملاً متفاوت است. تفاوت‌های مرتبط در محیط‌های جمع‌آوری داده‌ها شامل محیط‌های محاسباتی، ساختار نرم‌افزاری، فناوری شبکه، مشخصات کاربردها و نوع کسب و کاری است که پشتیبانی می‌شود. برای مثال، داده‌هایی که یک شرکت برق در مورد یک حمله به آسانی می‌تواند جمع‌آوری کند، با داده‌هایی که یک آژانس غیرنظامی فدرال در مورد این حادثه جمع‌آوری می‌کند، کاملاً متفاوت است. به همین ترتیب، دو هدف یک حمله باتنت می‌توانند دیدگاه‌های ایزوله شده متفاوتی را گزارش دهند که می‌تواند به صورت یک دیدگاه مشترک همبسته گردد. این به سازماندهی از پیش انتقال، جمع‌آوری و

رویکرد تجزیه و تحلیلی نیاز دارد که ما را به سمت خروجی همبسته سازی شده مشترکی هدایت کند. (به شکل ۹-۳ توجه کنید).

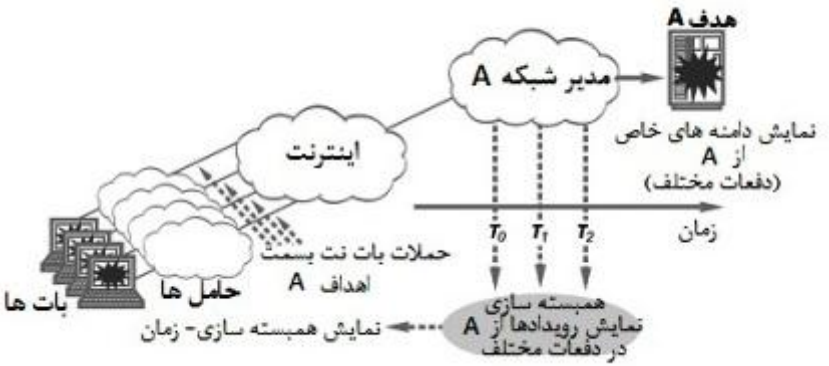


شکل ۹-۳- همبسته سازی مبتنی بر دامنه از یک حمله بات‌نت در دو هدف

- همبسته سازی مبتنی بر زمان: در این روش، داده‌های جمع‌آوری شده در طی یک دوره زمانی را با داده‌های جمع‌آوری شده در زمان دیگر مقایسه می‌کنند. منبع جمع‌آوری داده‌ها می‌تواند یکسان یا متفاوت باشد؛ اما بدیهی است که اگر منبع داده‌ها یکسان باشد، به علت حذف یک متغیر از تحلیل همبسته سازی، همبسته سازی مؤثرتر خواهد بود. بسیاری از انواع حملات، نسبت به زمان حساس نیستند و برای این نوع همبسته سازی مناسب نخواهند بود. برای مثال؛ یک ورود غیرمجاز که در طی آن یک بد افزار در سیستم مورد هدف جاسازی می‌شود، ممکن است نامزد خوبی برای همبسته سازی مبتنی بر زمان نباشد. حملاتی که در چند مرحله انجام می‌شوند، مثل بسیاری از آن‌هایی که از روش "کم و آهسته" استفاده می‌کنند، کاملاً مناسب هستند؛ دشمنان به طور فزاینده‌ای حملات بات‌نت را با برنامه توزیع‌شده حمله به هدف با شیوه‌ای آهسته‌تر و

عمدی‌تر نسبت به یک بمباران تک مرحله‌ای طراحی می‌کنند. کشف چنین رویدادی کاملاً مناسب با همبسته سازی زمانی می‌باشد زیرا دوره‌های زمانی بالقوه قابل‌ملاحظه‌ای بین مراحل متوالی یک حمله وجود دارد. همبسته سازی مبتنی بر زمان برای متصل کردن مراحل مرتبط و فیلتر کردن فعالیت‌های بی‌ربط و نویزی لازم هستند.

(به شکل ۹-۴ توجه کنید).



شکل ۱-۱-

شکل ۹-۴- همبسته سازی مبتنی بر زمان دریک حمله بات‌نت

ماهیت همبسته سازی در امنیت سایبری، شامل؛ مقایسه قطعات مختلف داده برای تعیین این است که آیا نفوذی در حال انجام است. در مجموعه‌ای از مطلوب‌ترین شرایط، این عمل شامل مقایسه دو قطعه از داده‌ها است که تمام ویژگی‌های مرتبط آن‌ها به جز یکی، یکسان است. چنین سناریویی به تحلیلگر اجازه می‌دهد که روی تنها یک ویژگی متمرکز شود. همبسته سازی مبتنی بر زمان، زمانی خوب عمل می‌کند که محیط جمع‌آوری دقیقاً یکی باشد، اما داده‌ها در زمان‌های متفاوتی جمع‌آوری شوند. در این

موارد تحلیلگر نباید نگران این باشد که فاکتورهای دیگر با گذشت زمان روی‌داده‌ها اثر بگذارند. با این حال، در پیچیده‌ترین حالت، چندین قطعه از داده‌ها از محیط‌هایی جمع‌آوری می‌شوند که در آن‌ها ویژگی‌های مرتبط متفاوت هستند. تحلیلگر باید نگران این باشد که چه ویژگی در چه محیطی ممکن است روی‌داده تأثیر بگذارد که این کار، همبسته سازی را خیلی پیچیده می‌کند. (به شکل ۹-۵ توجه کنید).

شکل ۹-۵- طبقه‌بندی سناریوهای همبسته سازی

طبقه‌بندی ویژگی‌های جمع‌آوری داده برای زیرساخت ملی مهم است؛ زیرا عملی‌ترین موارد، آن‌هایی هستند که بسیار پیچیده بوده و همبسته سازی آن‌ها مشکل است. اطلاعاتی که در هنگام یک حادثه، در دسترس قرار می‌گیرند، معمولاً، از منابع مختلف، با روش‌های متفاوت و ابزارهای گوناگون پردازش و از شبکه‌های مختلف جمع‌آوری شده‌اند. برای مثال، وقایعی از کرم در اینترنت را برخی سازمان‌ها با دقت قابل‌ملاحظه‌ای نظارت می‌کنند، البته ممکن است به نتایج خوبی نرسند؛ درحالی‌که، گروه‌های دیگر، ممکن است حتی به این موضوع توجه نکنند که واقعه امنیتی در حال انجام است. فقط مجرب‌ترین تحلیلگران همبسته سازی می‌توانند این اختلافات گسترده و دقیق در مورد امنیت را دسته‌بندی و از آن نتیجه‌گیری کنند امروزه، این کار به نیروی

انسانی باتجربه و آموزش دیده نیاز دارد. پیش از اینکه ابزارهای قابل‌اعتمادی در دسترس قرار گیرند تا همبسته سازی دقیق را روی چندین قطعه متنوع داده انجام دهند، تحقیقات بیشتری مورد نیاز خواهد بود.

۹-۱- روش‌های همبسته سازی امنیتی متداول

وضعیت فعلی، شیوه عمل روزمره همبسته سازی امنیت شبکه در محیط‌های زیرساخت ملی موجود بر اساس روشی است که به عنوان مدیریت تهدید شناخته می‌شود. در این رویکرد، داده‌های جمع‌آوری شده از منابع مختلف جهت شناسایی الگوها، روندها و رابطه‌ها همبسته سازی می‌شوند. رویکرد کلی، متکی بر اطلاعات امنیتی و مدیریت رویدادهای امنیتی (SIEM) برای جمع‌آوری زمینه‌ها و گردآوری داده‌های مرتبط است. یک سیستم SIEM بهترین کاری که می‌تواند در مورد شناسایی موارد همبسته سازی با بهترین الگوریتم‌های در دسترس برای تحلیل مشخصات، امضا، دامنه و زمان، با توجه به محدودیت‌های عملی که در بالا ذکر شد، انجام می‌دهد. در کادر زیر چهار ورودی اولیه برای یک ابزار SIEM تجاری در دسترس برای مدیریت تهدید لیست شده است.

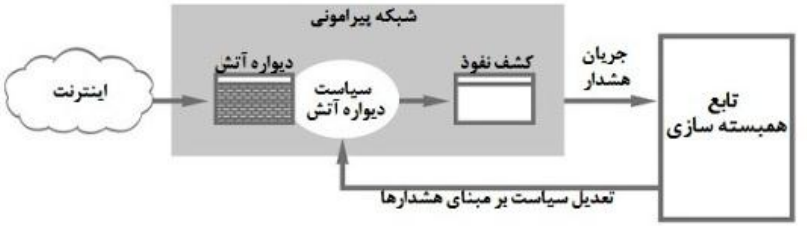
خوردهای اطلاعات برای مدیریت تهدید SIEM

- دنباله‌های ممیزی دیوار آتش: هنگامی‌که بعضی انواع رویدادهای مرتبط با امنیت؛ نظیر؛ تقاضای اتصال امتناع شده رخ می‌دهد، دیوارهای آتش رکوردهای ممیزی تولید می‌کنند. این رکوردها به صورت ایزوله استفاده محدودی دارند و معمولاً، در همبسته سازی با دیگر داده‌ها مفید هستند. اطلاعات ایستا در مورد دیوار آتش، نظیر؛ سیاست‌های ورودی و خروجی نیز برای همبسته سازی مهم هستند.

- هشدارهای سیستم کشف و جلوگیری از نفوذ: سیستم‌های کشف و جلوگیری از نفوذ به طور خاص برای تولید داده‌های هشدار هنگامی که فعالیت مشکوکی مشاهده می‌کنند طراحی‌شده‌اند. همیشه، مشخص کردن اینکه چیز مشکوک واقعاً بد است، آسان نیست. معمولاً، برای این تشخیص به همبسته سازی آن‌ها با داده‌های دیگر نیاز است.
- لاگ‌های کاربرد یا سیستم عامل: فایل‌های لاگ‌های خروجی که با فعالیت‌های سیستم عامل یا نرم‌افزارهای کاربردی تولید می‌شوند، می‌توانند نشانه‌ها و هشدارهای مفیدی برای امنیت ارائه دهند. برای مثال، اولین قدم در فارنسیک شامل امتحان و بررسی فایل‌های لاگ برای به‌دست آوردن شواهد است. (البته هکرهای مجرب چنین رد آشکاری از خود باقی نمی‌گذارند). علاوه بر لاگ ها، ویژگی‌های مخصوص سیستم‌عامل و کاربردها برای همبسته سازی مهم هستند. این ویژگی‌ها می‌توانند شماره نسخه، فروشنده و داده‌های پیکربندی باشند.
- متاداده‌های دستگاه‌های شبکه: اطلاعاتی در مورد رفتار شبکه به سرعت توسط کارشناسان امنیت سایبری شناخته می‌شود. این اطلاعات قدرتمندترین ابزار در دسترس برای مدیریت تهدید هستند. متاداده‌ها اطلاعات مربوط به آدرس منبع، مقصد، شماره پرت‌ها و همچنین، نوع پروتکل، جهت جریان اطلاعات، وضعیت پرچم‌های پروتکل و تنظیمات آن‌ها را ارائه می‌دهند و به تحلیلگر امنیتی دیدگاهی از فعالیت‌های شبکه را نشان می‌دهند که از هیچ طریق دیگری قابل‌دسترسی نیست.

در برخی مواقع، تعامل بین دستگاه‌های مختلف امنیتی در یک سیستم تهدید محلی ساده است. اگر یک دستگاه کشف نفوذ، هشداری را نشان دهد که علامت دهنده نوعی از مشکل IP آدرس منبع خاص و پرت متناظر مقصد باشد و محیط محلی اجازه ترافیک ورودی را به این پرت مقصد بدهد، فرآیند همبسته سازی یک توصیه به دیوار

آتش محلی برای بستن این آدرس منبع و این پرت تولید می‌کند. امروزه، بسیاری از دیوارهای آتش تجاری و سیستم‌های کشف نفوذ این قابلیت را ارائه می‌دهند. واقعیت این است که بسیاری از مدیران شبکه از این نوع حفاظت استفاده نمی‌کنند زیرا؛ با این فرآیند آشنایی ندارند و همین طور چیزی در مورد ترافیک ورودی و خروجی از طریق دروازه و محیط پیرامونی سازمان نمی‌دانند. این اتفاقی شرم‌آور است؛ زیرا هنگامی‌که این کار به طور درست و مناسبی انجام شود، به حفاظتی که می‌تواند کاملاً قدرتمند باشد، دست‌یافته‌ایم. (به شکل ۹-۶ توجه کنید).



شکل ۹-۶- همبسته سازی هشدارهای کشف نفوذ با قوانین سیاست‌های دیوار آتش

مثالی که در بالا ارائه شد، نشان‌دهنده حلقه بازخورد به عقب طبیعی‌ای است که هنگامی اتفاق می‌افتد که داده‌ها همبسته می‌شوند. یعنی؛ تفسیر نتیجه شده از کار همبسته سازی به عنوان داده جدید ورودی به دیوار آتش بازخورد به عقب می‌شود؛ روی پردازش اثر می‌گذارد و سرانجام، خروجی تابع همبستگی را تغییر می‌دهد. این حلقه بازخورد به عقب، زمانی متوقف می‌شود که تفسیر حاصل دیگر جدید نیست و هیچ تغییری برای گزارش به دیوار آتش ندارد. معمولاً، مدیران امنیتی سیستم‌های کشف نفوذ خود را زمانی پیکربندی می‌کنند که این حالت، برای متوقف کردن خروجی به صورت پایدار رخ می‌دهد. این کار، فشار روی اپراتور را کاهش می‌دهد، ولی باید بسیار دقت کرد که شاخص‌های معتبر از دست نروند.

عملگر همبسته سازی می‌تواند به قسمت‌های مختلف همان سازمان با شبکه‌ها، سرورها، کاربردها و گروه‌های مدیریتی متفاوت توسعه پیدا کند. تعجب‌آور است که بسیاری از فعالیت‌های همبسته سازی با چنین عدم تمرکزی پیچیده می‌شوند. فرض کنید دو گروه در یک شرکت مشکل امنیتی مشابهی را تجربه می‌کنند. برای تفسیر بهینه، باید داده‌های علت ریشه‌ای رسیده از هر دو گروه، با یکدیگر همبسته سازی شوند. برای مثال؛ اگر هر دو گروه بد افزار مشابهی را در سیستم‌هایشان یافته باشند، این مشاهده می‌تواند منبع حمله را مثلاً؛ یک فروشنده مشترک نرم‌افزار را نشان دهند. ممکن است مشخص کردن این واقعیت برای هر گروه به طور ایزوله آسان نباشد.

۹-۲- مسائل مربوط به کیفیت و قابلیت اطمینان در همبسته سازی داده‌ها

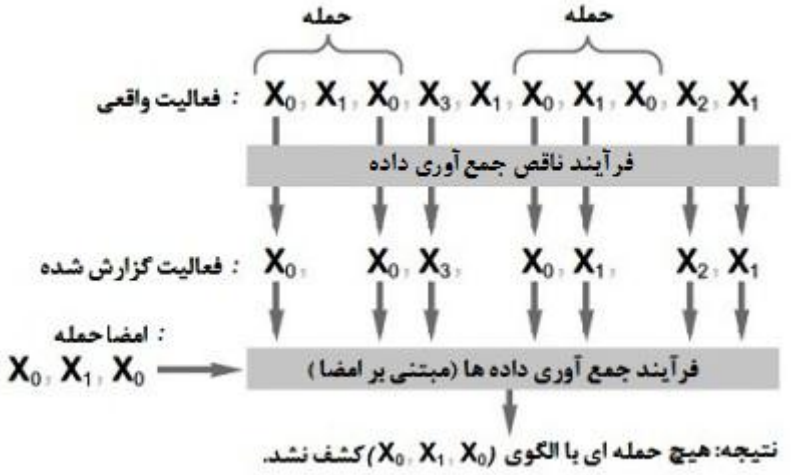
برای ایجاد یک فرآیند مناسب همبسته سازی امنیتی برای حفاظت از زیرساخت ملی که محیطی وسیع و بین سازمانی با قلمرو و مقیاس بزرگ را شامل می‌شود، باید چند شاخص فنی و عملیاتی را در نظر گرفت. مهم‌ترین چنین ملاحظاتی، کیفیت و قابل‌اطمینان بودن منابع داده‌ها است که تمام ابتکارات در سطح ملی را که برای آن‌ها کیفیت و قابل‌اطمینان بودن نمی‌توانند کنترل شوند، زیر سئوال می‌برد.

با توجه به کیفیت داده‌ها، بهترین حالت شامل یک توافق سطح سرویس (SLA) بین منبع داده و تابع همبسته سازی است. خدمات امنیتی مدیریت شده مفید هستند؛ زیرا ارائه‌دهنده سرویس، کیفیت داده‌ها را با پارامترهای به خوبی تعریف‌شده تضمین می‌کند. هنگامی که داده‌ها از مخلوطی از سازمان‌های بدون توافق سطح سرویس ناشی می‌شوند، داده‌های غیر دقیق، گمراه‌کننده و غیر معتبر در دسترس قرار می‌گیرند. تنها راه مقابله با آن، فیلتر کردن دستی یا اتوماتیک منابع داده و ویژگی‌های آن‌ها در تجزیه و تحلیل است. زمانی که همبسته سازی متکی بر اطلاعات ارائه‌شده به صورت داوطلبانه

روی اینترنت باشد، این مسئله می‌تواند مشکل‌ساز باشد. تلاش‌های عمومی برای جمع‌آوری داده‌های داوطلبانه، همیشه، باکیفیت داده‌های تضمین‌شده مشکل دارند.

به خصوص در مورد خوردهای داوطلبانه داده یک نگرانی مشابه در ارتباط با قابلیت اطمینان منابع داده‌ها وجود دارد. زمانی که داده‌ها برای تجزیه و تحلیل‌های به طور منظم، احتمالاً بر اساس مشخصات، مهم هستند. قابلیت اطمینان مداوم آن‌ها ضروری است. برای مثال؛ اگر یک رشته از داده‌ها وجود فاصله‌های خالی یا تغییراتی را به علت خیالات صاحب منبع داده تجربه کند، این موضوع به آسانی می‌تواند فرآیند همبسته سازی را سردرگم کند. فاصله‌های خالی در میان رشته داده می‌تواند عمل تطبیق فعالیت‌های مشاهده‌شده را با الگوهای مورد نظر سخت کند. زمانی که داده‌ها به صورت داوطلبانه از منابع مختلف گرفته شوند، مدیریت این مسئله مشکل می‌شود؛ بنابراین، علاوه بر مسائل مربوط به کیفیت، همبسته سازی مبتنی بر فرآیند جمع‌آوری ناقص، شامل استفاده از داده‌هایی است که به صورت داوطلبانه داده‌شده‌اند و باعث چالش‌های ذاتی می شوند که مربوط به قابلیت اطمینان است.

(به شکل ۹-۷ توجه کنید)



شکل ۹-۷- نتیجه غلط همبسته سازی به علت جمع‌آوری ناقص

امروزه، بسیاری از ابتکارات ملی متکی بر منابعی از داده‌ها هستند که آن منابع بر پایه بهترین تلاش در اختیار آن‌ها قرارگرفته‌اند. این ابتکارات را باید با شک و تردید زیاد در نظر گرفت؛ زیرا نتیجه‌گیری آن‌ها مبتنی بر زیرمجموعه‌ای از داده‌های مربوطه است و شامل ابتکاراتی است که در آن شرکت‌کنندگان هشدارهای دستگاه‌های کشف نفوذ، فایل‌های لاگ و خلاصه به شدت نمونه‌برداری شده‌ای از جریان داده‌ها را برای همبسته سازی می‌فرستند. اگر تحویل داده‌ها سازگار، قابل پیش‌بینی و تضمین‌شده نباشد، نتیجه همبسته سازی مشکوک خواهد بود. ممکن است الگوهای امضا حمله به طور غلط تطبیق داده شوند یا از دست بروند. مدیران زیرساخت ملی باید تنها داده‌هایی را جمع‌آوری کنند که به یک توافق سطح سرویس (SLA) باثبات مربوط می‌شوند.

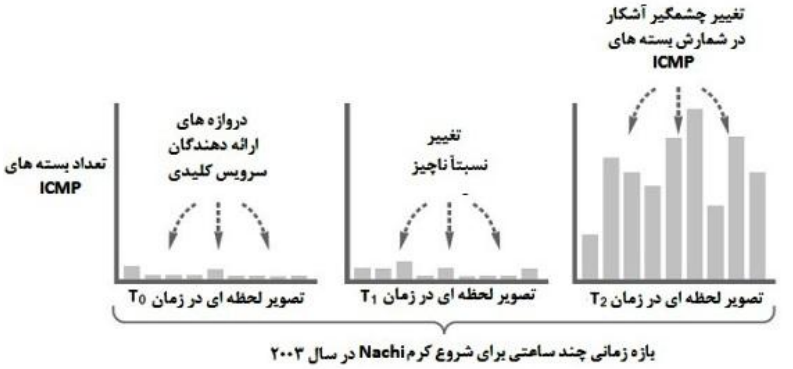
۹-۳- همبسته سازی داده‌ها برای کشف کرم

ارائه‌دهندگان خدمات شبکه، دیدگاه خوبی برای همبسته سازی داده‌ها از گستره وسیعی از شرکت‌ها، آژانس‌ها، گروه‌ها، افراد و نواحی دارند. تمام ترافیک داده‌های دولتی، تجاری و مصرف‌کنندگان زمانی باید از شبکه یک ارائه‌دهنده بک بن عبور کنند؛ بنابراین، این یک منبع عالی از اطلاعات همبسته سازی است. بدیهی است که اگر این کار انجام شود، دقت زیادی جهت اطمینان کامل از انطباق آن با قوانین مربوطه و احترام عمیق به ملاحظات حریم خصوصی باید در نظر گرفته شود. این تلاش‌ها، ارزش خود را خواهند داشت؛ زیرا ارائه‌دهندگان سرویس که جریان اطلاعات را به مقیاس وسیع جمع‌آوری می‌کنند، معمولاً می‌توانند فعالیت‌های مشاهده‌شده را با الگوهای شناخته‌شده برای کشف رویدادهای با مقیاس وسیع نظیر کرم‌ها، همبسته سازی کنند و این کار را با دقت بیشتری نسبت به کامپیوترها، تکنیک‌های امنیت کامپیوتری که از دیوارهای آتش استفاده می‌کنند، به انجام برسانند.

به عنوان مثال، یک دستگاه امنیتی مثل سیستم کشف نفوذ را در نظر بگیرید که برای کشف کرم‌ها و ویروس‌ها نصب شده است. متأسفانه، کشف بسیاری از کرم‌ها و ویروس‌ها برای سیستم کشف نفوذ آسان نیست؛ کرم Nachi چنین کرمی است؛ این کرم، در تابستان ۲۰۰۳، با استفاده از پروتکل ICMP به عنوان یکی از ابزارهای عمل خود در اینترنت جولان نمود. بعضی بر این باورند که این کرم برای یافتن سیستم‌های معیوب و آلوده در اینترنت و مرمت آن‌ها طراحی شده بود؛ اما جریان بسته‌های ICMP از کنترل خارج شد و این کرم باعث صدمات زیادی شد که شاید بیشتر از آن چیزی بود که منظور طراح آن بوده است.

بیشتر سیستم‌های کشف نفوذ برای کشف این مسئله به خوبی تنظیم‌نشده بودند؛ زیرا سیستم‌های کشف نفوذ علاقه‌ای به ایجاد تغییرات در برخی پرت‌های سرویس نداشتند. در مقابل، هر سیستم شبکه‌ای که بر جریان بسته‌های ICMP نظارت می‌کرد،

چیزهای بی‌موردی را می‌دید. هنگامی که کرم Nachi عمل کرد، افزایش بسته‌های ICMP در بک بن یک شبکه ارائه‌دهنده سرویس آشکار بود. با شمارش ساده بسته‌های ICMP که از دروازه‌های بک بن عبور می‌کردند، ارائه‌دهنده شبکه به سرعت می‌توانست افزایش ناگهانی جریان ترافیک را به علت وجود کرم در چندین دروازه کلیدی شبکه ببیند. نتیجه، همبسته سازی مبتنی بر زمان داده‌های ICMP جمع‌آوری شده در طی چند ساعت، رویداد نزدیک کرم را آشکار می‌ساخت. (به شکل ۹-۸ توجه کنید).



