اخبار

نخستین شکایت ایالتی از اوپن‌ای‌آی برای هک‌های سریالی

راب بونتا، دادستان کل ایالت کالیفرنیا از اوپن‌ای‌آی شکایت و این شرکت را به توسعه محصولات خطرناک بدون اقدامات ایمنی کافی یا نظارت متهم کرده است. به گزارش مهر به نقل از رویترز، این شکایت پس از ثبت گزارش‌هایی درباره آنکه مدل‌های هوش مصنوعی به‌طور مستقل حملات سایبری انجام دادند، ثبت شده است. این نخستین شکایتی است که یک ایالت به دلیل حملات سایبری هوش مصنوعی ثبت کرده است. در این حملات که ماه جولای افشا شدند، عامل‌های هوش مصنوعی پیشرفته اوپن‌ای‌آی از محیط آزمایشی خارج شدند و استارت آپ هاگینگ فیس را هک کردند. شکایت مذکور در دادگاه سن فرانسیسکو ثبت شده و اوپن‌ای‌آی را به نقض قانون حفاظت از مصرف‌کنندگان و ایجاد هرج و مرج عمومی یا به خطر انداختن ایمنی متهم کرده است. بونتا در کنفرانس خبری مربوط به این اقدام گفت هدف از این شکایت آن است که شرکت با دستور دادگاه نقض قانون را متوقف کند، تضمین کند آزمایش و توسعه مدل‌های آن به‌طور ایمن انجام می‌شود و خسارت نقض قانون را بپردازد. شکایت مذکور همچنین شرکت را به گمراه کردن مصرف‌کنندگان درباره تلاش‌هایش برای آزمایش ایمنی مدل‌ها، نقض قانون حمایت از مصرف‌کنندگان ایالت و ایجاد اختلال در فعالیت سازمان‌ها و خدمات محلی که مانعی در استفاده ساکنان کالیفرنیا از املاک و دارایی‌هایشان شده، متهم کرده است. دادستان کل ایالت کالیفرنیا در بیانیه خود همچنین گفت: حمله به هاگینگ فیس نتیجه قابل پیش‌بینی یک فرهنگ داخلی در اوپن‌ای‌آی است که رشد و توسعه سریع مدل‌ها را بر ایمنی و مسوولیت‌پذیری ارجح می‌داند و این فقط یکی از ۸۰ رویداد شناسایی شده است.

