هفتمین همایش سالانه بانکداری الکترونیک و نظام‌های پرداخت
نوآوری، بازیگران جدید و کارآیی در کسب وکار مالی
تهران، مرکز همایش‌های بین‌المللی برج میلاد – ۲و۳ بهمن ۱۳۹۶
7th Annual Conference on Electronic Banking and Payment Systems

ضرورت جمع‌آوری و نگهداری و نحوه بهره‌برداری از اطلاعات لاگ سیستم‌های حساس در سازمان‌های مالی

محمد دماوندی، کارشناس نظارت بر عملکرد شرکت‌های پرداخت شرکت شاپرک ، m.damavandi@shaparak.ir

چکیده (فارسی)

کلیدواژه: امنیت، پایش، شبکه پرداخت، مدیریت سوابق، بانک

امروزه امنیت در تمامی حوزه‌های کسب و کار اهمیت ویژه‌ای نسبت به پیش پیدا کرده است و با پیچیده‌تر شدن روش‌های سواستفاده از داده‌ها و اطلاعات سازمان‌ها، محافظ از دارایی‌های اطلاعاتی هر سازمان، حساس‌تر و دشوارتر شده است. بر همین اساس پایش مستمر وضعیت امنیت سازمان و بررسی رفتارهای منابع انسانی و عملکرد سامانه‌ها، نقشی حیاتی در این خصوص ایفا می‌کند. یکی از بنیادی‌ترین زیرساخت‌های لازم برای نیل به این هدف، استقرار سامانه جامع و بهینه جمع‌آوری و بررسی سوابق فعالیت منابع انسانی و نحوه عملکرد سامانه‌ها است. در این مقاله به ضرورت جمع‌آوری سوابق فعالیت‌ها و عملکردهای موجودیت‌های حیاتی در شرکت پرداخت و شبکه بانکی کشور پرداخته شده است و به سوالاتی همچون، جمع‌آوری چه فعالیتی و با چه جزییاتی را پاسخ داده شده است.

چکیده (انگلیسی)

Keywords: Security, Monitoring, Payment network, Bank, Log management

Security in all business areas has come to the fore, and with the complexity of the methods of data and information abuse, the protection of information assets of each organization has become more sensitive and difficult. Accordingly, the continuous monitoring of the organization's security status and the review of human resource behaviors and system performance plays a vital role in this regard. One of the most fundamental infrastructures required to achieve this goal is the establishment of a comprehensive and optimal system for collecting and reviewing the Logs of human resources activities and systems functionality. In this article, the necessity of collecting the Logs of activities and functionalities of vital entities in the organizations and the banking network of the country has been addressed and asked questions such as, collection, what activity and with what details have been answered.

مقدمه

یکی از کلیدی‌ترین اصول در هر طرح امنیت اطلاعات، پیاده‌سازی مفاهیم «دفاع در عمق[1]» است. دفاع در عمق در واقع یک استراتژی تاکتیکی، برای پیشگیری از دست رفتن اطلاعات و به خطر افتادن دارایی‌های اطلاعاتی است که به واسطه پیاده‌سازی لایه‌های مختلف به صورت هم‌پوشانی شده متشکل از سطوح چندگانه محافظتی است. در این روش، نقصان در یک لایه دفاعی، خللی در عملکرد کل سیستم دفاعی، ایجاد نمی‌کند.

هر استراتژی دفاع در عمق، معمولا شامل ترکیبی از تدابیر امنیتی در حوزه‌های پیشگیری، کشف و اصلاح است. ابتدایی‌ترین نمونه از دفاع در عمق را در اعصار گذشته و در ساخت دژ به عنوان تدبیر «پیشگرانه»، نگهبانان بالای برج مراقبت به منظور «کشف»، می‌توان مشاهده کرد. هرچند به کارگیری این استراتژی هزاران سال است که به اثبات رسیده، درسی که از مطالعه تاریخ می‌تواند گرفت، تکامل پیوسته روش‌های حمله و مهاجمان است. در مواقعی، دشمنان، قابلیت غلبه را به گونه‌ای پیشرفت می‌دهند که دیگر هیچ تدبیر دفاعی، کارساز نباشد. توانایی «کشف» سریع و به موقع چنین رویدادها و تطبیق تاکتیک‌های دفاعی متقابل، از مهمترین عوامل در حفاظت مستمر دارایی‌ها محسوب می‌شود. موفقیت در کشف تکنیک‌های حمله تکاملی مبنتی بر قابلیت بینش اجرایی[2] است. دارا بودن بینش اجرایی، مستلزم پایش مستمر لایه‌های دفاعی امنیتی و «وضعیت» دارایی‌هاست. هرگز، داشتن دژی مستحکم برای مقابله با مهاجمان بدون وجود نگهبانان، میسر نبوده و نخواهد بود. اگر پدافندهای امنیتی به صورت مستمر پایش نشوند، چگونه می‌تواند پی به وجود نقص و رخنه مهاجمان برد؟ قطعا صرفا بررسی حضور دارایی دیگر کافی نیست، مخصوصا در عصری که کپی یک دارای به اندازه خود دارایی ارزشمند است و اگر از دست دادن کپی آن بیش از خود دارایی ارزش نداشته باشد، کم‌تر از آن نیز نیست.

