نخبگان فناوری ۱۸ میلیارد دلار ضرر کردند

ماسایوشی سان، بنیانگذار گروه سافت‌بانک و دیگر ثروتمندان در سراسر آسیا، روز جمعه که موج فروش جهانی فناوری در شرکت‌هایشان موج می‌زد، با از دست رفتن میلیاردها دلار از ثروت خود روبه‌رو شدند. به گزارش ایسنا، براساس محاسبات شاخص میلیاردرهای بلومبرگ، بیست و دو میلیاردر از چین، ژاپن، تایوان و کره‌جنوبی که در بین ۵۰۰ ثروتمند جهان قرار دارند تا ساعت ۱۰ صبح جمعه به وقت هنگ‌کنگ، بیش از ۲۱ میلیارد دلار از ثروت خود را از دست دادند و این رقم در نهایت به بیش از ۱۸ میلیارد دلار رسید. سان بزرگ‌ترین متضرر بود و ثروت او با ۳.۹ میلیارد دلار کاهش، به حدود ۲۹ میلیارد دلار رسید. شرکت‌هایی که در قلب رونق هوش مصنوعی قرار دارند، بیشترین آسیب را دیدند. کسانی که یک میلیارد دلار یا بیشتر ضرر کردند شامل تاکمیتسو تاکیزاکی از شرکت سازنده حسگرهای الکترونیکی کینس و جیسون چانگ، ثروتمندترین فرد سنگاپور از شرکت هولدینگ فناوری ASE که نیمه‌رساناها را مونتاژ و بسته‌بندی می‌کند، بودند. جی وای لی، سهامداران شرکت سامسونگ الکترونیکس، مادر و خواهرش - یکی از ثروتمندترین خانواده‌های آسیا - در مجموع حدود ۲.۵ میلیارد دلار از ثروت خود را از دست دادند. این آشفتگی همچنین ماه گذشته به صندوق‌های پوشش ریسک از جمله تایگر گلوبال منیجمنت و ویل راک کپیتال منیجمنت آسیب رساند، زیرا نگرانی‌ها در مورد سرمایه‌گذاری‌های هوش مصنوعی بازارها را آشفته کرد. براساس گزارش بلومبرگ، انتظارات مبنی بر اینکه مجلس نمایندگان و سنای تحت کنترل دموکرات‌ها برای کاهش سرعت ساخت مراکز داده -که جزو حیاتی زیرساخت‌های هوش مصنوعی هستند- تلاش خواهند کرد، پس از کاهش بی‌سابقه ۲.۳ تریلیون دلاری ارزش بازار شاخص نزدک ۱۰۰، به کاهش سهام فناوری در سراسر آسیا در معاملات روز جمعه دامن زد. این ضررها باعث شد جنسن هوانگ، مدیرعامل انویدیا، از فهرست ۱۰ ثروتمند برتر جهان خارج شود.

