امنیت اطلاعات؛ دغدغه دنیای امروز

۱- امنیت اطلاعات در نظام بانکی

اهمیت امنیت اطلاعات در دنیای امروزه به طور گسترده درک شده است و سازمان‌ها به طور فزاینده‌ای در زمینه امنیت اطلاعات سرمایه‌گذاری می‌کنند، اما خطرات و هزینه‌های جرایم سایبری نیز به طور پیوسته در حال افزایش است. بانک‌ها و موسسات مالی به دلیل ماهیت فعالیت خود، به طور خاص مورد هدف مهاجمان قرار می‌گیرند. علاوه بر این، هزینه‌های دستکاری اطلاعات در صنعت مالی به‌شدت رو به افزایش است. سرمایه‌گذاری در امنیت اطلاعات به منظور کسب اعتماد مشتریان و سایر ذی‌نفعان و همچنین دستیابی به انطباق با الزامات قانونی بالادستی اجباری شده است. بنابراین، بانک‌ها و موسسات مالی با چالش های متعددی در حوزه امنیت اطلاعات روبرو هستند.

منابع تهدیدات امنیت اطلاعات

کلاه‌برداری‌های مالی بیشتر از خارج از بانک‌ها و موسسات مالی انجام می‌شود، جایی که مجرمان سایبری در تلاش برای سرقت اطلاعات یا جعل تراکنش‌ها هستند. این بانک‌ها و موسسات باید تعهد خود را برای دستیابی به بالاترین سطح امنیت نشان داده و همواره با جدیدترین تکنیک‌ها و فناوری‌ها به روز بمانند.

برخی از تهدیدات کلیدی که موسسات مالی با آن‌ها مواجه هستند عبارتند از:

باج‌افزار: مجرمان سایبری از باج‌افزار جهت رمزنگاری و قفل نمودن اطلاعات بانک‌ها و موسسات مالی و سپس درخواست پرداخت باج در ازای رمزگشایی استفاده می‌نمایند.

حملات فیشینگ: مهاجمان از طریق ایمیل‌ها یا وب‌سایت‌های جعلی، با فریب کاربران اطلاعات شخصی یا مالی آن‌ها را سرقت می‌کنند.

حملات زنجیره تأمین: مجرمان سایبری به تامین‌کنندگان سرویس‌های بانک‌ها و موسسات مالی نفوذ می‌کنند تا به سیستم‌ها و داده‌های آن‌ها دسترسی پیدا کنند.

حملات DDOS: این حملات با سیل ترافیک درخواست به وب‌سایت‌ها یا سرورها، آن‌ها را از دسترس خارج می‌کنند.

مهندسی اجتماعی: مجرمان سایبری با استفاده از فریب و تقلب کاربران را به افشای اطلاعات حساس یا انجام اقداماتی که به نفع مهاجم است، متقاعد می‌کنند.

تهدیدات داخلی: کارمندان ناراضی یا سهل‌انگار می‌توانند به طور ناخواسته یا عمدی به داده‌ها و سیستم‌ها آسیب برسانند.

حملات ابری: مجرمان سایبری به پلتفرم‌های ابری که بانک‌ها و موسسات مالی از آن‌ها استفاده می‌نمایند، نفوذ کرده و تهدیدات امنیتی را ایجاد می‌نمایند.

بدافزار: بدافزار نوعی نرم‌افزار مخرب است که می‌تواند به سیستم‌ها و داده‌ها آسیب برساند.

جعل اطلاعات: مجرمان اطلاعات مالی و یا سایر اطلاعات حساس را جعل نمایند.

سرقت: مجرمان به صورت فیزیکی به داده‌ها یا سیستم‌ها دسترسی پیدا کرده و آن‌ها را سرقت می‌کنند.

آسیب‌پذیری‌های API: مجرمان سایبری از آسیب‌پذیری‌های رابط‌های برنامه‌نویسی(API) برای دسترسی به داده‌ها و سیستم ها استفاده می‌کنند.

حملات بر روی برنامه‌های کاربردی وب: با توجه به گسترش استفاده از برنامه‌های کاربردی وب در سامانه‌های بانکی، در این حملات از نقاط ضعف برنامه‌های کاربردی وب برای نفوذ به سیستم‌ها و داده‌ها استفاده می‌شود.