تدابیر کشف در سیستم‌های اطلاعاتی

از زمان پیدایش کامپیوترهای الکترونیکی مدرن، مفهوم دفاع در عمق با محافظت از سیستم‌های اطلاعاتی گره خورده است. هنوز هم مساله تاریخی دارایی‌ها برای مهاجمان امروزی صادق است و روش‌ها همواره برای غلبه بر پدافندهای امنیتیِ سیستم‌های اطلاعاتی، در حال فرگشت هستند. خوشبختانه در دنیای امروز، قابلیت کشف تقریبا در تمامی سیستم‌های اطلاعاتی به صورت پیش‌فرض به واسطه پیاده‌سازی مکانیزم‌های ثبت سوابق[3]، در نظر گرفته شده است و این امکان، بینش کافی اجرایی را برای مقابله مورد نیاز با روش‌های حمله تکامل‌یافته، به سازمان می‌دهد.

عملکرد ثبت سوابق معمولا به واسطه سیستم‌عامل، تجهیزات شبکه و نرم‌افزارها، فراهم می‌شود. این موجودیت‌ها در زمان وقوع رخدادی مشخص، پیام کامپیوتری را تولید می‌کند. این پیام‌ها در قالب مفهوم کلی «سوابق» جمع‌آوری می‌شوند و رخدادهای زیادی را شامل شود؛ رخدادهایی همچون استفاده از منبعی از سیستم، تغییر وضعیت سیستم و سایر موارد. سوابق منابع بسیار ارزشمند اطلاعاتی محسوب می‌شوند چرا که در سیستم‌های اطلاعاتی، به توالی زمانی رخدادها و فعالیت‌هایی که به موقع می‌پیوندد، اشاره دارد.

---

[1] Defense in Depth
[2] Actionable Intelligence
[3] Log

در اصل این سوابق برای مصارف رفع اشکال و بهینه‌سازی ایجاد شدند و به گونه‌ای تکامل یافت تا در عمل به مهم‌ترین منبع اطلاعاتی در خصوص رخدادهای امنیتی سیستم اطلاعاتی تبدیل شدند. تلاش‌های ورود به سیستم، دسترسی به فایل یا داده‌ها، تغییر در سیاست‌های امنیتی و تغییر در حساب کاربری، نمونه‌هایی از این رخدادها محسوب می‌شود. به علت فراگیر شدن سرورهای شبکه، پایانه‌های کاری و سایر تجهیزات محاسباتی و همچنین افزایش روزافزون تهدیدات شبکه و سیستم‌ها، اساسا تعداد، حجم و تنوع سوابق، به طور چشم‌گیری افزایش یافته است[۴]. این موارد، برای سازمان‌ها اطلاعات بسیار گران‌بهایی را در خصوص وضعیت و کارایی تدابیر امنیت اطلاعات به منظور حفاظت از سیستم‌های اطلاعاتی سازمان فراهم می‌کند.

لزوم پایش سوابق

داشتن سوابق امنیتی و بهره‌گیری فعالانه از آنها به منظور پایش فعالیت‌های امنیتی در سازمان، دو موضوع کاملا متفاوت است. پرواضح است که چه تفاوت‌های بنیادی با هم دارند اما بسیاری از سازمان‌ها میان این دو سردرگم هستند. جمع‌آوری و ثبت سوابق پیام‌ها و رویدادها در سوابق امنیتی، ممکن– و البته الزامی – است تا در تحقیقات پس از رخنه، به فواید آن پی برد. اما در مقابل ثبت و جمع‌آوری سوابق بدون هیچ روالی برای بازبینی و تحلیل فعالانه آنها، تنها یک عنصر کوچک در پدافند و مدیریت مستمر امنیت اطلاعات محسوب می‌شود و در واقع بنا کردن دژی بدون نگهبان در عصر حاضر محسوب می‌شود. به منظور ثمربخشی هر چه بیشتر بهره‌گیری از سوابق امنیتی در محافظ از دارایی‌های اطلاعاتی، این سوابق باید پایش و تحلیل شوند به گونه‌ای که این فرایند تا حد امکان به صورت لحظه‌ای صورت پذیرد تا حملات در اسرع وقت شناسایی شود و اقدامات مقتضی برای تقویت پدافندهای موجود در زمان و مکان لازم، به کار گرفته شود. این روال، با پیچیده‌تر شدن حملات و مهاجمان، روز به روز از همیت بیشتری برخوردار می‌شود. بدون پایش و تحلیل فعال سوابق امنیتی، با کهولت پدافندهای امنیت اطلاعات به واسطه توانمندی روزافزون مهاجمان، عملا سازمان بی‌دفاع می‌شود و با از دست رفتن قابلیت کشف حملات، دقیقا همان دارایی‌های ارزشمندی که باید محافظت شوند، مورد حمله قرار می‌گیرند.