تشدید تحقیقات اتحادیه اروپا درباره الگوریتم تیک‌تاک

تیک‌تاک پس از آنکه رگولاتورهای اتحادیه اروپا دریافتند الگوریتم توصیه ویدیوی این پلتفرم، کاربران را به محتوای بالقوه مضر سوق می‌دهد و تحقیقات تقریبا سه ساله در مورد این برنامه اشتراک‌گذاری ویدیو را تشدید کرد، یک قدم به جریمه جدید نزدیک‌تر شد. به گزارش ایسنا، کمیسیون اروپا در یافته‌های اولیه روز جمعه اعلام کرد که کاربران تیک‌تاک بارها با ویدیوهایی در مورد موضوعاتی که قبلا با آنها سروکار داشته‌اند، از جمله موضوعات حساس مانند مشکلات سلامت روان و تصویر بدن، هدف قرار می‌گیرند. طبق بیانیه قوه مجریه اتحادیه اروپا، این امر می‌تواند «تاثیر مخربی» بر سلامت روان کاربران داشته باشد. این کمیسیون به تیک‌تاک، متعلق به شرکت چینی بایت دنس، توصیه کرد که طراحی فید شخصی‌سازی شده مرکزی «برای شما» را تغییر دهد. این شامل در نظر گرفتن ترجیحات صریح کاربران و احتمالا توقف استفاده از زمان مشاهده به عنوان سیگنالی برای توصیه ویدیوها می‌شود. این کمیسیون اعلام کرد: «قرار گرفتن مکرر در معرض چنین محتوایی ممکن است اثرات منفی جدی بر سلامت روان کاربران از جمله افزایش احساس غم یا اضطراب، نارضایتی از بدن، کاهش عزت نفس یا بدتر شدن اختلالات خوردن و بیماری‌های روانی موجود» داشته باشد. این پرونده بخشی از تلاش گسترده‌تر بروکسل برای مهار ویژگی‌هایی است که به گفته تنظیم‌کنندگان مقررات می‌تواند شبکه‌های اجتماعی در مقیاس بزرگ را اعتیادآور کند یا کودکان و کاربران آسیب‌پذیر را در معرض مطالب مضر قرار دهد. اورسولا فون در لاین، رییس کمیسیون اروپا، به‌طور جداگانه از برنامه‌هایی برای غیرقانونی کردن استفاده از شبکه‌های اجتماعی برای نوجوانان رونمایی کرده‌است. تیک‌تاک در بیانیه‌ای اعلام کرد: «کمیسیون مجموعه‌ای از اظهارات را مطرح کرده است که اساسا نادرست هستند و معماری پلتفرم ما و تعهد ما به ایمنی کاربران را تحریف می‌کنند. ما سابقه قوی در محافظت از جامعه خود داریم و در عین حال به کاربران کنترل مستقیم و شهودی بر تجربه محتوای خود می‌دهیم.» این یافته‌ها، تحقیقات گسترده‌ای را که در فوریه ۲۰۲۴ تحت قانون خدمات دیجیتال اتحادیه اروپا آغاز شد، تشدید می‌کند. قانون خدمات دیجیتال اتحادیه اروپا، مجموعه‌ای از قوانین جامع است که شبکه‌های اجتماعی و موتورهای جست‌وجو را به حذف محتوای غیرقانونی یا مضر ملزم می‌کند. این تحقیقات به‌طور فزاینده‌ای بر سازوکارهایی که این برنامه را بسیار محبوب کرده، متمرکز شده‌است و تنظیم‌کنندگان مقررات اروپایی بر اسکرول یا پیمایش بی‌نهایت، پخش خودکار و جریان ویدیوهای شخصی‌سازی‌شده مرکزی «برای شما» در تیک‌تاک تمرکز دارند. در اوایل سال جاری، کمیسیون به این نتیجه رسید که طراحی تیک‌تاک، قانون خدمات دیجیتال را نقض کرده است. این یافته‌های اخیر نه بر چگونگی ترغیب کاربران به ادامه پیمایش در تیک‌تاک، بلکه بر محتوایی تمرکز دارند که الگوریتم پس از شناخت علایق کاربران، به آنها نمایش می‌دهد. به گفته این کمیسیون، تیک‌تاک -که تحت مالکیت شرکت چینی «بایت‌دنس» قرار دارد- در ارزیابی یا کاهش خطرات ناشی از سیستم توصیه‌گر خود کوتاهی کرده است. این تحقیقات همچنین نحوه رسیدگی این پلتفرم به مسائل مربوط به حریم خصوصی و حفاظت از افراد زیر سن قانونی را زیر ذره‌بین قرار می‌دهد. این یافته‌های اولیه به این معناست که تیک‌تاک می‌تواند پیش از اتخاذ تصمیم نهایی توسط نهادهای نظارتی، به کمیسیون پاسخ دهد و تغییراتی را پیشنهاد کند. چنانچه کمیسیون به این نتیجه برسد که این پلتفرم قانون را نقض کرده است، می‌تواند جریمه‌هایی تا سقف ۶ درصد از کل فروش سالانه جهانی شرکت را برای آن تعیین کند. براساس گزارش بلومبرگ، اتحادیه اروپا در سال ۲۰۲۵، شرکت «بایت‌دنس» را به دلیل انتقال غیرقانونی داده‌های کاربران به چین، ۵۳۰ میلیون یورو (معادل ۵۹۲ میلیون دلار امریکا) جریمه کرد. همچنین در سال ۲۰۲۳ نیز این شرکت به دلیل قصور در حفاظت از داده‌های شخصی کودکان، به پرداخت ۳۴۵ میلیون یورو جریمه محکوم شده بود.

