راه اندازی مرکز عملیات امنیت

SOC

با بودجه محدود

ترجمه: مهندس شهرام آبابایی
با مقدمه: دکتر علیرضا صالحی

ایجاد یک مرکز عملیات امنیت

با حداقل منابع در کمترین زمان

برای بسیاری از سازمان‌ها (به‌غیراز آنهایی که به بانک‌ها وابسته‌اند) ایجاد یک مرکز، امری غیرممکن به نظر می‌رسد. با توجه به محدودیت منابع (زمان، کارشناس و بودجه)، ایجاد یک مرکز عملیاتی که با فناوری‌های نظارت امنیتی چندگانه و به‌روزرسانی بدون‌درنگ تهدیدات حمایت می‌شود به نظر امکان‌پذیر نیست. همچنین یک تیم با اعضای ماهر و تمام‌وقت برای ایجاد و مدیریت ابزارهای متفاوت، نیاز به ساختاری پویا دارد.
به این دلیل است که یافتن روش‌هایی برای ساده‌سازی و یکپارچگی نظارت امنیتی با هدف بهینه‌سازی فرایندهای مرکز و گروه ضروری است.

در هر بخش از این کتاب جزییات و مشخصات ضروری ایجاد، بررسی خواهدشد.

فصل اول:

افراد

گروه مرکز عملیات امنیت: باید وظایف و مسئولیت‌های کلیدی عملیات امنیتی مرکز برای ایجاد گروه بررسی شود. باید یادگیری مهارت‌ها و توانایی‌ها برای استخدام و تأمین کارکنان برای داشتن یک گروه عملیات امنیتی تهیه شود.

فصل دوم:

فرایندها

باید فرایندهای کلیدی موردنیاز ایجاد یک مرکز را ایجاد کرد. این فرایندها شامل رده‌بندی و تریاژ اولویت‌بندی و تحلیل، اصلاح و ترمیم و نیز ارزیابی و ممیزی است.

فصل سوم:

ابزار

بررسی ابزار ضروری نظارت امنیتی برای ایجاد مرکز که شامل استخراج دارایی‌ها، ارزیابی آسیب، شناسایی نفوذ، نظارت‌های رفتاری و **SIEM** و یا تحلیل امنیتی و شناسایی و معرفی فواید ملموس محکم‌سازی ابزار از طریق یک پلتفرم یکپارچه است، باید انجام گیرد.

فصل چهارم:

هوش

درک تفاوت میان تکنیک، استراتژی و هوش عملیاتی و روش‌های خاص مورداستفاده در این مراکز الزامی است. فواید ترکیب جمع‌سپاری اطلاعات تهدید نیز باید موردبررسی قرار گیرد.

فصل پنجم:

دنیای واقعی

برای ایجاد مرکز در دنیای واقعی لازم است متدولوژی استفاده از فناوری ارتباطات و هوش تهدیدی موردنظر قرار گیرد.

پیش گفتار

علیرضا صالحی

مرکز عملیات امنیت یکی از مهم‌ترین و درعین‌حال شاید مظلوم‌ترین قسمت‌های چرخه تأمین امنیت است. این بخش از حفاظت، نظارت و تأمین امنیت این‌قدر مهم و جذاب هست که همه سازمان‌ها به‌نوعی درگیر پیاده‌سازی یا تلاش برای پیاده‌سازی آن هستند. به همین نحو، شرکت‌های بسیاری در کار تأمین این زیرساخت، سامانه یا هر چیزی که خود از این نام برداشت می‌کنند هستند.

اما به مصداق اشاره مولانا که می‌فرماید «هرکسی از ظن خود شد یار من»، هرکسی تعبیر و تفسیری از SOC دارد و طبیعی است که حاصل این تعریف‌های ناهمگون، ایجاد آشفتگی و ناهماهنگی در تأمین این بخش حیاتی از زنجیره تأمین امنیت می‌شود.

خوشبختان کتاب حاضر با بیانی ساده، موجز و با توجه به محدودیت بودجه‌ای که اغلب سازمان‌ها مبتلابه آن هستند، موضوع پیاده‌سازی مرکز عملیات امنیت را بیان کرده است. بی‌شک این کتاب مدعای آن را ندارد که همه نکات و ریزه‌کاری‌های راه‌اندازی چنین مرکزی را تبیین کرده، اما می‌تواند مرجع بسیار خوبی باشد برای همسان کردن ادبیات این موضوع در کشور و راهبری تصمیم گیران و تصمیم سازان حوزه امنیت فناوری اطلاعات کشور تا با تصویر و تصوری صحیح به این مقوله بنگرند.

