کشف یک آسیب‌پذیری که فرآیند احراز هویت را دور می‌زند

کارشناسان امنیتی از انتشار یک آسیب‌پذیری امنیتی خبر داده‌اند که پیامدهای بسیار خطرناکی به همراه دارد چون به مهاجم اجازه می‌دهد فرآیند احراز هویت را کاملاً دور بزند و بدون داشتن اعتبار یا رمز عبور، به سامانه دسترسی پیدا کند. به گزارش ایسنا، آسیب‌پذیری امنیتی مجموعه‌ای نقاط ضعف و شکافی در سیستم‌های اطلاعاتی و نرم‌افزارها است که می‌تواند منجر به نفوذ، دسترسی غیرمجاز یا سوءاستفاده از اطلاعات شود. این آسیب‌پذیری‌ها به راحتی توسط مهاجم‌ها قابل دسترسی است و می‌توانند از آن استفاده کنند؛ بنابراین شناسایی و رفع این مسائل امری مهم به حساب می‌آید تا افراد بتوانند از اطلاعات خود محافظت کنند و از وقوع حملات جلوگیری کنند.

در حالی که یک آسیب‌پذیری به ضعف‌های سخت‌افزار، نرم‌افزار یا رویه‌ها می‌پردازد، راه ورود هکرها برای دسترسی به سیستم‌ها، یک سوءاستفاده با کد مخربی است که مجرمان سایبری برای استفاده از آسیب‌پذیری‌ها و به خطر انداختن زیرساخت فناوری اطلاعات استفاده می‌کنند. براساس اعلام رسمی به‌تازگی یک آسیب‌پذیری و شدت ۱۰ یک نقص امنیتی بحرانی در فرآیند احراز هویت (Authentication) ایجاد می‌کند که پیامدهای بسیار خطرناکی به همراه دارد. درباره جزییات می‌توان گفت این آسیب‌پذیری به مهاجم اجازه می‌دهد فرآیند احراز هویت را کاملاً دور بزند و بدون داشتن اعتبار یا رمز عبور، به سامانه دسترسی پیدا کند.

این ضعف زمانی رخ می‌دهد که سرور برای تولید توکن‌های JWT از گواهی (کلید خصوصی) پیش‌فرض یا ثابت (hardcoded) استفاده می‌کند. طبق اعلام مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای (ماهر)، در چنین شرایطی، مهاجم می‌تواند آن گواهی را به دست آورد (از طریق مهندسی معکوس، مستندات یا نسخه‌های لو رفته) و خودش توکن جعلی امضا کند و وارد سیستم شود با نقش دلخواه، از جمله دسترسی مدیریتی.

کارشناسان امنیتی برای مقابله این آسیب‌پذیری توصیه کرده‌اند استفاده از گواهی‌های پیش‌فرض در تولید توکن‌های JWT به‌طور کامل حذف و برای هر نصب، یک کلید امضای یکتا و ایمن تولید شود. همچنین فرآیند نصب نرم‌افزار به‌گونه‌ای طراحی شود که کلیدها به‌صورت خودکار و امن ساخته شوند و قابل حدس یا استخراج نباشند. بهتر است کنترل دسترسی مناسب روی فایل‌های کلید خصوصی اعمال شود.

گفتنی است چندی یک آسیب‌پذیری با شماره CVE-۲۰۲۵-۴۸۹۵۲ و شدت ۹ به عنوان یک نقص امنیتی بحرانی در سامانه NetAlertX (نرم‌افزار مانیتورینگ شبکه و سیستم هشداردهی) شناسایی شد که به مهاجم اجازه می‌داد فرآیند احراز هویت (Login) را بدون داشتن رمز عبور صحیح دور بزند. این نقص زمانی رخ می‌داد که کد برنامه در مقایسه مقدار هش رمز عبور وارد شده توسط کاربر و مقدار ذخیره‌شده در پایگاه داده، به‌جای استفاده از روش‌های ایمن، از عملگر مقایسه ساده == در زبان PHP استفاده شود.

صدور ۷۶ مجوز برای متقاضیان فعالیت در زیرساخت‌های حیاتی کشور

مرکز مدیریت راهبردی افتا، خرداد ماه گذشته، با درخواست صدور یا تمدید ۷۶ مجوز شرکت‌های متقاضی فعالیت در زیرساخت‌های حیاتی کشور موافقت کرد. به گزارش ایسنا، موافقت با درخواست صدور یا تمدید مجوز شرکت‌های متقاضی فعالیت در حوزه سایبری زیرساخت‌های حیاتی کشور در خرداد ماه گذشته به نسبت خرداد ماه سال ۱۴۰۳، بیش از دو برابر افزایش داشته است.

