اخبار

افزایش تهدید بدافزارها با مهندسی اجتماعی

کارشناس ارشد امنیت اداره کل اطلاعات و فناوری اطلاعات استان اصفهان گفت: بدافزارها با بهره‌گیری از مهندسی اجتماعی و لینک‌های فریبنده، امنیت کاربران را تهدید و اطلاعات حساس آنها را سرقت می‌کنند. سیدعمادالدین فرشته‌نژاد در گفت‌وگو با ایسنا اظهار کرد: بدافزارها، برنامه‌هایی مخرب هستند که با هدف آسیب رساندن به دستگاه‌ها و سیستم‌ها طراحی شده‌اند. این برنامه‌ها می‌توانند از راه‌های مختلفی مانند ایمیل‌های آلوده، دانلود از وب‌سایت‌های نامعتبر یا بهره‌برداری از آسیب‌پذیری‌های نرم‌افزاری وارد دستگاه‌ها شوند و پس از ورود، اقدامات گوناگونی انجام بدهند؛ از جمله سرقت اطلاعات شخصی، رمزگذاری فایل‌ها، دسترسی به فایل‌ها، دوربین و میکروفون و حتی تبدیل دستگاه به ابزاری برای انجام حملات سایبری. وی افزود: یکی از شایع‌ترین روش‌های نفوذ بدافزار، ترغیب کاربران به کلیک روی پیوندهای ناشناس است؛ پیوندهایی که معمولا از طریق پیامک یا شبکه‌های اجتماعی ارسال می‌شوند و ممکن است به صفحاتی جعلی یا حاوی بدافزار منتهی شوند. این بدافزارها غالباً با کسب تأیید از خود کاربر، بدون آنکه کاربر از ماهیت واقعی آنها آگاه باشد، روی دستگاه نصب شده و به اطلاعات حساس همچون داده‌های بانکی، رمزهای عبور و سایر اطلاعات شخصی دسترسی پیدا می‌کنند. این روش فریبکارانه که از تمایل یا ناآگاهی کاربران برای دریافت دسترسی سوءاستفاده می‌کند، به «مهندسی اجتماعی» معروف است. کارشناس ارشد امنیت اداره کل اطلاعات و فناوری اطلاعات استان اصفهان مخابرات ادامه داد: در این میان، لازم است تفاوت میان اپلیکیشن‌های معمولی و بدافزارها نیز روشن شود. اپلیکیشن‌های متعارف با اطلاع و رضایت کاربر نصب می‌شوند و هدف مشخص و مفیدی را دنبال می‌کنند، اما در مقابل، جاسوس‌افزارها و تروجان‌ها که نوعی بدافزار محسوب می‌شوند، معمولا بدون اطلاع کاربر و با اهداف مخرب وارد سیستم می‌شوند. جاسوس‌افزارها به‌طور خاص برای نظارت بر فعالیت‌های کاربر و جمع‌آوری اطلاعات شخصی طراحی شده‌اند، در حالی که تروجان‌ها می‌توانند مانند یک در پشتی عمل کرده و امکان اجرای انواع دستورات مخرب را برای مهاجم فراهم کنند. تفاوت اصلی میان این سه نوع نرم‌افزار، در نحوه عملکرد و هدف آنها نهفته است؛ جایی که اپلیکیشن‌های معمولی برای استفاده مشروع و شفاف ساخته می‌شوند، اما جاسوس‌افزارها و تروجان‌ها ماهیتی پنهان و تهدیدآمیز دارند. فرشته‌نژاد اضافه کرد: از آن جایی که سیستم‌عامل‌های مختلف، به‌ویژه اندروید و iOS، در برابر تهدیدات امنیتی شرایط یکسانی ندارند، درک تفاوت‌های آنها نیز اهمیت دارد. iOS به دلیل ساختار بسته و کنترل سخت‌گیرانه اپل بر فرآیند انتشار برنامه‌ها و به‌روزرسانی‌ها، از نظر امنیتی ایمن‌تر شناخته می‌شود. در مقابل، اندروید به سبب ماهیت متن‌باز، تنوع سخت‌افزارها و امکان نصب برنامه‌ها از منابع متفرقه، بیشتر در معرض خطر بدافزارها قرار دارد. با این حال، این بدان معنا نیست که iOS کاملا مصون است یا اندروید الزاما ناامن است. رعایت اصول امنیتی از سوی کاربران در هر دو سیستم‌عامل می‌تواند نقش مهمی در کاهش تهدیدات ایفا کند.

