استراتژی‌های تیم آبی

تالیف : میلاد چراغی

استراتژی‌های تیم آبی

میلاد چراغی

https://t.me/CheraghiMilad

www.linkedin.com/in/miladcheraghi

سخن مترجم

بمانَد سال‌ها این نظم و ترتیب
ز ما هر ذرّه خاک افتاده جایی

غرض نقشیست کز ما باز ماند
که هستی را نمی‌بینم بقایی

مگر صاحب‌دلی روزی به رحمت
کند در کار درویشان دعایی

سعدی

مقـــدمه

این کتاب شما را با مفهوم تیم آبی و نحوه عملکرد آن‌ها آشنا می‌کند. نگاهی به تاریخچه تشکیل تیم آبی و تأثیر آن بر کسب‌وکارها صورت گرفته و به حوزه‌های مختلفی که دفاع در آن‌ها اهمیت دارد، مانند امنیت ابر و امنیت شبکه، اشاره خواهد شد. همچنین، در این کتاب یاد خواهید گرفت چگونه یک تیم آبی را ایجاد کنید.

فهرست مطالب

فهرست مطالب

2 مدیریت تیم امنیت دفاعی

در فصل پیشین، درباره‌ی ترکیب معمول یک تیم آبی و نحوه‌ی استخدام افراد مناسب صحبت کردیم. در این فصل، تمرکز ما بر این خواهد بود که تیم مدیریتی یک سازمان چگونه می‌تواند اطمینان حاصل کند که تیم آبی به‌صورت مؤثر و کارآمد فعالیت می‌کند؛ آن هم از طریق معیارهای قابل اندازه‌گیری و ملموسی که می‌توان آن‌ها را تعریف کرد تا مطمئن شد که سازمان به‌خوبی محافظت می‌شود.

هر سازمانی باید معیارهایی را که برای آن مناسب و کاربردی هستند، بررسی و انتخاب کند. این کار نه‌تنها به آن‌ها کمک می‌کند تا سطح امنیت فعلی خود را به‌طور عینی و قابل اندازه‌گیری تعریف کنند، بلکه باعث می‌شود اطمینان حاصل کنند که با گذشت هر روز، در حال پیشرفت و بهبود هستند.

علاوه بر این، در این فصل بررسی خواهیم کرد که چگونه می‌توان بار کاری تیم آبی را کاهش داد و از طریق برخی ابزارهای محبوب، به سراغ خودکارسازی رفت. در این فصل به موضوعات زیر خواهیم پرداخت:

- چرا سازمان‌ها باید به متریک‌سازی امنیت سایبری توجه کنند؟
- چرا و چگونه سازمان‌ها می‌توانند این فرآیند را خودکار کنند؟

چرا سازمان‌ها باید به متریک‌سازی امنیت سایبری توجه کنند؟

متخصصان باتجربه امنیت سایبری توصیه می‌کنند که شرکت‌ها عملکرد تیم‌های مختلف سایبری خود را اندازه‌گیری کنند تا مدیران بتوانند این تیم‌ها را به شکل مؤثرتری مدیریت کنند. اگر سازمانی نتواند تلاش‌های امنیتی جاری خود را دنبال کند، هیچ‌گونه درکی از وضعیت امنیتی خوب یا بد خود نخواهد داشت. امنیت سایبری مسئله‌ای نیست که یک‌بار انجام شود و بعد فراموش شود. تهدیدهای سایبری دائماً در حال تحول هستند، همان‌طور که تکنیک‌ها و

فناوری‌های مقابله با آن‌ها نیز باید به‌روز شوند. به مدیران تیم آبی توصیه می‌شود فرآیندهایی برای ارزیابی اثربخشی اقدامات امنیتی اتخاذ شده به‌طور منظم داشته باشند.

شاخص‌های کلیدی عملکرد[1] ، شاخص‌های کلیدی ریسک[2] ، و تحلیل وضعیت امنیتی، تصویری از عملکرد تیم آبی در طول زمان ارائه می‌دهند. این موضوع به مدیران و رهبران سازمان کمک می‌کند تا بفهمند چه چیزهایی مؤثر هستند و چه چیزهایی نه، و تصمیمات هوشمندانه‌تری برای اقدامات آینده اتخاذ کنند.

متریک‌ها داده‌هایی قابل اندازه‌گیری و قابل راستی‌آزمایی هستند که اغلب برای ارائه به مدیریت و اعضای هیئت‌مدیره به کار می‌روند تا نشان داده شود که مدیران در حال تلاش برای محافظت از داده‌های حساس و دارایی‌های فناوری اطلاعات هستند. بسیاری از مدیران ارشد امنیت اطلاعات (CISO) و فناوری اطلاعات (CIO) دریافته‌اند که گزارش دادن و فراهم کردن زمینه برای متریک‌های امنیت سایبری، بخش مهمی از وظایف شغلی‌شان شده، چرا که انتظارات سهام‌داران، نهادهای نظارتی و اعضای هیئت‌مدیره به‌طور مداوم در حال افزایش است. بسیاری از اعضای هیئت‌مدیره در صنایع خاص مانند مالی، مسئولیت قانونی یا اخلاقی برای مدیریت ریسک امنیت سایبری و محافظت از داده‌های شناسایی‌شده‌ی شخصی دارند. برخی قوانین جدید، مانند:

