روندهای امنیت سایبری در سال ۲۰۱۷

مقدمه:

در امنیت همواره تغییر با خطر[1] همراه است. از آنجا که تغییر، همیشه وجود دارد، آگاهی از تغییرات کلیدی که خطر را افزایش می‌دهند، بخشی حیاتی از واکنش‌گرا[2] بودن در امنیت سایبری است. یک معادله ساده برای خطر به صورت زیر است:

در واقع تیم‌های امنیتی تنها نیمی از پارامتر "اقدام"[3] را کنترل می‌کنند. ما نمی‌توانیم زمان انجام یا گسترش تهدیدها را تعیین کنیم و آسیب‌پذیری‌ها به علت ضعف در افراد و فناوری انباشته می‌شوند. افراد به آرامی تغییر می‌کنند، اما فناوری به سرعت در حال تغییر است و پذیرش فناوری‌های جدید کسب و کار، همواره منجر به آسیب‌پذیری‌های جدیدی می‌شود که تهدیدهای تازه‌ای را ممکن می‌سازد. درک و پیش‌بینی نیاز کسب و کار برای فناوری‌های نوظهور یک عنصر کلیدی در برنامه‌های امنیتی موفقیت‌آمیز می‌باشد.

با هر موج جدیدی از فناوری، تهدیدها به سه شکل حملات انکار سرویس (DoS)[4]، جرایم سایبری و حملات دولتی رخ می‌دهند.

حملات DoS

هنگامی که نقاط ضعف در فناوری‌های جدید (عموماً توسط محققان، دانشگاهیان و گروه‌های هکری) افشا می‌شوند، برای شروع، ساده‌ترین روش حملات انکار سرویس هستند. این حملات، سیستم‌ها را از کار می‌اندازند یا منجر به هجمه‌های داده‌ای می‌شوند که شبکه‌ها را متوقف می‌سازند.

[1] Risk
[2] Proactive
[3] Action
[4] Denial of Service

جرایم سایبری

مجرمان سایبری و اکوسیستمی که این افراد را تحت حمایت قرار می‌دهند، حملات را با تمرکز بر روی روش‌هایی اصلاح می‌کنند که می‌توانند منجر به درآمد شوند. شایع‌ترین آنها به وسیله سرقت اطلاعات و استفاده از آن جهت فروش محصول یا خدمت به عنوان فروشنده مجاز یا پشتیبانی از حساب‌های تقلبی صورت می‌گیرد.

حملات دولتی

بیشتر حملات انجام شده توسط دولت اما نه همه آنها، از آسیب‌پذیری‌های فاش شده و تکنیک‌های توسعه‌یافته در دو مرحله قبل استفاده می‌کنند که جهت حملات به شدت اصلاح شده و هدفمند علیه اهداف خاص که دارای ارزش ملی هستند، توسعه می‌یابند.

در هر سه مورد، معمولاً آسیب‌پذیری‌های اصلی که مورد استفاده قرار می‌گیرند، تفاوتی ندارند. در حالیکه کاهش آسیب‌پذیری‌ها جهت پیشگیری یا به حداقل رساندن آسیب در تمام شکل‌های حمله، کلیدی و مهم است، آنچه که با گذشت زمان به طور چشمگیری تغییر می‌کند، مکانیزم تحویل[5] تهدیدها است.

تغییرات در تهدیدها تنها یکی از عواملی هستند که بر روی برنامه‌های امنیت سایبری تأثیر می‌گذارند. تغییرات فناوری و نیاز کسب و کار برای استفاده از فناوری‌های جدید اغلب منجر به شکست بسیار بزرگتری برای فرآیندها و کنترل‌های امنیتی موجود می‌شود. این مقاله به روند تهدید و روند فناوری کسب و کار که تیم‌های امنیت سایبری باید در سال ۲۰۱۷ مورد ملاحظه قرار دهند، توجه دارد تا به آنها کمک شود که منابع خودشان را در حوزه‌هایی با بیشترین سود متمرکز کنند.

روندهای تهدید:

سه روند در عرصه تهدید به ویژه در سال ۲۰۱۷ مطرح خواهند بود.