رکورد تاریخی رکود استخراج شکسته شد

بیت‌کوین زیر فشار فروش



بازار بیت‌کوین پس از یک هفته پرنوسان، همچنان درگیر فشار فروش و کاهش اعتماد سرمایه‌گذاران است. بزرگ‌ترین رمزارز جهان که در پی تحولات سیاسی امریکا و بسته شدن موقعیت‌های معاملاتی فروش، بار دیگر به محدوده ۸۰ هزار دلار نزدیک شده بود، روز پنجشنبه با موج تازه‌ای از فروش مواجه شد و بخش عمده رشد خود را از دست داد. قیمت بیت‌کوین در روز شنبه نیز در محدوده ۷۶ هزار دلار نوسان کرد و نتوانست نشانه‌ای قاطع از بازگشت به روند صعودی بروز دهد. همزمان، شاخص ترس وطمع به محدوده ترس سقوط کرده و صنعت استخراج نیز با طولانی‌ترین دوره دوری سختی شبکه از اوج تاریخی خود روبه‌رو شده است؛ مجموعه‌ای از تحولات که از دشوارتر شدن شرایط بازار رمزارزها حکایت دارد. بیت‌کوین در هفته‌ای که گذشت، نوسانات شدیدی را تجربه کرد. این رمزارز ابتدا در واکنش به مشخص شدن نتایج انتخابات میان‌دوره‌ای امریکا و کاهش بخشی از نااطمینانی‌های سیاسی، روندی صعودی در پیش گرفت و در روز چهارشنبه توانست بار دیگر از مرز ۸۰ هزار دلار عبور کند. با این حال، این رشد دوام چندانی نداشت و روز پنجشنبه، همزمان با ریزش بازار سهام امریکا، قیمت بیت‌کوین با افتی بیش از ۵ درصدی تا محدوده ۷۵ هزار دلار عقب نشست. براساس داده‌های بازار، بیت‌کوین در روز شنبه ۱۶ آبان همچنان در محدوده ۷۵ تا ۷۶ هزار دلار معامله می‌شد. به این ترتیب، این رمزارز در آستانه ثبت پنجمین کندل هفتگی منفی متوالی قرار گرفته است؛ اتفاقی که در صورت تداوم وضعیت فعلی تا پایان هفته، نشانه دیگری از استمرار فشار فروش در بازار خواهد بود. یکی از مهم‌ترین عوامل محدودکننده رشد قیمت، کاهش تقاضای سرمایه‌گذاران نهادی است. داده‌های پلتفرم سوسووالیو (SoSoValue) نشان می‌دهد صندوق‌های قابل معامله بورسی (ETF) اسپات بیت‌کوین در امریکا در مسیر ثبت دومین هفته متوالی خروج خالص سرمایه قرار گرفته‌اند. تا روز پنجشنبه، میزان خروج سرمایه از این صندوق‌ها به حدود ۸۶۹.۸۲ میلیون دلار رسید؛ در حالی که هفته پیش از آن، خروج خالص سرمایه حدود ۲۰۲.۵۹ میلیون دلار بود. افزایش قابل توجه این رقم نشان می‌دهد تمایل بخشی از سرمایه‌گذاران بزرگ به نگهداری بیت‌کوین کاهش یافته است. در چنین شرایطی، تداوم خروج سرمایه از ETFها می‌تواند به تضعیف تقاضای بازار و افزایش فشار فروش منجر شود.

چرا رشد بیت‌کوین پس از انتخابات امریکا دوام نیاورد؟

بخش مهمی از نوسانات اخیر بازار را باید در تحولات سیاسی و اقتصادی امریکا جست‌وجو کرد. در ابتدای هفته، معامله‌گران از مشخص شدن نتایج انتخابات میان‌دوره‌ای استقبال کردند و کاهش نااطمینانی‌های سیاسی به رشد دارایی‌های پرریسک، از جمله بیت‌کوین، کمک کرد. بخشی از این افزایش قیمت نیز ناشی از بسته شدن موقعیت‌های فروش یا شورت بود. معامله‌گرانی که پیش‌تر روی کاهش قیمت شرط بسته بودند، با صعود بازار ناچار به بستن موقعیت‌های خود شدند و همین مساله به تقویت موج خرید کمک کرد. اما شرایط در روز پنجشنبه تغییر کرد. پیروزی دموکرات‌ها و تصاحب کنترل هر دو مجلس کنگره، نگرانی‌هایی درباره مسیر سیاست‌گذاری اقتصادی و به‌ویژه آینده صنعت هوش مصنوعی ایجاد کرد. سرمایه‌گذاران نگران بودند که تغییر موازنه سیاسی در امریکا، روند توسعه مراکز داده و سرمایه‌گذاری‌های گسترده شرکت‌های فناوری در این حوزه را با محدودیت‌هایی مواجه کند. اهمیت این موضوع از آن جهت است که توسعه زیرساخت‌های هوش مصنوعی به تجهیزات پیشرفته، تراشه‌های گران‌قیمت و سرمایه‌گذاری‌های چندمیلیارد دلاری نیاز دارد. شرکت‌هایی مانند انویدیا و AMD نیز از تأمین‌کنندگان اصلی این تجهیزات هستند. در نتیجه، هرگونه نگرانی درباره محدود شدن توسعه مراکز داده یا کاهش بازدهی سرمایه‌گذاری‌های هوش مصنوعی می‌تواند چشم‌انداز درآمدی این شرکت‌ها را تحت تأثیر قرار دهد. از سوی دیگر، تردیدها درباره سودآوری سرمایه‌گذاری‌های سنگین در هوش مصنوعی از مدت‌ها قبل در بازار وجود داشت. مجموعه این عوامل در روز پنجشنبه موجی از فروش را در سهام شرکت‌های فناوری به راه انداخت. شاخص نزدک حدود ۵.۵ درصد افت کرد و سهام انویدیا و AMD نیز به ترتیب با کاهش ۹.۳ و ۱۷.۳ درصدی مواجه شدند. این موج فروش به بازار رمزارزها نیز سرایت کرد. با افزایش نگرانی‌ها درباره آینده سهام فناوری، سرمایه‌گذاران تمایل کمتری به نگهداری دارایی‌های پرریسک نشان دادند و بیت‌کوین نیز تحت تأثیر همین تغییر رفتار قرار گرفت. تا لطم بازار در نهایت به لیکوئید شدن گسترده موقعیت‌های معاملاتی اهرمی منجر شد. براساس داده‌های کوین گلس (CoinGlass)، بیش از ۵۰۰ میلیون دلار از موقعیت‌های معاملاتی بیت‌کوین در جریان این نوسانات بسته شدند. ابتدا رشد قیمت روز چهارشنبه به موقعیت‌های فروش آسیب زد و سپس سقوط روز پنجشنبه معامله‌گرانی را که روی افزایش قیمت شرط بسته بودند، با زیان مواجه کرد. این اتفاق بار دیگر ریسک استفاده از اهرم‌های معاملاتی بالا در شرایط بی‌ثبات بازار را نشان داد.

