ماهنامه برنا

Borna Network Managers
مدیران شبکه برنا

اخبار حوزه امنیت و شبکه (تیر ۱۴۰۵)

در این شماره، تازه‌ترین تحولات امنیت سایبری از فعالیت گروه‌های APT و شبکه‌های مخفی ORB تا جنگ سایبری در بحران‌های ژئوپلیتیکی، آینده احراز هویت بدون رمز عبور (Passkey) و نقش مدیران در مدیریت ریسک‌های سایبری بررسی شده است. همچنین با راهکارهای نوین دفاع چندلایه شامل DLP، PAM، NDR، XDR، EDR و Threat Intelligence برای مقابله با تهدیدات پیشرفته آشنا می‌شوید.

ویژه مدیران و کارشناسان شبکه و امنیت

www.bornanetwork.co
info@bornanetwork.co
۰۲۱-۷۴۰۲۸

خبرنامه امنیت سایبری - تیر ماه ۱۴۰۵

گروه چینی UAT-7810 شبکه مخفی ORB خود را با بدافزار جدید LONGLEASH گسترش داد

محققان امنیتی Cisco Talos از فعالیت گسترده یک گروه تهدید پیشرفته (APT) با منشأ چین به نام UAT-7810 خبر داده‌اند که با توسعه بدافزار جدید LONGLEASH در حال گسترش شبکه مخفی Operational Relay Box (ORB) خود است. این شبکه از دستگاه‌های اینترنتی آلوده برای پنهان کردن منشأ حملات سایبری و هدایت عملیات سایر مهاجمان استفاده می‌کند.

ORB چیست؟

شبکه ORB مجموعه‌ای از روترها، تجهیزات شبکه و دستگاه‌های اینترنت اشیا (IoT) است که پس از آلوده شدن به عنوان سرورهای واسط (Relay) عمل می‌کنند. مهاجمان با عبور دادن ترافیک خود از این دستگاه‌ها، هویت واقعی و محل حملاتشان را مخفی می‌کنند و ردیابی عملیات را برای مدافعان بسیار دشوار می‌سازند.

LONGLEASH نسل جدید ابزارهای نفوذ

بررسی‌های Cisco Talos نشان می‌دهد نسخه جدید بدافزار LONGLEASH نسبت به نسخه قبلی (SHORTLEASH) قابلیت‌های پیشرفته‌تری در اختیار مهاجمان قرار می‌دهد، از جمله:

- ایجاد تونل و پروکسی برای پروتکل‌های HTTP، DNS، SOCKS، UDP، TCP و ICMP
- ایفای نقش به‌عنوان سرور واسط فرماندهی و کنترل (C2)
- مدیریت ارتباط میان گره‌های آلوده
- حذف خودکار بدافزار و آثار آن در صورت تشخیص دستکاری یا تحلیل سیستم

علاوه بر LONGLEASH، دو ابزار جدید دیگر نیز شناسایی شده‌اند:

- DOGLEASH یک بک‌دور لینوکسی برای اجرای کد دلخواه روی دستگاه آلوده
- JARLEASH ابزاری مبتنی بر Java برای مدیریت فایل‌ها، FTP، SFTP و دسترسی از راه دور به سرورهای آلوده

همچنین ابزار LEASHTEST برای آزمایش عملکرد بدافزار روی تجهیزات مبتنی بر معماری MIPS مورد استفاده قرار گرفته است.

www.bornanetwork.co
info@bornanetwork.co
۰۲۱-۷۴۰۲۸

روترهای اینترنتی هدف اصلی مهاجمان

این گروه برای نفوذ به تجهیزات شبکه از آسیب‌پذیری‌های شناخته‌شده اما وصله‌نشده در روترهای Ruckus و ASUS AiCloud سوءاستفاده می‌کند. پس از آلوده شدن دستگاه، آن را به یکی از گره‌های شبکه ORB تبدیل می‌کند تا سایر گروه‌های وابسته بتوانند حملات خود را از طریق آن انجام دهند.

تهدید برای سازمان‌ها

کارشناسان معتقدند هدف اصلی UAT-7810 سرقت مستقیم اطلاعات نیست؛ بلکه ایجاد زیرساختی مخفی برای استفاده سایر گروه‌های وابسته به چین در حملات آینده است. به همین دلیل، سازمان‌هایی که از تجهیزات شبکه در معرض اینترنت استفاده می‌کنند باید بروزرسانی امنیتی روترها، پایش تجهیزات لبه شبکه و نظارت بر ترافیک غیرعادی را در اولویت قرار دهند.

