عنوان مقاله:

طراحی مدل اجرای مرکز عملیات امنیت (SOC) در صنعت بانکداری

محل انتشار:

دوفصلنامه مدیریت بحران, دوره 12, شماره 0 (سال: 1402)

تعداد صفحات اصل مقاله: 31

نویسندگان:

سید زین العابدین حسینی – دانشجوی دکترای مدیریت فناوری اطلاعات، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران

منصور اسماعیل پور – دانشیار گروه مهندسی کامپیوتر، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران

علیرضا اسلامبولچی – استادیار، گروه مدیریت، واحد همدان، دانشگاه آزاد اسلامی، همدان، ایران

محمدرضا ربیعی مندجین – استادیار گروه مدیریت، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران

علیرضا امیرکبیری – استادیار گروه مدیریت، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران

خلاصه مقاله:

یکی از مهم ترین چالش های امنیتی در مراکز عملیات امنیت با الکترونیک، ناتوانی ذاتی اینترنت در مقابله با حملات است. این حملات به راحتی اجراشده و به صورت محلی یا از راه دور قابل کنترل می باشند. اکثر این حملات در رسیدن به اهداف اصلی حمله، موفق بوده و مهاجم را به خواسته های خود می رساند. علت این امر در این است که مکانیسم های زیادی برای راه اندازی حملات بر اساس مشخصات سرور قربانی وجود دارد، همین امر خود موجب می شود که نتوان یک راه حل دفاعی جامع در برابر حملات ارائه نمود. راهکارهای متعددی برای شناسایی و مقابله با حملات مزبور ارائه شده است که در این مقاله راهکار ترکیب الگوریتم انتخاب ویژگی ژنتیک و روش های یادگیری ماشین ازجمله الگوریتم درخت تصمیم، شبکه عصبی عمیق و KNN به صورت تلفیقی ارائه شده است. برای اعتبار سنجی راهکار ارائه شده، نتایج حاصل با سایر روش ها ازجمله روش های یادگیری ماشین و ترکیبی با سایر روش های بهینه سازی مورد مقایسه و ارزیابی شده است. در این پژوهش از ۱۰% مجموعه داده KDD Cup ۹۹ برای شبیه سازی استفاده شده است که ابتدا در مرحله پیش پردازش داده ها، مقادیر کلیه مشخصه ها به اعداد تبدیل و همچنین مقادیر مشخصه خروجی به دو مقدار صفر و یک تغییر داده شده است. نتایج حاصل از پژوهش نشان از دقت بالای راهکار ارائه شده برای تشخیص نفوذگران نسبت به سایر روش های اخیر در حدود ۵% است.

کلمات کلیدی:

مرکز عملیات امنیت, بانکداری الکترونیک, فرآیند کاوی, یادگیری ماشین