کد خبر: ۲۹۴۵۱۷
شنبه ۲۸ تیر ۱۴۰۴ ۱۱:۳۴

پژوهش

بررسی چارچوب‌های هوش تهدید سایبری

تهدیدات سایبری به چالشی اساسی برای سازمان‌ها و دولت‌ها تبدیل‌شده‌اند و هوش تهدید سایبری به‌عنوان یک راهکار پیشگیرانه برای شناسایی و ارزیابی آن‌ها، با استفاده از چارچوب‌های زنجیره کشتار سایبری و MITRE ATT&CK، به سازمان‌ها کمک می‌کند تا سریع‌تر واکنش نشان دهند و از آسیب‌ها جلوگیری کنند.

در دنیای امروز، تهدیدات سایبری به یک چالش اساسی برای سازمان‌ها و دولت‌ها تبدیل‌شده‌اند. این تهدیدات نه‌تنها می‌توانند
باعث خسارات مالی شوند، بلکه اعتبار سازمان‌ها و امنیت اطلاعات کاربران را نیز به خطر می‌اندازند. با افزایش گستره و پیچیدگی این حملات، دیگر نمی‌توان به دفاع‌های سنتی سایبری معمول اکتفا نمود. سازمان‌ها به ابزارها و فرآیندهایی نیاز دارند که به‌صورت پیشگیرانه و در لحظه، بتوانند تهدیدات را شناسایی و ارزیابی کنند. در این میان هوش تهدید سایبری به‌عنوان یک راهکار مؤثر و مهم مطرح گردیده است.

هوش تهدید سایبری به اطلاعات و تحلیل‌هایی اشاره می‌کند که منجر به درک بهتر تهدیدات و حملات سایبری، روش‌های حمله و اهداف احتمالی مهاجمان می‌گردد. با تجزیه‌وتحلیل داده‌ها و اطلاعات مختلف از قبیل الگوهای رفتار مهاجم، شناسایی نقاط ضعف و آسیب‌پذیری‌ها، سازمان‌ها می‌توانند دید جامعی از فضای تهدیدات به دست آورند. این دید به آن‌ها کمک می‌کند تا از وقوع حملات جلوگیری نموده و یا در صورت وقوع، به‌طور هوشمندانه و به‌سرعت واکنش نشان دهند.
چارچوب‌های هوش تهدید ساختارهایی را برای فکر کردن در مورد حملات و مهاجمان ارائه می‌دهند. این چارچوب‌ها درک گسترده‌ای از چگونگی فکر کردن مهاجمان، روش‌های مورداستفاده توسط آن‌ها و جایی که در چرخه حیات حمله رویدادهای
خاص اتفاق میافتد را به وجود می‌آورند. این دانش به مدافعان سایبری اجازه می‌دهد که سریع‌تر به حملات واکنش داده و بتوانند آن‌ها را زودتر متوقف کنند. زنجیره کشتار سایبری Lockheed Martin و چارچوب MITRE ATT&CK که از مهم‌ترین چارچوب‌های هوش تهدید هستند، در این گزارش موردبررسی قرار خواهند گرفت.

زنجیره کشتار سایبری توسط شرکت Lockheed Martin معرفی‌شده است و با تجزیه‌وتحلیل مراحل مختلف حمله، به سازمان‌ها کمک می‌کند تا فرآیند حملات را در مراحل ابتدایی شناسایی کرده و از پیشروی آن جلوگیری کنند. این مدل به
شناسایی و تجزیه‌وتحلیل مرحله‌به‌مرحلهٔ حملات می‌پردازد و به سازمان‌ها این امکان را می‌دهد که نقاط مختلف حمله را شناسایی کنند و راهکارهایی برای متوقف‌سازی حمله پیاده‌سازی کنند. با تحلیل و شناسایی زودهنگام مراحل اولیه حمله، سازمان‌ها می‌توانند اقدامات پیشگیرانه را قبل از رسیدن به مراحل خطرناک‌تر اجرا کنند.
چارچوب MITRE ATT&CK یک پایگاه دانش مبتنی بر سناریوهای واقعی از حملات سایبری است. این چارچوب توسط موسسه MITRE توسعه داده‌شده و مجموعه‌ای از تاکتیک‌ها، فن‌ها و رویه‌های (TTP) مورداستفاده مهاجمان را در اختیار سازمان‌ها قرار می‌دهد MITRE ATT&CK این امکان را فراهم می‌کند که سازمان‌ها نه‌تنها رفتار مهاجمان را بهتر بشناسند، بلکه بتوانند متناسب با فن‌های مورداستفاده آن‌ها، راهکارهای مقابله‌ای خود را بهینه‌سازی کنند. با استفاده از این چارچوب، سازمان‌ها می‌توانند از تاکتیک‌های دفاعی خود یک نقشه جامع ایجاد

کرده و رفتارهای مهاجمین را به‌طور دقیق‌تر پیش‌بینی کنند. در این گزارش، مفاهیم کلی هوش تهدید سایبری بیان گردیده و دو چارچوب مهم یعنی زنجیره کشتار سایبری و MITRE ATT&CK بررسی شده است. باتوجه‌به مرجع بودن پایگاه دانش MITRE ATT&CK، بررسی بیشتری روی آن صورت گرفته و علاوه بر معرفی جزئیات ارائه‌شده در این پایگاه دانش، در مورد نگاشت Enisa Threat Landscape، نگاشت حملات وAPT های مهم به TTP های Mitre و استفاده از Mitre برای هوش تهدید نیز مطالبی مهمی بیان شده است.

متن کامل این گزارش را از اینجا دریافت کنید.