فهرست مطالب

1

2

6

7

8

CHAPTER 1

- **آشنایی با مرکز عملیات امنیت (SOC)**

فصل اول

آشنایی با مرکز عملیات امنیت (SOC)

مرکز عملیات امنیت (Security Operations Center) شامل مجموعه‌ای هماهنگ و مدیریت‌شده از ساختار و سیاست‌های امنیتی شبکه می‌باشد که به منظور یکپارچگی، مدیریت و نظارت سایر تمهیدات امنیتی موجود در هر سازمان، راه اندازی می‌شود.

۱.۱ مقدمه

در تمامی مشاغل و صنعت‌ها نیاز به کنترل و پایش وجود دارد؛ تا در هنگام بروز مشکلات به راحتی بتوان آن را حل و مسبب ایجاد مشکل را پیدا کرد.

در همه‌ی صنعت‌ها نیز این کار توسط یک سیستم مکانیزه شامل ابزارها و نیروهای انسانی انجام می‌گیرد. ازاین‌رو فناوری اطلاعات به‌عنوان یکی از صنعت‌هایی که بسیار رو به رشد و همه‌گیر می‌باشد نیازمند کنترل دقیق است.

ازآنجایی‌که تمام نقاط جهان از طریق بستر اینترنت باهم در ارتباط هستند و تمامی سازمان‌ها و نهادها نیز دارای شبکه‌های کامپیوتری هستند، خطرات و تهدیدات نیز افزایش پیدا می‌کند.

همان‌گونه که این خطرات زیرساخت‌های سازمان‌ها را تهدید می‌کند، تأثیرات منفی و مخربی روی کاربران و مشتریان نیز می‌گذارد.

به منظور جلوگیری و مقابله با این تهدیدات و مشکلات، در تمامی زیرساخت‌ها کنترل دقیق و پایش در تمام سطوح باید انجام گیرد.

این کنترل‌ها در سطوح برنامه‌های کاربردی، شبکه، ترافیک‌های ورودی و خروجی، درخواست‌های کاربران و... انجام می‌گردد.

از چندین سال قبل بحث پیاده‌سازی این‌گونه سامانه‌ها تحت عنوان مراکز عملیات امنیت (SOC[1]) مطرح گردید. مرکز عملیات امنیت که از چندین بخش تشکیل‌شده است تمامی وظایف کنترلی و مقابله با تهدیدات در فضای سایبر را بر عهده دارد.

۱.۲ آشنایی با SOC

مرکز عملیات امنیت شبکه، (SOC) مکانی جهت مانیتورینگ و کنترل ۲۴ ساعته ورود و خروج اطلاعات در شبکه می‌باشد. به طورکلی هر مرکز SOC به سه سطح عمده تقسیم می‌شود که هر یک وظایف خاصی را بر عهده دارند. این سطوح عبارت‌اند از:

سطح یکم، نقطه تماسClient ها و مسئول پاسخ‌گویی به اخطارهای دریافتی از Clientهاست. در این سطح به کلیه اخطارهایی که از پیچیدگی پایین‌تری برخوردارند، پاسخ داده می‌شود.

سطح دوم، در حقیقت مکمل سطح یکم است و مسئول پاسخ‌گویی به مشکلات پیچیده‌تر در سیستم‌های امنیتی شبکه می‌باشد. برای اخطارهایی که از اهمیت بالایی برخوردارند، سیستم‌های سطح دوم به‌طور کامل درگیر می‌شوند.

سطح سوم، در این سطح کارشناسان ارشد و مشاوران امنیتی شبکه قرار دارند. این سطح در حقیقت پشتیبان دو سطح پایین‌تر است. درصورتی‌که به اشکالات امنیتی در دو سطح پایین پاسخ داده نشود، کارشناسان و سیستم‌های این سطح، درگیر می‌شوند. کلیه تدابیر امنیتی و مدیریت امنیت شبکه، در این سطح اندیشیده می‌شود.

در طراحی مراکز عملیات امنیت، متدولوژی‌های مختلفی مطرح می‌باشد. با این‌حال پایه همه متدولوژی‌ها بر اساس ترکیب تکنولوژی، نیروی انسانی، فرآیندها در هسته فعالیت این مرکز امنیتی و احاطه آن توسط فرآیندهای اجرایی می‌باشد. این فرآیندها شامل برنامه‌ریزی، طراحی، پیاده‌سازی، عملیاتی نمودن و توسعه مرکز عملیات امنیت می‌باشد.

