9th SASTech Symposium on Advances in Science & Technology (2014)
نهمین سمپوزیوم پیشرفت های علوم و تکنولوژی
مشهد- ۱۳ آذر- ۱۳۹۳
کمیسیون دوم: همایش ملی علوم و مهندسی کامپیوتر
بامحوریت
امنیت ملی و توسعه پایدار
برگزارکننده: موسسه آموزش عالی خاوران
www.khi.ac.ir

مرکز عملیات امنیت و ضرورت ایجاد آن در ایران

محمد صادق مقدس[۱]،دکتر مرتضی الیاسی [۲]

۱- دانشجوی کارشناسی ارشد، موسسه آموزش عالی روزبهان، ساری، ایران

۲- عضو هیات علمی دانشگاه آزاد اسلامی واحد قائمشهر، قائمشهر، ایران

Sadegh.moghaddas@gmail.com

نام ارائه‌دهنده: محمد صادق مقدس

خلاصه

با گسترش روزافزون استفاده از ارتباطات و انتقال اطلاعات در بستر شبکه‌ها و اینترنت، حجم وسیعی از مبادلات تجاری و اداری، از این طریق صورت می‌پذیرد. امروزه سرویس‌های اینترنتی و تحت شبکه، به عنوان قابل‌اعتمادترین، سریع‌ترین و در دسترس‌ترین ابزارهای ارتباطی به شمار می‌روند. با توجه به اهمیت فوق العاده‌ای که شرکت‌های بزرگ به استفاده از چنین بسترهایی در اداره امور خود می‌دهند، جایگاه و اهمیت مقوله امنیت به وضوح مشخص است. مرکز عملیات امنیت، مرکزی با پایش ۲۴*۳۶۵ شبکه است که نمایی بلادرنگ از وضعیت امنیتی شبکه را فراهم کرده و تا حدی از بروز حادثه پیشگیری می‌کند و در صورت بروز حادثه، در سریع‌ترین زمان ممکن حادثه را تشخیص داده و تیم‌های امداد حوادث رایانه‌ای را در رفع حادثه یاری می‌کند. در این مقاله به توضیح عملکرد مرکز عملیات امنیت پرداخته و اهمیت ضرورت موضوع با توجه به جایگاه ویژه امنیت بررسی شده و در پایان به درجه امنیت در ایران می پردازیم.

کلمات کلیدی: مرکز عملیات امنیت، نفوذ، آسیب پذیری، تیم رسیدگی به حادثه، پایگاه داده آسیب پذیری

۱. مقدمه

ترکیب تکنولوژی‌های مختلف با هدف برآورده نمودن نیازمندی‌های کسب و کار، سازمان ها را با چالش‌هایی جدید روبرو نموده است، چرا که عموماً هیچ روش یا مکانیزمی با هدف جمع آوری، نرمال سازی، مرتبط سازی و اولویت‌بندی میلیون‌ها رخداد گزارش شده از سوی تکنولوژی‌ها و سامانه‌های مختلف وجود ندارد. در چنین وضعیتی استفاده از تکنولوژی‌های مختلف و نامتجانس جز افزایش سربار فعالیت‌های امنیتی سازمان، مضاعف شدن این فعالیت‌ها، ایجاد مدل‌های امنیتی ضعیف و عدم موفقیت فرایندهای ممیزی، نتیجه‌ای به همراه نخواهد داشت. در چنین وضعیتی، مرتبط سازی بلادرنگ وقایع مختلف (که توسط تجهیزات و ابزارهای مختلفی تولید شده است) و شناسایی یک حمله یا نفوذ مشخص، بسیار مشکل و عموما غیرممکن می‌باشد. علاوه بر این، تحلیل‌های پس از وقوع حوادث نیز بسیار کند انجام خواهند شد چرا که ترکیب اطلاعاتی که به روش‌های متفاوت در ابزارها و تجهیزات مختلف نگهداری می‌شوند.

مرکز عملیات امنیت[۱] (SOC)، دیدی بلادرنگ و جامع نسبت به وضعیت امنیت شبکه سازمان ایجاد می‌نماید. در واقع، این مرکز بواسطه اطلاع رسانی‌های اتوماتیک حوادث و وقایع، تولید گزارشات جزئی و کلی، پاسخ‌دهی اتوماتیک به حوادث و وقایع، رویکردی پیشگیرانه را در جهت مدیریت ریسک‌های امنیتی ایجاد خواهد نمود. همچنین، این مرکز، وقایع و حوادث را اولویت بندی می‌نماید، دارایی‌های متاثر شده از وقایع اتفاق افتاده را مشخص نموده و راهکارهای اصلاحی و یا پیشگیرانه را پیشنهاد داده و یا در مواردی از پیش تعیین شده، اجرا می‌نماید. این مرکز، با ارایه گزارشاتی در سطوح مختلف، نیازمندی‌های مربوط به فرایندهای ممیزی و همچنین ارزیابی بخشی از ریسک‌های عملیاتی زیرساخت شبکه را برآورده می‌نماید.

[1] Security Operation Center