[5] delivery mechanism

ادامه‌دار بودن صدرنشینی آسیب‌پذیری‌های شناخته‌شده

در حالیکه حملاتی که آسیب‌پذیری‌های صفر روزه[6]را مورد استفاده قرار می‌دهند، تحت بیشترین پوشش خبری قرار می‌گیرند، آن حملاتی که آسیب‌پذیری‌های شناخته‌شده را بکار می‌گیرند، بیشترین خسارت‌ها را به کسب و کار وارد می‌کنند. شرکت امنیتی SANS تخمین می‌زند که بیش از ۸۰ درصد از حوادث امنیت سایبری، آسیب‌پذیری‌های شناخته‌شده را مورد استفاده قرار می‌دهند و گزارش سالانه از سوی مؤسسه Verizon با عنوان بررسی رخنه داده‌ها[7]نیز ارقام مشابه را نشان می‌دهد [1]. گارتنر خیلی بیشتر پیش می‌رود و برآورد می‌کند که تا سال ۲۰۲۰، ۹۹ درصد از آسیب‌پذیری‌های مورد استفاده به مدت حداقل یک سال است که توسط متخصصان امنیتی و IT شناخته شده‌اند [2].

با توجه به روندهای فناوری کسب و کار (در ادامه مورد بررسی قرار گرفته)، میزان آسیب‌پذیری‌های صفر روزه صرفاً به دلیل افزایش تعداد محصولات و سیستم‌عامل‌های مورد استفاده، افزایش خواهند یافت. با این حال، هنوز هم بیشترین خطرات، از آسیب‌پذیری‌های شناخته‌شده و به خوبی درک شده ناشی خواهند شد. کلید کاهش آسیب کسب و کار، تشخیص سریع‌تر آسیب‌پذیری‌ها و کاهش سریع‌تر و دقیق‌تر آن است. در حالیکه کاهش، همچون اصلاح یا جایگزینی نرم‌افزار قدیمی امکان‌پذیر نیست، محافظت کردن از طریق پیشگیری از نفوذ و تکنیک‌های دیواره آتش لایه کاربرد، حیاتی می‌باشد. حداقل سیستم‌هایی با آسیب‌پذیری-های شناخته‌شده که میزبان داده‌های حیاتی هستند باید مکلف گردند تا به منظور امکان تشخیص سریع‌تر حملات و خطرات، تحت نظارت مستمر باشند.

رخنه‌ها تمام ماجرا نخواهند بود

چند سال قبل، حملات تکامل یافته که از محققان و گروه‌های هکری نشأت گرفته بودند، منجر به حملات انکار سرویس شدند تا مجرمان اینترنتی درصدد سرقت اطلاعات مشتری و کسب و کار به قصد کلاهبرداری از حساب و سایر جرایم مالی باشند. به دنبال حملات دولتی، با انجام بررسی‌های صورت گرفته ثابت شد که سازمان‌های جاسوسی آمریکا و چین حملاتی را مرتکب شده‌اند.

[6] zero-day
[7] Data Breach Investigation

امکان مشاهده رخنه‌ها باعث شده تا بسیاری از سازمان‌ها روی پایش پایگاه داده‌ها و شبکه‌ها برای یافتن نشانه‌هایی از اختلال داده تمرکز کنند. هرچند از سال ۲۰۱۵ تا ۲۰۱۶ تعداد رخنه‌ها ۱۷ درصد افزایش یافت، اما تعداد میانگین رکوردهای داده فاش شده در هر رخنه به ۸۲ درصد کاهش پیدا کرد، چون شرکت‌ها در تشخیص برون‌رفت انبوهی از داده‌ها هوشیارتر شدند [3].

با این حال، مجرمان ثابت نمی‌مانند. در طی سال‌های ۲۰۱۵ و ۲۰۱۶ حملات باج‌افزار[8] رشد زیادی را نشان دادند (شکل ۱).

شکل ۱- باج‌افزار در حال گسترش است [4].

در واقع باج‌افزار، یک شکل از حمله انکار سرویس است که از بدافزار برای رمزنگاری داده‌های حیاتی یا اجرایی استفاده می‌کند؛ در نتیجه سرویس‌های کسب و کارهای کلیدی متوقف می‌شوند. حملات باج‌افزار تمایل به استفاده از آسیب‌پذیری‌هایی مانند تلاش‌های رخنه دارند، اما این حملات نقاط ضعف در فرآیندهای پشتیبان-گیری از داده‌ها و نظارت بر ترافیک را نیز مورد توجه قرار می‌دهند.

