دانشکده مهندسی کامپیوتر

استاد درس: دکتر دیانت

زمستان ۱۴۰۲

پروژه فرمیم
امنیت سیستم های کامپیوتری

ستاره باباجانی - ملیکا محمدی فخار
شماره دانشجویی: ۹۹۵۲۱۱۰۹ - ۹۹۵۲۲۰۸۶

بررسی کلی

همزمان با رشد حجم داده‌ها و اهمیت تجاری آنها، استفاده از خدمات ابری برای مدیریت داده‌ها افزایش می‌یابد. با این حال، ۷۴ درصد از تصمیم‌گیرندگان امنیتی گزارش داده‌اند که حریم داده‌های حساس سازمان‌شان در سال ۲۰۲۲ دستکم یک بار نقض شده است. مطالعه‌ای که توسط Con- Forrester sulting برای Cyera انجام شده نشان می‌دهد که سازمان‌های مستقر در آمریکای شمالی با تلاش برای ایجاد تعادل بین امنیت و توانمندسازی کسب‌وکار دست و پنجه نرم می‌کنند. کنترل‌های امنیتی به صورت دستی، بزرگترین چالشی است که رهبران امنیتی با آن روبرو هستند. اتوماسیون امنیت داده‌ها به عنوان یک گام حیاتی دیده می‌شود که نه تنها ارزش تجاری را حفظ می‌کند، بلکه به شرکت‌ها کمک می‌کند تا وضعیت امنیتی قوی و پایداری را تقویت و حفظ کنند، و ۷۰ درصد از پاسخ‌دهندگان انتظار دارند که سرمایه‌گذاری در این حوزه منافع قابل توجه یا تحول‌آفرینی به همراه داشته باشد.

یافته‌های کلیدی

- رهبران امنیتی انتظار دارند که بیشترین منافع تحول‌آفرین از اتوماسیون امنیت داده‌ها، به‌ویژه ارزیابی‌های خطر، کشف داده‌ها و دسته‌بندی آن‌ها حاصل شود.
- کنترل‌های امنیتی ناکارآمد منابع را هدر داده و به کسب‌وکار آسیب می‌زنند. هفتاد و یک درصد از رهبران امنیتی گفته‌اند که فناوری‌های قدیمی و فرآیندهای دستی مانع موفقیت کسب‌وکارشان هستند.
- رهبران امنیتی در حال سرمایه‌گذاری در اتوماسیون هستند تا از جریمه‌های تنظیمی اجتناب کنند، کارایی عملیاتی را بهبود ببخشند، و اعتماد مشتریان را حفظ کنند.

مفهوم Trust Zero اولویت اصلی رهبران امنیتی است.

تصمیم‌گیرندگان امنیت اطلاعات اهداف مهمی برای سال آینده دارند که ۶۰% از پاسخ‌دهندگان هشت هدف برجسته شده در این مطالعه را به عنوان اولویت‌های حیاتی ارزیابی کرده‌اند. اما هدف اصلی برای رهبران امنیتی، تقویت موقعیت امنیتی Trust Zero سازمان‌هایشان است (۸۴%). این موضوع با نظرسنجی امنیتی Forrester در سال ۲۰۲۲ مطابقت دارد که نشان داد شرکت‌ها به طور متوسط ۱۴% از بودجه امنیتی خود را به امنیت ابری اختصاص داده‌اند و تقویت استراتژی امنیت ابری اولویت اصلی در سال ۲۰۲۳ است. بدون حفاظت مناسب از داده‌های ابری، سازمان‌ها نمی‌توانند داده‌های محلی را به ابر منتقل کنند. بهبود موقعیت امنیتی Trust Zero و امنیت داده‌ها اطمینان می‌دهد که داده‌های حساس به دست افراد غیرمجاز نیفتند. بهبود دقت ارزیابی خطر داده‌ها (۸۲%)، وضعیت امنیتی داده

در ابر (۷۹%)، و افزایش اتوماسیون کنترل‌های امنیتی (۷۶%) اولویت‌های حیاتی برای رهبران امنیتی هستند.

کسب‌وکارها به انتقال داده‌های بیشتر به پلتفرم‌ها و پایگاه‌های داده ابری ادامه خواهند داد.