این پروانه‌های فعالیت برای شرکت‌های متقاضی در حوزه‌های چهارگانه خدمات افتایی (عملیاتی، مدیریتی، فنی و آموزشی) و محصولات فتایی، صادر شده است. مرکز مدیریت راهبردی افتا همچنین با ۵ درخواست اخذ مجوز به دلیل عدم احراز صلاحیت فنی موافقت نکرده است. این مرکز، در بهار گذشته در مجموع با درخواست صدور یا تمدید ۳۲۸ مجوز شرکت‌های متقاضی فعالیت در زیرساخت‌های حیاتی کشور، موافقت کرده است.

شبکه ملی اطلاعات فیلترینگ نیست؛ هیچ کشوری داده‌اش را به دیگران نمی‌دهد

معاون توسعه شبکه ملی اطلاعات گفت: شبکه ملی اطلاعات، فیلترینگ نیست بلکه منظور حفاظت از دارایی‌های ملی فناوری پایه است. به گزارش مهر، رسول لطفی معاون توسعه شبکه ملی اطلاعات در یکی از شبکه‌های اجتماعی در خصوص شبکه ملی اطلاعات و فیلترینگ گفت: شبکه ملی اطلاعات، فیلترینگ نیست، این تعریف که به غلط در ذهن‌ها جانمایی شده باید اصلاح شود. وی افزود: شبکه ملی اطلاعات، شبکه شبکه‌ها و زیرساخت اصلی اقتصاد دیجیتال و حفاظت از دارایی‌های ملی فناوری پایه است. معاون توسعه شبکه ملی اطلاعات گفت: هیچ کشوری در جهان داده‌های ملی‌اش را به دیگران هدیه نمی‌دهد.

فیلترینگ و قطعی، دسترسی توسعه‌دهندگان به ابزارهای جهانی را مختل کرده است

اختلال سراسری اینترنت؛ خیز بلند به عقب

هر ساعت قطعی کامل اینترنت، بیش از ۱.۵ میلیون دلار خسارت مستقیم به اقتصاد کشور وارد می‌کند، آماری که نت‌بلاکس و اتحادیه کسب‌وکارهای اینترنتی ایران نیز آن را تأیید کرده‌اند. این ضرر فقط هزینه لحظه‌ای نیست؛ اعتماد کاربران کاهش می‌یابد، کمپین‌های بازاریابی شکست می‌خورند و کسب‌وکارها - از فروشگاه‌های آنلاین تا اکوسیستم‌های فناوری - با ریزش نیروی متخصص و فرسایش زیرساخت‌ها مواجه می‌شوند.

در روزهایی که اقتصاد دیجیتال، محور توسعه کشورهای پیشرو جهان است، ایران بار دیگر با یک بحران پرهزینه در بستر اینترنت روبرو شده است. اختلال اینترنتی فراتر از یک قطعی فنی، به یک تهدید گسترده برای اقتصاد و توسعه ملی تبدیل شده است. قطع اینترنت، دریافت «به‌روزرسانی امنیتی» سیستم‌ها را مختل می‌کند و در نتیجه، سرورهای داخلی با حفره‌های امنیتی قدیمی رها می‌مانند؛ وضعیت خطرناکی که امنیت ملی را به خطر می‌اندازد. این «خودتحریمی امنیتی» زمینه‌ای برای حملات باج‌افزاری، سرقت داده و خرابکاری فراهم می‌کند، بدون اینکه در کوتاه‌مدت قابل اندازه‌گیری باشد. تحریم‌های بین‌المللی دسترسی توسعه‌دهندگان ایرانی به ابزارهای کلیدی را مسدود کرده‌اند؛ تنها راه فرار استفاده از VPN بود. حالا با انسداد پروتکل‌های ارتباطی، حتی این راه فرعی بسته شده است. نتیجه: جامعه فناوری ایران عملاً از اکوسیستم جهانی جدا مانده و فرار مغزها و سرمایه‌ها شدت گرفته است.

هزینه سنگین هر ساعت قطعی اینترنت

هر ساعت اختلال کامل اینترنت حدود ۱.۵ میلیون دلار خسارت مستقیم برای ایران در پی دارد. این رقم بر مبنای شاخص‌های بین‌المللی از جمله گزارش‌های نت‌بلاکس و اتحادیه کسب‌وکارهای اینترنتی ایران محاسبه شده و تنها زیان‌های آنی نظیر افت فروش، توقف تبلیغات آنلاین و کاهش ترافیک کاربران را در بر می‌گیرد. اما هزینه واقعی به مراتب بیشتر است. کمپین‌های بازاریابی ناتمام می‌مانند، کاربران بی‌اعتماد می‌شوند، کسب‌وکارها از اجرای پروژه‌های نوآورانه بازمی‌مانند و در نهایت، رقابت‌پذیری برندهای ایرانی در بازار داخلی و بین‌المللی کاهش می‌یابد. این خسارات قابل سنجش نیستند، اما آثار آن در بلندمدت ساختار اکوسیستم دیجیتال کشور را تخریب می‌کند.