دستکاری داده: مجرمان داده‌ها را تغییر یا حذف می‌کنند تا به نفع خود یا به ضرر موسسه مالی عمل کنند.

اقدامات مقابله با منابع تهدیدات امنیت اطلاعات

بانک‌ها و موسسات مالی باید برای مقابله با این تهدیدات، اقدامات متعددی انجام دهند. مهم-ترین این اقدامات عبارتند از:

ایجاد یک برنامه جامع امنیت سایبری: این برنامه باید شامل ارزیابی ریسک، کنترل‌ها و اقدامات پیشگیرانه، فرآیندهای پاسخ به رخداد و آموزش و آگاهی باشد.

استفاده از فناوری‌های امنیتی قوی: این فناوری‌ها شامل فایروال‌ها، سیستم‌های تشخیص نفوذ، نرم‌افزار ضد بدافزار و رمزگذاری هستند.

ایجاد یک فرهنگ امنیتی قوی: کارکنان باید در مورد تهدیدات سایبری و نحوه محافظت از خود و موسسه آموزش ببینند آگاهی‌رسانی عمومی و مستمر امنیت اطلاعات در این زمینه ضروری است.

به‌روز نگه داشتن سیستم‌ها و نرم‌افزارها: این امر به منظور از بین بردن آسیب‌پذیری‌هایی که می‌توانند توسط مجرمان سایبری مورد سوء استفاده قرار گیرند، ضروری است. بسیاری از حملات امنیتی از طریق تهدیدات روز امنیتی صورت می‌پذیرد؛ لذا به‌روزرسانی سیستم‌ها و تجهیزات بسیار حیاتی است.

انجام تست‌های نفوذ منظم: این تست‌ها به شناسایی و رفع نقاط ضعف امنیتی قبل از اینکه توسط مجرمان سایبری مورد سوء استفاده قرار گیرند، کمک می‌کند.

داشتن یک برنامه قوی برای بازیابی در برابر بلایا: این برنامه باید به بانک کمک کند تا در صورت وقوع یک حمله سایبری، به‌سرعت فعالیت خود را بازیابی کند. برنامه‌های بازیابی حوادث استاندارد یکی از راهکارهای اصولی مقابله با تهدیدات امنیت اطلاعات است.

با سرمایه‌گذاری در امنیت سایبری، موسسات مالی می‌توانند از خود در برابر تهدیدات رو به رشد محافظت کرده و از اطلاعات و دارایی‌های خود و مشتریان خود در امان نگه دارند.

تأثیر اطلاعات مخدوش در مؤسسات مالی

دستکاری داده‌ها می‌تواند منجر به نرخ غیرعادی بالای ریزش مشتریان و همچنین تحقیقات و مجازات‌های شدید توسط نهادهای نظارتی شود. به همین دلیل، بانک‌ها و موسسات مالی باید واکنش سریع و قاطعی به دستکاری داده‌ها و سایر حوادث امنیتی نشان دهند تا از آسیب به شهرت و اعتبار خود جلوگیری نمایند.

از جمله اقدامات ضروری برای مقابله با دستکاری داده‌ها و حوادث امنیتی عبارتند از:

آموزش کارکنان: آگاهی و آموزش کارکنان در مورد تهدیدات سایبری و نحوه مقابله با آن‌ها، نقشی اساسی در پیشگیری از حوادث امنیتی ایفا می‌کند. بانک‌ها و موسسات مالی باید به طور منظم آموزش‌های لازم را به کارکنان خود ارائه دهند.

استفاده از رمزنگاری قوی: رمزنگاری داده‌ها یکی از موثرترین روش‌ها برای محافظت از اطلاعات در برابر دسترسی غیرمجاز است. بانک‌ها و موسسات مالی باید از رمزنگاری قوی برای تمام داده‌های حساس خود، از جمله داده‌های مشتریان، استفاده نمایند.

تقویت تیم‌های واکنش به حادثه: یکی از موثرترین اقداماتی که بانک‌ها و موسسات مالی می‌توانند برای کاهش هزینه‌های از دست رفتن داده‌ها و حفظ امنیت اطلاعات خود انجام دهند استفاده از تیم واکنش به حادثه یا تیم پاسخگویی به حوادث امنیتی است. بانک‌ها و موسسات مالی باید تیم‌های واکنش به حادثه (Incident Response Team) خود را با آموزش و تجهیز مناسب تقویت کنند تا بتوانند به طور موثر به حوادث امنیتی پاسخ دهند. بر این اساس بانک‌ها بسته به تعهدات قانونی و مقرراتی، فرهنگ سازمانی، موقعیت جغرافیایی و اندازه خود می‌توانند از بین دو گزینه CSIRT داخلی یا خارجی یکی را انتخاب نمایند.