شکل ۹-۸- همبسته سازی مبتنی بر زمان جهت کشف کرم

از مثال بالا می‌توان نتیجه گرفت که با نظارت بر ترافیک جمع‌آوری شده شبکه در سراسر سازمان‌ها، می‌توان تصویر امنیتی خیلی دقیق‌تری را رسم کرد. نتیجه تکمیلی دیگری که از این مثال می‌توان به دست آورد، این است که ارائه‌دهندگان خدمات شبکه به وضوح نقش کلیدی در کشف حملات مقیاس وسیع ایفا می‌کنند. در دهه‌های گذشته، بسیاری از مسئولیت‌های امنیتی به عهده کاربران انتهایی و مدیران امنیتی سازمان‌ها گذارده شده بود و هیچ راهبرد مشترکی برای حفاظت از زیرساخت وجود نداشت. زمانی که یک مشکل رخ می‌داد، همه کاربران انتهایی آسیب‌پذیر برای مشخص کردن یک ابزار مناسب برای مقابله با آن تلاش می‌کردند که ممکن بود این کاربران

رویکردهای متناقضی داشته باشند. یک گروه ممکن بود تمام بسته‌های مربوط به آن حمله را نادیده بگیرد و حذف کند. درحالی‌که، گروه دیگر تمام این بسته‌ها را جمع‌آوری کرده؛ پردازش می‌کرد و پاسخی به منابع بسته‌های حمله می‌فرستاد. این توزیع مسئولیت امنیتی ایجاب می‌کرد که حفاظت از زیرساخت ملی درجه‌ای از عملیات متمرکز را نیز داشته باشد. برای خدمات شبکه‌ای با مقیاس وسیع، ارائه‌دهنده سرویس می‌تواند این کار را به طور معقولی مدیریت کند.

۹-۴- همبسته سازی داده‌ها برای کشف بات‌نت

امروزه، شرورانه‌ترین نوع حمله‌ای که می‌توان در یک محیط شبکه‌ای با مقیاس وسیع، توزیع‌شده و متصل به اینترنت یافت، بات‌نت است. روش کار بات‌نت به این صورت است که حمله‌کننده ابتدا مجموعه‌ای از کامپیوترها را مشخص می‌کند که به اینترنت وصل هستند و می‌توان به عنوان بات از آن‌ها استفاده کرد. این کامپیوترها، معمولاً، کامپیوترهای شخصی‌ای هستند که به یک سرویس باند وسیع خانگی متصل هستند و کاربر خانگی به طور ضعیفی آن‌ها را مدیریت می‌کند. چنین مدیریت سیستم نامناسبی، اجازه می‌دهد که بد افزار به آسانی روی سیستم نصب شود. احتمالاً، این عمل با phishing یا ابزارهای مهندسی اجتماعی انجام می‌شود.

زمانی که در کامپیوترهای بات، نرم‌افزار بدخواه جاسازی شد، از طریق کنترل کننده‌های بات که در سراسر اینترنت قرار دارند، فرمان‌هایی به این کامپیوتر داده می‌شود. کنترل کننده‌های بات عموماً از پروتکل شناخته‌شده‌ای مثل IRC به راحتی استفاده می‌کنند. گرچه می‌توانند از هر پروتکل مخابراتی دیگری برای تعامل با بات هایشان استفاده کنند، هدف این است که کنترل‌کننده‌های بات فرمان‌هایی به بات ها، بفرستند، برای انجام حمله‌ای که هدف آن از قبل توسط اپراتور بات‌نت مشخص شده است. این کار به نفع حمله کننده است؛ زیرا بات‌ها در سراسر طیف وسیع جغرافیایی گسترده شده‌اند و

ظرفیت پهنای باند آن‌ها فراوان است، به خصوص اگر این ظرفیت را به صورت قابلیت جمعی در نظر بگیریم.

اگر دو بات در ثانیه یک مگابایت ترافیک حمله ایجاد کنند، یک هدف با اتصال ورودی 1Gpbs می‌تواند با ۲۰۰۰ بات پر گردد که یک بات‌نت با ۲۰۰۰ بات، اندازه متوسطی برای بات‌نت‌های موجود است. در پی این منطق، یک بات‌نت خیلی بزرگ‌تر شاید با صدها هزار یا حتی میلیون‌ها بات، می‌تواند به عنوان مشکل اساسی برای زیرساخت ملی در نظر گرفته شود که نیاز به توجه دارد. مشکل همبسته سازی در این مورد این است که هیچ نقطه انتهایی به تنهایی دیدگاه مناسبی برای تعیین اندازه، قلمرو و شدت حمله یک بات‌نت داده‌شده ندارد. تنها شانس معقولی که می‌توان با آن همبسته سازی مناسبی نسبت به بات‌نت انجام داد، در زمینه‌ی زیرساخت‌های حامل است.

مراحل کشف بات‌نت

مراحل دخیل در کشف بات‌نت از طریق تجزیه و تحلیل همبسته سازی توسط یک حامل شبکه، تقریباً به شرح زیر است:

- جمع‌آوری گسترده داده‌ها: کشف بات‌نت نیاز به دیدگاه به اندازه کافی گسترده‌ای دارد که بتواند داده‌ها را از کامپیوترهای شخصی که با باند وسیع به اینترنت متصل شده‌اند و همین طور سرورهای شرکت‌ها که از اینترنت قابل دید هستند، جمع‌آوری کند. نوع اطلاعات مورد نیاز، ضرورتاً متاداده‌های جریان شبکه است که معمولاً، اطلاعات منبع، مقصد و نوع ترافیک را در خوددارند.
- همبسته سازی ارتباطات یک به چند: از داده‌های جمع‌آوری شده، تجزیه و تحلیل همبسته سازی باید متمرکز بر شناسایی الگوهای ارتباطات یک به چندی که در بات‌نت‌های توزیع‌شده یافت می‌شود باشد. این الگو

می‌تواند شامل چند کنترل‌کننده بات‌نت باشد؛ بنابراین، چندین رابطه یک به چند در بات‌نت‌ها هم پوشانی دارند.

- همبسته سازی محل جغرافیایی: با استفاده از آدرس IP می‌توان بات‌نت‌ها و کنترل‌کننده‌های آن‌ها را با یک مکان جغرافیایی منطبق کرد. IP، دقت زیادی در تشخیص محل ارائه نمی‌دهد؛ اما یک احساس کلی از محلی که بات‌ها و کنترل‌کننده‌های آن‌ها در آن جا قرار دارند، ارائه می‌کند.
- نظارت هوشیارانه بر فعالیت‌ها: تجزیه و تحلیل امنیتی باید شامل تماشای هوشیارانه و از نزدیک فعالیت بات‌ها و سرورها باشد. مهم‌ترین فعالیتی که باید شناسایی شود، حمله توزیع‌شده از طرف بات‌ها به برخی هدف‌ها است.

مراحلی که در بالا به آن‌ها اشاره شد، اجازه می‌دهد که یک نقشه منطقی از یک بات‌نت که در آن محل جغرافیایی بات‌ها و ارائه‌دهنده سرویس به آن‌ها (که معمولاً یک حامل باند وسیع محلی است) و مجموعه سرورهایی که به عنوان کنترل‌کننده بات‌نت بکار گرفته‌شده‌اند و نمایش عمومی فعالیت مرتبط آن‌ها را بسازیم. فعالیت‌های معمولی یک بات‌نت شامل استخدام بات‌های جدید و همین طور حملات از بات‌ها به سمت هدف‌های تعیین شده است. (به شکل ۹-۹ توجه کنید).

شکل ۹-۹- نمایش همبسته سازی یک بات‌نت معمولی

نمودار بات‌نت برخی نتیجه‌گیری‌هایی را نشان می‌دهد که می‌توان بلافاصله از چنین تجزیه و تحلیل‌هایی گرفت. الگوی معمولی تراکم بات‌ها که در یک بات‌نت یافت می‌شود، ممکن است به نکاتی در مورد مهندسی اجتماعی یا طعمه‌هایی اشاره کند که برای تعبیه بد افزار در داخل کامپیوترهای شخصی هدف و تبدیل آن به بات بکار می‌رود. نکات مفید دیگری همچنین ممکن است از نواحی که بات‌نت‌ها به نظر می‌رسد در آن نواحی هیچ باتی ندارند بتوان جمع‌آوری کرد. یکی از زمینه‌هایی که تجزیه و تحلیل همبسته سازی، معمولاً، مفید نیست تلاش جهت تعیین همبسته سازی بین محل‌های جغرافیایی کنترل‌کننده‌های بات‌نت است. این تلاش‌ها، معمولاً، اطلاعات مفیدی را نتیجه نمی‌دهد؛ چون کنترل‌کننده‌های بات‌نت تمایل به پراکنده بودن در سراسر دنیادارند و هکرهای فرصت‌طلب آن‌ها را هدایت می‌کنند.

سرانجام، باید بگوییم که حفاظت از زیرساخت ملی نیاز به قابلیتی بی‌درنگ برای نظارت و مونیتور کردن پیکربندی و فعالیت‌های بات‌نت دارد. در سال‌های اخیر، خطر ناشی از بات‌نت‌ها به‌شدت افزایش یافته است، قسمتی از این افزایش خطر، به علت این

است که باتنت‌ها توانسته‌اند تحت رادار بیشتر دولت‌ها و سازمان‌های تجاری وجود داشته باشند. اولین گام برای کاهش این خطر، شامل ایجاد یک توانایی ملی جهت جمع‌آوری اطلاعات در مورد باتنت‌ها و توصیه به شرکت‌کنندگان یا متقاضیان این اطلاعات در مورد این است که چگونه فریب هکرها را برای هک نمودن دیگران را نخورند؛ بات نشوند و به طور مستقیم، هدف یک حمله قرار نگیرند.

۹-۵- فرآیند همبسته سازی مقیاس وسیع

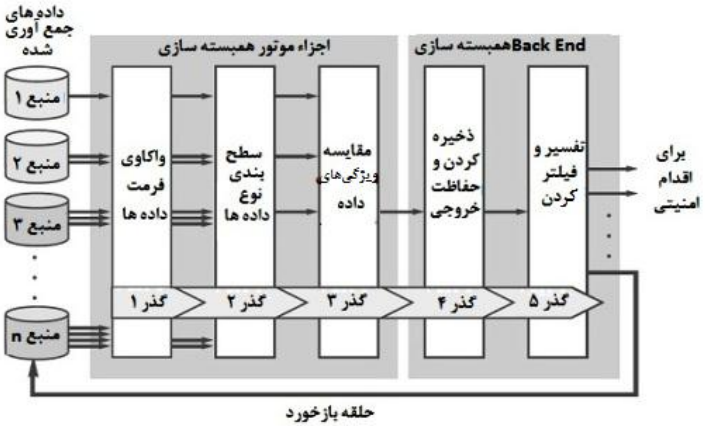
برای حفاظت از زیرساخت ملی، همبسته سازی مقیاس وسیع داده‌های تمام منابع به وسیله سازمان‌هایی با دیدگاه گسترده به خاطر چندین عامل فنی، عملیاتی و کسب و کاری زیر پیچیده است:

- فرمت‌های داده‌ها: هر کدام از محیط‌های سرمایه ملی به احتمال زیاد داده‌هایی با فرمت‌های ناسازگار را جمع‌آوری می‌کنند و این به دلیل آن است که در ابزارهای جمع‌آوری داده‌های امنیتی استانداردی وجود ندارد. در نتیجه، تقریباً تمام داده‌های مرتبط با امنیت با فرمت‌های اختصاصی به صورت محلی تعریف‌شده و جمع‌آوری می‌شوند. این چالش قابل ملاحظه‌ای برای هر سیستم جمع‌آوری داده‌های با مقیاس وسیع از منابع مختلف است.
- اهداف جمع‌آوری: هر کدام از محیط‌های سرمایه‌ها، احتمالاً داده‌هایی از انواع مختلف رویدادها و تریگرها را جمع‌آوری خواهد کرد. برای مثال؛ ممکن است بعضی از آن‌ها اطلاعات مشروحی در مورد شبکه‌ها و تنها اطلاعات محدودی از سیستم‌ها جمع‌آوری کنند. در مقابل، ممکن است دیگران به طور معکوس عمل کنند. بدیهی است که این موضوع مقایسه اطلاعات گردآوری‌شده از منابع مختلف را پیچیده می‌کند.

- رقابت: گروه‌های تجاری مختلف که ممکن است باهم رقابت کاری داشته باشند، داده‌های مربوطه را جمع‌آوری می‌کنند (بیشتر گروه‌های دولتی معترف هم هستند که باهم رقابت مشترک دارند). این مشخصات رقابتی ایجاب می‌کند که هرگونه اطلاعات جمع‌آوری شده و هرگونه تفسیری را که از تحلیل همبسته سازی نتیجه‌گیری می‌شود، باید به دقت محافظت و همراه با گمنامی مناسب باشد.

برای مقابله با این چالش‌ها در مقیاس وسیع، باید یک فرآیند همبسته سازی عمدی بکار گرفته شود. این فرآیند باید هر جز عمل همبسته سازی را به عناصر گسسته‌ای بشکند، طوری که هر کدام دارای ورودی و خروجی کاملاً خوب تعریف‌شده‌ای باشند. این فرآیند، در مجموع دارای پنج گذر مختلف است که از جمع‌آوری داده‌ها شروع می‌شود و تا اطلاعات قابل عمل ادامه می‌یابد.

(به شکل ۹-۱۰ توجه کنید).



شکل ۹-۱۰- فرآیند همبسته سازی چند گذری مقیاس وسیع با بازخورد (فیدبک)

پنج گذر برای رسیدن به اطلاعات عملی:

۱- اولین گذر در این طرح، شامل حل مسئله فرمت داده‌های غیر سازگار از منابع مختلف است. علاوه بر داده‌هایی که دستگاه‌های امنیتی شناخته‌شده تولید می‌کنند، داده‌های دیگر ورودی می‌توانند توسط انسان تولیدشده؛ یا از طریق تلفن یا فرآیندهای اجتماعی کسب‌شده باشند. راه حل باید به طور خودکار از طریق فیلتر، یک خروجی با فرمت مشترک را تولید کند. تعجب‌آور است که برای استاندارد کردن فرمت مربوطه کار تحقیقاتی کمی در مجامع امنیت کامپیوتری انجام شده است.

۲- دومین گذر در این طرح، سطح‌بندی انواع مختلف داده‌های جمع‌آوری شده است. متداول‌ترین کار در این گذر، طبقه‌بندی داده‌های مشابه در یک مجموعه مناسب خود در طبقه‌بندی است. به علت اینکه سازمان‌های مختلف به طور منظم به حوادث امنیتی یکسان با نام‌های مختلفی اشاره می‌کنند، کار طبقه‌بندی باید انجام شود. ابزارهای تجاری نیز تمایل دارند که به یک نوع حمله با اسامی و هشدارهای مختلف اشاره کنند؛ بنابراین، همبسته سازی با مقیاس وسیع به درک مشترکی از معنی و مفهوم مربوط به یک فعالیت مورد علاقه نیاز دارد. متدولوژی‌های تجزیه و تحلیل با مقیاس کوچک با استفاده از ابزار مشترک مدیریت تهدید از یک فروشنده، می‌توانند این مرحله را دور بزنند؛ ولی تجزیه و تحلیل‌های با مقیاس وسیع از منابع مختلف و متنوع نمی‌توانند این کار را بکنند.

۳- سومین گذر در این طرح، شامل مقایسه عملی داده‌های جمع‌آوری شده با ویژگی‌های مربوطه است. کارشناسان امنیت کامپیوتری، این گذر را همبسته سازی می‌نامند. این گذر جایی است که الگوریتم‌های همبسته سازی مبتنی بر مشخصات، امضا دامنه و زمان در تجزیه و تحلیل

گنجانیده می‌شوند. این گذر، معمولاً، شامل ترکیبی از پردازش‌های خودکار با استفاده از ابزارها همراه با تفسیر متخصصان انسانی هستند. در بهترین حالت، این گذر در فرایند به سرعت اتفاق می‌افتد، تقریباً، به صورت بی‌درنگ و زمان واقعی، اما واقعیت این است که مراحل تجزیه و تحلیل در مورد سناریوهای پیچیده ممکن است به زمان قابل‌توجهی نیاز داشته باشد. این گذر همراه با دو گذر قبلی، به عنوان موتور همبسته سازی در نظر گرفته می‌شوند.

۴- گذر چهارم این طرح، شامل ذخیره‌سازی و حفاظت خروجی است. این گذر، احتمالاً، شامل تفسیر داده‌ها در زمانی است که آن‌ها جمع‌آوری و مقایسه شدند. در این مرحله از فرآیند، بینش‌هایی مشهود است که می‌تواند اطلاعات ذخیره‌شده عمدی در یک پایگاه داده یا اطلاعاتی باشد که برای تحلیلگران امنیتی که در کل فرآیند درگیر هستند، شناخته شده است. برای کاربردهای با مقیاس وسیع، اندازه اطلاعات جمع‌آوری شده می‌تواند عظیم باشد که لازمه آن ممکن است فناوری‌های مخصوص پایگاه داده با توانایی مقیاس‌پذیری مورد نیاز باشد.

۵- پنجمین و آخرین گذر در فرآیند این طرح، شامل فیلتر کردن و انتشار اطلاعات است. که باعث ایجاد یک حلقه فیدبک می‌شود که توصیه‌های خروجی، ورودی سری‌های جدیدی از گذرهای پنج مرحله‌ای شوند. یا اینکه خروجی می‌تواند به وسیله طرف‌های مربوطه مناسب برای اعمال فوری مثل واکنش بی‌درنگ و زمان واقعی به حوادث استفاده شود. این گذر با گذر قبلی ذخیره‌سازی، مجموعاً عقبه همبسته سازی را تشکیل می‌دهند.

۹-۶- برنامه همبسته سازی ملی

پیاده‌سازی یک برنامه همبسته سازی ملی احتمالاً دو جهت خاص را به دنبال دارد.

اول، قدم‌هایی برداشته شود که ممکن است برای تشویق هر کدام از سازمان‌هایی که دارای مسئولیت در زیرساخت ملی جهت ایجاد و پیروی از یک برنامه محلی جمع‌آوری داده است، باشد. این با تعبیه الزامات همبسته سازی در داخل ممیزی استاندارد و اعطا گواهی‌نامه استاندارد و همین طور در داخل هر برنامه درخواست پروژه در زیرساخت‌های مرتبط با دولت می‌تواند انجام شود. احتمال موفقیت این رویکرد بالا است. بنابراین، تصویب فوری آن در سطح سیاست ملی توصیه می‌شود.

دوم، ممکن است برنامه‌هایی در سطح ملی ایجاد شود تا داده‌های جمع‌آوری شده در بالاترین سطح از تمام منابع در دسترس را همبسته کند. این رویکرد خیلی چالش آورتر است و احتیاج به پرداختن به مسائل فنی و عملیاتی به شرح زیر دارد:

- عملیات شفاف: رویکرد تجزیه و تحلیلی است که برای همبسته سازی بکار می‌رود و باید به طور کامل برای تمام شرکت‌کنندگان در آن شناخته شده باشد؛ بنابراین، اینکه آیا مشخصات، امضاها یا شبیه به آن‌ها استفاده می‌شوند، باید فرآیند مربوطه به طور روشن توضیح و نشان داده شود. این به شرکت‌کنندگان اجازه می‌دهد که به بهبود جنبه‌هایی از فرآیند نظیر، ارائه و تهیه خورد داده، الگوریتم‌های کاهش حجم داده، تفسیر داده در عقبه یا مدیریت کمک کنند.
- خوردهای داده تضمین‌شده: هر شرکت‌کننده در ارائه داده به فرآیند همبسته سازی، باید متعهد به ارائه داده‌های تضمین‌شده در سطح سرویس باشد. بدیهی است که این سطح می‌تواند تغییر کند، ولی فقط تحت شرایط کنترل شده‌ای که در تجزیه و تحلیل در نظر گرفته می‌شود. بدون چنین تضمین‌هایی، الگوریتم همبسته سازی مؤثر نخواهد بود.

- گزاره‌های ارزش به طور واضح تعریف‌شده: شرکت‌کنندگان برای ارائه داده‌هایشان باید گزاره‌های ارزش به طور واضح تعریف‌شده‌ای را بشناسند. بدترین حالت، فرآیند جمع‌آوری "سوراخ سیاه" است، جایی که توصیه‌های خروجی از فعالیت‌های همبسته سازی معمولاً مشترک نیست.
- تمرکز بر آگاهی موقعیتی: خروجی فرآیند حتماً باید عمل‌گرا باشد. همچنین، باید محدودیت‌های ذاتی در همبسته سازی وسیع تشخیص داده شود. بعید است که تابع همبسته سازی در سطح ملی قادر به ارائه نسخه مطلوب به صورت زمان واقعی و بی‌درنگ به هر کدام از شرکت‌کنندگان باشد. بیشتر احتمال دارد که خروجی همبسته سازی، آگاهی موقعیتی را ارائه دهد که در تفسیر و واکنش به یک رویداد کمک می‌کند.

با پرداختن به این مسائل، امکان سنجش فنی و عملیاتی یک تابع همبسته سازی موفق در سطح ملی، به شدت افزایش می‌یابد. متأسفانه، بسیاری از مسائل قانونی، اجتماعی و سیاسی خارج از قلمرو عمومی این کتاب فرض می‌شوند و ایجاد چنین تابعی را پیچیده خواهند کرد.

فصل ۱۰: آگاهی

هوش، اطلاعات و دانش در مورد دشمن که با مشاهده، تحقیق، تجزیه و تحلیل و درک به دست می‌آید، محصولی است که آگاهی فضای جنگ و درگیری را فراهم می‌کند. ادوارد والتز[۱۳].

آگاهی موقعیتی به درک جمعی بی‌درنگ در داخل یک سازمان از وضعیت خطر امنیتی خود اشاره می‌کند. ریسک امنیتی، احتمال اینکه یک حمله، نتیجه قابل‌ملاحظه‌ای را برای برخی از سرمایه‌های دارای ارزش محلی ایجاد نماید، اندازه‌گیری می‌کند. چالش عمده در اندازه‌گیری ریسک، وجود فاکتورهایی است که معمولاً، به طور محلی قابل‌کنترل نیستند و دشمن عمداً آن‌ها را پنهان نگه می‌دارد. برای بهینه‌سازی آگاهی موقعیتی، زمان، تلاش و حتی خلاقیت قابل‌ملاحظه‌ای باید صرف شود. متأسفانه، بیشتر شرکت‌ها و آژانس‌های موجود با مسئولیت‌هایی در زیرساخت ملی، دارای هیچ یا مقدار کمی نظم و انضباط در این زمینه هستند. تعجب‌آور است که سئوالی که معمولاً، رهبریت ارشد سازمان می‌پرسد، این است که آیا سازمان یک ریسک امنیتی را تجربه می‌کند یا در زمان معینی مورد حمله قرار می‌گیرد؟

آگاهی از وضعیت امنیتی مستلزم در نظر گرفتن چند عامل فنی، عملیاتی، کسب و کاری و عوامل خارجی یا جهانی است. این عوامل عبارت‌اند از:

- آسیب‌پذیری‌های شناخته‌شده: کسب دانش مشروح از آسیب‌پذیری‌های مربوطه از فروشندگان، ارائه‌دهندگان سرویس، دولت، دانشگاهیان و مجامع هکرها، برای آگاهی موقعیتی کارآمد ضروری است. معمولاً،

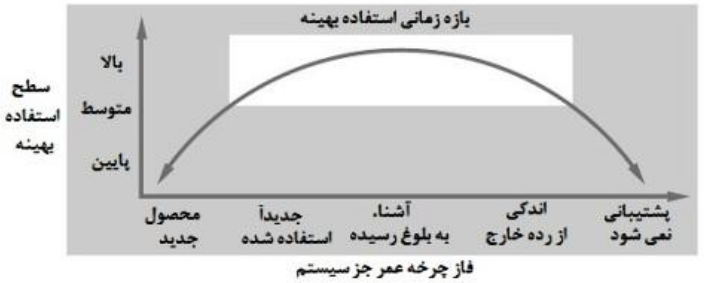
رویدادهای خاص، نظیر کنفرانس‌های برجسته هکرها، منبع غنی از داده‌های آسیب‌پذیری‌های جدید هستند.

