



اخبار حوزه امنیت و شبکه (مرداد ۱۴۰۵)

در این شماره، تازه‌ترین تحولات امنیت سایبری از تهدیدات هوش مصنوعی و حملات نوین علیه زیرساخت‌های سازمانی تا آسیب‌پذیری Secure Boot، امنیت زیرساخت‌های حیاتی و اهمیت حاکمیت داده بررسی شده است. همچنین با ضرورت مدیریت Firmware، امنیت Patch Management، IT/OT، تاب‌آوری دیجیتال و راهکارهای دفاعی EDR، XDR و Threat Intelligence برای مقابله با تهدیدات پیشرفته آشنا می‌شوید.

ویژه مدیران و کارشناسان شبکه و امنیت

امنیت سایبری؛ ستون پنهان زیرساخت‌های انرژی آینده

وقتی صحبت از امنیت سایبری می‌شود، اغلب ذهن‌ها به سمت حفاظت از رایانه‌ها، سرورها یا شبکه‌های سازمانی می‌رود. اما واقعیت این است که با گسترش فناوری‌های هوشمند، امنیت دیگر تنها به داده‌ها محدود نمی‌شود؛ بلکه به‌طور مستقیم با زیرساخت‌های حیاتی مانند برق، انرژی، حمل‌ونقل و صنایع نیز گره خورده است.

در همین راستا، شرکت ESET و گروه EVC از آغاز همکاری راهبردی برای توسعه نسل جدیدی از سامانه‌های ذخیره‌سازی انرژی با محوریت امنیت سایبری خبر داده‌اند. هدف این همکاری، طراحی راهکارهایی است که از همان ابتدای توسعه، امنیت را به‌عنوان یکی از ارکان اصلی سیستم در نظر بگیرند؛ نه اینکه پس از نصب تجهیزات، لایه‌ای امنیتی به آن اضافه شود.

امروزه سامانه‌های ذخیره‌سازی انرژی (Battery Energy Storage Systems یا BESS) نقش مهمی در پایداری شبکه‌های برق و مدیریت انرژی ایفا می‌کنند. این تجهیزات به شبکه‌های ارتباطی متصل هستند، از راه دور مدیریت می‌شوند و با سایر سامانه‌های صنعتی تبادل اطلاعات دارند. همین اتصال گسترده، آن‌ها را به یکی از اهداف بالقوه حملات سایبری تبدیل کرده است.

در گذشته، هنگام انتخاب تجهیزات صنعتی، معیارهایی مانند ظرفیت، راندمان و هزینه اهمیت بیشتری داشت. اما امروز یک شاخص جدید نیز به این فهرست اضافه شده است.

این موضوع تنها به صنایع انرژی محدود نیست. بسیاری از سازمان‌ها از تجهیزات هوشمند، سیستم‌های کنترل صنعتی، تجهیزات شبکه، دوربین‌های نظارتی، سامانه‌های کنترل دسترسی و دستگاه‌های اینترنت اشیا (IoT) استفاده می‌کنند. هر یک از این تجهیزات در صورت نبود تنظیمات امنیتی مناسب یا به‌روزرسانی نشدن Firmware، می‌توانند مسیر ورود مهاجمان به شبکه سازمان باشند.

امنیت اطلاعات بدون امنیت شبکه معنا ندارد. زمانی که یک تجهیز صنعتی یا یک دستگاه متصل به شبکه مورد نفوذ قرار گیرد، مهاجم تنها به همان دستگاه دسترسی پیدا نمی‌کند؛ بلکه ممکن است از آن به‌عنوان سکوی پرتاب برای حرکت در شبکه، دسترسی به سرورها و سرقت اطلاعات استفاده کند. به همین دلیل، مرز میان امنیت فناوری اطلاعات (IT) و امنیت فناوری عملیاتی (OT) هر روز کمرنگ‌تر می‌شود.

یکی از مهم‌ترین پیام‌های این همکاری، تغییر نگرش نسبت به امنیت است. امنیت نباید قابلیت‌ای باشد که در پایان پروژه به سیستم اضافه شود؛ بلکه باید از مرحله طراحی، انتخاب تجهیزات و معماری شبکه در نظر گرفته شود. این همان مفهومی است که امروزه با عنوان Security by Design شناخته می‌شود.

برای مدیران شبکه و امنیت، این موضوع یک یادآوری مهم است. بسیاری از حملات موفق سایبری نه به دلیل پیچیدگی مهاجمان، بلکه به دلیل وجود تجهیزات قدیمی، Firmware های به روزرسانی نشده، تنظیمات پیش فرض یا نبود تقسیم بندی مناسب شبکه (Net- work Segmentation) رخ می دهند.

اگر سازمان شما از تجهیزات صنعتی، سیستم های هوشمند، تجهیزات IoT یا زیرساخت های حساس استفاده می کند، اکنون زمان مناسبی است تا وضعیت امنیتی آن ها را بازبینی کنید. برخی اقدامات کلیدی عبارت اند از:

- به روزرسانی منظم Firmware تجهیزات شبکه و صنعتی.
- جداسازی شبکه های عملیاتی از شبکه های اداری.
- محدود کردن دسترسی های راه دور و استفاده از احراز هویت چند مرحله ای.
- پایش مستمر ترافیک شبکه و رویدادهای امنیتی.
- ارزیابی دوره ای آسیب پذیری تجهیزات متصل به شبکه.
- انتخاب تجهیزاتی که امنیت در طراحی آن ها لحاظ شده است، نه اینکه بعداً به آن اضافه شود.
- آینده زیرساخت های دیجیتال، وابسته به امنیت آن ها است. همان طور که امروزه عملکرد، ظرفیت و پایداری از معیارهای اصلی انتخاب تجهیزات هستند، امنیت سایبری نیز باید به یکی از معیارهای اصلی تصمیم گیری مدیران تبدیل شود.