باگی که مایکروسافت را شرمنده عالم کرد

باگی که هفته گذشته نرم‌افزار بهره‌وری مایکروسافت را فلج کرد و باعث اختلال گسترده در فعالیت مشتریان تجاری و دولتی آن در سراسر جهان شد، از جولای در مراکز داده این شرکت وجود داشت و شناسایی نشده بود. به گزارش ایسنا، هنگامی که این غول نرم‌افزاری، چهارشنبه گذشته ۱۱ نوامبر، مسیریابی مجدد ترافیک کاربران را انجام داد، سیستم دچار مشکل شد. سپس سرورهای حیاتی برای تیمز (Teams)، اوت‌لوک، دستیار هوش مصنوعی کوپایلوت (Copilot) و چندین سرویس دیگر شروع به از کار افتادن کردند و در نهایت، دسترسی کاربران در سراسر جهان را با اختلال روبه‌رو کرد. طبق گزارش اولیه‌ای که مایکروسافت در اواخر روز یکشنبه ۱۵ نوامبر ارایه کرد، در ۱۵ ساعت بعد از بروز این مشکل، در بحبوحه خرابی‌های پراکنده سرور، این سازنده نرم‌افزار تصور نمی‌کرد که مشکل بزرگ‌تری در حال شکل‌گیری است. سپس مایکروسافت ۱۵ ساعت دیگر را صرف شناسایی و عرضه یک ترمیم کرد. درست بعد از ساعت ۸ شب به وقت نیویورک در ۱۱ نوامبر، ترافیک از سرویس ویدیو کنفرانس و چت تیمز به‌طور خودکار به سیستم جداگانه سرورهایی که ترافیک اوت‌لوک را نیز مدیریت می‌کنند، تغییر مسیر داد. این وضعیت، همراه با از دست دادن ظرفیت سرور ناشی از یک مشکل نامربوط در اوایل هفته، باعث بروز این باگ شد و موجب شد حافظه سرورها پس از افزایش غیرمنتظره ترافیک، پر شود. سرورها کم‌کم از کار افتادند. این مشکل پس از آن بدتر شد که سیستم‌های خودکار، ایمیل‌ها و ترافیک کاربران را به سمت آنچه که سیستم مایکروسافت فکر می‌کرد سرورهای سالم و دیگری هستند، تغییر مسیر داد و باعث شد که باگ در آنجا نیز نمایان شود. در ساعت ۱۱ و ۳۰ صبح پنجشنبه ۱۲ نوامبر -درست زمانی که ترافیک کسب و کار در امریکا به اوج خود می‌رسید- مایکروسافت متوجه شد که مشکلی وجود دارد. پانزده ساعت دیگر زمان برد تا مایکروسافت، عیب‌یابی کرده و راه‌حلی برای رفع مشکل بیابد. در این بین، کار در بسیاری از مشتریان شرکتی و دولتی مایکروسافت متوقف شد، زیرا صندوق‌های دریافت ایمیل بارگیری نشدند، دعوت‌نامه‌های تیمز ناپدید شدند و کارمندان به تماس‌های تلفنی و قلم و کاغذ متوسل شدند. این قطعی مایه شرمسازی مایکروسافت و یادآور خطرات اتکای شدید به یک فروشنده فناوری بود. جدول زمانی جامع‌تر که در به‌روزرسانی برای تکنولوژیست‌هایی که از بسته نرم‌افزاری مایکروسافت ۳۶۵ استفاده می‌کنند گنجانده شده است، نشان می‌دهد که چگونه تلاش‌های خودکار این شرکت برای فعال نگه‌داشتن نرم‌افزارش، به شکست تصاعدی دامن زد. در بدترین مقطع این اختلال در ۱۲ نوامبر، بیش از ۸۰ درصد از سرورهای مربوط به اوت‌لوک، پاسخگو نبودند.

پلیس فتا از افزایش پرونده‌های کلاهبرداری رمزارزی خبر داد

از شناسایی ریسک‌ها تا صیانت از دارایی کاربران



افزایش فعالیت سکوهای تبادل رمزارز و تبدیل دارایی‌های دیجیتال به بخشی از سرمایه مردم، ضرورت نظارت بر امنیت سایبری این کسب‌وکارها را بیش از گذشته برجسته کرده است. در همین راستا، پلیس فتا از شناسایی ۱۴۰ سکوی فعال در این حوزه خبر داده و اعلام کرده است که ۳۰ سکوی مهم‌تر، براساس میزان فراگیری، حجم فعالیت و ملاحظات مالی، در اولویت ارزیابی‌های امنیتی قرار گرفته‌اند. همزمان، مرکز ملی فضای مجازی به این سکوها یک ماه فرصت داده تا سطح امنیت خود را ارتقا دهند و به رتبه مطلوب ارزیابی برسند.