چالش‌های پایش سوابق

پیشرفت‌های فناوری باعث بهبود مهارت افراد کژاندیش شده است. با پیچیده‌تر و افزایش سرعت حملات و مهاجمان، ارتقای دانش و مهارت مدیران و کارشناسان امنیتی در نگهداشت و بهبود تدابیر امنیتی در محافظت از دارایی‌های اطلاعات، بیش از پیش حیاتی شده است که شامل ارتقای مهارت در کشف حملات و نقصان‌های امنیتی «پیش» از تبدیل آن به رخنه و رخداد امنیتی در سازمان شود. متاسفانه براساس داده‌های آماری بدست آمده، واحدهای امنیت هنوز به توانمندی لازم نرسیده‌اند، چرا که متوسط زمان میان رخنه در سیستم‌ها و کشف آن بین چندین هفته و چندین ماه اعلام شده است در صورتی که باید حداکثر طی چندساعت و چند روز تشخیص داده شود[۵]. این وضعیت با فراگیر شدن آسیب‌پذیری‌هایی که در سیستم‌های اطلاعاتی و چالش‌های به‌روزرسانی و نصب وصله‌های امنیتی به مراتب بغرنج‌تر می‌شود. ابزارهای زیادی برای انجام فعالیت‌های

[۴] براساس مقاله NIST با عنوان «راهنمای مدیریت سوابق امنیتی سیستم‌ها»

[5] https://www.ponemon.org/blog/2015-cost-of-data-breach-global

مرتبط با امنیت وجود دارد اما در سازمان‌ها برای اموری همچون مدیریت آسیب‌پذیری نسبت به پایش سوابق، اهمیت بیشتری را در نظر می‌گیرند[۶].

همچنین تعداد سیستم‌هایی که در حال تولید سوابق هستند به سرعت رو به افزایش است. بهره‌گیری روزافزون از فناوری‌های مجازی‌سازی و ضرورت مقیاس‌پذیری منابع پردازشی بسیاری از سازمان‌ها را قادر به یکپارچه‌سازی بیش از پیش سیستم‌ها و نرم‌افزارها در قالب معماری‌های کوچک‌تر سخت‌افزار می‌کنند. در جایی که قبلا محدودیت فیزیکی برای محل نگهداری اطلاعات وجود داشت، مجازی‌سازی – یا در عمل خدمات ابر محور – این مساله را از پایه حل کرده است. افزایش چگالی سیستم‌ها، رشد نمایی حجم داده‌های سوابق را نیز به همراه داشته است. همین عامل، فشار قابل توجهی را بر گروه‌های امنیتی به منظور پردازش سریع حجم عظیمی از اطلاعات بدون افزایش منابع برای تسهیل این فعالیت، وارد کرده است. به علاوه معمولا زبان مشترکی برای سوابق وجود ندارد. استاندارد جهانی برای ساختار یا قالب داده‌های سوابق وجود ندارد و سوابق به اشکال و قالب‌های گوناگونی وجود دارند. برخی از تجهیزات و سیستم‌ها به زبان خوانا در قابل فایل متن، سوابق را تولید می‌کنند در حالی که سایر سیستم‌ها سوابق را در قالب زبان ماشین یا درون پایگاه‌داده‌ها، تولید می‌کنند. برخی دیگر نیز قالب اختصاصی خود را در تولید داده‌های سوابق در نظر می‌گیرند. و البته رویکرد مشابهی نیز در تفیسر و تولید اطلاعات رویدادها برای ذخیره سوابق وجود ندارد. ممکن است رویدادی مشابه به روش‌های متفاوت در سیستم‌های مختلف تفیسر و تولید شوند.

همانگونه که پیشتر اشاره شد، همه این عوامل، وظایف سنگین و قابل توجهی را برای فعالان عرصه امنیت به همراه دارد. تعجبی ندارد که با وجود چنین سربارهایی برای پایش و تحلیل سوابق و در مقابل محدودیت منابع، بسیاری از سازمان‌ها مزایای پایش فعال سوابق امنیت، صرفه اقتصادی ندارد و به سادگی منابع مورد نیاز را در جایی دیگر صرف می‌کنند. در صورتی که برای کارایی بیشتر در حوزه پایش سوابق، سازمان‌ها باید رهیافتی ساخت‌یافته برای تولید، انتقال، ذخیره و تحلیل در بهینه‌ترین حالت ممکن داشته باشند. همچنین فرآیند مدیریت سوابق نیز باید همسو با استراتژی مدیریت ریسک سازمان باشد تا منابعی که به صورت کارآمد و به بودجه به صورت بهینه، تخصیص داده شود. این رهیافت باید براساس ماموریت کسب و کاری سازمان تدوین شود و همراستا با فرهنگ و فناوری مختص همان سازمان باشد.

گذری بر الزامات امنیت صنعت پرداخت

براساس استاندارد و مرجع بین‌اللملی در زمینه امنیت شبکه پرداخت، «PCI DSS» و سند «الزامات امنیت شاپرک»، سوابق سیستم‌های دامنه پرداخت باید به صورت مستمر پایش شود. در کنترل ۱۰٫۶ از الزامات PCI DSS و ۲٫۵ الزامات امنیت شاپرک، بر پایش مستمر سوابق تاکید شده است. در این بخش از مقاله به تشریح هدف و نحوه پایش سوابق پرداخته شده است.

این استانداردها و الزامات با هدف دفاع در عمق، شامل اقدامات پیشگیرانه، تشخیصی و اصلاحی تدوین و ابلاغ شده است و علاوه بر بیان رهنمون برای حفظ دارایی‌ها، تلاش برای ارتقا شرکت و سازمان برای بروز رفتارهای عاملانه در پایش و پیشگیری از روخدادهای امنیتی را در دستور کار دارند.