امنیت شبکه تنها وظیفه واحد فناوری اطلاعات نیست؛ بلکه پایه ای برای حفاظت از اطلاعات، تداوم کسب و کار و پایداری خدمات سازمان است. هرچه تجهیزات بیشتری به شبکه متصل می شوند، اهمیت داشتن یک معماری امن، به روزرسانی مستمر و نظارت مداوم نیز بیشتر خواهد شد.

در نهایت، سازمان هایی که امنیت را از مرحله طراحی زیرساخت در نظر می گیرند، نه تنها در برابر تهدیدات امروز مقاوم تر خواهند بود، بلکه آمادگی بیشتری برای مواجهه با چالش های امنیتی آینده نیز خواهند داشت.



چرا دولت‌ها به دنبال راهکارهای بومی و منطقه‌ای امنیت سایبری هستند؟

در بسیاری از سازمان‌ها، تمرکز اصلی بر مقابله با بدافزارها، حملات باج‌افزاری یا نفوذهای خارجی است؛ اما در کنار این تهدیدات، باید به موضوع حاکمیت داده (Data Governance) نیز توجه کرد. اینکه اطلاعات سازمان در کجا ذخیره می‌شود، چه افرادی به آن دسترسی دارند و تحت قوانین کدام کشور مدیریت می‌شود، امروزه بخشی از راهبرد امنیت اطلاعات محسوب می‌شود.

این موضوع ارتباط مستقیمی با امنیت شبکه نیز دارد. هرچه وابستگی سازمان به سرویس‌های ابری، سامانه‌های آنلاین و خدمات برون‌سپاری‌شده بیشتر شود، مدیریت ارتباطات شبکه، کنترل دسترسی، رمزنگاری، ثبت رویدادها و نظارت بر تبادل اطلاعات اهمیت بیشتری پیدا می‌کند. در واقع، امنیت شبکه اولین خط دفاعی برای حفاظت از داده‌هایی است که میان کاربران، سرورها و سرویس‌های مختلف جابه‌جا می‌شوند.

تحولات سال‌های اخیر نشان می‌دهد که امنیت سایبری دیگر تنها یک موضوع فنی نیست، بلکه به یکی از ارکان اصلی امنیت ملی، استقلال دیجیتال و تداوم خدمات حیاتی کشورها تبدیل شده است. به همین دلیل، دولت‌ها علاوه بر ارزیابی قابلیت‌های فنی محصولات امنیتی، به موضوعاتی مانند محل نگهداری داده‌ها، حریم خصوصی، شفافیت، قوانین حاکم بر اطلاعات و میزان وابستگی به فناوری‌های خارجی نیز توجه ویژه‌ای دارند.

در همین راستا، دولت مرکزی هلند به‌تازگی یک توافق‌نامه جامع با شرکت اروپایی ESET امضا کرده است تا سازمان‌های دولتی بتوانند با شرایطی یکپارچه و از پیش تعیین‌شده، از راهکارهای امنیت سایبری این شرکت استفاده کنند. هدف اصلی این توافق، افزایش تاب‌آوری دیجیتال و کاهش وابستگی به فناوری‌های خارج از اروپا عنوان شده است.

نکته قابل توجه این است که پیش از امضای این توافق، موضوعاتی مانند حریم خصوصی، محل ذخیره‌سازی داده‌ها، نحوه پردازش اطلاعات و سازوکارهای نظارتی به‌صورت دقیق بررسی و درباره آن‌ها توافق شده است. این موضوع نشان می‌دهد که امروزه انتخاب یک راهکار امنیتی تنها بر اساس قابلیت‌های فنی انجام نمی‌شود، بلکه نحوه مدیریت داده‌ها نیز به یکی از معیارهای اصلی تصمیم‌گیری تبدیل شده است.



از سوی دیگر، این توافق نشان می‌دهد که دولت‌ها به دنبال ایجاد تاب‌آوری دیجیتال (Digital Resilience) هستند؛ مفهومی که فراتر از جلوگیری از حملات سایبری است. تاب‌آوری دیجیتال یعنی سازمان بتواند حتی در شرایط وقوع حمله، اختلال یا بحران نیز خدمات حیاتی خود را با کمترین وقفه ادامه دهد.

برای دستیابی به این هدف، مدیران فناوری اطلاعات و امنیت باید علاوه بر استفاده از ابزارهای امنیتی، بر روی معماری شبکه، مدیریت دارایی‌ها، برنامه‌های بازیابی، نسخه‌های پشتیبان، کنترل دسترسی و پایش مداوم زیرساخت نیز سرمایه‌گذاری کنند.

چند اقدام کلیدی که می‌تواند به افزایش تاب‌آوری دیجیتال سازمان‌ها کمک کند عبارت‌اند از:

- بازیابی محل ذخیره‌سازی و پردازش اطلاعات حساس.
- ارزیابی امنیت تأمین‌کنندگان و سرویس‌های شخص ثالث.
- پیاده‌سازی اصل حداقل دسترسی (Least Privilege).
- به‌روزرسانی مستمر تجهیزات شبکه و سامانه‌های امنیتی.
- ثبت و پایش مداوم رویدادهای امنیتی.
- تدوین و آزمایش برنامه پاسخ به حوادث و بازیابی خدمات.

