ده گام برای مدیریت موثر آسیب‌پذیری‌ها

چالش‌های مدیریت آسیب‌پذیری

برای هر سازمانی اطلاعات، سرمایه با ارزشی است، با این حال این اطلاعات به چالشی برای امنیت تبدیل شده‌است. وقتی که مقدار اطلاعات به‌طور قابل توجهی افزایش می‌یابد به همان اندازه نیز انگیزه تبهکاران و هکرها برای دستیابی به آن بیشتر و بیشتر می‌شود، اما برخلاف سایر سرمایه‌های با ارزش همچون پول، اطلاعات در محل ایمنی که بتوان براحتی از آن محافظت کرد از امنیت برخوردار نیست. در عوض، اطلاعات در سرتاسر سیستم‌ها، شبکه‌ها و دستگاه‌ها گسترده شده‌است که آن را در معرض خطر قرار می‌دهد. رقیبان و مخالفان تلاش می کنند تا اطلاعات را به سرقت ببرند. این افراد می‌توانند شامل گروه های زیر باشند:

هکرهای سنتی که توانایی کشف و شناسایی سیستم را دارند یا افراد آنلاینی که برای تغییرات سیاسی یا اجتماعی اقدام به سرقت و تغییر در اطلاعات سیستم‌ها می کنند یا تبهکارانی که از این اطلاعات برای رسیدن به اهداف مالی استفاده می کنند و یا جاسوسان اجیر شده‌ای باشند که از آنها برای جست‌وجو و رصد این اطلاعات استفاده می‌شود. اگرچه این ابزارها و روش‌ها از نظر پیچیدگی به‌گونه‌ای هستند که به‌وسیله گروه‌های مختلفی به خدمت گرفته می‌شوند، اما همه این ابزارها بر ضعفی مبتنی هستند که در سیستم کامپیوتری وجود دارد؛ مثلاً فقدان وصله‌های نرم‌افزاری ضروری، کلمات عبور ضعیف، پیکربندی بد سیستم. تغییراتی که امروزه در سازمان‌ها و بعضی از نرم‌افزارهای تعبیه شده در آنها ایجاد می‌شود، کاملا به نفع هکرها خواهد بود که وظیفه آنها در گام نخست شناسایی آسیب‌پذیری سیستم است.

واژه «آسیب‌پذیر» در فرهنگ لغت انگلیسی آکسفورد «در معرض حمله یا خسارت قرار گرفتن» معنا شده‌است. روش کلاسیک در رصد آسیب‌پذیری یک سیستم به این گونه است که سیستم‌ها و برنامه‌های کاربردی موجود در

سیستم‌ها را در فواصل زمانی خاصی برای پیدا کردن ضعف امنیتی رصد می‌کند. این فواصل زمانی، ممکن است برای مثال به‌صورت اسکن‌های فصلی یا ماهانه باشد. مشکل این روش این است که رؤیت آسیب‌پذیری سازمان فقط در بازه‌های زمانی خاصی ممکن خواهدبود و اگر فرایند رصد با سایر فرایندهای موجود در داخل سازمان یکپارچه نشود در این‌صورت ممکن است امکان دسترسی به سیستم‌های جدیدی که به شبکه اضافه می‌شوند و نیز امکان شناسایی آسیب‌پذیری‌های جدید موجود در سیستم‌ها یا دیگر آیتم‌هایی که آسیب‌پذیری سیستم‌ها را نشان می‌دهد و نیاز به مدیریت آنها است، فراهم نشود.

یک برنامه مؤثر مدیریت آسیب‌پذیری باید به‌نحوی عمل کند که احتمال سیستم‌های در معرض خطر را کاهش دهد. این امر در مقایسه با سیستم‌های ساده رصد به چشم‌انداز جامع‌تری نیاز دارد تا نشان دهد که چگونه می‌توان آسیب‌پذیری‌های موجود را مدیریت کرد و عکس‌العمل شایسته‌ای در قبال نتایج داشت. آنچه لازم به نظر می‌رسد برنامه جامع مدیریت آسیب‌پذیری است که به‌طور محکم با سایر فرایندهای ضروری عملیاتی امنیت همچون هم‌زمان‌سازی فرایندها و ارتباطات سرتاسر گروه‌ها، مدیریت سرمایه، مدیریت پچ و پاسخ رویداد، ترکیب می‌شود.