سکوت در برابر تهدیدات سایبری

قطع ارتباط ایران با اینترنت بین‌المللی، نه‌تنها راه را بر استفاده از سرویس‌های ضروری خارجی می‌بندد، بلکه به شکاف امنیتی دامن می‌زند. بسیاری از نرم‌افزارها و سیستم‌های زیرساختی، برای مقابله با حملات سایبری، نیاز به به‌روزرسانی‌های پیوسته دارند. وقتی اتصال جهانی قطع می‌شود، این روند نیز متوقف شده و سرورهای داخلی در برابر آسیب‌پذیری‌های شناخته‌شده‌ای که به‌راحتی قابل اصلاح بودند، بی‌دفاع باقی می‌مانند. در گزارش‌های اخیر مرکز ملی فضای مجازی و مراکز بین‌المللی همچون CISA و FBI نیز تأکید شده که نبود آپدیت‌های امنیتی باعث گسترش باج‌افزارها، حملات فیشینگ، و سرقت اطلاعات کاربران می‌شود. این تهدیدات نه فقط کاربران عادی، بلکه بانک‌ها، ادارات دولتی و حتی زیرساخت‌های حیاتی مانند نیروگاه‌ها و صنایع نفت و گاز را در معرض خطر قرار می‌دهد.

خاموشی هوش مصنوعی و سکون نوآوری

بخش مهمی از خدمات ارایه‌شده در پلتفرم‌های داخلی، بر پایه پردازش‌های هوش مصنوعی عمل می‌کند؛ از جمله تشخیص تصویر، رتبه‌بندی آگهی‌ها و فیلتر محتوای نامناسب. این فرآیندها، به اتصال مداوم با سرورهای قدرتمند ابری نیاز دارند که اغلب در خارج از کشور مستقر هستند. با قطع اینترنت، این سامانه‌ها عملاً از کار می‌افتند؛ در ظاهر همه‌چیز فعال است، اما مغز تحلیلگر که در پس‌زمینه فعالیت دارد، خاموش می‌شود. نتیجه این خاموشی، افزایش خطای تشخیص، افت کیفیت خدمات و نارضایتی کاربران است. با گذشت زمان، این ناکارآمدی به وجهه برندهای داخلی لطمه زده و زمینه‌ساز مهاجرت کاربران به سرویس‌های خارجی از طریق ابزارهای غیررسمی می‌شود.

فیلترینگ در برابر جریان دانش

یکی دیگر از ابعاد مهم بحران اینترنت در ایران، تأثیر آن بر گردش آزاد دانش و آموزش است. میلیون‌ها جوان ایرانی برای یادگیری زبان، توسعه مهارت‌های فنی، شرکت در دوره‌های آنلاین یا مشارکت در پروژه‌های علمی، به اینترنت نیاز دارند. پلتفرم‌هایی مانند Coursera، Udemy، Github و StackOverflow که برای توسعه‌دهندگان و دانشجویان حیاتی‌اند، در شرایط فیلترینگ و قطع ارتباط جهانی عملاً بلااستفاده می‌شوند. در نتیجه، ایران نه‌تنها از آموزش‌های روز دنیا عقب می‌ماند، بلکه زمینه‌های نوآوری و تولید دانش نیز در کشور به‌شدت تضعیف می‌شود. بسیاری از جوانانی که می‌توانستند موتور محرک اقتصاد دیجیتال باشند، ناامید شده و به فکر مهاجرت می‌افتند.

خودتحریمی مضاعف در بستر فناوری

اگر تحریم‌های بین‌المللی موجب محدودیت در دسترسی به ابزارهای کلیدی توسعه نرم‌افزار شده‌اند، تصمیم داخلی برای فیلترکردن یا قطع ارتباط با اینترنت جهانی، عملاً یک «خودتحریمی مضاعف» است. توسعه‌دهندگان ایرانی با استفاده از VPN و روش‌های جایگزین سعی در حفظ ارتباط خود با جهان داشتند، اما با محدودسازی پروتکل‌های رمزنگاری‌شده و فیلترینگ سنگین، حتی این راه‌های جایگزین نیز مسدود شده‌اند. در این شرایط، حتی کار ساده‌ای مثل نصب یک کتابخانه کد یا به‌روزرسانی سیستم‌عامل به یک چالش تبدیل می‌شود. روند توسعه کند شده، پروژه‌ها نیمه‌کاره می‌مانند و کارفرمایان از همکاری با برنامه‌نویسان داخلی دلسرد می‌شوند. بدین ترتیب، راه برای برون‌سپاری پروژه‌ها به شرکت‌های خارجی یا مهاجرت نخبگان بیش از پیش باز می‌شود.