دنایای امروز نشان داده است که امنیت سایبری دیگر تنها به نصب یک محصول یا راهکار امنیتی خلاصه نمی‌شود. آنچه سازمان‌ها را در برابر تهدیدات آینده مقاوم می‌کند، ترکیبی از فناوری، معماری صحیح شبکه، مدیریت داده‌ها، سیاست‌های امنیتی و برنامه‌ریزی بلندمدت است.

توافق اخیر دولت هلند نمونه‌ای از این رویکرد است؛ رویکردی که در آن امنیت، حریم خصوصی، استقلال دیجیتال و تاب‌آوری به‌عنوان اجزای یک راهبرد واحد در نظر گرفته می‌شوند. برای مدیران شبکه و امنیت نیز این می‌تواند یادآوری مهمی باشد که حفاظت از اطلاعات سازمان، تنها با مقابله با تهدیدات امکان‌پذیر نیست؛ بلکه نیازمند طراحی زیرساختی است که از ابتدا بر پایه امنیت، شفافیت و اعتماد بنا شده باشد.



هوش مصنوعی؛ فرصتی برای سازمان‌ها یا ابزاری در اختیار مهاجمان؟

در سال‌های اخیر، هوش مصنوعی به یکی از مهم‌ترین ابزارهای افزایش بهره‌وری در سازمان‌ها تبدیل شده است. از تولید محتوا گرفته تا تحلیل داده‌ها، خودکارسازی فرایندها و حتی مدیریت زیرساخت‌های فناوری اطلاعات، استفاده از AI روزبه‌روز گسترده‌تر می‌شود. اما همان‌طور که این فناوری در اختیار کسب‌وکارها قرار گرفته، مهاجمان سایبری نیز از آن برای افزایش سرعت، دقت و مقیاس حملات خود استفاده می‌کنند.

بر اساس گزارش Threat Report H1 2026 منتشرشده توسط ESET، حملات سایبری در نیمه نخست سال ۲۰۲۶ بیش از هر زمان دیگری به سمت استفاده از هوش مصنوعی حرکت کرده‌اند. نکته نگران‌کننده این است که مهاجمان دیگر صرفاً به دنبال ساخت بدافزارهای جدید نیستند؛ بلکه با استفاده از AI، همان حملات قدیمی را بسیار هوشمندتر، سریع‌تر و باورپذیرتر اجرا می‌کنند.

یکی از مهم‌ترین یافته‌های این گزارش، شناسایی نزدیک به ۹۰۰ هزار AI Skill است. این Skill‌ها در واقع ماژول‌هایی هستند که به عامل‌های هوش مصنوعی آموزش می‌دهند چگونه یک وظیفه مشخص را انجام دهند. در میان این تعداد، ده‌ها هزار مورد مشکوک و هزاران مورد کاملاً مخرب شناسایی شده‌اند که می‌توانند برای اجرای حملات، ایجاد ماندگاری در سیستم یا سوءاستفاده از زیرساخت‌های سازمانی مورد استفاده قرار گیرند.

از سوی دیگر، ESET اولین نمونه شناخته‌شده از بدافزار اندرویدی مجهز به هوش مصنوعی مولد را نیز شناسایی کرده است. این موضوع نشان می‌دهد که AI دیگر تنها ابزاری برای تولید متن یا تصویر نیست، بلکه به تدریج در حال تبدیل شدن به بخشی از ساختار بدافزارها و حملات سایبری است.

یکی دیگر از روندهای مهم گزارش، گسترش حملات ClickFix است. در این روش، مهاجم با نمایش پیام‌های خطای جعلی یا صفحات راهنمای ساختگی، کاربر را متقاعد می‌کند که برای رفع مشکل، دسترسی را اجرا یا افزونه‌ای را نصب کند. امروزه این صفحات حتی با ظاهر سرویس‌های شناخته‌شده هوش مصنوعی طراحی می‌شوند و همین موضوع احتمال فریب کاربران را افزایش داده است.

همزمان، حملات مبتنی بر کدهای QR یا Quish-ing نیز رشد قابل توجهی داشته‌اند. در این روش، لینک‌های مخرب در قالب QR Code ارسال می‌شوند تا از فیلترهای امنیتی عبور کرده و کاربر را به استفاده از تلفن همراه برای ورود به صفحات جعلی هدایت کنند. بسیاری از کاربران هنوز تصور می‌کنند اسکن یک QR Code اقدامی بی‌خطر است، در حالی که این روش به یکی از ابزارهای محبوب مهاجمان تبدیل شده است.

در بخش دیگری از گزارش، ESET به روند نگران‌کننده حملات باج‌افزاری اشاره می‌کند. مهاجمان پیش از رمزگذاری اطلاعات، تلاش می‌کنند ابزارهای امنیتی مانند EDR را غیرفعال کنند. تاکنون بیش از ۱۰۰ ابزار مختلف برای از کار انداختن سامانه‌های EDR شناسایی شده است؛ موضوعی که نشان می‌دهد مهاجمان ابتدا به دنبال حذف دید و کنترل تیم امنیت هستند و سپس حمله اصلی را آغاز می‌کنند.

این گزارش یک پیام مهم برای مدیران شبکه و امنیت دارد: دیگر نمی‌توان تنها با نصب یک آنتی‌ویروس یا فایروال انتظار مقابله با تهدیدات نوین را داشت. مهاجمان از فناوری‌های جدید برای دور زدن لایه‌های امنیتی استفاده می‌کنند و سازمان‌ها نیز باید رویکرد دفاعی خود را متناسب با این تغییرات به‌روزرسانی کنند.

