تفاوت میان NOC و SOC

مرکز عملیات شبکه و مرکز عملیات امنیت چه تفاوتی با یکدیگر دارند؟

دنیای امنیت همانند دریای خروشانی پر تلاطم است و هر روزه شاهد تغییرات و پیشرفت‌های مختلفی است. حملات هکری و نفوذهای سال 2019 میلادی نشان دادند بسیاری از شرکت‌ها در برابر حملات سایبری آسیب‌پذیر هستند و متاسفانه برخی دیگر نسبت به پروتکل‌ها و خط‌مشی‌های امنیتی بی تفاوت هستند. امروزه دیگر صحبت از نصب یک ضدویروس ساده یا دیوارآتش در میان نیست و شرکت‌ها به چیزی فراتر از نصب چند ابزار ساده یا وصله‌های مربوطه نیاز دارند. پیشرفت‌های انجام شده در دنیای زیرزمینی هکرها پر شتاب است، به همین دلیل شرکت‌ها مجبور هستند به سراغ مفاهیم تخصصی‌تری همچون مرکز عملیات امنیت و مرکز عملیات شبکه بروند. دو مفهوم کاربردی که قصد داریم در این مقاله به معرفی آن‌ها بپردازیم.

مرکز عملیات امنیت (SOC) و مرکز عملیات شبکه (NOC) دو مفهوم نزدیک به یکدیگر هستند که شباهت‌ها در برخی موارد زیاد است.

مرکز عملیات امنیت (SOC) چیست؟

مرکز عملیات امنیت مجموعه‌ای متمرکز است که مسئولیت پیگیری اتفاقات و حوادث امنیتی به وجود آمده در سازمان‌ها را عهده‌دار است. این مرکز با هدف تشخیص و واکنش سریع در برابر حملات امنیتی طراحی می‌شود که با استفاده از یک کنسول مرکزی، اتفاقاتی که در یک شبکه در حال انجام است را نشان می‌دهد. مرکز عملیات امنیت ظرفیت بالایی در نظارت و مدیریت بلادرنگ بر جنبه‌های مختلف امنیتی دارد و قادر است تمامی اتفاقات امنیتی را شناسایی و اولویت‌بندی کرده و سطح مخاطرات و خطراتی که پیرامون دارایی‌ها قرار دارد را تشخیص دهد. مرکز عملیات امنیت می‌تواند راه‌حل‌های درستی هماهنگ با هر رخداد پیشنهاد داده و راه‌حل‌ها را اجرایی کند. برخی موارد دو اصطلاح مرکز عملیات امنیت و مرکز عملیات شبکه دو مفهوم یکسان تعبیر می‌شوند، زیرا وجوه تشابه زیادی با یکدیگر دارند، در حالی که این‌گونه نیست و تفاوت‌هایی وجود دارد. مرکز مدیریت شبکه (NOC) به منظور کنترل ترافیک و مدیریت عملکرد و تنظیمات شبکه ارتباطی پایه‌ریزی می‌شود، در حالی که مرکز عملیات امنیت مسئولیت پیگیری اتفاقات امنیتی، مدیریت مخاطرات و پاسخ‌گویی به اتفاقات امنیتی را عهده‌دار است. در حقیقت این مرکز با هدف محافظت از اطلاعات سازمانی تاسیس می‌شود. این مرکز قادر است بر زیرساخت‌ها و خدمات الکترونیکی نظارت کاملی داشته باشد. از ویژگی‌های شاخص یک مرکز عملیات امنیت می‌توان تشخیص سریع روخدادهای امنیتی، پاسخ‌گویی سریع و موثر به رخدادهای امنیتی و تامین امنیت شبکه در برابر حملات سایبری، ارزیابی دقیق رخدادهای امنیتی، کم کردن آثار بر جای مانده از یک حمله امنیتی، بررسی امنیتی مستمر ترافیک شبکه به لحاظ شناسایی ترافیک‌های غیر عادی، تحلیل و ارزیابی مخاطرات اثربخش روی داده‌های تحت شبکه، بهبود امنیت و پایداری زیرساخت‌ها داده‌ای با اتکا بر محافظت از بانک‌های اطلاعاتی، ترافیک بسته‌های اطلاعاتی و داده‌های مشتریان، پیاده‌سازی یک مدیریت درست بر وصله‌های امنیتی و چرخه تامین اشاره کرد.