- قانون حفاظت از داده اتحادیه اروپا (GDPR)
- قانون حریم خصوصی مصرف‌کننده کالیفرنیا (CCPA)
- قانون حفاظت از داده‌های شخصی برزیل (LGPD)

و بسیاری دیگر در سراسر جهان، به این روند شتاب بخشیده‌اند. در بخش بعدی، برخی از شاخص‌های کلیدی را بررسی می‌کنیم که تیم آبی می‌تواند برای اطمینان از انطباق و امنیت سازمان پایش کند.

---

[1] KPI
[2] KRI

شاخص‌های کلیدی ریسک تیم آبی

KRIs یا شاخص‌های کلیدی ریسک، معیارهایی هستند که یک سازمان از آن‌ها برای پایش ریسک‌های کنونی و بالقوه در حوزه‌های عملیاتی، مالی، شهرت، انطباق و استراتژیک استفاده می‌کند. نوع ریسک‌هایی که یک سازمان با آن مواجه است بسته به دپارتمان یا بخش کاری متفاوت است. به‌عنوان مثال:

- یک شعبه بانک ممکن است نگران افتتاح حساب بدون تأیید هویت مناسب باشد.
- در حالی‌که بخش فناوری اطلاعات همان بانک نگران نفوذ به داده‌هاست.
- بخش رسیدگی به خسارت بیمه‌ای ممکن است نگران ادعاهای جعلی باشد.
- و تیم مدیریت پروژه‌های فناوری اطلاعات، دغدغه افزونگی سرورها برای جلوگیری از قطعی سیستم را دارد.

KRIs هم ریسک مرتبط با اقدامات خاص و هم ریسک‌های روزمره را ارزیابی می‌کنند و مانند یک سیستم هشداردهنده عمل می‌کنند تا مسائل مالی (از دست رفتن درآمد)، مشکلات عملیاتی (کاهش بهره‌وری) و آسیب‌های شهرتی (از دست رفتن اعتبار) را گزارش دهند.

KRIs معمولاً به‌صورت درصدی اندازه‌گیری می‌شوند و نمایی از وضعیت فناوری و ریسک‌های کسب‌وکار سازمان ارائه می‌دهند. این معیارها به مدیریت کمک می‌کنند تا عملیات را در نقاط نیازمند بهبود ارتقا دهند. برخی مزایای استفاده از این رویکرد:

- هشدار زودهنگام برای اقدام پیش‌گیرانه که باعث کاهش حوادث امنیتی و صرفه‌جویی در هزینه‌ها می‌شود.
- تحلیل گذشته‌نگر از رویدادهای ریسکی جهت اجتناب از اشتباهات پیشین.
- اطلاع به مدیران ارشد یا هیئت‌مدیره درباره تطابق با میزان پذیرش ریسک.
- ارائه اطلاعات عملیاتی و قابل اقدام در زمان واقعی به تصمیم‌گیران و مدیران ریسک.

اکنون که با مفهوم KRIs آشنا شدیم، بیایید ببینیم تیم آبی چگونه باید طراحی آن‌ها را آغاز کند.

تیم آبی چگونه طراحی KRIs را آغاز می‌کند؟

تیم‌های آبی در صنایع مختلف معمولاً چند مرحله مشخص را برای شناسایی بهترین متریک‌ها برای سازمان خود طی می‌کنند. این مراحل تکرارپذیر هستند و باید در بازه‌های زمانی منظم مرور شوند، زیرا نیازهای فنی یا تجاری سازمان، و همچنین چشم‌انداز تهدیدات، در طول زمان تغییر می‌کنند. این مراحل پنج‌گانه عبارتند از:

مرحله اول، کشف[1]

در این مرحله، تمام دارایی‌های فناوری اطلاعات در سراسر سازمان شناسایی می‌شوند. این کار به پوشش کامل سطح حمله کمک می‌کند. باید دارایی‌هایی که جدید، ناشناخته یا خارج از فرایندهای انطباق روزمره هستند، شناسایی شوند.

تیم آبی می‌تواند اطلاعات اولیه را وارد سیستم‌های اسکن دارایی پیشرفته‌تر کند. این باعث می‌شود بتواند دارایی‌ها را بر اساس فناوری مورد استفاده شان دسته‌بندی کند. این شامل همه چیز از ایستگاه‌های کاری تا سرورها و تجهیزات شبکه است؛ چه در زیرساخت‌های داخلی و چه ابری. همچنین باید با واحدهای تجاری مربوطه گفتگو شود تا اهمیت هر دارایی مشخص گردد. تیم آبی سپس به هر دارایی یک درجه ریسک اختصاص می‌دهد که منعکس‌کننده‌ی ارزش تجاری و سطح تهدید آن است. جزئیات این موضوع در فصل سوم (ارزیابی ریسک) مطرح خواهد شد.

