استفاده از داده‌های کلان در امنیت سایبری

محققان امنیتی در خصوص داده‌های کلان هیجان‌زده هستند و آن را یک بررسی‌کننده‌ی بزرگ در حوزه‌ی جرایم سایبری می‌دانند. اگر سازمان شما مورد نفوذ قرار گرفته و اطلاعات مشتریان آلوده شده، شما می‌توانید بر روی سامانه‌های خود از داده‌های کلان استفاده کرده و اطلاعات انبوهی را بدست آورید. در ادامه می‌توانید بینش وسیع‌تری از آنچه که اتفاق افتاده را بدست آورید.

اما داده‌های کلان زمانی می‌تواند مورد استفاده قرار گیرد که جرمی صورت گرفته باشد و نمی‌تواند از وقوع این اتفاقات جلوگیری کند. به عبارت دیگر وقوع نفوذهای سایبری همچنان امکان‌پذیر است و مشتریان از این موضوع عصبانی بوده و سازمان‌های استاندارد نیز ممکن است شرکت شما را جریمه کنند.

اینجا جایی است که داده‌های کلان با وعده‌های خود شکست می‌خورد. همان‌طور که از قدیم گفته‌اند «ادراک بهترین دید است.» به‌طور قطع پس از وقوع حادثه اگر از داده‌های کلان استفاده شود، دید وسیع‌تری را در اختیار شما قرار خواهد داد. با این حال داده‌های کلان به شما این قابلیت را نمی‌دهد که وقوع حوادث سایبری را شناسایی کنید و در حین وقوع جرم نیز نمی‌توانید آن را متوقف کنید. به این دلیل داده‌های کلان نمی‌تواند برای سازمان، کسب‌وکار و اطلاعات حساس شما امنیت را به ارمغان آورد.

موافقان داده‌های کلان معتقدند شما با در اختیار داشتن دید وسیع می‌توانید مشکلات سامانه را برطرف کرده و از وقوع جرم در مراحل اولیه جلوگیری کنید. به عبارت دیگر شما می‌توانید اشکالات را شناسایی کرده و آن‌ها را وصله کنید و از وقوع مجدد حملات سایبری جلوگیری نمایید.

هرچند این موضوع درست است که شما می‌توانید از وقوع مجدد حملات جلوگیری کنید ولی حملات سایبری به همین سادگی اتفاق نمی‌افتند. عرصه‌ی تهدیدات سایبری بسیار پویاست و هر روزه آسیب‌پذیری‌های جدیدی کشف می‌شود.

علاوه بر این مهاجمان سایبری نیز مانند سایر مجرمان هستند. زرنگ و دانا و سازگار با محیط. به‌گونه‌ای که با ماهیت انسانی می‌توانند حملات پویا و جدیدی را انجام دهند. آن‌ها همواره دنبال یافتن ضعف‌های شما هستند و بزرگ‌ترین ضعف شما در سازمان نیروی انسانی و کارکنان شما هستند. بسیاری از مهاجمان سایبری با استفاده از دربِ پشتی به سامانه‌ها نفوذ نمی‌کنند. آن‌ها با بدست آوردن گواهی‌نامه‌های معتبر و قانونی، از دربِ جلویی وارد می‌شوند.

بنابراین در بسیاری از موارد، تجزیه و تحلیل داده‌های کلان نشان می‌دهد مهاجمان با گواهی‌نامه‌های کارکنان شما وارد کارگزارها شده‌اند. این گذرواژه‌ها با استفاده از روش‌های مهندسی اجتماعی و رایانامه‌های فیشینگ در اختیار مهاجمان قرار می‌گیرد.

با این بینش جدید، احتمال دارد شما تصمیم بگیرید تا دوره‌های آموزشی سایبری را برای کارکنان خود برگزار کنید تا آن‌ها بدانند که چگونه با رایانامه‌های فیشینگ برخورد کنند و از خطرات کلیک بر روی پیوندهای مخرب مطلع شوند. آموزش امنیت سایبری به کارکنان بسیار ضروری است ولی نوش‌دارو نیست.

انسان‌ها جایزالخطا هستند. آن‌ها زمانی که خسته، آشفته هستند یا عجله دارند ممکن است اشتباه کنند. علاوه بر این، هیچ آموزشی نمی‌تواند جلوی فعالیت‌های مخرب داخلی را بگیرد. یک کارمند ناراضی یا کارمند سابق شرکت را در نظر بگیرید که می‌خواهد به شرکت شما حمله کند و اطلاعات مهم و حساس را در نت تاریک بفروشد.