راهکارهای Endpoint Detection & Response (EDR) قادر هستند رفتارهای غیرعادی، اجرای فایل‌های مشکوک، ارتباطات غیرمجاز و فعالیت‌های پس از نفوذ را شناسایی و قبل از گسترش حمله متوقف کنند.

XDR دید جامع نسبت به کل زنجیره حمله

در حملاتی مانند UAT-7810 معمولاً چندین لایه از زیرساخت سازمان به صورت همزمان هدف قرار می‌گیرند؛ از تجهیزات شبکه گرفته تا سرورها، End-pointها و سرویس‌های ایمیل.

راهکارهای Extended Detection & Response (XDR) با تجمیع رخدادهای امنیتی از منابع مختلف، ارتباط بین این رویدادها را شناسایی کرده و امکان کشف حملات پیچیده و چندمرحله‌ای را فراهم می‌کنند.

NDR پایش ترافیک شبکه

از آنجا که بدافزار LONGLEASH ارتباطات متعددی با سرورهای فرماندهی و کنترل (C2) برقرار می‌کند، استفاده از راهکارهای Network Detection & Response (NDR) می‌تواند ارتباطات غیرعادی، تونل‌های ناشناس و ترافیک مشکوک را در سریع‌ترین زمان ممکن شناسایی کند.

Threat Intelligence شناسایی تهدیدات پیش از وقوع حمله

یکی از مهم‌ترین نکات این گزارش، استفاده مهاجمان از زیرساخت‌های شناخته‌شده و کمپین‌های قبلی است.

راهکارهای Threat Intelligence با جمع‌آوری اطلاعات تهدید از منابع معتبر، امکان شناسایی IPها، دامنه‌ها، بدافزارها و تاکتیک‌های مورد استفاده مهاجمان را پیش از وقوع حمله فراهم می‌کنند.

PAM جلوگیری از سوءاستفاده از حساب‌های دارای دسترسی بالا

در صورتی که مهاجم موفق به نفوذ اولیه شود، معمولاً تلاش می‌کند به حساب‌های دارای دسترسی بالا دست پیدا کند.

راهکارهای Privileged Access Management (PAM) مانند ARCON PAM و Sectona PAM با مدیریت و کنترل دسترسی‌های حساس، ضبط نشست‌ها، اعمال احراز هویت چندعاملی و مدیریت رمزهای عبور، احتمال موفقیت مهاجم در حرکت جانبی (Lateral Movement) را به میزان قابل توجهی کاهش می‌دهند.

DLP؛ جلوگیری از خروج اطلاعات

اگر هدف نهایی مهاجم سرقت اطلاعات سازمان باشد، راهکارهای Data Loss Prevention (DLP) مانند Safetica و Zecurion DLP می‌توانند از انتقال غیرمجاز فایل‌ها، اسناد و اطلاعات حساس از طریق ایمیل، USB، فضای ابری یا پیام‌رسان‌ها جلوگیری کنند.

مدیریت آسیب‌پذیری (Vulnerability Management)

در این حمله، مهاجمان از آسیب‌پذیری‌های وصله‌نشده تجهیزات شبکه سوءاستفاده کرده‌اند. بنابراین استفاده از راهکارهای Vulnerability Assessment و اجرای فرآیند مستمر Patch Management، یکی از مهم‌ترین اقدامات برای کاهش ریسک چنین حملاتی محسوب می‌شود.

جمع‌بندی

حمله اخیر گروه UAT-7810 نشان می‌دهد که مهاجمان امروزی از ترکیب آسیب‌پذیری‌های تجهیزات شبکه، بدافزارهای پیشرفته و زیرساخت‌های مخفی برای اجرای حملات پیچیده استفاده می‌کنند. مقابله با این تهدیدات تنها با یک آنتی‌ویروس امکان‌پذیر نیست و سازمان‌ها باید از معماری امنیتی چندلایه شامل EDR، XDR، NDR، Threat Intelligence، PAM، DLP و مدیریت مستمر آسیب‌پذیری‌ها بهره بگیرند تا بتوانند حملات را در مراحل اولیه شناسایی و از گسترش آن‌ها جلوگیری کنند.