- زیرساخت امنیتی: شناخت حالت تمام اجزا امنیتی فعال در محیط محلی، برای آگاهی موقعیتی مناسب، مورد نیاز است. این شامل اطلاع از نسخه‌های نرم‌افزارهای امنیتی برای مدیریت یکپارچگی و پردازش ضد بد افزارها، به‌کارگیری امضاها برای دستگاه‌های امنیتی نظیر سیستم‌های تشخیص نفوذ و وضعیت نظارت برای هر نوع مجموعه‌های امنیتی و سیستم‌های پردازشی است.
- شبکه و ساختار محاسباتی: برای درک حالت امنیتی موقعیتی سازمان، اطلاع از شبکه و معماری محاسباتی مهم است. باید فهرست دقیقی از تمام سرویس‌های ورودی و خروجی از طریق دروازه‌های خارجی تهیه شود به خصوص در حین یک حادثه که در آن ممکن است از پرت‌ها و پروتکل‌های خاص استفاده شود.
- محیط کسب‌وکار: وضع امنیتی، مستقیماً به فعالیت‌های کسب‌وکار می‌پردازد؛ مثل؛ شروع فرستادن محصولات جدید به بازار، شروع پروژه‌های جدید، اطلاعات ارائه‌شده توسط روابط عمومی به مطبوعات، فعالیت‌های اجرایی شامل هر چیزی که حتی به طور متوسط سئوال برانگیز باشد، و به خصوص عدم موفقیت کسب‌وکار. هر نوع مذاکرات در مورد قراردادهای بین مدیریت و پایگاه‌های کارمندان دارای اثر مستقیم روی وضعیت امنیتی موقعیتی محلی خواهد بود.
- تهدیدات جهانی: هر تهدید سیاسی یا جهانی، قطعاً، روی وضعیت امنیتی موقعیتی سازمان اثر خواهد داشت. در نواحی که در آن ترتیبات برون سپاری برقرار شده، باید به دقت بر تهدیدات جهانی نظارت شود. از آنجا

که برون سپاری در نواحی دور از سازمان اتفاق می‌افتد، وضعیت تهدید جهانی قابل ملاحظه تر شده است.

- مشخصات سخت افزاری و نرم‌افزاری: مشاهده دقیق تمام نرم‌افزارها و سخت‌افزارهایی است که در سازمان استقرار دارند؛ این مشاهده، برای آگاهی موقعیتی ضروری است. مشکل عمومی که وجود دارد، اجرای بعضی نسخه‌های محصولاتی است که خیلی قدیمی هستند و نمی‌توانند امنیت مناسب را با برنامه‌های وصله زنی یا ارتقا امنیتی ایجاد کنند. مشکل دیگر، به سیستم‌هایی مربوط می‌شود که خیلی جدید هستند و نیرومندی و قدرت خود را در مقابل حملات مشخص نکرده‌اند. بین دو دوره، یعنی دوره نصب اولیه که محصول یا سیستم کاملاً جدید است و دوره به‌کارگیری انتهایی که فروشنده ممکن است خدمات پس از فروش خود را قطع کند، دوران بهینه عمل محصول ظاهر می‌شود.

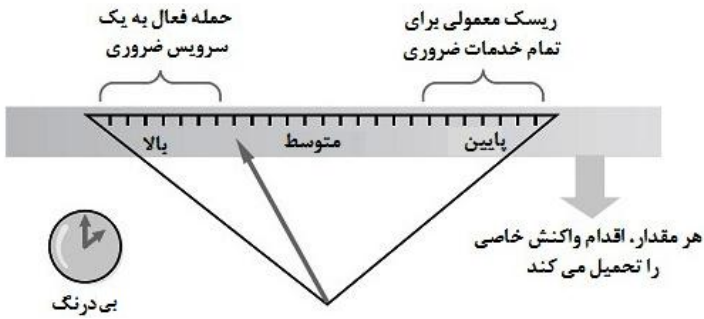
(به شکل ۱۰-۱ توجه کنید).



شکل ۱۰-۱- دوره بهینه بهره‌برداری سیستم برای امنیت سایبری

هر کدام از عوامل بالا، مجموعه‌ای از چالش‌های منحصربه‌فرد را برای تیم‌های امنیتی ایجاد می‌کنند. برای مثال؛ درگیری جهانی در حال ظهور، احتمالاً با مشخصات

آسیب‌پذیری‌های نرم‌افزارهایی که به صورت محلی در حال اجرا در یک سازمان هستند، کاری ندارند. با این حال، وابستگی‌های آشکاری وجود دارد که بین عوامل در عمل به وجود می‌آیند و آگاهی موقعیتی را بهبود خواهند بخشید. به عنوان مثال؛ هنگامی‌که آسیب‌پذیرهایی توسط گروه‌هایی از هکرها گزارش می‌شود، حالت امنیتی سازمان بستگی به مشخصات زیرساخت امنیتی، سخت‌افزار و نرم‌افزارهای محلی خواهد داشت. در نتیجه، معمولاً، برای یک سازمان عاقلانه است تا ارزش تمام عوامل وضعیت موقعیتی را در یک معیار عمومی حالت امنیتی خود ترکیب نماید. این معیار باید بتواند تخمین غیر دقیقی از ریسک امنیتی سازمانی ارائه دهد که به طور وسیع در یک زمان داده شده باشد. سپس، باید احتمال پیامدهای بالقوه یک حمله جدی را در مقابل سطح ریسک معمولی و روزمره‌ای بسنجد که سازمان با آن به طور روزانه زندگی می‌کند. احتمالاً ریسک بر پایه برآورد روزبه‌روز آن باید پایین‌تر از دوران حملات جدی باشد، به این دلیل است که یک متریک غیر دقیق، وضعیت را به صورت ریسک بالا، متوسط یا پایین مشخص می‌کند. (به شکل ۱۰-۲ توجه کنید).



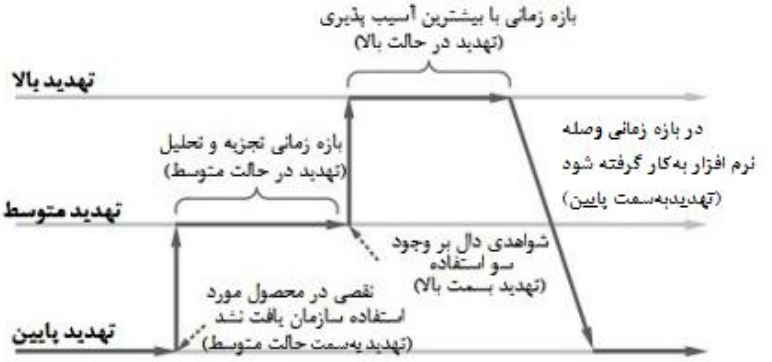
شکل ۱۰-۲- برآورد غیر دقیق داشبورد از حالت امنیتی سایبری

متأسفانه، درک عمومی از طبقه‌بندی ریسک‌های امنیتی به صورت بالا، متوسط و یا پایین این است که طبقه‌بندی اطلاعات مفیدی را ارائه نمی‌دهد. قبلاً وزارت امنیت داخلی آمریکا از چنین واحدهایی برای اندازه‌گیری تهدید عمومی و مشخص کردن

ریسک استفاده می‌کرد. مشکل این متریک این بود که شهروندان را مجبور به انجام هیچ عمل قاطعی نمی‌کرد. اگر ریسک به عنوان پایین مشخص شده بود، به شهروندان هشدار داده می‌شد که هشیار، مراقب و آماده باشند. اگر ریسک متوسط یا حتی بالاتر تعیین می‌شد، توصیه در اصل همان بود و به شهروندان گفته می‌شد که به زندگی طبیعی خود ادامه دهند و بیشتر مراقب باشند. بدیهی است که چنین توصیه‌ای باعث سردرگمی می‌شد و در حفاظت از زیرساخت ملی باید از آن اجتناب شود.

تنها راهی که یک متریک حالت می‌تواند مفید باشد، این است که با رویدادهای بی‌درنگ کشیده شود و مستقیماً به یک برنامه واکنش و پاسخ به حوادث صریح متصل باشد. زمانی که چنین کاری انجام شود، یک ریتم مداوم توسعه می‌یابد که در آن حالت موقعیتی به هدایت فعالیت‌های مدیریت امنیت کمک خواهد کرد. این می‌تواند شامل کشف شدن نقص‌های جدی در سازمان شود که باعث بالا رفتن سطح تهدید می‌گردد. سپس، ابزار سواستفاده از نقص‌ها کشف می‌شود که میزان تهدید را بیشتر بالا خواهد کشید در ادامه با یک فعالیت وصله زنی که باعث پایین کشیده شدن سطح تهدید گردد، مسئله رفع می‌شود.

(به شکل ۱۰-۳ توجه کنید).



شکل ۱۰-۳- تغییرات حالت امنیتی بر اساس فعالیت و واکنش و پاسخ

بدون در نظر گرفتن درک عمومی نسبت به متریک‌های تهدید قبلی دولت، هر برنامه آگاهی موقعیتی برای امنیت سایبری، باید شامل مشخص کردن وسیع و گسترده ریسک‌های بی‌درنگ باشد. ویژگی‌های این مشخص کردن گسترده بر پایه درک بسیار دقیق‌تر از حالت زمان واقعی خواهد بود. در مجموع، از این حالت به عنوان آگاهی موقعیتی یاد می‌شود و بر پایه درک این موضوع است که آیا زیرساخت تحت حمله می‌باشد، یا خیر؟ کدام آسیب‌پذیری‌ها مربوط به زیرساخت محلی هستند؟ چه نوع اطلاعاتی در دسترس است؟ خروجی فرآیند مدیریت ریسک چیست و اطلاعاتی که یک مرکز عملیات امنیت زمان واقعی تولید می‌کند، کدام‌اند. این عناصر در بخش‌هایی که در ادامه آمده است، توضیح داده خواهد شد.

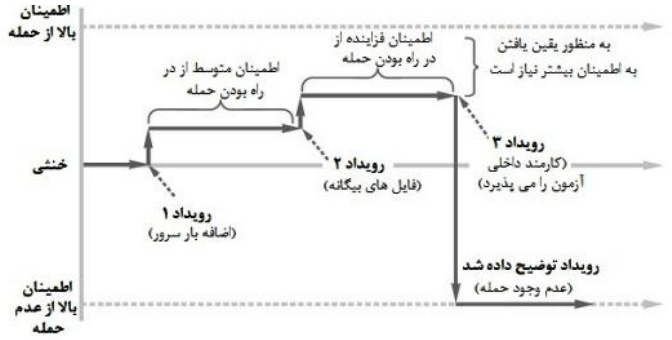
۱۰-۱- کشف حملات به زیرساخت

فرآیند تعیین اینکه آیا حمله‌ای به زیرساخت ملی در حال انجام است، بسیار مشکل‌تر از آنچه به نظر می‌آید، می‌باشد. در ظاهر، با مشاهده شاخص‌های کلیدی به راحتی می‌توان تعیین کرد که آیا حمله‌ای شروع‌شده یا در حال انجام است. با همبسته سازی فعالیت‌های مشاهده‌شده با مشخصات، امضاها و نظایر آن‌ها، می‌توان اساس یک الگوریتم قدرتمند را ارائه کرد و محصولاتی نظیر سیستم‌های کشف نفوذ، ابزارهایی برای پیاده‌سازی خواهند بود. به‌هرحال، این عوامل گمراه‌کننده هستند و در حقیقت هیچ کار امنیتی سخت‌تر و پیچیده‌تر از کشف یک حمله در حال انجام نیست، به خصوص زمانی که دشمن ماهر باشد.

برای نشان دادن این چالش، فرض کنید که متوجه می‌شوید یک سرور مهم با حالت تنبلی عمل می‌کند، ولی نمی‌توانید مشکل را تشخیص داده و توضیح دهید که چرا این‌گونه عمل می‌نماید. بدیهی است که این حالت مشکوک است و می‌تواند نشان‌دهنده این باشد که به سرور شما حمله شده است، اما نمی‌توانید این موضوع را به صورت یقین بیان کنید. میلیون‌ها دلیل برای اینکه سرور کند عمل کند، وجود دارد و

بیشتر آن‌ها با مسائل امنیتی ارتباطی ندارند. با این حال، فرض کنید که کشف کرده‌اید که اخیراً یک فهرست راهنما روی سرور نصب‌شده که پر از فایل‌های غیر آشنا و عجیب و غریب است. این موضوع شک شما را بالا خواهد برد، اما هنوز توضیحات متعددی وجود دارد که حمله‌ای را نشان نمی‌دهد. شاید، سرانجام، در شرکت کسی پا جلو بگذارد و بگوید که در حال انجام برنامه‌های تست خوش‌خیم و بی‌خطری روی سرور است. بنابراین، شرایط کندی سیستم را توضیح می‌دهد. اعتماد به اینکه هدف، مورد حمله است؛ بسته به جزییات چیزهایی که مشاهده شده است، بالا و پایین می‌رود. آشکار است که آستانه‌ای وجود دارد که در هر دو سوی آن، سطح اعتماد برای تصمیم گرفتن به اندازه کافی بالا است. در بسیاری از موارد عملی، تجزیه و تحلیل، هرگز، به چنین آستانه اطمینانی، به خصوص در محیط‌های پیچیده زیرساخت ملی، منجر نخواهد شد.

(به شکل ۱۰-۴ توجه کنید).



شکل ۱۰-۴- تغییرات اطمینان از حمله بر پایه رویدادها

در مثال ما، سرانجام مطمئن می‌شوید که حمله‌ای در حال انجام نیست. بسیاری از سناریوها به این پاکیزگی تمام نمی‌شوند. در عوض، رویدادها رشته پیوسته‌ای از اطلاعات مداوم را نشان می‌دهند که می‌توانند اثر مثبت، منفی یا خنثی روی تعیین این بگذارند که چه چیزی در حال انجام است. در بسیاری از موارد اطلاعاتی که غلط هستند و یا به طور نامناسبی تفسیر شده‌اند باعث سردرگمی در فرآیندمی شوند. فناوری‌های

نسبتاً جدید، مثل؛ خدمات بی‌سیم گوشی‌های همراه، تمایل به نشان دادن این ویژگی دارند به خصوص در مواردی که حادثه خاصی اتفاق بیفتد که قبلاً هرگز دیده نشده است. اشکال اولیه هرگز مشخص نشدن علت ریشه‌ای یک حمله این است که وضعیت امنیتی نمی‌تواند به دقت اندازه‌گیری شود. این موضوع به خصوص زمانی مشکل‌ساز است که حمله شدید و اهداف، سرویس‌های ضروری زیرساخت ملی باشند.

۱۰-۲- مدیریت اطلاعات آسیب‌پذیری

یک نگاه بدبینانه رایج از امنیت کامپیوتری این است که کارشناسان آن درگیر چیزی هستند که بیشتر از پیگیری یک بازی بی‌اهمیت در مورد حمله و اطلاعات آسیب‌پذیری نیست. پشتیبانی از چنین دیدگاهی در کتاب‌های امنیتی که امروزه چاپ می‌شوند، آشکار است. بیشتر آن‌ها صفحات زیادی از حمله‌های مشکوک را دارند که معمولاً، مدت‌ها است نامربوط شده‌اند. این موضوع در محافل اجتماعی؛ نظیر؛ کنفرانس‌های امنیتی و مجامع هکرها نیز مشهود است. جایی که بحث‌ها به ندرت مباحث بنیادی مهندسی نرم‌افزار و طراحی سیستم‌ها را نشان می‌دهند و به جای آن بر مسائل بی‌اهمیت؛ مانند این متمرکزشده‌اند که کدام سیستم، کدام اشکال را در کدام نسخه دارد. بعضی کارشناسان امنیتی و هکرها تبدیل به دایره المعارف زنده چنین دانستنی‌هایی شده‌اند و داشتن این اطلاعات را نشانه قدرت و مهارت می‌دانند. هر کسی که به اندازه کافی جزییات این دانستنی‌ها را نداند، به او برچسب مبتدی، ناکارآمد می‌زنند.

با وجود این پدیده عجیب و غریب، آگاهی موقعیتی برای حفاظت از زیرساخت ملی، احتیاج به درجه‌ای از توجه به چیزهای بی‌اهمیت روزمره در مورد اطلاعات آسیب‌پذیری دارد. از این اطلاعات به عنوان بی‌اهمیت نام می‌بریم؛ زیرا به سادگی اگر مورد نظر قرار گیرند و مرمت شوند، ارزش خود را کاملاً از دست می‌دهند. با این حال، جمع‌آوری اطلاعات مهم است و بیشتر تیم‌های زیرساخت ملی رویکرد پیش فرضی از فرصت‌طلبی فعال دارند و مقدار مشخصی از تلاش‌هایشان را صرف جمع‌آوری داده

می‌کنند. هر چیزی که همراه این داده‌ها جمع‌آوری شود، نیز مورد استقبال قرار می‌گیرد. مشکل فرصت‌طلبی فعال این است که هرگز، کامل نیست و نمی‌تواند وابسته به تصمیمات دقیق مدیریت باشد. برای مثال؛ آیا یک آسیب‌پذیری خاص که توسط یک اکسپلویت مورد استفاده قرارگرفته و به صورت کد در داخل آن پیاده‌سازی شده و در اینترنت در دسترس قرار گرفته است، می‌تواند توسط یک نفر، دو نفر یا پنجاه نفر مورد تحقیق قرار گیرد؟ اگر شواهدی از چنین اکسپلویتی به دست نیامد، نتیجه ضعیفی گرفته می‌شود که چنین اکسپلویتی وجود ندارد. بدیهی است که اطلاعات در مورد آسیب‌پذیری‌ها را می‌توان در بحث‌های اینترنتی و از سایت‌های گمنام هکرها به دست آورد؛ ولی تا زمانی که تیم امنیتی آن‌ها را نیابد، مطمئناً از وجود آن‌ها مطلع نخواهند شد.

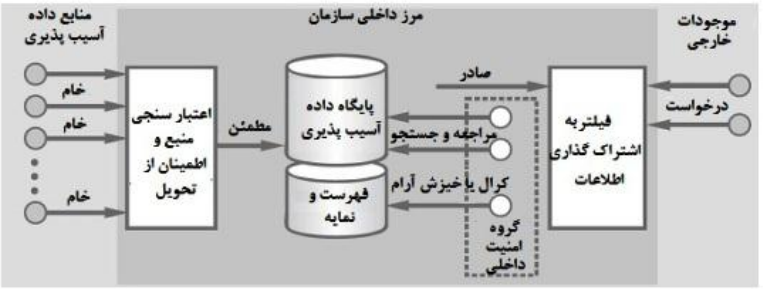
بهترین راه، ایجاد یک فرآیند جمع‌آوری اطلاعات آسیب‌پذیری‌های کامل و فعال

است. ابتکارات عملی که در گذشته برای حفاظت از زیرساخت مفید بوده‌اند، در کادر زیر آورده شده است.

ابتکارات عملی برای مدیریت اطلاعات آسیب‌پذیری

- جمع‌آوری ساختارمند؛ ریشه تمام فرآیندهای مدیریت آسیب‌پذیری باید نوعی از رویکرد جمع‌آوری ساختارمند باشد. با ابزارهایی برای اطمینان از تحویل، اعتبارسنجی منابع، فهرست‌نویسی مناسب اطلاعات با طبقه‌بندی مناسب و نگهداری یک پایگاه داده مفید برای مراجعه زمان واقعی و بی‌درنگ با پیش‌بینی‌هایی برای نمایه‌سازی و در اختیار قرار دادن داده‌های آسیب‌پذیری‌ها به صورت بی‌درنگ و زمان واقعی. این رویکرد ساخت‌یافته در داخل فعالیت‌های امنیت سایبری به صورت روزبه‌روز باید یکپارچه شود، به طوری که اطلاعات دقیق آسیب‌پذیری در دسترس کل

تیم امنیتی و زیرساخت آن قرار گیرد. باید فیلترهایی موجود باشد تا داده‌های ورودی را تضمین کند و در همان حال ضمانت نماید که موجودات خارجی فقط اطلاعات مناسب را به دست آورند.
(به شکل ۱۰-۵ توجه کنید).



شکل ۱۰-۵- ساختار مدیریت آسیب‌پذیری

- فرض‌های بدترین حالت: حالاتی ایجاد می‌شوند که در آن تیم امنیتی نمی‌تواند معین کند که آیا قسمت مهمی از اطلاعات مربوط به آسیب‌پذیری افشا شده است و برای گروه‌هایی از دشمن شناخته شده است. به بلوغ رسیده‌ترین و سالم‌ترین رویکرد در چنین سناریویی، فرض کردن بدترین حالت است. بیشتر کارشناسان باید به این توافق برسند که اگر بعضی از آسیب‌پذیری‌ها به صورت خارجی شناخته‌شده باشند، احتمالاً این آسیب‌پذیری‌ها فاش شده و شناخته‌شده هستند.
- نتیجه‌گیری‌های نامعین: اظهارنظرهای قطعی در مورد امنیت زیرساخت ملی توصیه نمی‌شود. موارد زیادی وجود دارد که یک تیم امنیتی با اطمینان نتیجه می‌گیرد که سیستم امن است، بر خلاف این اطمینان، اطلاعات مرتبط با آسیب‌پذیری‌های سیستم را بعداً به دست می‌آورد.

برای مثال؛ مدیران باتجربه می‌دانند که همیشه، باید هشدارهایی را در گزارشات وضعیت امنیتی به رهبران ارشد در دولت یا صنعت می‌دهند، بگنجانند.

- اتصال به تمام منابع: مدیریت اطلاعات آسیب‌پذیری باید شامل اتصالات به تمام منابع ممکن؛ مثل؛ گروه‌های صنعتی، خدمات گزارش‌های آسیب‌پذیری، کنفرانس‌های هکرها، گزارشات کارمندان داخلی و داده‌های مشتریان باشد. در برخی مواقع، حیاتی‌ترین قسمت اطلاعات آسیب‌پذیری از بعیدترین منابع به دست می‌آید.

ابتکاراتی که در بالا لیست شد، کمک می‌کند تا اطمینان حاصل شود که بهترین داده‌های در دسترس جمع‌آوری، ذخیره و استفاده می‌شوند. این ابتکارات، هرگز، نمی‌توانند تضمین کنند که فرآیند مدیریت آسیب‌پذیری کامل و بدون نقص است. در عوض، به مدیران توصیه می‌شود که از سه قانون زیر پیروی کنند:

- همیشه فرض کنید که دشمن نیز به اندازه شما یا حتی بیشتر از شما در مورد زیرساخت شما اطلاع دارد.
- فرض کنید که دشمن، همیشه، رمزهای مرتبط با آسیب‌پذیری را از شما پنهان نگه می‌دارد.
- هرگز، فرض نکنید که همه چیز را در مورد امنیت زیرساختتان می‌دانید.

دستیابی به چنین اطلاعات کاملی در محیط زیرساخت ملی که بزرگ و پیچیده است، ممکن نیست.

۱۰-۳- گزارشات اطلاعات امنیت سایبری

روشی که به طور معمول در محیط‌های مجامع اطلاعاتی دولتی استفاده می‌شود؛ ولی هرگز، در محیط شرکت‌ها از آن استفاده نمی‌شود، ایجاد و استفاده از گزارش

اطلاعاتی است که معمولاً، روزانه، به طور منظم چاپ می‌شوند. برای امنیت سایبری، چنین گزارشی معمولاً شامل متریک‌های مرتبط با امنیت، شاخص‌ها، اطلاعاتی در مورد حمله، تجزیه و تحلیل علل ریشه‌ای و ... برای یک دوره زمانی تعیین شده است. معمولاً، این گزارش‌ها به مدیران ارشد و همین طور تمام تصمیم سازان امنیتی و تیم‌های زیرساخت ارائه می‌شود. گزارش‌ها باید برای جستجوها جهت اطلاعات فعلی و قبلی نمایه گزاری شده باشند، گرچه این شیوه عمل رایجی نیست.

گرچه زمان تناوب و محتوای گزارش‌های اطلاعاتی باید مناسب نیازهای محیط محلی باشد، برخی از اطلاعاتی که می‌توان در یک گزارش اطلاعات روزانه انتظار داشت، شامل موارد زیر است:

- وضعیت امنیتی جاری: وضعیت موقعیتی ریسک امنیتی فعلی در هر گزارش امنیتی مورد نیاز است، به خصوص گزارشاتی که به صورت روزانه و هفتگی منتشر می‌شوند (گزارش‌های ماهانه برای اطلاعاتی که باید به صورت "Intelligence" فرض شوند، فاصله زمانی طولانی ایجاد می‌کنند).
- خطرات امنیتی بالا و جدید: مهم است که در گزارش اطلاعاتی خطرات بالا و همین طور خطرات جدید، گنجانیده شود. معمولاً، استفاده از تکنیک‌های تجسمی و دیگر روش‌ها برای برجسته کردن تغییرات در وضعیت ریسک مفید هستند.
- متریک‌های خود کارشده: سیستم‌های امنیتی هستند که متریک‌ها را تولید می‌کنند و باید ورودی به گزارش‌های اطلاعاتی را فراهم کنند. نباید گزارش‌های حجیمی تهیه کرد که هیچ کس آن‌ها را نمی‌خواند. همین طور، خروجی‌های خام برخی دستگاه‌ها غیرقابل تشخیص هستند باید خلاصه شوند و از قرار دادن آن‌ها در گزارش اجتناب شود.
- تفسیرهای انسانی: سرانجام مفیدترین اطلاعات امنیت سایبری شامل تجزیه و تحلیل اطلاعات توسط افراد متخصص و باتجربه‌ای است که

می‌توانند داده‌های امنیتی در دسترس را تفسیر کرده و برنامه عمل مناسبی را توصیه کنند. بعید است که این عمل تفسیر، در آینده نزدیکی به صورت خودکار انجام شود.