تجربه جهانی؛ خسارت‌بار و بی‌نتیجه

ایران تنها کشوری نیست که از اینترنت به عنوان ابزاری برای اعمال کنترل سیاسی یا امنیتی استفاده کرده است. تجربه هند، پاکستان، روسیه، چین و برخی کشورهای آفریقایی نیز نشان می‌دهد که قطع ارتباط جهانی نه‌تنها در تحقق اهداف امنیتی موفق نبوده، بلکه موجب افزایش نارضایتی اجتماعی، افت اقتصادی و فرار سرمایه‌ها شده است. براساس گزارش سال ۲۰۲۳ NetBlocks، مجموع خسارت جهانی ناشی از قطعی اینترنت در یک سال گذشته بالغ بر ۹ میلیارد دلار بوده است. ایران در این میان یکی از پنج کشور با بالاترین سطح اختلال بوده است، و بیشترین افت شاخص آزادی اینترنت را نیز تجربه کرده است.

آینده‌ای مبهم؛ ضرورت تصمیم‌گیری شفاف

با افزایش اختلالات اینترنتی، نه‌تنها وضعیت اقتصادی شکننده‌تر شده، بلکه بی‌اعتمادی اجتماعی نیز تعمیق یافته است. کاربران ایرانی در روزهای اخیر در شبکه‌های اجتماعی نسبت به عدم شفافیت دولت در خصوص دلایل اختلالات اعتراض کرده‌اند. در حالی که مسوولان هنوز توضیح رسمی و روشنی ارایه نداده‌اند، تحلیلگران معتقدند که رویکرد امنیتی به اینترنت باید بازنگری شود. اینترنت دیگر نه یک ابزار تفریحی، بلکه زیرساختی حیاتی در سطح خدمات شهری، اقتصاد، آموزش و امنیت است. تداوم روند محدودسازی، می‌تواند کشور را به انزوای کامل دیجیتال بکشاند؛ مسیری که پیامدهای آن تا سال‌ها آینده بر توسعه ایران سایه می‌اندازد. ایران در نقطه‌ای حساس از مسیر توسعه دیجیتال قرار دارد. تصمیم امروز درباره نحوه مدیریت اینترنت، آینده اقتصاد، امنیت، آموزش و حتی اعتماد عمومی را رقم خواهد زد. اگرچه دغدغه‌های امنیتی قابل درک‌اند، اما برخورد حذفی با اینترنت در نهایت به تضعیف امنیت پایدار منجر می‌شود. بازنگری در سیاست‌های فیلترینگ، سرمایه‌گذاری بر امنیت داده، توسعه شبکه ملی اطلاعات در تعامل با اینترنت جهانی، و حرکت به سوی حکمرانی دیجیتال شفاف، می‌تواند مسیر تازه‌ای را پیش‌روی کشور قرار دهد. در غیر این صورت، هر ساعت اختلال اینترنت، فقط یک عقب‌گرد فنی نیست؛ بلکه گامی دیگر به سوی انزوایی بلندمدت و پرهزینه است.