[6] https://www.blackhat.com/docs/webcast/04162015-enterprise-defense-onapsis.pdf

برای درک بهتر الزامات امنیت در این حوزه ابتدا کنترل ۱۰٫۶ الزامات PCI DSS مرور می‌شود.

در کنترل ۱۰٫۶ بیان شده است:

> *تمامی سوابق و رخدادهای امنیتی همه «اجزای شبکه پرداخت[۷]» به منظور کشف فعالیت‌های نامتعارف و مشکوک بررسی شود.*

این کنترل متشکل از سه زیرکنترل است که نحوه انطباق با این کنترل را تشریح می‌کند:

- ۱۰٫۶٫۱ «*پایش روزانه*» فعالیت‌های زیر:
  - تمامی «*رخدادهای امنیتی*»
  - سوابق تمامی اجزای شبکه پرداخت که اطلاعات دارندگان کارت یا اطلاعات حساس کارت را «ذخیره»، «پردازش» و «انتقال» می‌دهند
  - سوابق تمامی «*اجزای حیاتی شبکه پرداخت*»
  - سوابق تمامی اجزای شبکه پرداخت که عملکرد و ماهیت امنیتی دارند (مانند دیواره آتش، IPS/IDS، سرورهای احراز هویت، سرورهای کسب و کار و سایر موارد)
- ۱۰٫۶٫۲ بررسی دوره‌ای سوابق تمامی اجزای شبکه پرداخت براساس سیاست‌ها و استراتژی مدیریت ریسک سازمان که با توجه به ارزیابی مخاطرات سالانه، مشخص شده است.
- پیگیری خطاها و رفتارهای نامتعارفی که در فرایند بررسی کشف شده است.

به منظور درک هر چه بهتر، مفهوم و کاربرد برخی از کلیدواژه‌ها باید شفاف شود.

پایش روزانه

اگر برای مدیریت امنیت، این آگاهی وجود داشته باشد که مخاطرات، حملات، مهاجمان شب و روز، تعطیلی و عید را نمی‌شناسند، رویکرد مناسبی برای پردافندهای عاملانه انتخاب می‌شود. پایش روزانه نه به روز کاری و نه روز تقویم اشاره دارد. بلکه در تلاش برای هرچه نزدیک‌تر شدن بررسی‌ها به زمان لحظه‌ای است که تا قبل از آن که نفوذ به نقض امنیتی تبدیل شود، جلوگیری شود. از آنجایی که ممکن است سازمان‌ها منابع کافی برای پایش و پردازش لحظه‌ای را نداشته باشند، PCI DSS این زمان را حداکثر ۲۴ ساعت یا یک روز در نظر گرفته است.

رخداد امنیتی

رخداد امنیتی، رخدادی است که از نظر سازمان دارای پیامدهای امنیتی بالقوه برای سیستم‌ها و محیط باشد. در صنعت پرداخت این رخداد به شناسایی فعالیت‌های مشکوک و نامتعارف اطلاق می‌شود. نه عنوان نمونه به مواردی همچون تلاش برای ورود با حساب کاربری جعلی، ورود مکرر گذرواژه نادرست، توقف یا خاموش شدن سرویس‌های حیاتی، می‌توان اشاره کرد. نکته بسیار مهم در این زمینه تعریف و تبیین انواع رخدادها براساس هر محیط است و سازمان‌ها باید پیش از هر اقدامی، این

[۷] در متن سند الزامات PCI DSS این عبارت به عنوان System Components آورده شده است.

گونه رخدادها برای محیط خود مشخص کنند. هر قدر سازمان سرمایه‌گذاری بیشتری برای تعریف و شفاف‌سازی منظور خود از رخداد امنیتی در نظر بگیرد، مدیریت امنیت سازمان نیز به همین میزان افزایش می‌یابد. در کنترل ۱۰،۲ الزامات PCI DSS، به برخی از رخدادهای امنیتی اشاره شده است.

اجزای شبکه پرداخت

همواره باید در نظر داشت که هر سیستم یا نظام اطلاعاتی متشکل از اجزایی که هر یک نقشی در این سیستم را ایفا می‌کند. در این مقاله، سیستم اطلاعاتی، به شبکه پرداخت هر سازمان ارایه‌دهنده خدمات پرداخت اطلاق می‌شود و اجزای آن نیز هر دارایی فیزیکی یا غیرفیزیکی محسوب می‌شود. این اجزا می‌توانند سرور یا تجهیزات شبکه یا حتی نرم‌افزارها را نیز شامل شود که به نحوی به اطلاعات دارنده کارت یا اطلاعات حساس کارت دسترسی یا عملکرد و ماهیت امنیتی دارند.

متاسفانه بسیاری از شرکت‌های نرم‌افزارها و دارایی‌های منطقی را در نظر نگرفته و دچار ضعف‌هایی می‌شوند که از تا مدت‌ها از وجود آنها بی‌خبر خواهد بود و پس وقوع رخداد امنیتی (در صورت مدیریت صحیح) ممکن است به وجود آن پی ببرند. از این دسته نرم‌افزارها می‌تواند به مواردی همچون، سوییچ پرداخت، کنسول‌های مدیریتی، hypervisorها، آنتی‌ویرس‌ها و سایر نرم‌افزارهای خاص هر سازمان در محیط اطلاعات دارندگان کارت[۸]، اشاره کرد. درصورت تعریف صحیح دامنه اجرا در شبکه پرداخت، می‌توان این اجزا را شناسایی کرد.

