

عنوان مقاله:

ارابه یک الگوریتم مناسب برای پیش بینی حملات سایبری مبتنی بر یادگیری

محل انتشار:

دومین کنفرانس ملی مهندسی برق و کامپیوتر (سال: 1396)

تعداد صفحات اصل مقاله: 20

نویسندگان:

پروانه سلیمانی برایجانی - دانشجوی کارشناسی ارشد دانشگاه صنعتی مالک اشتر

علی جبار رشیدی - دانشیار دانشگاه صنعتی مالک اشتر

کوروش داداش تبار احمدی - استادیار دانشگاه صنعتی مالک اشتر

خلاصه مقاله:

امروزه حملات سایبری، به طور گسترده با استفاده از آسیب پذیری های موجود در شبکه ها با قابلیت ها و شیوه های مختلفی، با اهداف متنوع به ویژه حمله به دارایی های اقتصادی، سیاسی و امنیتی افراد، سازمان ها و کشورها در حال افزایش هستند. طی سال های اخیر تحقیقات گسترده ای در حوزه سایبری صورت گرفته که اکثر این تحقیقات تمرکز خود را بر شناسایی و تشخیص نفوذ قرار داده اند. این سیستم ها، تشخیص خود را پس از وقوع حمله یا در حین اجرای آن صورت می دهند. حال آنکه برای افزایش توانایی و قابلیت سیستم های دفاع سایبری، نیاز به بکارگیری مدل های پیشرفته تری وجود دارد که بتوانند علاوه بر تشخیص بهنگام، راهکارهای پیش بینی و دفاع پیش دستانه را نیز فراهم و حملات را قبل از وقوع و قبل از انجام فعالیت های خرابکارانه در شبکه متوقف سازند. این مقاله پس از بررسی مهمترین روش های پیش بینی نفوذ موجود، به معرفی و ارايه یک سیستم کارآمد برای کمک به عملکرد و پاسخگویی به موقع و دقیق تر سیستم های سایبری مبتنی بر پیش بینی با برخورداری از الگوهای یادگیرنده می پردازد. سیستم ارايه شده قبل از آنکه شبکه در معرض خطر قرار گیرد آن را پایش کرده و از اطلاعات گذشته در راستای پیش بینی آینده استفاده می نماید. این سیستم پیش بینی نفوذ، می تواند کلاس یا گام بعدی حمله در حال اجرا را با بکارگیری تکنیک های یادگیری عمیق با دقت و سرعت مناسبی تعیین نماید و در مقابل حملات سایبری چند مرحله ای سطح امنیت شبکه را ارتقاء بخشد. نتایج نشان می دهد که به کمک این سیستم پیش بینی، می توان یک مکانیسم دفاعی فعال در مقابل حملات پیشرو را فراهم آورد و امنیت هرچه بیشتر شبکه را تضمین نمود.

کلمات کلیدی:

پیش بینی نفوذ، حملات چندمرحله ای، دفاع سایبری، هشدار، شبکه

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/731172>