نکته مهم دیگر این کتاب آ است که توسط یکی از مدیران باسابقه فناوری اطلاعات و امنیت ترجمه‌شده که خود سال‌ها دستی بر آتشی داشته و با زیروبم‌ها و محدودیت‌های سازمان‌ها آشنا بوده است.

مطالعه این کتاب می‌تواند برای همه مدیران و کارشناسان افتای کشور مفید باشد.

ساختار مرکز عملیات امنیت

گروه مرکز عملیات امنیت مسئول نظارت، تشخیص، تضمین و اصلاح (تأثیر) تهدیدات (فناوری اطلاعات) در برنامه‌های حیاتی، تجهیزات و سیستم‌ها در محیط‌های خصوصی و عمومی ابر، همانند محیط‌های فیزیکی هستند.
با استفاده از فناوری‌های متنوع و فرایندها، گروه مرکز عملیات امنیت از آخرین تهدیدات هوشمند برای تعیین تهدیدات فعال در حال رخ دادن و همچنین تشخیص گستردگی تأثیر آن برای ترمیم استفاده می‌کند.
مسئولیت‌ها و نقش این مرکز در استنتاج وقایع همراه با افزایش و شدت رخدادها به‌صورت ادامه‌دار خواهدبود.

معرفی اصول
مرکز عملیات امنیت

اگر در حال تأمین امنیت یک بانک یا فروشگاه مواد غذایی هستید مسلما قوانین رایج امنیتی را به کار خواهیدگرفت و ضمن تجهیز درهای ورودی و خروجی و صندوق‌ها و گاوصندوق‌ها به قفل، از حفاظت این مکان‌ها با دوربین و دیگر امکانات بهره خواهیدبرد.
به طریق مشابه، برای زیرساخت ابر، ابر عمومی و شبکه‌های خصوصی نیز قوانین امنیتی به کار گرفته‌می‌شوند. کنترل دسترسی‌ها با ابزارهایی مانند کلمات عبور، فهرست‌های کنترل دسترسی، قوانین فایروال و دیگر ابزارها و روش‌ها که البته کافی نیستند. شما باید بتوانید به‌طور مداوم زیرساخت حیاتی خود را نظارت کنید تا امکان کشف فعالیت غیرعادی را که ممکن است نشانه‌ای از نفوذ باشد، فراهم آورید.

ابزارهایی که برای نظارت و تحلیل امنیت به کار می‌روند می‌توانند فراتر از یک شبکه دوربین مداربسته ولی با همان مفهوم باشند.

متأسفانه برخلاف دوربین‌های مداربسته نمی‌توان با مشاهده صفحه یک نمایشگر، یک تهدید را بلافاصله تشخیص داد و یا یک جرم را با استفاده از یک سیستم ضبط ویدئویی مورد تعقیب قرارداد.
تنها تکه کوچکی از رخدادهای امنیت سایبری و افشای آنها متفاوت‌تر، گسترده‌تر و پنهان‌تر از آن چیزی است که در تصویر یک دوربین بتوان یافت و به همین دلیل است که بیش از یک ابزار برای نظارت مؤثر به محیط لازم است.

فصل اول

افراد

همچون تفاوت‌های افراد، هر سازمان امنیتی نیز با سازمان دیگر متفاوت است. در برخی سازمان‌ها تیم اجرایی، اهمیت امنیت سایبری را در مسیر تجاری شرکت شناسایی می‌کند و به رسمیت می‌شناسد. در این حالت تیم مرکز در جایگاهی ویژه، با بودجه کافی برای ابزار، کارکنان کافی برای مدیریت آنها و به‌صورت برجسته به‌عنوان سرمایه انسانی اجرایی تحت حمایت هستند.

متأسفانه در بیشتر موارد مشخصه فوق به واقعیت بدل نمی‌شود!

بیشتر گروه‌های مرکز عملیات امنیت در حال فعالیت بدون نفرات کافی، بدون زمان کافی و بدون توجه کافی و عدم اطمینان از آنچه انجام می‌دهند به سر می‌برند. به همین دلیل است که لازم به نظر می‌رسد بر مجموعه ابزار و سازمان‌دهی مؤثر تمرکز کرد. یک تیم مرکز عملیات امنیتی، مهارت مناسب و توانایی به‌کارگیری حداقل منابع در شناسایی تهدیدات فعال و در حال ظهور را داراست و این هدف اصلی در ایجاد تیم مرکز است.

حال سؤال این است چگونه به این هدف دست‌یابیم؟

در اینجا لازم است تا نکاتی درباره نقش‌های عملیاتی و مسئولیت‌های حمایتی مرکز بررسی شود.