مدیریت سطح حمله

رونا کدمی – 29 مارس 2022

با انتقال به فضای ابری، افزایش برنامه‌های نرم‌افزار به‌عنوان سرویس (SaaS) و افزایش ناگهانی توانایی‌های کار از راه دور، سطح حمله بیشتر سازمان‌ها بزرگ‌تر و پیچیده‌تر شده است و تعریف و دفاع از آن را به طور فزاینده‌ای دشوار می‌سازد. از آنجا که تقریباً هر دارایی می‌تواند نقطه ورود یک حمله سایبری باشد، بهبود دید سطح حمله در سراسر دارایی‌ها – چه شناخته شده و چه ناشناخته، در محل یا در فضای ابری، داخلی یا خارجی – اهمیت بیشتری پیدا کرده است.

مدیریت سطح حمله چیست؟

مدیریت سطح حمله، کشف، نظارت، ارزیابی، اولویت‌بندی و رفع مداوم بردارهای حمله در زیرساخت‌های فناوری اطلاعات سازمان است.

در حالی که شبیه به کشف دارایی یا مدیریت دارایی است که اغلب در راه‌حل‌های بهداشتی فناوری اطلاعات یافت می‌شود، تفاوت اساسی در مدیریت سطح حمله این است که از دیدگاه مهاجم به کشف تهدید و مدیریت آسیب‌پذیری می‌پردازد. با این کار، سازمان مجبور می‌شود تا ریسک‌های ناشی از دارایی‌های شناخته‌شده و همچنین اجزای ناشناخته و سرکش را شناسایی و ارزیابی کند.

سطح حمله چیست؟

سطح حمله به شبکه به هم پیوسته‌ای از دارایی‌های فناوری اطلاعات اشاره دارد که می‌تواند توسط یک مهاجم در طول یک حمله سایبری مورد بهره‌برداری قرار گیرد. به طور کلی، سطح حمله یک سازمان شامل چهار مؤلفه اصلی است:

1. دارایی‌های لوکال: دارایی‌هایی که در محل قرار دارند، مانند سرورها و سخت‌افزارها.
2. دارایی‌های ابری: هر دارایی که از ابر برای عملیات یا تحویل استفاده می‌کند، مانند سرورهای ابری، بارهای کاری ابری، برنامه‌های SaaS یا پایگاه‌های داده میزبانی‌شده در ابر.
3. دارایی‌های خارجی: یک سرویس آنلاین خریداری‌شده از یک فروشنده یا شریک خارجی که داده‌های شرکت را ذخیره و پردازش می‌کند یا با شبکه سازمانی یکپارچه می‌شود.
4. شبکه‌های وابسته: شبکه‌هایی که توسط بیش از یک سازمان به اشتراک گذاشته می‌شوند، مانند آن‌هایی که توسط یک شرکت هولدینگ در صورت ادغام یا تملک، مالکیت دارند.

توجه به این نکته مهم است که سطح حمله سازمان با گذر زمان تکامل می‌یابد زیرا دستگاه‌ها به طور مداوم افزوده می‌شوند، کاربران جدید معرفی می‌شوند و نیازهای کسب و کار تغییر می‌کنند. به همین دلیل، سازمان‌ها باید به طور مداوم همه دارایی‌ها را نظارت و ارزیابی کنند و آسیب‌پذیری‌ها را پیش از بهره‌برداری توسط مجرمان سایبری شناسایی کنند.