سقوط احساسات سرمایه‌گذاران به محدوده ترس

همزمان با افت قیمت بیت‌کوین، شاخص ترس و طمع نیز کاهش محسوسی را تجربه کرده است. این شاخص که در اواخر اکتبر در محدوده بالاتر از ۶۰ قرار داشت، پس از تحولات منفی بازار تا سطح ۲۵ پایین آمد؛ رقمی که بیانگر ورود بازار به محدوده «ترس شدید» و پایین‌ترین سطح این شاخص طی حدود سه ماه بود. هرچند آخرین داده‌های در دسترس از بهبود نسبی این معیار و قرار گرفتن آن در محدوده ۳۲ حکایت دارد، وضعیت کلی احساسات سرمایه‌گذاران همچنان در محدوده ترس قرار گرفته است. ماجرای هک بایننس، تحولات سیاسی امریکا و ریزش بازار سهام فناوری از جمله عواملی بودند که در روزهای اخیر بر نگرانی معامله‌گران افزودند. کاهش شاخص ترس و طمع در چنین شرایطی نشان می‌دهد سرمایه‌گذاران با احتیاط بیشتری به بازار نگاه می‌کنند و تمایل کمتری به پذیرش ریسک دارند.

رکود بی‌سابقه در صنعت استخراج بیت‌کوین

فشارهای بازار تنها به قیمت و رفتار سرمایه‌گذاران محدود نمانده و صنعت استخراج بیت‌کوین را نیز تحت تاثیر قرار داده است. سختی استخراج شبکه اکنون ۳۷۴ روز متوالی است که پایین‌تر از اوج تاریخی خود باقی مانده؛ دوره‌ای که طولانی‌ترین رکود سختی استخراج در تاریخ بیت‌کوین محسوب می‌شود. سختی استخراج در ۲۹ اکتبر ۲۰۲۵ به رکورد ۱۵۵.۹۷ تریلیون رسید، اما از آن زمان تاکنون نتوانسته به این سطح بازگردد. به این ترتیب، رکورد قبلی این شاخص که پس از بحران سال ۲۰۱۱ به مدت ۳۶۴ روز زیر اوج تاریخی باقی مانده بود نیز شکسته شده است. در بحران سال ۲۰۲۱ و پس از ممنوعیت استخراج در چین، سختی شبکه برای ۲۵۳ روز پایین‌تر از رکورد قبلی خود باقی ماند. با این حال، شرایط کنونی از نظر طول دوره رکود بی‌سابقه است. سرمایه‌گذاری در زیرساخت‌های هوش مصنوعی و مراکز داده از جمله مسیرهایی است که این شرکت‌ها برای جبران کاهش درآمدهای استخراج دنبال می‌کنند. ظرفیت زیرساختی و دسترسی به انرژی، امکان ورود بخشی از ماینرها به این بازار را فراهم کرده است؛ هرچند تغییر مدل کسب‌وکار نیز به سرمایه‌گذاری و هزینه‌های قابل توجهی نیاز دارد. با وجود رکود طولانی سختی استخراج، بازگشت نرخ هش شبکه به بالای یک زتاهش بر ثانیه نشان می‌دهد امنیت شبکه بیت‌کوین همچنان در سطح بالایی قرار دارد. بنابراین، افت سختی استخراج لزوماً به معنای تضعیف امنیت بلاک‌چین نیست، بلکه بیشتر از متوقف شدن روند رشد بی‌وقفه ظرفیت استخراج و تغییر شرایط اقتصادی فعالیت ماینرها حکایت دارد.