مرحله دوم، انتخاب دارایی‌ها و KRIs مرتبط

پس از درک اهمیت دارایی‌ها، باید KRIs مرتبط و قابل اندازه‌گیری و پیش‌بینی‌پذیر را برای پایش آن‌ها انتخاب کرد. توصیه می‌شود ترکیبی از شاخص‌های پیش‌نگر و پس‌نگر گردآوری شود.

در ابتدا، تعداد کمی از KRIs که ردیابی آن‌ها سخت اما برای انطباق یا ریسک‌های خاص حیاتی‌اند، تنظیم می‌شوند. همچنین باید این شاخص‌ها با توجه به تغییرات تهدیدات و استراتژی‌های سازمانی به‌روزرسانی شوند.

[1] Discovery

مرحله سوم، تعیین خط پایه و آستانه‌ها

در این مرحله باید برای هر دارایی، سطح پایه‌ی انطباق برای هر KRI تعریف شود. این خطوط پایه باید به‌صورت دوره‌ای بازبینی و به‌روز شوند.

مثلاً اگر یک سرور دارای اهمیت بالا باشد، ممکن است تیم آبی خواستار ۱۰۰٪ انطباق با وصله‌های امنیتی، آنتی‌ویروس، سخت‌سازی و سایر معیارها باشد. در مقابل، برای پرتال داخلی کارکنان ممکن است سطح انطباق کمتری کافی باشد.

مرحله چهارم، پایش، بررسی و گزارش‌دهی

هر KRI باید به‌صورت منظم پایش شود. اگر عدم انطباقی مشاهده شد، تحلیل‌گران باید آن را گزارش داده و به مدیر SOC اطلاع دهند تا با تیم مربوطه برنامه‌ی اقدامی تنظیم شود. این مدیریت معمولاً از طریق سیستم تیکتینگ سازمان انجام می‌شود تا وضعیت ریسک‌های باز و مسئولان پیگیری آن‌ها مشخص باشد.

در اینجا ممکن است هشدارهای نادرست (False Positive) نیز رخ دهند که وظیفه‌ی تیم آبی است که آن‌ها را بررسی کرده و ببندد. همچنین ممکن است نیاز به تعدیل KRIs برای کاهش نرخ هشدارهای نادرست باشد. در برخی موارد، ممکن است یک دلیل تجاری برای عدم انطباق وجود داشته باشد؛ در این صورت، تیم آبی می‌تواند کنترل‌های جایگزین پیشنهاد دهد یا در موارد خاص، ریسک را برای مدت زمان مشخصی بپذیرد.

مرحله پنجم، مدیریت ریسک

قاعده‌ای وجود دارد که می‌گوید: "هزینه‌ی امنیت نباید از ارزش دارایی بیشتر باشد". اگرچه ارزش دقیق یک دارایی همیشه قابل محاسبه نیست، اما باید سطح امنیت متناسب با اهمیت نسبی آن دارایی باشد. اینجاست که ارزیابی ریسک نقش کلیدی ایفا می‌کند (که در فصل سوم به آن خواهیم پرداخت). همچنین باید توجه داشت که KRIs به‌هیچ‌وجه نباید فقط به‌صورت کپی و پیاده‌سازی باشند. تیم آبی باید ساختار فناوری و نیازهای سازمان را درک کند و آماده باشد که متریک‌ها را به‌طور منظم تنظیم کند.

Server Patching	
Compliant	60%
Partial Compliant	20%
Non Compliant	20%

Endpoint Patching	
Compliant	50%
Partial Compliant	15%
Non Compliant	35%

Network Device Patching	
Compliant	30%
Partial Compliant	0%
Non Compliant	70%

Server Hardening	
Compliant	80%
Non Compliant	20%

Endpoint Hardening	
Compliant	70%
Non Compliant	30%

Network Device Hardening	
Compliant	60%
Non Compliant	40%

User ID: Application Access	
Review Complete	95%
Review Pending	5%
Non Compliant	0%

Privilege Accounts: Servers	
Review Complete	92%
Review Pending	3%
Non Compliant	5%

Privilege Accounts: Desktops	
Review Complete	92%
Review Pending	0%
Non Compliant	8%

Antivirus Compliance	
Compliant	95%
Non Compliant	5%

Open Vulnerabilities	
Risk Open	1556
Risk Accepted	298

Open Audit Findings	
Risk Open	19
Risk Accepted	2

Database Patching	
Compliant	100%
Partial Compliant	0%
Non Compliant	0%

Database Hardening	
Compliant	97%
Non Compliant	0%
Review Pending	3%

Privilege Accounts: Databases	
Review Complete	20%
Review Pending	0%
Non Compliant	80%

(شکل 2 – 1 : نمونه داشبورد)

انتخاب معیارهای ضروری برای امنیت سایبری

وقتی صحبت از شاخص‌های کلیدی ریسک در حوزه امنیت سایبری می‌شود، هیچ قانون ثابت و قطعی وجود ندارد. این شاخص‌ها بستگی به صنعت شما، نیازهای کسب‌وکار، قوانین، استانداردها، بهترین رویه‌ها و در نهایت، میزان پذیرش ریسک شما دارند. با این حال، باید از معیارهایی استفاده کنید که برای همه افراد، از جمله ذی‌نفعان غیر فنی، قابل درک باشد. اگر همه ذی‌نفعان این معیارها را متوجه نمی‌شوند، باید معیارهای دیگری را انتخاب کنید یا آن‌ها را بهتر توضیح دهید.