امنیت اطلاعات امروز بیش از هر زمان دیگری به امنیت شبکه وابسته است. اگر مهاجم بتواند از طریق یک ایمیل فیشینگ، یک QR Code، یک صفحه جعلی یا یک سرویس ابری وارد شبکه شود، حفاظت از داده‌های سازمان بسیار دشوار خواهد شد. به همین دلیل، امنیت شبکه دیگر تنها به کنترل ترافیک یا پیکربندی فایروال محدود نمی‌شود؛ بلکه شامل نظارت مستمر، تحلیل رفتار کاربران، مدیریت دسترسی، محافظت از هویت دیجیتال و پایش مداوم تهدیدات نیز هست.

مدیران فناوری اطلاعات باید به این نکته توجه داشته باشند که هوش مصنوعی، همان‌قدر که می‌تواند بهره‌وری سازمان را افزایش دهد، در صورت نبود کنترل‌های امنیتی مناسب می‌تواند سطح حمله (Attack Surface) را نیز گسترش دهد. استفاده از ابزارهای AI باید همراه با سیاست‌های امنیتی، کنترل دسترسی، آموزش کاربران و پایش مداوم باشد.

برای کاهش ریسک این تهدیدات، پیشنهاد می‌شود سازمان‌ها اقدامات زیر را در اولویت قرار دهند:

- آموزش مستمر کاربران درباره روش‌های جدید مهندسی اجتماعی و فیشینگ.
- استفاده از راهکارهای EDR و XDR برای شناسایی رفتارهای مشکوک.
- به‌روزرسانی مداوم تجهیزات شبکه، سیستم‌عامل‌ها و نرم‌افزارهای امنیتی.
- فعال‌سازی احراز هویت چندمرحله‌ای (MFA) و نظارت بر دسترسی‌های ابری.
- محدودسازی اجرای اسکریپت‌ها و ابزارهای ناشناس در ایستگاه‌های کاری.
- پایش مداوم لاگ‌ها و رویدادهای امنیتی برای شناسایی حملات در مراحل اولیه.
- واقعیت این است که آینده امنیت سایبری، رقابتی میان استفاده مشروع و سوءاستفاده از هوش مصنوعی خواهد بود. سازمان‌هایی که از امروز برای تقویت امنیت شبکه، آموزش کاربران و افزایش دید امنیتی خود برنامه‌ریزی کنند، آمادگی بیشتری برای مقابله با تهدیدات فردا خواهند داشت.

آیا Secure Boot به تنهایی برای محافظت از سازمان شما کافی است؟

در دنیای امنیت سایبری، بسیاری از مدیران فناوری اطلاعات تصور می‌کنند فعال بودن قابلیت Secure Boot به معنای ایمن بودن کامل سیستم‌ها در برابر حملات سطح پایین است. اما یافته‌های جدید محققان ESET نشان می‌دهد حتی مکانیزم‌هایی که سال‌ها به عنوان یکی از مهم‌ترین لایه‌های دفاعی شناخته می‌شدند، در صورت عدم به‌روزرسانی می‌توانند به نقطه ورود مهاجمان تبدیل شوند.

بر اساس تحقیقات منتشرشده توسط ESET، یازده نسخه قدیمی از UEFI Shim Bootloader که سال‌ها قبل توسط مایکروسافت امضا شده‌اند، همچنان در بسیاری از سیستم‌ها مورد اعتماد هستند. همین اعتماد قدیمی، فرصتی را در اختیار مهاجمان قرار می‌دهد تا بدون نیاز به شکستن مکانیزم Secure Boot، کدهای غیرمجاز خود را در همان ابتدای فرآیند راه‌اندازی سیستم اجرا کنند.

آنچه این موضوع را نگران‌کننده‌تر می‌کند، پیچیدگی پایین این حمله است. مهاجم نیازی به بهره‌برداری از یک آسیب‌پذیری جدید یا استفاده از تکنیک‌های پیشرفته ندارد؛ تنها کافی است نسخه‌ای از یک Boot-loader قدیمی اما همچنان معتبر را در اختیار داشته باشد تا بتواند زنجیره اعتماد سیستم را دور بزند.

در بسیاری از سازمان‌ها، تمرکز اصلی بر امنیت سیستم‌عامل، نرم‌افزارها و تجهیزات شبکه است؛ در حالی که امنیت واقعی از لایه‌های پایین‌تر آغاز می‌شود. BIOS، UEFI، Firmware و Bootload-er نیز بخشی از زنجیره امنیت اطلاعات هستند و هرگونه ضعف در این بخش‌ها می‌تواند تمام سرمایه‌گذاری‌های انجام‌شده در سایر لایه‌های امنیتی را بی‌اثر کند.

این موضوع تنها به رایانه‌های کاربران محدود نمی‌شود. بسیاری از تجهیزات شبکه مانند سرورها، فایروال‌ها، ذخیره‌سازها و حتی برخی تجهیزات ارتباطی نیز دارای Firmware و مکانیزم‌های راه‌اندازی مشابه هستند. اگر این تجهیزات به‌روزرسانی نشوند یا Firmware قدیمی آن‌ها همچنان مورد استفاده قرار گیرد، مهاجم می‌تواند پیش از فعال شدن کنترل‌های امنیتی، به زیرساخت سازمان دسترسی پیدا کند.