اپل از مهندس طراح سابق خود شکایت کرد

شرکت اپل در دادخواست جدید خود مدعی شده است که یکی از مهندسان سابق این شرکت، اسرار توسعه هدست واقعیت ترکیبی «ویژن پرو» (Vision Pro) را افشا کرده است. به گزارش ایسنا، شرکت اپل از یکی از مهندسان طراح سابق خود به اتهام سرقت گنجینه‌ای از اسرار تجاری که سپس به کارفرمای جدیدش، شرکت اسنپ (Snap) ارایه داده بود، شکایت کرده است. به نقل از سیلیکون‌ولی، این مهندس سابق اپل به نام «دی لیو» (Di Liu) پس از ۷ سال کار در اپل، نقش خود را به عنوان مهندس ارشد طراحی محصول ترک کرد و دلایل شخصی و خانوادگی را دلیل استعفای خود از این شرکت ذکر کرد. وی قبل از ترک اپل روی توسعه هدست «Vision Pro» کار می‌کرد، جایی که طبق دادخواست اپل، به فناوری‌های مختلف اپل که در این هدست گنجانده شده‌اند یا هنوز منتشر نشده‌اند، دسترسی داشت. این دادخواست همچنین ادعا می‌کند که «لیو» دو هفته قبل از استعفا، به اپل نگفته است که شرکت اسنپ (جایی که این طراح طبق پروفایل لینکدین خود از ژانویه ۲۰۲۵ در آن مشغول به کار است) به او شغلی پیشنهاد داده است که به‌طور قابل توجهی مشابه با نقش وی در شرکتی است که از آن جدا شده است. شرکت اسنپ علاوه بر مالکیت برنامه «اسنپ‌چت» عینک‌های واقعیت افزوده به نام «Spectacles» را نیز تولید می‌کند که در حال حاضر نسل پنجم آن عرضه شده است. طبق این گزارش، تصمیم «لیو» برای عدم اطلاع‌رسانی به اپل مبنی بر اینکه به زودی روی محصولی مشابه با «Vision Pro» در شرکت دیگری کار خواهد کرد، به او اجازه داد تا در یک دوره استاندارد دو هفته‌ای از اپل جدا شود. در این دادخواست ادعا شده است که «لیو» سه روز قبل از ترک اپل، از مجوزهای دسترسی خود برای دانلود هزاران سند شرکتی اپل استفاده کرده و آنها را در فضای ابری شخصی خود بارگذاری کرده است. این دادخواست ادعا می‌کند که او احتمالا با توجه به شباهت‌های آشکار بین این محصولات، قصد داشته عمدا از اطلاعات اختصاصی اپل در شرکت اسنپ استفاده کند. وی همچنین فایل‌هایی را از لپ‌تاپ کاری خود حذف کرده است که می‌توانست او را به دردسر بیندازد.

ابزارهای کنترل اینترنت چگونه کسب‌وکارها را نشانه گرفته‌اند؟

خطر فروپاشی اکوسیستم دیجیتال ایران

در روزهایی که اقتصاد دیجیتال یکی از معدود مسیرهای امیدبخش برای عبور از بحران‌های مزمن اقتصادی ایران تلقی می‌شود، دو نهاد صنفی شاخص کشور با صدای بلند نسبت به فروپاشی این اکوسیستم هشدار داده‌اند. نامه‌های انجمن صنفی کسب‌وکارهای اینترنتی و انجمن تجارت الکترونیک تهران، تصویری شفاف و نگران‌کننده از خسارت‌های روزافزون محدودیت‌های اینترنتی، انسداد کانال‌های تبلیغات دیجیتال، و نااطمینانی در تصمیم‌سازی‌های کلان ترسیم می‌کند؛ وضعیتی که اگر بی‌پاسخ بماند، نه‌تنها سرمایه‌گذاران را فراری می‌دهد، بلکه ستون اقتصاد دیجیتال را نیز فرو می‌ریزد. دو نهاد مهم در حوزه اقتصاد دیجیتال کشور - انجمن صنفی کسب‌وکارهای اینترنتی و انجمن تجارت الکترونیک تهران - در نامه‌هایی جداگانه به مقامات عالی‌رتبه دولت از جمله رییس‌جمهور، معاون اول، وزیر ارتباطات، وزیر صمت و رییس مرکز ملی فضای مجازی، نسبت به تبعات سنگین محدودیت‌ها و اختلالات اینترنتی هشدار داده‌اند. این دو نامه به شکلی کم‌سابقه بر یک مساله واحد تمرکز داشتند: خطر فروپاشی اکوسیستم دیجیتال ایران. به گفته انجمن صنفی، تداوم اختلالات اینترنتی، نه‌تنها به کاهش چشمگیر درآمدهای دیجیتال منجر شده، بلکه اعتماد کاربران و سرمایه‌گذاران را نیز خدشه‌دار کرده است. این وضعیت به‌ویژه در شرایطی رخ می‌دهد که ایران بیش از هر زمان دیگری به توسعه اقتصاد دیجیتال نیاز دارد تا بتواند از فشار تحریم‌ها بکاهد و نوسانات اقتصادی را کنترل کند.