[8] Ransomware Attacks

شکل جدیدی از باج‌افزار که مسلماً رشد خواهد یافت، "جاسوس فساد"[9]است. در حالیکه جاسوس فساد، امکان استفاده از مزایای آسیب‌پذیری‌های مشابه را مانند سایر حملات باج‌افزار فراهم می‌کند؛ اما برای مخفی کردن یا رمزنگاری داده‌ها از بدافزار استفاده نمی‌کند، بلکه بر روی رایانه‌های شخصی و سرورهای شرکت دانلود می‌کنند و فایل‌ها، تصاویر یا فیلم‌ها را آلوده می‌سازند. با تهدید به افشای محتوای جاسوسی شده، مهاجمان یا به دنبال مبالغ باج می‌روند یا به طور حیله‌گرانه‌تر کاربران را متقاعد می‌کنند که نام کاربری/رمز عبور معتبرشان را ارائه دهند. چون استفاده کاربران کسب و کار از رسانه اجتماعی افزایش می‌یابد و مراکز داده، بکارگیری سرویس‌های ابری را گسترش می‌دهند، این حمله راحت‌تر انجام می‌شود. آسیب‌پذیری Cloudbleed که CloudFlare به تازگی آن را افشا کرده، ماهیت در حال تغییر این خطر را نشان می‌دهد [5].

حملات شخص چهارم افزایش خواهند یافت

در سال ۲۰۱۳، شرکت خرده‌فروشی آمریکایی Target دچار یک رخنه شد، به طوریکه بیش از ۴۰ میلیون مورد از حساب‌های مشتریان افشا شد و شرکت، بیش از ۱۰۰ میلیون دلار در هزینه‌های مستقیم متحمل هزینه گردید. ابتدا مهاجمان یک پیمانکار سیستم گرمایش و تهویه مطبوع[10](HVAC) را مورد هدف قرار دادند که به فروشگاه‌های Target دسترسی راه دور داشت و سپس از تقسیم‌بندی شبکه Target و نظارت ضعیف بر آن سوءاستفاده نمودند. رخنه Target امکان مشاهده این خطرات شخص ثالث را افزایش داده است، اما مهاجم تمایل دارد که حرکتش را به سمت بیرون در زنجیره تأمین ادامه دهد تا اشخاص چهارم مانند طرفین قرارداد فرعی، تأمین‌کننده خارجی، ارائه‌دهندگان سرویس ابری و سازندگان دستگاه را احاطه کند.

با اطمینان از اینکه سرویس‌های شخص سوم و چهارم به اندازه کافی برای استفاده در کسب و کار ایمن هستند، تیم‌های امنیتی نیاز پیدا می‌کنند تا در فرآیند انتخاب تأمین‌کننده درگیر شوند و فرآیندها و کنترل‌هایی را در محل داشته باشند تا به طور مستمر آسیب‌پذیری و وضعیت در معرض خطر شرکای تجاری و تأمین‌کنندگان را نظارت کنند.

[9] Badness Planting
[10] Heating, Ventilation and Air Conditioning (HVAC)

روندهای فناوری کسب و کار:

در بسیاری از روش‌ها، تغییرات در تهدیدها نسبت به تغییرات در کسب و کار در جهت استفاده از فناوری‌ها و سرویس‌های جدید، قابل مدیریت‌تر است. یک حمله جدید ممکن است به سازمان شما یا آسیب بزند یا نزند؛ اما زمانی که یک سازمان امنیتی مانع شروع یک کسب و کار جدید می‌شود، ۱۰۰ درصد منجر به خسارت خواهد شد. در اینجا چند نمونه از مهم‌ترین روندها را معرفی می‌کنیم و توضیح می‌دهیم که چگونه بر امنیت اثر می‌گذارند.

قابلیت انتقال و افزایش استفاده از سرویس‌های ابری

تاجران به دو دلیل عمده مجبور شده‌اند که روش کسب و کار خود را تغییر دهند. (۱) فراوانی دستگاه‌های موبایل، چه متعلق به یک شرکت یا یک فرد باشد و (۲) افزایش استفاده از سرویس‌های ابری. به عنوان مثال در سال ۲۰۱۶، ۸۳ درصد از کارمندان، سر کار موبایل‌های هوشمند داشته‌اند که دو سوم آنها چندین بار در روز از آن استفاده می‌کرده‌اند [6]. IDC پیش‌بینی می‌کند که تا سال ۲۰۲۰، بیش از ۷۰ درصد از نیروی کار موبایل خواهند داشت [7]. افراد در کسب و کار منافع خودشان را در صرفه‌جویی هزینه‌ها می‌بینند و تغییر و نوآوری را با قابلیت انتقال افزایش می‌دهند.