از سوی دیگر، این خبر بار دیگر اهمیت مدیریت دارایی‌های فناوری اطلاعات را یادآوری می‌کند. بسیاری از سازمان‌ها از نسخه سیستم‌عامل کاربران خود اطلاع دارند، اما اطلاعات دقیقی از نسخه BIOS، Firmware یا Bootloader تجهیزات در اختیار ندارند. همین نقاط کور می‌تواند در آینده به یکی از مهم‌ترین مسیرهای نفوذ تبدیل شود.

در امنیت اطلاعات اصطلاحی وجود دارد که می‌گوید: «امنیت به اندازه ضعیف‌ترین حلقه زنجیره قدرتمند است.» یافته اخیر ESET نیز دقیقاً همین موضوع را اثبات می‌کند. حتی اگر تمام سامانه‌های امنیتی سازمان به‌روز باشند، وجود یک مؤلفه قدیمی اما مورد اعتماد می‌تواند کل زنجیره اعتماد را زیر سؤال ببرد.

خبر اخیر ESET تنها درباره یک آسیب‌پذیری جدید نیست؛ بلکه هشدار است برای تمام سازمان‌هایی که تصور می‌کنند فعال بودن یک قابلیت امنیتی، تضمینی برای ایمن بودن زیرساخت آن‌هاست. در دنیای امروز، امنیت یک وضعیت ثابت نیست؛ بلکه فرآیندی مستمر از ارزیابی، به‌روزرسانی و مدیریت ریسک است. سازمان‌هایی که این فرآیند را به‌صورت مستمر اجرا می‌کنند، در برابر تهدیدات آینده نیز آمادگی بیشتری خواهند داشت.

برای مدیران شبکه، این خبر یک یادآوری مهم است که برنامه‌های Patch Management نباید تنها به سیستم‌عامل و نرم‌افزارها محدود شود. Firmware تجهیزات، به‌روزرسانی‌های Revocation، UEFI، امنیتی، Firmware سوئیچ‌ها، روترها، فایروال‌ها و سایر تجهیزات نیز باید به‌صورت مستمر بررسی و به‌روزرسانی شوند.

همچنین پیشنهاد می‌شود سازمان‌ها به‌صورت دوره‌ای موارد زیر را در برنامه امنیتی خود قرار دهند:

- بررسی نسخه Firmware و UEFI تمامی تجهیزات حیاتی
- اعمال آخرین به‌روزرسانی‌های امنیتی منتشرشده توسط تولیدکنندگان
- بازبینی تجهیزات قدیمی که سال‌ها بدون به‌روزرسانی در شبکه فعال هستند
- پایش مستمر زنجیره اعتماد (Chain of Trust) در زیرساخت‌های حیاتی

• استفاده از راهکارهای EDR و Threat Detection برای شناسایی رفتارهای غیرعادی در مراحل اولیه راه‌اندازی سیستم

در نهایت باید به این نکته توجه داشت که امنیت اطلاعات تنها با استقرار چند محصول امنیتی حاصل نمی‌شود. امنیت واقعی زمانی شکل می‌گیرد که تمام اجزای زیرساخت، از Firmware و Bootloader گرفته تا تجهیزات شبکه، سرورها، سیستم‌عامل‌ها و کاربران، به‌عنوان یک زنجیره واحد محافظت شوند.



هشدار ۱۱ آسیب‌پذیری بحرانی

شرکت‌های HashiCorp، Veeam و بنیاد Django مجموعه‌ای از ۱۱ آسیب‌پذیری امنیتی را در محصولات خود برطرف کرده‌اند. مهم‌ترین مورد، آسیب‌پذیری با امتیاز CVSS 10.0 در Terraform MCP Server است که در برخی پیکربندی‌ها می‌تواند باعث استفاده مجدد از توکن‌های Terraform بین کاربران مختلف (Cross-Tenant) شود. همچنین نقص‌های بحرانی در Veeam Service Provider Console و Django می‌توانند به افشای اطلاعات حساس یا اجرای کد منجر شوند.

مهم‌ترین آسیب‌پذیری‌های شناسایی‌شده

Terraform MCP Server: آسیب‌پذیری CVSS 10.0 که در برخی سناریوها امکان استفاده از توکن یک کاربر توسط کاربر دیگر را فراهم می‌کند.

Veeam Service Provider Console: آسیب‌پذیری با امتیاز 9.5 که می‌تواند بدون احراز هویت، اطلاعات اعتباری Agent‌ها را افشا کند.

Django (GeoDjango): نقص امنیتی که در شرایط خاص می‌تواند به نوشتن فایل‌های غیرمجاز و اجرای کد منجر شود.

اقدامات امنیتی پیشنهادی

سازمان‌ها باید Terraform MCP Server را به نسخه 1.1.0 یا بالاتر ارتقا دهند، Veeam Service Provider Console را به آخرین نسخه اصلاح‌شده به‌روزرسانی کرده و آخرین وصله‌های Django را نصب کنند. محدودسازی دسترسی به سرویس‌های مدیریتی، بازبینی محیط‌های چندکاربره و پایش لاگ‌ها نیز ضروری است.

اهمیت اعمال سریع وصله

با گسترش MCP Server‌ها و ابزارهای مبتنی بر هوش مصنوعی، امنیت نشست‌ها، توکن‌ها و جداسازی کاربران اهمیت بیشتری پیدا کرده است. اعمال سریع وصله‌ها و بازبینی تنظیمات این سرویس‌ها می‌تواند ریسک نفوذ به زیرساخت‌های سازمانی را کاهش دهد.