دیدگاه مدیران شبکه برنا

امنیت سایبری امروز تنها به پیشگیری محدود نمی‌شود؛ آنچه اهمیت دارد، توانایی سازمان در شناسایی سریع، پاسخ مؤثر و جلوگیری از گسترش حمله است. راهکارهایی نظیر ESET Protect (EDR/XDR)، Safetica DLP و Zecurion DLP، ARCON PAM و سرویس‌های Threat Intelligence Threat Mon، در کنار یکدیگر لایه‌های دفاعی لازم برای مقابله با تهدیدات پیشرفته‌ای مانند UAT-7810 را فراهم می‌کنند.

واکنش‌های فضای دارک وب به درگیری نظامی ایران و اسرائیل؛ افزایش حملات سایبری و فعالیت گروه‌های Hacktivist

درگیری‌های اخیر میان ایران، اسرائیل و ایالات متحده تنها به میدان‌های نظامی محدود نشده است. همزمان با افزایش تنش‌های منطقه‌ای، فضای سایبری نیز شاهد موج جدیدی از فعالیت گروه‌های Hacktivist ، انتشار اطلاعات در شبکه‌های اجتماعی و افزایش عملیات تبلیغاتی در دارک وب بوده است.

بررسی‌های انجام‌شده نشان می‌دهد بسیاری از گروه‌های فعال در دارک وب و پیام‌رسان‌هایی مانند Telegram تلاش کرده‌اند از این بحران برای اجرای حملات سایبری، انتشار روایت‌های رسانه‌ای و جنگ روانی استفاده کنند.

افزایش فعالیت گروه‌های Hacktivist

پس از آغاز حملات نظامی، فعالیت گروه‌های Hacktivist به شکل محسوسی افزایش یافت. این گروه‌ها معمولاً با انگیزه‌های سیاسی یا ایدئولوژیک اقدام به انجام حملات سایبری علیه سازمان‌ها و زیرساخت‌های کشورهای درگیر می‌کنند.

رایج‌ترین حملات مشاهده‌شده عبارت بودند از:

- حملات منع سرویس توزیع‌شده (DDoS)
- تغییر ظاهر وب‌سایت‌ها (Website Defacement)
- انتشار اطلاعات و اسناد سرقت‌شده (Data Leak)
- حملات تبلیغاتی و جنگ رسانه‌ای

در بسیاری از موارد، اهداف این حملات شامل سازمان‌های دولتی، شرکت‌های مخابراتی و زیرساخت‌های حیاتی منطقه بوده است.

تمرکز حملات بر کشورهای خاورمیانه

بر اساس گزارش‌های منتشرشده توسط شرکت‌های امنیت سایبری، تنها در روزهای ابتدایی بحران ده‌ها سازمان در خاورمیانه هدف حملات DDoS قرار گرفتند. بخش عمده این حملات علیه سازمان‌های دولتی، مراکز زیرساختی، شرکت‌های مخابراتی و نهادهای عمومی صورت گرفته است.

برخی گروه‌های Hacktivist نیز آشکارا حمایت خود را از یکی از طرفین درگیری اعلام کرده و حملات خود را با اهداف سیاسی توجیه کرده‌اند.

تلگرام؛ مرکز اصلی جنگ اطلاعاتی

همزمان با حملات سایبری، Telegram به یکی از مهم‌ترین بسترهای انتشار اخبار و عملیات روانی تبدیل شد. در این شبکه موارد زیر به‌صورت گسترده منتشر شد:

- تصاویر حملات موشکی
- ویدئوهای خسارات جنگ
- اطلاعیه‌های رسمی
- هشدارهای امنیتی
- تحلیل‌های سیاسی
- تصاویر تولیدشده توسط هوش مصنوعی

در بسیاری از موارد، صحت این تصاویر قابل تأیید نبوده و ترکیبی از محتوای واقعی، تصاویر قدیمی و تصاویر تولیدشده با هوش مصنوعی مشاهده شده است.

استفاده از هوش مصنوعی در عملیات رسانه‌ای

یکی از نکات قابل توجه این بحران، افزایش استفاده از تصاویر و ویدئوهای تولیدشده توسط هوش مصنوعی بود. گروه‌های مختلف با انتشار این محتوا تلاش کردند:

- روایت موردنظر خود را تقویت کنند.
- افکار عمومی را تحت تأثیر قرار دهند.
- فضای رسانه‌ای را مدیریت کنند.
- اخبار جعلی را با تصاویر واقعی ترکیب نمایند.

این روند تشخیص اطلاعات معتبر را برای کاربران دشوارتر کرده است.