مرکز عملیات شبکه چیست؟

مرکز عملیات شبکه (NOC) سرنام Network Operation Center مسئولیت نظارت بر عملکرد و دسترس‌پذیری شبکه و آنلاین بودن سرویس‌ها را عهده‌دار است. این مرکز مشکلات مرتبط با زیرساخت فناوری‌اطلاعات (پایگاه‌های داده‌ای، سرورها، ماشین‌های مجازی) را شناسایی و برطرف می‌کند. اگر سایت‌ها، برنامه‌های کاربردی، سرورها یا حتا خود شبکه با خرابی همراه شوند، مرکز عملیات شبکه مسئولیت شناسایی و برطرف کردن مشکلات را عهده‌دار است. از مهم‌ترین مسئولیت‌های مرکز عملیات شبکه می‌توان به نظارت مستمر و ارزیابی دقیق عملکرد شبکه، ارائه گزارش در ارتباط با وضعیت موجود و پیشنهاداتی در ارتباط با بهبود عملکرد، پاسخ به موقع در ارتباط با حوادثی که باعث قطعی شبکه می‌شود، برنامه‌ریزی برای افزایش ظرفیت و اعمال تغییرات در بخش‌های مختلف شبکه اشاره کرد. مرکز عملیات شبکه توسط یک اتاق کنترل مرکزی فعالیت می‌کنند. مرکزی که تمام زوایای عملکرد آنلاین شبکه یک شرکت کنترل و ویرایش می‌کند.

چه تفاوتی میان این دو مرکز وجود دارد؟

یک متخص مرکز عملیات شبکه باید در ارتباط با مهندسی شبکه، برنامه‌های و سامانه‌های تحت شبکه تجربه کافی داشته باشد، در حالی که یک متخصص عملیات امنیت بیشتر به مهارت‌های مهندسی امنیت نیاز دارد. مرکز عملیات امنیت روی تهدیدات هوشمند متمرکز است، اما در نقطه مقابل مرکز عملیات شبکه روی حل مشکلات طبیعی و خرابی سامانه‌های متمرکز است. به همین دلیل است که دو مرکز فوق مکمل یکدیگر هستند و هر یک وظیفه دیگری را تکمیل می‌کند. مرکز عملیات شبکه مسئولیت نگه‌داری و حصول اطمینان از درست کار کردن شبکه و زیرساخت سازمان را عهده‌دار است، در حالی که مرکز عملیات امنیت مسئولیت رسیدگی به حملات هکری و مشکلات امنیتی و محافظت از شبکه را عهده‌دار است. در برخی موارد فعالیت‌های این دو مرکز با یکدیگر هم‌گرایی دارد که از آن جمله می‌توان به نظارت بر عملیات شبکه، عیب‌یابی شبکه، تشخیص نفوذ به شبکه، مدیریت گزارش‌ها و رخدادها، پیگیری و ردیابی بسته‌های اطلاعاتی، نظارت بر عملیات شبکه اشاره کرد. در مقابل برقراری و حصول اطمینان از عملکرد درست زیرساخت، مسئولیت عملیاتی سازی شبکه بر عهده مرکز عملیات شبکه است، در حالی که مدیریت رخدادهای امنیتی جفظت محافظت از شبکه، مدیریت و ارزیابی مخاطرات امنیتی، مدیریت یکپارچه رخدادهای امنیتی، واکنش در محل به حوادث، شناسایی روش‌های نفوذ و تقلب در شبکه، تحلیل و بررسی حوادث از مسئولیت‌های مرکز امنیت شبکه است.

تاریخ انتشار:

21 دی 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/16448/%E2%80%8C%E2%80%8C%D9%85%D8%B1%DA%A9%D8%B2-%D8%B9%D9%85%D9%84%DB%8C%D8%A7%D8%AA-%D8%B4%D8%A8%DA%A9%D9%87-%D9%88-%D9%85%D8%B1%DA%A9%D8%B2-%D8%B9%D9%85%D9%84%DB%8C%D8%A7%D8%AA-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%DA%86%D9%87-%D8%AA%D9%81%D8%A7%D9%88%D8%AA%DB%8C-%D8%A8%D8%A7-

%DB%8C%DA%A9%D8%AF%DB%8C%DA%AF%D8%B1-
%D8%AF%D8%A7%D8%B1%D9%86%D8%AF%D8%9F