فعالیت مرتبط با تحقق یک گزارش اطلاعات امنیت سایبری می‌تواند به عنوان یک فرآیند مداوم و تکرارشونده در نظر گرفته شود که از سه کار تشکیل شده است.

(به مطالب زیر توجه کنید).

وظایف جهت ایجاد یک گزارش اطلاعات امنیت سایبری

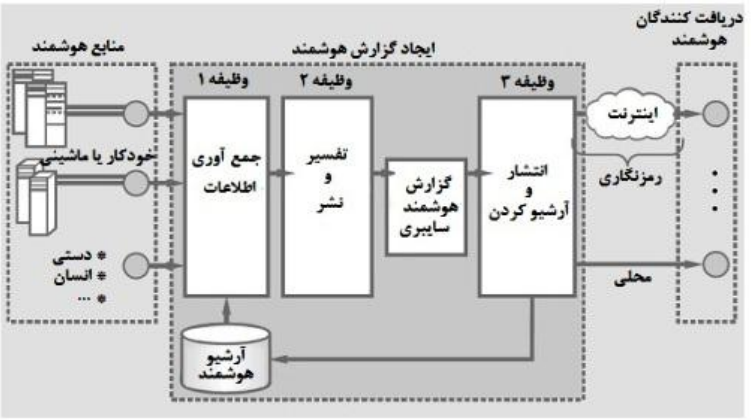
۱- اولین وظیفه؛ جمع‌آوری اطلاعات آسیب‌پذیری‌های قابل‌دسترسی و داده‌های وضعیت امنیتی است. این عمل می‌تواند به صورت خودکار انجام شود؛ ولی باید اجازه دهد افرادی که ممکن است اطلاعات مفیدی داشته باشند، آن را به صورت دستی تسلیم نمایند تا به اشتراک گذارده شود. بسیاری از سازمان‌ها، این جمع‌آوری اطلاعات را در ساعات اولیه صبح، پیش از شروع بخش عمده فعالیت‌های کسب‌وکار، انجام می‌دهند.

(یک کار تجملی که در شرکت‌های جهانی وجود ندارد).

۲- دومین وظیفه؛ تفسیر و انتشار داده‌های جمع‌آوری شده است، به صورت فرآیندی مشابه آنچه در انتشار روزنامه‌ها انجام می‌شود. تفسیرها باید متمرکز بر مدعوین باشد، طوری که هرگز دانش خیلی زیاد یا خیلی کم را از جانب خوانندگان انتظار نداشت. در این مرحله است که خلاصه تفسیر انسانی از داده‌های جمع‌آوری شده نوشته می‌شود.

۳- سومین وظیفه؛ انتشار محافظت‌شده و آرشیو کردن گزارش برای کاربران انتهایی است که نیاز دارند اطلاعات موجود در گزارش را بدانند. معمولاً،

انتقال گزارش با رمزگذاری حفاظت می‌شود و گزارش‌های آرشیوشده و ذخیره‌شده با کنترل‌های دسترسی حفاظت می‌شوند.
(به شکل ۱۰-۶ توجه کنید).



شکل ۱۰-۶- ایجاد و انتشار گزارش اطلاعات امنیت سایبری

یک محصول جانبی ایجاد گزارش اطلاعاتی این است که به هدایت فرهنگ محلی به سمت توجه بیشتر به ملاحظات امنیتی بی‌درنگ و زمان واقعی کمک می‌کند. هر کسی می‌داند که چگونه می‌تواند در هنگام حوادث، مختصر فعالیت‌های واکنشی، راه خود را به سمت مدیران ارشد پیدا می‌کنند که باعث بالا رفتن تمرکز روی دقت و کامل بودن گزارش می‌شود همچنین، اگر حادثه‌ای اتفاق بیفتد که در گزارش‌ها راه نیابد، مدیران می‌توانند در مورد کامل بودن گزارش حادثه سئوال کنند.

۱۰-۴- فرآیند مدیریت ریسک

مدیران سرویس‌های ضروری ملی باید ریسک‌های امنیتی مرتبط با زیرساخت‌های اساسی خود را درک کنند. این کار می‌تواند با استفاده از انواع طبقه‌بندی‌های فانتزی

ریسک، ابزارها و متدولوژی‌ها انجام شود؛ اما رویکرد توصیه‌شده حفظ ساده یک فهرست ارجحیت بندی شده است. بسته به شدت خطرات در لیست، مدیران می‌توانند روی زیرمجموعه‌ای از آن‌هایی که بالاترین خطر را دارند؛ مثلاً؛ تصمیم به تمرکز روی بالاترین ۱۰ یا ۲۰ مورد اول را بگیرند. پس از آن تصمیمات مربوط به تخصیص منابع و بودجه برای امنیت سایبری می‌تواند به وسیله مشخصات ریسک امنیتی سازمان به جلو برده شود. باید در نظر گرفت که فهرست ریسک‌ها باهر تغییری در محیط تهدیدات، به‌کارگیری فناوری‌ها و آسیب‌پذیری‌های گزارش‌شده تغییر خواهد کرد.

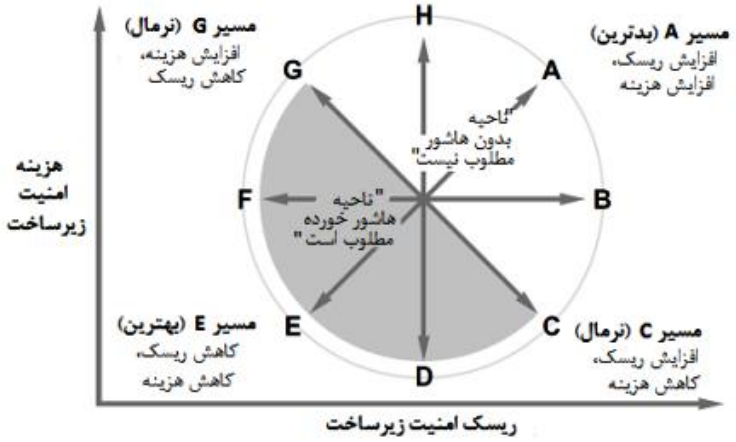
رویکردی که به صورت عمومی برای اندازه‌گیری ریسک امنیتی مرتبط با اجزا خاص مورد توافق قرار گرفته است، با دو برآورد شروع می‌شود:

- محتمل بودن: برآورد محتمل بودن یک حمله که ممکن است به طور موفقیت‌آمیز بر علیه یکی از اجزا خاص و مورد علاقه انجام شود.
- پیامدها: برآورد این است که اگر یک حمله به طور موفقیت‌آمیز انجام شود، چقدر ممکن است نتایج جدی داشته باشد.

این دو برآورد باید در زمینه دامنه عددی مورد توافقی انجام شوند. هنگامی‌که برآوردها افزایش یا کاهش می‌یابند، مقادیر واقعی کمتر از مقادیر نسبی در دامنه مورد نظر اثرگذار خواهند بود. ساده‌ترین و رایج‌ترین مقادیری که به کار می‌روند، اعدا ۱، ۲ و ۲ متناظر با پایین، متوسط و بالا برای هر دو برآورد هستند. هنگامی که محتمل بودن پیامدها تخمین زده شد، ریسک با ضرب دو مقدار محتمل بودن و پیامدها در هم به دست می‌آید؛ بنابراین، اگر برخی از اجزا دارای احتمال بالای حمله باشند (مقدار ۳) و پیامدهای متوسطی از حمله داشته باشند (مقدار ۲)، ریسک مرتبط با آن‌ها ۶=۲*۳ خواهد بود. برای کاهش یک احتمال حمله اگر اقدامات امنیتی به مقدار متوسط (مقدار ۲) انجام شود، ریسک به مقدار ۲*۲=۴ کاهش خواهد یافت. مقدار مطلق ریسک اهمیت کمتری نسبت به مقدار نسبی آن که بر اساس آن تصمیمات گرفته می‌شود، دارد می‌باشد.

یک سازه مفید برای تجزیه و تحلیل تصمیمات امنیتی در زیرساخت، ریسک امنیتی نسبی را با هزینه‌های مربوط به فعالیت‌های توصیه‌شده مقایسه می‌کند. این سازه به مدیران اجازه می‌دهد که مسیرهای تصمیم‌گیری را که ممکن است ریسک امنیتی را افزایش یا کاهش دهد؛ یا بدون تغییر بگذارد، همراه با مفروضاتی در مورد افزایش، کاهش یا بدون تغییر بودن هزینه‌های متناظر آن‌ها در نظر بگیرند.

(به شکل ۱۰-۷ توجه کنید).



شکل ۱۰-۷- ساختار مسیر تصمیم ریسک نسبت به هزینه

برای تفسیر انتخاب‌ها در ساختار مسیر انتخاب، از وسط دیاگرام شروع می‌کنیم و اثرات هر مسیری که از A تا H برچسب‌گذاری شده را در نظر می‌گیریم. (به شکل ۱۰-۷ توجه کنید). مسیر یا برچسب G تصمیم امنیتی را نشان می‌دهد که برای کاهش ریسک، هزینه را افزایش می‌دهد. این یک تصمیم مدیریتی طبیعی است که معمولاً، تا زمانی که بودجه کافی در دسترس باشد، می‌توان از آن دفاع کرد. به طور مشابه، مسیر

با برچسب C نیز یک مسیر طبیعی است؛ زیرا برای کاهش هزینه، ریسک را افزایش می‌دهد که متأسفانه، تصمیم رایجی است.

قابل توجه است که هر مسیر تصمیمی که در ناحیه هاشور زده در شکل باشد، در بسیاری موارد پذیرفته می‌شود؛ زیرا رابطه بین هزینه و ریسک قابل‌قبول است. مسیرهای تصمیم‌گیری در ناحیه بدون هاشور گراف، معمولاً، پذیرفته نمی‌شود؛ زیرا تعادل عجیب و غریبی بین دو عامل هزینه و ریسک است. برای مثال؛ مسیر تصمیم H بدون تأثیر روی ریسک امنیتی هزینه را افزایش می‌دهد. این مورد، متناظر با حالتی است که خیلی زیاد با آن مواجهه می‌شویم جایی که محافظت‌هایی برای امنیت سیستم خریداری‌شده دارای اثر صفر روی مشخصات ریسک هستند.

به طور خلاصه، تمام تصمیمات در مورد حفاظت از زیرساخت ملی باید در زمینه دو ملاحظه مدیریتی صریح گرفته شود:

(۱) حفظ یک فهرست اولویت‌بندی شده از ریسک‌های امنیتی سیستم مورد نظر.

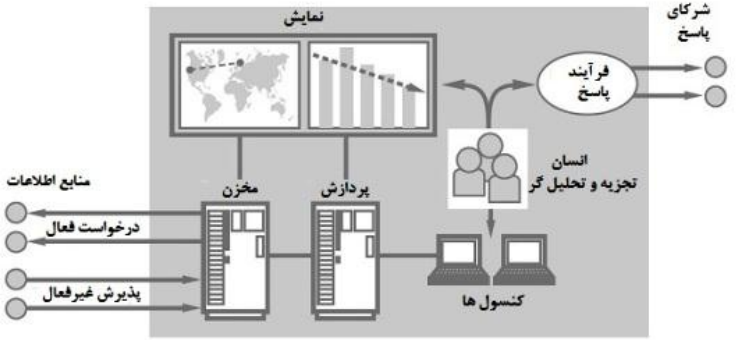
(۲) توجیه تمام تصمیمات به عنوان متناظر با مسیرهای ناحیه هاشور زده از ساختار مسیر تصمیم که در شکل ۱۰-۷ نشان داده شده است.

اگر رعایت این دو نکته ساده اجباری بود، زمان، تلاش و پول قابل‌ملاحظه‌ای برای تیم‌های مدیریت زیرساخت صرفه‌جویی می‌شد.

۱۰-۵- مراکز عملیات امنیت

محسوس‌ترین و قابل دیدترین تحقق آگاهی موقعیت امنیتی بی‌درنگ، مرکز عملیات امنیت یا SOC است که گاهی به آن مرکز ادغام نیز می‌گویند. پایه‌ای‌ترین مدل عملیات SOC؛ شامل؛ چندین ورودی داده، اطلاعات و هوش است که تحلیلگر انسانی برای عملیاتی نظیر تفسیر، همبسته سازی، نمایش، ذخیره‌سازی، آرشیو کردن و تصمیم سازی، آن را به داخل یک مخزن ریخته و از آن استفاده می‌کند. مخزن SOC با

درخواست فعال یا پذیرش غیرفعال اطلاعات ورودی ساخته می‌شود. پردازش اطلاعات؛ تجزیه و تحلیل انسانی را با پردازش خودکار و نمایش بصری ترکیب می‌نماید.
(به شکل ۱۰-۸ توجه کنید).



شکل ۱۰-۸- طراحی سطح بالای مرکز عملیات امنیت (SOC)

بیشتر طراحی‌های SOC با مدل سنتی متمرکزی شروع می‌شوند که در آن امکانات به طور نزدیکی با عملیات مرکز گره خورده است. یعنی روش‌ها و رویه‌هایی ایجادشده‌اند که در آن‌ها فرض می‌شود که منابع SOC شامل تمام نیروی انسانی است در یک محل قرار دارند، بدون اینکه به هیچ‌گونه هماهنگی از راه دور نیاز داشته باشند. تمام داده‌ها در یک مخزن محلی ذخیره‌شده و دریک محل محافظت می‌گردند. این رویکرد مزایای خود را دارد؛ زیرا بسیاری از متغیرهای مرتبط با هماهنگی را از معادله مدیریت حذف می‌کند. یک SOC را می‌توان با منابع توزیع‌شده در مکان‌های پراکنده جغرافیایی نیز ایجاد کرد. مخازن داده می‌توانند توزیع‌شده باشند و تجزیه و تحلیل می‌تواند با استفاده از ابزارهای هماهنگی از راه دور انجام شود. به طور کلی، این رویکرد به کار بیشتری نیاز دارد، مزیت و سود اصلی آن این است که در این رویکرد می‌توان

تحلیلگران خبره بیشتری را استخدام کرد، به خصوص اگر عملیات SOC به صورت ۲۴/۷ یعنی به صورت هر ۲۴ ساعت در ۷ روز هفته حمایت شود. برای حمایت از روش ۲۴/۷ می‌توان متخصصان و کارشناسانی را از سراسر دنیا به صورت "در تعقیب خورشید" استخدام کرد.

توابع معمولی عملیاتی که در SOC حمایت می‌شوند؛ شامل؛ تفسیر انسانی داده‌ها به وسیله کارشناسان، مدیریت حوادث خاصی که به وجود می‌آیند، حمایت خدمات تماس در مواردی که افراد می‌خواهند اطلاعات مرتبط با امنیت را به اشتراک بگذارند و پردازش هشدارها یا بلیط‌هایی که به یک مدیریت تهدید و یا سیستم کشف نفوذ متصل شده‌اند. جنبه ۲۴/۷ عمل SOC، به خصوص برای آگاهی موقعیتی در سطح ملی مفید است؛ زیرا مدیران کلیدی حفاظت از زیرساخت می‌توانند وضعیت موقعیتی امنیتی را در هر زمانی از یک فرد، در تماس با SOC به دست بیاورند. تلاش‌های تدارکات دولتی برای خدمات ملی باید شامل الزامات این نوع پوشش در SOC باشد.

۱۰-۶- برنامه آگاهی ملی

برای بیشتر مدیران امنیتی و مدیران زیرساخت نباید هدف از حمایت از یک دیدگاه سطح ملی از موقعیت امنیتی بحث‌برانگیز باشد. همه موافق‌اند که چنین دیدگاهی برای حمایت تصمیمات مدیریتی در مورد حفاظت از زیرساخت ملی لازم و مفید است. با این حال، چالش در ملاحظات مهم عملی زیر قرار دارد:

- اطلاعات تجاری در مقابل اطلاعات دولتی: دستیابی به آگاهی موقعیتی کامل در سطح ملی نیاز به حمایت قابل‌توجهی از طرف نهادهای تجاری و دولتی دارد. گروه‌هایی که اطلاعات وضعیت امنیتی را ارائه می‌دهند، باید مشوق‌ها و انگیزه‌هایی برای چنین عملی بدهند. توجیه‌های میهن‌پرستانه کمک می‌کند؛ ولی شرکت‌های جهانی باید برای به اشتراک گذاردن اطلاعات با دولت سنجیده‌تر عمل کنند.

- طبقه‌بندی اطلاعات: زمانی که اطلاعات طبقه‌بندی می‌شوند، الزامات مرتبط با اداره آن‌ها افزایش می‌یابد و برای ادغام کردن اطلاعات مشکل ایجاد می‌کند در حقیقت، جوهره محفظه‌ای کردن داده‌ها برای طبقه‌بندی اطلاعات، جلوگیری و اجتناب از هر نوع ادغام مخصوصاً با داده‌های بدون طبقه‌بندی است. در نتیجه، آگاهی موقعیتی در سطح ملی دارای دو دیدگاه است: یکی؛ طبقه‌بندی نشده و عمومی و دیگری؛ بر اساس دیدگاه‌های حساس‌تر از اطلاعات طبقه‌بندی شده.
- سیاست‌های آژانس: آژانس‌های دولتی برای استفاده از اطلاعات به عنوان پایه‌ای برای برنامه‌های سیاسی شامل حمایت از بودجه پروژه‌ها، برنامه‌های استخدامی و توسعه امکانات معروف هستند. این گرایش، مخالف با اهداف به اشتراک‌گذاری اطلاعات برای آگاهی موقعیتی است؛ بنابراین باید با دقت مدیریت شود.
- مسئولیت SOC: اگر یک SOC ملی ایجاد شود، باید سازمانی مشخص شود که آن را اداره کند. تصمیم در مورد اینکه این سازمان باید با وزارت دفاع و یا سازمان‌های غیرنظامی مرتبط باشد، خارج از بحث این کتاب است؛ اما بسیاری از کارشناسان امنیتی معتقدند که ابتکارات آگاهی مرتبط با دفاع فعلی، بسیاری از عناصر لازم را برای عملکرد کامل یک SOC ارائه می‌کند.

اگر به طور مناسبی به این چالش‌ها رسیدگی نشود، ریسک دیدگاه‌های غیر دقیق از آگاهی موقعیتی ایجاد می‌شود. برای مثال؛ اگر یک آژانس از یک آسیب‌پذیری مطلع شود و تصمیم بگیرد که اطلاعات آن را در اختیار دیگران نگذارد، در برآورد ریسک در سطح ملی، یک سوراخ ایجاد می‌شود. به طور مشابه، اگر یک سازمان تجاری نتواند اطلاعات طبقه‌بندی شده را دریافت و پردازش کند، دیدگاه آن‌ها از موقعیت ریسک امنیتی جاری، دقیق نخواهد بود. شاید توجه به مدیریت این مسائل بر اساس روش مورد به مورد، به عنوان قسمتی از وظایف یک SOC، بهترین رویکرد باشد.

فصل ۱۱: پاسخ و واکنش

واکنش به حادثه بخش مهم و حیاتی از هر برنامه موفق فناوری اطلاعات است که اغلب، نادیده گرفته می‌شود تا اینکه مسئله اورژانس امنیتی بزرگی اتفاق بیفتد و باعث شود مقدار زیادی از وقت و پول مصرف شود. هنوز، از فشار عصبی که یک بحران ایجاد می‌کند، حرفی نزده ایم.[۱۴] Kenneth Van Wyk and Richard Forno

آشناترین جز هر برنامه امنیت سایبری، فرآیند واکنش و پاسخگویی به حوادث است. این فرآیند شامل کلیه فعالیت‌هایی در مورد امنیت است که به علت حمله‌ای نزدیک، مشکوک، در حال انجام یا پایان یافته شروع می‌شوند. معمولاً، پاسخ به حادثه برای محیط محلی در یک سازمان بهینه شده است، اما در بیشتر حالات شامل حداقل چهار فاز متمایز فرآیند به صورت زیر است:

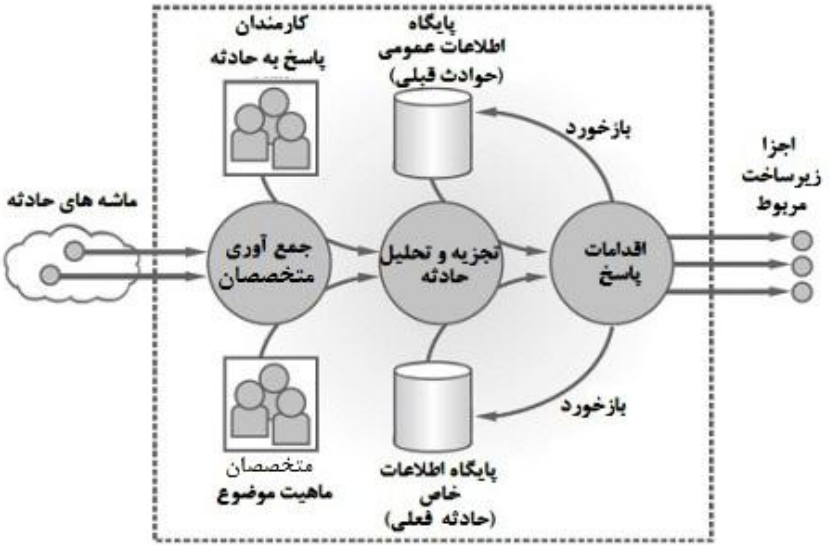
- تریگر حادثه: برخی هشدارها یا رویدادها باید باعث تریگر شروع و راه‌اندازی فرآیند پاسخ و واکنش شوند. بدیهی است که اگر این تریگر شامل سیستمی باشد که قبلاً مورد حمله بدخواهانه قرار گرفته است، واکنش باید بر بازسازی و بازیافت فاجعه متمرکز باشد. اگرتریگر شامل یک هشدار اولیه است، امکان دارد که فرآیند پاسخ به حادثه بتواند از آثار منفی قابل دید و مهم جلوگیری کند.
- جمع کردن کارشناسان: گردهمایی کارشناسان مناسب، برای تجزیه و تحلیل وضعیت و ارائه توصیه‌های مناسب است. بیشتر سازمان‌ها مجموعه پایه‌ای از کارمندان متخصص واکنش به حادثه دارند که روی حوادث کار می‌کنند و مخزنی از اطلاعات مرتبط با حوادث قبلی را مدیریت می‌نمایند. همچنین، برای کار کردن روی جزییات حادثه یک متخصص

موضوع خاص به داخل فرآیند واکنش آورده می‌شود. این کارشناسان یک پایگاه اطلاعات محلی مرتبط با حادثه اتفاق افتاده را ایجاد می‌کنند.

- تجربه و تحلیل حادثه: تجزیه و تحلیل حادثه، وظیفه اصلی کارشناسانی است که در طی واکنش به حادثه دور هم جمع می‌شوند. تجزیه و تحلیل‌ها می‌تواند شامل فارنسیک فنی مشروح، تجزیه و تحلیل داده‌های شبکه و حتی امتحان فرآیندهای کسب‌وکار باشد. معمولاً، مشکل‌ترین قسمت هر تجزیه و تحلیل شامل دانستن علل زمینه‌ای حادثه است. زمانی که این موضوع مشخص شد، توسعه بهترین راه حل، هدف کلیدی خواهد بود.
- فعالیت‌های پاسخ و واکنش: خروجی هر فرآیند واکنش به حادثه، مجموعه‌ای از توصیه‌های مدیریتی در مورد چگونگی مقابله با حادثه است. این توصیه‌ها، معمولاً، شامل بازسازی سیستم، کار در مورد مسائل، مطلع ساختن مشتریان و نظیر آن‌ها است. ارائه این اطلاعات به افراد و سازمان‌های مرتبط، مستلزم این است که تیم‌های واکنش به حادثه به درستی بدانند که چه گروه‌هایی مسئول کدام عملکردها هستند.

فرآیندهای خاص واکنش به حادثه، از سازمانی به سازمان دیگر متفاوت هستند؛ اما تقریباً فرآیند هر شرکت یا آژانس بر اساس نسخه‌ای از این چهار عنصر می‌باشد و شامل فرآیندهای واکنش به حادثه محلی سازمان و منابع واکنش‌های خاص است که برای شهروندان، کسب و کارها و گروه‌های دولتی به وجود آمده‌اند.