اجزای حیاتی شبکه پرداخت

اجزای حیاتی، دارایی‌هایی محسوب می‌شوند که نقشی انکارناپذیر در عملیات یا امنیت ایفا می‌کنند و به خطر افتادن آنها اثر و تبعات چشم‌گیری به همراه دارد. این پیامدهای ممکن است مالی یا خدشه در اعتبار نیز باشد. همراستا با تعریف و تبیین رخدادهای امنیتی سازمان، معرفی اجزای حیاتی نیز فرایندی حیاتی در مدیریت امنیت سازمان محسوب می‌شود.

بررسی سوابق

براساس آنچه در سند الزامات امنیت PCI DSS بیان شده است، این زمان ۲۴ ساعته به منظور حفظ انطباق سازمان‌ها با منابع کم‌تر در نظر گرفته شده است. بنابراین مفهوم بازبینی و بررسی سوابق به معنی انجام آن به صورت دستی نیست و این بررسی می‌تواند توسط ابزارهای مختلف تجاری یا متن‌باز صورت پذیرد و عملیات بررسی را تسهیل کند. بر همین اساس در کنترل ۱۰،۶ جمع‌آوری، پالایش و اخطار را برای حفظ انطباق توصیه کرده است.

کنترل ۱۰،۶،۳ اگر مهم‌ترین بند الزامات نباشد قطعا یکی از مهم‌ترین کنترل‌های امنیتی برای حفظ امنیت است.

چگونگی پایش

با توجه به مفاهیمی که تا کنون بررسی شد، عناصر پایه‌ای بود که در فرآیند پایش لازم است تا مدیریت امنیت را برای محافظت از دارایی‌های سازمان یاری کند. آن چه در استانداردها و الزامات مطرح می‌شود، ضرورت پایش است و به صورت کلی به مفاهیم اشاره دارد. اما آن چه در پس این کنترل نهفته است و در بخش‌های مختلف به آن به صورت ضمنی اشاره شده است، چگونگی پایش و نحوه رسیدگی به حوادث است. برای انجام هرچه بهتر چگونگی پایش و برنامه‌ریزی برای آن، درک دو

[8] Cardholder Data Environment (CDE)

مفهوم پایه‌ای بسیار مهم است؛ داده‌های رویداد و داده‌های وضعیت. این مفاهیم نه تنها مدیریت امنیت سازمان را تسهیل می‌کند بلکه در انتخاب محصول و ابزار پایش نیز کمک شایانی می‌کند.

متاسفانه معمولا راه‌کارها تمرکز خود را برای حل مساله از دست داده‌اند و حفظ انطباق را ارجح بر حفظ امنیت می‌دانند و معمولا سعی دارند تا انطباق خود با الزامات امنیت را نمایش دهند اما نباید فراموش شود که هدف اصلی ایجاد فضای امن و حفظ انطباق است. هنگامی که سخن از قابلیت پایش[9] فعالیت‌ها سازمان به میان می‌آید، دو راه‌کار در صدر جدولی است: مدیریت امنیت اطلاعات و رخدادها (SIEM[10]) و مدیریت سوابق[11]. این دو راه‌کار برای پایش آنچه در سازمان و شبکه آن درحال وقوع است بسیار حیاتی است و نقش مهمی در قابلیت پایش ایفا می‌کند.

نکته مهم درک تفاوت این دو در دنیای فناوری اطلاعات است. تفاوت ساده‌ای وجود دارد. این تفاوت در نوع داده‌ها[12] نهفته است؛ درواقع درک تفاوت میان این دو راه‌کار، درک منابعی است که از آنها جمع‌آوری داده‌ها صورت می‌پذیرد و در حال پایش هستند.

به صورت کلی داده‌هایی را که هر یک از این راه‌کارها جمع‌آوری می‌کنند را می‌توان به دو دسته مجزا، طبقه‌بندی کرد:

1. داده‌هایی که رخدادی را تشریح می‌کنند یا
2. داده‌هایی که وضعیت یک سیستم را در شبکه بیان می‌کنند.

داده‌های رخداد

داده‌های رخداد[13]، داده‌هایی است که به شرح رویدادی در شبکه می‌پردازد. سیستم‌های شبکه به گونه‌ای پیکربندی می‌شوند که قابلیت رهگیری فعالیت‌ها در قالب سوابق[14] رویدادها، نگهداری شوند. برای نمونه، هرگاه فردی بر روی دامنه‌ای احراز هویت هویت شود، رکورد متناظر آن ثبت می‌شود. داده‌هایی همچون آدرس شبکه‌ای[15] مبدا، آدرس شبکه‌ای مقصد، نام کاربری، شرح رویداد، شناسه رویداد[16]، پیام و نتیجه فعالیت به همراه این رکورد نگهداری می‌شود. همچنین احراز هویت‌های ناموفق نیز به همراه داده‌های بسیاری از سایر انواع داده‌های رخداد، ذخیره می‌شود.

عمل مشترکی که هم سامانه مدیریت سوابق[17] و هم سامانه مدیریت امنیت اطلاعات و رخدادها انجام می‌دهند، جمع‌آوری و نگهداری داده‌های رخداد از هزاران تجهیز و سیستم در شبکه است. در واقع یکی از مهم‌ترین عوامل در فرایند تامین یا تهیه این راه‌کارها، حصول اطمینان از قابلیت جمع‌آوری این گونه داده‌ها است.