خسارت‌های روزانه و نابودی تدریجی مشاغل

طبق اعلام انجمن صنفی کسب‌وکارهای اینترنتی، بیش از ۴۰۰ هزار کسب‌وکار خرد و متوسط (SME) در کشور به شکل مستقیم و غیرمستقیم از اینترنت بهره می‌برند. این کسب‌وکارها طی ماه‌های گذشته با موجی از قطعی‌ها، کاهش سرعت، فیلترینگ گسترده و محدودیت‌های زیرساختی مواجه شده‌اند؛ وضعیتی که به گفته این انجمن، در حال تبدیل شدن به بحرانی جدی است و منجر به تعدیل نیرو، تعطیلی شرکت‌ها، مهاجرت فعالان حوزه و رکود در سرمایه‌گذاری شده است. در بخشی از نامه آمده است که گزارش‌های مستند از داخل شرکت‌ها نشان می‌دهد «روزانه میلیاردها تومان خسارت به بخش خصوصی وارد می‌شود» و هیچ سازوکاری نیز برای جبران این خسارت‌ها وجود ندارد. این پیامدهای منفی، نه تنها کسب‌وکارهای نوپا، بلکه شرکت‌های تثبیت‌شده و حتی فروشگاه‌های آنلاین بزرگ را نیز دربر گرفته است.

محدودیت زیرساختی و انسداد Google Ads

از سوی دیگر، انجمن تجارت الکترونیک تهران نیز در نامه‌ای جداگانه، به مسدود شدن دامنه تبلیغاتی Google Ads اعتراض کرده است. طبق این نامه، انسداد www.googleadservices.com که پیش‌تر بدون اطلاع‌رسانی عمومی صورت گرفت، کسب‌وکارهای فعال در حوزه تبلیغات دیجیتال را با کاهش شدید بازدهی و کاهش فروش مواجه کرده است. برای بسیاری از برندهای ایرانی که از طریق Google Ads به مخاطبان هدف خود در داخل و خارج از کشور دسترسی داشتند، این انسداد به معنی از دست رفتن کانال‌های حیاتی بازاریابی بوده است. انجمن تجارت الکترونیک هشدار داده که این محدودیت‌ها منجر به بی‌اعتمادی مشتریان و خروج تدریجی کاربران از پلتفرم‌های داخلی می‌شود. در نامه انجمن تجارت الکترونیک تهران به وزیر ارتباطات نوشته شده است که برخی محدودیت‌های فنی و زیرساختی، مانعی جدی بر سر راه فعالیت این مجموعه‌ها شده است. یکی از مهم‌ترین این محدودیت‌ها، انسداد دامنه تبلیغاتی Google Ads (به نشانی www.googleadservices.com) است که از شریان‌های اصلی هدایت ترافیک کاربران به سمت کسب‌وکارهای دیجیتال به شمار می‌رود. این انسداد باعث کاهش محسوس فروش، افت بازدید و دشواری در فرایندهای جذب مشتری شده و در روزهایی که نیاز به پایداری اقتصادی بیش از هر زمان دیگری احساس می‌شود، ضربه‌ای جدی به بدنه فعال و مولد این بخش وارد کرده است. در ادامه این نامه آمده است: «بیشتر کسب‌وکارهای دیجیتال، به‌ویژه در شرایط تحریم و محدودیت‌های بازار داخلی، وابسته به سرویس‌های تبلیغات دیجیتال برای دسترسی به مخاطبان هدف هستند. در چنین شرایطی، انتظار می‌رود به‌جای افزودن بر موانع، مسیر تنفس این بخش راهبردی اقتصاد کشور باز شود.» در بخش دیگر این نامه نوشته شده است، در روزهایی که مردم ایران زیر سایه تهدید و تجاوز آشکار دشمن قرار گرفتند و فضای عمومی کشور در گیر التهاب و نگرانی بود (و البته آثار آن همچنان ادامه دارد) کسب‌وکارهای حوزه اقتصاد دیجیتال نیز همچون دیگر اجزای جامعه، خود را موظف به همراهی، تاب‌آوری و تداوم خدمت‌رسانی می‌دانند. در این مسیر، پلتفرم‌ها، فروشگاه‌های آنلاین، سامانه‌های خدمات‌رسان و شرکت‌های فناوری، باوجود تمام محدودیت‌ها، تلاش کردند تا چرخ اقتصاد دیجیتال کشور را زنده نگه داشته و هم‌زمان، به مسوولیت اجتماعی خود در کنار مردم عمل کنند. انجمن تجارت الکترونیک تهران در این نامه ادامه داده است: «ما ضمن ابراز همدردی با مردم شریف ایران و اعلام تعهد خود به ایستادگی و تداوم خدمت‌رسانی، خواستار آن هستیم که محدودیت ایجاد شده بر بستر تبلیغاتی Google Ads در اسرع وقت بررسی و مرتفع شود و در مسیر تصمیم‌سازی، از ظرفیت تشکل‌ها و نمایندگان رسمی بخش خصوصی استفاده شود تا تصمیمات، هم‌راستا با واقعیت‌های میدانی و اقتضائات اقتصادی کشور باشد. کسب‌وکارهای دیجیتال، ستون اقتصاد نوین ایران هستند. این ستون را در روزهای سخت، تنها نگذاریم.»