(به شکل ۱۱-۱ توجه کنید).



شکل ۱۱-۱- طرح عمومی فرایند واکنش به حادثه

با وجود اشتراک ذاتی در فرآیندهای واکنش به حادثه که در شرکت‌ها و آژانس‌های مختلف یافت می‌شود، تفاوت‌های بزرگی در الگوی موفقیت آن‌ها وجود دارد. بیشترین اختلاف‌ها در مؤثر بودن نسبی واکنش به حوادث، در جلوگیری به جای تنها واکنش ساده به مسائل جدی زیرساخت است. برای بهینه کردن جنبه‌های هشدارهای اولیه واکنش به حادثه، باید برخی ملاحظات کلیدی را به خوبی درک کرد. این جنبه‌های کلیدی شامل تمرکز بر واکنش قبل از حادثه به جای بعد از حادثه، درک جزییات اینکه چه چیزهایی یک نشانه معتبر هشدار است، ساختار مناسب اینکه چگونه یک تیم واکنش به حادثه باید مدیریت شود، بهترین شیوه‌های عمل برای تجزیه و تحلیل فارنسیک، تعامل بهینه با مجریان قانون و فرآیندهای خوب برای بازیابی از فجایع. در مورد این عناصر در زیر به طور مفصل بحث شده است، با تأکید بر اینکه چگونه فرآیندهای واکنش زیرساخت ملی باید ساخته‌شده و عمل نمایند.

۱۱-۱- واکنش قبل، نسبت به بعد از حمله

بحرانی‌ترین فاکتور متمایزکننده بین فرآیندهای واکنش به حادثه شامل دو نوع تریگر اساسی است که واکنش‌های به حوادث را شروع می‌کنند. اولین نوع تریگر، آثار ملموس و قابل‌مشاهده یک حمله یا حادثه بدخواهانه است. معمولاً، کاربران انتهایی آثار آن را به صورت عملکرد کند و تنبل شده برنامه‌های کاربردی، عملکرد دروازه‌های مسدود، ناتوانی در دریافت پست الکترونیکی، دسترسی به اینترنت کند و یا غیرقابل‌دسترسی ملاحظه می‌کنند. واکنش به حادثه در این موارد فوری و معمولاً متأثر، از شکایت زبانی از طرف کاربر انتهایی است. نوع دوم تریگر شامل هشدار زودهنگام و اطلاعات نشانه‌ها است که در اطلاعات برخی سیستم‌ها یا اطلاعات مدیریت شبکه جاسازی شده‌اند. معمولاً، این تریگرها را کاربران انتهایی مشاهده نمی‌کنند اما مستعد تولید سطح بالایی از واکنش‌های مثبت کاذب هستند که در آن هشدارها واقعاً به یک عمل بدخواهانه مرتبط نیستد.

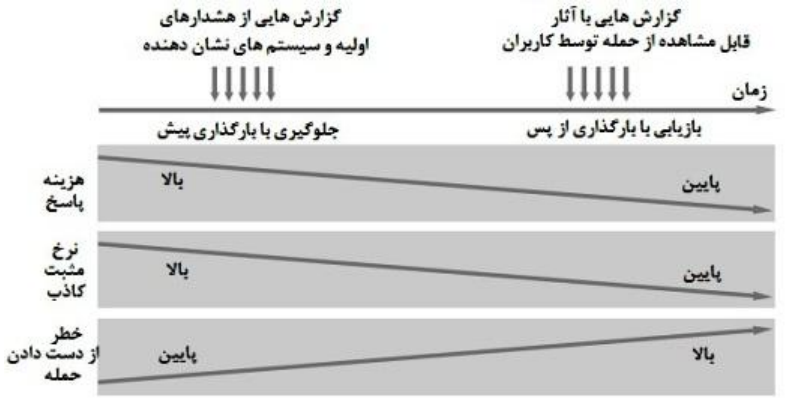
بنابراین، فرآیندهای واکنش به حوادث می‌توانند بر اساس درجه‌ای که با این تریگرها برخورد می‌شود، به دو رویکرد خاص طبقه‌بندی می‌شوند.

- پیشگیری بارگذاری شده، پیش از حمله: فرآیندهای واکنش به حوادثی است که مخصوصاً برای جمع‌آوری نشانه‌ها و اطلاعات هشدارها برای پیشگیری زودهنگام از حملات امنیتی طراحی‌شده‌اند. مزیت این فرآیندها در این است که ممکن است با تمرکز زودهنگام برخی حملات را خنثی کنند، اما عیب آن‌ها این است که باعث میزان بالایی از واکنش‌های مثبت کاذب می‌شوند که می‌توانند هزینه‌های واکنش به حادثه را به طور چشمگیری افزایش دهند.

- بازیابی بارگذاری شده، پس از حمله: فرآیندهای واکنش به حادثه‌ای است که برای جمع‌آوری اطلاعات از منابع مختلفی طراحی‌شده‌اند که می‌توانند

اطلاعات ملموس و قابل دیدی را در مورد حمله‌ای ارائه دهند که ممکن است در حال انجام یا کامل شده باشد. این رویکرد میزان مثبت‌های کاذب را کاهش می‌دهد؛ اما برای متوقف کردن حمله بر اساس داده‌های هشدارهای زودهنگام مؤثر نیست.

فرآیندهای واکنش به حادثه دورگه که سعی در پردازش هر دو نوع اطلاعات در دسترس را دارند نیز قطعاً ممکن است، اما نکته تصمیم واقعی این است که آیا از نظر زمان، منابع و پول لازم روی پیشگیری بارگذاری شده از پیش، سرمایه‌گذاری کنیم، یا خیر. این دو نوع فرآیند را می‌توان روی خط زمانی اطلاعاتی نشان داد که در زمانی در اختیار تیم امنیتی قرار می‌گیرد که حمله جلو می‌رود. برای فرآیندهای پیشگیرانه بارگذاری شده از پیش، هزینه‌های واکنشی مربوطه و نرخ‌های مثبت کاذب بالا است، اما ریسک مرتبط با از دست دادن اطلاعات که می‌توانند حمله را علامت دهند، پایین‌تر است. برای فرآیندهای واکنش بارگذاری شده از پس، مقادیر بالا معکوس هستند. (هزینه‌ها پایین‌تر، ریسک گم شدن اطلاعات بالاتر) (به شکل ۱۱-۲ توجه کنید).



شکل ۱۱-۲- مقایسه فرآیندهای واکنشی بارگذاری شده از پیش و پس

واکنش به حوادث بارگذاری شده از پس ممکن است برای اجزا زیرساخت کوچک‌تر و کمتر حیاتی قابل‌قبول باشد، اما برای حفاظت از خدمات ملی ضروری در مقابل حملات سایبری تنها گزینه عاقلانه، تمرکز روی پیشگیری بارگذاری شده از پیش، برای این مسائل است. زیرساخت ملی، با تعریف خود، سرویس‌های ضروری را حمایت می‌کند. بنابراین، هر فرآیندی که برای تنزل این سرویس‌ها طراحی شده باشد، با ماهیت اصلی زیر ساخت در تضاد است. اولین پیامد این است که هزینه‌های مربوط به واکنش به حادثه در حفاظت از زیرساخت ملی نسبت به وضعیت‌های مربوط به شرکت‌های معمولی، گرایش به بالاتر بودن خواهند داشت. پیامد دوم این است که متریک آشنای مثبت کاذب را که معمولاً، در محیط بنگاه‌های تجاری به عنوان کاهش‌دهنده هزینه یافت می‌شود، باید از واژگان مدیران حفاظت از زیرساخت ملی حذف کرد.

۱۱-۲- نشانه‌ها و هشدارها

با توجه به اهمیت پیشگیری‌های از پیش بارگذاری شده، مبتنی بر نشانه‌های زودهنگام و اطلاعات در حفاظت از زیرساخت ملی، ضروری است که انواع تریگرهای اولیه‌ای را توضیح دهیم که برای آغاز و راه‌اندازی فرآیندهای واکنش بکار می‌روند. به علت اینکه این تریگرها بین سازمان‌ها به خاطر تفاوت‌های آشکار در محیط‌های مربوطه‌شان تغییر خواهند کرد، بهترین کاری که می‌توان انجام داد، دسته‌بندی انواع مختلف تریگرها در داخل یک طبقه‌بندی گسترده است. آشکار است که برخی از عناصر طبقه‌بندی با بیشتر متدولوژی‌های فعلی سازگار هستند؛ درحالی‌که، دیگر عناصر کاملاً با شیوه عمل جاری متفاوت بوده و احتیاج به ارتقا فرآیند دارند.

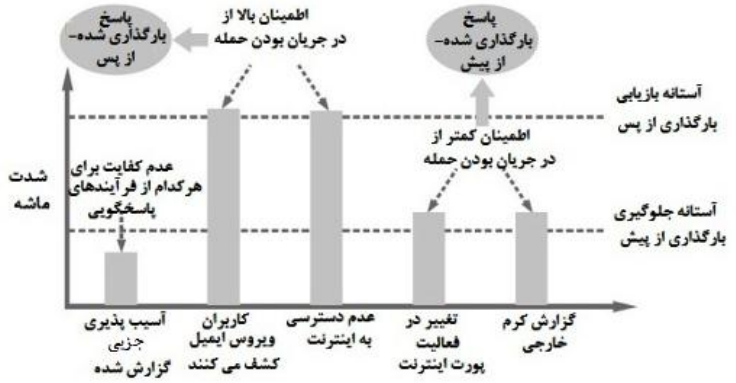
طبقه‌بندی تریگرهای فرآیند هشدار زودهنگام

طبقه‌بندی تریگرهای فرآیند هشدار زودهنگام شامل:

- اطلاعات آسیب‌پذیری: اطلاع از هر آسیب‌پذیری جدید یک تریگر بدیهی برای پیشگیری بارگذاری از پیش است. آسیب‌پذیری ممکن است هرگز مورد سواستفاده قرار نگیرد، اما تیم‌های واکنش باید گزینه‌های محتمل را تجزیه و تحلیل کنند و برای توسعه قدم‌های پیشگیرانه برای اطمینان از اینکه این نتواند اتفاق بی افتد کار نمایند. در بیشتر موارد آسیب‌پذیری توسط فروشنده گزارش می‌شود که این حاکی از این است که آن‌ها بایستی تبدیل به قسمتی از فرآیند واکنش به حادثه محلی بشوند.
- تغییرات در متریک‌های مشخصات رفتاری: تیم واکنش به حوادث باید از تغییرات معنی‌دار در هر متریک رفتاری اندازه‌گیری شده، به عنوان تریگر راه‌اندازی فرآیند استفاده کند که می‌تواند شامل تغییر رفتار شبکه، تغییرات در استفاده از پردازنده یا تغییر در برخی مشخصات برنامه‌های کاربردی باشد. شروع فرآیند واکنش به حادثه، به عنوان یک نتیجه تغییرات رفتاری، انحرافی چشمگیر از فرآیندهای واکنش به حوادث فعلی در بیشتر سازمان‌ها است.
- انطباق با الگوی متریک حمله: اگر امضا یا الگوی متریک حمله در برخی کاربردها، سیستم‌ها یا شبکه کشف شود، واکنش به حادثه پیشگیرانه امر می‌کند که تجزیه و تحلیل روی‌داده‌های برای پیامدهای امنیتی انجام شود. این نیز یک انحراف از رویکردهای فعلی واکنش به حادثه است.
- ناهنجاری‌های اجزا: هر رفتار غیرعادی که در یک جز زیرساخت کشف شود، نشانگر یک تریگر برای واکنش به حادثه است. بدیهی است که بیشتر ناهنجاری‌های رفتاری شدید یافته شده در بیشتر اجزا حیاتی زیرساخت، فرآیندهای پاسخگویی بزرگ‌تری را تریگر خواهند کرد.

- اطلاعات حمله خارجی: اطلاعاتی است که از منابع خارجی در مورد حملاتی می‌آیند که ممکن است مسائل محلی باشد که می‌توانند فرآیند واکنش به حادثه را تریگر نمایند. برای حفاظت از زیرساخت ملی، اگر اطلاعاتی که از منبع معتبری می‌آید، در مورد سیستم‌ها و فناوری‌هایی باشد که دارای اهمیت محلی هستند، این مسئله می‌تواند حتی مهم‌تر هم باشد.

یک راه جهت مشاهده تفاوت بین روش‌های بارگذاری از پیش و پس، در زمینه شدت تریگر لازم برای شروع فرآیند واکنش به حادثه است. برای رویکردهای تریگری که در بالا فهرست شد، باید اطلاعات کافی وجود داشته باشد تا تیم واکنش به حادثه را مجبور به عمل فوری نماید. در زمینه‌های متعارف‌تر و آشناتر، این تریگرها برای چنین اعمالی نباید کافی باشند. (به شکل ۱۱-۳ توجه کنید).



شکل ۱۱-۳- مقایسه آستانه‌های شدت تریگر برای واکنش

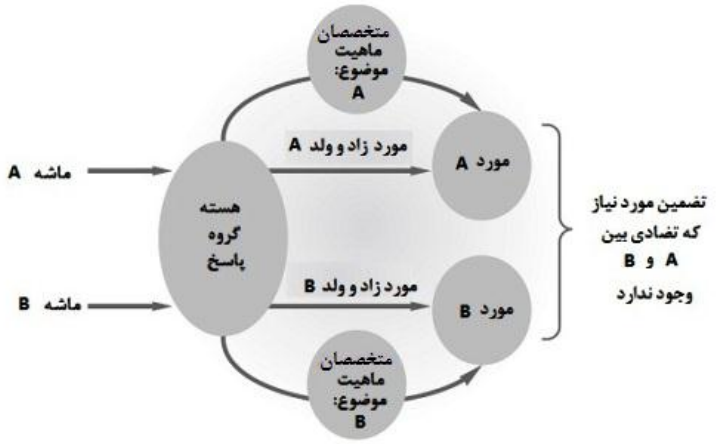
تریگرها برای واکنش بارگذاری شده از پیش در یک جنبه مهم، مشترک هستند. این تریگرها اطلاعات جزیی را ارائه می‌دهند که ممکن است حمله ممکنی را علامت دهد. این اطلاعات می‌تواند در زمینه‌های غیرامنیتی نیز تفسیر گردند. بنابراین، وظیفه اصلی تیم واکنش به حادثه در پیشگیری بارگذاری شده از پیش، این است که این اطلاعات جزیی را در کنار هم قرار داده و تا حد ممکن یک تصویر کامل ارائه دهند؛ از این تصویر کلی، باید محافظه‌کارانه ترین توصیه برای حفاظت از زیرساخت ملی ارائه شود. یعنی، اگر تیم پیشگیری از انجام حادثه در حال وقوعی مطمئن نیست، باید فرض کند که حمله‌ای در حال انجام است. این باعث بالا رفتن هزینه و کاهش راحتی کارکنان محلی می‌گردد. گرچه این مسئله به اشتباه به سمت احتیاط رفته است؛ ولی برای حفاظت از زیرساخت ملی مناسب می‌باشد.

۳-۱۱- تیم‌های واکنش به حادثه

تیم واکنش به حادثه بهینه، برای حفاظت از زیرساخت ملی دو جز متفاوت دارد.
اول، هسته‌ای از افراد که فرآیند واکنش به حادثه را مدیریت می‌کنند؛ از مخزن اطلاعات مربوطه نگهداری می‌نمایند؛ تمام داده‌های مرتبط با حادثه را مستند می‌کنند؛ جلسات توجیهی برای هر کسی که در این فرآیند نفع می‌برد، برگزار می‌کنند؛ و تعامل با تیم‌های دیگر واکنش به حوادث را انجام می‌دهند.
دوم، زمانی که سیستم مورد حمله قرار می‌گیرد، باید یک مجموعه پویا از کارشناسان موضوع حادثه را که مسئله را بهتر می‌فهمند، به داخل فعالیت‌های واکنش به حادثه آورده شوند.

در موقعیت‌های خیلی پیچیده، تیم هسته واکنش به حادثه، احتمالاً، روی چند حادثه به طور همزمان کار می‌کند؛ معمولاً، با مجموعه‌های متفاوتی از کارشناسان موضوع مورد حمله سروکار دارد. بنابراین، تریگرهای واکنش باعث تولید موارد جدیدی می‌شود که تا کامل شدن موفقیت‌آمیز واکنش به صورت موازی باهم کار می‌کنند. در محیط‌های

کوچک‌تر، به ندرت چند کار همزمان اجرا می‌شوند، اما در مورد زیرساخت‌های حیاتی پیچیده، یافتن زمان‌هایی که چند مورد واکنش به حادثه همزمان در حال اجرا نباشند، غیرعادی خواهد بود؛ بنابراین، اطمینان از اینکه فعالیت‌های واکنش به حادثه همزمان و موازی متقابلاً باهم در تعارض نباشند، عمل به یکی از تعهدات واکنش به حادثه در حفاظت از زیرساخت ملی است. (به شکل ۱۱-۴ توجه کنید).



شکل ۱۱-۴- مدیریت موارد واکنش به طور همزمان

متأسفانه، مفهوم مدیریت واکنش همزمان در حوزه امنیت کامپیوتری معمولی ناشناخته؛ است زیرا هر سازمان خیلی بزرگ سرانجام به این نتیجه خواهد رسید که در حالت طبیعی، همه‌ی این موارد موازی و همزمان می‌تواند وجود داشته باشند. همچنین، سناریوهای حملات در سطح ملی با نتایج بالقوه بسیار جدی برای زیرساخت، به طور روتین شامل حملات چندگانه همزمان به همان شرکت یا آژانس هستند. تیم‌های واکنش به حادثه باید در محیط‌های ملی برای مدیریت چندگانه و همزمان موارد واکنش

به حوادث مختلف برنامه‌ریزی کنند. برخی ملاحظات که به ما برای برنامه‌ریزی مناسب برای این حالات ممکن، کمک می‌کنند، شامل موارد زیر است:

- پرهیز از افراد با یک نقطه تماس منحصربه‌فرد: اگر فردی مدیریت فرآیندهای واکنش به حادثه را به عهده دارد، خطر ازدحام موارد مدیریتی به وجود می‌آید؛ ممکن است یکی از جزییات مدیریتی کم اهمیت و کوچک به نظر برسد، اما با توجه به اهمیت واکنش، به خصوص در سناریوهای بازیابی، باید از این ضعف‌ها دوری کرد.
- اتوماسیون مدیریت پرونده‌ها: استفاده از خودکارسازی و اتوماسیون در مدیریت، لاگ کردن، بایگانی کردن موارد واکنش به حادثه، باعث بهبود بهره‌وری تیم هسته واکنش به حوادث می‌گردد و می‌تواند منجر به تجزیه و تحلیل ساده‌تر شود، به خصوص اگر اطلاعات موارد قبلی برای جستجو و پرس و جوی اتوماتیک در دسترس باشد.
- حمایت سازمانی برای دخالت متخصصان و کارشناسان: در صورت درخواست برای واکنش به حوادث سازمان باید همه امکانات و کارشناسان را در اختیار تیم واکنش قرار دهد. زمانی که این فرآیند از روش بازیابی بارگذاری از پس، پیروی کند، به علت اینکه هر کسی از نتایج حادثه آگاه است، این مسئله بحث‌برانگیز نخواهد بود. ولی هنگامی‌که از رویکرد پیشگیری بارگذاری شده از پیش، استفاده می‌شود، تریگرهایی که نسبت به حادثه واکنش نشان می‌دهند، زیرکانه‌تر عمل خواهند کرد و این مسئله چالش‌برانگیزتر است.
- حمایت عملیاتی ۲۴/۷: بدون پوشش ۲۴/۷ کامل در هر روز هفته در هر سال، احتمال موفقیت آمیز مدیریت موارد واکنش به حوادث چندگانه همزمان، به طور قابل ملاحظه‌ای کاهش می‌یابد. بیشتر سازمان‌ها عملکرد

و قابلیت واکنش به حوادث خود را در یک SOC یکپارچه می‌کنند تا پوشش مدیریتی مناسب تضمین شود.

یک گرایش اخیر در مدیریت زیرساخت، برون‌سپاری بعضی عملیات امنیتی به اشخاص ثالث است. برای نظارت بر حالت برخی دستگاه‌های امنیتی؛ مثل؛ دیوارهای آتش و سیستم‌های تشخیص نفوذ، این یک فعالیت به بلوغ رسیده‌ای می‌باشد و اثرات مادی منفی روی تلاش‌های فعالیت امنیت محلی نخواهد گذاشت؛ مگر اینکه شرکت برون‌سپاری شده نامناسب و بی‌صلاحیت باشد. حتی برای برخی از عملیات SOC، برو نسپاری یک ایده بسیار عالی است، به خصوص به علت اینکه اگر دیدگاه وسیع باشد، جمع‌آوری و همبسته سازی مؤثرتر است. برون‌سپاری عملیات SOC می‌تواند برای تیم امنیتی دسترسی به مهارت‌های فنی را ایجاد کند که ممکن است به صورت محلی موجود نباشد.

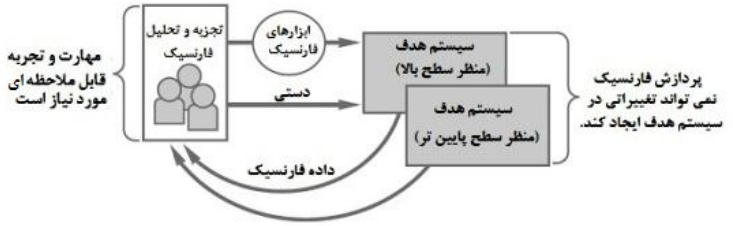
فرآیندهای واکنش به حادثه، به علت طبیعت تلاش‌های بازیابی و جلوگیری، تعبیه شده در زیرساخت محلی، برون‌سپاری کامل می‌تواند ناشیانه باشد. قطعاً، ارائه دهندگان خدمات برون‌سپاری یا فروشندگان می‌توانند و باید کمک کنند و متخصصان SOC ممکن است رهنمودها و توصیه‌های عالی و ارزشمندی را به صورت شخص ثالث ارائه نمایند. نهایتاً، واکنش به حادثه باید یک عملکرد مدیریت محلی باشد و سازمان چاره‌ای جز صرف کردن وقت، انرژی و منابع برای اطمینان از این ندارد که تصمیمات مدیریت محلی درست گرفته شود. اشخاص ثالث، هرگز، نمی‌توانند فعالیت‌ها را اولویت‌بندی کنند؛ یا فرآیندهای بازیابی را به خوبی خود سازمان متناسب محیط محلی نمایند. در عوض، آن‌ها باید برای تقویت عملکردهای محلی برای ارائه رهنمودهای کارشناسی، اتوماسیون فرآیندها و مدیریت دستگاه‌ها و شبکه‌ها مورد استفاده قرار گیرند تا جمع‌آوری داده‌ها و همبسته سازی را حمایت و به بازیابی کمک کنند.

۱۱-۴- تجزیه و تحلیل فارنسیک

تجزیه و تحلیل فارنسیک، شامل فعالیت‌های لازم برای بررسی علل ریشه‌ای و محتوایی برخی حوادث در هر دو سطح بالا یعنی کلیات و سطح پایین یعنی مشروح و جزییات است. نمونه‌هایی از سئوالاتی که در طی فرآیند تجزیه و تحلیل فارنسیک به آن‌ها پرداخته می‌شود؛ عبارت‌اند از:

- علل ریشه‌ای: چگونه سیستم، هدف حمله قرار گرفت؟
- ابزارهای: از چه آسیب‌پذیری‌ها یا ابزارهایی در حمله استفاده شده است؟
- حالت: آیا دشمن، هنوز، در حال حمله به سیستم است؟
- پیامدها: چه اجزایی از سیستم، خوانده، دزدیده، تغییریافته یا مسدود و بلاک شده‌اند؟
- اقدام: چه اقداماتی حمله‌ی درحال انجام را متوقف یا از انجام آن در آینده جلوگیری می‌کند؟

برای پاسخ به این سئوالات مشکل، در حین واکنش به حادثه، تجزیه و تحلیل فارنسیک، احتیاج دارد برای جمع‌آوری اطلاعات مربوطه عمیقاً به داخل سیستم هدف مورد نظر کشیده شود. این عمل باید طوری انجام شود که هرگز، روی شواهد کلیدی اثر نگذارد و آن‌ها را نابود نکند؛ یا تغییر ندهد. این یک نیاز حیاتی است؛ زیرا ممکن است تجزیه و تحلیل ناشیانه و خام فارنسیک روی فایل‌های مهم بنویسد؛ زمان‌های مهرشده روی منابع سیستم را عوض کند؛ یا روی قسمت‌هایی از حافظه بازنویسی نماید که شواهد حیاتی دارد. تجزیه و تحلیل فارنسیک یک کار مشکل است که به مهارت بالا، لیاقت و همین طور توانایی تحقیق و بررسی در یک سیستم، هم به طور دستی و هم با کمک ابزارهای خاص، نیاز دارد. (به شکل ۱۱-۵ توجه کنید).