علی‌رغم این مزایا، قابلیت انتقال خطرات جدیدی را نیز به وجود آورده است. موبایل‌ها ناهمگون می‌باشند و به سرعت تغییر می‌کنند. در کسب و کار، سرویس‌های زیرساختی و نرم‌افزاری ابری برای کاهش هزینه و زمان مبادلات و تجارت حیاتی می‌باشند.

تحقیقی در سال ۲۰۱۷ توسط شبکه‌های Skyhigh منتشر شده است که نشان می‌دهد در سرمایه‌گذاری روزانه به طور متوسط ده‌ها سرویس ابری مجاز و صدها سرویس ابری غیرمجاز استفاده می‌شود [8]. اگرچه این تعداد در چند سال آینده به علت رکود سرویس‌های ابری به دلیل ازدحام بالا، کاهش می‌یابد؛ اما حجم انتقال داده‌های حیاتی به سرویس‌های ابری و وابستگی بالای کسب و کار به این سرویس‌ها افزایش خواهند یافت (جدول ۱ را ببینید).

جدول ۱- انتقال به ابر توسط بخش تجاری [9]

بخش‌ها	سرویس ابر	اندازه مجموع تجارت در سال ۲۰۱۶	مجموع انتقال به ابر در سال ۲۰۱۶	نرخ انتقال به ابر تا سال ۲۰۲۰
برون‌سپاری فرآیندکسب و کار	BPaaS	۱۱۹ میلیارد دلار	۴۲ میلیارد دلار	۴۳ درصد
نرم‌افزار کاربردی	SaaS	۱۴۴ میلیارد دلار	۳۶ میلیارد دلار	۳۷ درصد
نرم‌افزار زیرساخت کاربردی	PaaS	۱۷۷ میلیارد دلار	۱۱ میلیارد دلار	۱۰ درصد
زیرساخت سیستم	laaS	۲۹۴ میلیارد دلار	۲۲ میلیارد دلار	۱۷ درصد
PaaS: فرآیند کسب و کار به صورت یک سرویس، **laaS**: زیرساخت به صورت یک سرویس، **PaaS**: پلت‌فرم به صورت یک سرویس، **SaaS**: نرم‌افزار به صورت یک سرویس				

افزایش استفاده از سرویس‌های ابری، روش‌های سنتی مدیریت فناوری اطلاعات و فرآیندهای عملیاتی را نقض می‌کند که به نوبه خود قابلیت مشاهده و کنترل برنامه امنیتی را تحت تأثیر قرار می‌دهد.

استفاده از SaaS نمایانگر این است که یک برنامه نرم‌افزاری منحصر به فرد جدیدی مورد استفاده قرار گرفته و استفاده از laaS به اضافه شدن یک مرکز داده جدید به مجموعه شباهت دارد که بدون آن، فناوری اطلاعات قادر به دیکته کردن یک سری از دستورها مانند کنترل نسخه و بررسی کد نیست. بیشتر سازمان‌های فناوری اطلاعات باید فرآیندهای عملیاتی، مدیریتی، تضمین کیفیت و توسعه خود را بروزرسانی کنند.

همانطور که نیازهای تجاری، فناوری اطلاعات را مجبور به انتقال به سرویس‌های ابری می‌کند، سازمان‌های امنیتی نیز باید مطمئن شوند که کنترل‌های امنیتی حفظ شوند و یا حتی در آنها بهبود حاصل شود. به منظور کاهش خطرات جابجایی به سمت سرویس‌های ابری، فناوری اطلاعات باید فرآیندهای امنیتی خود را برای نظارت مداوم و مدیریت آسیب‌پذیری به سرویس‌های موردنظر اضافه کند. این موضوع شامل موارد زیر است:

- اطمینان حاصل شود که تیم امنیتی در فرآیند انتخاب سرویس ابری شرکت می‌کنند و نیازهای امنیتی فراهم شده و معیار ارزیابی امنیتی از درجه بالایی برخوردار است.
- تأکید بر پیکربندی و ارزیابی آسیب‌پذیری برنامه‌ها قبل از استقرار برنامه نهایی بر روی سرویس ابری.