معیارهای مقایسه‌ای و مقایسه با استانداردهای صنعت، راهی ساده برای درک حتی پیچیده‌ترین اندازه‌گیری‌ها ارائه می‌دهند. همچنین، به یاد داشته باشید که هر KRI باید با یک سیاست یا استاندارد فنی سازمان هماهنگ باشد. داشتن یک سیاست قابل‌اعتماد، پایه و اساس KRI ها است.

چنین معیارهایی باید به‌عنوان ابزاری برای دستیابی به سطح‌های تطابقی که سازمان تعیین کرده، تلقی شوند. بنابراین، ارتباط دادن هر KRI با سیاست مرتبط، به تیم آبی قدرت لازم برای پیگیری سطح‌های موردنیاز از تطابق را می‌دهد.

توصیه‌های زیادی درباره حوزه‌ها و معیارهایی که سازمان‌ها باید روی آن تمرکز کنند وجود دارد. مرکز امنیت اینترنت (CIS) فهرستی از ۱۸ کنترل را در آدرس زیر ارائه داده که می‌تواند برای یک سازمان معمولی مفید باشد:

https://www.cisecurity.org/controls/cis-controls-list

این فهرست به‌عنوان نقطه شروع عمل می‌کند و هر سازمان باید با تأمل و بررسی، بهترین‌ها را برای خود انتخاب کند. این کنترل‌ها شامل موارد زیر است:

- فهرست و کنترل دارایی‌های سازمانی[1]

تیم‌های آبی باید از تمام دارایی‌هایی که به سازمان تعلق دارند، آگاه باشند. این شامل سرورها، نقاط پایانی، و اجزای شبکه، چه در محل سازمان و چه در زیرساخت‌های ابری، می‌شود. این گام به‌عنوان نقطه شروعی برای درک شبکه سازمان و اطمینان از پوشش کامل کنترل‌های دفاعی عمل می‌کند. بنابراین، داشتن KRI برای اندازه‌گیری تعداد دارایی‌های ناشناخته اهمیت دارد.

- فهرست و کنترل دارایی‌های نرم‌افزاری[2]

مشابه فهرست دارایی‌ها، آگاهی از فهرست نرم‌افزارهای مورد استفاده در سازمان نیز ارزشمند است. این به تیم دفاع کمک می‌کند تا ابزارها و نرم‌افزارهای استفاده‌شده را بشناسد و مراقب آسیب‌پذیری‌های شناخته‌شده باشد. بنابراین، داشتن KRI برای شناسایی نرم‌افزارهای غیرمجاز یا تأییدنشده در شبکه دارای اهمیت است.

---

[1] Inventory and Control of Enterprise Assets

[2] Inventory and Control of Software Assets

- حفاظت از داده[1]

این KPI به تیم آبی کمک می‌کند چرخه عمر داده‌های سازمان را پیگیری کند. اطمینان از اینکه داده‌ها مطابق با سیاست‌های تیم امنیتی، شناسایی، طبقه‌بندی، مدیریت، نگهداری و حذف می‌شوند، ارزشمند است.

- پیکربندی امن دارایی‌ها و نرم‌افزارهای سازمانی[2]

همان‌طور که در دو مورد قبلی ذکر شد، سازمان باید فهرستی از دارایی‌ها و نرم‌افزارهای تأییدشده خود را داشته باشد. در این کنترل، سازمان باید اطمینان حاصل کند که هر یک از این دارایی‌ها به‌صورت ایمن نصب و پیکربندی شده‌اند. این KPI به پیگیری دارایی‌هایی کمک می‌کند که مطابق با استانداردهای پیکربندی امنیتی نیستند.

- مدیریت حساب‌های کاربری[3]

این KPI تمام حساب‌های کاربری ایجادشده برای هر دارایی را ردیابی می‌کند. این کمک می‌کند تا تیم آبی متوجه شود که آیا حسابی ایجاد شده که با فرآیندهای امنیتی مغایرت دارد یا خیر. همچنین، پیگیری جداگانه حساب‌های دارای سطح دسترسی بالا مانند root و administrator نیز ارزشمند است، چون توجه به این حساب‌های پرخطر اهمیت بالایی دارد.