آیا افت قیمت بیت‌کوین عمیق‌تر می‌شود؟

مجموع تحولات اخیر نشان می‌دهد بیت‌کوین در شرایطی دشوار قرار گرفته است. از یک سو، خروج سرمایه از ETFهای اسپات، کاهش تمایل سرمایه‌گذاران نهادی و فشار ناشی از افت سهام فناوری، مانع شکل‌گیری یک روند صعودی پایدار شده است. از سوی دیگر، کاهش شاخص ترس و طمع و تداوم رکود در صنعت استخراج نیز از شکنندگی شرایط بازار حکایت دارند. از منظر تکنیکال، محدوده ۷۶ هزار دلار یکی از سطوح مهم پیش روی بیت‌کوین است. تثبیت قیمت بالاتر از این محدوده می‌تواند نخستین نشانه از بازگشت نسبی خریداران باشد؛ اما از دست رفتن حمایت‌های فعلی، احتمال حرکت قیمت به سمت محدوده ۶۷ هزار دلار را افزایش می‌دهد. در مقابل، بازپس‌گیری محدوده ۸۰ هزار دلار و تثبیت بالای آن می‌تواند بخشی از نگرانی‌های بازار را کاهش دهد. با این حال، تا زمانی که جریان خروج سرمایه از ETFها معکوس نشود و تقاضای خرید قدرت کافی پیدا نکند، نمی‌توان بازگشت قیمت را قطعی دانست. در مجموع، بیت‌کوین در شرایطی به استقبال هفته جدید می‌رود که هم بازار معاملات با فشار فروش مواجه است و هم صنعت استخراج طولانی‌ترین دوره رکود سختی شبکه را پشت‌سر می‌گذارد. تداوم این وضعیت می‌تواند مسیر بازیابی بزرگ‌ترین رمزارز جهان را دشوارتر کند و معامله‌گران را بیش از گذشته به مدیریت ریسک و پرهیز از موقعیت‌های اهرمی سنگین وادار سازد.

هوش مصنوعی در کمین زیرساخت‌های حیاتی

حملات خودکار کابوس دولت‌ها شد

مجموعه‌ای از رخدادهای امنیت سایبری در سال ۲۰۲۶ نشان می‌دهد که گسترش توانمندی‌های هوش مصنوعی در حال تغییر معادلات سنتی امنیت دیجیتال است. به گزارش مهر، کشف آسیب‌پذیری‌های گسترده در زیرساخت‌های نرم‌افزاری اینترنت، فعالیت خارج از کنترل عامل‌های هوش مصنوعی، افزایش حملات خودکار و اختلال در خدمات عمومی و مالی، دولت‌ها را با محیط تهدیدی مواجه کرده است که در آن سرعت شناسایی و بهره‌برداری از آسیب‌پذیری‌ها می‌تواند از ظرفیت واکنش سازمان‌های مسوول پیشی بگیرد. اهمیت این تحولات زمانی آشکارتر می‌شود که اختلال در یک مولفه نرم‌افزاری مشترک بتواند به‌صورت همزمان خدمات بانکی، حمل‌ونقل، مالیات و سامانه‌های دولتی چندین کشور را تحت تأثیر قرار دهد. بر همین اساس، در جولای ۲۰۲۶ وزارت تحول دیجیتال آلمان در واکنش به خروج یک عامل هوش مصنوعی شرکت اوپن‌ای‌آی از محیط کنترل‌شده آزمایشگاهی و حمله به زیرساخت‌های شرکت «HuggingFace»، این رخداد را نشانه «تغییر پارادایم» در توانمندی عامل‌های هوش مصنوعی توصیف کرد. اداره فدرال امنیت اطلاعات آلمان (BSI) نیز هشدار داد که افزایش سرعت توسعه مدل‌های پیشرفته می‌تواند ماهیت تهدیدات سایبری را به شکل بنیادین تغییر دهد. این ارزیابی از آن جهت اهمیت دارد که تهدید جدید صرفاً به استفاده مجرمان از ابزارهای هوشمند محدود نمی‌شود و رفتار پیش‌بینی‌نشده سامانه‌های خودمختار را نیز در برمی‌گیرد.

وقتی یک حفره نرم‌افزاری خدمات چند کشور را مختل می‌کند

یکی از برجسته‌ترین نمونه‌های این تحول، بحران امنیتی اکتبر ۲۰۲۶ در زبان برنامه‌نویسی «PHP» بود. در تاریخ ۲۱ اکتبر توسعه‌دهندگان این زبان برای آسیب‌پذیری‌هایی که سال‌ها در نرم‌افزار وجود داشتند و با استفاده از هوش مصنوعی شناسایی شده بودند، اصلاحیه‌های اضطراری منتشر کردند. با افشای اطلاعات آسیب‌پذیری‌ها، تلاش مهاجمان برای بهره‌برداری از آنها به سرعت افزایش یافت. مدیر عامل «Cloudflare» در واکنش به این رخداد اعلام کرد که تعداد تلاش‌های شناسایی‌شده از چند هزار مورد پیش از اعلام عمومی، به ده‌ها هزار مورد در ۴۵ دقیقه نخست و صدها هزار مورد طی دو ساعت رسید و سپس از مرز میلیون‌ها مورد تلاش عبور کرد. پیامد این رخداد به زیرساخت‌های فنی محدود نماند. موسسات مالی ژاپن، شرکت‌های هواپیمایی و راه‌آهن، سازمان‌های مالیاتی و برخی ارایه‌دهندگان خدمات عمومی در اروپا و آسیا ناچار شدند دسترسی به بخشی از سامانه‌های خود را موقتاً متوقف کنند. در فنلاند شرکت دولتی «Valtori» که مسوول خدمات فناوری اطلاعات دولت است، ضمن نصب وصله‌های امنیتی اعلام کرد که بازگرداندن کامل خدمات ممکن است چند روز یا حتی چند هفته زمان ببرد. نکته مهم آن است که این شرکت اختلالات خود را ناشی از اقدامات پیشگیرانه دانست و وقوع نفوذ موفق را تأیید نکرد. بنابراین بحران «PHP» نشان داد که حتی بدون اثبات نفوذ گسترده، آشکار شدن یک آسیب‌پذیری مشترک می‌تواند موجب اختلال فراگیر در ارایه خدمات دیجیتال شود. این رخداد وابستگی متقابل دستگاه‌های اجرایی به نرم‌افزارهای مشترک و زیرساخت‌های خارج از کنترل مستقیم دولت را آشکار ساخت. در چنین ساختاری امنیت هر خدمت عمومی تنها به سامانه همان دستگاه وابسته نیست و وضعیت امنیتی زنجیره‌ای از توسعه‌دهندگان، ارایه‌دهندگان خدمات ابری و پیمانکاران فناوری نیز در تداوم فعالیت آن نقش تعیین‌کننده دارد.