خوشبختانه یک راه‌حل وجود دارد: یادگیری ماشین که از الگوریتم‌های ریاضیاتی برای آموزش و به‌روزرسانی بلادرنگ استفاده می‌کند. این روش رایانه‌ها را قادر می‌سازد بدون برنامه‌نویسی صریح، یاد بگیرند. یادگیری ماشین روشی است که باعث بوجود آمدن خودروهای بدون سرنشین شده است و روشی است که ما در برابر نفوذگران می‌توانیم از آن استفاده کنیم.

روش‌های یادگیری ماشین حفاظت‌هایی را فراهم می‌کند که داده‌های کلان از آن ناتوان است. بجای اینکه پس از وقوع حادثه کشف کنیم که یک اتفاق چرا رخ داده است، یادگیری ماشین می‌تواند یک نقض داده را در حین رخ دادن شناسایی کند. یادگیری ماشین کمک می‌کند تا بدانیم یک حمله چگونه اتفاق افتاده و هشداری را صادر می‌کند تا بتوانیم روند حمله را متوقف کرده و از ضرر و زیان‌های بیشتر جلوگیری کنیم.

روش یادگیری ماشین تنها از داده‌های کلان بهره نمی‌برد بلکه آن‌ها را تحلیل کرده و از آن اطلاعاتی را استخراج می‌کند. این فرآیند استخراج اطلاعات نسبت به کار گروه‌های امنیتی بسیار سریع‌تر است. به دلیل قابلیت‌های پیش‌بینی این روش، می‌تواند رویکرد فعالی داشته باشد. روش یادگیری ماشین می‌تواند به‌طور بلادرنگ استفاده از گواهی‌نامه‌ها توسط نفوذگران را شناسایی کرده و از ورود آن‌ها به سامانه جلوگیری کند.

این روش در حوزه‌ی شبکه بسیار پخته نیست ولی برای برنامه‌های کاربردی و داده‌ها بسیار سودمند است. این سپر دفاعی هر ورودی به سامانه در هر ساعتی را مورد نظارت و بررسی قرار می‌دهد تا رفتارهای عادی را از رفتارهای ناهنجار تشخیص دهد.

به‌طور مثال این الگوریتم‌ها زمانی که کاربری بخواهد از مکان ناشناخته‌ای وارد سامانه شود، هشداری را صادر می‌کند. همچنین وقتی کاربر بخواهد به بخشی از سامانه دست یابد که برای انجام کارش ضروری نیست و یا مثلاً اگر بخواهد نیمه شب وارد حساب کاربری خود شود، هشدار می‌دهد. به دلیل اینکه روش‌های یادگیری ماشین الگویی از رفتارهای عادی کاربر را استخراج می‌کند، می‌تواند هر رفتار ناهنجاری را شناسایی و مسدود کند تا مسئول فناوری اطلاعات به این مسئله رسیدگی کند.

روش‌های یادگیری ماشین بینشی فوری، حیاتی و عملیاتی از داده‌های کاربران را ارائه می‌دهد. این روش‌ها حفاظت‌های بلادرنگ در برابر حملات نفوذگران را برای شما فراهم می‌کنند که داده‌های کلان از آن ناتوان هستند. یادگیری ماشین روشی عالی برای امن کردن سامانه‌ها است چرا که به‌طور مداوم رفتارهای هنجار و ناهنجار را یاد می‌گیرد و می‌تواند پیش از ورود نفوذگر به سامانه و سرقت اطلاعات، اطلاعاتی را به شما ارائه کند.

این فناوری در حال حاضر وجود دارد، توسعه داده شده است و در نمونه‌های زیادی حملات و سرقت داده‌های حساس سازمان‌ها و نقض حریم خصوصی کاربران را هشدار داده است. این فناوری در آینده به روشی با کارایی بالا برای امنیت داده‌ها تبدیل خواهد شد. بنابراین اگر داده‌های کلان محققی در صحنه‌ی جرم هستند، شما می‌توانید بگویید که یادگیری ماشین مانند ماشین پلیس در حال گشت است. این روش از سامانه‌های شما در برابر مهاجمان حفاظت کرده و اعمال قانون می‌کند و اگر جرمی در حال وقوع باشد آن را متوقف می‌نماید.