واکنش گروه‌های افراطی

برخی گروه‌های افراطی نیز از این بحران برای انتشار پیام‌های تبلیغاتی خود استفاده کردند. در میان این گروه‌ها می‌توان به موارد زیر اشاره کرد:

- گروه‌های برتری‌طلب سفیدپوست
- جریان‌های نئونازی
- گروه‌های افراط‌گرای مذهبی
- شبکه‌های وابسته به داعش و القاعده

این گروه‌ها تلاش کرده‌اند در بسترهای مختلف، روایت‌های ایدئولوژیک خود را با تحولات نظامی منطقه پیوند دهند.

فعالیت گروه‌های وابسته به ایران

کانال‌های منتسب به گروه‌های همسو با ایران نیز فعالیت قابل توجهی در Telegram داشته‌اند.

محتوای منتشرشده شامل ادعای انجام عملیات نظامی، انتشار تصاویر تبلیغاتی، معرفی اهداف احتمالی، پیام‌های ایدئولوژیک، تصاویر فرماندهان و شخصیت‌های سیاسی بوده است. این محتوا عمدتاً با هدف تقویت جنگ روانی و افزایش حمایت رسانه‌ای منتشر شده است.

تهدیدات سایبری در شرایط بحران

بررسی رفتار بازیگران سایبری نشان می‌دهد در شرایط تنش‌های ژئوپلیتیکی معمولاً شاهد افزایش تهدیدات زیر هستیم:

- حملات DDoS
- حملات باج‌افزاری
- افشای اطلاعات سازمانی
- فیشینگ هدفمند
- حملات علیه زیرساخت‌های حیاتی
- انتشار اخبار جعلی
- عملیات نفوذ با اهداف اطلاعاتی

به همین دلیل سازمان‌ها باید علاوه بر تقویت تجهیزات امنیتی، پایش مستمر فضای دارک وب، شبکه‌های اجتماعی و کانال‌های تهدید را نیز در دستور کار خود قرار دهند.

خبرنامه امنیت سایبری - تیر ماه ۱۴۰۵

اهمیت مدیریت زیرساخت‌های امنیتی در شرایط بحران

در کنار تهدیدات ناشی از حملات سایبری، رخدادهای اخیر، نشان داده‌اند که اختلال در مؤلفه‌های حیاتی زیرساخت امنیتی، حتی در صورت نبود شواهدی از نفوذ یا حمله سایبری، می‌تواند بر دسترس‌پذیری و تداوم ارائه خدمات الکترونیکی تأثیرگذار باشد. ازاین‌رو، سازمان‌ها باید علاوه بر مقابله با تهدیدات خارجی، مدیریت چرخه عمر گواهی‌های دیجیتال (Digital Certificate Lifecycle Management)، پایش مستمر تجهیزات امنیتی و آمادگی برای مواجهه با خطاهای عملیاتی را نیز به‌عنوان بخشی از راهبرد امنیت سایبری خود در نظر بگیرند. چنین رویکردی نقش مهمی در افزایش تاب‌آوری زیرساخت‌های حیاتی و کاهش ریسک اختلال در سرویس‌های حساس ایفا می‌کند.

جمع‌بندی

تحولات اخیر نشان می‌دهد جنگ‌های مدرن تنها در میدان‌های نظامی جریان ندارند؛ فضای سایبری، دارک وب و شبکه‌های اجتماعی نیز به بخش جدایی‌ناپذیر از این درگیری‌ها تبدیل شده‌اند. از سوی دیگر، رخدادهای عملیاتی مرتبط با زیرساخت‌های امنیتی نیز نشان می‌دهد که حفظ پایداری خدمات تنها به مقابله با حملات سایبری محدود نمی‌شود و مدیریت صحیح دارایی‌های امنیتی، گواهی‌های دیجیتال، تجهیزات حیاتی و فرآیندهای عملیاتی نیز نقش تعیین‌کننده‌ای در تداوم کسب‌وکار دارد.گروه‌های Hack-tivist، جریان‌های افراطی و بازیگران سایبری با بهره‌گیری از حملات سایبری، انتشار اطلاعات و عملیات روانی تلاش می‌کنند بر روند تحولات تأثیر بگذارند.

در چنین شرایطی، استفاده از راهکارهای Threat In-telligence، Dark Web Monitoring، SOC و سامانه‌های پایش تهدیدات می‌تواند نقش مهمی در شناسایی زودهنگام حملات و کاهش ریسک سازمان‌ها ایفا کند. شرکت مدیران شبکه برنا پیشرو در ارائه خدمات و راهکارهای امنیتی با بیش از 15 سال سابقه، با ارائه راهکار Threat Mon می‌تواند در این راستا پاسخگوی نیازها و چالش‌های موازی با موارد مذکور باشد. جهت آشنایی بیشتر با این راهکار و همچنین راهکارهای امنیتی دیگر با ما در ارتباط باشید.