شکل ۱۱-۵- نمودار عمومی فرآیند فارنسیک سطح بالا

فرآیند فارنسیک روی یک کامپیوتر، برای تعیین این است که چگونه، کی و کجا برخی حوادث در آن کامپیوتر اتفاق افتاده که نتیجه عمل سخت‌افزار، نرم‌افزار، انسان یا شبکه می‌باشد. برای مثال؛ معمولاً، گروه‌های امنیتی شرکت‌ها، تجزیه و تحلیل فارنسیک را روی یک کامپیوتر زمانی انجام می‌دهند که صاحب آن کامپیوتر مشکوک به نقض بعضی رهنمودها یا الزامات باشد. گروه‌های مجری قانون اقدامات مشابهی را روی کامپیوترهای ضبط‌شده از افراد مشکوک که به ارتکاب جنایت متهم هستند انجام می‌دهند. به هر حال، کسب ادله و شواهد قانونی می‌تواند روی هدفی خیلی وسیع‌تر از یک کامپیوتر انجام شود. به خصوص برای حفاظت از سرویس‌های ضروری ملی، سازمان باید دارای توانایی تجزیه و تحلیل فارنسیک روی کل زیرساخت حمایتی آن سرویس باشد.

نوشتن مهارت‌های فنی مورد نیاز جهت انجام چنین تجزیه و تحلیل فارنسیک وسیع و گسترده آسان است؛ ولی استخدام پرسنل واجد شرایط همیشه، آسان نیست. این مسئله برای بیشتر سازمان‌های بزرگ چنان شدید و جدی است که غیرمعمول نیست که یک شرکت یا آژانس هیچ کارشناس محلی بامهارت کافی برای هدایت مناسب بررسی حملات گسترده به زیرساخت نداشته باشد. این موضوع پذیرفتنی نیست؛ زیرا تنها گزینه برای آن سازمان؛ محل یابی این استعدادها در خارج سازمان است و باعث

فرآیند ارزیابی کم آشناتری از محیط سازمان خواهد شد. کارمندانی با قراردادهای درازمدت که متعهد بکار حرفه‌ای و شغلی در سازمان هستند، همیشه، نسبت به مشاوران یا اشخاص ثالث آگاه‌تر هستند. همچنین، آن‌ها برای بررسی حادثه‌ای که منجر به تعطیلی طولانی محیط محلی می‌شود، به طور مناسبی قابل‌اطمینان هستند.

به این ترتیب، بیشتر شرکت‌ها و آژانس‌ها باید به اندازه کافی عاقلانه عمل کرده و مجموعه‌ای از استعدادها را با این مهارت‌ها بسازند و پرورش دهند. معمولاً برای نگهداری و جلب رضایت کارشناسان فارنسیک، رعایت چند چیز زیر لازم است:

- فرهنگ آزادی نسبی: بیش‌ترین تحلیلگران فارنسیک کاردان، افراد خلاقی هستند که حرفه خود را با بررسی و کشف مطالب آموخته‌اند و تمایل آن‌ها به حفظ مهارت‌هایشان به کمک بررسی‌ها و اکتشاف‌هایشان تداوم می‌یابد. بنابراین، سازمان‌ها باید به آن‌ها آزادی برای جست‌وجو و تحلیل سیستم‌ها، شبکه‌ها، برنامه‌های کاربردی و دیگر عناصر مورد علاقه‌شان را بدهند. هنگامی‌که آن‌ها روی یک حادثه کار می‌کنند، هدفشان مشخص است؛ اما هنگامی‌که آن‌ها روی چیز مشخصی کار نمی‌کنند، مدیران باید به آن‌ها آزادی عمل بدهند که بر روی آنچه خود مناسب می‌دانند، تحقیق کنند. این برای بعضی مدیران کار آسانی نیست، به خصوص در سازمان‌هایی که نسبتاً به بلوغ رسیده‌اند و کنترل‌های سختی برای کارمندان خوددارند.
- دسترسی به فناوری‌های جالب: خوشحال نگه‌داشتن تحلیلگران فارنسیک یکی از نیازهای مرتبط با محیط محلی است که با دسترسی دایمی به فناوری‌های در حال ظهور، متغیر و جالب امکان‌پذیر می‌شود. مأمور کردن بهترین کارشناس فارنسیک به عملیات روزمره با یک فناوری تنها، بهترین ایده نمی‌باشد.

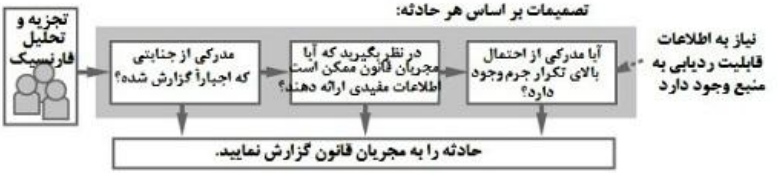
- توانایی برای تعامل با خارج: تحلیلگران فارنسیک، همچنین برای فراگیری از کارشناسان خارج از سازمان، به آزادی عمل در تعامل نیاز دارد. این تعامل باید مجاز بوده و تشویق شود.

این عناصر محیطی منحصر به کارشناسان امنیتی نیستند، بلکه از میان تمام مجموعه‌های مهارتی مورد نیاز در زمینه حفاظت از زیرساخت ملی انتخاب می‌شوند؛ بنابراین، به دست آوردن تجزیه و تحلیل فارنسیک برای سازمان از همه مشکل‌تر است. تحلیلگران فارنسیک کاردان بر بالاترین قسمت دریافت حقوق در بازار کار حکومت می‌کنند و حفظ آن‌ها برای سازمان مشکل است، به خصوص در مشاغل دولتی با حقوق نسبتاً پایین. اگر سازمان داشتن توانایی اجرای تحلیل فارنسیک را به عنوان قسمتی از فرآیند واکنش به حوادث انتخاب کند، باید به کیفیت زندگی و کار تحلیلگران فارنسیک توجه کند.

۱۱-۵- مسائل مربوط به اجرای قانون

مسئله عمومی که تیم‌های واکنش به حوادث با آن مواجه‌اند، این است که آیا باید یک حادثه خاص را برای حمایت به مجریان قانون ارجاع داد، یا خیر. بیشتر کشورها قوانینی دارند که تیم‌های واکنش به حوادث را مجبور می‌کنند که در مواردی که بعضی جرائم اتفاق می‌افتد، با گروه‌های مجری قانون تماس بگیرند. گروه‌های واکنش به حوادث باید با این قوانین آشنا باشند و بدون سئوال از آن‌ها اطاعت کنند. آن‌ها پس از بررسی کامل قانونی توسط شورای حقوقی سازمان می‌توانند در فرآیند واکنش به حادثه درگیر شوند. موضوع دخالت مجریان قانون به خصوص هنگامی که زمان و کوشش زیادی در جهت مقابله با حادثه مصرف شده باشد، با ملاحظات عاطفی نیز همراه خواهد بود. تیم‌های واکنش به حوادث، معمولاً، آرزو می‌کنند که مجازات‌های ملموسی را ببینند که شاید شامل به زندان رفتن افراد بدخواه باشد.

در پایان، برای تعامل با مجریان قانون برای حفاظت از زیرساخت باید از فرآیند روتین و سنجیده‌تری پیروی کنند. حفاظت از زیرساخت ملی یک هدف منحصربه‌فرد است که تحویل دقیق و مداوم سرویس‌های ضروری به شهروندان و کسب و کارهای یک ملت را تضمین می‌کند. این هدف، شامل دستگیری افراد بدخواه و به زندان انداختن آن‌ها نیست. حتی اگر تیم‌های امنیتی علاقه‌مند به این نتیجه باشند. نتیجه اینکه درگیری احتیاطی مجریان قانون تنها هنگامی باید در نظر گرفته شود که تیم امنیتی معتقد باشد این درگیر شدن کمکی به حادثه جاری شاید از طریق ارائه بعضی داده‌های مرتبط و اشارات کند و بتواند از حوادث آتی جلوگیری کند. که این کار با دور کردن گروه‌هایی انجام می‌شود که به نظر تکرارکننده جرم هستند. یک فرآیند تصمیم‌گیری برای درگیر شدن مجریان قانونی در شکل ۱۱-۶ نشان داده شده است.



شکل ۱۱-۶- فرآیند تصمیم‌گیری برای دخالت مجریان قانون در فارنسیک ها

این فرآیند تصمیم‌گیری، از نیاز آشکاری حمایت می‌کند که بر اساس آن، جرائم گزارش می‌شوند. شکل فوق جنبه‌های مبهم و فازی امنیت سایبری را برجسته می‌کند؛ برای اثبات اینکه جرمی اتفاق افتاده است ،کشف رفتار مشکوک در یک شبکه کامپیوتری، معمولاً، مدرک کافی تلقی نمی‌شود.حتی اگر مدرکی دال بر ورود غیرمجاز به سیستمی مشاهده شود، می‌توان استدلال کرد که هیچ جرمی اتفاق نیفتاده است.

به‌خصوص، اگر این ورود غیرمجاز نتیجه بعضی فرآیندهای اتوماتیک که می‌توان در بات‌نت‌ها یافت باشد.

در نتیجه، تیم‌های حفاظت از زیرساخت ملی احتیاج به درک فرآیند تصمیم‌گیری برای مجریان قانون دارند و باید از آن در طی هر حادثه به دقت پیروی کنند. همچنین، احتیاج دارند که یک فرآیند محلی ایجاد کنند تا بتوانند تعیین کنند که آیا در زمینه زیرساخت آن‌ها جرمی اتفاق افتاده است، یا خیر. نتیجه نه فقط واسط بین سازمان و مجریان قانون را بهینه خواهد کرد، بلکه تقاضای منابع غیرقابل اجتنابی را کمینه خواهد کرد که برای تیم محلی، اگر مجریان قانون دخالت کنند، مورد نیاز خواهد بود.

۱۱-۶- بازیابی از بلایا

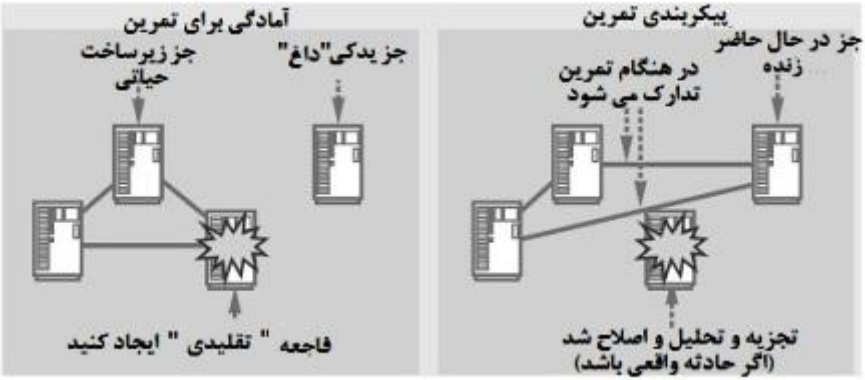
پس از یک حمله امنیتی، فرآیند بازیابی از بلایا نسبت به زمینه‌های دیگر واکنش به حادثه بلوغ بیشتری دارد که از اشتراکاتی نشأت می‌گیرد که بین بازیابی از حمله و بازیابی از بلایای طبیعی نظیر سیل، گردباد، آتش‌سوزی و مانند آن‌ها وجود دارد. متأسفانه، بسیاری از سازمان‌های بزرگ که مسئولیت زیرساخت ملی را به عهده‌دارند، در برنامه‌ریزی‌هایشان به طور مناسبی به تعهدات خود که شامل بازیابی از بلایا است توجه نمی‌کنند. برنامه‌های بازیابی از بلایا، سه جز اصلی دارند، چه آن‌هایی که نگران حملات سایبری بدخواهانه هستند و چه آن‌هایی که نگران بلایای طبیعی.

سه قسمت یک برنامه بازیابی از بلایا

- آماده سازی: تصمیم به آمادگی از قبل برای بازیابی از بلایا، ساده است؛ ولی حمایت از آن در عمل خیلی مشکل‌تر است. معمولاً، بودجه عملیاتی سد کننده راه است، زیرا فرآیند آماده سازی برای مواجهه با بلایا از قبل، شامل چیزهایی بیش از نوشتن یک لیست از اقدامات بالقوه است و

معمولاً، برای جلوگیری از شکست سیستم به خاطر شکست در، یک نقطه احتیاج به تغییرات ساختاری در سیستم می‌باشد. یعنی سیستم باید نسبت به شکست‌های تک نقطه‌ای اغماض پذیر باشد و از ابزارهای مطمئن و با افزونگی برای ارتباطات بین تیم‌های بازیابی استفاده شود و حتی ممکن است نیاز به ارتقا سخت‌افزاری و نرم‌افزاری سیستم‌های امنیت سایبری باشد تا حفاظت مطلوب در هنگام فاجعه تضمین شود.

- برنامه‌ریزی: عنصر اساسی در دستور کار بازیابی از بلایا، داشتن برنامه صریح و روشنی است که نوشته‌شده و در تمام روش‌های عملیاتی و رویه‌ها گنجانیده شده باشد. این برنامه می‌تواند با توجه به مقابله سازمان با فجایع و بلایا، بهبود یابد. برای مثال؛ بسیاری از سازمان‌هایی که متکی بر هواپیماهای تجاری جهت جابه‌جایی دستگاه‌ها به محل بلایا بودند، پس از حادثه ۹/۱۱ دریافتند که این روش خوب کار نمی‌کند.
- تمرین: تصمیم به تمرین برای بلایا نیز یک روش پر خرج است و احتیاج به تیم‌هایی از کارشناسان دارد که باید برای حمایت از این تمرین‌های ساختگی به آنان پرداخت‌هایی شود. بهترین راه برای تمرین یک فاجعه، ایجاد سناریویی واقع‌گرایانه و کار از طریق جزییات برنامه نوشته شده است. معمولاً، این روش شامل استفاده از ظرفیت یدکی محاسباتی یا شبکه‌ای است که در موقعیت‌های داغ و غیرعادی کنار گذاشته می‌شوند. (به شکل ۱۱-۷ توجه کنید).



شکل ۱۱-۷- پیکربندی‌های تمرین بازیابی از فجایع و بلایا

در واقع، سازمان‌های بسیار کمی برای بلایا تمرین می‌کنند. این تمرینات نیاز به انضباطی دارد که در بیشتر تیم‌های شبکه و سیستم شرکت وجود ندارد. اگر تیم رهبریت ارشد آن را یک اولویت قرار دهد، می‌تواند مؤثر باشد؛ اما متأسفانه تنها پس از اینکه بلایا اتفاق افتادند، به آن توجه می‌شود، به خصوص اگر آن‌ها اثری روی زیرساخت محلی داشته باشند. فرآیند آشنای جدی گرفتن بلایا را پس از اینکه آن‌ها اتفاق افتادند، در جامعه‌هایمان شاهد بوده‌ایم، به خصوص زمانی که مربوط به فجایع طبیعی و تروریسم بوده است. این نگرش برای حفاظت مناسب از زیرساخت ملی در مقابل حملات سایبری باید تعدیل شود.

۱۱-۷- برنامه واکنش ملی

مهم‌ترین عملکرد در هر برنامه واکنش به حوادث ملی، شامل هماهنگی اضطراری بین دولت، کسب‌وکار، شهروندان و ملل دیگر در طول یک حادثه حمله سایبری است. رابط‌های بین این عناصر باید به عنوان قسمتی از برنامه‌ریزی برای واکنش، شناسایی و

مدیریت شوند. برنامه‌های ملی می‌تواند هماهنگی مرکزی را ایجاد نماید؛ اما هماهنگی بین بخش‌های داخلی نیز باید تشویق شود. (به شکل ۱۱-۸ توجه کنید).

این عملکرد هماهنگی به نظر بدیهی می‌رسد، اما بیشتر برنامه‌های واکنش به حوادث اضطراری ملی موجود و تیم‌های واکنش به حوادث اضطراری کامپیوتری (CERT) به تمرکز روی انتشار اطلاعات مربوط به آسیب‌پذیری گرایش دارند. این برای سازمان‌های کوچک‌تری که تیم امنیتی ندارند مفید است. اما این تمرکز، گرایش به باقی گذاردن فواصل خالی در هماهنگی‌های سطح ملی در زمانی که یک حادثه ملی عمده اتفاق می‌افتد دارد. با اینکه تا کنون چنین حادثه ملی عمده‌ای هنوز اتفاق نیفتاده است، اما اگر به زودی چنین اتفاقی بیفتد، بعید است که هماهنگی ملی در ایالات‌متحده به صورت روان باشد. توجه فوری برای حفاظت مناسب زیرساخت ملی که به اثرات حمله سایبری توجه شود مورد نیاز است.

شکل ۱۱-۸- رابطهای هماهنگی برنامه واکنش به حوادث ملی

فصل ۱۲: نمونه الزامات حفاظت از زیرساخت ملی

هر بحثی در مورد امنیت کامپیوتری، با بیانیه‌ای از الزامات شروع می‌شود.

"کتاب نارنجی" وزارت دفاع ایالات‌متحده آمریکا.

(معیار ارزیابی سیستم کامپیوتری مورد اعتماد .DoD 5200.28-STD).

خوانندگان این کتاب که با سازمان‌های اقتصادی در ارتباط هستند، باید ترجمه مطالب امنیتی ارائه‌شده در این کتاب را به عنوان یک برنامه عمل مرتبط با محیط محلی خود در نظر بگیرند. برای اکثریت، این شامل ایجاد مجموعه‌ای از الزامات جدید امنیتی برای حفاظت از زیرساخت است. سناریوهای معتبر ممکن است شامل تعبیه الزامات امنیتی جدید برای جمع‌آوری و همبسته سازی در درخواست برای پیشنهاد (RFP) توسط مقامات دولتی باشد. ممکن است این مقامات نوشتن انواع جدیدی از الزامات سیاست امنیتی در مورد فیلتر کردن حمله جلوگیری از سرویس (DDOS) گسترده را برای مهندسان امنیتی که شرکت آن‌ها هدف حمله می‌باشد و همین طور تعبیه کردن الزامات امنیتی جدید برای ظروف عسل گمراه‌کننده در برنامه‌های نوآوری، برای محققان و مهندسان تولید محصولات را بگنجانند.

بدیهی است که بهترین راه برای اینکه هر نیاز به طور مناسبی منطبق با محیط هدف باشد، این است که این نیاز به طور ویژه متناسب با آن محیط شود. و مهندس امنیتی که الزامات را می‌نویسد، باید درک درستی از محدودیت‌های محلی داشته و بینش کافی در مورد اهداف و مقاصد کنترل‌های امنیتی جدید داشته باشد. به این دلیل نمی‌توان برای حفاظت از زیرساخت ملی مجموعه‌ای از الزامات را پیشنهاد نمود که به طور کامل تمام حالات را بپوشاند. در عوض، مجموعه‌ای از الزامات اساسی نمونه که زمینه‌ها را ارائه می‌دهد و نمایش آن برای خوانندگانی که مصمم به تعبیه بعضی از

ایده‌های ارائه‌شده در این کتاب به داخل برنامه محلی خود هستند، در زیر ارائه شده است.

هر نمونه از الزامات به صورت محدودیت‌هایی در مورد این که چگونه یک سازمان خاص عمل کند نوشته می‌شود. در حقیقت، واژگان ما برای نمونه‌ها از یک فرمت عمومی "سازمان باید ..." پیروی می‌کند. خوانندگان باید بتوانند جملات مخصوص را به فرمت محلی "انجام چنین و چنان تحت شرایط xyz در محیط ABC به منظور IJK" مناسب کنند. الزامات جامع نیستند؛ بنابراین، ایده بریدن و چسباندن مثال‌ها برای ایجاد یک سیاست جدید نظر بدی خواهد بود. نیازها کامل هم نیستند بنابراین نباید فرض کرد که نمونه الزامات در مورد همبسته سازی، خلاصه کافی از مطالب ارائه‌شده در این زمینه را ارائه می‌دهد؛ این ضمیمه به عنوان یک ابزار آموزشی برای کمک به خوانندگان برای ایجاد الزاماتی نیست که فقط در حفاظت از زیرساخت مؤثر هستند؛ بلکه معنی‌دار بوده و در محیط محلی عملی خواهند بود، ارائه شده است.

۱۲-۱- نمونه الزامات فریب دادن (فصل دوم)

در این بخش، سه نمونه از الزامات فریب دادن را ارائه می‌کنیم که خطر حمله به جزیی از زیرساخت هدف را کاهش می‌دهند این الزامات برای حمله‌کننده ابهام ایجاد می‌کند و ابزارهایی برای تجزیه و تحلیل حملات زنده پیشنهاد می‌کند، با این حال، به خوانندگان هشدار داده می‌شود که پیش از به‌کارگیری ظرف عسل، مسائل قانونی مربوطه محلی باید به دقت بررسی شوند. متأسفانه، وکلای مطلع در زمینه به‌کارگیری عملی فریب دادن کاملاً کمیاب هستند.

سازمان باید:

- (DEC-1): قابلیت ظرف عسل فریب را در مورد زیرساخت‌هایی که از سرویس‌های ضروری جذاب حمایت می‌کنند و برای کارمندان داخلی بدخواه به صورت محلی قابل‌دسترسی می‌باشند فعال نماید. این الزام تضمین می‌کند که تلاش‌هایی برای گرفتن و به تله انداختن کارکنان داخلی؛ مانند، کارمندان، مشاوران، بازدیدکنندگان و پیمانکارانی انجام شده است که ممکن است بخواهند مقاصد بدخواهانه‌یی را برای خرابکاری در سیستم یا خروج غیرمجاز داده‌ها مرتکب شوند. این پیاده‌سازی نباید به صورت گسترده باشد؛ بلکه باید متناسب با اندازه و قلمرو قسمتی از زیرساخت باشد که از آن حفاظت می‌شود. تصمیم به اینکه فریب دادن از طریق ظرف عسل پنهانی یا غیر پنهانی باشد، می‌تواند یک تصمیم محلی باشد. نشان دادن انطباق با اهداف فعال کردن ظرف عسل، می‌تواند شامل تستی باشد که نشان می‌دهد ظرف عسل از طریق شبکه داخلی قابل‌دسترسی است و به اندازه کافی خوب طراحی شده است و استفاده از آن می‌تواند برای یک دشمن داخلی معمولی متقاعدکننده باشد.
- (DEC-2): قابلیت ظرف عسل را در حمایت از سرویس‌های ضروری که جذاب هستند و افراد خارجی بدخواه که می‌توانند از خارج سیستم به آن‌ها دسترسی داشته باشند. فعال کنند این الزام تضمین می‌کند که تلاش‌هایی برای فعال کردن قابلیت تله اندازی انجام شده است که متمرکز بر افراد خارجی بدخواهی است که ممکن است منابع سازمان را از طریق اینترنت یا از نقاط دسترسی خارجی دیگر مثل اکسترانت یا شبکه‌های VPN هدف‌گیرند. پیاده‌سازی قابلیت نباید به صورت گسترده باشد، اما باید با محیط هدف متناسب شده باشد و بسته به نیازهای

محلی، بتواند به صورت پنهانی یا غیر پنهانی، انجام شود. از تست نفوذ در اینترنت می‌توان برای تست انطباق استفاده کرد.

- (DEC-3): شواهدی ارائه کند که بر اساس آن تمام قابلیت ظرف عسل فریب‌دهنده مربوط به مدیریت صریح و سیستم‌های حمایتی به منظور آغاز واکنش به حادثه است. این الزام تضمین می‌کند که سازمان سیستم‌های پشتیبانی کافی ، برای اینکه فریب دادن مؤثر باشد را دارد، به خصوص اگر این فریب دادن‌ها به صورت پنهانی انجام شود. در صورتی که این الزام در سیستم اطلاع دهنده هشدار ظرف عسل به یک انسان آموزش‌دیده جهت تفسیر نتایج و هدایت عمل واکنش وصل شود، به بهترین نحو عمل خواهد کرد. بدون چنین سیستم پشتیبانی، بعید است که فریب دادن مؤثر باشد. به طور کلی، مهم است که قسمت‌های داخل سیستم ابزارهایی برای مقابله با کاربران مجاز بی‌گناهی داشته باشد که به طور سهوی به ظرف عسل دسترسی یافته‌اند.