با کم اهمیت شدن زیرساخت‌های محلی، استفاده از پلتفرم‌ها به عنوان یک سرویس (PaaS) و پایگاه‌های داده به عنوان یک سرویس (DBaaS) در سازمان‌ها در دو سال آینده افزایش خواهد یافت. هر چند که انتظار می‌رود استفاده برنامه‌ریزی شده از زیرساخت به عنوان یک سروی (IaaS) و نرم‌افزار به عنوان یک سرویس (SaaS) کمی کاهش یابد، آن‌ها همچنان پرکاربردترین محیط‌های ابری باقی می‌مانند. بسیاری از رهبران امنیتی نیاز خواهند داشت تا داده‌ها را در یک محیط هیبریدی حفظ و ایمن کنند. آن‌ها باید نحوه مدیریت و ایمن‌سازی این محیط‌ها را بازاندیشی کنند. از آنجایی که محیط‌های ابری مختلف نیز عملکرد امنیتی داخلی را ارائه می‌دهند، رهبران امنیتی باید معاوضه استفاده از قابلیت‌های داخلی (مانند فرآیندهای دستی، استقرار چندپاره و پیاده‌سازی طولانی‌مدت را در مقابل بهترین راه‌حل‌های شخص ثالث ارزیابی کنند.

اکثر شرکت‌ها در دست‌یابی به اهداف امنیتی خود همزمان با بهبود کسب‌وکارشان، با مشکل مواجه هستند.

قابلیت‌های تجاری کسب‌وکار مبتنی بر بینش‌های پیشرفته برای کسب و حفظ مزیت رقابتی است. رشد و بلوغ فقط محدود به کیفیت داده برای ایجاد ارزش مادی از داده نیست. تضمین امنیت، حفظ حریم خصوصی و اطمینان از انطباق، برای تبدیل داده‌ها به بینش‌های مفید، حیاتی هستند. این موضوع شامل رعایت الزامات قانونی، نیازهای شریکان تجاری و الزامات قراردادی است. بدون اینکه رهبران سازمان‌ها را به گونه‌ای طراحی کنند که گروه‌ها را با هدف تصمیم‌گیری مبتنی بر داده از طریق استفاده مناسب از اطلاعات انحصاری یا حساس هماهنگ کند، هیچ مقدار داده‌ای، صرف‌نظر از کیفیت آن، نمی‌تواند تفاوتی ایجاد کند. استفاده از داده‌ها برای بهبود کسب‌وکار، بزرگترین چالشی است که رهبران امنیتی اطلاعات با آن مواجه هستند، به طوری که ۷۰% از آنها گزارش داده‌اند که این برای سازمان‌هایشان بسیار چالش‌برانگیز است. این تلاش برای استفاده از داده‌ها عمدتاً به دلیل ناتوانی در شناسایی مخاطرات امنیتی برای داده‌های حساس (۶۶٪) و تخلفات انطباقی (۶۱٪) است.

امروزه نیاز به رویکردی جدید برای حفظ امنیت داده‌ها احساس می‌شود.

رویکردهای سنتی که از ابزارهای متداول در امنیت سایبری استفاده می‌کنند، نمی‌توانند امکان اعمال کنترل‌های امنیتی قوی بر داده‌ها را فراهم کنند. نود و هشت درصد از پاسخ‌دهندگان گفته‌اند که وضعیت فعلی امنیت داده‌ها در شرکت‌شان مشکل‌ساز است. همزمان با اینکه سازمان‌ها به نوسازی سیستم‌های خود ادامه می‌دهند و به محیط‌های ابری وابسته‌تر می‌شوند، باید چالش‌های جدیدی در امنیت داده‌ها را پشت سر بگذارند که این کار آسانی نیست. چالش‌های رایج ناشی از فناوری‌های قدیمی، استقرارهای تکه‌تکه و پیاده‌سازی‌های طولانی‌مدت، به طور جمعی مشکلات سیستمی را نشان می‌دهند که بایست از رویکردی جدید در امنیت داده بهره‌مند شوند. این فرآیندهای دستی و پیچیده، مستقیماً با کنترل‌های امنیتی پویا که یک معماری Trust Zero را فعال می‌کنند و برای حفاظت از داده‌های حساس در شبکه‌ها، هویت‌ها و دستگاه‌ها طراحی شده‌اند، در تضاد هستند.

کمبود اتوماسیون به کسب‌وکارهای امروزی آسیب می‌زند.

تنها داده‌هایی که شناسایی و بر اساس خطراتشان اولویت‌بندی شده‌اند، می‌توانند به طور مؤثری محافظت شوند. قابلیت‌های امنیتی بومی ابری و پلتفرم‌های تخصصی امنیت داده که می‌توانند محیط‌های ابری و در محل را پوشش دهند اما فاقد اتوماسیون هستند، نمی‌توانند فهرست‌های فعلی دارایی‌ها را حفظ کنند. شصت و نه درصد شرکت‌ها همچنان به صورت دستی فهرست دارایی‌ها را حفظ می‌کنند. شرکت‌ها محیط‌های ابری را مانند یک گاراژ بزرگ قابل توسعه برای حجم‌های رو به رشد دارایی‌های داده‌ای تلقی می‌کنند. تعجبی ندارد که ۵۹% اعتراف می‌کنند که در حفظ فهرست داده‌های دقیق دچار مشکل هستند. هفتاد و یک درصد از پاسخ‌دهندگان گزارش داده‌اند که فرآیندهای دستی امنیت داده موفقیت کسب‌وکارشان را محدود می‌کند. رهبران امنیتی که راه‌های جدیدی برای اتوماتیک کردن فرآیندها و کنترل‌های امنیت داده پیدا می‌کنند، نه تنها امنیت را بهبود می‌بخشند، بلکه ارزش‌های مادی را به شیوه‌های جدیدی تولید می‌کنند. شناسایی داده‌ها و کسب دیدگاه در مورد خطرات آن قبل از اینکه بتوان آن‌ها را محافظت و استفاده کرد، ضروری است.