وقتی عامل‌های هوش مصنوعی از محدوده ماموریت خارج می‌شوند

دسته دیگری از رخدادهای اخیر به فعالیت پیش‌بینی نشده عامل‌های هوش مصنوعی مربوط می‌شود. برخلاف ابزارهای متعارف که اجرای عملیات آنها مستقیماً به دستورات مشخص کاربران وابسته است، عامل‌های خودمختار می‌توانند برای تحقق اهداف تعیین‌شده مجموعه‌ای از اقدامات متوالی را برنامه‌ریزی و اجرا کنند. این ویژگی ضمن افزایش بهره‌وری، مساله کنترل حدود اختیارات و رفتار سامانه را به یکی از چالش‌های امنیتی تبدیل کرده است. در اکتبر ۲۰۲۶ شبکه «ABC» استرالیا گزارش داد که یک عامل هوش مصنوعی اوپن‌ای‌آی در ماه ژوئن به یک برنامه تحت وب متعلق به سازمان پارک‌های ملی و حیات‌وحش ایالت نیوساوت‌ولز وارد شده است. این سامانه حاوی اطلاعات تاریخی و داده‌های مربوط به آتش‌سوزی در منطقه مذکور بود. شرکت اوپن‌ای‌آی تأیید کرد که مدل از حدود کاربرد مورد انتظار فراتر رفته است. با این حال بررسی‌های صورت گرفته دسترسی غیرمجاز به اطلاعات شخصی را نشان نداد. موضوع مهم دیگر فاصله زمانی میان وقوع رخداد و اطلاع‌رسانی حادثه به دولت بود که پرسش‌هایی درباره سازوکار شناسایی، گزارش‌دهی و مسوولیت ارایه‌دهندگان مدل‌های هوش مصنوعی ایجاد کرد. این مساله برای دولت‌ها واجد دو پیامد اساسی است. نخست آنکه سامانه‌های هوش مصنوعی ممکن است حتی بدون قصد مجرمانه توسعه‌دهندگان، رفتاری خارج از محدوده مجاز داشته باشند. دوم آنکه وابستگی دستگاه‌های عمومی به خدمات هوش مصنوعی شرکت‌های خصوصی می‌تواند کنترل دولت بر زمان کشف رخداد، دسترسی به شواهد فنی و ارزیابی پیامدهای امنیتی را محدود کند.

هوش مصنوعی چگونه مقیاس حملات سایبری را تغییر می‌دهد؟

افزایش قابلیت‌های هوش مصنوعی در شناسایی آسیب‌پذیری‌ها، تولید کد و اجرای زنجیره‌ای عملیات، هزینه و زمان مورد نیاز برای حملات سایبری را کاهش داده است. بر همین اساس، سامانه پایش رخدادهای هوش مصنوعی سازمان بین‌المللی توسعه و همکاری اقتصادی (OECD.AI) به مواردی از استفاده مجرمان سایبری از عامل‌های خودمختار برای نفوذ به وب‌سایت بیش از ۱۰۰ شرکت و حمله به بیش از ۴۰۰ بانک اشاره کرده است. گزارش سپتامبر ۲۰۲۶ تیم واکنش اضطراری رایانه‌ای اتحادیه اروپا (CERT-EU) نیز که بر بررسی ۳۵۸ گزارش منبع‌باز استوار است، از گسترش سرقت دسترسی به مدل‌های زبانی، سوءاستفاده از اعتبار خدمات هوش مصنوعی و فعالیت عامل‌های خودمختار در عملیات نفوذ خبر می‌دهد. این گزارش به رخدادی در اسپانیا اشاره می‌کند که طی آن یک عامل هوش مصنوعی در جریان فعالیت مهاجم، آسیب‌پذیری‌ها را شناسایی کرده، به سامانه‌ها وارد شده و در نهایت به اسناد مالی دسترسی یافته و داده‌های شخصی را تغییر داده است. چنین تحولاتی بیانگر آن است که مزیت زمانی مهاجمان می‌تواند افزایش یابد و الگوهای دفاعی مبتنی بر واکنش انسانی با محدودیت بیشتری مواجه شوند. در مقابل، استفاده از هوش مصنوعی برای کشف تهدیدات و ارزیابی مستمر آسیب‌پذیری‌ها نیز به یکی از محورهای تحول دفاع سایبری دولت‌ها تبدیل شده است.