لایه بعدی در طراحی مرکزSOC، شامل ابزارها و معیارهایی است که از طریق آن‌ها خدمات ارائه شده ارزیابی می‌گردند. این ابزارها و معیارها شامل چشم‌انداز، منابع، زمان، هزینه، ارتباطات و ریسک‌های موجود درراه اندازی SOC می‌باشد.

---

۱ Security Operations Center

نکته قابل توجه در طراحی یکSOC، انعطاف‌پذیریِ متدولوژی طراحی آن است که به واسطه آن می‌توان برای هر یک از مشتریان مطابق سرویس‌های مورد نیازشان راه‌حل خاصی برای مدیریت امنیت ارتباطات ارائه نمود.

در هر یک از سطوح مطرح‌شده، ابزاری برای مدیریت سیستم‌های امنیتی در نظر گرفته می‌شود. این ابزارها، امنیت شبکه را از دو دیدگاه درون سازمانی و برون‌سازمانی موردبررسی قرار می‌دهند. برای این منظور، هرSOC دارای یک سری تجهیزات در داخل شبکه و یک سری تجهیزات در خود مرکز می‌باشد. همه سرویس‌هایی که از مراکز SOC ارائه می‌گردند، مانیتورینگ و مدیریت‌شده هستند. دیگر سرویس‌هایی که از طریق این مراکز قابل‌ارائه می‌باشند، سرویس‌های پیشرفته‌ای به شرح زیر می‌باشد:

- توسعه سیاست‌های امنیتی
- آموزش مباحث امنیتی
- طراحی دیواره‌های آتش
- پاسخگویی آنی (CERT[۲])
- مقابله با خطرات

سرویس‌هایی که از طریق این مراکز ارائه می‌گردند، عبارت‌اند از سرویس‌های مدیریت‌شده‌ای که از تجهیزات و ارتباطات مرکز SOC محافظت می‌نمایند. این سرویس‌ها از متدولوژی و ابزارهای نرم‌افزاری و سخت‌افزاری قدرتمندی برای مدیریت امنیت استفاده می‌نمایند. اجزای سخت‌افزاری که در شبکه‌ها توسط سیستم‌های مدیریت‌شده برای اعمال سیاست‌های امنیتی مورداستفاده قرار می‌گیرند، عبارت‌اند از: سیستم‌های کشف و رفع حملات(Intrusion Detection and Prevention System) ، سیستم‌های فایروال و سیستم‌های مدیریت امنیت در شبکه‌های خصوصی مجازی.

۱.۳ معماری SOC

SOC بستری است که سرویس‌های کشف و واکنش را در مقابل حوادث امنیتی فراهم می‌آورد. طبق این تعریف می‌توان پنج نوع عملیات مختلف را در حوزه SOC در نظر گرفت:

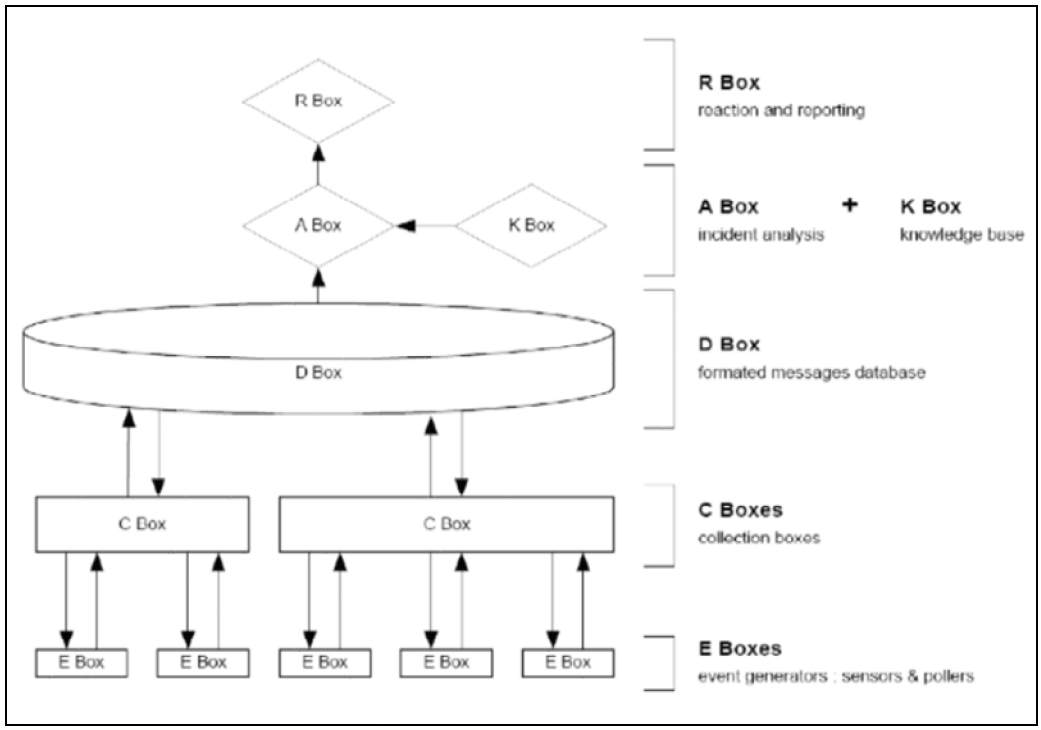
- ثبت رخداد امنیتی
- جمع‌آوری

---

۲ Computer emergency response team

- ذخیره‌سازی
- تحلیل
- واکنش

جهت آسان‌تر شدن مفهوم، معماری SOC را با کادرهایی نشان می‌دهیم که هر یک از این کادرها، گروه عملیاتی از ماژول‌هایی است که عملیات خاصی را انجام می‌دهند:



شکل ۱.۱ معماری مرکز عملیات امنیت

درمعماری SOC چیستی اطلاعات جمع‌آوری‌شده و چگونگی تحلیل، پردازش و ارتباط این اطلاعات مشخص می‌شود. ایجاد یک SOC با معماری مناسب مستلزم موارد ذیل است:

۱. تعیین دارایی‌ها
۲. تصمیم‌گیری در مورد اطلاعات امنیتی که بایستی جمع‌آوری گردند
۳. تعیین اطلاعات مرتبط و قابل‌تحلیل

۴. تحلیل پدیده‌های امنیتی مرتبط

۵. از کارشناسان امنیتی به نحو شایسته بهره گرفته شود.

۱.۴ نتیجه‌گیری

مراکز عملیات امنیت (SOC) یک مجموعه کاملاً مکانیزه و پیشرفته می‌باشند که دارای یک معماری استاندارد و کامل می‌باشند که جهت مانیتورینگ ۲۴ ساعته پیاده‌سازی می‌شوند.

در این معماری ساخت‌یافته هر یک از اعضا (کارشناس) در یک بخش یا گروه عملیاتی خاص به همراه یکسری تجهیزات و ابزارها کار می‌کنند.

به‌طورکلی مراکز عملیات امنیت به سه سطح نقطه تماس Clientها، مسئول پاسخ‌گویی به مشکلات و اخطارها و کارشناسان ارشد امنیتی تقسیم می‌گردند.

۱.۵ سؤالات فصل اول

۱. مرکز عملیات امنیت (SOC) را به همراه سطوح مختلف آن تعریف نمایید؟

۲. انواع سرویس‌های پیشرفته موجود در SOC را شرح دهید؟

۳. معماری یک مرکز عملیات امنیت (SOC) را توضیح دهید؟

۴. ایجاد یک مرکز عملیات امنیت موفق مستلزم رعایت چه مواردی می‌باشد؟

۵. انواع گروه‌های عملیاتی را در معماری SOC نام ببرید؟

۱.۶ منابع

[1] http://www.sans.org/event/security-operations-center-summit-2015
[2] http://www.secureworks.com/it_security_services/advantage/soc/
[3] Security Operation Center Concepts & Implementation by Renaud Bidou
[4] Network Intrusion Detection by Stephen Northcutt, Judy Novak
[5]http://h71028.www7.hp.com/enterprise/downloads/software/ESP-BWP014-052809-09.pdf
[6]http://www.ey.com/GL/en/Services/Advisory/EY-cybersecurity-security-operations-centers
[7]https://www.giac.org/paper/gslc/8336/security-operations-centre-soc-utility-organization/138736