چرا مایکروسافت دیگر به SMS اعتماد ندارد؟

سال‌ها دریافت یک کد پیامکی، آخرین مرحله برای ورود به حساب‌های کاربری بود و بسیاری از کاربران آن را مطمئن‌ترین روش احراز هویت می‌دانستند. اما اکنون مایکروسافت تصمیم گرفته این روش را به‌تدریج کنار بگذارد و کاربران را به استفاده از فناوری Passkey تشویق کند؛ تصمیمی که نشان می‌دهد چشم‌انداز امنیت سایبری در حال تغییر است و روش‌های سنتی دیگر پاسخگوی تهدیدهای امروزی نیستند.

چرا پیامک دیگر امن نیست؟

زمانی که احراز هویت دومرحله‌ای (2FA) معرفی شد، تحول بزرگی در امنیت حساب‌های کاربری ایجاد کرد. حتی اگر رمز عبور یک کاربر به سرقت می‌رفت، مهاجم بدون کد ارسال‌شده از طریق پیامک نمی‌توانست وارد حساب شود.

اما مجرمان سایبری نیز بیکار ننشستند. آن‌ها با توسعه روش‌های جدید، توانستند این لایه امنیتی را نیز هدف قرار دهند.

یکی از شناخته‌شده‌ترین این حملات SIM Swapping یا جابه‌جایی سیم‌کارت است. در این روش، مهاجم با استفاده از مهندسی اجتماعی یا سوءاستفاده از فرایندهای اپراتور تلفن همراه، شماره تلفن قربانی را به سیم‌کارت دیگری منتقل می‌کند. از آن لحظه تمام پیامک‌های حاوی کدهای امنیتی مستقیماً به دستگاه مهاجم ارسال می‌شود.

به همین دلیل، حتی داشتن یک رمز عبور قوی نیز همیشه تضمین‌کننده امنیت حساب نخواهد بود.

رمز عبور؛ ضعیف‌ترین حلقه زنجیره امنیت

امروزه بسیاری از حملات سایبری نه با نفوذ مستقیم به سرورها، بلکه از طریق حساب‌های کاربری آغاز می‌شوند.

استفاده از رمزهای عبور تکراری، انتخاب رمزهای ساده، ذخیره اطلاعات ورود در مرورگرهای ناامن یا فریب خوردن در حملات فیشینگ، همچنان از مهم‌ترین دلایل نفوذ به حساب‌های کاربران هستند.

به همین دلیل شرکت‌های بزرگ فناوری به این نتیجه رسیده‌اند که آینده امنیت دیجیتال، در حذف وابستگی به رمز عبور و استفاده از روش‌های نوین احراز هویت است.

Passkey چیست؟

Passkey نسل جدید احراز هویت محسوب می‌شود.

در این روش دیگر نیازی به حفظ کردن رمز عبور یا دریافت کد پیامکی نیست. کاربر تنها با اثر انگشت، تشخیص چهره یا PIN دستگاه خود هویتش را تأیید می‌کند.

نکته مهم این است که اطلاعات بیومتریک هرگز از دستگاه خارج نمی‌شود. وب‌سایت یا سرویس آنلاین تنها یک تأییدیه رمزنگاری‌شده دریافت می‌کند و هیچ‌گاه به اثر انگشت یا تصویر چهره کاربر دسترسی نخواهد داشت.

همین ویژگی باعث می‌شود حملاتی مانند فیشینگ، سرقت رمز عبور و بسیاری از روش‌های مهندسی اجتماعی تا حد زیادی بی‌اثر شوند.