پنجمین نشست رتبه‌بندی و ارزیابی خدمات‌دهندگان فضای مجازی با موضوع بررسی امنیت سایبری سکوهای تبادل رمزدارایی، روز گذشته با حضور سیدمحمدامین آقامیری، دبیر شورای عالی و رییس مرکز ملی فضای مجازی، سردار مجید، رییس پلیس فتا، علی حجت، رییس مرکز فرماندهی عملیات امنیت سایبری، محسن پاشا، معاون امنیت مرکز ملی فضای مجازی و جمعی از مدیران سکوهای رمزارزی برگزار شد. در این نشست، پلیس فتا به عنوان دستگاه هماهنگ‌کننده، گزارشی از وضعیت رتبه‌بندی ۱۵ سکوی سطح الف تبادل رمزدارایی، شاخص‌های مورد استفاده در ارزیابی و مهم‌ترین چالش‌های اجرایی این حوزه ارایه کرد. محور اصلی این ارزیابی‌ها سنجش میزان آمادگی سکوها در برابر تهدیدهای سایبری و شناسایی نقاط ضعف زیرساختی با هدف کاهش ریسک‌های احتمالی و حفاظت از دارایی کاربران عنوان شد. مدیران سکوهای رمزارزی نیز در این جلسه به بیان دیدگاه‌ها و مشکلات خود پرداختند. همکاری و هم‌افزایی میان دستگاه‌های مسوول و کسب‌وکارهای فعال در این حوزه، تأمین امنیت سرمایه مردم، دسترسی پایدار به شبکه ارتباطی، رفع مشکلات عملیاتی شرکت‌ها، بهبود زیرساخت‌ها و تسهیل فرآیندهای اجرایی از جمله موضوعاتی بود که در این گفت‌وگوها مطرح شد.

یک ماه فرصت برای ارتقای امنیت سکوها

سیدمحمدامین آقامیری، دبیر شورای عالی و رییس مرکز ملی فضای مجازی، در این نشست با تأکید بر نقش رتبه‌بندی امنیت سایبری در بهبود کیفیت خدمات فضای مجازی اظهار کرد: هدف از برگزاری این جلسات، کمک به ارایه خدمات پایدارتر و باکیفیت‌تر به مردم و کاهش ریسک‌های موجود در این حوزه است. شفافیت در ارزیابی‌ها می‌تواند به بهبود رقابت اقتصادی و انتخاب آگاهانه‌تر کاربران کمک کند، به گونه‌ای که مردم با شناخت بیشتری از سطح ریسک، خدمات مورد نیاز خود را انتخاب کنند. وی با بیان اینکه هدف اصلی این ارزیابی‌ها ارتقای سطح عملکرد تمام مجموعه‌هاست، افزود: انتظار این است که همه خدمات‌دهندگان به سطح مطلوب ارزیابی برسند و بتوانیم اعلام کنیم که فعالیت در این حوزه با ریسک کمتری همراه است و کاربران می‌توانند با اطمینان بیشتری از خدمات آنها استفاده کنند. رییس مرکز ملی فضای مجازی با اشاره به حملات سایبری علیه سکوهای رمزارزی در سطح جهان گفت: در بخش‌های مختلف با چنین مسائلی مواجه هستیم و مدتی است وضعیت داخلی و خارجی این حوزه را بررسی می‌کنیم. با وجود محدودیت‌ها و مشکلات موجود در زمینه زیرساخت، تجهیزات، سخت‌افزار و نرم‌افزار، نیروهای متخصص کشور توانمندی‌های قابل توجهی از خود نشان داده‌اند. نباید