برنامه‌های BCM و DR : برنامه‌های تداوم کسب‌وکار (Business Continuity Management - BCM) و بازیابی در برابر بلایا (Disaster Recovery - DR) به بانک‌ها و موسسات مالی کمک می‌کند تا در صورت وقوع یک حادثه امنیتی، به سرعت فعالیت خود را بازیابی نمایند.

بیمه سایبری: خرید بیمه سایبری می‌تواند به جبران خسارات مالی ناشی از حوادث امنیتی کمک کند.

مسئولیت مؤسسه و کارمند برای اطمینان از جریان امن اطلاعات

درست است که وجود نرم‌افزارها و ابزارهای امنیتی در سازمان ضروری است، اما این به تنهایی کافی نیست. برای اینکه امنیت اطلاعات به طور کامل تضمین شود، لازم است که کارکنان نیز در این زمینه آگاهی و آموزش لازم را داشته باشند.

کارکنان می‌بایست:

- با تهدیدات امنیتی در حوزه کاری خود آشنا باشند.
- اهمیت ابزارهای امنیتی و نحوه استفاده صحیح از آنها را درک کنند.
- همیشه حواسشان باشد که اطلاعات را باید محرمانه نگه دارند.
- فریب اقدامات فریبنده و مهندسی اجتماعی را نخورند.

بانک‌ها و موسسات مالی باید در این زمینه پیشقدم شوند. این موسسات موظفند که تعهد خود را به امنیت اطلاعات نشان داده و منابع لازم را برای آموزش و آگاهی‌بخشی به کارکنان خود اختصاص دهند. با بالا بردن آگاهی و آموزش کارکنان، می‌توان تاب‌آوری سازمان در برابر تهدیدات سایبری را به طور قابل توجهی افزایش داد.

برخی از اقدامات ضروری در این زمینه عبارتند از:

- ❖ تدوین و اجرای سیاستی جامع در مورد نحوه مدیریت امنیت اطلاعات
- ❖ اختصاص اختیارات و منابع کافی به واحد امنیت اطلاعات برای انجام وظایف خود
- ❖ برگزاری جلسات آموزشی و آگاهی‌بخشی برای کارکنان در مورد خطمشی‌ها و فرآیندهای امنیتی
- ❖ آموزش نحوه انتخاب و استفاده از رمزهای عبور قوی و منحصر به فرد
- ❖ تعیین تکلیف در مورد نحوه استفاده از تجهیزات و دستگاه‌های متعلق به سازمان

استراتژی مداوم برای ایمن نگه داشتن اطلاعات

استراتژی امنیت اطلاعات باید از اهداف کسب و کار سازمان پشتیبانی کند. استفاده از اثربخشی و کارایی باید بهبود یابد تا خدمات بهتری برای مشتریان ارائه شود. در انجام عملیات امنیتی بابت اطلاعاتی که بانک در اختیار کارکنان قرار می دهد باید توجه ویژه ای داشته باشد و این امر به نحو مناسب و به موقع انجام شود. بانک‌ها و مؤسسات مالی باید به شدت متعهد به پیاده‌سازی یک سیستم مدیریتی برای مقابله با امنیت اطلاعات با بکارگیری افراد با تجربه و آشنا به مسائل امنیتی باشند.

پیاده‌سازی ISMS بر اساس استانداردهای مدیریتی، تضمین بزرگی است که یک سازمان الزامات نظارتی خود را رعایت می‌کند تا مراقب خطرات امنیت اطلاعات باشد و ISMS قادر است اطلاعات لازم را در اختیار کل سازمان قرار دهد. استاندارد سیستم مدیریت امنیت اطلاعات ISO/IEC 27001 تضمین می‌کند که سازمان‌ها خطرات امنیت اطلاعات را به شیوه‌ای ساختار یافته بررسی می کنند. سازمان‌هایی که گواهینامه ISO/IEC 27001 را دریافت می-نمایند، تأیید می‌کنند که امنیت اطلاعات مالی، مالکیت معنوی، جزئیات کارکنان، یا اطلاعاتی که از طرف اشخاص ثالث به آنها سپرده شده است با موفقیت مدیریت می شوند و به طور مستمر بر اساس رویکرد ها و چارچوب با بهترین عملکرد بهبود می یابند.