---

[9] Visibility
[10] Security Information and Event Management
[11] Log Management
[12] Data Type
[13] Event Data
[14] Log
[15] IP
[16] Event ID
[17] Log Management Solution

وضعیت هر یک از اجزای شبکه پرداخت

اگر هر دو راه‌کار اقدام به جمع‌آوری داده‌های رخداد می‌کنند، پس تفاوت در چیست و چگونه می‌توان محصولات مختلف را از هم تمیز داد؟ پاسخ به این سوال در جواب سوالی ساده پنهان شده است: آیا محصول/راه‌کار مورد نظر، داده‌های وضعیت[18] را نیز جمع‌آوری می‌کند؟

قابلیت جمع‌آوری داده‌ها بیش از داده‌های رخداد، نکته متمایزکننده راه‌های مدیریت سوابق و SIEM محسوب می‌شود.

داده‌های وضعیت

داده‌های وضعیت، داده‌هایی است که وضعیت یک رخداد را بیان می‌کند. نحوه پیکربندی، برنامه‌های نصب شده، کاربران، منابع به اشتراک گذاشته شده، پروسس‌ها، پیکربندی جاری، تنظیمات رجیستری، ACLها، آسیب‌پذیری‌ها و مواردی از این دست، در قالب وضعیت یک سیستم بیان می‌شود. با دانستن این ویژگی‌های کلیدی درباره هر دارایی، درک کاملی از وضعیت سیستم به دست می‌آید.

با مرور مجدد یک رخداد به همراه داده‌های نگهداری شده و تعریف داده‌های رخداد و داده‌های وضعیت، داده‌های وضعیت تنها جزییات رخداد را بیان می‌کند. هیچ اطلاعات دیگری از سیستم که سوابق از آن بدست آمده، وجود ندارد چرا که داده‌های وضعیت در این رکورد وجود ندارد.

اهمیت داده‌های وضعیت

همواره اهمیت جمع‌آوری، پایش و بازبینی داده‌های سوابق ممیزی، آموزش داده می‌شود. استانداردهای معتبر بین‌اللملی همچون NIST 800-53، DoD 8500.2، PCI، ISO 17799، SANS Critical Controls، الزامات امنیت شاپرک و مواردی از این دست، برای این حوزه از امنیت اطلاعات، الزام‌آور است. چرا که نکته حیاتی، در هنگام حملات، آگاهی از وضعیت جاری محیط و شبکه سازمان است. با این حال، همزمان با اهمیت پایش مستمر داده‌های رخداد، همواره این سوال باید پرسیده شود که: «آیا پایش مستمر داده‌های رخداد، امنیت سازمان را به حد مورد نظر می‌رساند؟». متاسفانه به احتمال زیاد پاسخ منفی است. اگر چه هرگز در امنیت راه‌کار طلایی وجود ندارد اما داشتن درک صحیحی از نحوه ارتقای آگاهی سایبری، بسیار حائز اهمیت است. بر همین اساس ترکیب بازبینی داده‌های وضعیت به همراه داده‌های رخداد، امنیت را به سطحی بالاتر ارتقا می‌دهد. ***به واسطه تحلیل داده‌های وضعیت، درک کاملی از حواشی رویداد، به دست آورده می‌شود***. برای مثال، زنجیره‌ای از احراز هویت‌های ناموفق هنگامی ارزشمند است که به دنبال آنها، احراز هویت موفق صورت گرفته است و همه این داده‌ها حاکی از تغییری در وضعیت سرور است.

در بررسی روزانه سوابق، شایسته است داده‌های وضعیت در اختیار تحلیلگران گذاشته شود تا به منظور استخراج مفاهیم و علل وقوع از میان هزاران رخداد روزانه، استفاده شود. علاوه بر این مزیت، گردآوری داده‌های وضعیت، منافع دیگری نیز به ارمغان می‌آورد. جمع‌آوری و تحلیل این داده‌ها می‌تواند به سازمان کمک می‌کند تا درک عمیق‌تری از وضعیت و پیکربندی متناسب

[18] Status Data

سیستم‌های شبکه براساس استانداردهای مشخصی همچون، DISA STIG[19]، USGCB[20] و CIS بدست آورد. کلمه کلیدی در جمله قبل، می‌تواند است. چرا که دو اتفاق باید رخ دهد تا بتوان تشخیص داد که سیستم یا تجهیزی، درست پیکربندی شده است. اول، وضعیت سیستم باید جمع‌آوری شود. دوم، که گام بزرگی است، داده‌هایی که وضعیت سیستم را تشریح می‌کنند باید به اطلاعات انطباق[21]، تبدیل شود. در مقام سخن، ساده به نظر می‌رسد اما در عمل بسی دشواری‌ها دارد. برای مثال به منظور حفظ انطباق با استاندارد DISA STIG برای ویندوز سرور ۲۰۰۸، مدیر سیستم می‌تواند کنسول مدیریت پیکربندی ویندوز را باز کند (MS SCOM یا SCCM) و نمای کاملی از پیکربندی را پیش روی خود ببیند. این ابزار اجازه می‌دهد تا مدت زمان قفل شدن حساب کاربری، وصله‌های نصب شده، سرویس‌های جاری و سایر موارد را بررسی کرد. آنچه از دیده پنهان است، انطباق این مدت زمان قفل شدن حساب کاربری با مجموعه استانداردهای DISA STIG است. در این میان باید امکانی وجود داشته باشد تا داده‌های پیکربندی را به منظور تایید انطباق، به داده‌های انطباق ترجمه کند. به این عمل «گام آخر انطباق» گفته می‌شود. ابزارهای بسیاری برای تشریح داده‌های وضعیت وجود دارد اما تعداد کمی از آنها واقعا توانایی ترجمه این داده‌های پیکربندی به داده‌های بامعنای انطباق را دارا هستند.