ظرفیت‌های داخلی را دست کم بگیریم؛ فعالیت مجموعه‌هایی که با همین امکانات توانسته‌اند زیرساخت‌های خود را حفظ کنند، ارزشمند است و باید با افتخار درباره آن صحبت کرد. آقامیری با اشاره به توافق بر سر شاخص‌های ارزیابی امنیت سایبری تصریح کرد: شاخص‌های تعیین‌شده مورد تأیید مجموعه‌های حاضر است و لازم است در یک ماه آینده تلاش شود سطح کیفی تمام سکوها ارتقا پیدا کند و به رتبه A برسند. رعایت حداقل الزامات امنیتی نیز ضروری است. برای سال آینده، شاخص‌ها را سخت‌گیرانه‌تر خواهیم کرد تا انگیزه بیشتری برای بهبود عملکرد و افزایش سطح امنیت ایجاد شود. وی در ادامه به برخی مشکلات کسب‌وکارهای فعال در حوزه رمزارز، از جمله مسائل مربوط به دامنه‌های اینترنتی اشاره کرد و گفت: پیشنهاد استفاده از دامنه‌های موضوعی یا داخلی برای جلوگیری از مصادره دامنه‌های دات کام، پیشنهاد درستی است. می‌توانیم با استعلام از دستگاه‌های مسوول، فرآیند استفاده از این دامنه‌ها را تسهیل کنیم. همچنین مجموعه‌هایی که با مشکلات عمومی و اجرایی مواجه هستند، باید گزارش دقیقی از مسائل خود تهیه کنند تا از طریق وزارت فرهنگ و ارشاد اسلامی یا بانک مرکزی و با دستور رییس جمهور، اقدامات لازم برای رفع آنها انجام شود. دبیر شورای عالی فضای مجازی با اشاره به موانع توسعه اقتصاد دیجیتال در کشور اظهار کرد: اقتصاد دیجیتال با دشواری‌هایی روبه‌رو است، زیرا در برخی بخش‌ها با مدل‌های سنتی اصطکاک دارد. با این حال، کسب‌وکارهای دیجیتال با ایجاد شفافیت و کاهش هزینه‌ها در حوزه‌هایی مانند بیمه، فروشگاه‌های اینترنتی، دارورسانی و رمزارزها، در حال ایجاد تحول هستند. این کسب‌وکارها علاوه بر ارایه خدمات جدید، امکان دسترسی گسترده‌تر به بازار، خدمات و آموزش را فراهم می‌کنند. آقامیری با اشاره به فعالیت شرکت‌های فین‌تک و کسب‌وکارهای نوآورانه ادامه داد: مجموعه‌هایی که در این مسیر فعالیت می‌کنند، در حال ایجاد فضایی تازه و پیشبرد شیوه‌های متفاوت کسب‌وکار هستند. طبیعتاً در برابر هر تحول جدیدی موافقان و مخالفانی وجود دارند، اما راه عبور از موانع، گفت‌وگو، همکاری و تعامل میان بخش‌های مختلف است. وی با تأکید بر وجود حمایت از نوآوری و تحول در سطوح بالای کشور گفت: تلاش می‌کنیم این اقدامات به نتیجه برسد و زمینه پیشرفت و توسعه نوآوری در کشور فراهم شود. انتظار داریم مجموعه‌های فعال در این حوزه طی یک ماه آینده برای ارتقای سطح ارزیابی خود تلاش کنند و در گزارش بعدی بتوانیم اعلام کنیم که همه آنها به رتبه A رسیده‌اند.