نااطمینانی ساختاری و نیاز به شفافیت

هر دو انجمن به یک دغدغه بنیادین اشاره کرده‌اند: نبود شفافیت در سیاست‌گذاری اینترنتی کشور. تصمیم‌گیری‌های ناگهانی، بدون اطلاع قبلی و بدون مشارکت بخش خصوصی، موجب تشدید نااطمینانی در فضای کسب‌وکار شده است. انجمن صنفی پیشنهاد داده است که داشبوردی عمومی برای گزارش‌گیری وضعیت لحظه‌ای اینترنت در کشور راه‌اندازی شود تا همه ذی‌نفعان از وضعیت فنی شبکه، زمان قطع یا افت کیفیت، علت اختلال و اقدامات اصلاحی مطلع باشند. همچنین تأکید شده که تدوین و اجرای سیاست‌های ارتباطی و زیرساختی بدون مشارکت بخش خصوصی و فعالان اکوسیستم دیجیتال، ناکارآمد و پرهزینه خواهد بود. این نهادها خواستار گشودن مسیر تعامل مستقیم با وزارت ارتباطات، مرکز ملی فضای مجازی و سایر نهادهای مسوول شده‌اند.

مهاجرت نخبگان و خروج سرمایه انسانی

یکی دیگر از هشدارهای مشترک این دو نهاد صنفی، افزایش مهاجرت فعالان حوزه فناوری و متخصصان دیجیتال از کشور است. قطعی‌ها و فیلترینگ، ضمن ایجاد مانع در فعالیت حرفه‌ای، امکان تعامل با بازارهای بین‌المللی و انجام پروژه‌های فریلنسری را به‌شدت کاهش داده است. به گفته کارشناسان، محدودیت‌های مداوم اینترنت موجب کاهش انگیزه، افت نوآوری و رشد پدیده «فرار مغزهای دیجیتال» شده است؛ پدیده‌ای که جبران آن در کوتاه‌مدت امکان‌پذیر نیست.

ابزارهای محدودسازی از DPI تا مسدودسازی تبلیغاتی

برخی گزارش‌ها و منابع فنی حاکی از آن است که محدودیت‌های اعمال‌شده، تنها محدود به فیلتر شدن دامنه‌ها نیست. استفاده از ابزارهایی مانند بازرسی عمیق بسته‌ها (Deep Packet Inspection یا DPI)، مسدودسازی پروتکل‌های ارتباطی مانند QUIC و اختلال در سیستم‌های نام دامنه (DNS) نیز به عنوان بخشی از سازوکار محدودسازی به کار گرفته شده‌اند. این ابزارها اگرچه در برخی کشورهای اقتدارگرا برای کنترل محتوا استفاده می‌شوند، اما در ایران به علت شدت و وسعت اجرا، آسیب‌های جدی به عملکرد طبیعی اینترنت وارد کرده‌اند.

تبعات جهانی برای اقتصاد دیجیتال ایران

ایران به‌رغم برخورداری از ظرفیت بالای انسانی و فنی، طی سال‌های گذشته سهم محدودی از اقتصاد دیجیتال جهانی داشته است. تحریم‌های بین‌المللی، محدودیت دسترسی به ابزارهای پرداخت جهانی، و عدم امکان مشارکت در پلتفرم‌های بین‌المللی، بخشی از این عقب‌ماندگی را توضیح می‌دهد. اما بخش دیگر، ناشی از تصمیم‌های داخلی و محدودیت‌های تحمیلی بر زیرساخت اینترنت است. فیلترینگ گسترده و بی‌ثباتی در کیفیت ارتباطات، موجب کاهش جذابیت سرمایه‌گذاری در حوزه فناوری شده و مسیر توسعه صادرات دیجیتال را مسدود کرده است. کارشناسان معتقدند که حتی در صورت رفع تحریم‌های خارجی، تداوم این سیاست‌های داخلی مانع دستیابی ایران به جایگاه شایسته در اقتصاد دیجیتال خواهد بود. خواسته‌های نهادهای صنفی در این دو نامه به روشنی قابل استخراج است: نخست، توقف محدودیت‌های زیرساختی و تبلیغاتی، دوم، ایجاد شفافیت در سیاست‌گذاری اینترنتی، سوم، استفاده از ظرفیت نهادهای صنفی برای طراحی تصمیمات کلان، و در نهایت، تدوین برنامه‌ای برای احیای اکوسیستم دیجیتال کشور. به باور این نهادها، تنها با تقویت اعتماد عمومی، حفظ آزادی نسبی در دسترسی به اطلاعات، و مشارکت بخش خصوصی در تصمیم‌سازی‌ها می‌توان از فروپاشی اقتصاد دیجیتال جلوگیری کرد.