شناخت ضعف‌های کلیدی و مهم

بسیاری از حوزه‌ها وجود دارد که می‌تواند سیستم‌ها را در معرض آسیب قرار دهد. برخی از این حوزه‌ها شامل موارد زیر هستند:

نرم‌افزار

تمام نرم‌افزارها، ذاتا دارای باگ‌هایی (خطاها) هستند. برخی از این باگ‌ها هرگز شناسایی نمی‌شوندو نرم‌افزار ممکن است به‌درستی کار کند، اما بعضی از آنها ممکن است موجب مشکلات عملکرد شوند. برخی باگ‌ها منجر به ضعف‌های امنیتی می‌شوند که اگر از این باگ‌ها بهره‌برداری شود، می‌تواند قابلیت اعتماد، صحت و درستی یا امکان دسترسی به محتویات آن نرم‌افزار یا اطلاعات موجود داخل آن را تحت‌تاثیر قرار دهد. اکثر فروشندگان مرتبا بسته‌های به‌روزرسانی را برای نرم‌افزارهایشان منتشر می‌کنند تا این باگ‌ها را تصحیح کنند. به‌روزرسانی نرم‌افزار با آخرین و جدیدترین بسته‌های آپدیت، یک عنصر کلیدی در تضمین امنیت سیستم‌ها است.

پیاده‌سازی و پیکربندی

گام دیگر در تضمین امنیت سیستم‌ها این است که پیاده‌سازی و پیکربندی صحیح سیستم‌ها تضمین شود. با این حال شاید برخی از سیستم‌ها به لحاظ امنیتی تنظیم نشده‌باشند یا پیکربندی آنها به‌خاطر فرایند نگهداری و عیب‌یابی سیستم که به‌طور پیوسته انجام می‌گیرد، تغییر کند. مشکلات پیاده‌سازی و پیکربندی همچون سرویس‌های امنیتی در حال اجرا، استفاده از کلمات عبور پیش‌فرض یا ضعیف یا فعال نبودن عملکردهای تشخیص‌دهنده روی یک سیستم تولیدی، ممکن است باعث تمام آسیب‌پذیری‌های امنیتی شود.

تغییر

طبیعت سیستم‌های رایانه‌ای پیشرفته این است که این سیستم‌ها مرتب تغییر می‌کنند. این تغییرات می‌تواند ناشی از فعالیت طراحی‌شده‌ای همچون یک به‌روزرسانی باشد که شامل بسته‌های نرم‌افزاری جدید برای کمک به روند عیب‌یابی مسائل موجود است. با این حال، اگر این تغییرات مدیریت نشوند، می‌توانند آسیب‌پذیری‌هایی را به محیط معرفی کنند. یک عنصر کلیدی در رسیدگی به این چالش‌های امنیتی در حقیقت توانایی توصیف کلی از حالت جاری این سیستم‌ها و تشخیص سریع و شناسایی هر نوع آسیب‌پذیری جدید است.

انسان

انسان یک عنصر کلیدی است که اغلب در تامین امنیت یک شبکه نادیده گرفته می‌شود. اکثر مردم به‌راحتی شاهد رایانه‌ها، برنامه‌های کاربردی و شبکه‌ها هستند که از آنها به‌عنوان ابزارهایی برای کمک و تسهیل انجام امور خود استفاده می‌کنند. با این حال، اگر مردم در استفاده درست و ایمن از سیستم‌ها به شکل صحیحی آموزش نبینند سیستم‌ها را در معرض تهدیدهای امنیتی قرار می‌دهند. مردم ممکن است از کلمات عبور ضعیف استفاده کنند، نرم‌افزار امنیتی خود را برای بهبود عملکرد رایانه‌هایشان غیرفعال کنند، نرم‌افزار را از یک منبع غیرمجاز