- مدیریت کنترل دسترسی[4]

این KPI فرآیندهای مدیریت هویت و دسترسی (IAM) سازمان را دنبال می‌کند. باید شامل KRIs برای پیگیری هرگونه انحراف از کنترل‌های تعریف‌شده در تنظیم دسترسی، لغو دسترسی، و بازبینی دوره‌ای باشد. این به اطمینان از مشروع بودن و همچنان مورد نیاز بودن حساب‌های تأییدشده کمک می‌کند.

---

[1] Data Protection
[2] Secure Configuration of Enterprise Assets and Software
[3] Account Management
[4] Access Control Management

- مدیریت مستمر آسیب‌پذیری‌ها[1]

تیم‌های آبی باید به‌صورت منظم فرآیندهایی برای شناسایی آسیب‌پذیری‌ها در کل سازمان و همه دارایی‌های شناسایی‌شده در دو کنترل قبلی اجرا کنند. دفعات این اسکن ها باید براساس رتبه ریسک دارایی مورد نظر تعیین شود. پیگیری آسیب پذیری های شناخته‌شده، یک KRI مهم به‌شمار می‌رود.

- مدیریت گزارش‌های لاگ[2]

ثبت، جمع‌آوری و نگهداری گزارش‌های لاگ از همه دارایی‌ها، کنترل بسیار مهمی برای نظارت امنیتی است. دلایل قانونی و نظارتی زیادی وجود دارد که نشان می‌دهد باید مدیریت لاگ‌ها به‌درستی انجام شود. هر دارایی‌ای که نتواند با استانداردهای مدیریت لاگ سازمان تطابق داشته باشد، باید به‌عنوان یک ریسک دنبال شود.

- محافظت‌های ایمیل و مرورگر وب[3]

سازمان باید همه دروازه‌های پیرامونی خود، از جمله دروازه‌های ایمیل و پروکسی اینترنت، را ایمن‌سازی کند. این کار به تیم آبی کمک می‌کند از سازمان دفاع کرده و تهدیدهایی که از این منابع وارد می‌شوند را فیلتر کند.

- دفاع در برابر بدافزارها[4]

تیم آبی باید کنترل‌هایی برای جلوگیری و مهار گسترش و اجرای هرگونه بدافزار در اختیار داشته باشد. اگر یکی از دارایی‌ها آلوده شود، باید کنترل‌هایی وجود داشته باشد تا دارایی آلوده سریعاً قرنطینه و ایزوله شود تا از گسترش آلودگی در سازمان جلوگیری شود. تیم آبی باید شاخص‌های کلیدی ریسک (KRI) را دنبال کند تا اطمینان حاصل شود همه دارایی‌ها از سطح مورد نیاز این کنترل‌ها برخوردارند.

---

[1] Continuous Vulnerability Management
[2] Audit Log Management
[3] Email and Web Browser Protections
[4] Malware Defenses

- بازیابی داده‌ها[1]

هر سازمان باید اطمینان حاصل کند که همه دارایی‌ها به‌طور منظم از داده‌هایشان پشتیبان‌گیری می‌شود. این مسئله به بازیابی پس از وقوع حادثه کمک می‌کند. هر دارایی که از روند تعریف‌شده پشتیبان‌گیری منحرف شود، باید به‌عنوان یک ریسک در نظر گرفته شده و با کمک شاخص‌های کلیدی ریسک پیگیری شود.

- مدیریت زیرساخت شبکه[2]

در برخی موارد، کارکنان ممکن است دستگاه‌های شخصی خود را به شبکه سازمان متصل کنند یا مهمان‌ها بخواهند دستگاه شان را به شبکه شرکت متصل نمایند. اگرچه این موارد می‌توانند غیرخصمانه باشند، اما احتمال این نیز وجود دارد که یک نفوذگر بخواهد دستگاه خود را با اهداف مخرب به شبکه متصل کند. یک دارایی ناسازگار ممکن است تهدیداتی برای کل سازمان ایجاد کند؛ بنابراین باید کنترل‌هایی وجود داشته باشد تا در صورت نیاز چنین دستگاه‌هایی ایزوله و کاملاً مسدود شوند.

- نظارت و دفاع از شبکه[3]

هر سازمانی باید در برابر حملات احتمالی به شبکه‌اش از خود دفاع کند. ثبت و پایش لاگ‌ها برای شناسایی فعالیت‌های مشکوک نیز به همان اندازه اهمیت دارد. تیم آبی باید راهبردهای دفاعی لازم را طراحی کرده و انحراف‌ها را رصد کند تا پوشش کامل امنیتی فراهم گردد.

- آگاهی امنیتی و آموزش مهارت‌ها[4]

کاربران یک سازمان می‌توانند ضعیف‌ترین حلقه زنجیره امنیتی باشند. اگر کنترل‌های امنیتی به خوبی عمل نکنند، آمار مربوط به سطح آموزش کاربران می‌تواند دیدگاه خوبی

---

[1] Data Recovery
[2] Network Infrastructure Management
[3] Network Monitoring and Defense
[4] Security Awareness and Skills Training

در مورد علل ضعف ارائه دهد. یکی از شاخص‌های کلیدی، درصد افرادی است که دوره‌های آموزشی امنیتی را گذرانده‌اند. همچنین، جلسات تخصصی مانند توسعه امن کد[1] برای تیم‌های مرتبط بسیار مفید خواهند بود.