چشم‌انداز ناپایدار؛ بازسازی یا واگذاری؟

سوال کلیدی اینجاست: آیا دولت می‌خواهد به سمت بازسازی اعتماد دیجیتال حرکت کند یا به تدریج میدان را به بازیگران خارجی و زیرزمینی واگذار کند؟ در وضعیت فعلی، بسیاری از کاربران ایرانی به استفاده از VPN، ابزارهای دور زدن فیلترینگ و حتی مهاجرت کامل به پلتفرم‌های خارجی روی آورده‌اند. اگر این روند ادامه پیدا کند، نه تنها کسب‌وکارهای ایرانی در رقابت شکست می‌خورند، بلکه بخش مهمی از حاکمیت داده‌ها نیز از کنترل ملی خارج خواهد شد. در شرایطی که اقتصاد کشور نیازمند توسعه صادرات غیرنفتی، جذب سرمایه، و تقویت زیرساخت دیجیتال است، انسداد مسیرهای ارتباطی و بازاریابی آنلاین، نوعی ناسازگاری جدی با اهداف اعلام‌شده توسعه است. از این منظر، بازبینی در سیاست‌های اینترنتی نه تنها ضرورتی فناورانه، بلکه ضرورتی اقتصادی و سیاسی است. مجموع محتوای دو نامه صنفی اخیر، هشداری روشن است نسبت به ادامه وضع موجود. اگرچه دلایل امنیتی، سیاسی یا فرهنگی ممکن است در پس محدودیت‌های اینترنتی مطرح شود، اما واقعیت این است که ادامه این رویکرد، زیربنای اقتصاد نوین کشور را تهدید می‌کند. اقتصاد دیجیتال ایران، با تمام چالش‌ها و ظرفیت‌هایش، نیازمند سیاست‌گذاری شفاف، زیرساخت پایدار، و آزادی معقول در دسترسی به اطلاعات و تبلیغات دیجیتال است. تنها در صورتی که تصمیم‌گیران به این هشدارها توجه کرده و مسیر تعامل با بخش خصوصی را باز کنند، می‌توان به احیای اعتماد عمومی، تثبیت بازارهای آنلاین و جلوگیری از مهاجرت نخبگان امیدوار بود. در غیر این صورت، اقتصاد دیجیتال ایران به‌جای موتور رشد، به یکی از قربانیان اصلی سیاستگذاری‌های غیرشفاف تبدیل خواهد شد.

فیلترشکن‌ها دروازه‌ای به روی بدافزارها و تهدیدات سایبری

درباره فیلترشکن‌ها بارها هشدار داده شد که نصب آن با این وسعت برروی انواع دستگاه‌هایی که همه افراد اطلاعات خود را برروی آنها نگه می‌دارند، خطرناک است و این موضوع با توجه به اتفاقات اخیر، از اهمیت ویژه‌ای برخوردار شده و در نتیجه نصب آن باعث دسترسی به اطلاعات شخصی یا حساس می‌شود و تهدید بزرگی برای فرد و دستگاهی که برروی آن فیلترشکن نصب شده، محسوب می‌شود. بهناز آریا، رییس کمیسیون افتای سازمان نظام صنفی رایانه‌ای کشور در گفت‌وگو با ایسنا، با بیان این مطلب، درباره امنیت سایبری و اهمیت آن اظهار کرد: امنیت سایبری در شرایط فعلی ایران بیشتر از یک مساله فنی بوده و می‌توان گفت تبدیل به یک اولویت به عنوان امنیت ملی شده است. وی افزود: با توجه به تحولات منطقه‌ای اخیر و فعالیت گروه‌های مختلف سایبری و نفوذگر باید امنیت سایبری را این گونه تعریف کرد که یک اکوسیستم و یک زیست‌بوم یکپارچه از سیاست‌ها، فناوری‌ها، فرآیندها و نیروی انسانی است که برای حفاظت از زیرساخت‌های حیاتی، اطلاعات حساس و حاکمیت دیجیتال کشور طراحی شده است و نقش بخش خصوصی به عنوان بخشی از این زیست‌بوم امنیت سایبری و شریک استراتژیک حاکمیت در تولید راه‌حل‌های بومی و خدمت‌رسانی و پیاده‌سازی باید نقشی کلیدی محسوب شود. آریا گفت: توسعه ابزارهای تشخیص تهدید، سیستم‌های رمزنگاری، تجهیزات و نرم‌افزارهای بومی که باید توسط بخش خصوصی تولید شود نقش بخش خصوصی را در این حوزه بسیار ویژه و کلیدی می‌کند. رایج‌ترین تهدیدات سایبری که این روزها با آن مواجهیم و با سرعت بالایی در شرایط فعلی در حال اتفاق افتادن هستند، حملات باج‌افزاری است که اخیرا بسیار زیاد شده است مخصوصا حملات هدفمند علیه بسیاری از زیرساخت‌های حیاتی و خدمات‌دهندگان به آنها و دستگاه‌های اجرایی. رییس کمیسیون افتا سازمان نظام صنفی رایانه‌ای تهران تشریح کرد: علاوه بر موارد گفته شده مهندسی اجتماعی یا فیشینگ همیشه جزو مهم‌ترین حملات بوده و همچنان هم به دلیل اینکه عامل انسانی در آن دخیل است ادامه دارد و می‌تواند درصد موفقیت بالایی داشته باشد. همچنین حملاتی که با عنوان تهدیدات مداوم پیشرفته یا APTها شناخته می‌شوند، نیز به صورت هدفمند همواره جزو تهدیدات پرخطر بوده‌اند.