این تغییر فقط مخصوص مایکروسافت نیست
حرکت به سمت Passwordless Authentication تنها به مایکروسافت محدود نمی‌شود. بسیاری از شرکت‌های بزرگ فناوری طی سال‌های اخیر سرمایه‌گذاری گسترده‌ای روی این فناوری انجام داده‌اند.
دلیل آن نیز روشن است؛ تجربه نشان داده است که در بسیاری از رخدادهای امنیتی، مهاجمان از آسیب‌پذیری‌های فنی وارد شبکه نمی‌شوند، بلکه از طریق حساب‌های کاربری و اطلاعات هویتی به اهداف خود می‌رسند.
به همین دلیل، کارشناسان امنیت توصیه می‌کنند کاربران در صورت امکان از Passkey یا نرم‌افزارهای تولیدکننده کد یکبارمصرف (Authenticator) به جای پیامک استفاده کنند.
امنیت فقط به حساب کاربری ختم نمی‌شود
اگرچه محافظت از هویت کاربران اهمیت بالایی دارد، اما امنیت تنها به مرحله ورود به حساب محدود نمی‌شود.
در بسیاری از حملات، مهاجم پس از دسترسی به حساب یک کاربر، تلاش می‌کند در شبکه حرکت کند، به فایل‌های سازمانی دسترسی پیدا کند یا اطلاعات حساس را استخراج کند.
به همین دلیل امروزه سازمان‌ها از مفهوم امنیت لایه‌ای (Defense in Depth) استفاده می‌کنند؛ رویکردی که در آن، احراز هویت تنها یکی از چندین لایه دفاعی است.

راهکارهایی مانند حفاظت از نقاط پایانی (End-point Security)، کنترل دسترسی، پایش مداوم شبکه، شناسایی رفتارهای مشکوک و محافظت از داده‌ها، در کنار هم احتمال موفقیت مهاجمان را به حداقل می‌رسانند.
آینده امنیت؛ بدون رمز عبور
تصمیم مایکروسافت نشان می‌دهد صنعت امنیت سایبری وارد مرحله تازه‌ای شده است.
چند سال پیش داشتن یک رمز عبور پیچیده کافی به نظر می‌رسید. سپس احراز هویت دومرحله‌ای به یک استاندارد تبدیل شد و اکنون Passkey در حال تبدیل شدن به نسل جدید احراز هویت است.
این فناوری علاوه بر افزایش امنیت، تجربه کاربری را نیز ساده‌تر می‌کند؛ زیرا دیگر نیازی به حفظ ده‌ها رمز عبور یا انتظار برای دریافت پیامک نخواهد بود.
سوالات متداول
چرا مایکروسافت احراز هویت پیامکی را حذف می‌کند؟
زیرا پیامک در برابر حملاتی مانند SIM Swapping، رهگیری پیامک و مهندسی اجتماعی آسیب‌پذیر است و دیگر امنیت کافی برای حفاظت از حساب‌های کاربران را فراهم نمی‌کند.

جایگزین پیامک چیست؟

مایکروسافت استفاده از Passkey را پیشنهاد می‌کند؛ روشی که با استفاده از اثر انگشت، تشخیص چهره یا PIN دستگاه، بدون نیاز به رمز عبور یا پیامک، هویت کاربر را تأیید می‌کند.

آیا احراز هویت پیامکی کاملاً ناامن است؟

خیر. استفاده از پیامک همچنان از نداشتن احراز هویت دومرحله‌ای بسیار امن‌تر است، اما در مقایسه با روش‌هایی مانند Passkey یا Authenticator، سطح امنیت پایین‌تری دارد و در برابر برخی حملات آسیب‌پذیر است.

آیا همچنان می‌توان با رمز عبور وارد حساب مایکروسافت شد؟

بله. در حال حاضر امکان ورود با رمز عبور همچنان وجود دارد، اما مایکروسافت کاربران را به استفاده از روش‌های بدون رمز عبور مانند Passkey تشویق می‌کند.

جمع‌بندی

تصمیم مایکروسافت برای فاصله گرفتن از پیامک، تنها یک تغییر در شیوه ورود به حساب‌های کاربری نیست؛ بلکه نشانه‌ای از تغییر رویکرد صنعت امنیت سایبری است.

امروزه دیگر اتکا به یک رمز عبور یا حتی یک کد پیامکی برای محافظت از اطلاعات کافی نیست. امنیت مؤثر زمانی شکل می‌گیرد که چندین لایه دفاعی در کنار یکدیگر قرار گیرند؛ از احراز هویت امن گرفته تا حفاظت از دستگاه‌ها، شبکه و داده‌های سازمان.

چرا مدیران هنوز امنیت سایبری را یک هزینه می‌بینند؟

تقریباً همه مدیران ارشد سازمان‌ها یک هدف مشترک دارند؛ رشد کسب‌وکار، افزایش درآمد و حفظ مزیت رقابتی. برای رسیدن به این اهداف، بودجه‌های قابل توجهی صرف توسعه محصولات، بازاریابی، فروش و فناوری می‌شود. اما هنوز هم در بسیاری از سازمان‌ها، امنیت سایبری به‌عنوان یک هزینه دیده می‌شود، نه یک سرمایه‌گذاری.