- استفاده از یک سیستم کنترل دسترسی به شبکه برای مدیریت دستگاه‌هایی که به شبکه متصل می‌شوند
- بررسی ثبت رخدادهایی که روی سرورهای DHCP در شبکه وجود دارد تا تعیین کند که به چه دستگاه‌هایی یک آدرس IP اختصاص داده شده‌است
- بررسی منظم ثبت رخدادهای سرور DNS ، دستگاه‌هایی را که منتظر ارتباط روی شبکه هستند شناسایی می کند
- نصب نماینده‌های اسکن آسیب‌پذیری روی داده‌ها و اسکن آنها و ارائه گزارش به یک مدیر مرکزی آسیب‌پذیری

۲) شناسایی آسیب‌پذیری

با آگاهی از اینکه چه آسیب‌پذیری‌هایی برای هر داده و اهمیت آن وجود دارد، می‌توان به بهترین نحو از آن داده محافظت کرد. ممکن است روی هر دستگاه و اطلاعاتی به‌خاطر فقدان پچ‌ها، نرم‌افزار قدیمی، کلمات عبور یا پیکربندی‌های ضعیف آسیب‌پذیری وجود داشته‌باشد. اینکه بهره‌برداری از این آسیب‌پذیری چقدر می‌تواند آسان باشد درجه و سطح آسیب‌پذیری را تعیین می کند. فهم درجه و سطح آسیب‌پذیری شناسایی‌شده، سازمان‌ها را قادر می‌سازد تا منابع مورد نیاز را برای حفاظت از داده‌ها بر اساس اولویت دسته‌بندی کند.

۳) آسیب‌پذیری سازگار

در بازه زمانی کوتاه، رصد آسیب‌پذیری فقط دید محدودی از موقعیت امنیتی بالقوه را فراهم می‌آورد. هر زمان که آسیب‌پذیری جدید که نتیجه باگ‌های نرم‌افزاری است معرفی می‌شود، دستگاه‌های جدیدی به شبکه اضافه می‌شوند یا تغییراتی که به سیستم‌ها اعمال می‌شود، تشخیص داده نخواهندشد و تا زمان انجام اسکن بعدی این سیستم‌ها همچنان در معرض خطر قرار دارند و آسیب‌پذیری‌ها شناسایی نمی‌شوند. چنان‌چه اسکن‌ها به اندازه کافی انجام نگیرد، همچنان تعداد زیادی از آسیب‌پذیری‌ها وجود خواهد داشت که بعد از هر اسکن شناسایی می‌شوند. در برخی از موارد، حجم کاملی از آسیب‌پذیری‌های کشف شده، می‌تواند هر اقدام و عمل جبرانی را از عمل باز دارد.

۴) ارزیابی ریسک

تمام دستگاه‌ها و اطلاعات به سطح یکسانی از امنیت نیاز ندارند. بسته به ارزش اطلاعات یک سازمان و اینکه چقدر این اطلاعات در معرض ریسک قرار دارد، گام‌هایی برای محافظت از آنها نیاز خواهدبود. ریسک اغلب به‌عنوان اثر یک حمله موجود، توصیف می‌شود که با احتمال رخداد و پیچیدگی موفقیت موازنه می‌شود. آسیب‌پذیری در حقیقت چیزی است که به حمله‌کننده اجازه می‌دهد تا یک ورودی را در یک محیط محافظت‌شده دیگری پیدا کند. یک کلمه عبور ضعیف احتمال ریسک را افزایش می‌دهد و اجازه دسترسی غیرمجاز به سیستم را می‌دهد. یک پچ گم شده بر روی یک سرور وب ریسک یک حمله‌کننده را که از آن آسیب‌پذیری استفاده می کند، افزایش می‌دهد تا دسترسی به سرور را به‌دست آورد. تصمیمات اتخاذ شده مدیریت ریسک بر سطوحی از ریسک که در مقابل اطلاعات قرار دارد به جزییات دقیق و به‌موقعی در مورد آسیب‌پذیری‌های موجود نیاز دارد. استفاده از یک روش مدیریت آسیب‌پذیری سازگار، داده‌هایی را فراهم می کند تا از یک فرایند مدیریت موثر ریسک حمایت کند.

