عنوان مقاله:
پیاده سازی IDS/IPS به منظور امنیت در مسیریاب های شبکه بانک (مطالعه موردی بانک کشاورزی)

محل انتشار:
دومین کنفرانس بین المللی و سومین همایش ملی کاربرد فناوری های نوین در علوم مهندسی (سال: 1394)

تعداد صفحات اصل مقاله: 17

نویسندگان:
مجید نانکلی - *کارشناس مسؤل سیستم عامل بانک کشاورزی ایران*

رضا همایون زاده بائی - *کارشناس مسؤل زیرساخت و دیتاسنتر بانک کشاورزی ایران*

محمدرضا خنداخند - *کارشناس مسؤل شبکه بانک کشاورزی ایران*

خلاصه مقاله:
با عنایت به گستردگی شبکه بانک کشاورزی در سطح کشور بعنوان تنها بانک دارنده سیستم یکپارچه ، با اتصال تمام نقاطزیرمجموعه این بانک، شامل شعب، سرپرستی، صندوق های بیمه، کارگزاری ها و شرکت های تابعه به مرکز، اقدام به ثبت تراکنشهای مالی و غیر مالی خود بطور مستقل نماید. در این راستا بهکارگیری سیستمهای تشخیص و پیشگیری از نفوذ (IDS/IPS)که توانایی کشف، ثبت رویداد و حتی واکنش به حملات امنیتی را دارا میباشد به عنوان اصلی ترین راهکار معماری امنیت شبکهفناوری اطلاعات بانکها در این پروژه پژوهشی تعیین شد، همچنین با توجه به اینکه به کارگیری غیرصحیح سیستمهای تشخیص وپیشگیری از نفوذ، ریسک های عملیاتی در حوزه سرویس های فناوری اطلاعات سازمانها را، بدلیل انحراف در شناسایی ترافیک هاینرمال از غیرنرمال، بهمراه خواهد داشت، سفارشی سازی یک سیستم تشخیص نفوذ، متناسب با سرویس ها و سامانه های بانکی علاوهبر کاهش این ریسک ها، می تواند به امنیت بیشتر در حوزه بانکداری الکترونیک کمک نماید. در راه حل پیشنهادی، از سیستمتشخیص نفوذ Snort که قابلیت بهرمندی از یک زبان انعطاف پذیر برای تعریف قوانین ثبت وقایع می باشد استفاده می شود و درمرحله پیاده سازی سعی خواهد شد ضمن ارائه یک معماری پیشنهادی شبکه، سفارشی سازی سیستم Snort با در نظر گرفتنآسیب پذیری سامانه ها و سرویس های بانکداری اینترنتی، در شبکه نمونه بانکی (یکی از بانک های خصوصی کشور) انجام پذیرد ونهایتاً در این پروژه به منظور بررسی عملکرد و ارزیابی سیستم تشخیص نفوذ سفارشی شده، از مجموعه داده های Darpa1999 کهبهعنوان یک داده ی استاندارد برای ارزیابی سیستمهای تشخیص نفوذ پذیرفته شده استفاده می شود تا نتایج حاصل از تحلیل داده هایآزمایش، عملکرد سیستم تشخیص نفوذ Snort سفارشی شده برای سامانه های بانکی در مقایسه با سیستم Snort با تنظیماتپیش فرض را مشخص نماید.

کلمات کلیدی:
امنیت شبکه، نفوذ، تشخیص و پیشگیری از نفوذ، تشخیص مبتنی برامضاء، تشخیص مثبت اشتباه، تشخیص منفی اشتباه، شناسایی آسیب پذیری