عنوان مقاله:
توسعه تکنولوژی SIEM برای مقابله با تهدیدات APT

محل انتشار:
دومین همایش ملی پژوهش های کاربردی در علوم کامپیوتر و فناوری اطلاعات (سال: 1393)

تعداد صفحات اصل مقاله: 7

نویسندگان:
ندا علی نژاد - *دانشجوی کارشناسی ارشد، موسسه آموزش عالی روزبهان ساری*

مرتضی الیاسی - *عضو هیئت علمی دانشگاه آزاد اسلامی واحد قائمشهر*

خلاصه مقاله:
انواع مختلف حملات سایبری دهه ها است که در جهان به وقوع می پیوندد. منتها ضرب کند سال گذشته این یورش را به شکل بسیار خطرناکی صورت می گیرد. به طوری که شاهد یورش هایی هستیم که از سوی کشورهایی بر ضد به ملت های دیگر صورت می گیرد. از طرفی هم در قوانین جنگی و نیز اخلاق عرفی از حملات سایبری تقریباً هیچ صحبتی به میان نیامده است و برخلاف جنگ های متداول، هیچ مرزی برای این حملات مشخص نشده است. هیچ مقاوله نامه ای هم وجود ندارد که استانداردها این را در قوانین بین المللی برای چگونه انجام گرفتن یا نگرفتن چنین جنگ هایی قرار دهد. نگرانی عمده از ناحیه اینترنت این است که بیشتر، زیرساخت های اطلاعات دفاعی و اقتصادی را مقابل حملات سایبری آسیب پذیر کرده است. تهدیدات پیشرفت و مستمر که تحت عنوان APT شناخته می شوند امروز از مهم ترین چالش های امنیت فضای سایبر محسوب می شوند. در چنین شرایطی رصد و نظارت مستمر و همه جانبه بر فضای سایبر به منظور کشف این گونه فعالیت های بدخواهانه و پایش آن ها به منظور بررسی و شناسایی به هنگام، به عنوان ضرورتی اجتناب ناپذیر برای تأمین امنیت فضای سایبر محسوب می گردد. در این مقاله به نحوه شکل دهی SIEM به آن یک ابزار امنیتی قدرتمند برای مقابله با این تهدیدات پیچیده و مستمر پرداخته شده است. بدین منظور ابتدا برای مقدمه به طور مختصر تهدیدات APT را تعریف و چالش های موجود بررسی شده است و در ادامه تکنولوژی SIEM جدیدترین و به نحوه توسعه آن برای مقام تهدیدات APT پرداخته می شود .

کلمات کلیدی:
APTI ، SIEM ، لاگ، تهدید