امنیت به زبان ساده: جرم‌شناسی شبکه چیست؟ - دیجیاتو

شایان ضیایی | دوشنبه، ۱۱ اسفند ۱۳۹۹

اگر هک اخیر شرکت SolarWinds و ابزار مدیریت شبکه‌اش یک چیز به ما آموخته باشد، اینست که هرکسی می‌تواند به قربانی حملات سایبری تبدیل شود. در واقع سال ۲۰۲۰ سالی بود که بیشترین میزان حملات سایبری علیه شرکت‌های بریتانیایی ترتیب داده شده و در قیاس با سال ۲۰۱۹، حدودا ۲۰ درصد شرکت‌های بیشتری با تهدیدات امنیت سایبری روبه‌رو شدند. حملات باج‌افزار در سه‌ماهه سوم ۲۰۲۰ رشد ۸۰ درصدی را تجربه کردند و در نیمه نخست همان سال، حملات وب اپلیکیشن هم ۸۰۰ درصد افزایش یافتند.

اگرچه پاندمی کووید-۱۹ و نیاز به دورکاری کارمندان مشخصا نقشی برجسته در افزایش هرچه بیشتر این دست از حوادث داشته است، اما چنین خطراتی در حالت عادی نیز وجود دارند و کسب‌وکارها باید تمام تلاش خود را برای پیشگیری از حوادث غیر قابل جبران و همینطور جبران خسارات به کار بگیرند. اما به جای سرمایه‌گذاری صرف روی ابزارهای امنیتی و امیدوار بودن به عدم وقوع اتفاقات ناگوار، الکس استاموس، مشاور امنیتی SolarWinds و مدیر ارشد امنیتی سابق فیسبوک به کسب‌وکارها پیشنهاد می‌کند با این حقیقت غیر قابل اجتناب کنار بیایند که ممکن است هک شوند.

او در سخنرانی اخیر خود که اوایل ماه گذشته میلادی صورت گرفت پیشنهاد کرد که کسب‌وکارها به استراتژی‌های تشخیص، پایش و پاسخدهی به حملات سایبری فکر کنند و ابزارهایی برای هر مرحله از زنجیره مقابله سایبری با هکرها داشته باشند. آنچه او پیشنهاد می‌کند اساسا همان چیزی است که تحت عنوان «جرم‌شناسی شبکه» شناخته می‌شود و بر شناسایی دلایل رخنه امنیتی و استفاده از این دانش برای ایمن‌سازی هرچه بهتر در مقابل حملات آتی تمرکز دارد. جرم‌شناسی شبکه ضمنا می‌تواند به معنای ساخت یک استراتژی پاسخدهی موفقیت‌آمیزتر به اثرات بالقوه هک نیز باشد.

اگرچه هیچ شرکتی دوست ندارد تجربه‌ای مشابه SolarWinds از نظر حملات سایبری به دست آورد، اما قطعا می‌توان با نیم‌نگاهی به جرم‌شناسی شبکه، از تجربه این کمپانی آمریکایی آموخت.

جرم‌شناسی شبکه چیست؟

اساسا جرم‌شناسی شبکه یکی از زیرمجموعه‌های جرم‌شناسی دیجیتال به حساب می‌آید که آن نیز خود زیرمجموعه‌ای از علم جرم‌شناسی است. در این علم، متخصصین و مقامات قضایی به تکنولوژی و داده‌ای که ممکن است حاوی شواهدی از یک جرم یا مدرکی از مجرم دخیل در ماجرا باشد نگاه می‌اندازند، اظهارات را با یکدیگر مقایسه می‌کنند و اسنادی که توسط متهمان ارائه شده تا بی‌گناهی خود را اثبات کنند مورد بررسی قرار می‌گیرند.

جرم‌شناسی شبکه، به شکلی نه‌چندان غافلگیرکننده، به معنای بررسی و تحلیل تمام ترافیکی است که روانه شبکه‌ای شده که احتمالا در پیاده‌سازی یک جرم سایبری دخیل بوده است، مثلا انتشار گسترده بدافزاری که اطلاعات کاربران را به سرقت می‌برد یا یک حمله سایبری با استفاده از تکنیک‌های رایج.

مراجع قانونی از جرم‌شناسی شبکه برای تحلیل داده‌های ترافیک شبکه‌ی استخراج شده از شبکه مظنون به استفاده در جرایم مجرمان یا یک حمله سایبری استفاده می‌کنند. برای مثال تحلیلگران به دنبال داده‌هایی می‌گردند که به ارتباطات انسانی، دستکاری‌های فایل و استفاده از کلمات کلیدی خاص اشاره دارند. با استفاده از جرم‌شناسی شبکه، مراجع قانونی می‌توانند ارتباطات را پایش کنند و براساس رویدادهای لاگ شده توسط سیستم‌های کنترل شبکه، یک تایم‌لاین کامل از وقایع منتهی به هک بسازند.

بیرون از پرونده‌های مجرمانه، جرم‌شناسی شبکه به صورت معمول برای تحلیل رویدادهای شبکه استفاده می‌شود تا منبع حملات هک و حوادث مرتبط با امنیت شناسایی شوند. این پروسه می‌تواند شامل جمع‌آوری اطلاعات راجع به اتفاقات نامتعارف و مصنوعات شبکه و همینطور پرده برداشتن از حوادثی باشد که با دسترسی غیرمجاز به شبکه به وقوع پیوسته‌اند.

جرم‌شناسی شبکه معمولا به دو متد انجام می‌شود. نخستین متد «تا جایی که می‌توانی بگیرش – Catch it as You Can» نام دارد که شامل ثبت تمام ترافیک شبکه برای تحلیل می‌شود و پروسه‌ای بسیار طولانی است که فضای ذخیره‌سازی بسیار زیادی نیز طلب می‌کند.

تکنیک دوم «بایست، نگاه کن و گوش بده» نام دارد که شامل تحلیل هر پکت داده که در شبکه به جریان افتاده می‌شود و سپس آن داده‌هایی که مشکوک به نظر می‌رسد و ارزش تحلیل هرچه بیشتر را دارند جمع‌آوری می‌شوند. این رویکرد هم نیازمند قدرت پردازی فراوان است، اما برخلاف روش قبلی فضای ذخیره‌سازی چندانی طلب نمی‌کند.

برخلاف جرم‌شناسی دیجیتال، جرم‌شناسی شبکه کاری بسیار دشوارتر است، زیرا داده برخی اوقات در شبکه مخابره و سپس گم می‌شود. در جرم‌شناسی کامپیوتر، داده معمولا در یک دیسک یا یک حافظه حالت جامد ذخیره‌سازی می‌شود تا دسترسی به آن آسان‌تر باشد.

لازم به اشاره است که قوانین حریم شخصی و حفاظت از داده، پایش فعالانه و تحلیل ترافیک شبکه را بدون جوازهای لازم ممنوع کرده‌اند. بنابراین اگر بخواهید از ابزارهای جرم‌شناسی شبکه استفاده کنید، باید از قبل با مراجع قانونی هماهنگ باشید.

دیجیاتو