از اختلال دیجیتال تا خسارت میلیاردی هزینه واقعی حملات سایبری

اختلالات سایبری اخیر نشان داده‌اند که هزینه حملات دیگر به بازیابی داده‌ها یا اصلاح سامانه‌های آسیب‌دیده محدود نیست. توقف خدمات، پرداخت خسارت، کاهش اعتماد مشتریان و افزایش هزینه‌های امنیتی می‌تواند پیامدهای اقتصادی گسترده‌تری ایجاد کند. خبرگزاری رویترز در ۲۶ اکتبر گزارش داد که شرکت ژاپنی «GMO Internet» پس از حمله به خدمات معاملات ارزی خود، پرداخت خسارت به مشتریان و پرداخت مبلغ ۵۰۰۰ ین به هر مشتری را اعلام کرد. ارزش سهام این شرکت نیز در یک روز نزدیک به ۱۶ درصد کاهش یافت. شرکت «Park۲۴» نیز پس از افشای اطلاعات شخصی مشتریان، پرداخت غرامت و ثبت زیان فوق‌العاده ۵.۵ میلیارد ینی را پیش‌بینی کرد. بر اساس داده‌های وبگاه «TrendAI» تا ۲۰ اکتبر ۲۰۲۶ تعداد ۷۲۳ رخداد امنیت سایبری در ژاپن ثبت شده بوده که از مجموع دو سال گذشته فراتر رفته است. همچنین، در بخش عمومی نیز حمله باج‌افزاری گروه «Rhysida» به شبکه اداری برلین نمونه‌ای از آسیب‌پذیری اطلاعات دولتی محسوب می‌شود. گزارش «CERT-EU» از سرقت حدود ۵.۷۹ ترابایت داده خبر داده است. دولت محلی برلین نیز تأیید کرده که بخش عمده خروج اطلاعات در فاصله ۷ تا ۱۲ آگوست رخ داده و داده‌های سرقت‌شده در سپتامبر منتشر شده‌اند.

دولت‌ها در برابر تهدیدات خودمختار ضرورت بازنگری در دفاع سایبری

تحولات اخیر ضرورت عبور از مدیریت منفرد امنیت سامانه‌ها به سمت حکمرانی یکپارچه تاب‌آوری دیجیتال را برجسته کرده است. تجربه اتحادیه اروپا در اجرای قانون تاب‌آوری عملیاتی دیجیتال (DORA) نمونه‌ای از این رویکرد است. مطابق نخستین گزارش سالانه نهادهای نظارتی مالی اروپا در ژوئن ۲۰۲۶، از مجموع ۳۳۸۳ رخداد عمده مرتبط با فناوری اطلاعات در بخش مالی، حدود یک‌سوم دارای آثار فرامرزی بوده‌اند. تنها ۱۰ درصد این رخدادها به امنیت سایبری مربوط بوده است و اختلالات سیستمی و رویدادهای خارجی سهم اصلی را داشته‌اند. این آمار مستقیماً بیانگر حملات مبتنی بر هوش مصنوعی نیست، اما میزان وابستگی متقابل خدمات مالی و ضرورت مدیریت مخاطرات تأمین‌کنندگان فناوری را نشان می‌دهد. در همین چارچوب، دولت ژاپن در اکتبر از برنامه تشکیل تیمی برای شبیه‌سازی حملات سایبری با استفاده از هوش مصنوعی و شناسایی ضعف سامانه‌ها خبر داد. این اقدام نیز بیانگر حرکت به سمت بهره‌گیری از همان فناوری‌هایی است که قابلیت‌های مهاجمان را تقویت کرده‌اند. بر آیند این تجربیات چهار ضرورت را برای سیاستگذاری امنیت سایبری برجسته می‌کند: توسعه ظرفیت شناسایی و پاسخ خودکار، ارزیابی امنیتی عامل‌های هوش مصنوعی پیش از استقرار، تقویت نظارت بر ارایه‌دهندگان خدمات فناوری و ایجاد سازوکارهای هماهنگ گزارش‌دهی رخدادها. رخدادهای سال ۲۰۲۶ نشان می‌دهند که هوش مصنوعی در حال تغییر سه مولفه اساسی امنیت سایبری، شامل سرعت شکل‌گیری تهدید، مقیاس انتشار اختلال و میزان کنترل انسانی بر رفتار سامانه‌هاست. بحران «PHP» وابستگی ساختاری خدمات عمومی به زیرساخت‌های نرم‌افزاری مشترک را آشکار کرد. همچنین فعالیت خارج از کنترل عامل‌های هوشمند نیز محدودیت‌های الگوهای متعارف نظارت بر سامانه‌های خودمختار را نشان داده است. در همین حال، حملات علیه شبکه‌های دولتی و موسسات مالی ابعاد اقتصادی و اداری نامنی دیجیتال را برجسته ساختند. نتیجه راهبردی این تحولات آن است که امنیت سایبری دیگر صرفاً وظیفه واحدهای فنی دستگاه‌های اجرایی نیست و به یکی از مولفه‌های اصلی ظرفیت حکمرانی دولت‌ها تبدیل شده است. در محیط جدید، توانایی حفظ استمرار خدمات عمومی، کنترل وابستگی‌های فناورانه و بازیابی سریع عملکرد زیرساخت‌ها می‌تواند به اندازه توانایی جلوگیری از نفوذ اهمیت داشته باشد. دولت‌هایی که بتوانند ظرفیت دفاع سایبری مبتنی بر هوش مصنوعی را با سازوکارهای موثر نظارت، پاسخگویی و مدیریت بحران تلفیق کنند، آمادگی بیشتری برای مواجهه با نسل جدید اختلالات دیجیتال خواهند داشت.