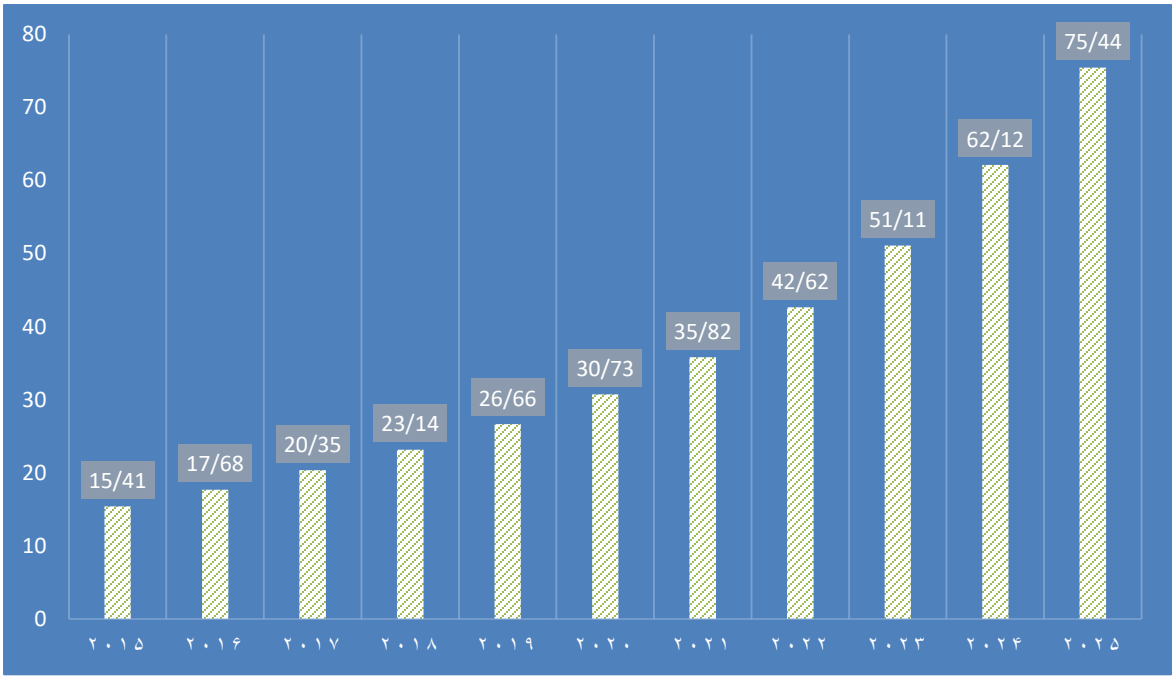
- یکپارچه‌سازی نظارت مستمر به آسیب‌پذیری‌های امنیتی و بروزرسانی مدیریت فناوری اطلاعات و فرآیندهای عملیاتی همانطور که استفاده از ابر ترکیبی و IaaS رشد می‌کنند.
- ادغام داده‌های نظارتی به دست آمده از سرویس‌های ابری و برنامه‌های موجود در مرکز داده شرکت.

افزایش استفاده از سرویس‌های ابری منجر به افزایش سرویس‌های امنیتی می‌شود. زمانی که فناوری اطلاعات یک مکانیزم تحویل جدیدی را اضافه می‌کند، بخش امنیتی نیز باید همان مکانیزم را اضافه کند. تحویل مبتنی بر ابر سرویس‌های امنیتی در طی چند سال گذشته به سرعت افزایش یافته است و همانطور در حال افزایش است. معماری‌های ترکیبی که در آن کنترل‌های امنیتی با قابلیت‌های امنیتی مبتنی بر ابر تجمیع می‌شوند، معیاری استاندارد برای همه شرکت‌های بزرگ و سازمان‌های دولتی می‌باشند.

اینترنت اشیاء

حملات Mirai در سال ۲۰۱۶ اثبات کرد که حملات در دنیا بر علیه آسیب‌پذیری‌های اینترنت اشیاء، منجر به خسارت جدی به سازمان‌ها شده‌اند [10].

به طور ساده، اینترنت اشیاء شامل هر چیزی است که اتصالی با اینترنت دارد. با توجه به این تعریف می‌توان گفت که اشیاء نسبت به سایر فناوری‌های پیشین بسیار رشد کرده است (شکل ۲ را ببینید).



شکل ۲: انتظار می‌رود که تعداد دستگاه‌های اینترنت اشیاء در یک دهه پنج برابر شوند [11].