تا این مرحله به نکات زیر پوشش داده شده است:

- تمامی SIEM و ابزارهای مدیریت لاگ، نظر به داده‌های رخداد دارند.
- داده‌های رخداد، داده‌هایی است که وقوع یک اتفاق را بیان می‌کند؛ مثلا ورود موفقیت‌آمیز.
- داده‌های وضعیت، داده‌هایی است که وضعیت هر سیستم را به صورت کامل بیان می‌کند که می‌تواند شامل و نه محدود به این موارد باشد:
  - تنظیمات رجیستری
  - وصله‌های نصب شده
  - کاربران
  - پیکربندی‌های جاری سیستم
  - دسترسی‌ها
  - سایر
- برای ارتقای بینش سایبری، ترکیب داده‌های وضعیت با گروه تحلیل، مفاهیم و فراست بیشتری را نسبت به فضای حاکم سازمان ارایه می‌کند.
- داده‌های وضعیت می‌تواند به اطلاعات انطباق منتهی شود به شرطی که این داده‌های جمع‌آوری شده به اطلاعات انطباق، ترجمه شود.

[19] Security Technical Implementation Guides [https://iase.disa.mil/stigs/Pages/index.aspx]
[20] U.S Government Configuration Baseline [https://usgcb.nist.gov]
[21] Compliance Data

نحوه تشخیص ابزار مناسب

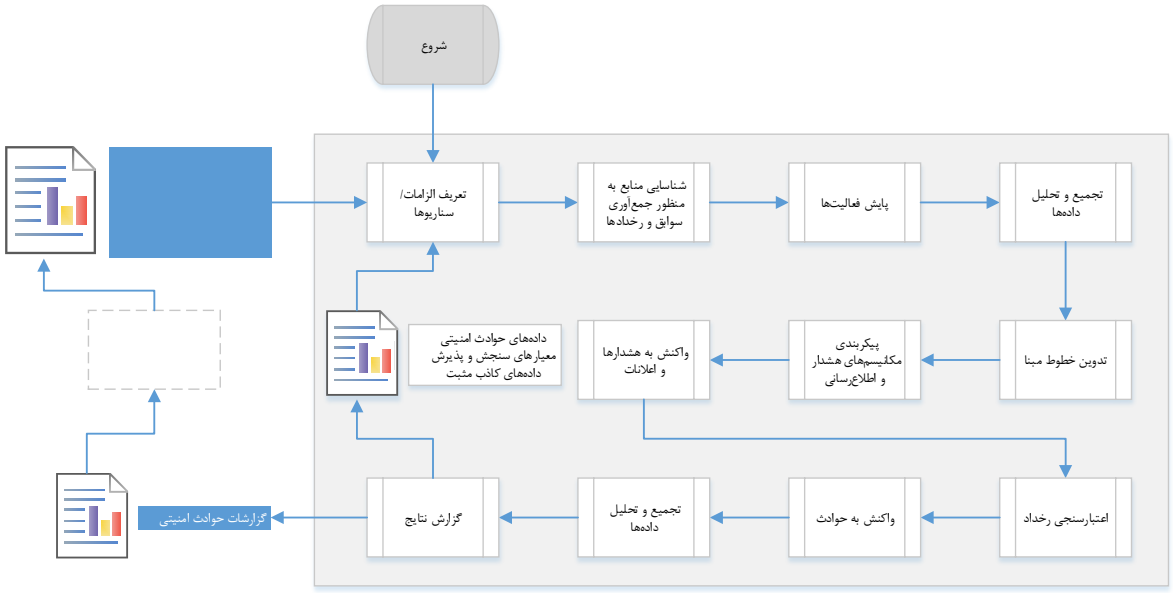
ابتدا می‌توان فهرست بلندبالایی از نیازمندی‌ها را مجتمع کرد و با ارزیابی تک‌تک راه‌کارهای بازار و پوشش امکانات محصولات موجود، به همراه تحقیق و مطالعه، تعدد راه‌کارها را برای انتخاب، محدود کرد. در نهایت مشخص می‌شود که تقریبا اکثر موارد فهرست شده، در همان وهله اول، هسته مدیریت سوابق در سیستم مدیریت امنیت اطلاعات و رخدادها، برای همه مشترک است. اگر در عمل تفاوتی هم بین تمامی این راه‌کارها وجود داشته باشد، تا زمانی که سوالات درست و بجا پرسیده نشود، این وجوه تمایز، آشکار نمی‌شود و در ظاهر هیچ تفاوت پایه‌ای و بنیادی وجود نخواهد داشت.