ژاپن به تدابیر اضطراری امنیت سایبری متوسل شد

ژاپن در واکنش به مجموعه‌ای از نقض‌های اطلاعاتی شخصی، روز جمعه، از اقدامات اضطراری امنیت سایبری، از جمله تشخیص تهدید مبتنی بر هوش مصنوعی و تیم‌های واکنش تخصصی، رونمایی کرد. به گزارش ایسنا، خبرگزاری کیودو نیوز گزارش کرد که هدف از این بسته که در جلسه‌ای به ریاست نخست‌وزیر سانائه تاکایچی تصویب شد، تقویت دفاع در برابر دسترسی غیرمجاز و بهبود پاسخ‌ها به حملات سایبری است. این اقدامات بر چهار حوزه بهبودهای امنیتی مبتنی بر هوش مصنوعی، جمع‌آوری اطلاعات پیشرفته، پاسخ‌های استراتژیک به حملات و کمک بیشتر به قربانیان تمرکز دارند. دولت ژاپن یک تیم «تیپ برتر» از متخصصان امنیت سایبری را برای مقابله با هکرها و استقرار هوش مصنوعی برای شناسایی آسیب‌پذیری‌ها در سیستم‌های رایانه‌ای ایجاد خواهد کرد. یک «تیم نجات» جداگانه متشکل از کارشناسان بخش دولتی و خصوصی به شرکت‌های آسیب‌دیده از حملات سایبری کمک خواهد کرد، در حالی که واحد دیگری به شرکت‌هایی که با تهدیدهای بالقوه روبه‌رو هستند، مشاوره خواهد داد. توکیو همچنین قابلیت‌های دفاع سایبری فعال خود را گسترش خواهد داد و به مقامات اجازه می‌دهد تا طبق قانونی که در ماه اکتبر به اجرا درآمد، به‌طور فعال به سرورهای مورد استفاده مهاجمان دسترسی پیدا کنند. دولت ۱۰ میلیارد ین (۶۳ میلیون دلار) از بودجه ذخیره مالی ۲۰۲۶ را برای تقویت امنیت سایبری، از جمله قابلیت‌های جمع‌آوری اطلاعات پلیس، اختصاص داده است.

هلندی‌ها در اعتراض به ساخت دیتاسنتر تظاهرات کردند

در آغاز اعتراضاتی دوروزه، در محل ساخت یک دیتاسنتر مایکروسافت در آمستردام تظاهراتی رخ داد. به گزارش مهر به نقل از رویترز، این رویداد بخشی از واکنش منفی شدید نسبت به گسترش سریع زیرساخت‌ها و ظرفیت پردازشی مورد نیاز برای هوش مصنوعی است. ائتلاف «دیتاسنترهای کثیف را متوقف کنید» اعلام کرد: گروه‌های کنشگر در ۱۶ کشور انجام اقداماتی اعتراضی در روزهای جمعه و شنبه انجام می‌دهند. این ائتلاف در تلاش است گروه‌های محیط‌زیستی و کارزارهای حامی حقوق دیجیتال را حول درخواست برای توقف موقت ساخت‌وسازهای گسترده مقیاس بسیج و متحد کند. بیش از ۱۰۰ کنشگر روز جمعه در محل ساخت دیتا سنتر هوش مصنوعی مایکروسافت در آمستردام تجمع کردند، آنها بازو در بازوی یکدیگر راهپیمایی کردند و سپس در حالی که پلیس در محل حضور داشت، وارد محل ساخت وساز شدند، از جرثقیل‌ها بالا رف