۲-آخرین فناوری‌های امنیت اطلاعات در دنیا

در این بخش با بعضی از فناوری‌های روز دنیا در حوزه امنیت اطلاعات آشنا خواهیم شد.

نماد افزودن کاربر تجزیه و تحلیل رفتاری

تجزیه و تحلیل رفتاری، دنیای دیجیتال را زیر ذره‌بین می‌برد تا الگوهای رفتاری کاربران را در وب‌سایت‌ها، اپلیکیشن‌های موبایل، سیستم‌ها و شبکه‌ها رمزگشایی کند. این ابزار قدرتمند در دستان متخصصان امنیت سایبری، به مثابه یک سپر نامرئی عمل می‌کند و به آنها در شناسایی تهدیدات و آسیب‌پذیری‌های پنهان یاری می‌رساند.

تجزیه و تحلیل رفتاری با موشکافی الگوهای رفتاری، رویدادها و اقدامات غیرعادی را آشکار می‌سازد و این دقیقاً همان نقطه‌ای است که می‌تواند زنگ خطر را برای تهدیدات سایبری به صدا درآورد.

تصور کنید حجم غیرمعمولی از داده‌ها ناگهان از یک دستگاه سرازیر می‌شود؛ این می‌تواند نشان‌دهنده یک حمله سایبری در حال وقوع یا در حال انجام باشد. زمان‌بندی عجیب و غریب رویدادها و اقداماتی که در توالی غیرطبیعی رخ می‌دهند، از دیگر شاخص‌هایی هستند که تجزیه و تحلیل رفتاری به مثابه یک ردیاب ماهر آن‌ها را آشکار می‌کند.

تجزیه و تحلیل رفتاری فراتر از صرف شناسایی تهدیدات عمل می‌کند و مزایای قابل توجهی را به ارمغان می‌آورد:

تشخیص زودهنگام: با شناسایی الگوهای مشکوک، حملات احتمالی را قبل از وقوع خنثی می‌کند.

پیش‌بینی تهدیدات: با تحلیل روندها، گامی پیشاپیش از تهدیدات آینده برداشته و تدابیر لازم را اتخاذ می‌کند.

خودکارسازی تشخیص و پاسخ: فرآیند شناسایی و مقابله با تهدیدات را به صورت خودکار انجام می‌دهد و از اتلاف زمان و خطای انسانی می‌کاهد.

در دنیای پرشتاب و پیچیده امروز، که تهدیدات سایبری به طور مداوم در حال تکامل هستند، اتکا به روش‌های سنتی امنیت سایبری کافی نیست. تجزیه و تحلیل رفتاری با ارائه یک دید عمیق از رفتار کاربران، به سازمان‌ها قدرت تشخیص و مقابله با تهدیدات را در زمانی می‌دهد که فرصت برای خنثی کردن آن‌ها وجود دارد.

بنابراین، سرمایه‌گذاری در تجزیه و تحلیل رفتاری، نه تنها ضرورتی انکارناپذیر برای ارتقای امنیت سایبری است، بلکه به مثابه گامی هوشمندانه در جهت حفظ دارایی‌ها، اطلاعات و اعتبار سازمان‌ها عمل می‌کند.

نماد مکعب بلاک چین

بلاک‌چین، فراتر از یک پایگاه داده ساده، تحولی شگرف در عرصه امنیت سایبری رقم زده است. این فناوری نوین، با معماری منحصر به فرد خود، گویی گاوصندوقی نفوذناپذیر برای داده‌ها عمل می‌کند و گامی بلند در جهت مصونیت بخشیدن به سیستم‌ها و اطلاعات در دنیای دیجیتال برمی‌دارد. در قلب بلاک‌چین، رمزنگاری و اتصال زنجیره‌وار بلوک‌ها نهفته است. داده‌ها در بلوک‌هایی امن ذخیره شده و به وسیله رمزنگاری به یکدیگر پیوند می‌خورند. این فرآیند، دستکاری یا حذف اطلاعات را غیرممکن می‌سازد و حافظی مطمئن برای نگهداری از آن‌ها به ارمغان می‌آورد.