- مدیریت ارائه‌دهندگان خدمات[2]

چشم‌انداز تهدیدات یک سازمان فقط به مرزهای فیزیکی آن محدود نمی‌شود و معیارهای عملکرد امنیتی تیم آبی باید این موضوع را منعکس کنند. وجود یک چارچوب رسمی برای مدیریت ریسک‌های طرف سوم، یکی از شاخص‌های کلیدی ریسک حیاتی برای تیم آبی است. مانند محصولات سازمان، سطح اهمیت ارائه‌دهندگان خدمات نیز متفاوت است. بنابراین، ارزیابی ریسک توسط بخش‌های کسب‌وکار برای تعیین میزان بررسی مورد نیاز ضروری است. داشتن یک چارچوب برای مدیریت و ارزیابی سطح امنیتی همه ارائه‌دهندگان خدمات، در مدیریت این نوع ریسک‌ها مؤثر خواهد بود.

- امنیت نرم‌افزارهای کاربردی[3]

همه نرم‌افزارهای تجاری – چه داخلی و چه خریداری‌شده – باید به‌طور منظم از نظر تهدیدات امنیتی یا آسیب‌پذیری‌ها بررسی شوند. برای محصولات داخلی، استفاده از فرآیندهای اسکن کد منبع نیز باید برای شناسایی آسیب‌پذیری‌ها در نظر گرفته شود. معمولاً محصولات آماده (off-the-shelf) به‌طور منظم بروزرسانی‌هایی منتشر می‌کنند تا آسیب‌پذیری‌های شناخته‌شده را برطرف کنند؛ این بروزرسانی‌ها نیز باید توسط تیم آبی پیگیری شوند. همچنین باید دقت شود که فناوری‌های منسوخ تهدیدی برای سازمان ایجاد نکنند.

---

[1] Secure Code Development
[2] Service Provider Management
[3] Application Software Security

- مدیریت واکنش به حادثه[1]

تیم‌های آبی باید توانایی پاسخ‌گویی به هرگونه حادثه امنیتی سایبری و بازیابی پس از آن را داشته باشند. این موضوع نیازمند برنامه‌ریزی دقیق و تهیه راهنمای پاسخ به حوادث[2] است. آزمایش‌های منظم این برنامه‌ها نیز برای اطمینان از اثربخشی آن‌ها ضروری است.

- تست نفوذ[3]

سازمان‌ها باید به‌صورت منظم دفاع‌های خود را با شبیه‌سازی گام‌هایی که یک مهاجم ممکن است برای نفوذ به کنترل‌های امنیتی بردارد، آزمایش کنند. این آزمایش‌ها می‌توانند توسط تیم آبی یا شرکت‌های شخص ثالث مورد اعتماد انجام شوند. برخی از سازمان‌ها حتی برنامه‌های باگ‌بانتی برگزار می‌کنند تا از قدرت جمعی تعداد زیادی از متخصصان امنیتی بهره ببرند و آسیب‌پذیری‌ها را شناسایی کنند.

این بخش شاخص‌های کلیدی ریسک رایج را که می‌توانند برای یک سازمان ارزشمند باشند توضیح داد و نشان داد تیم آبی باید به چه مواردی توجه داشته باشد. ممکن است این موارد در ابتدا دلهره‌آور به نظر برسند. در بخش بعدی، به راه‌هایی خواهیم پرداخت که بتوان مقدار زیادی از این کارها را خودکار کرد تا تیم آبی بتواند زمان خود را بهتر مدیریت کند.

چرا و چگونه سازمان‌ها می‌توانند این فرآیند را خودکار کنند؟

فرآیندهای مدیریت ریسک سایبری دیدگاه جامعی از تهدیدها و ریسک‌هایی که یک شرکت با آن مواجه است ارائه می‌دهند. این فرآیندها به کارکنان مجاز اجازه می‌دهند که ریسک‌ها را ارزیابی

---

[1] Incident Response Management
[2] playbooks
[3] Penetration Testing

کرده و به آن‌ها شاخص‌هایی اختصاص دهند، تغییرات در پروفایل ریسک سازمان را ثبت کنند، و ریسک‌ها و شاخص‌ها را در برابر اهداف و سطح تحمل‌پذیری[1] بررسی و پیگیری کنند.
ایجاد یک رجیستر ریسک[2] با اهداف شرکتی و سیاست‌هایی که توسط مدیریت ارشد تعریف شده‌اند، و همچنین منابع معتبر و استانداردها، تسهیل می‌شود. پرسش‌نامه‌های ارزیابی ریسک از این رجیستر استخراج شده و برای انجام ارزیابی‌ها استفاده می‌شوند. نتایج این ارزیابی‌ها، راهنمای طراحی و پیاده‌سازی برنامه‌های کاهش یا مقابله با ریسک خواهند بود. همچنین این استراتژی‌ها و نتایج حاصل به اطلاع مدیریت ارشد رسانده می‌شود.