بهتر است بجای صرف ساعت‌ها تحقیق طاقت‌فرسا و حضور در جلسات بازاریابی تامین‌کنندگان، فقط با طرح سوالی با پاسخ ساده شروع کرد: »راه‌کار مورد نظر چه داده‌هایی را از دستگاه‌ها، سیستم‌ها و تجهیزات شبکه سازمان، جمع‌آوری می‌کند؟« پاسخی سرراست ممکن است به این صورت باشد که: «محصول ما داده‌های پیکربندی، کارایی، آسیب‌پذیری و جریان داده‌ها را از تمامی دستگاه‌ها جمع‌آوری می‌کند». به منظور شفافیت بیشتر نیز می‌توان پرسید: «آیا محصول مورد نظر می‌تواند وضعیت کامل پیکربندی سیستمی که پایش می‌کند را بیان کند؟» و پاسخ مثبت یا منفی کلید انتخاب خواهد بود.

معماری پایش

پس از تعیین اولویت‌های سازمان براساس برنامه استراتژی امنیت و تهیه ابزار مناسب برای پایش وضعیت امنیت سازمان، طراحی معماری پایش به منظور محافظت از دارایی‌های سازمان، گام مهم بعدی است.

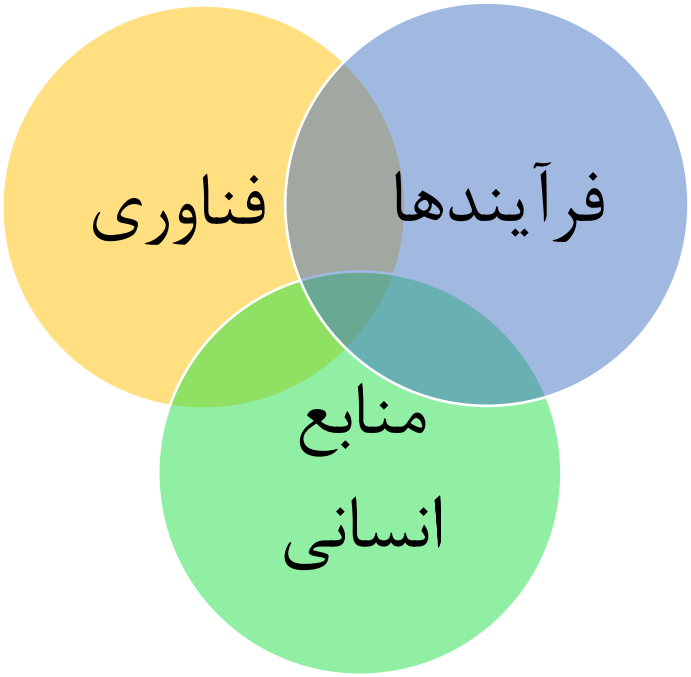
پایش وضعیت امنیت سازمان، ابزار یا فناوری نیست بلکه فرآیندی است که مستلزم بهبودی دائمی است. در نمودار زیر، فعالیت‌های کلیدی که برای این فرایند باید در نظر گرفته شوند آورده شده است.



جمع‌بندی

اهمیت و ضرورت حفاظت از دارایی‌های سازمان بر تمامی اعضای هر سازمان واضح و مبرهن است و تمامی تلاش‌ها، حفظ انطباق با الزامات و استانداردهای گوناگون در واحدهای مختلف سازمان و در راس آن واحد امنیت اطلاعات، محافظت از دارایی‌های اطلاعاتی و ارزش‌ها و اعتبار سازمان است. برای رسیدن به این هدف، داشتن بینش کاملی از وضعیت امنیت سازمان، در گرو بررسی وضعیت تک‌تک اجزای شبکه پرداخت است. هرچه بیشتر به صورت لحظه‌ای تغییر وضعیت دارایی‌های حیاتی را براساس استراتژی مدیریت و راهبری امنیت سازمان، اطلاعات به دست آورده شود، به همان میزان هم ارتقای وضعیت امنیتی سازمان نیز صورت می‌پذیرد.

در این مقاله تلاش شد تا نکات اصولی و بنیادی به منظور حفظ امنیت یکی از ارکان مهم در امنیت سازمان مورد بررسی قرار گیرد اما در راستای حفظ امنیت دو رکن مهم دیگر وجود دارند که پایش و ارزیابی و بهبود مستمر آنها را نباید فراموش کرد. چه بسا که در عمل و «منابع انسانی» و «فرآیندها» نقش بسیار مهمی را ایفا می‌کنند و «فناوری» ابزاری است تا در خدمت دو عامل دیگر باشد و تسهیلات، امکانات و اطلاعات مناسبی را برای بر آنها فراهم کند.



منابع و مأخذ

- شاپرک، ۱۳۹۴، *الزامات امنیت اطلاعات شاپرک*
- PCI Security Standards Council, 2016, *Payment Card Industry (PCI) Data Security Standard*
- The Center for Internet Security, 2016, *Critical Security Controls for Effective Cyber Defense*
- Ponemon Institute, 2017, *2017 Cost of Data Breach Study*
- GFI Software, *Automated event log management for PCI DSS compliance*
- Matt Bromiley, 2016, Incident Response Capabilities in 2016
- NIST Special Publication 800-53, ver 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- Karen Kent, Murugiah Souppaya, 2006, Guide to Computer Security Log Management