در حالی که متخصصان امنیت معتقدند امروزه بزرگ‌ترین ریسک بسیاری از سازمان‌ها، نه رقبا بلکه حملات سایبری است.

شکاف میان مدیران و تیم امنیت

بر اساس پژوهشی که شرکت MetaCompliance با مشارکت بیش از ۲۰۰ مدیر امنیت اطلاعات (CISO) در اروپا انجام داده است، حدود ۷۸ درصد از مدیران امنیت معتقدند مدیران ارشد سازمان‌ها درک درستی از تهدیدهای سایبری امروز ندارند.

بیشتر این مدیران اعلام کرده‌اند که هیئت‌مدیره و مدیران اجرایی، نقش کارکنان در ایجاد یا جلوگیری از حملات سایبری را دست‌کم می‌گیرند و تصور می‌کنند امنیت صرفاً وظیفه واحد فناوری اطلاعات است.

در حالی که واقعیت چیز دیگری است.

بزرگ‌ترین نقطه ضعف؛ انسان

بسیاری تصور می‌کنند هکرها با استفاده از ابزارهای بسیار پیچیده از دیوارهای امنیتی عبور می‌کنند، اما در عمل، بخش زیادی از حملات از یک اشتباه ساده انسانی آغاز می‌شود.

کلیک روی یک لینک جعلی، دانلود یک فایل آلوده یا اعتماد به یک ایمیل جعلی می‌تواند راه ورود مهاجم به کل شبکه سازمان باشد.

به همین دلیل است که متخصصان امنیت همواره می‌گویند:

قوی‌ترین فایروال دنیا هم نمی‌تواند از اشتباه یک کاربر جلوگیری کند.

هوش مصنوعی، حملات را واقعی‌تر کرده است

در گذشته بسیاری از ایمیل‌های فیشینگ به‌راحتی قابل شناسایی بودند؛ متن‌های ضعیف، غلط‌های نگارشی و ظاهر غیرحرفه‌ای آن‌ها باعث می‌شد کاربران راحت‌تر متوجه جعلی بودنشان شوند.

اما امروز شرایط کاملاً تغییر کرده است.

مهاجمان از هوش مصنوعی برای تولید ایمیل‌های کاملاً طبیعی، وب‌سایت‌های جعلی، تقلید صدا (Voice Cloning) و حتی ویدئوهای دیپ‌فیک استفاده می‌کنند.

در نتیجه تشخیص حملات روزبه‌روز دشوارتر می‌شود و اتکا به تجربه شخصی کارکنان دیگر کافی نیست.

امنیت، مسئولیت همه سازمان است

یکی از مهم‌ترین پیام‌های این پژوهش آن است که امنیت سایبری دیگر فقط وظیفه واحد IT نیست.

از مدیرعامل گرفته تا کارمند تازه‌وارد، همه در امنیت سازمان نقش دارند.

اگر مدیران بودجه آموزش امنیت را حذف کنند، اجرای احراز هویت چندمرحله‌ای را به تعویق بیندازند یا برنامه مشخصی برای مقابله با حوادث نداشته باشند، احتمال موفقیت مهاجمان به‌مراتب افزایش پیدا می‌کند.

هزینه پیشگیری یا هزینه بحران؟

گاهی برخی سازمان‌ها برای صرفه‌جویی، بودجه امنیت را کاهش می‌دهند. اما تجربه نشان داده است که هزینه یک حمله موفق می‌تواند چندین برابر هزینه پیشگیری باشد.

نشت اطلاعات مشتریان، توقف خدمات، پرداخت باج، جریمه‌های قانونی و از بین رفتن اعتماد مشتریان تنها بخشی از خسارت‌هایی است که ممکن است یک حمله سایبری ایجاد کند.

به همین دلیل بسیاری از مدیران موفق، امنیت را یک سرمایه‌گذاری برای حفظ تداوم کسب‌وکار می‌دانند، نه یک هزینه اضافی.

امنیت فقط خرید تجهیزات نیست

اشتباه رایج دیگر این است که تصور شود خرید یک فایروال یا آنتی‌ویروس قدرتمند به‌تنهایی امنیت سازمان را تضمین می‌کند.