ضرورت نظارت پیشگیرانه بر امنیت سکوهای رمزارزی

در ادامه این نشست، سردار مجید، رییس پلیس فتا، با تأکید بر ضرورت نظارت مستمر بر امنیت زیرساخت‌های سکوهای اینترنتی اظهار کرد: پلیس فتا از سال ۱۳۹۶ و براساس ابلاغیه مرکز ملی فضای مجازی، موضوع امنیت سایبری زیرساخت‌ها را دنبال می‌کند. اقداماتی که در مرکز ملی فضای مجازی برای تأمین امنیت سکوهای اینترنتی انجام شده و توجه مستمر به این موضوع، قابل تقدیر است. وی رتبه‌بندی امنیت سایبری خدمات‌دهندگان فضای مجازی را اقدامی مهم در مسیر سنجش میزان آمادگی سکوها در برابر تهدیدهای احتمالی دانست و افزود: باتوجه به حساسیت این موضوع، لازم است سطح امنیت سکوها به‌صورت دقیق و قابل اندازه‌گیری ارزیابی شود. این طرح در چارچوب اسناد و الزامات ابلاغی مرکز ملی فضای مجازی دنبال می‌شود و می‌تواند در شناسایی نقاط ضعف و بهبود عملکرد خدمات‌دهندگان موثر باشد. رییس پلیس فتا با اشاره به گسترش فعالیت سکوهای تبادل رمزارز و افزایش سهم دارایی‌های رمزنگاری‌شده در سبد دارایی مردم تصریح کرد: مرکز ملی فضای مجازی از سال‌ها قبل به اهمیت این حوزه توجه داشته و در زمینه سیاست‌گذاری و تعیین چارچوب‌های قانونی آن پیشگام بوده است. با این حال، ماهیت فناوری و سرعت تحولات آن موجب شده در برخی بخش‌ها همچنان شکاف‌هایی در زمینه قانون‌گذاری، تعیین مسیر فعالیت و تنظیم‌گری وجود داشته باشد. به گفته وی، ضروری است فرآیند تنظیم‌گری سکوهای تبادل رمزارز با سرعت بیشتری دنبال شود تا فعالیت این کسب‌وکارها در چارچوب سیاست‌ها و ضوابط مشخص قرار گیرد و از بروز مشکلات و آسیب‌های احتمالی جلوگیری شود. سردار مجید همچنین با تشریح رویکرد پلیس فتا در مواجهه با تهدیدهای سایبری تأکید کرد: در برخورد با حوادث سایبری نباید صرفاً منتظر وقوع حادثه ماند و پس از آن برای رفع مشکل اقدام کرد. لازم است اقدامات پیشگیرانه، نظارت مستمر و ارزیابی‌های دوره‌ای پیش از وقوع حوادث نیز در دستور کار قرار گیرد تا نقاط آسیب‌پذیر شناسایی و برطرف شوند.

شناسایی ۱۴۰ سکوی رمزارزی و اولویت ارزیابی ۳۰ مجموعه

رییس پلیس فتا در بخش دیگری از سخنان خود از شناسایی ۱۴۰ سکو در حوزه تبادل رمزارز خبر داد و گفت: از میان این مجموعه‌ها، ۳۰ سکو به دلیل گستردگی فعالیت، میزان فراگیری و ملاحظات مالی، حساسیت و اهمیت بیشتری دارند و در اولویت ارزیابی‌های امنیتی قرار گرفته‌اند. وی درباره معیارهای این ارزیابی توضیح داد: شاخص‌های مورد استفاده براساس مدیریت امنیتی تجهیزات CIF و با بهره‌گیری از تجربیات عملیاتی و تخصصی بخش‌های مختلف تدوین شده‌اند. این شاخص‌ها موضوعاتی مانند اعمال تنظیمات امنیتی، امنیت شبکه و حفاظت از سیستم‌ها و اپلیکیشن‌ها را در بر می‌گیرند و امکان بررسی دقیق‌تر وضعیت امنیتی سکوها را فراهم می‌کنند. سردار مجید در ادامه با اشاره به افزایش پرونده‌های مرتبط با کلاهبرداری در حوزه رمزارز اظهار کرد: در سال ۱۳۹۹ و همزمان با ورود جدی‌تر پلیس فتا به این حوزه، حدود ۲۷۲ پرونده تشکیل شد. در این پرونده‌ها، شگردهایی مانند ایجاد کیف پول‌های جعلی، دریافت رمزارز از کاربران بدون تحویل دارایی وعده‌داده‌شده و سوءاستفاده از عنوان پشتیبانی سکوهای تبادل رمزارز برای فریب کاربران مشاهده می‌شد. وی با بیان اینکه میزان کلاهبرداری‌های مرتبط با رمزارز در سال‌های اخیر افزایش یافته است، افزود: شناسایی دقیق‌تر روش‌ها و الگوهای مجرمانه و استفاده از ظرفیت‌های تحلیلی و داده‌کاوی می‌تواند در پیشگیری از جرایم و افزایش امنیت دارایی‌های مردم نقش موثری داشته باشد. رییس پلیس فتا همچنین به مشکلات حقوقی رسیدگی به پرونده‌های مرتبط با رمزارز اشاره کرد و گفت: در سال‌های ابتدایی شکل‌گیری این جرایم، خلأهای قانونی در زمینه تعیین تکلیف دارایی‌های دیجیتال و مشخص نبودن مجازات برخی جرایم مرتبط با آنها، فرآیند رسیدگی قضایی را با دشواری‌هایی مواجه کرده بود. برای جلوگیری از تأثیر این خلأها بر روند رسیدگی به پرونده‌ها، هماهنگی‌هایی با مراجع قضایی انجام شده است تا پرونده‌های مرتبط با جرایم رمزارزی با موانع کمتری پیگیری شوند. در این نشست، نمایندگان سازمان نظام صنفی رایانه‌ای، انجمن فین‌تک و مدیران برخی سکوهای تبادل رمزارز نیز حضور داشتند. گفتنی است پیش از این نیز خدمات‌دهندگان پیامک‌های انبوه، بانک‌ها، دانشگاه‌ها و پایگاه‌های داده‌ملی از منظر امنیت سایبری مورد ارزیابی قرار گرفته بودند و به این مجموعه‌ها فرصت یک ماهه‌ای برای اصلاح و بهبود فرآیندهای امنیتی داده شده بود.