همانطور که توسط رهبران امنیت اطلاعات نشان داده شده است، ابزارهای امنیت داده های بومی ابری با اتوماسیون آماده هستند که تأثیر قابل توجهی بگذارند.

قابلیت‌های کلیدی مانند کنترل‌های امنیتی پویا، تشخیص نوردهی در زمان واقعی، و مدیریت وضعیت امنیت داده به عنوان محرک‌های تغییر معنادار برجسته می‌شوند. قابل‌توجه، پاسخ‌دهندگان بر پتانسیل

تحول‌آفرین اتوماسیون امنیت داده تأکید می‌کنند، با فروشندگانی که عملکردهای AI/ML را برای فعال کردن کنترل‌های پویا یکپارچه می‌کنند. این تغییر نوید به ساده‌سازی اتوماسیون و هماهنگ‌سازی سیاست‌های امنیتی، کاهش پیچیدگی مدیریت کنترل‌های امنیتی برای سازمان‌های مدرن را می‌دهد.

اتوماسیون برای حفظ یک وضعیت امنیتی قوی، به ویژه با پذیرش فزاینده فناوری‌های ابری و حجم فزاینده داده، ضروری است.

مزایای سرمایه‌گذاری در کشف خودکار داده‌ها، طبقه‌بندی و ارزیابی ریسک شامل افزایش بلوغ اعتماد صفر، اجتناب از جریمه‌های قانونی، بهبود کارایی عملیاتی و افزایش انعطاف‌پذیری در برابر تهدیدات باج‌افزار است. علاوه بر این، اتوماسیون تلاش‌های امنیتی را با الزامات تجاری، مانند حفظ اعتماد مشتری و افزایش کارایی عملیاتی، هماهنگ می‌کند.

زمان به ارزش به عنوان یک ملاحظات حیاتی برای رهبران امنیت اطلاعات شناسایی شده است، و سهولت اجرا بسیار مهم است.

راه حل هایی که ایجاد فهرست خودکار داده ها، اصلاح داخلی و سازگاری با محیط های مختلف را ارائه می دهند بسیار ارزشمند هستند. این مطالعه بر اهمیت پرداختن به چالش‌های امنیت داده‌های مدرن از طریق اتوماسیون تأکید می‌کند، زیرا بسیاری از سازمان‌ها برای ایجاد تعادل بین اهداف امنیتی و فعال‌سازی کسب‌وکار تلاش می‌کنند. یک رویکرد جامع برای ایمن سازی استقرار چند ابری و ترکیبی با تاکید بر نیاز به جایگزینی رویکردهای تکه تکه با معماری های مناسب برای حجم کار و داده های ابری مورد حمایت قرار می گیرد. اتوماسیون، به ویژه در کشف داده‌ها، طبقه‌بندی و ارزیابی ریسک، برای افزایش امنیت و باز کردن ارزش کسب‌وکار ضروری است.

نتیجه گیری

خودکارسازی فرآیندهای مهم کلیدی برای رسیدگی به چالش های مدرن امنیت داده است. این مطالعه نشان داد که:

- بسیاری از شرکت ها برای رسیدن به اهداف امنیتی در حالی که کسب و کار را قادر می سازند، تلاش می کنند. این چالش‌های اغلب مرتبط با یکدیگر، از جمله شناسایی داده‌های حساس، مشاهده مواجهه‌های امنیتی و خطرات انطباق، و فعال کردن کنترل‌های داده‌ها، یک رویکرد جدید برای امنیت داده را ضروری می‌سازد.

- یک رویکرد تکه تکه برای ایمن سازی استقرار چند ابری و ترکیبی کارساز نخواهد بود. برای دستیابی به زمان به ارزش سریع، رویکردهای پراکنده و چرخه های پیاده سازی طولانی را با معماری و قابلیت های متناسب با ماهیت نامحدود حجم کار و داده های ابری جایگزین کنید.
- اتوماسیون امنیت را بهبود می بخشد و ارزش کسب و کار را باز می کند. بزرگترین ارتقاء از طریق کشف و طبقه بندی داده های خودکار و ارزیابی ریسک داده حاصل می شود.