نحوه مقابله با تهدیدات سایبری چگونه است؟

وی در ادامه صحبت‌هایش با اشاره به نحوه مقابله با تهدیدات ذکر شده، تصریح کرد: برای مقابله با انواع تهدیدات حتما نیاز به روش‌ها و مدل‌های مختلفی برای دفاع در عمق و آمادگی خود داریم اما در رأس همه راهکارها نیازمند ارتقای دانش، آموزش و آگاهی رسانی هستیم و هرچه بر روی این موضوع تأکید کنیم کم است. همچنین می‌توان ارتباط مناسبی بین بخش خصوصی و حاکمیت برقرار کرد به گونه‌ای که بخش خصوصی بازوی واقعی مشورتی و اجرایی حاکمیت باشد تا بتوانیم به درستی برنامه‌های پیشگیرانه و مقابله با بحران درستی را با برنامه‌ریزی، تمرین و در زمان مناسب اجرایی کنیم. او گفت: البته لازم است محصولات و خدمات استاندارد و قابل رقابت داخلی داشته باشیم تا در صورت امکان جایگزین محصولات خارجی شوند و با روش‌هایی مانند ایجاد بیمه سایبری، حسابرسی فناوری اطلاعات و حمایت از توسعه صنعت افتا به بهبود وضعیت امنیت سایبری کشور کمک کنیم. به گفته آریا حمایت از توانمندتر شدن بخش خصوصی می‌تواند کمک کند که صنعت امنیت سایبری و افتا تقویت و آنچه که لازمه تأمین امنیت مطلوب ملی است فراهم و موارد لازم به این بخش برون‌سپاری شود. رییس کمیسیون افتا نصر تهران تصریح کرد: در زمینه تفاوت بین امنیت سایبری و امنیت اطلاعات باید گفت این موضوع عملا در فضای کسب و کاری ایران اهمیت ویژه‌ای دارد. امنیت اطلاعات شامل حفاظت از اطلاعات در تمام قالب‌ها از جمله اسناد فیزیکی، مکالمات، پایگاه‌های داده حتی اطلاعاتی که در درون ذهن کارکنان وجود دارد می‌شود. وی ادامه داد: اما امنیت سایبری متمرکز بر محافظت از دارایی‌های دیجیتال و سیستم‌های تحت بسترهای مبتنی بر فناری اطلاعات است. ما در حوزه امنیت سایبری و حفاظت از دارایی‌های دیجیتال خود باید اهمیت ویژه قائل شده و برنامه‌های ویژه‌ای داشته باشیم. آموزش قوی‌ترین سلاحی است که می‌توان برای تغییر جهان به کار برد و باید آموزش و آگاهی‌رسانی یک استراتژی و سرمایه‌گذاری ملی باشد. به گفته آریا، از آن جا که بالای ۹۰ درصد حملات سایبری از طریق خطاهای انسانی صورت می‌گیرد، در این راستا می‌توان به بخش خصوصی نقش کلیدی آموزش مهارت محور و مبتنی بر آگاهی‌رسانی را داد تا سطح بلوغ امنیت سایبری را ارتقا بدهیم. همچنین از سن کم می‌توان آموزش و آگاهی‌رسانی را از طریق مدارس و تحصیلات نهادینه کرد تا بحران نیروی انسانی هم برای سال‌های آتی بهبود یابد. در عین حال پیاده‌سازی برنامه‌های آگاهی‌رسانی امنیت در سازمان‌ها برای تغییر رفتار در مقابل تهدیدات سایبری می‌تواند بسیار کمک کننده باشد.