۱۲-۲- نمونه الزامات جداسازی (فصل سوم)

در این بخش، شش نمونه از الزاماتی را معرفی می‌کنیم که چگونه می‌توان از دیوارهای آتش، کنترل‌های دسترسی و فیلترها برای کمک به حفاظت از زیرساخت ملی استفاده کرد. گنجاندن الزامات فیلترینگ برای سیستم‌های بی‌سیم متحرک در بسیاری از محیط‌ها بحث‌برانگیز است؛ زیرا چنین قابلیتی ممکن است به صورت محلی قابل‌دسترسی نبوده و با ابزارهای عملی هم قابل‌استفاده نباشد.

سازمان باید...

- (SEP-1): ترافیک زنده DDOS را به طور پیشگیرانه تغییر مسیر دهد؛ یا پیش از اینکه به نقاط ورودی شبکه محلی برسند، آن‌ها را فیلتر کند. این الزام تضمین می‌کند که سازمان قدم‌هایی را برای کاهش خطر مربوط به حملات DDOS ورودی بردارد. یک گزینه خوب در اینجا ارائه‌دهنده سرویسی است که بهره‌برداری از فیلترها در بک بن ظرفیت بالا را در شبکه بعهده دارد. مقدار فیلتر کردن ترافیک باید با چند برابر ظرفیت ورود به داخل بیان شود. بدیهی است که این ضریب باید چند برابر یک باشد و هر چه بیشتر باشد، بهتر است. به دلایل واضح فیلترها نباید روی دروازه‌های ورودی عمل نمایند. تست این قابلیت باید با دقت انجام شود؛ زیرا ایجاد حمله ورودی زنده می‌تواند به آسانی از کنترل خارج شود (رویه‌های بازیابی از بلایا قبل از ایجاد یک حمله آزمایشی زنده روی هر چیزی همیشه باید همیشه آماده عمل باشند).
- (SEP-2): شواهدی ارائه کند که حملات به داخل، روی برنامه‌های کاربردی که از خارج قابل‌دسترسی هستند، نمی‌تواند حملات DDOS مبتنی بر تقویت روی نقاط خروجی شبکه محلی ایجاد کند. این الزام تضمین می‌کند که سازمان باید به مقابله با خطر حملات تقویت‌کنندگی ورودی در برنامه‌های کاربردی بپردازد که ضعیف طراحی‌شده و از خارج قابل‌دسترسی هستند. شواهد نتیجه، مجموعه‌ای از تست‌های عملکردی، مرور کدهای برنامه‌نویسی و ممیزی الزامات است،باید شواهدی چک شود که سئوالات کوچکی از یک برنامه کاربردی نتواند پاسخ‌های بسیار بزرگی به متقاضی خارجی بدهد. این کار در بیشتر محیط‌های کاربردهای پیچیده می‌تواند خطر DDOS خارجی را از بین ببرد، اما فرآیند

جمع‌آوری شواهد باید مسائل بدیهی را شناسایی کند. همچنین، باید آگاهی عمومی از این خطر را برای توسعه‌دهندگانی که کاربردهای جدید تولید می‌کنند، بالا ببرد.

- (SEP-3): کنترل‌های دسترسی شبکه را به طور انعطاف‌پذیری (دیوار آتش) بین گروه‌های مشخصی از کارکنان داخلی اعمال کند، به خصوص آن‌هایی که مستقیماً در حمایت خدمات ضروری کار می‌نمایند. این الزام تضمین می‌کند که سازمان از دیوارهای آتش برای ایجاد دامنه‌های داخلی مورد اعتماد استفاده می‌کند. کارکنان داخلی اتفاقی، اکثریت کارمندان معمولی، نباید توانایی مشاهده، تغییر و مسدود کردن مجموعه گسترده‌ای از منابع داخلی را در نتیجه دسترسی مخصوص به عنوان کارمند، پیمانکار و بازدیدکننده داشته باشند و این به ویژه باید برای دسترسی به سیستم‌های پشتیبانی‌کننده خدمات ضروری نیز درست باشد. قطعاً، کارمندانی که روی قسمت خاصی کار می‌کنند، ممکن است بتوانند مشکلات محلی ایجاد کنند؛ اما این اثر باید محدود به آن جز محلی باشد. این کار می‌تواند با دیوارهای آتش، لیست‌های دسترسی در رو ترها و سوئیچ‌ها، سیستم‌های مبتنی بر رمزنگاری و دیگر انواع مکانیسم‌های امنیتی انجام شود. برای تست رعایت شدن، می‌توان از تست نفوذ از مکان‌های اینترنت استفاده کرد.
- (SEP-4): کنترل‌های دسترسی به شبکه (دیوار آتش) را به طور انعطاف‌پذیری بین منابع سازمان و هر شبکه نامطمئن خارجی شامل زیرساخت بی‌سیم متحرک اعمال کند. بخش آشنای این الزام شامل دیوارهای آتش بین یک سازمان و شبکه‌های خارجی نامطمئن مثل اینترنت است. تقریباً، هر سازمانی می‌تواند این نیاز را برآورده کند، حتی با مدل قدیمی محیط پیرامونی که ممکن است شامل صدها و حتی

هزاران استثنای دسترسی در پایگاه قواعد خود باشند. قسمت ناآشنای این الزام این است که دسترسی مبتنی بر تحرک روی شبکه‌های حامل بی‌سیم در دستگاه‌های میان‌گیر گنجانیده شود. به علت اینکه بیشتر شرکت‌ها و آژانس‌ها دسترسی اسانی به موتور اعمال کننده سیاست‌های موبایل شرکت‌ها ندارند، برای آن‌ها همکاری با حامل‌های شبکه موبایل لازم است (متعجب نشوید، اگر حامل شما در پشتیبانی نیازهای شما مشکل دارد، این قلمرو بسیار جدیدی است).

- (SEP-5): پست الکترونیکی ورودی و ویروس‌های مبتنی بر وب، هرزنامه و دیگر بد افزارهای ورودی را پیش از رسیدن به نقاط ورودی شبکه به سمت زیرساخت محلی که از خدمات ضروری حمایت می‌نماید باید متوقف کند. این الزام تضمین می‌کند که ترافیک ناخواسته ورودی قبل از اینکه به نقاط ورودی شبکه هدف که احتمالاً، اینترانت سازمانی است، برسد، جمع‌آوری گردد. این کار، تا حد زیادی خطر یک حمله مبتنی بر حجم را که از این خدمات استفاده می‌کند، کاهش می‌دهد و الزامات امنیتی دروازه‌ها را ساده می‌کند. نگرانی‌های بهره‌وری و کاهش هزینه، محصول جانبی خوبی در این رویکرد هستند، گرچه آن‌ها انگیزه‌های اصلی در این رابطه نیستند. رعایت الزامات می‌تواند با تزریق ساده ترافیک ورودی به مقصد هدف تست و برقرار شود.
- (SEP-6): نشان دهد که کنترل‌های جداسازی مبتنی بر سیاست‌های امنیتی سازمان برای کاربردها، منابع و سیستم‌ها به میزبانی اَبر برای خدمات ضروری مستقر هستند. این الزام تضمین می‌کند که استفاده از زیرساخت اَبری برای کاربردها، میزبانی، ذخیره‌سازی و دیگر اجزا پشتیبانی خدمات ضروری بر اساس قواعد سیاست امنیتی به طور مناسبی حفاظت می‌شود. با پذیرش فزاینده خدمات ابری برای نرم‌افزارها، ذخیره‌سازی،

کاربردها و سیستم‌ها، این الزام به تدریج به مجموعه‌ای از بهترین شیوه‌های عمل برای امنیت مبتنی بر ابر توسعه خواهد یافت یکپارچه کردن قابلیت مدیریت شناسه سازمانی موجود، احتمالاً، یکی از پر چالش تر ین جنبه‌ی امنیت ابری است.

۱۲-۳- نمونه الزامات تنوع (فصل ۴)

در این بخش، دو نوع الزام تنوع را معرفی می‌کنیم که پیاده‌سازی آن‌ها در بیشتر محیط‌ها آسان نیست. در واقع، بیشتر مسئولان ارشد اطلاعاتی (CIO) عمداً شبکه‌هایی ایجاد کرده‌اند که فاقد تنوع بوده و استاندارد و مقرون به صرفه هستند، اما به خاطر تک فروشنده‌ای بودن، احتمال شکست آن‌ها وجود دارد و فروشندگان جایگزین دیگر برای محصولات خریداری‌شده، وجود ندارد. سیستم‌عامل کامپیوترهای رومیزی مثال خوبی برای این بی تنوعی است. با این حال، این الزامات سلاح قدرتمندی برای کاهش اثر آبشاری برخی از حملات هستند و تیم امنیتی باید از این الزامات پشتیبانی کند. تصمیم به عدم در پیش گرفتن راه‌های متنوع، فقط باید پس از بحث‌های دقیق و در نظر گرفتن تمام گزینه‌های در دسترس گرفته شود. یک مصالحه و سازش، می‌تواند محدود کردن تنوع به زمینه‌هایی بسیار متمرکز در مورد سیستم‌های حیاتی مخصوص باشد.

سازمان باید...

- (DIV-1): شواهدی ارائه کند که شکست یا نقض امنیتی هیچ فروشنده‌ای به تنهایی نتواند در سراسر ترکیبی از کاربردها، محیط‌های محاسباتی، یا اجزا شبکه‌ای که خدمات ضروری را پشتیبانی می‌کنند، اثر آبشاری ایجاد کند. این الزام، خطر زنجیره آبشاری از شکست‌ها را کاهش می‌دهد که می‌توانند در زیرساخت ملی به علت وجود نقص در محصول

یک فروشنده مشترک در یک فناوری ایجاد شود. همان طور که در بالا اشاره شد، برای بیشتر سازمان‌ها برآورده کردن این نیاز برای سیستم عامل کامپیوترهای رومیزی با توجه به همه‌گیر شدن یک معماری مشترک و مجموعه‌ای از کاربردها، کاری مشکل است. با وجود این، حیاتی است که به مسئله آبشاری با توجه به تنوع پرداخته شود. رعایت این الزام می‌تواند به صورت دستی چک شود.

- (DIV-2): برای حمایت خدمات ضروری، حداقل از یک فروشنده فعال جایگزین فروشنده اصلی، به طور اساسی برای تمام نرم‌افزارها، کامپیوترهای شخصی، سرورها، قسمت‌ها و اجزا شبکه استفاده کند. برای هر جز و قسمتی که DIV-1 را رعایت می‌کند، یک جایگزین دیگر به صورت فعال و زنده وجود دارد. این الزام ممکن است با درصدی از هدف متناسب شود. برای مثال، در این الزام، ممکن است گفته شود که حداقل ۱۰٪ از تمام سیستم‌های عامل کامپیوترهای شخصی که در پشتیبانی خدمات ضروری هستند، از فروشنده جایگزین دیگری خریداری می‌شوند. رعایت این الزام می‌تواند به صورت دستی چک شود.

۱۲-۴- نمونه الزامات اشتراک (فصل ۵)

در این بخش دو نمونه از الزامات اشتراک گنجانده شده است که باید برای یکپارچه‌سازی بیشتر محیط‌ها با آن‌ها متناسب شود. هدف بیشتر سازمان‌ها این است که به جای اینکه سیاست‌ها را از اول ایجاد کنند، سیاست‌ها و راهبردهای انطباق و رعایت کردن را بهبود بخشند.

سازمان باید...

- (COM-1): دارای سیاست امنیتی نوشته‌شده‌ای باشد، با برنامه آموزش برای تصمیم گیران، مکانیزم‌های قابل ممیزی برای انطباق و فرآیندهای نوشته‌شده برای مجازات متخلفان بر اساس این الزام، سیاست امنیتی باید با مکانیسم‌های انطباق (رعایت کردن) استقرار یافته باشد. قسمت ناآشنای این نیاز، بر آموزش برای تصمیم گیران و فرآیندهای نوشته‌شده برای مقابله با متخلفان تأکید کند.
- (COM-2): تطابق و رعایت کامل سازمانی به حداقل یک استاندارد امنیت اطلاعات شناخته‌شده را نشان دهد که یک ممیز خارجی آن را تأیید کند. این الزام تضمین می‌کند که سازمان حداقل یک استاندارد امنیتی نسبتاً خوب را برای رعایت کردن و انطباق مورد نظر و هدف قرار داده است. از آنجا که بین استانداردها اختلافاتی وجود دارد و استانداردهای شناخته‌شده همگی دارای یک مجموعه هسته‌ای از الزاماتی هستند که ضرورتاً کنترل‌های از نوع یکسانی را دیکته می‌کنند. باید حداقل از یکی آن‌ها استفاده کند.

۱۲-۵- نمونه الزامات (دفاع در عمق) (فصل ۶)

در این بخش، سه نمونه از الزاماتی پیشنهاد می‌شوند که برای بهبود عمق لایه‌های مکانیسم امنیتی خدمات ضروری هستند. این الزامات متمرکز بر دسترسی، شکست، یکپارچگی و رمزنگاری هستند و خوانندگان می‌توانند به راحتی این تأکید را روی دیگر زمینه‌های فنی یا امنیتی قیاس یا برون‌یابی کنند.

سازمان باید...

- (DEP-1): شواهدی ارائه کند که هیچ فردی در داخل یا خارج از سازمان نمی‌تواند به طور مستقیم به سیستم‌هایی که از یک سرویس ضروری پشتیبانی می‌نمایند، بدون حداقل دو چالش تأیید هویت امنیتی متنوع دسترسی پیدا کند. این الزام، تضمین می‌کند که از دو نوع تأیید هویت برای دسترسی به زیرساخت ضروری استفاده می‌شود، به تفسیر محلی برای تعیین اینکه روش‌های انتخاب‌شده به اندازه کافی متنوع هستند نیاز است. برای مثال؛ معمولاً، برای ارائه اعتبارسنجی شناسه دو فاکتوری، یک شماره شناسایی فردی (PIN) با یک تأیید هویت کننده دستی کفایت می‌کند؛ با این حال، ممکن است که گروه‌هایی این دو فاکتوری را به صورت یک چالش تنها تفسیر کنند.
- (DEP-2): شواهدی ارائه کند که شکست هر سیستم حفاظتی نمی‌تواند منجر به نقض امنیتی مستقیم در هر قابلیت کاربردی، محاسباتی و شبکه‌ای که خدمات ضروری را حمایت می‌کنند گردد. این الزام تضمین می‌کند که شکست یک سیستم تنهای حفاظتی، نمی‌تواند نقض امنیتی مأموریت کلی سیستم را به همراه داشته باشد. با امنیت مبتنی بر شبکه، دوبله کردن و توزیع یا وسایل دیگر می‌توان به این هدف رسید. دیوارهای آتش، معمولاً، نقاط تنهای دفاعی هستند که نیاز به گزینه‌های دیگری از روش‌های حفاظتی دارند.
- (DEP-3): شواهدی ارائه کند که تمام اطلاعاتی که افشای غیرمجاز آن‌ها می‌تواند مستقیماً روی یکپارچگی و عملیات خدمات ضروری اثر بگذارد، تحت اثر حداقل دو سطح متنوع از رمزنگاری در طی عملیات ذخیره‌سازی و انتقال قرار می‌گیرند. این الزام، تضمین می‌کند که بیشتر اطلاعات حیاتی برای خدمات ضروری دو بار با استفاده از وسایل متنوعی رمزنگاری می‌شوند. تفسیر اینکه چه چیزی "حیاتی‌ترین اطلاعات" را تشکیل

می‌دهد، می‌تواند به صورت محلی مورد بحث قرار گیرد و باید متناظر با اطلاعاتی باشد که محرمانگی آن‌ها برای عملیات یک سرویس ضروری حیاتی است. می‌توان تصور کرد که این اطلاعات جز بسیار کوچکی از اطلاعات در انواع محدودی از شرایط هستند. رمزنگاری انتها به انتها و در سطح یک لینک، مثالی هستند، از اینکه چگونه ممکن است این الزام در برخی موارد رعایت شود.

۱۲-۶- نمونه الزامات احتیاط (فصل ۷)

این بخش، دو نمونه از الزاماتی در مورد اینکه چگونه باید با اطلاعات رفتار شود را معرفی می‌نماید. این نیازها بسیار معمولی هستند و بسیاری از سازمان‌ها، رعایت این مثال‌ها را چالش‌برانگیز نمی‌یابند. به‌هرحال هدف واقعی، ایجاد فرهنگ احتیاط در یک سازمان است. متأسفانه، نوشتن نیازهای ذهنی اینکه چقدر خوب یک فرهنگ برای حفاظت از زیرساخت‌های حیاتی مناسب می‌باشد را بتواند اندازه‌گیری کند، تمرین بیهوده و کم ارزشی نیست. الزامات نمونه زیر حداقل یک شروع را ارائه می‌کند.

سازمان باید ...

- (DIS-1): شواهدی ارائه کند که اطلاعات سازمانی مرتبط با هر خدمت ضروری به طور مناسبی نشانه‌گذاری شده است و علامت گذاری به طور مناسبی اجرا می‌شود. این نیاز باید بر اساس شواهدی شاید از طریق ممیزی برنامه‌ریزی نشده‌ای، بر اساس اینکه تمام مستندات باید دارای نشانه‌های مناسب باشند انجام شود. بسیاری از سازمان‌ها این اصل ساده را نقض می‌کنند؛ زیرا این موضوع می‌تواند حفاظت قدرتمندی در مقابل بعضی از انواع نشت داده باشد. برای مثال، ابزارهای نشت داده می‌توانند طوری

تنظیم شوند که مدارکی را کشف کنند که به طور مناسبی نشانه‌گذاری شده‌اند و به طور غیر عمدی به یک مقصد غیرقابل‌اعتماد ممکن است انتقال یابند.

- (DIS-2): شواهدی ارائه کند که کارمندان سازمان که مرتبط با خدمات ضروری هستند، برای چگونگی اداره اطلاعات و به اشتراک‌گذاری آن‌ها به صورت خارجی، به طور کامل با توجه به سیاست‌های محلی تربیت می‌شوند. تجزیه و تحلیل انطباق و رعایت کردن آن، نیاز به تفسیر دارد، همان‌گونه که بیشتر سازمان‌ها سطحی از آموزش را دارند. سئوال کلیدی این است که آیا این آموزش قابل‌قبول فرض می‌شود و همین طور سازمان به چه میزان تضمین می‌کند که تمام کارمندان این آموزش‌ها را به طور منظم کامل می‌کنند. بدیهی است که اگر هر کدام از الزاماتی که در اینجا بیان شد، در سیاست‌های سازمان گذارده شود، آموزش نیز باید بر اساس آن بروز شود.

۱۲-۷- نمونه الزامات جمع‌آوری داده (فصل ۸)

این بخش دو نمونه از الزامات جمع‌آوری داده را معرفی می‌نماید که به استقرار سیاست‌های رسمی‌تر و نوشته‌شده در مورد این که چگونه اطلاعات با اهداف امنیتی جمع‌آوری شوند می‌پردازد. یک هدف کلیدی در استقرار هر نوع سیاست جمع‌آوری داده‌ها، تضمین این است که ملاحظات محرمانگی پایه‌ای به طور کامل در آن گنجانیده شود، طوری که به تیم امنیتی اجازه دسترسی کافی به داده‌ها برای شناسایی نشانه‌های زودهنگام و اجرای مناسب تجزیه و تحلیل فارنسیک امنیتی را بدهد.

سازمان باید ...

- (COL-1): شواهدی ارائه کند که مجموعه‌ای از معیارها برای جمع‌آوری و ذخیره‌سازی هر نوع اطلاعات در هر زمینه‌ای در سازمان استقرار یافته‌اند. معیارهای جمع‌آوری و ذخیره‌سازی باید شامل توجه به فاکتورهای مختلف؛ از جمله؛ محرمانگی باشند، اما در اینجا تمرکز روی امنیت است. مقصود الزام به استمرار مجموعه‌ای از معیارها است، برای اینکه در یابیم چه مطالبی باید جمع‌آوری و ذخیره‌سازی شوند. باهدف تضمین اینکه حملات و نشانه‌های مربوطه در میان داده‌های جمع‌آوری شده قابل کشف باشند. اگر فرآیند جمع‌آوری شامل نمونه‌برداری بسته‌ها با نرخ درصد کوچک از لینک‌های شبکه باشد، احتمال کشف نشانه‌های امنیتی مهم پایین می‌آید.
- (COL-2): شواهدی ارائه کند که بر اساس آن، سیستم‌ها جهت جمع‌آوری به صورت بی‌درنگ و ذخیره‌سازی به طور امن تمام اطلاعات مطلوب از کاربردها، سیستم‌ها و شبکه‌ها مستقرشده‌اند. داشتن دسترسی بی‌درنگ به داده‌ها، توانایی ایجاد هشدارهای زودهنگام به حملات را ایجاد می‌کند. اگر فرآیند جمع‌آوری در مد batch تصادفی با استفاده از گزارش‌های روزانه، هفتگی یا حتی ماهانه انجام شود، پیش از اینکه حتی به گرایش متناظر حمله توجه شود، ممکن است خسارات بزرگی برای خدمات ضروری اتفاق بیفتد.

۱۲-۸- نمونه الزامات همبسته سازی (فصل ۹)

این بخش، دو نمونه از الزامات همبسته سازی را که به تمرکز یک سازمان به رویکرد ساختار یافته برای اطمینان از اینکه تجزیه و تحلیل داده‌ها به طور مناسب در محیطی انجام شود که اجازه آگاهی و واکنش را بدهد، معرفی می‌نماید.

سازمان باید ...

- (COR-1): شواهدی ارائه کند که الگوریتم‌های کارآمد برای همبسته سازی اطلاعات مرتبط به صورت بی‌درنگ در جهت نتایج قابل عمل استقراریافته‌اند. الگوریتم‌های همبسته سازی نباید پیچیده باشند؛ بلکه باید کارآمد بوده و به طور مناسبی در محل خود قرار بگیرند و باید نوعی از فرآیندهای امنیتی قابل عمل را حمایت کنند. در حقیقت، الگوریتم‌های پیچیده ممکن است حتی مطلوب هم نباشند. دیده‌شده که شمارنده‌های ساده بسته‌ها، اطلاعات مربوطه بیشتری از سیستم‌های جلوگیری از نفوذ مبتنی بر تطابق الگوهای امضا پیچیده ارائه می‌کنند.
- (COR-2): شواهدی ارائه کند که خروجی همبسته سازی (احتمالاً در یک مرکز عملیات امنیتی) به قابلیت‌های آگاهی و واکنش سازمان متصل می‌باشد. این نیاز تضمین می‌کند که قابلیت‌های همبسته سازی، جمع‌آوری، آگاهی و واکنش همگی به هم متصل هستند. این پیش‌فرض که این اتصال در مرکز عملیات امنیت انجام می‌شود مبتنی بر مشاهدات عملی است که بیشتر سازمان‌ها سعی در اطمینان از این که این اتصالات در مرکز عملیات امنیت انجام شود دارند.

۱۲-۹- نمونه الزامات آگاهی (فصل ۱۰)

این بخش سه نمونه از الزاماتی را معرفی می‌نماید که متمرکز بر تعبیه قابلیت‌های آگاهی موقعیتی در داخل زیرساخت روزبه‌روز یک سازمان است. تأکید خاص بر قابلیت‌های بی‌درنگ و جامع گذارده شده است.

سازمان باید ...

- (AWA-1): شواهدی ارائه کند که اطلاعات امنیت سایبری که مرتبط با خدمات ضروری هستند، به طور منظم جمع‌آوری شده و برای تصمیم گیران به موقع منتشر می‌گردد. این الزام تضمین می‌کند که فرآیند جمع‌آوری اطلاعات استقرار یافته است. این فرآیند باید دارای مکانیسم‌هایی برای به دست آوردن داده‌های خام به صورت امن و برای تفسیر داده‌ها به طوری باشد که محدودیت‌های یکپارچگی و محرمانگی آن‌ها حفظ شود و برای کنترل‌های امنیتی سایبری مجموعه اطلاعات قابل عمل ایجاد نماید.
- (AWA-2): شواهدی را ارائه کند که بر اساس آن یک قابلیت عملیاتی بی‌درنگ امنیتی وجود دارد که عملیات واکنشی و پیشگیرانه را بر اساس اطلاعات جمع‌آوری شده و تجزیه و تحلیل همبسته سازی (احتمالاً، در مرکز عملیات) هماهنگ می‌کند. این الزام، تضمین می‌کند که سازمان در نتیجه جمع‌آوری اطلاعات دارای ابزاری برای عمل است. بسیاری از گروه‌ها، فرآیندهای فانتزی جمع‌آوری اطلاعات امنیتی ایجاد می‌کنند، الگوهای جالبی را روی تابلوهای دیواری بزرگ و درخشان ارائه می‌کنند و می‌توانند داستان‌هایی در مورد همه نوع حملات قبلی بیان کنند. به هر

حال، کمتر سازمانی را می‌توان یافت که اقداماتش را بر اساس اطلاعات در دسترس هماهنگ کند.