بلاک‌چین، گنجینه‌ای از مزایا را برای ارتقای امنیت سایبری به ارمغان می‌آورد که از آن جمله می‌توان به موارد زیر اشاره نمود:

حریم خصوصی: با حفاظت از داده‌ها و هویت کاربران، حریم خصوصی را به طور چشمگیری ارتقا می‌دهد.

کاهش خطا: با حذف واسطه‌ها و ثبت خودکار تراکنش‌ها، خطای انسانی را به حداقل می‌رساند.

شفافیت: زنجیره شفاف و قابل ردیابی تراکنش‌ها، اعتمادی بی‌نظیر را در سیستم ایجاد می‌کند.

صرفه‌جویی در هزینه: با حذف نیاز به تأیید شخص ثالث، در هزینه‌ها صرفه‌جویی قابل توجهی به ارمغان می‌آورد.

این فناوری نوین، با ارائه راه‌حلی امن، شفاف و کارآمد، نقشی کلیدی در محافظت از اطلاعات و سیستم‌ها در دنیای دیجیتال ایفا می‌کند و گامی بلند به سوی آینده‌ای امن‌تر به شمار می‌رود.

نماد ساعت امنیتی Context-Aware

امنیت متن‌آگاه نوعی فناوری امنیت سایبری است که به کسب و کارها کمک می کند تا تصمیمات امنیتی بهتری را در زمان واقعی اتخاذ کنند.

فناوری‌های امنیت سایبری سنتی با پرسیدن سؤالات بله/خیر ارزیابی می‌کنند که آیا اجازه می‌دهند کسی به یک سیستم یا داده دسترسی داشته باشد یا نه. این فرآیند ساده می‌تواند باعث انکار برخی از کاربران قانونی شود و بهره‌وری را کاهش دهد.

امنیت متن آگاه احتمال ممانعت از ورود به یک کاربر مجاز را کاهش می دهد. به جای تکیه بر پاسخ به سوالات ثابت بله/خیر، امنیت متن‌آگاه از اطلاعات پشتیبانی مختلفی مانند زمان، مکان و شهرت URL برای ارزیابی قانونی بودن یا نبودن کاربر استفاده می‌کند.

امنیت متن آگاه فرآیندهای دسترسی به داده ها را ساده می‌کند و انجام کار را برای کاربران قانونی آسانتر می‌کند. با این حال، نگرانی های حفظ حریم خصوصی کاربر نهایی یک چالش است.

نماد بررسی سپر هوش مصنوعی دفاعی (AI)

در دنیای پیچیده و دائماً در حال تحول جنگ‌های سایبری، هوش مصنوعی (AI) به ابزاری حیاتی برای هر دو جبهه مدافعان و مهاجمان تبدیل شده است. در حالی که متخصصان امنیت سایبری از هوش مصنوعی دفاعی برای شناسایی و خنثی کردن تهدیدات سایبری استفاده می‌کنند، مجرمان سایبری نیز از هوش مصنوعی تهاجمی برای طراحی حملات پیچیده‌تر و مخفی‌تر بهره می‌برند. مجرمان سایبری از هوش مصنوعی تهاجمی برای طراحی ابزارها و روش‌های نوینی جهت فریب سیستم‌های امنیتی و نفوذ به شبکه‌ها استفاده می‌کنند. برخی از رایج‌ترین نمونه‌های هوش مصنوعی تهاجمی عبارتند از:

جعل عمیق: این فناوری برای ایجاد ویدیوها، تصاویر و صداهای جعلی به منظور فریب کاربران یا انتشار اطلاعات نادرست به کار می‌رود.

شخصیت‌های مجازی: مجرمان سایبری می‌توانند از هوش مصنوعی برای ایجاد چت‌بات‌ها و دستیارهای مجازی که می‌توانند با کاربران تعامل داشته باشند و اطلاعات حساس را از آنها سرقت کنند، استفاده کنند.

یادگیری ماشینی متخاصم: این روش از هوش مصنوعی برای آموزش مدل‌های یادگیری ماشین به منظور فریب دادن سیستم‌های امنیتی و دور زدن اقدامات حفاظتی استفاده می‌کند.