امنیت در دنیای مجازی؛ از تهدید تا پیشگیری

در دنیای دیجیتال امروز، حفاظت از هویت افراد در فضای اینترنت اهمیت زیادی دارد زیرا با افزایش تهدیدات سایبری از جمله کلاهبرداری‌ها و سوءاستفاده‌های افراد ناشناس، نیاز به مراقبت از اطلاعات شخصی بیشتر از همیشه حس می‌شود. اگر در این زمینه بی‌احتیاطی شود ممکن است اطلاعات کاربران به دست سودجویان بیفتد؛ بنابراین آگاهی از روش‌های محافظت از هویت و استفاده از ابزارهای امنیتی ضروری است. به گزارش ایسنا، اقدامات مرتبط با محافظت از هویت و استفاده از ابزارهای امنیتی می‌تواند شامل استفاده از رمزهای عبور قوی، فعال‌سازی احراز هویت دومرحله‌ای و اجتناب از اشتراک‌گذاری اطلاعات حساس در شبکه‌های اجتماعی باشند. در نهایت، حفظ حریم خصوصی آنلاین نه‌تنها به امنیت فردی کمک می‌کند، بلکه به ایجاد یک فضای اینترنتی امن‌تر برای همه نیز می‌انجامد. اولین راهکار برای حفظ امنیت آنلاین این است که از حساب‌های کاربری قدیمی که نام آنها تغییر یافته است، استفاده نکنید. به عنوان مثال، اگر قبلاً در پلتفرم‌هایی مانند واتس آپ با نام واقعی خود حساب کاربری ایجاد کرده‌اید و سپس نام آن را تغییر داده‌اید، بهتر است از این حساب برای فعالیت‌های خود استفاده نکنید. دلیل این امر این است که ممکن است اطلاعات قدیمی شما هنوز قابل بازیابی باشد و این موضوع می‌تواند منجر به افشای هویت شما شود. برای حفظ امنیت آنلاین، هرگز حساب کاربری ناشناس خود را به حساب‌های دیگر متصل نکنید. به‌طور مثال اگر در شبکه واتس‌اپ با یک حساب ناشناس فعالیت می‌کنید، آن را به حساب‌هایی مانند اینستاگرام که هویت واقعی شما در آن مشخص است، وصل نکنید. اتصال حساب‌های مختلف به همدیگر می‌تواند به افراد ناشناس و سودجو کمک کند تا از طریق لینک‌ها یا تصاویر مرتبط، رد شما را پیدا کرده و به اطلاعات واقعی شما دست یابند. اتصال حساب‌های ناشناس به حساب‌های شناخته‌شده، خطر افشای هویت و اطلاعات شخصی را افزایش می‌دهد. انتخاب نام کاربری از قرار دادن اطلاعات واقعی مانند نام و فامیل خود پرهیز کنید. این اطلاعات می‌توانند به‌راحتی برای شناسایی شما استفاده شوند و امنیت شما را به خطر بیندازند. به‌جای آن، از یک نام کاربری خلاقانه و غیرقابل حدس استفاده کنید که هویت شما را مخفی نگه دارد. انتخاب نام‌های تصادفی یا ترکیبی از کلمات می‌تواند به افزایش حریم خصوصی شما کمک کند. با این کار، احتمال شناسایی شما در فضای آنلاین به حداقل می‌رسد و امنیت حساب کاربری‌تان بیشتر می‌شود. علی‌اصغر زارعی - مدرس دانشگاه و کارشناس ارشد مدیریت سیستم‌های اطلاعاتی و مهندسی فناوری اطلاعات - در گفت‌وگو با ایسنا، با بیان اینکه خاموش کردن موقعیت مکانی یا لوکیشن در دستگاه‌ها و حساب‌های کاربری یکی از مراحل مهم حفظ حریم خصوصی است. اظهار کرد: با فعال بودن این گزینه، اطلاعات مربوط به محل زندگی یا فعالیت‌های روزانه شما می‌تواند به‌راحتی در دسترس دیگران قرار گیرد. بنابراین، برای جلوگیری از شناسایی مکان شما، لازم است این گزینه را خاموش کنید. وی افزود: برای اینکار ابتدا به تنظیمات دستگاه خود بروید و بخش مربوط به حریم خصوصی یا موقعیت مکانی را پیدا کنید. سپس اطمینان حاصل کنید که گزینه مربوط به اشتراک‌گذاری موقعیت مکانی خاموش باشد. همچنین، در تنظیمات حساب‌های کاربری مختلف مانند شبکه‌های اجتماعی یا اپلیکیشن‌های پیام‌رسان، این گزینه را بررسی کنید. زارعی گفت: حتی اگر به‌طور پیش‌فرض خاموش باشد، بهتر است دوباره آن را چک کنید تا مطمئن شوید به‌طور ناخواسته روشن نشده است. با خاموش کردن این گزینه، شما کنترل بیشتری بر روی اطلاعات شخصی خود خواهید داشت و می‌توانید از خطرات احتمالی ناشی از افشای موقعیت مکانی جلوگیری کنید. عضو کمیسیون کسب‌وکارهای مجازی و اقتصاد دیجیتال نصر کشور با تأکید بر اینکه برای ایجاد حساب‌های کاربری ناشناس، استفاده از یک ایمیل و شماره تلفن جدید ضروری است؛ ادامه داد: این کار به شما کمک می‌کند تا هویت اصلی‌تان را از دید دیگران پنهان نگه دارید. هرگز نباید شماره یا ایمیل اصلی خود را به این حساب‌ها متصل کنید، زیرا این کار می‌تواند منجر به افشای اطلاعات شخصی‌تان شود. همچنین، استفاده از سرویس‌های ایمیل موقت یا شماره‌گیری موقت می‌تواند به افزایش امنیت شما کمک کند. همچنین در فضای مجازی، حفظ حریم خصوصی و امنیت اطلاعات شخصی از اهمیت بالایی برخوردار است. هرگز نباید اطلاعات حساسی مانند آدرس، مکان یا جزییات مالی خود را به اشتراک بگذارید، چون این اطلاعات می‌توانند به‌راحتی توسط افراد نادرست مورد سوءاستفاده