۵) مدیریت تغییر

تغییرات دائما روی بسیاری از شبکه‌ها و سیستم‌ها رخ می‌دهد. نرم‌افزار به‌روزرسانی می‌شود، سخت‌افزار اضافه یا حذف می‌شود و برنامه‌های کاربردی دائما به‌روزرسانی می‌شوند. هر تغییری، این پتانسیل را دارد که مشکلات یا آسیب‌پذیری‌های جدیدی را معرفی کند. این آسیب‌پذیری‌ها می‌تواند امنیت سازمان را به مخاطره بیندازد. یکپارچه‌سازی مدیریت تغییر با یک فرایند مدیریت آسیب‌پذیری سازگار از مشکلات امنیتی بالقوه‌ای جلوگیری می کند که این مشکلات قبلا شناسایی و به آنها رسیدگی شده‌است.

۶. مدیریت وصله

یک برنامه مدیریت آسیب‌پذیری مؤثر باید به‌آرامی با وصله، یکپارچه‌سازی شده و فرایندهای مدیریت را پیاده‌سازی کند.

به‌روزرسانی نرم‌افزارها، مطابق با معیارهای سازمانی آنها برای سیستم‌ها و دارایی‌ها انجام می‌شود. بازخوردهای برنامه مدیریت وصله باید برای برنامه مدیریت آسیب‌پذیری به کار گرفته شود تا به‌واسطه این برنامه به آسیب‌پذیری‌ها پرداخته شود.

فراینـــد مدیریـــت وصله باید بـــا فرایند مدیریـــت تغییر، یکپارچه‌ســـازی شود تا انجام به‌روزرســـانی‌های نرم‌افزاری و نســـخه‌ها را در یک حالت کنترل‌شـــده‌ای تضمین کند. همچنین مهم اســـت که تضمین کند هرگونه به‌روزرسانی را در یک حالت صحیح و مشخصی انجام دهد.

۷. مدیریت دستگاه تلفن همراه

دســـتگاه‌های تلفن همراه، در حـــال حاضر بخش فراگیری از چشـــم‌انداز فناوری اطلاعات است که مدیریت ریسک و امنیت منحصربه‌فردی را تضمین می‌کند. دستگاه‌های تلفن همراه از روش‌های مدیریت انطباق و آســـیب‌پذیری سنتی و مالکیت مخلوط و مدل‌های کنترل (دســـتگاه‌های متعلق به شـــرکت در مقابل دســـتگاه‌های BYOD) که در سیاست اختلاف ایجاد می‌کند، دوری می‌کنند.

یکپارچه‌سازی با سیستم‌های مدیریت دستگاه تلفن همراه (MDM) یا فناوری درحال توســـعه مثل عوامل این امکان را به ســـازمان‌ها می‌دهد که دســـتگاه‌های تلفن همراه را به دارایی‌های معلوم خود اضافه کرده و به‌عنوان بخشی از برنامه مدیریت آسیب‌پذیری مدیریت کنند.

۸. مدیریت کاهش خطرات

یکی از عناصری که به‌عنوان بخشی از یک برنامه مدیریت آســـیب‌پذیری مؤثر نادیـــده گرفته می‌شـــود، چگونگی مدیریت آســـیب‌پذیری اتفاقاتی است که در به‌روزرسانی نرم‌افزار یا رســـیدگی به آســـیب‌پذیری‌های موجود است. همیشه از زمان کشف یک آسیب‌پذیری تا رفع دائمی آن، یـــک دوره زمانی وجود دارد؛ درنتیجه در مورد دارایی‌های یک سازمان، توافق می‌شود تا این آسیب‌پذیری رفع شود. یک برنامه مؤثر مدیریت آسیب‌پذیری، تا زمان رفع مشکل توســـط تأمین‌کننده، راه‌های جایگزیـــن را برای مدیریت مواجهـــه از قبیل تغییـــر قواعد دیوارآتـــش (firewall)، افزایـــش نظارت‌هـــای ورودی یا به‌روزرســـانی امضاهای دیجیتال در نظر می‌گیرد.

۹. پاسخ‌گویی به حادثه

امنیت سیستم‌های سازمانی فقط روی نحوه پاسخ‌گویی به نقض امنیتی تأثیر دارد. پاســـخ‌گویی ســـریع به یک حادثه امنیتی، اثر این حادثه را روی سازمان تا حدود زیادی کاهش می‌دهد. هرچند که بســـیاری از سازمان‌ها به پاسخ‌گویی به حادثه به چشم یک عملکرد که فقط درصورت نقض امنیت مورداستفاده قرار می‌گیرد، نگاه می‌کنند. چشم‌انداز تهدید مدرن نیاز به یک رویکرد پیشـــگیرانه‌تر برای پاسخ‌گویی به حوادث بالقوه و شناخته‌شده دارد.