راهکارهای مدیریت ریسک می‌توانند برای فعالیت‌ها و وظایفی پیاده‌سازی شوند که مشخص، قابل سنجش، مرتبط و به‌موقع هستند. درک استانداردهای KRI و معیارهای اندازه‌گیری برای رسیدن به این هدف بسیار حیاتی است. همچنین باید از منابع و تکنیک‌های مختلف برای شناسایی تأمین‌کنندگان داده‌های تحلیلی سازمان و مصرف‌کنندگان شاخص‌ها استفاده کرد.

یکی از مهم‌ترین مزایای استفاده از فناوری برای مدیریتKRI ها، حذف کارهای دستی وقت‌گیر و ناکارآمد است. این فناوری‌ها به خودکارسازی فرآیند جمع‌آوری داده‌ها کمک کرده، تعریف حدود قابل قبول را ساده می‌سازند و در صورت وقوع یک حادثه، پیگیری مشکلات و اقدامات را تسهیل می‌کنند. علاوه بر این، این شاخص‌ها می‌توانند در پاسخگویی به الزامات قانونی، نظارتی و حسابرسی نیز نقش داشته باشند.

از چه اشتباهاتی باید به هنگام خودکارسازی جریان کاری تیم آبی اجتناب کرد؟

وقتی که می‌خواهید جریان کاری کل تیم آبی را خودکارسازی کنید، از همان مراحل ابتدایی که به دنبال پیاده‌سازی یک راه‌حل فنی هستید، با چالش‌های متعددی روبه‌رو خواهید شد. بسیاری از سازمان‌ها با اشتباهات مشابهی مواجه می‌شوند که توصیه می‌شود تا حد امکان زودتر از آن‌ها جلوگیری شود. برخی از این مشکلات عبارت‌اند از:

---

[1] Tolerance
[2] Risk Register

- نبود استانداردها و بهترین رویه‌ها[1]

ابزارهای استاندارد معمولاً با تمرکز بر قابلیت‌ها و ویژگی‌هایی طراحی می‌شوند که در سازمان‌های دیگر موفق بوده‌اند. متأسفانه، هیچ استاندارد یکپارچه‌ای وجود ندارد که در تمام صنایع یا حتی بین صنایع مختلف قابل استفاده مستقیم برای تیم‌های آبی باشد.

- گرایش مدیریت

مدیریت ارشد سازمان باید کنترل‌هایی را که مزایای کسب‌وکار را به‌صورت واضح و با ارزش پولی مشخص توضیح می‌دهند، درک کند و انتظار داشته باشد. مفهوم شاخص‌های امنیتی[2] هنوز در دنیای کسب‌وکار نسبتاً جدید است. بسیاری از مدیران ارشد از ارزش آن مطمئن نیستند و درباره طراحی این شاخص‌ها سردرگم‌اند و تمایل ندارند منابعی را برای توسعه آنها اختصاص دهند.

- سرعت تغییرات

فناوری‌ها با سرعت بسیار بالایی تغییر می‌کنند و ریسک‌های مرتبط یا ذاتی در یک فناوری خاص ممکن است با انتشار نسخه‌های جدید یا پیشرفت‌های آن تغییر کنند. (افزایش یا کاهش یابند). فرآیندهای کاری مرتبط با یک فناوری خاص یا حتی فرایندهای مبتنی بر فناوری باید هر زمان که فناوری پایه به‌روزرسانی قابل توجهی داشته باشد، مجدداً ارزیابی شوند.

- اقدامات برای حفظ کنترل

قبل از آنکه شاخص‌های مؤثر بتوانند طراحی و اجرا شوند، باید کنترل‌های داخلی برقرار شده باشند. سازمانی که نسبت به کنترل‌های خود اطمینان ندارد، قادر نخواهد بود شاخص‌های معنی‌داری برای آن طراحی کند. خوشبختانه بسیاری از سازمان‌ها قبلاً تمرین‌های طولانی‌مدتی برای ثبت مکانیزم‌های کنترل اساسی به‌عنوان بخشی

---

[1] Best Practices

[2] security metrics

از فرایندهای انطباق خود انجام داده‌اند. این کنترل‌ها معمولاً برای تعیین شاخص‌های ریسک فعال در ابزارهای اتوماسیون امنیتی مختلف استفاده می‌شوند و می‌توانند برای توسعه شاخص‌های قابل اندازه‌گیری به‌کار روند.

- مدیریت ریسک کسب‌وکار

افرادی که مسئول استقرار و مدیریت فناوری هستند، معمولاً بیشتر نگران خود فناوری هستند تا ریسک کسب‌وکار ناشی از شکست آن. علاوه بر این، اندازه‌گیری میزان تأثیر یک حادثه امنیتی بر کسب‌وکار دشوار است. این موضوع باعث ایجاد اصطکاک بین تیم‌های آبی و مدیران آن‌ها می‌شود، چون نمی‌توانند به خوبی نیاز به کنترل‌ها را بیان کنند.