با این وجود، از لحاظ امنیتی اهمیت دارد تا به دستگاه‌های مختلفی که اینترنت اشیاء را تشکیل می‌دهند توجه کنیم. SANS چهار دسته را تعریف می‌کند:

- کامپیوترهای شخصی، سرورها، مسیریاب‌ها، سوئیچ‌ها و دستگاه‌های مشابه که اصولاً با کابل متصل می‌شوند و توسط فناوری اطلاعات سازمان‌ها خریداری می‌شوند.
- دستگاه‌های پزشکی، اسکادا، کنترل فرآیند، کیوسک‌ها و فناوری‌های مشابه که اصولاً با کابل متصل می‌شوند و توسط فناوری عملیاتی سازمان‌ها خریداری می‌شوند.
- گوشی‌های هوشمند و تبلت‌ها که به عنوان دستگاه‌های فناوری اطلاعات توسط مصرف‌کنندگان (کارمندان) خریداری می‌شوند، اتصال بی‌سیم را استفاده می‌کنند و غالباً از چندین اتصال بی‌سیم پشتیبانی می‌کنند.
- دستگاه‌های تک‌منظوره (توسط مصرف‌کنندگان، فناوری اطلاعات یا فناوری عملیاتی خریداری می‌شوند) که قابلیت اتصال بی‌سیم را دارند. (عمدتاً یک نوع اتصال)

سه نمونه دستگاه اول امروزه مورد استفاده قرار می‌گیرند. هر نمونه‌ای که به وجود می‌آید، منجر به شکست امنیتی بزرگی می‌شود و نیازمند تغییرات امنیتی همچون یکپارچه‌سازی فناوری اطلاعات یا فناوری عملیاتی (IT/OT)، کنترل‌های امنیتی با خود دستگاه، کنترل دسترسی به شبکه و اشکال جدید مدیریت و ارزیابی آسیب‌پذیری می‌باشد.

رشد در طول چند سال آینده جزء چهارمین دسته خواهد بود. این دستگاه‌های تک‌منظوره در زیرساخت (ساختمان‌های هوشمند، ماشین‌های هوشمند، سیستم‌های پایش محیطی) و همچنین در محصولات انفرادی که کارمندان (نه مشتریان) استفاده می‌کنند، تعبیه می‌شوند و معمولاً به شبکه‌های تجاری متصل می‌گردند.. افزایش ناهمگونی منجر به شکست در کشف، ارزیابی آسیب‌پذیری و کنترل‌ها و فرآیندهای مدیریتی می‌شود که مهاجمان را قادر خواهد ساخت تا با استفاده از اشیاء آسیب‌پذیر، انواع حملات را به سمت سیستم شما روانه سازند.

محدوده و قابلیت مشاهده نقض سونی در سال ۲۰۱۴ روندی را آغاز کرد که در سال ۲۰۱۷ و بعد از آن تسریع خواهد شد. هیئت‌های مدیره شرکت‌ها به طور فزاینده‌ای تحت فشار قرار می‌گیرند تا به امنیت سایبری به عنوان بخشی از نقش نظارتی خود توجه داشته باشند. پیش از نقض سونی، ۷ درصد از مدیران، امنیت

سایبری را به عنوان یک اولویت بالا در نظر می‌گرفتند. با توجه به ضرر اقتصادی بزرگ سونی، درصد توجه مدیران به ۳۰ درصد در سال ۲۰۱۶ افزایش یافت [12].

SANS تخمین می‌زند که امروزه، بیش از ۶۰ درصد از مدیران امنیت اطلاعات شرکت‌های بزرگ، حداقل یک بار در سال به هیئت مدیره گزارش می‌دهند. تا پایان سال ۲۰۱۸، ۷۰ درصد از تمام هیئت مدیره‌ها نیاز دارند که مدیران امنیت اطلاعات به آنها هر سه ماه یک بار گزارش دهند. علاوه بر نقض‌های افشا شده عمومی که عامل پیشران این علاقه است، نهادهای نظارتی و کنگره از مدیران سازمان‌ها و شرکت‌ها درباره سطح درک و نظارت خود بر ریسک‌های مربوط به امنیت سایبری سؤال می‌کنند.

در نتیجه‌ی توجه بیشتر به مسائل امنیتی، اعضای هیئت مدیره انتظارات بالایی در مورد کیفیت و ارزش استراتژیک اطلاعات دریافتی از مدیران امنیت اطلاعات خواهند داشت. هیئت‌های مدیره از مدیران تجاری انتظار دارند تا خطرات سطح بالا و استراتژی‌های مالی را مورد بحث قرار دهند و آنها را برای مقابله با مشکلات آماده کنند. اکنون از مدیران امنیتی انتظار می‌رود که اطلاعات استراتژیک مشابه را در حوزه امنیت برای هیئت مدیره آماده کنند.