کشف آسیب‌پذیری بحرانی به‌خودی‌خود به این معنا نیست که نقض امنیتی اتفاق افتاده‌اســـت، بلکه نشان می‌دهد که فرایند پاسخ‌گویی به حادثه هشدار می‌دهد که پاسخ‌گویی به حادثه می‌تواند مزایایی نیز داشته‌باشد و همچنین این اجازه را به گروه پاسخ‌گویی به حادثه می‌دهد که ابزارهای مناسب را در اختیار داشته‌باشند و نظارت بر امنیت را به‌منظور پاسخ مناســـب به کار ببرند. وقتی یک حادثـــه رخ می‌دهد، لازم است که فرایند مدیریت آسیب‌پذیری، یکپارچه‌سازی شود تا سیستم‌ها بتوانند آســـیب‌پذیری بالقوه را به‌عنوان نقطه بالقوه توافق، بپذیرند یا حذف کنند. به‌علاوه فرایند مدیریت آســـیب‌پذیری می‌تواند به گروه پاســـخ‌گویی به حادثه در شناخت آسیب‌پذیری‌های بالقوه‌ای یاری برساند که هکرها می‌توانند به‌عنوان اهرمی برای ورود به سیستم از آن استفاده کنند.

۱۰. اتوماسیون

کلیـــد نهایی بـــرای برنامه مدیریت آســـیب‌پذیری موفق، اتوماسیون اســـت. راه‌حل‌های امنیتی به‌عنوان وسیله‌ای برای توقف یا پیشـــگیری از نقض امنیتی مورداستفاده قرار می‌گیـــرد. هرچند درواقع این مســـئله به‌عنوان یک مورد بالقوه به شمار نمی‌رود. بسته به کسی یا چیزی که سیستم را هک می‌کند، راه‌حل‌های امنیتی مختلف ممکن اســـت، فرایند هک کردن را تســـریع کند یـــا اینکه آن را صرفاً به تأخیر بیندازد.

بنابرایـــن این راه‌حل‌ها، اهمیت بســـیار زیادی دارند. یکی دیگـــر از انگیزه‌های اســـتفاده از اتوماســـیون، این اســـت کـــه حجم اطلاعات موردنیاز به‌خوبی بررســـی و پردازش می‌شـــود. این مســـئله هم به اندازه و پیچیدگی محیطی بســـتگی دارد که آن را مدیریت می‌کنیم، اما بســـیاری از شـــبکه‌های بزرگ به‌صورت همواره دستگاه‌هایی را اضافه می‌کنند، تغییر می‌دهند و حذف می‌کنند.

پـــردازش دســـتی مقادیـــر زیـــادی از اطلاعات، بســـیار وقت‌گیر اســـت. همچنین در چنین پردازشی، احتمال خطا

نیز بالا می‌رود. دلیل نهایی و اصلی اســتفاده از اتوماسیون، کاهش نقش عنصر انســانی در فرایندهاست تا بدین‌وسیله ریسک حاصل از خطای انسانی را کاهش دهیم.

شـاخص‌های عملکـرد کلیـدی بـرای بهبـود مدیریـت آسیب‌پذیری

یک برنامه مؤثر برای مدیریت آســیب‌پذیری نیاز به مراقبت مداوم دارد. یک ضرب‌المثل معروف در مدیریت وجود دارد که می‌گوید شــما نمی‌توانید مسائلی را که قابل‌اندازه‌گیری نیســتند، مدیریــت کنید. ایــن ضرب‌المثــل در مواردی صادق اســت که داریم از یک برنامه مدیریت آسیب‌پذیری اســتفاده می‌کنیم. در درک میزان تأثیر این برنامه تا تعیین زمینه‌هایی که می‌توانند بهبود یابند، داشــتن چند شاخص عملکــرد کلیدی (KPIs) بــرای تأکید بر جاهایی که برنامه مدیریت آســیب‌پذیری قابل‌اجراســت، جاهایی قابل‌اجرا نیست و جاهایی که نیاز به تمرکز بر منابع و اقدامات است، موفقیت‌آمیز است.