قرار گیرند. حتی ارسال عکس‌ها یا ویدیوهایی که ممکن است نشانه‌هایی از هویت یا موقعیت شما داشته باشند، خطرناک است. به گفته‌ی دوستان مجازی نیز همیشه قابل اعتماد نیستند و ممکن است اطلاعات شما را به اشتباه یا به عمد منتشر کنند بنابراین باید با احتیاط رفتار کنید و از به اشتراک‌گذاری هرگونه اطلاعات شخصی خودداری کرد. بررسی‌ها حاکی از آن است در فضای مجازی، لینک‌ها ممکن است منبع خطر باشند، حتی اگر از سوی دوستان مجازی ارسال شده باشند. برخی از این لینک‌ها می‌توانند حاوی بدافزار یا نرم‌افزارهای مخرب باشند که به هدف سرقت اطلاعات شخصی شما طراحی شده‌اند. بنابراین، همیشه باید نسبت به لینک‌هایی که دریافت می‌کنید، محتاط باشید و از باز کردن آنها خودداری کنید، به‌ویژه اگر ناشناس یا مشکوک به نظر برسند. همچنین، لینک‌هایی که وعده خدمات رایگان مانند فیلترشکن یا اپلیکیشن‌های عجیب‌وغریب را می‌دهند، ممکن است به‌منظور نفوذ به دستگاه شما طراحی شده باشند. در نهایت، بهتر است تنها از منابع معتبر و شناخته‌شده لینک‌ها را باز کنید و همیشه امنیت اطلاعات خود را در اولویت قرار دهید. علاوه بر موارد گفته‌شده اعتماد نکردن به ربات‌ها و ابزارهای ناشناس یکی از نکات مهم در حفظ امنیت اطلاعات شخصی است. بسیاری از این ابزارها ادعا می‌کنند که می‌توانند امنیت یا ناشناس بودن کاربر را تضمین کنند، اما درواقع ممکن است اطلاعات شما را جمع‌آوری کرده و با خطر مواجه شوند. این ربات‌ها ممکن است به‌سادگی ترفندهایی برای فریب کاربران باشند و اطلاعات حساس را از آنها سرقت کنند. به همین دلیل، بهتر است از ارایه هرگونه اطلاعات شخصی به این ابزارها خودداری کنید. قبل از استفاده از هر ربات یا ابزاری، تحقیق کنید و از اعتبار آن اطمینان حاصل کنید. محدود کردن دسترسی اپلیکیشن‌ها در دستگاه‌های هوشمند یکی از راه‌های مهم برای حفظ حریم خصوصی و امنیت اطلاعات شخصی است. بسیاری از اپلیکیشن‌ها به‌طور پیش‌فرض به داده‌ها و امکاناتی مانند موقعیت مکانی، دوربین و میکروفون دسترسی دارند که ممکن است برای عملکرد آنها ضروری نباشد. بررسی کنید که هر اپلیکیشن به چه نوع اطلاعاتی دسترسی دارد و آیا این دسترسی‌ها منطقی و ضروری هستند یا خیر. درصورتی که اپلیکیشن‌ها به اطلاعات حساسی نیاز ندارند، بهتر است این دسترسی‌ها را غیرفعال کنید. به اعتقاد کارشناسان یکی از روش‌های موثر برای محافظت از حریم خصوصی و جلوگیری از افشای هویت، تنظیم حساب‌های کاربری به حالت خصوصی یا Private است. با انجام این کار، فقط افرادی که شما آنها را تأیید کرده‌اید می‌توانند به اطلاعات و محتوای شما دسترسی داشته باشند. این تنظیمات معمولاً در شبکه‌های اجتماعی و پلتفرم‌های آنلاین قابل دسترسی هستند. با محدود کردن دسترسی به پروفایل خود، می‌توانید کنترل بیشتری بر روی آنچه دیگران مشاهده می‌کنند داشته باشید. همچنین، این اقدام می‌تواند از سوءاستفاده‌های احتمالی و مزاحمت‌های آنلاین جلوگیری کند. پاک‌سازی ردپاهای دیجیتال به معنای حذف اطلاعات و محتواهایی است که ممکن است هویت شما را در فضای مجازی شناسایی کند. این اطلاعات شامل پست‌ها، کامنت‌ها، عکس‌ها و هر نوع محتوای دیگری است که در شبکه‌های اجتماعی یا وب‌سایت‌ها به اشتراک گذاشته‌اید. با گذشت زمان، این داده‌ها می‌توانند به‌راحتی توسط دیگران پیدا شوند و حریم خصوصی شما را تهدید کنند. برای این کار، ابتدا باید حساب‌های کاربری غیرضروری خود را شناسایی کرده و آنها را حذف کنید. سپس به بررسی محتواهای موجود در حساب‌های فعال بپردازید و مواردی که ممکن است باعث شناسایی شما شوند، مانند عکس‌ها یا نظرات، را پاک کنید. همچنین می‌توانید تنظیمات حریم خصوصی خود را تغییر دهید تا دسترسی دیگران به اطلاعات شما محدود شود. مراقبت از فریب‌های اجتماعی در فضای مجازی بسیار مهم است. افراد و گروه‌های مختلف ممکن است با استفاده از سوالات شخصی یا داستان‌های عاطفی سعی کنند شما را فریب دهند تا اطلاعات حساس خود را به اشتراک بگذارید. هیچ‌کس حق ندارد حریم خصوصی شما را نقض کند یا شما را تحت فشار قرار دهد. کاربران سایبری ممکن است به دنبال جمع‌آوری اطلاعات شما باشند تا هویت شما را شناسایی کنند. حفاظت از حریم خصوصی در فضای مجازی نه‌تنها به امنیت فردی شما کمک می‌کند، بلکه از سوءاستفاده‌های احتمالی دیگران نیز جلوگیری می‌کند. با رعایت نکات امنیتی، می‌توانید اطلاعات شخصی خود را از دسترس افراد سودجو دور نگه دارید و مانع از سرقت هویت یا کلاهبرداری شوید. درنتیجه، آگاهی و احتیاط در این زمینه به حفظ امنیت جامعه نیز کمک می‌کند.