تهدید به نام فیلترشکن‌ها

وی درباره خطرات فیلترشکن‌ها توضیح داد: در زمینه فیلترشکن‌ها بارها هشدار داده شد که نصب آن با این وسعت روی انواع تجهیزات و دستگاه‌هایی که همه در حال استفاده هستند و اطلاعات خود را روی آنها نگه می‌دارند، خطرناک است. با توجه به اتفاقات اخیر این موضوع از اهمیت ویژه‌ای برخوردار است و نصب آن باعث دسترسی به اطلاعات شخصی یا حساس می‌شود که در نهایت تهدید بزرگی برای فرد و دستگاهی که بر روی آن فیلترشکن نصب شده، محسوب می‌شود. آریا تاکید کرد: ما نهادهای حاکمیتی مختلفی را داریم که تعدد و موازی‌کاری‌شان شاید بیش از پیش نشان داده می‌شود. تعداد متولیان و نهادهای ما که در این حوزه مسوولیت دارند بسیار زیاد است و فکر می‌کنم به دلیل این موازی‌کاری و نبود یک استراتژی واحد و شفاف با چالش بزرگی برای برنامه‌ریزی بلندمدت و حتی سرمایه‌گذاری هدفمند و موثر بخش خصوصی در این حوزه مواجهیم. رییس کمیسیون افتای سازمان نصر تهران با اشاره به راهکاری مورد نیاز گفت: ما بارها در این زمینه صحبت کردیم که نیازمندیم مجوز، متولیان و استراتژی‌های ما به صورت متمرکز و با برنامه‌ریزی موثر و به روز به امنیت ملی بپردازند. در این زمینه نقش بخش خصوصی بسیار پررنگ است که بعضا نادیده گرفته می‌شود. به تاکید وی، بخش خصوصی باید یک بازوی اجرایی قدرتمند برای سیاست‌های امنیت سایبری ملی کشور باشد و در سیاست‌گذاری‌ها نقش مشورتی داشته باشد. همچنین تجارب ما در نظر گرفته شود و از این بخش حمایت شود تا بتواند توسعه پیدا کند. وی تصریح کرد: ما نیازمند پیاده‌سازی مواردی مانند مدل‌های تداوم کسب‌وکار هستیم و از قبل باید برای آن برنامه‌ریزی و سرمایه‌گذاری کنیم. به‌شدت به آموزش و آگاهی‌رسانی و افزایش سطح بالای دانش نیاز داریم. علاوه بر موارد گفته‌شده موضوع نیروی انسانی متخصص بسیار مهم است و باید سرمایه‌گذاری‌های لازم انجام شود. آریا در پایان با بیان اینکه باید امنیت سایبری را با روش‌های درست توسعه بدهیم، اظهار کرد: در کنار موارد گفته شده باید سرمایه‌گذاری مناسبی در مراکز داده، شبکه ملی، مراکز پشتیبان‌گیری و... انجام شود که در زمان‌های بحران زیرساخت‌های حیاتی ما دچار مشکل نشوند. به‌نظر من کلید همه این موارد در تعامل مناسب بین بخش خصوصی و بخش دولتی است. بخش خصوصی باید شریک استراتژیک حاکمیت در تقویت امنیت ملی سایبری باشد آن هم در دورانی که با وجود هوش مصنوعی، با پدیده‌ای در تهدیدات و مخاطرات مواجهیم که امنیت سایبری را جزو اولویت‌های اول همه کشورهای جهان قرار داده و نقشی تعیین‌کننده در تامین امنیت ملی هر کشوری دارد.

دنیای فناوری

اطلاعات ۶ میلیون مشتری شرکت هواپیمایی استرالیایی هک شد

شرکت هواپیمایی استرالیایی کوانتاس اعلام کرد مجرمان سایبری یکی از مراکز تماس مشتریان آن را هدف گرفته‌اند و سیستم رایانشی را با استفاده از یک طرف ثالث هک کرده‌اند. به گزارش مهر به نقل از دویچه وله، این شرکت هواپیمایی اعلام کرد در سیستم مذکور اطلاعات حساس ۶ میلیون مشتری‌اش از جمله نام، ایمیل، شماره موبایل و تاریخ تولد آنان بوده است. البته کوانتاس تاکید داشت جزییات و اطلاعات کارت‌های اعتباری و شماره پاسپورت افراد در این سیستم ذخیره نشده بوده است. در بیانیه شرکت آمده است: این رویداد زمانی رخ داد که یک مجرم سایبری مرکز تماسی را هدف گرفت و به وسیله یک پلتفرم خدمات مشتریان طرف ثالث دسترسی یافت. این امر هیچ تاثیری روی فعالیت‌های کوانتاس یا ایمنی شرکت هواپیمایی نداشته است. کوانتاس همچنین اعلام کرده تحقیقی درباره حمله سایبری آغاز کرده است. در بخش دیگر بیانیه آن آمده است: ما همچنان به تحقیق درباره میزان داده‌های سرقت‌شده ادامه می‌دهیم هرچند پیش‌بینی می‌شود این شاخص بالا باشد. همچنین شرکت اعلام کرده با مشتریانش درباره این رویداد تماس گرفته و جزییاتی درباره پشتیبانی فراهم کرده است. علاوه بر آن رویداد مذکور به سازمان «هماهنگ‌کننده ملی امنیت سایبری استرالیا» (National Cyber Security Coordinator) اطلاع‌رسانی شده است. البته این نخستین‌باری نیست که طی سال‌های اخیر کوانتاس با چالش‌های امنیت سایبری روبه‌رو می‌شود. این شرکت در سال ۲۰۲۴ میلادی پس از آنکه یک اختلال در اپ موبایل آن منجر به نشت نام و جزییات سفر مسافران شد، از مشتریانش عذرخواهی کرد.