روندهایی که بر روی برنامه‌های امنیتی اثر می‌گذارند، به معماری‌ها، فرآیندها، کنترل‌ها و مهارت‌هایی برای حفظ سطوح قابل قبولی از خطر سایبری نیاز دارند. درست همانطور که وزن کم کردن همواره نیاز به غذا خوردن کمتر و ورزش بیشتری دارد، برخی از حوزه‌های کلیدی امنیت سایبری هستند که نباید تغییر کنند، ولی پایه و اساس ضروری برای برخورد با خطرات جدید را فراهم می‌آورند.

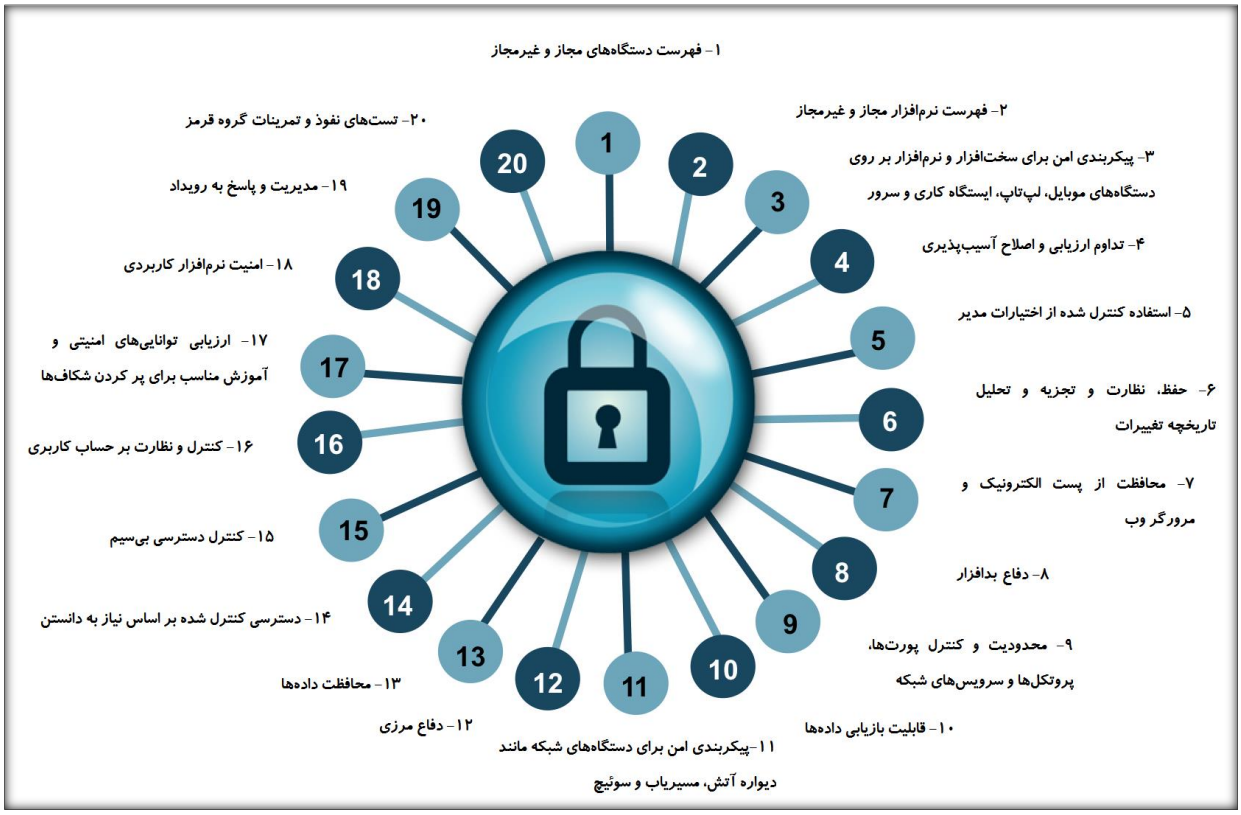
سلامت امنیت پایه[11]

همانطور که قبلا اشاره شد، اکثریت قریب به اتفاق حملات موفق، به استفاده از آسیب‌پذیری‌های شناخته‌شده- اساساً افشای عدم سلامت امنیت پایه ادامه خواهند داد. شرکت امنیتی SANS مدت زیادی است که از تلاش کنترل‌های امنیتی حیاتی[12] که در سال ۲۰۰۸ در آژانس امنیت ملی آغاز به کار کرد و در حال حاضر یک تلاش جمعی هماهنگ توسط مرکز امنیت اینترنت (CIS)[13] می‌باشد، پشتیبانی می‌کند. کنترل‌های مرکز امنیت

[1] Basic Security Hygiene [1]
[1] Critical Security Controls (C[2]SC)
[1] Center for Internet Security [3]

اینترنت ثابت کرده‌اند که یک چارچوب مؤثر برای تمرکز منابع امنیتی بر روی کنترل‌های امنیتی مؤثر و کارآمد هستند که بیشترین موانع را برای حملات دنیای واقعی ایجاد می‌کنند.