حمله جاسوس افزار پیشرفته به سازمان‌های روسیه

جاسوس‌افزار ناشناخته باتاویا (Batavia)، از ژوئیه ۲۰۲۴، با استفاده از یک عملیات فیشینگ پیچیده، سازمان‌های صنعتی روسیه را هدف قرار داده است. به گزارش ایسنا، محققان شرکت کسپرسکی از اوایل مارس ۲۰۲۵، افزایش چشمگیر موارد شناسایی شده را مشاهده کرده‌اند و بیش از ۱۰۰ کاربر در ده‌ها سازمان، قربانی ایمیل‌های طعمه‌گذاری‌شده در قالب توافقنامه‌های قراردادی شده‌اند. این ایمیل‌ها که اغلب حاوی نام فایل‌هایی مانند «قرارداد» و «پیوست» هستند، کارمندان را به دانلود اسکریپت‌های مخربی که یک فرآیند آلودگی چند مرحله‌ای را آغاز می‌کنند، ترغیب می‌کنند. هدف نهایی باتاویا، استخراج اسناد داخلی حساس و داده‌های سیستم است که تهدیدی قابل توجه برای امنیت سازمان محسوب می‌شود. بر اساس گزارش بلیپینگ کامپیوتر، محققان معتقدند که حمله این بدافزار، حداقل از ژوئیه سال گذشته آغاز شده و همچنان ادامه دارد. بر اساس داده‌های تله‌متری، ایمیل‌های فیشینگ حاوی باتاویا، به کارمندان ده‌ها سازمان روسی که هدف قرار گرفته‌اند، رسیده است. از ژانویه ۲۰۲۵، شدت این حمله افزایش یافته و تا پایان فوریه، به اوج خود رسیده است. سازمان‌ها باید برای مقابله با چنین تهدیدهایی، یک استراتژی دفاعی چندلایه اتخاذ کنند. ممیزی‌های امنیتی منظم و به‌روزرسانی محافظت از دستگاه‌های اندپوینت نیز برای شناسایی و خنثی‌سازی زودهنگام چنین حملات چندمرحله‌ای ضروری هستند.