جاهایــی از ســازمان که شــاخص‌های عملکــرد کلیدی (KPIs) در آنها قابل‌اجراســت بر اســاس تعداد مسائل مثل اندازه ســازمان، صنعت موجود، نوع سیستم مورداستفاده و منطقه‌ای که سیســتم در آن قرارگرفته، می‌تواند تا حدود زیادی تغییر کند.

برخــی از شــاخص‌های عملکرد کلیــدی (KPIs) که برای اندازه‌گیری و سنجش به کار می‌روند، عبارت‌اند از:

تعــداد آســیب‌پذیری‌ها بــه ازای هر فروشنده

این شــاخص عملکرد کلیدی (KPI) می‌تواند در شناسایی فروشــندگانی که ســابقه خوبی در تأمین راه‌حل‌های امن دارند، مفید و مؤثر واقع شود. یک فروشنده باید مقادیر بسیار زیادی از آســیب‌پذیری‌هایی را داشته‌باشد که نشان‌دهنده کنترل کیفیت در فرایندهای توســعه اســت. این اطلاعات در هنگام انتخاب راه‌حل‌های جدید فروشــنده‌ها می‌تواند مفید باشد. وقتی فروشــنده‌هایی که در سابقه خود، تعداد بســیار زیادی از آســیب‌پذیری‌هایی را دارند که مخصوصاً دارای ماهیت بحرانی هســتند، ممکن است ریسک بالاتری نســبت به فروشندگانی داشته باشــند که تعداد کمتری از آسیب‌پذیری را دارند.

تعداد آسیب‌پذیری‌ها به‌ازای هر محصول

ایــن شــاخص عملکــرد کلیــدی (KPI) می‌تواند در مواردی مفید واقع شــود که اکثر آســیب‌پذیری‌ها و انواع محصولات ناشــی از آن، غیرواقعی هستند. همچنین این شاخص برای تخصیص منابع مناسب در افزایش امنیت این محصولات نیز به‌کاربرده می‌شود. در تعیین جایگزین‌های مناسب برای محصولات موردنظر نیز این روش مفید و مؤثر است.

بالارفتن سن آسیب‌پذیری

این شاخص عملکرد کلیدی (KPI) را می‌توان برای ســنجش اثربخشی برنامه وصله مورداستفاده قرار داد. این KPI به‌صورت ایده‌آل، بیشــتر بر اســاس بحرانی بودن آســیب‌پذیری‌ها با مشکل مواجه می‌شــود. دانستن اینکه معمولاً اســتفاده از این وصله برای یک آسیب‌پذیری چقدر طول می‌کشد و اینکه در هنگام تعیین مواجهه یک سازمان با یک آســیب‌پذیری که جدیداً اعلام شده چه اقداماتی باید انجام داد به همین شاخص بستگی دارد.

درصد سیستم اسکن شده

شــبکه‌هایی که به‌موجب ماهیت‌شان دارای محیط‌های فراری هســتند و سیستم‌ها و دستگاه‌هایی که به‌طور مرتب از شــبکه قطع و وصل می‌شــوند جزء همین شاخص به شــمار می‌روند. وقتی یک بررسی آسیب‌پذیری انجام می‌شود هیچ تضمینی وجود ندارد که همه دستگاه‌ها بررســی شود. دانستن درصد املاک کامپیوتری سازمان که تحت بررســی بوده، می‌تواند به تعیین بررسی‌هایی که باید به‌طــور مرتب و در حالات مختلف، انجام شــود کمک کند. همچنین اگر وســایل جایگزین و مؤثرتری برای بررسی نیاز باشد باید از همان وسایل استفاده کرد.

تعداد آسیب‌پذیری‌ها در طول زمان

نظارت بر تعداد آسیب‌پذیری‌ها در طول زمان، یک شــاخص عملکرد کلیدی (KPI) مهم به شمار می‌رود. اگر تعداد آسیب‌پذیری‌هایی که به‌طور ایده‌آل در طول زمان تشــخیص داده می‌شــوند روندی نزولی داشته‌باشد، یعنی اینکه برنامه مدیریت آسیب‌پذیری درست کار می‌کند.

منبع: Tenable Network Security