در مقابل این تهدیدات رو به رشد، متخصصان امنیت سایبری از هوش مصنوعی دفاعی برای تقویت جبهه دفاعی خود استفاده می‌کنند. هوش مصنوعی دفاعی طیف وسیعی از قابلیت‌ها را برای خنثی کردن حملات سایبری مبتنی بر هوش مصنوعی ارائه می‌دهد، از جمله:

تشخیص ناهنجاری: هوش مصنوعی می‌تواند الگوهای رفتاری غیرعادی در شبکه‌ها را شناسایی کند و از این طریق حملات سایبری را در مراحل اولیه شناسایی کند.

تحلیل تهدید: هوش مصنوعی می‌تواند نوع و دامنه یک حمله سایبری را به سرعت و با دقت تجزیه و تحلیل کند و به متخصصان امنیت سایبری در انتخاب روش مناسب برای مقابله با آن کمک کند.

تقویت سیستم‌ها: هوش مصنوعی می‌تواند نقاط ضعف سیستم‌های امنیتی را شناسایی کرده و برای رفع آنها راه‌حل‌هایی ارائه دهد.

با وجود این چالش‌ها، هوش مصنوعی به عنوان ابزاری قدرتمند در حال دگرگونی عرصه امنیت سایبری است. استفاده هوشمندانه از هوش مصنوعی دفاعی، کلید حفظ امنیت سازمان‌ها و زیرساخت‌های حیاتی در برابر تهدیدات سایبری پیچیده و رو به رشد در دنیای امروز است.

نماد تعجب Zero Trust

امنیت شبکه سنتی از شعار «اعتماد کن، اما تأیید کن» پیروی می‌کند، با این فرض که کاربران در محدوده شبکه یک سازمان، تهدیدات مخربی نیستند. از سوی دیگر، Zero Trust خود را با شعار "هرگز اعتماد نکنید، همیشه تأیید کنید" همسو می کند.

Zero Trust چارچوبی برای نزدیک شدن به امنیت شبکه، همه کاربران را قبل از دسترسی به داده‌ها یا برنامه‌های یک سازمان، احراز هویت می‌کند.

Zero Trust فرض نمی‌کند که کاربران داخل شبکه بیش از دیگران قابل اعتماد هستند. این بررسی دقیق تر روی همه کاربران می‌تواند منجر به امنیت اطلاعات کلی بیشتر برای سازمان شود.

متخصصان امنیت سایبری می توانند از Zero Trust برای مقابله ایمن‌تر با کارگران راه دور و چالش‌هایی مانند تهدیدات باج افزار استفاده کنند. یک چارچوب Zero Trust ممکن است ابزارهای مختلفی از جمله احراز هویت چند عاملی، رمزنگاری داده ها و امنیت نقطه پایانی را ترکیب کند.

تشخیص گسترده و پاسخ (XDR) – فراتر از مرزهای امنیت سایبری سنتی

در دنیای امروز که تهدیدات سایبری به طور مداوم در حال تکامل و پیچیده‌تر شدن هستند، راه‌حل‌های امنیتی سنتی دیگر پاسخگوی نیازها نیستند. در اینجا، تشخیص و پاسخ گسترده (XDR)به عنوان نسل جدیدی از فناوری‌های امنیتی، گامی بلند در جهت ارتقای سطح حفاظت از شبکه‌ها و داده‌ها برمی‌دارد.

XDR یکپارچه‌سازی و ارتقای قابلیت‌های EDR (تشخیص و پاسخ نقطه پایانی) است. این فناوری فراتر از نقاط پایانی عمل می‌کند و دید کاملی از کل محیط امنیتی، شامل شبکه، ابر و بارهای کاری را ارائه می‌دهد. XDR با جمع‌آوری و تجزیه و تحلیل داده‌ها از منابع مختلف، تصویری جامع از فعالیت‌ها در شبکه ایجاد می‌کند و به متخصصان امنیت سایبری امکان می‌دهد تا تهدیدات را به طور دقیق‌تر و سریع‌تر شناسایی و به آن‌ها پاسخ دهند.

با ارائه دید جامع، تشخیص و پاسخ سریع‌تر و اتوماسیون، XDR به سازمان‌ها در محافظت بهتر از شبکه‌ها و داده‌ها در برابر تهدیدات سایبری پیچیده و رو به رشد کمک می‌کند.