وقتی ربات‌ها اپراتور می‌شوند

با گسترش فناوری‌های هوش مصنوعی، نسل تازه‌ای از اپراتورها در راه ورود به دنیای خدمات دیجیتال هستند؛ اپراتورهایی که می‌توانند فراتر از پاسخگویی، بخشی از وظایف انسانی را بر عهده بگیرند. حالا با تصویب آیین‌نامه شکل‌گیری اپراتورهای هوش مصنوعی مسیر ورود این بازیگران جدید به اقتصاد دیجیتال وارد مرحله تازه‌ای شده، تحولی که می‌تواند از ارتباطات و کسب‌وکار تا پزشکی و آموزش را تحت تاثیر قرار دهد. به گزارش ایسنا، در سال‌های اخیر نوآوری‌ها و پیشرفت‌های زیادی در حوزه هوش مصنوعی به وجود آمده که در گذشته تنها در حوزه فیلم‌های علمی-تخیلی دیده می‌شد ولی کم کم به وسیله ربات‌های هوش مصنوعی به واقعیت تبدیل شد. یکی از ویژگی‌های قابل توجه هوش مصنوعی این است که می‌تواند با دریافت اطلاعات مختلف، الگوهای موجود در داده‌ها را تشخیص داده و از آنها برای داشتن عملکرد بهتر استفاده کند، به همین دلیل می‌توان گفت که هوش مصنوعی این پتانسیل را دارد که بسیاری از صنایع و کسب‌وکارها را متحول کند و سطح زندگی انسان‌ها را ارتقا دهد. امروز اپراتورهای هوش مصنوعی نقشی نوظهور و حیاتی در عصر دیجیتال دارند و با ترکیب مهارت‌های فنی و انسانی پلی میان انسان و ماشین ایجاد می‌کنند. همزمان با رشد فناوری و نیاز به تعامل هوشمند، اپراتورها می‌توانند آینده‌ای شفاف، سریع و انسانی‌تر برای هوش مصنوعی رقم بزنند و مدیریت، هدایت و نظارت بر سیستم‌های هوش مصنوعی را بر عهده بگیرند. شهریور ماه امسال، احسان چیت‌ساز، معاون سیاستگذاری و برنامه‌ریزی توسعه فاوا و اقتصاد دیجیتال وزارت ارتباطات، از تصویب و ابلاغ آیین‌نامه شکل‌گیری اپراتورهای هوش مصنوعی در هیات دولت خبر داد و اعلام کرد که چارچوب هوش مصنوعی تنظیم‌گری شده و به تایید کمیسیون تنظیم مقررات رسیده است و باتوجه به فراخوان داده شده اپراتورهای هوش مصنوعی شکل گرفته و تا ۱۸ ماه آینده در اختیار مجموعه محققین و کسب و کارهای حوزه اقتصاد دیجیتال قرار می‌گیرند. محمدحافظ حکمی، معاون نوآوری، فناوری و امور بین‌الملل وزارت ارتباطات اخیرا در یک گفت‌وگوی تلویزیونی از مشارکت بخش خصوصی در ماه‌های پیش رو در زمینه توسعه زیرساخت‌های هوش مصنوعی خبر داد و گفت: باتوجه به توان دانشگاه‌ها و نیروهای نخبه در سال‌های آینده شاهد انقلابی از خدمات هوشمندسازی مبتنی بر هوش مصنوعی در کشور خواهیم بود. به دنبال تصویب قانون