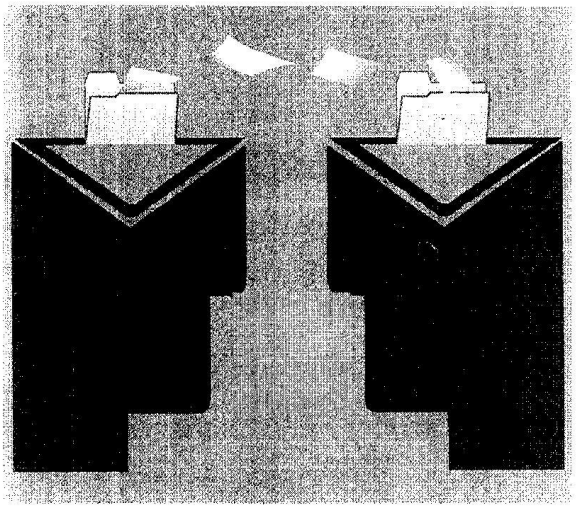
پیاده‌سازی مرکز عملیات امنیت SOC (Security Operation Center)

نگارش: علی ثاقب موفق ـ رئیس گروه امنیت شبکه، لیسانس کامپیوتر ـ نرم‌افزار و فوق‌لیسانس مهندسی فناوری اطلاعات از دانشگاه امیرکبیر



امنیت، از نیازهای اصلی انسان و بالطبع همه ابداعات و مصنوعات نرم‌افزاری اوست. جدیدترین این ابداعات شامل کامپیوتر، شبکه و اینترنت می‌شود که ضمن دیجیتالی کردن اطلاعات، باعث مبادله ساده آن نیز شده است، بنابراین امنیت آن اهمیت ویژه‌ای دارد لذا شایسته است جایگاه و ساختاری برای آن در نظر گرفته شود.

این جایگاه در واقع مکان و سایتی است که وظیفه آن برقراری امنیت در شبکه یک سازمان بوده و نام آن، مرکز عملیات امنیت (SOC) است. مرکز عملیات امنیت شبکه، مکانی برای مانیتورینگ و کنترل دائم وضعیت شبکه به لحاظ ایمنی است که عموماً در سه سطح و با کمک ابزارهای متنوع امنیتی انجام می‌شود.

در سطح اول، کارشناسان گروه امنیت شبکه به مسائل و مشکلات امنیتی مربوط به Clientهای کاربران پاسخ داده و مسئولیت رفع مشکلات جزئی مربوط به امنیت سیستم‌های کاربران را عهده‌دار می‌باشند. در این سطح به اخطارهای دریافتی از Clientها که از پیچیدگی کمتری برخوردار هستند پاسخ داده می‌شود.

در سطح دوم، کارشناسان سطح بالاتر امنیت شبکه، پاسخگوی مشکلات ناشی از سیستم‌های امنیتی شبکه و نرم‌افزارهای مربوطه می‌باشند و چنانچه در نرم‌افزار امنیتی شبکه مشکلی ایجاد شود، کارشناسان مذکور موضوع را بررسی و نسبت به رفع مشکل اقدام می‌نمایند. سیستم‌های این سطح، برای اخطارهای پراهمیت، کاملاً درگیر می‌شوند.

در سطح سوم، کارشناسان ارشد و مشاوران باتجربه امنیت شبکه، سیاست‌های امنیت شبکه سازمان را وضع نموده و کلیه تدابیر امنیتی و مدیریتی شبکه را مشخص و تبیین می‌نمایند. این سطح در واقع پشتیبان دو سطح قبلی است.

با توجه به موارد فوق، واضح است که عموماً در یک مرکز امنیت شبکه، تکنولوژی، نیروی انسانی و فرآیندها، از بخش‌های اصلی آن به شمار می‌رود و نکته قابل تأمل، این است که برای هر یک از کاربران و مشتریان، مطابق با سرویس‌های موردنیازشان، راه‌حل خاصی جهت مدیریت امنیت شبکه ارائه می‌گردد. این موضوع با کمک ابزارهایی انجام می‌شود که بایستی از دیدگاه درون سازمانی و برون سازمانی مورد بررسی قرار گیرند. گروه کارشناسان امنیت شبکه، اقدامات فوق را در SOC طبق موضوعات چهارگانه: فایر وال‌ها (Firewall) ـ شبکه خصوصی مجازی (VPN) ـ سیستم کشف حملات (IDS) و آنتی‌ویروس (Antivirus)ها انجام داده و سپس براساس آنها سرویس‌های پیشرفته (توسعه سیاست‌های امنیتی، آموزش مباحث امنیتی، طراحی دیواره‌های آتش، پاسخگویی آنی، مقابله با خطرات امنیتی و پیاده‌سازی آن) را ارائه می‌دهند.

بدیهی است برای تحقق این امور نیاز به ابزارهای نرم‌افزاری و سخت‌افزاری است که برخی ابزارهای سخت‌افزاری به کار رفته آن عبارتند از: سیستم‌های کشف و رفع حملات (Intrusion Detection System) سیستم‌های فایروال و سیستم‌های مدیریت امنیت در شبکه‌های خصوصی مجازی (VPN).