نماد شرح استفاده سازنده (Manufacturer Usage Description)

در دنیای امروز، اینترنت اشیا (IoT) نقشی حیاتی در زندگی روزمره ما ایفا می‌کند. با این حال، افزایش تعداد دستگاه‌های متصل به اینترنت، نگرانی‌هایی را در خصوص امنیت آن‌ها به وجود می‌آورد. گروه ضربت مهندسی اینترنت (IETF) با درک این چالش، اقدام به معرفی استاندارد (MUD) کرده است.

MUD استانداردی است که به منظور ارتقای امنیت دستگاه‌های IoT در مشاغل کوچک و شبکه‌های خانگی طراحی شده است. این استاندارد با ارائه مجموعه‌ای از الزامات و دستورالعمل‌های ساده، به تولیدکنندگان و توسعه‌دهندگان کمک می‌کند تا دستگاه‌های IoT را به گونه‌ای طراحی و تولید کنند که در برابر حملات سایبری رایج مقاوم باشند.

دستگاه‌های IoT به طور فزاینده‌ای در معرض حملات سایبری قرار دارند. این حملات می‌توانند منجر به سرقت اطلاعات حساس، اختلال در عملکرد دستگاه‌ها و حتی آسیب‌های فیزیکی شوند. MUD با ارائه چارچوبی ساده و کارآمد، به ایمن‌تر شدن دستگاه‌های IoT و محافظت از آن‌ها در برابر این تهدیدات کمک می‌کند. MUD با ارائه راهکاری ساده و مقرون به صرفه، گامی بلند در جهت ارتقای امنیت دستگاه‌های IoT در مشاغل کوچک و شبکه‌های خانگی برمی‌دارد. این استاندارد به تولیدکنندگان، توسعه‌دهندگان و متخصصان امنیت سایبری کمک می‌کند تا دستگاه‌های IoT را به گونه‌ای طراحی، تولید و مدیریت کنند که در برابر تهدیدات سایبری امروزی مقاوم باشند.

نماد تنظیم مقررات

از آنجایی که فراوانی حملات سایبری هر سال به طور قابل توجهی در حال افزایش است، دولت‌ها شروع به استفاده و ترویج قوانین بهترین عملکرد کرده‌اند. در گذشته، دولت‌ها اغلب درگیر مسائل امنیت سایبری نمی‌شدند. این تحولات در مقررات امنیت سایبری، تاثیرات قابل توجهی بر سازمان‌ها دارد. سازمان‌ها باید برای انطباق با مقررات جدید، اقدامات امنیتی خود را ارتقا دهند. این امر شامل موارد زیر می‌شود:

ارزیابی و به‌روزرسانی برنامه‌های امنیتی موجود: سازمان‌ها باید به طور منظم برنامه‌های امنیتی خود را ارزیابی کنند تا از انطباق آن‌ها با آخرین قوانین و مقررات اطمینان حاصل شود.

ایجاد و اجرای کنترل‌های امنیتی جدید: سازمان‌ها ممکن است نیاز به ایجاد و اجرای کنترل‌های امنیتی جدیدی برای برآورده کردن الزامات خاص قوانین و مقررات جدید داشته باشند.

آموزش و آگاهی‌بخشی به کارکنان: کارکنان باید در مورد قوانین و مقررات جدید امنیت سایبری و نحوه تأثیر آنها بر سازمان آموزش ببینند.

مدیریت ریسک سایبری: سازمان‌ها باید به طور مداوم ریسک‌های سایبری خود را ارزیابی و مدیریت کنند و اقداماتی را برای کاهش این ریسک‌ها انجام دهند.

افزایش نقش دولت‌ها در امنیت سایبری مزایای متعددی دارد، از جمله:

بهبود حفاظت از داده‌ها: قوانین و مقررات جدید می‌توانند به محافظت بهتر از داده‌های کاربران در برابر دسترسی غیرمجاز، افشا و سوء استفاده کمک کنند.

کاهش حملات سایبری: الزامات امنیتی قوی‌تر می‌تواند به کاهش تعداد و شدت حملات سایبری کمک کند. و ایجاد یک فضای آنلاین امن‌تر: با افزایش امنیت سایبری، اعتماد به نفس کاربران برای استفاده از اینترنت افزایش می‌یابد و این امر می‌تواند منجر به نوآوری و رشد اقتصادی بیشتر شود.

اداره امنیت فناوری اطلاعات