کنترل‌های مرکز امنیت اینترنت به صورت دوره‌ای با آخرین نسخه (6.1) که در دسامبر ۲۰۱۵ انتشار یافته است، به روزرسانی می‌شوند (شکل ۳).



شکل ۳- کنترل‌های امنیتی حیاتی مرکز امنیت اینترنت، نسخه 6.1

تغییرات عمده شامل موارد زیر هستند:

- "استفاده کنترل شده از اختیارات مدیر" در اولویت افزایش یافت، حرکت از کنترل مرکز امنیت اینترنت ۱۲ به کنترل مرکز امنیت اینترنت ۵، تشخیص تعداد زیادی از حملات که امکان استفاده از حساب‌های کاربری با اختیارات بالا را به وجود آوردند.
- "مهندسی شبکه امن" که کنترل مرکز امنیت اینترنت ۱۹ بود، به دلیل هم‌پوشانی مفاهیم کلیدی تقسیم‌بندی در سایر حوزه‌ها حذف گردید.

- "محافظت از پست الکترونیک و مرورگر وب" به عنوان یک کنترل جدید اضافه شد، به طوریکه بر اساس درصد بالایی از حوادث بود و از تهدیدهای آغاز شده توسط حملات فیشینگ ناشی می‌شد.

کنترل‌های فرعی برای کمک به طرح‌ریزی استقرار و واضح بودن نگاشت به چارچوب‌هایی مانند چارچوب امنیت سایبری مؤسسه ملی فناوری و استانداردها (NIST)[1]،[14] به یکی از سه دسته سیستم، شبکه و برنامه کاربردی گروه‌بندی شدند.

شرکت‌ها با تمرکز بر روی پنج کنترل ابتدایی مرکز امنیت اینترنت، می‌توانند پایه‌ای قوی برای برخورد با روندهای مشخص شده در این مقاله را به وجود آورند و بسیاری از حوادث امنیتی رایج را کاهش داده یا از آنها پیشگیری نمایند.

منابع:

[1] "2015 Data Breach Investigations Report," Verizon, https://msisac.cisecurity.org/whitepaper/documents/1.pdf

[2] Gartner's Top 10 Security Predictions 2016," June 15, 2016, www.gartner.com/smarterwithgartner/top-10-security-predictions-2016

[3] "Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout," Identity Theft Resource Center, Jan. 19, 2017, www.idtheftcenter.org/2016databreaches.html

[4] "Kaspersky Security Bulletin 2016," https://kasperskycontenthub.com/securelist/files/2016/12/KASPERSKY_SECURITY_BULLETIN_2016.pdf

[5] "Quantifying the Impact of 'Cloudbleed,'" https://blog.cloudflare.com/quantifying-the-impact-of-cloudbleed

[6] "New CareerBuilder Survey Reveals How Much Smartphones Are Sapping Productivity at Work," June 9, 2016, www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=6%2F9%2F2016&id=pr954&ed=12%2F31%2F2016

[7] "Why You Should Care About Mobile Workforce Management," http://tech.co/mobile-workforce-management-2016-01

[8] "Cloud Adoption and Risk Report," Q4 2016, www.skyhighnetworks.com/cloud-report

[9] "Gartner Says by 2020 'Cloud Shift' Will Affect More Than $1 Trillion in IT Spending," July 20, 2016, www.gartner.com/newsroom/id/3384720

[10] "Port 7547 SOAP Remote Code Execution Attack Against DSL Modems," SANS ISC InfoSec Forums, https://isc.sans.edu/forums/diary/Port+7547+SOAP+Remote+Code+Execution+Attack+Against+DSL+Modems/21759

[1] National Institute of Standards and Technology

[11] "IoT platforms: enabling the Internet of Things," IHS Markit, March 2016, https://cdn.ihs.com/www/pdf/enabling-IOT.pdf

[12] "Improving The Security Conversation For CIOs, CISOs, & Board Members," DarkReading, Sept. 28, 2016, www.darkreading.com/careers-and-people/improving-the-security-conversation-for-cios-cisos-and-board-members/d/d-id/1327030