سرویس‌های مدیریت شده در SOC شامل: دیواره آتش یا firewall، سیستم‌های تشخیص حملات یا IDS، امکان فیلتر کردن محتوا، امکان تشخیص ویروس و سرویس‌های AAA

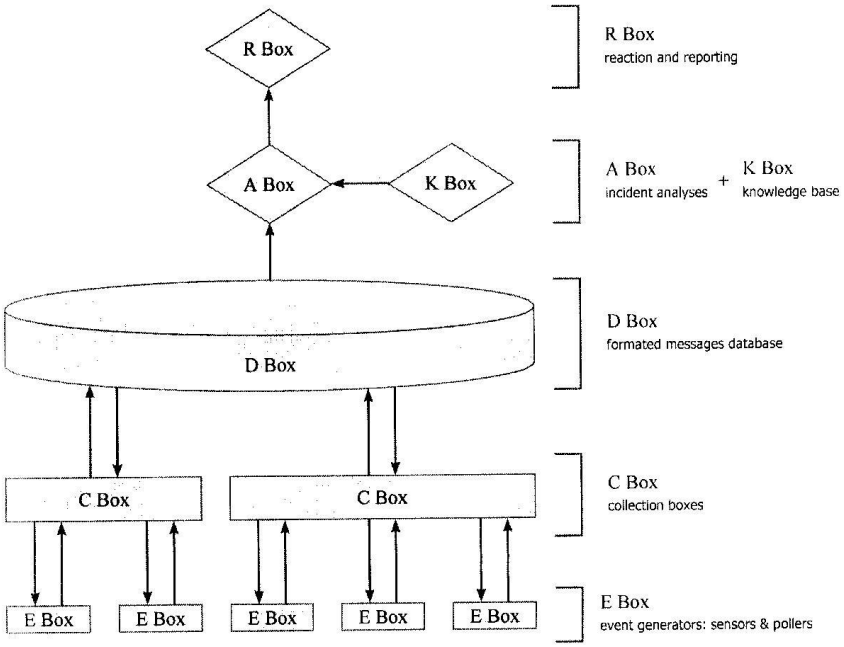
هستند، همچنین در مرکز عملیات امنیت، حملات به شبکه در سه رده verification (حصول اطمینان از بخش‌هایی که کنترل مستقیم بر روی آنها وجود ندارد) و Visibility (مانیتورینگ امنیت تجهیزات شبکه) و Vulnerability (به‌روز رسانی تجهیزات به کار رفته در این رده به محض نصب و راه‌اندازی) بررسی می‌شوند.

حال اگر بخواهیم SOC را به لحاظ فرآیندی بررسی نماییم باید بگوییم که مرکز عملیات امنیت (SOC) از پنج ماجول ساخته شده است، که عبارتند از: تولیدکننده‌های رویداد، تجمیع‌کننده‌های رویداد، بانک اطلاعاتی پیام‌ها، موتورهای تحلیل و نرم‌افزار مدیریت واکنش و مسأله اصلی در SOC، اجتماع این ماجول‌ها است. مرکز عملیات امنیت به منظور فراهم نمودن سرویس کشف و واکنش به حوادث امنیتی است. شکل زیر ارتباط بین این ماجول‌ها را در یک مرکز SOC نمایش می‌دهد. برای سادگی کار از boxهای ماجول استفاده شده است.

در شکل (۱) E Box مربوط به بخش‌های تولیدکننده رویداد، C Box مربوط به قسمت‌های تجمیع رویدادها، D Box بانک اطلاعاتی پیام‌های فرمت‌بندی شده، A Box برای تحلیل حوادث، K Box برای استفاده از دانش و نهایتاً R Box به منظور تهیه گزارش و همچنین واکنش به رویدادها است.

به عنوان مثال، مرکز JSOC یکی از بزرگ‌ترین مراکز مونیتورینگ ژاپن است که چشمان خود را ۲۴ ساعته بر روی دروازه‌های امنیتی باز نگه می‌دارد و شامل firewall و IDS و سیستم‌های عملیاتی و شبکه‌ها است و آنها را از خطرات خارجی مثل ویروس‌های کامپیوتری، هکرهای مجازی و Wormها محافظت می‌کند. در اینجا، تحلیل ساده log فایل firewall و هشدارهای IDS دسترسی‌های تعریف نشده و نامعتبر خطرناک را که به حوادث جدی ختم می‌شود، پیش‌بینی می‌کند. با استفاده از STP (Soc Technology Platform) یک تحلیل هماهنگ در الگوریتم‌های معین روی مقادیر زیادی از هشدارهای IDS و Logهای فایروال انجام می‌دهیم. این کار به منظور حذف کشف‌نشده‌ها و کاهش دسترسی‌های نامعتبر است. تحلیلگر انسانی، هر رویداد نامعتبر را که توسط STP کشف شده را دوباره تحلیل می‌کند و نهایتاً هرگونه موضع کشف‌نشده‌ای را حذف می‌کند. در این روش، تنها دسترسی‌های نامعتبر به Client گزارش می‌شود. لذا با استفاده از ترکیب STP و تحلیل انسانی به سمت بهبود کارایی در کشف دسترسی‌های غیرمجاز پیش می‌رویم.

لذا ایجاد یک چنین سیستم امنیتی با اطمینان بالا (SOC)، مستلزم پرسنل کارآمد، تجهیزات نرم‌افزاری و سخت‌افزاری متناسب بدون وابستگی به محصول خاصی است که طبق استاندارد (BS۷۷۹۹) ISMS قابل پیاده‌سازی خواهد بود.



شکل (۱) معماری SOC