- (AWA-3): شواهدی ارائه کند که فرآیند مدیریت جامع و بی‌درنگ آسیب‌پذیری‌ها و تهدیدها استقراریافته و داده‌های مربوطه برای کمینه کردن خطرات امنیتی برای تمام دستگاه‌ها و نرم‌افزارهایی بکار گرفته می‌شوند که خدمات ضروری را پشتیبانی می‌نمایند. یافتن فرآیند مدیریت تهدید و آسیب‌پذیری در یک سازمان، غیرمعمول نیست، ولی تضمینی نیست که این فرآیند بی‌درنگ و جامع باشد. به عبارت دیگر، داده‌ها ممکن است به صورت دلخواه در دسترس قرار گیرند و مسائل پوشش برای تمام دستگاه‌ها و نرم‌افزارهایی که خدمات ضروری را پشتیبانی می‌کنند، ممکن است به طور مناسبی در نظر گرفته نشده باشد.

۱۲-۱۰- نمونه الزامات واکنش (فصل ۱۱)

این بخش، دو نمونه از الزامات را معرفی می‌کند، در مورد اینکه چگونه سازمان عمل واکنش به حادثه را انجام می‌دهد. تأکید بر ارتقا فرآیندهای واکنش فعلی وجود دارد تا واکنش‌های پیشگیرانه بیشتری را به نشانه‌ها و همین طور مستندسازی و متریک‌های اصلاح‌شده‌ای را دارا شود.

سازمان باید ...

- (RES-1): شواهدی ارائه کند که سازمان دارای توانایی واکنش به نشانه‌ها و سیگنال‌های هشدار، پیش از حمله، به هر منبع بحرانی و حیاتی است. این الزام تضمین می‌کند که واکنش به حادثه می‌تواند به جای اینکه تنها به علت قطع شدن‌ها شروع شود، بر اساس نشانه‌ها آغاز گردد. هر سازمان

توانایی توجه به چیزهایی را که کاملاً نابسامان و خراب شده‌اند، دارد (مثل، شبکه‌ای که خراب‌شده، پست الکترونی که کار نمی‌کند ...) اما گروه‌های مهاجم‌تر، فرایندهایی برای واکنش به داده‌های زیرکانه‌تر شاید از دستگاه‌های شبکه، سرورها یا سیستم‌های امنیتی ساخته‌اند.

(RES-2): شواهدی ارائه کند که سازمان مدارک و متریک‌هایی را در مورد ریشه علل مسائل امنیتی گذشته و همین طور کارآمدی اقدامات واکنشی در مورد حوادث امنیتی در گذشته و حال را نگهداری می‌کند. تعجب‌آور است که درخواست‌های کمی شامل این الزام هستند در حقیقت، به عنوان یکی از اعضای تیم ارائه‌کننده سرویس‌های امنیتی در ۲۵ سال گذشته، در درخواست‌های خرید عمده دولتی فقط چند دفعه به صورت جزیی از این الزام را در آن‌ها دیده‌ام. بیشتر الزامات عمومی شیوه‌های عمل گذشته، معمولاً، به وسیله خریداران دولتی مشخص شده است (در محیط‌های تجاری، بندرت یا هرگز) اما موارد خاص مربوط به متریک‌های ریشه علل، کارآمدی‌های مستند شده و دیگر آمار به ندرت دیکته شده‌اند.

مراجع

[1]T.Friedman, The World Is Flat: A Brief History of the Twenty-First Century, Farrar, Straus, and Giroux, New York, 2007. (Friedman provides a useful economic backdrop to the global aspect of the cyber attack trends suggested in this chapter).

[2]Executive Office of the President, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, U.S. White House, Washington, D.C., 2009 (http://handle.dtic.mil/100.2/ADA501541).

[3] Much of the material on botnets in this chapter is derived from work done by Brian Rexroad, David Gross, and several others from AT&T.

[4]R. Kurtz, Securing SCADA Systems, Wiley, New York, 2006. (Kurtz provides an excellent overview of SCADA systems and the current state of the practice in securing them).

[5]The Honeynet Project, Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community, Addison–Wesley Professional, New York, 2002. (I highly recommend this amazing and original book.) See also B. Cheswick and S. Bellovin, Firewalls and Internet Security: Repelling the Wily Hacker, 1st ed., Addison–Wesley Professional, New York, 1994; C. Stoll, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, Pocket Books, New York, 2005.

[6]D. Denning, Information Warfare and Security, Addison–Wesley, New York, 1999, p. 354.

[7]R. Krutz, Securing SCADA Systems, John Wiley & Sons, New York, 2006

[8]Quoted in "Taking Cues from Mother Nature to Foil Cyber Attacks" (press release), Office of Legislative and Public Affairs, National Science Foundation, Washington, D.C.,2003 http://www.nsf.gov/od/lpa/news/03/pr03130.htm.

[9] Quoted in A. K. Dewdney, "Computer recreations: of worms, viruses and Core War," Sci. Am., 260(3), 90–93, 1989.

[10] S. Levy, The open secret: public key cryptography—the breakthrough that revolutionized email and ecommerce-was first discovered by American geeks. Right? Wrong, Wired, 7(4), 1999.

[11] S. Northcutt, Network Intrusion Detection: An Analyst's Handbook, New Riders Publishing, Berkeley, CA, 1999, p. 34.

[12] D. Denning, Information Warfare and Security, Addison-Wesley, New York, 1999, p. 362

[13] E. Waltz, Information Warfare: Principles and Operations, Artech House, Norwood, MA, 1998

[14] K. van Wyk and R. Forno, Incident Response, O'Reilly Media, Sebastopol, CA, 2001.

واژه‌نامه.

Access Control Lists	فهرست‌های کنترل دسترسی
Access Controls	کنترل‌های دسترسی
Access Paths	مسیرهای دسترسی
Access Techniques	تکنیک‌های دسترسی
Accuracy	دقت
Actionable Jnformation	اطلاعات عملی
Active Opportunism	فرصت‌طلبی فعال
Actual Assets	سرمایه‌های واقعی
Administration	مدیریت
Adversary	دشمن
Aggregation	تجمیع
Air Gap	فاصله هوایی

Alarm	هشدار
Algorithm	الگوریتم
Amplification	تقویت
Analysis	آنالیز یا تجزیه و تحلیل
Antivirus Software	نرم افزار ویروس کش
Application	کاربرد
Approach	رویکرد
Architecture	ساختار، معماری
Asset	سرمایه
Attack	حمله
Attention	توجه
Attribute	ویژگی، صفت
Audit	ممیزی
Authentication	تأیید هویت، تصدیق اصالت
Authorize	اجازه دادن
Automation	خودکاری، اتوماسیون
Availability	دسترس‌پذیری
Awareness	آگاهی
Backup	پشتیبانی
Behavior	رفتار
Best Practice	بهترین شیوه عمل
Bogus	ساختگی
Botnet	بات‌نت
Boundary	مرز
Business	کسب و کار

Career Path	مسیر شغلی
Cascade	آبشار
Case Study	مورد کاوی
Centralize	متمرکز سازی
CERT	گروه واکنش به حوادث و اضطرار رایانه‌ای
Certification	گواهی، تصدیق صدور گواهینامه
Circuit Switched	سوییچ مداری
Classification	طبقه بندی، رده بندی
Clearance	نداشتن سوسابقه، پاکی امنیتی
Cloud Computing	محاسبات ابری
Clutter	درهم به رهمی و بی نظمی
Collection	مجموعه، جمع آوری
Commercial	تجاری
Commission	کمیسیون، هیئت
Commonality	اشتراک، مشترکات
Compartment	محفظه
Competition	رقابت
Complex	پیچیده
Component	جز

Confidentiality	محرمانگی، محرمانه بودن
Consistency	ثبات
Consumer	مصرف کننده
Content	محتوا، مفاد
Content Distribution Networks (CDN)	شبکه‌های توزیع محتوا
Correlation	همبسته سازی
Cost	هزینه
Coverage	پوشش
Critical	حیاتی
Culture	فرهنگ
Cyber Attack	حمله سایبری
Cyber Security Methodology	متدولوژی امنیت سایبری
Data Base	پایگاه داده
Data Collection	جمع آوری داده‌ها
Data Feeds	خوردهای داده
Data Format	قالب داده، فرمت داده
Data Leakage	نشت داده
Data Marking	نشانه گذاری داده
Data Sampling	نمونه برداری داده

Data Services	خدمات داده
Data Sources	منابع داده
Data Storage	ذخیره سازی داده
DDOS	امتناع از سرویس گسترده
Deception	فریب دادن
Decision Makers	تصمیم گیرندگان
Decision Process	فرآیند تصمیم
Decomposition	تجزیه
Defense in Depth	دفاع در عمق
Designer	طراح
Desktop Computer	رایانه رومیزی
Developer	توسعه دهنده
Digital Rights Management	مدیریت حقوق دیجیتال
Disaster Recovery Process	فرآیند بازیابی از بلایا
Disclosure	فاش کردن
Discovery	اکتشاف، کشف
Discretion	احتیاط یا صلاحدید
Distributed Denial Of Service (DDOS).	امتناع از سرویس گسترده
Diversity	تنوع

Data Leakage Protection (DLP).	حفاظت از نشت داده
Domain Name System (DNS).	سیستم نام دامنه
Domain-Based Correlation	همبسته سازی مبتنی بر دامنه
Dual Homing	دوخانگی
Duplication	تکرار، نسخه برداری
Duty Controls	کنترل وظایف
E-mail	پست الکترونیکی
Emergency Response	پاسخ اضطراری
Encryption	رمزگذاری
End User	کاربر نهایی
Enforceability	قابل اجرا بودن
Enterprise	بنگاه اقتصادی
Expert	متخصص یا کارشناس
Exploitation	بهره برداری یا سو استفاده
Expose	در معرض قرار گرفتن
External	خارجی یا بیرونی
False Positive	مثبت کاذب
Financial	مالی
Firewall	دیوار آتش

FISMA	مدیریت امنیت اطلاعات فدرال
Fix	اصلاح، مرمت و تعمیر
Flaw	عیب
Forensic	فارنسیک، ادله قانونی
Front- Loaded Response	پاسخ بارگذاری شده از پیش
Functional Control	کنترل عملکردی
Functional Separation	جداسازی عملکردی
Fusion Centers	مراکز ادغام
Global Threat	تهدید جهانی
Government Agency	آژانس دولتی
Hacking	هک کردن
Hardware Profile	مشخصات سخت افزار
Hidden Probe	کاوشگر پنهانی، پر وب پنهان
HMI	واسط بین ماشین و انسان
Honey Pot	ظرف عسل
HTTP	پروتکل انتقال فراداده متن
ICMP	پروتکل پیام رسانی کنترل اینترنت
Identity Management	مدیریت شناسه
Identity Theft	دزدی یا سرقت شناسه

IEC	کمیسیون الکترونیکی بین‌المللی
In-band Detection	کشف داخل باند
Incrdent	حادثه
Incident Response	واکنش به حادثه
Inclusiveness	فراگیر و جامع
Indication	نشانه
Industry	صنعت
Information	اطلاعات
Information Reconnaissance	شناسایی اطلاعات
Information sharing	تسهیم و اشتراک گذاری اطلاعات
Infrastructure	زیرساخت
Insider	کارمند داخلی یا خودی
Integrity	یکپارچگی یا امانت داری
Intelligence	هوشمندی یا اطلاعات
Intelligence Community	جامعه اطلاعاتی
Intelligence Reports	گزارش‌های اطلاعاتی
Interface	واسط
Internal Adversary	دشمن داخلی
Internal Firewall	دیوار آتش داخلی

جداسازی داخلی	Internal Separation
کمیسیون‌الکتروتکنیکی بین‌المللی	International Electrotechnical commission
سازمان بین‌المللی استاندارد	International Organization for Standardization
جستجوگر اینترنت یا مرورگر	Internet Explorer
پروتکل اینترنت	Internet Protocol (IP).
پروتکل اینترنت روی ماهواره	Internet Protocol Over Satellite (IPOS)
رله گپ زدن اینترنت	Internet Relay Chat (IRC)
کشف نفوذ	Intrusion Detection
جلوگیری از نفوذ	Intrusion Prevention
فرآیندهای انبارداری و فهرست موجودی	Inventory Processes
سرمایه گذاری	Investment
شبکه محلی	Local Area Network (LAN)
مقیاس وسیع	Large Scale
اجرای قانون	Law Enforcement
کنترل‌های دسترسی لایه‌ای	Layered Access Controls
رمزگذاری لایه‌ای	Layered Encryption
قانونی بودن	Legality
احتمال	Likelihood

Log Files	فایل‌های ثبت وقایع، فایل‌های لاگ
Logical Access Control	کنترل دسترسی منطقی
Logical Diversity	تنوع منطقی
Mainframe	رایانه بزرگ یا مرکزی
Malware	بدافزار
Mandatory Controls	کنترل‌های اجباری
Master Terminal Unit	واحد پایانه اصلی
Meaningful Best Practices	بهترین شیوه‌های عمل معنی دار
Measurable Best Practices	بهترین شیوه‌های عمل قابل اندازه گیری
Media Access Control (MAC)	کنترل دسترسی رسانه
Meta Data	متا داده یا فرا داده
Military Support Services	سرویس‌های حمایتی نظامی
Misinformation	اطلاعات غلط
Multi Level Security (MLS)	امنیت چند سطحی
Monitoring	نظارت یا مانیتورینگ
Multiple Access Control Systems	سیستم‌های کنترل دسترسی چندگانه
National Infrastructure	زیرساخت ملی
National Programs	برنامه‌های ملی
Network Based Firewalls	دیوارهای آتش مبتنی بر شبکه

داده‌های شبکه	Networks Data
پیرامون شبکه	Networks Perimeter
مسیرهای شبکه	Network Routes
ارائه دهنده خدمات شبکه	Network Service Provider
فناوری شبکه	Network Technology
انتقال شبکه	Network Transmission
نتیجه گیری غیرقطعی	Nondefinitive Conclusions
غیریکنواختی یا ناهمسانی	Nonuniformity
لایه‌های ابهام	Obscurity Layer
دیوارهای آتش تجاری آماده فروش	Off-The-Shelf Firewalls
ارتباطات یک به چند	One-to-Many Communication
دسترسی برخط	Online Access
چالش‌های عملیاتی	Operational Challenges
درخواست‌های علنی	Open Solicitation
پیکربندی عملیاتی	Operational Configurations
هزینه‌های عملیاتی	Operational cost
فرهنگ سازمانی	Organizational Culture
قطعی	Outage
همبسته سازی ازخارج باند	Out Of Band Correlation

Outsourcing	برو نسپاری
Packet Filtering Routers	مسیریاب‌های فیلتر کننده بسته
Packet Switched Technology	فناوری سوئیچ بسته‌ای
Parcelling	آماده سازی
Past Security Practice	شیوه عمل امنیتی گذشته
Patching	وصله زنی
Pattern	الگو
Payment Card Industry Data Security Standard (PCIDSS).	استاندارد امنیتی داده‌های صنعت کارت‌های پرداخت
Personal Computer	رایانه شخصی
Personally Identifiable Information (PII)	اطلاعات شناسایی اشخاص
Physical Attack	حمله فیزیکی
Physical Diversity	تنوع فیزیکی
Physical Security	امنیت فیزیکی
Physical Separation	جداسازی فیزیکی
Plain Old Telephone Service (POTS)	سرویس تلفنی قدیمی ساده
Planning	برنامه ریزی
Platform	سکو
Politics	علم سیاست
Policy	سیاست یا خط مشی

Port Scanner	پویش کننده پورت
Post-Attack	پس از حمله
Power Control Networks	شبکه‌های کنترل نیرو
Practical Experience	تجربه عملی
Practice	شیوه عمل یا تمرین
Pre-Attack	پیش از حمله
Predators	شکارچیان
Preparation	آماده سازی
Prevention	جلوگیری
Privacy Policy	سیاست حریم خصوصی
Procedural Controls	کنترل‌های رویه‌ای
Process Allowance	کمک هزینه فرآیند
Process Coordination	هماهنگی فرآیند
Procurement Discipline	انضباط تدارکات
Profile-Based Correlation	همبسته سازی مبتنی بر مشخصات
Proof Factors	فاکتورهای اثبات
Proprietary Information	اطلاعات اختصاصی
Protection	حفاظت
Public Key Infrastrucure (PKI)	زیرساخت کلید عمومی

Public Speaking	صحبت عمومی
Public Swiched Telephone Network (PSTN)	شبکه تلفن سوئیچ مداری
Quality Issues	مسائل مربوط به کیفیت
Real Assets	سرمایه‌های واقعی
Real Time	بی‌درنگ، زمان واقعی
Reliability	قابلیت اطمینان
Remote Terminal Unit (RTU)	واحد پایانه از راه دور
Removal Option	گزینه حذف
Replication	تکرار
Request For Information (RFI)	درخواست برای اطلاعات
Request For Proposal (RFP)	درخواست برای پیشنهاد
Response	پاسخ یا واکنش
Return On Investment (ROI)	بازگشت سرمایه
Reward Structure	ساختار پاداش
Right-Of-Way Routes	مسیرهای با حق راه
Risk Management Process	فرآیند مدیریت ریسک
Risk Reduction	کاهش ریسک
Root Cause	علت ریشه‌ای
Salary	حقوق و دستمزد

Sarbanes-Oxley Controls	کنترل‌های ساربینز – اُکسلی
Sasser Worm	کرم سا سر
Satellite Data Services	خدمات داده ماهواره ای
Scaling Issues	مسائل مربوط به مقیاس
Scanning Stage	مرحله پویش
Search For Leakage	جستجو برای نشت
Secure Commerce	تجارت امن
Secure Sokets Layer (SSL)	لایه سو کت‌های امن
Security Audit	ممیزی امنیتی
Security Information And Event Management (SIEM)	اطلاعات امنیتی و مدیریت رویداد
Security Information Management System(SIMS)	سیستم مدیریت اطلاعات امنیتی
Security Operation Center (SOC)	مرکز عملیات امنیت
Security Policy	سیاست امنیتی
Security Posture	وضعیت امنیتی
Security Standard	استاندارد امنیتی
Security Team	گروه امنیتی
Security Through Obscurity	امنیت از طریق ابهام
Segregation	سیاست جداسازی و تبعیض

Segregation Of Duties	جداسازی وظایف
Senior Management	مدیر ارشد
Sensitive Information	اطلاعات حساس
Separation	جداسازی
Service Level Agreement (SLA)	توافق سطح خدمت
Service Ports	پورت‌های سرویس
Signature-Based Correlation	همبسته سازی مبتنی بر امضا
Signature Sharing	اشتراک گذاری امضا
Single Sign-On (SSO)	ثبت نام تنها
Situational Awareness	آگاهی موقعیتی
Sizing Issues	مسائل مربوط به اندازه
Smart Devices	دستگاه‌های هوشمند
Software Bugs	اشکالات نرم افزار
Software Engineering Standards	استانداردهای مهندسی نرم افزار
Software Life Cycle	چرخه عمر نرم افزار
Spam	هرزنامه
Sponsered Research	تحقیقات حمایت شده
Standard Audit	ممیزی استاندارد
Stream Of Consciouness Design	طراحی با جریانی از آگاهی

Subjective Estimation	برآورد ذهنی
Sufficient Detail	جزییات کافی
Suitability	تناسب، شایستگی
Supervisory Control And Data Acquisition	کنترل نظارت و به‌دست آوردن داده‌ها
Supplier Adversary	دشمن تأمین کننده
Supplier	تأمین کننده
Supply Chain	زنجیره تأمین
Support And Trainning	پشتیبانی و آموزش
System Administration	مدیریت سیستم
Trailored Separation	جداسازی متناسب شده
Target Factor	شاخص هدف
Telecommunication	ارتباطات از راه دور
Terrorist Attacks	حملات تروریستی
Theft	دزدی یا سرقت
Threat	تهدید
Threat Management	مدیریت تهدید
Time-Based Correlation	همبسته سازی مبتنی بر زمان
Time Division Multiplex (TDM)	تسهیم با تقسیم زمانی
Tools	ابزارها

Top Secret	فوق محرمانه
Transmission Control Protocol (TCP)	پروتکل کنترل انتقال
Transparency	شفافیت
Transportation Infrastructure	زیرساخت حمل و نقل
Trap	تله
Trend	روند
Trusted Computing Base	پایه محاسباتی مورد اعتماد
Uncertainity	عدم قطعیت و عدم یقین
Usage Metric	متریک استفاده
Use-Case Study	مطالعات موردی استفاده
Utilization Metric	متریک استفاده
Value Proposition	گزارش ارزش
Vantage Point	دیدگاه
Vendors	فروشندگان
Vigilant Watch	دیدبان هوشیار یا دیده بانی هوشیارانه
Violation Issues	مسائل مربوط به نقض یا تخطی
Virus	ویروس
Vulnerability	آسیب پذیری
Well Known Computer Security Techniques	تکنیک‌های امنیتی رایانه‌ی معروف

Wide Area	پهنه وسیع
Work Function	تابع کار
World Class	کلاس جهانی
Worms	کرم‌ها
Worst Case Assumption	فرض بدترین حالت

کوتاه نوشته‌ها
ACL : Access Control
BSS : British Security Standard
CDN : Content Distribution Network
CEO : Chief Executive Officer
CERT : Computer Emergency Response Team
CIO : Chief Information Officer
CISSP : Certified Information Systems Security Professional
CPU : Central Processing Unit
DDOS : Distributed Denial Of Service
DLP : Data Leakage Protection
DNS : Domain Name Service
DOS : Denial Of Service
FISMA : Federal Information Security Management Act
Gbps : Giga bit per second
3G : Third Generation
4G : Fourth Generation
HIPAA : Health Insurance Portability And Accountability Act
HMI : Human Machine Interface
HTTP : Hyper Text Transfer Protocol
ICMP :Internet Control Messaging Protocol
IDS : Intrusion Detection System
IEC : International Electrotechnical Commission

IP : Internet Protocol

IPOS : Internet Protocol Over Satellite

IP SEC : Internet Protocol Security

IRC : Internet Relay Chat

ISO : International Standard Organization

IT : Information Technology

Kbps : Kilo bit per second

LAN : Local Area Network

MAC : Media Access Control

Mbps : Mega bit per second

MLS : Multi Level Security

MTU : Master Terminal Unit

O.S : Operating System

PC : Personal Computer

PCIDSS : Payment Card Industry Data Security Standard

PII : Personally Identifiable Information

PIN : Personal Identification Number

PKI : Public Key Infrastructure

POTS : Plain Old Telephone Service

PSTN : Public Swiched Telephone Network

RFI : Request For Information
RFP : Request For Proposal
ROI : Return On Investment
RTU : Remote Terminal Unit
SCADA : Supervisory Control And Data Aquisition
SIEM : Security Information And Event Management
SIMS : Security Information Management System
SLA : Service Level Agreement
SMTP : Single Mail Transport Protocol
SOC : Security Operation Center
SQL : Strucured Query Language
SSL : Secure Sockets Layer
SSO : Single-Sign On
STD : Standard
TCB : Trusted Computing Base
TCP : Transmission Control Protocol
TDM : Time Divission Multiplex
UDP : User Datagram Protocol
U.S : United States
VPN : Virtual Private Network
WiFi : Wireless Fidelity

بیوگرافی مترجم کتاب

احمد صلاحی در سال ۱۳۴۹از دانشکده فنی دانشگاه تهران در رشته مهندسی برق فارغ‌التحصیل شد.در سال ۱۹۷۴ از دانشگاه کانزاس فوق‌لیسانس مهندسی برق ودرسال ۱۹۷۹ از دانشگاه پردو در ایالات‌متحده آمریکا در مهندسی برق(کامپیوتر)دکترای Ph.D اخذ نمود.

دکتر صلاحی از سال ۱۳۵۹ در مرکز تحقیقات مخابرات ایران مشغول بکار بوده‌اند و مدیر سه پروژه ملی سوئیچ عصر ،ترانزیت و سوئیچ پر ظرفیت و از سال ۸۶ تا ۸۹ مدیر گروه امنیت شبکه بوده‌اند. دو بار در ششمین و سیزدهمین جشنواره خوارزمی جایزه دوم و اول تحقیقات کاربردی را دریافت کرده‌اند و در دو سال (۱۳۸۰و۱۳۹۰) پژوهشگر برتر کشور شده‌اند.ایشان جز هیئت‌علمی (دانشیار) مرکز تحقیقات بوده و۸ درس مختلف در مقطع کارشناسی ارشد ارائه کرده‌اند