در حالی که امنیت واقعی از ترکیب چندین لایه دفاعی شکل می‌گیرد؛ از جمله:

- آموزش مستمر کارکنان
- اجرای احراز هویت چندعاملی (MFA)
- شبیه‌سازی حملات فیشینگ
- مدیریت دسترسی کاربران
- پایش مداوم شبکه
- برنامه واکنش به رخدادهای امنیتی
- به‌روزرسانی مستمر تجهیزات و نرم‌افزارها

این همان چیزی است که متخصصان از آن با عنوان دفاع چندلایه (Defense in Depth) یاد می‌کنند.

جمع‌بندی

با پیچیده‌تر شدن حملات سایبری و استفاده روزافزون مهاجمان از هوش مصنوعی، امنیت دیگر یک موضوع فنی صرف نیست؛ بلکه به یکی از مهم‌ترین موضوعات مدیریتی تبدیل شده است.

سازمان‌هایی که امنیت را تنها مسئولیت واحد فناوری اطلاعات می‌دانند، دیر یا زود هزینه این نگاه را خواهند پرداخت. در مقابل، کسب‌وکارهایی که امنیت را در تصمیم‌های مدیریتی، بودجه‌ریزی و فرهنگ سازمانی خود جای می‌دهند، آمادگی بیشتری برای مقابله با تهدیدهای آینده خواهند داشت.

سوالات متداول

چرا بسیاری از مدیران امنیت از مدیران ارشد سازمان‌ها انتقاد می‌کنند؟

زیرا بسیاری از مدیران ارشد هنوز امنیت سایبری را یک موضوع صرفاً فنی یا هزینه‌بر می‌دانند و اهمیت آن را در مدیریت ریسک‌های کسب‌وکار به‌طور کامل درک نکرده‌اند.

چرا امروزه حملات فیشینگ موفق‌تر از گذشته هستند؟

مهاجمان با استفاده از هوش مصنوعی، ایمیل‌ها، صفحات جعلی، تقلید صدا و حتی ویدئوهای دیپ‌فیک بسیار واقعی تولید می‌کنند که تشخیص آن‌ها برای کاربران دشوارتر شده است.

آیا امنیت سایبری فقط وظیفه واحد فناوری اطلاعات (IT) است؟

خیر. امنیت یک مسئولیت سازمانی است و مدیران، کارکنان و واحدهای مختلف همگی در حفظ امنیت اطلاعات نقش دارند.

مهم‌ترین اقدام سازمان‌ها برای کاهش ریسک حملات چیست؟

ترکیب آموزش مستمر کارکنان، استفاده از احراز هویت چندعاملی، پایش مداوم شبکه، اجرای معماری دفاع چندلایه و حمایت مدیریت ارشد از برنامه‌های امنیتی، مؤثرترین راهکار برای کاهش ریسک حملات سایبری است.

سخن پایانی

شرکت « مدیران شبکه برنا » با پشتوانه ای از تجربه و دانش تخصصی و تمرکز بر ارائه راهکارهای نوین امنیت شبکه همواره تلاش کرده است تا نیازهای امنیتی سازمان ها و شرکت ها را در بالاترین سطح پوشش دهد . ما با بهره گیری از محصولات و فناوری های برتر جهانی در حوزه های چون , DLP XDR , EDR فایروال ؛ انتی ویروس DRM و NDR سعی کرده ایم فضای سایبری امن و پایدار برای مشتریان خود فراهم کنیم. ماموریت ما فراتر از ارائه محصول است . ما به دنبال ارائه راهکارهایی هستیم که نه تنها امنیت شبکه و داده های سازمان ها را تضمین می کنند بلکه امکان مدیریت هوشمند تهدیدات ؛ انطباق پذیری با الزامات قانونی و افزایش بهره وری فناوری اطلاعات را نیز به همراه دارند . در این مسیر ؛ تیم فنی متخصص ؛ پشتیبانی سریع و ارائه مشاوره دقیق ؛ از ارزش های محوری شرکت ما به شمار می آیند. ما باور داریم که امنیت سایبری صرفا یک محصول نیست ؛ بلکه یک تعهد دائمی و یک رویکرد حرفه ای برای حفظ سرمایه های اطلاعاتی سازمان هاست.شرکت مدیران شبکه برنا همواره همراهی قابل اعتماد برای سازمان ها و مدیران فناوری اطلاعات بوده و خواهد بود.

در پایان ؛ امیدواریم این رزومه بتواند نمایی شفاف از توانمندی ها ؛ حوزه های تخصصی و خدمات ما ارائه دهد و زمینه ساز همکاری های حرفه ای و مؤثر با سازمان شما باشد . آماده ایم تا در کنار شما ؛ گامی مطمئن در مسیر توسعه و امنیت برداریم.