گوگل به جمع‌آوری اطلاعات از دستگاه‌های خاموش متهم شد

هیات منصفه دادگاهی در ایالت کالیفرنیا اعلام کرد گوگل از داده‌های موبایل مشتریانش سواستفاده کرده و باید بیش از ۳۱۴.۶ میلیون دلار غرامت به کاربران تلفن‌های هوشمند اندروید در این ایالت بپردازد. به گزارش مهر به نقل از رویترز، هیات منصفه دادگاهی در ایالت کالیفرنیا به نفع شاکیان رأی داد و اعلام کرد شرکت گوگل بدون رضایت کاربران، اقدام به ارسال و دریافت اطلاعات از دستگاه‌های اندرویدی در حالت خاموش کرده است. خوزه کاستاندا، سخنگوی گوگل، در بیانیه‌ای اعلام کرد این شرکت قصد دارد نسبت به رأی صادره درخواست تجدیدنظر دهد. وی همچنین افزود که در این حکم، سرویس‌هایی که برای امنیت، عملکرد و اعتمادپذیری دستگاه‌های اندرویدی به کار گرفته می‌شوند، لحاظ نشده‌اند. در مقابل، گلن سامرز، وکیل شاکیان اظهار داشت که رأی دادگاه از اهمیت مسائل مطرح‌شده در این پرونده حمایت می‌کند و بیانگر جدی بودن تخلف گوگل است. این شکایت دسته‌جمعی در سال ۲۰۱۹ به نمایندگی از حدود ۱۴ میلیون نفر از ساکنان ایالت کالیفرنیا در دادگاه ایالتی مطرح شد. شاکیان ادعا کردند که گوگل به‌طور غیرمجاز اطلاعات تلفن‌های اندرویدی راحتی در حالت غیرفعال جمع‌آوری کرده و از آنها برای اهدافی مانند تبلیغات هدفمند استفاده کرده است. همچنین، این شرکت با انتقال داده‌ها از طریق اینترنت تلفن همراه، هزینه‌هایی را به کاربران تحمیل کرده است. در دفاع از خود، گوگل به دادگاه اعلام کرده است که هیچ‌یک از کاربران به دلیل این انتقال داده‌ها متحمل خسارت نشده‌اند. افزون بر این، گوگل مدعی شد که کاربران در قالب شرایط استفاده از خدمات و سیاست‌های حریم خصوصی شرکت، رضایت خود را نسبت به انتقال داده‌ها اعلام کرده‌اند.

هواوی باید با اتهامات کیفری روبه‌رو شود

یک قاضی در امریکا، با درخواست «هواوی تکنولوژیز» برای رد بخش عمده‌ای از کیفرخواست فدرال که این غول فناوری چینی را به تلاش برای سرقت اسرار فناوری از رقبای امریکایی و گمراه کردن بانک‌ها در مورد فعالیتش در ایران متهم می‌کرد، مخالفت کرد. به گزارش ایسنا، اتهامات وارد شده به هواوی پیرامون ایران، مربوط به ادعای کنترل هواوی بر شرکت هنگ کنگی اسکای کام است که در ایران فعالیت می‌کرد. آن دانلی، قاضی منطقه‌ای امریکا در بروکلین، روز سه‌شنبه گفت: دادستان‌ها به‌طور رضایت‌بخشی ادعا کردند که اسکای‌کام، به‌عنوان شرکت تابعه هواوی در ایران فعالیت می‌کرد و در نهایت به‌طور غیرمستقیم از بیش از ۱۰۰ میلیون دلار انتقال پول از طریق سیستم مالی امریکا، سود برده است. هواوی خود را بی‌گناه خوانده و به دنبال رد شدن ۱۳ مورد از ۱۶ اتهام مطرح شده بوده و خود را «هدفی برای تعقیب کیفری» نامیده است. این پرونده کیفری در دوره اول ریاست جمهوری دونالد ترامپ در سال ۲۰۱۸ آغاز شد؛ همان سالی که وزارت دادگستری، طرح «ابتکار چین» را برای رسیدگی به سرقت ادعایی مالکیت معنوی توسط پکن، آغاز کرد. منگ وانژو، مدیر ارشد مالی هواوی که پدرش بنیانگذار این شرکت بود، متهم بود و تقریبا سه سال در کانادا بازداشت شد تا اینکه اجازه بازگشت به چین را پیدا کرد. اتهامات علیه او در سال ۲۰۲۲ رد شد. دولت جو بایدن، رییس جمهور وقت امریکا، در سال ۲۰۲۲، طرح «ابتکار چین» را لغو کرد، زیرا منتقدان، این طرح را به نژادپرستی متهم کردند و گفتند که این طرح باعث ایجاد ترس و وحشتی می‌شود که تحقیقات علمی را متوقف می‌کند. بر اساس گزارش رویترز، شرکت هواوی که در شنژن مستقر است، در بیش از ۱۷۰ کشور فعالیت می‌کند و حدود ۲۰۸ هزار کارمند دارد. دولت امریکا از سال ۲۰۱۹، دسترسی هواوی به فناوری امریکایی را با استناد به نگرانی‌های امنیت ملی محدود کرده است. اما هواوی این ادعا را که این شرکت چینی، تهدیدی برای امنیت ملی امریکا است، رد می‌کند.