تهدید جدید Interrupt Injection

محققان امنیتی از حمله‌ای جدید با نام Interrupt Injection خبر داده‌اند که با سوءاستفاده از نحوه مدیریت وقفه‌ها (Interrupts) در پردازنده‌های مدرن و Hypervisor می‌تواند مرزهای امنیتی میان ماشین‌های مجازی و میزبان را تضعیف کرده و زمینه افشای اطلاعات حساس را فراهم کند.

این حمله در دسته Side-Channels و Transient Execution Attacks قرار می‌گیرد و نسل جدیدی از تهدیدات مبتنی بر اجرای حدسی (Speculative Execution) محسوب می‌شود.

تهدید زیرساخت‌های مجازی‌سازی

Interrupt Injection از مکانیزم مدیریت وقفه‌ها در محیط‌های مجازی‌سازی سوءاستفاده می‌کند و می‌تواند باعث نشت اطلاعات میان ماشین‌های مجازی یا از Hypervisor شود. این مسئله برای زیرساخت‌های Cloud، مراکز داده و محیط‌های Multi-Tenant اهمیت ویژه‌ای دارد. هرچند بهره‌برداری موفق به شرایط خاصی نیاز دارد، تأثیر احتمالی آن بر جداسازی امنیتی ماشین‌های مجازی قابل توجه است.

اقدامات امنیتی پیشنهادی

سازمان‌ها باید آخرین به‌روزرسانی‌های Kernel، Hypervisor و Microcode پردازنده را نصب کرده و BIOS/UEFI و Firmware سرورها را نیز به‌روزرسانی کنند. اعمال وصله‌های منتشرشده توسط تولیدکنندگان سیستم‌عامل و Hypervisor و بررسی تنظیمات مرتبط با Speculative Execution Mitigations نیز ضروری است.

در محیط‌های Cloud، اطلاعیه‌های امنیتی ارائه‌دهندگان خدمات باید به‌صورت مستمر پایش و وصله‌های منتشرشده سریعاً اعمال شوند.

تکامل حملات سخت‌افزاری

این پژوهش نشان می‌دهد حملات مبتنی بر Microarchitecture همچنان در حال تکامل هستند. حتی بدون امکان اجرای کد از راه دور، ضعف در جداسازی سخت‌افزاری می‌تواند امنیت زیرساخت‌های مجازی‌سازی و رایانش ابری را تحت تأثیر قرار دهد.

کشف حملات جدید HTTP

پژوهشگر امنیتی James Kettle از شرکت PortSwigger سیستمی مبتنی بر هوش مصنوعی با نام HTTP Terminator معرفی کرده است. این پژوهش نشان می‌دهد عامل‌های هوش مصنوعی می‌توانند فراتر از شناسایی آسیب‌پذیری‌های شناخته‌شده عمل کرده و تکنیک‌ها و مسیرهای جدید حمله به برنامه‌های وب را کشف کنند.

این سیستم با ترکیب مدل زبانی بزرگ (LLM)، مرورگر Headless و ابزارهای Fuzzing، رفتار برنامه‌های وب را تحلیل می‌کند، فرضیه‌های حمله می‌سازد و سپس آن‌ها را آزمایش می‌کند. این فرآیند به کشف تکنیک‌های مرتبط با حملات HTTP مانند HTTP Desync و مسیرهایی منجر شده که ممکن است در روش‌های سنتی تست امنیت نادیده گرفته شوند.

نقش هوش مصنوعی

هوش مصنوعی در حال تبدیل شدن به ابزاری برای تحقیقات امنیتی خودکار است. مدل‌های AI می‌توانند منطق برنامه‌ها، پاسخ‌های HTTP و رفتارهای غیرعادی را تحلیل کنند. همچنین حملات مبتنی بر منطق (Log-Based Attacks) ممکن است از قوانین ثابت WAF عبور کنند. این توانایی می‌تواند فاصله میان کشف یک ضعف امنیتی و سوءاستفاده از آن را کاهش دهد.

اقدامات امنیتی سازمان‌ها

سازمان‌ها باید تست نفوذ مبتنی بر سناریوهای واقعی را جدی‌تر بگیرند و علاوه بر آسیب‌پذیری‌های شناخته‌شده، منطق برنامه‌های وب را نیز بررسی کنند. به‌روزرسانی و تنظیم صحیح WAF همراه با تحلیل رفتاری، پیاده‌سازی Secure Development Lifecycle (SSDLC) و پایش مستمر API‌ها و ترافیک HTTP برای شناسایی الگوهای غیرعادی اهمیت بالایی دارد.

آینده امنیت وب

این تحقیق نشان می‌دهد آینده امنیت وب می‌تواند به رقابتی میان عامل‌های هوش مصنوعی دفاعی و تهاجمی تبدیل شود. AI سرعت کشف ضعف‌ها را افزایش می‌دهد، اما هم‌زمان نیاز سازمان‌ها به مدیریت ریسک، مانیتورینگ و توسعه امن نرم‌افزار را نیز بیشتر می‌کند.

آسیب‌پذیری بحرانی WordPress

پژوهشگران یک آسیب‌پذیری Pre-Authentication Re-flected XSS با شناسه CVE-2026-64638 و امتیاز CVSS 8.9 در صفحه ورود WordPress شناسایی کرده‌اند. این نقص در تمام نسخه‌های WordPress وجود داشته و مهاجم برای اجرای XSS اولیه به حساب کاربری یا سطح دسترسی خاصی نیاز ندارد.