سونامی اخراج کارکنان غول‌های فناوری جهان فروکش کرد

بزرگ‌ترین شرکت‌های فناوری جهان در ۶ ماه اول سال میلادی جاری، در مجموع ۷۲ هزار نفر از کارکنان خود را اخراج کردند. به گزارش ایسنا، داده‌ها نشان می‌دهد که از سال ۲۰۲۳، روند اخراج کارکنان غول‌های فناوری کند شده است و حدود ۲۱۳ هزار نفر در نیمه اول سال ۲۰۲۳ و حدود ۱۰۰ هزار نفر در نیمه اول سال ۲۰۲۴ شغل خود را از دست داده‌اند. داده‌های منتشر شده نشان می‌دهد که اخراج کارکنان شرکت‌های بزرگ فناوری در نیمه اول سال ۲۰۲۵ در مقایسه با مدت مشابه سال گذشته، ۲۸ درصد کاهش یافته است. شرکت مایکروسافت در ماه مه، با اشاره به تلاش برای بازسازی ساختار خود، ۳۰۰۰ نفر از کارکنان این شرکت و در مجموع ۱۲ هزار نفر را در نیمه اول سال ۲۰۲۵ اخراج کرد. این غول نرم‌افزاری، برای اخراج ۹۰۰۰ نفر از دیگر کارکنان خود آماده می‌شود که چهار درصد از نیروی کار جهانی این شرکت را تشکیل می‌دهند. خبرگزاری آناتولی گزارش کرد، شرکت امنیت سایبری «کراوداسترایک» (CrowdStrike) در ماه مه، اعلام کرد که برای همگام شدن با پیشرفت‌های هوش مصنوعی، پنج درصد از نیروی کار خود را کاهش خواهد داد. طبق داده‌های وب‌سایت رتبه‌بندی شرکت‌های فناوری بر اساس ارزش بازار آنها، ارزش بازار شرکت‌های فناوری با این اخراج کارکنان، افزایش می‌یابد.

افزونه کروم سارق اطلاعات از آب درآمد

یک افزونه پرطرفدار و تایید شده در مرورگر کروم و اج اطلاعات کاربران را ردیابی می‌کند و بخشی از یک کمپین جاسوسی بزرگ‌تر با ۱۸ افزونه به شمار می‌آید. به گزارش مهر به نقل از رجیستر، یک افزونه کروم و مرورگر اج با بیش از ۱۰۰ هزار بار دانلود که نشان تأیید گوگل را نیز دارد، یک ابزار انتخابگر رنگ را در اختیار کاربران قرار می‌دهد. اما به گفته محققان امنیتی این افزونه متاسفانه داده‌های هر بار استفاده از مرورگر را نیز سرقت، فعالیت‌ها را در وب‌سایت‌ها ردیابی و در مرورگرهای وب قربانیان، درهای پشتی ایجاد می‌کند. ابزارهای انتخابگر رنگ به کاربران اجازه می‌دهند هر رنگی را از یک وب‌سایت انتخاب کرده و آن را برای استفاده بعدی در کلیپ‌بورد کپی کنند. این قابلیت برای طراحی برنامه‌ها، وب‌سایت‌ها و موارد مشابه مفید است. افزونه مذکور هنوز هم از طریق فروشگاه‌های مربوطه مایکروسافت و گوگل در زمان انتشار این خبر برای دانلود در دسترس است. از سوی دیگر گوگل و مایکروسافت، شرکت‌های ارایه‌دهنده این مرورگرها و فروشگاه‌های آنها به سوالات نشریه پاسخ نداده‌اند. افزونه مذکور به Geco extension تعلق دارد و بیش از ۸۰۰ نقد در وب استور کروم و ۴.۲ امتیاز نیز دارد.

هوش مصنوعی ایلان ماسک در ترکیه مسدود شد

دادگاهی در ترکیه دسترسی به گراک، چت‌بات هوش مصنوعی ایلان ماسک را مسدود کرد زیرا پاسخ‌های تولیدی آن به گفته مقامات اهانت‌به‌رجب‌طیب اردوغان رییس جمهور این کشور به حساب می‌آمدند. به گزارش مهر به نقل از رویترز، چالش‌های سوگیری سیاسی، نفرت پراکنی و دقت چت‌بات‌های هوش مصنوعی از زمان عرضه چت جی پی تی شرکت اوپن‌ای آی در ۲۰۲۲ میلادی یکی از نگرانی‌های کارشناسان بودند. دفتر دادستانی کل در آنکارا، پایتخت ترکیه تحقیقاتی رسمی درباره این رویداد را آغاز کرده است این نخستین‌باری است که دسترسی به یک ابزار چت مصنوعی در ترکیه ممنوع می‌شود. تاکنون پلتفرم ایکس یا ایلان ماسک، مالک آن درباره این تصمیم اظهارنظر نکرده‌اند. این چت‌بات هوش مصنوعی که توسط شرکت xAI ساخته شده در پلتفرم ایکس یکپارچه شده و طبق گزارش‌ها هنگامی که سوالاتی خاص به زبان ترکی از آن پرسیده شد، محتوای اهانت‌آمیزی درباره اردوغان تولید کرد. سازمان تنظیم مقررات و ارتباطات رادیویی ترکیه (BTK) پس از دستور دادگاه این ممنوعیت را به دلیل نقض قوانین ترکیه اعمال کرده که طبق آن توهین به رییس جمهور جرم است و مجازاتی تا چهار سال زندان دارد.