خودکارسازی جمع‌آوری و ارائه شاخص‌های کلیدی ریسک

پس از اینکه تیم آبی روی شاخص‌های کلیدی ریسک کار کرد، باید فرکانس لازم برای گزارش‌دهی هر یک را تعریف کند. اینجاست که خودکارسازی وارد عمل می‌شود و به کاهش حجم کاری تیم کمک می‌کند و تمرکز تیم را بر روی نقاطی که بیشترین نیاز را دارند، قرار می‌دهد.

خودکارسازی جمع‌آوری KRI از طریق موارد کاربردی مختلفی امکان‌پذیر است که با استفاده از راهکارهای امنیتی متنوعی که قبلاً در زیرساخت سازمان نصب شده‌اند، ساخته و بهینه شده‌اند. ابزارها و محصولات متعددی در این زمینه وجود دارند. برخی سازمان‌ها از محصولات Governance, Risk, and Compliance (GRC) برای ثبت چنین شاخص‌هایی در بخش‌های مختلف استفاده می‌کنند. همچنین راهکارهای Security Information and Event Management (SIEM) می‌توانند برای جمع‌آوری، اندازه‌گیری، ثبت و نمایش داده‌ها به صورت آمار روی داشبوردهای داخل این محصولات امنیتی به کار روند. علاوه بر این، اتوماسیون فرآیند رباتیک[1] نیز می‌تواند استفاده شود، که در آن فناوری برای انجام وظایف مشخص‌شده بر اساس قوانین برنامه‌ریزی شده به کار می‌رود و با برنامه‌ها و سیستم‌های موجود تعامل دارد.

[1] Robotic Process Automation - RPA

تمام فرآیند اندازه‌گیری، ثبت و ارائه شاخص‌های کلیدی ریسک می‌تواند به‌طور کامل خودکار شود. بسیاری از شرکت‌ها با اتوماسیون جمع‌آوری و نمایشKRI ، مرکز عملیات امنیت (SOC) خود را برای رعایت الزامات انطباقی بهبود داده و بالغ کرده‌اند. این کار به ایجاد فرهنگ تصمیم‌گیری مبتنی بر داده کمک می‌کند و سازمان‌ها را قادر می‌سازد تا روی ریسک‌هایی که بیشترین تناسب را با آن‌ها دارند تمرکز کنند.

داشبوردهای پویا نیز می‌توانند ایجاد شوند تا بررسی کنند که آیا شاخص‌های کلیدی ریسک (KRIs) به سطح پایه مشخصی تنظیم شده‌اند یا خیر و همچنین چگونگی دفعات خروج یک دارایی از حالت انطباق را پایش کنند. پس از تغییر این KRIs ، هشدارهایی می‌توانند فعال شده و به مالک کنترل مربوطه ارسال شوند. برای برخی از KRIs ، گزارش‌های استثنا یا تیکت‌هایی نیز ممکن است بنا به نیازهای سازمان ایجاد شوند. تحلیل‌های علم داده نیز می‌توانند برای رصد داشبوردهای مختلف KRI مانند ایجاد کاربران مجاز و لغو دسترسی به‌موقع برای خروج و انتقال افراد به کار روند. قبل از اعمال تغییرات در KRIs در سراسر شبکه و سیستم‌ها، ممکن است داشبورد نظارت مداومی تنظیم شود تا اطمینان حاصل شود که همه تغییرات به‌درستی تأیید و تصویب شده‌اند.

نتیجه‌ی اجرای موفق داشبورد این است که تیم آبی باید احساس توانمندی کند و بتواند به صورت پیشگیرانه دارایی‌های فناوری اطلاعات خود را قبل از وقوع هرگونه حادثه سایبری محافظت کند. در نهایت، پیشگیری از حوادث همیشه ارزان‌تر و بهتر از درمان آن‌ها خواهد بود.

خلاصه

در این فصل، اهمیت شاخص‌های کلیدی ریسک مرتبط با امنیت سایبری را درک کردیم. درباره چگونگی آغاز مسیر برای تعیین شاخص‌های قابل اندازه‌گیری و قابل اطمینان برای یک سازمان صحبت کردیم. همچنین در مورد خودکارسازی و استفاده از برخی ابزارها برای کمک به تیم آبی در عملیاتی کردن این کار و بهره‌برداری بهتر از این فرآیند، بحث کردیم.

سپس بررسی کردیم که چگونه تیم مدیریت می‌تواند با نگاه دقیق به سازمان خود اطمینان حاصل کند که امنیت سازمان به‌صورت مؤثر اندازه‌گیری می‌شود و همچنین پیشرفت شاخص‌ها سالم و به تدریج با تغییر تهدیدات و روندهای صنعت رو به بهبود است.

در فصل بعدی، یاد خواهیم گرفت که ارزیابی ریسک‌ها چگونه باید در یک سازمان انجام شود و این ارزیابی‌ها چگونه می‌توانند برای تیم‌های آبی مفید باشند.

3 فصل سوم به زودی