در شرایط مشخص، این آسیب‌پذیری می‌تواند در قالب یک زنجیره حمله، از XSS اولیه به اجرای کد PHP روی سرور منجر شود.

زنجیره اجرای حمله

مهاجم ابتدا یک درخواست دستکاری‌شده به صفحه Login ارسال می‌کند. ورودی مخرب، عناصر DOM تحت کنترل مهاجم ایجاد کرده و JavaScript داخلی Word-Press را به سمت یک درخواست REST تحت کنترل مهاجم هدایت می‌کند.

در شرایط لازم، امکان سوءاستفاده از Application Pass-word فراهم می‌شود و مهاجم می‌تواند به REST API دسترسی احرازشده پیدا کرده و Plugin مخربی را Upload کند. در نهایت، این Plugin می‌تواند برای اجرای کد PHP مورد استفاده قرار گیرد.

شرایط اجرای کامل

مسیر کامل تا PHP Execution به شرایط دیگری مانند وجود Administrator واردشده، فعال بودن Application Passwords و برخی تنظیمات مربوط به Upload و اجرای PHP نیاز دارد. بنابراین ریسک XSS اولیه نباید با احتمال اجرای موفق PHP یکسان در نظر گرفته شود.

راهکار دفاعی WordPress

نسخه WordPress 7.0.3 در ۶ آگوست ۲۰۲۶ این نقص را برطرف کرده و وصله برای شاخه‌های قدیمی‌تر نیز Backport شده است. نسخه‌های قدیمی‌تر از 4.7 خارج از محدوده Backport فعلی هستند.



حملات CSS علیه Webmail

پژوهش جدید PortSwigger نشان می‌دهد مهاجمان می‌توانند با سوءاستفاده از قابلیت‌های مجاز HTML و CSS در سرویس‌های Webmail، رمز میان محتوای ایمیل و رابط کاربری مورد اعتماد را تضعیف کنند.

این تکنیک‌ها روی Outlook، Gmail، Fastmail، Proton Mail، Yahoo Mail و AOL Mail آزمایش شده‌اند و بسته به سرویس و شرایط حمله می‌توانند برای سرقت رمز عبور و Token، ربودن اقدامات کاربر، افشای اطلاعات و حتی سوءاستفاده از ابزارهای AI متصل به ایمیل به‌کار روند.

نمونه‌های مهم حمله

در Outlook و Firefox، صفحه ورود جعلی Microsoft برای دریافت رمز عبور ایجاد شد. در Yahoo Mail و AOL Mail نیز حمله Paste Race می‌تواند به افشای Token ورود منجر شود.

در Gmail، زنجیره‌ای شامل Prompt Injection و اتصال Gmail به Claude Cowork برای استخراج Slack Token نمایش داده شد. در Fastmail نیز تکنیک‌های CSS می‌توانند کلیک کاربران را به اقدامات ناخواسته هدایت کنند. حتی در برخی سناریوها امکان استخراج تدریجی اطلاعات عددی و Token‌ها از طریق CSS وجود دارد.

وضعیت واقعی تهدید

این پژوهش بر پایه Proof-of-Concept انجام شده و گزارشی از بهره‌برداری مخرب واقعی ارائه نمی‌کند. بااین‌حال، برخی تکنیک‌های معرفی‌شده هنگام انتشار همچنان قابل اجرا بوده‌اند.

راهکارهای دفاعی پیشنهادی

سازمان‌ها باید محتوای HTML ایمیل را در محیط‌های ایزوله و Sandbox اجرا کرده و CSS را با Allowlist دقیق محدود کنند. کنترل Custom Attribute، CSS Selectorهای خطرناک، Select Menu و درخواست‌های Image نیز اهمیت دارد.

همچنین اتصال مستقیم Agentهای هوش مصنوعی به Inboxهای حساس بدون کنترل‌های امنیتی کافی توصیه نمی‌شود. برای Tokenها و Sessionهای حساس نیز باید مانیتورینگ و امکان Revoke سریع فراهم شود.

این تحقیق نشان می‌دهد HTML و CSS در Web-mailهای مدرن می‌توانند بخشی از سطح حمله رابط کاربری و حتی زنجیره حملات AI باشند..

باچافزار Gunra و زیرساخت‌ها

مقامات امنیت سایبری کره جنوبی و آمریکا درباره فعالیت Gunra Ransomware علیه سازمان‌ها و زیرساخت‌های حیاتی هشدار داده‌اند. مهاجمان برای دسترسی اولیه به شبکه از آسیب‌پذیری‌های تجهیزات Schneider Electric Pow- و Fortinet FortiOS/FortiProxy erLogic P5 سوءاستفاده کرده‌اند.

دو آسیب‌پذیری مهم مورد استفاده شامل CVE-2025-24472 در FortiOS/FortiProxy و CVE-2024-5559 در Schneider Electric PowerLogic P5 هستند.

گسترش حمله در شبکه

پس از نفوذ، Gunra از ابزارهایی مانند Impacket برای حرکت جانبی و سرقت Credential استفاده می‌کند. در برخی حملات، مهاجمان لاگ‌ها و Command History را پاک کرده و اطلاعات سرقت‌شده را پیش از رمزگذاری به سرویس‌هایی مانند MEGA، OneDrive و SharePoint منتقل کرده‌اند.

دور زدن احراز هویت

یکی از خطرناک‌ترین بخش‌های حمله، دور زدن MFA است. مهاجمان در برخی موارد با دستکاری پردازش احراز هویت در محیط VDI توانسته‌اند OTP مشخصی را معتبر جلوه دهند. سرقت Session Cookie نیز امکان Session Hijacking و جعل هویت کاربران را فراهم کرده است.