ارزش مدیریت سطح حمله

با فرض نگرش مهاجم و تقلید از ابزارهای آن‌ها، سازمان‌ها می‌توانند دید خود را در سراسر بردارهای حمله احتمالی بهبود بخشند و بدین ترتیب، قادر به اتخاذ گام‌های هدفمند برای بهبود وضعیت امنیتی با کاهش ریسک مرتبط با برخی دارایی‌ها یا کاهش سطح حمله شوند. یک ابزار مدیریت سطح حمله مؤثر می‌تواند به سازمان‌ها کمک کند تا:

- کشف، بازبینی و رفع خودکار دارایی‌ها
- نقشه‌برداری از همه دارایی‌ها به صورت پیوسته
- شناسایی سریع و غیرفعال کردن دارایی‌های سایه و سایر دارایی‌های ناشناخته قبلی
- حذف آسیب‌پذیری‌های شناخته‌شده مانند رمزهای عبور ضعیف، پیکربندی‌های نادرست و نرم‌افزارهای قدیمی یا بدون پچ

عملکردهای اصلی مدیریت سطح حمله

پنج عملکرد اصلی برای استراتژی مؤثر مدیریت سطح حمله وجود دارد:

مرحله 1: کشف

در این مرحله اولیه، سازمان‌ها تمامی دارایی‌های دیجیتال را در سطح حمله داخلی و خارجی شناسایی و نقشه‌برداری می‌کنند. در حالی که راه‌حل‌های قدیمی ممکن است قادر به کشف دارایی‌های ناشناخته، سرکش یا خارجی نباشند، یک راه‌حل مدرن مدیریت سطح حمله ابزارهای مورد استفاده توسط تهدیدگران را برای پیدا کردن آسیب‌پذیری‌ها و ضعف‌های داخل محیط فناوری اطلاعات تقلید می‌کند. این امر دید کلی به سطح حمله را بهبود می‌بخشد و اطمینان می‌دهد که سازمان هر دارایی که به‌عنوان بردار حمله استفاده شود، نقشه‌برداری کرده است.

مرحله 2: آزمایش

سطح حمله به طور مداوم تغییر می‌کند زیرا دستگاه‌های جدید متصل می‌شوند، کاربران اضافه می‌شوند و کسب‌وکار توسعه می‌یابد. بنابراین، مهم است که ابزار قادر به انجام نظارت و آزمایش مداوم سطح حمله باشد. یک راه‌حل مدرن مدیریت سطح حمله دارایی‌ها را به صورت 7/24 بازبینی و تحلیل می‌کند تا از معرفی آسیب‌پذیری‌های جدید امنیتی جلوگیری کند، شکاف‌های امنیتی را شناسایی کند و پیکربندی‌های نادرست و سایر ریسک‌ها را از بین ببرد.

مرحله 3: زمینه

در حالی که هر دارایی می‌تواند به‌عنوان یک بردار حمله عمل کند، اما همه اجزای فناوری اطلاعات ریسک یکسانی ندارند. یک راه‌حل پیشرفته مدیریت سطح حمله تحلیل سطح حمله را انجام می‌دهد و اطلاعات مربوط به دارایی در معرض و زمینه آن در محیط فناوری اطلاعات را فراهم می‌کند. عواملی مانند زمان، مکان و نحوه استفاده از دارایی، مالک دارایی، آدرس IP و نقاط اتصال شبکه می‌تواند به تعیین شدت ریسک سایبری برای کسب‌وکار کمک کند.

مرحله 4: اولویت‌بندی

به دلیل اینکه راه‌حل مدیریت سطح حمله برای کشف و نقشه‌برداری تمامی دارایی‌های فناوری اطلاعات طراحی شده است، سازمان باید راهی برای اولویت‌بندی تلاش‌های رفع آسیب‌پذیری‌ها و ضعف‌های موجود داشته باشد. مدیریت سطح حمله امتیازات ریسک عملی و رتبه‌بندی‌های امنیتی را بر اساس تعدادی از عوامل، مانند میزان قابل مشاهده بودن آسیب‌پذیری، قابلیت بهره‌برداری از آن، میزان پیچیدگی رفع ریسک و سابقه بهره‌برداری ارائه می‌دهد. برخلاف تست نفوذ، رد تیم و سایر

روش‌های سنتی ارزیابی ریسک و مدیریت آسیب‌پذیری که ممکن است کمی موضوعی باشند، امتیازات مدیریت سطح حمله بر اساس معیارهای عینی است که با استفاده از پارامترهای سیستمی پیش‌تنظیم شده و داده‌ها محاسبه می‌شود.