Gunra از مدل Double Extortion استفاده می‌کند؛ یعنی ابتدا اطلاعات را سرقت و سپس فایل‌ها را رمزگذاری می‌کند. این گروه از سال ۲۰۲۵ دست‌کم ۵۱ قربانی را فهرست کرده است.

اقدامات دفاعی ضروری

سازمان‌ها باید تجهیزات Internet-Facing به‌ویژه Fortinet و Schneider Electric را فوراً Patch کنند. بررسی VPN و تجهیزات Perimeter، استفاده از MFA مقاوم، جداسازی بخش‌های IT و OT، پایش Impacket و SMB و بررسی Session‌های مشکوک ضروری است.

همچنین نگهداری Backup‌های Immutable، ثبت متمرکز و غیرقابل‌تغییر لاگ‌ها و بررسی Ac-count‌های بلااستفاده و Default Credential‌ها اهمیت بالایی دارد.

درس اصلی این حمله روشن است: آسیب‌پذیری Firewall یا VPN ممکن است تنها نقطه ورود باشد؛ خطر اصلی زمانی شکل می‌گیرد که مهاجم از آن برای دسترسی به Credential‌ها، VDI، Backup‌ها و سرورهای حیاتی استفاده کند.

Microsoft Defender و ShieldBreak

یک پژوهشگر امنیتی با نام Chaotic Eclipse یک Proof-of-Concept با نام ShieldBreak منتشر کرده که ادعا می‌کند وصله مایکروسافت برای آسیب‌پذیری CVE-2026-50656 (RoguePlanet) در Microsoft Defender قابل دور زدن است.

RoguePlanet یک آسیب‌پذیری Privilege Escalation در موتور Microsoft Malware Protection Engine یا mpengine.dll است که می‌تواند امکان اجرای Shell با سطح دسترسی SYSTEM را فراهم کند.

اهمیت ShieldBreak

PoC روی Windows 11 25H2 و Windows Server 2025 آزمایش شده و پژوهشگر نرخ موفقیت آن را در محیط آزمایش شده ۱۰۰ درصد اعلام کرده است. Windows 10 در PoC فعلی پشتیبانی نمی‌شود، اما احتمال آسیب‌پذیری آن مطرح شده است.

مایکروسافت در حال بررسی این ادعاست و در زمان انتشار گزارش، سوءاستفاده واقعی از ShieldBreak به صورت مستقل تأیید نشده بود.

دور زدن Patch

ShieldBreak یک آسیب‌پذیری کاملاً جدید نیست، بلکه به عنوان Patch Bypass برای CVE-2026-50656 مطرح شده است. بنابراین نصب Patch قبلی به تنهایی نباید تضمینی برای مصونیت کامل سیستم‌ها در نظر گرفته شود.

اقدامات دفاعی ضروری

سازمان‌ها باید Patch‌های امنیتی August 2026 مایکروسافت را در اولویت قرار داده و وضعیت Microsoft Defender و Malware Protection Engine را بررسی کنند.

پایش EDR برای شناسایی Process‌های غیرعادی با دسترسی SYSTEM، ایجاد Shell، Privilege Escalation و رفتارهای مشکوک mpengine.dll اهمیت بالایی دارد. همچنین Domain Controllerها، سرورهای مدیریتی و VDI باید در اولویت بررسی قرار گیرند.

درس اصلی روشن است: نصب یک Patch پایان فرآیند امنیت نیست. احتمال Patch Bypass نیز باید در مدل تهدید و فرآیند Patch Management سازمان در نظر گرفته شود.

سخن پایانی

در پایان؛ امیدواریم این رزومه بتواند نمایی شفاف از توانمندی‌ها؛ حوزه‌های تخصصی و خدمات ما ارائه دهد و زمینه ساز همکاری‌های حرفه‌ای و مؤثر با سازمان شما باشد. آماده‌ایم تا در کنار شما؛ گامی مطمئن در مسیر توسعه و امنیت برداریم.

شرکت «مدیران شبکه برنا» با پشتوانه‌ای از تجربه و دانش تخصصی و تمرکز بر ارائه راهکارهای نوین امنیت شبکه همواره تلاش کرده است تا نیازهای امنیتی سازمان‌ها و شرکت‌ها را در بالاترین سطح پوشش دهد. ما با بهره‌گیری از محصولات و فناوری‌های برتر جهانی در حوزه‌های چون، DLP، EDR، XDR فایروال؛ انتی ویروس DRM و NDR سعی کرده‌ایم 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 داده‌های سازمان‌ها را تضمین می‌کنند بلکه امکان مدیریت هوشمند تهدیدات؛ انطباق‌پذیری با الزامات قانونی و افزایش بهره‌وری فناوری اطلاعات را نیز به همراه دارند. در این مسیر؛ تیم فنی متخصص؛ پشتیبانی سریع و ارائه مشاوره دقیق؛ ارزش‌های محوری شرکت ما به شمار می‌آیند. ما باور داریم که امنیت سایبری صرفاً یک محصول نیست؛ بلکه یک تعهد دائمی و یک رویکرد حرفه‌ای برای حفظ سرمایه‌های اطلاعاتی سازمان‌هاست. شرکت مدیران شبکه برنا همواره همراهی قابل اعتماد برای سازمان‌ها و مدیران فناوری اطلاعات بوده و خواهد بود.