مرحله 5: رفع

بر اساس مراحل خودکار در پنج مرحله اول برنامه مدیریت سطح حمله، کارکنان فناوری اطلاعات اکنون مجهز به شناسایی شدیدترین ریسک‌ها و اولویت‌بندی رفع هستند. از آنجایی که این تلاش‌ها اغلب توسط تیم‌های فناوری اطلاعات انجام می‌شود، و نه حرفه‌ای‌های امنیت سایبری، مهم است که اطمینان حاصل شود که اطلاعات در سراسر هر عملکرد به اشتراک گذاشته می‌شود و همه اعضای تیم بر روی عملیات امنیتی هماهنگ هستند.

چگونه سازمان شما می‌تواند خطرات سطح حمله را کاهش دهد؟

برای شناسایی و متوقف کردن مجموعه رو به رشد تاکتیک‌های دشمنان، تیم‌های امنیتی نیاز به دید 360 درجه از سطح حمله دیجیتال خود دارند تا تهدیدات را بهتر شناسایی کرده و از شرکت خود دفاع کنند. این نیاز به دید پیوسته از تمام دارایی‌ها دارد، از جمله شبکه‌های داخلی سازمان، حضور آنها در خارج از فایروال و آگاهی از سیستم‌ها و نهادهایی که کاربران و سیستم‌ها با آنها در تعامل هستند.

همانطور که سازمان‌ها به سمت دیجیتالی شدن پیش می‌روند، ممکن است نگهداری دید به سطح حمله گسترده‌تر دشوارتر شود. بارهای کاری ابری، برنامه‌های SaaS، میکروسرویس‌ها و سایر راه‌حل‌های دیجیتالی، پیچیدگی بیشتری به محیط فناوری اطلاعات افزوده‌اند و شناسایی، بررسی و پاسخ به تهدیدات را چالش‌برانگیزتر کرده‌اند.

RiskIQ Illuminate شرکت CrowdStrike با پلتفرم ®CrowdStrike Falcon یکپارچه شده است تا به طور یکپارچه تل‌متری نقاط انتهایی داخلی را با پتابایت‌های داده‌های اینترنتی خارجی که در طول بیش از یک دهه جمع‌آوری شده است، ترکیب کند. افزودن هوش اینترنتی بر روی داده‌های نقاط انتهایی در یک مکان، زمینه مهمی را برای وقایع داخلی فراهم می‌کند و به تیم‌های امنیتی کمک می‌کند تا بفهمند دارایی‌های داخلی چگونه با زیرساخت‌های خارجی تعامل دارند تا بتوانند حملات را مسدود کرده یا جلوگیری کنند و بدانند که آیا نفوذ شده‌اند یا خیر.

قابلیت‌ها و مزایای اصلی RiskIQ Illuminate شامل:

1. تسریع تشخیص و پاسخ: توانمندسازی تیم امنیتی با زمینه 360 درجه و دید بهبود یافته داخل و خارج از فایروال برای بهتر دفاع کردن از شرکت در برابر جدیدترین تهدیدات، مانند نقض داده‌ها و حملات باج‌افزاری.
2. توانمندسازی همکاری: RiskIQ Illuminate به تیم‌های امنیتی سازمانی این امکان را می‌دهد که به طور یکپارچه در تحقیقات تهدید یا مشارکت در پاسخ به وقایع همکاری کنند، با افزودن دانش داخلی و هوش تهدید به نتایج تحلیل‌گر.
3. مدیریت پیشگیرانه سطح حمله دیجیتال: دید کامل به همه دارایی‌های خارجی و اطمینان از مدیریت و حفاظت آنها.

منبع سایت CrowdStrike

تهیه شده توسط تیم ترجمه TryHackBox

ما را به دوستانتان معرفی کنید .