توسعه هوش مصنوعی در مجلس و ابلاغ آن، مقرر شده سازمان هوش مصنوعی در کشور ایجاد شود. در همین راستا، وزارت ارتباطات به عنوان متولی شبکه زیرساختی و ارتباطی کشور اقدامات لازم را در این خصوص آغاز کرده و توسعه زیرساخت‌های هوش مصنوعی را در دستور کار قرار داده است. همچنین بسیاری از سکوها و پیام‌رسان‌های داخلی در حال ارایه خدمات هوش مصنوعی به کاربران هستند. معاونت علمی و فناوری ریاست جمهوری نیز در بحث معافیت‌های مالیاتی در حوزه سرمایه‌گذاری در زیرساخت‌های هوش مصنوعی وارد عمل شده است. اپراتورهای هوش مصنوعی، نسل جدیدی از سیستم‌های هوشمند هستند که می‌توانند مثل یک اپراتور انسانی درخواست‌ها را درک و اطلاعات مورد نیاز را جمع‌آوری کنند و با نرم‌افزارهای سازمانی ارتباط برقرار کنند. برای مثال، یک اپراتور فروش هوشمند می‌تواند نیاز مشتری را بررسی کند، محصول مناسب را پیشنهاد دهد و فرآیند فروش را آغاز کند. طی هفته‌های اخیر سازمان فناوری اطلاعات برای ایجاد زیرساخت‌های هوش مصنوعی در کشور فراخوان داده تا شرکت‌هایی که توانایی و قابلیت لازم را داشته باشند در این زمینه مشارکت کنند، چنانچه محمدمحسن صدر، رییس سازمان فناوری اطلاعات در گفت‌وگو با ایسنا، اعلام کرد که سه شرکت که از شرایط لازم برخوردار بودند در فراخوان پذیرفته شدند و از آنجا مسوول نهایی صدور پروانه با سازمان تنظیم مقررات و ارتباطات رادیویی است، این سه شرکت به رگولاتوری معرفی شده‌اند تا موافقت اصولی اولیه را صادر کنند. به گفته وی، این شرکت‌ها مراحل نهایی صدور پروانه را طی می‌کنند و اگر مستندات مالی و ضمانت‌نامه‌هایی که باید به دولت بسپارند، ارایه شود، موافقت اصولی آنها آماده خواهد شد. به اعتقاد کارشناسان یکی از مهم‌ترین کارکردهای اپراتورهای هوش مصنوعی این است که در تامین زیرساخت‌های پردازشی و پشتیبانی از فعالیت‌های مرتبط با هوش مصنوعی عمل می‌کنند و ارایه خدمات مربوط به داده‌ها از بسترهای پیش‌بینی شده برای فعالیت این اپراتورهاست.

شناسه آگهی: ۲۳۱۷۰۵۷
اداره کل ثبت اسناد و املاک استان بوشهر
اداره ثبت اسناد و املاک حوزه ثبت ملک برازجان
هیات موضوع قانون تعیین تکلیف وضعیت ثبتی اراضی و ساختمانهای فاقد سند رسمی

آگهی موضوع ماده ۳ قانون و ماده ۱۳ آئین نامه قانون تعیین تکلیف وضعیت ثبتی و اراضی و ساختمانهای فاقد سند رسمی

برابر رای شماره ۱۴۰۵۶۰۳۲۴۰۰۲۰۰۶۷۰۷ هیات اول موضوع قانون تعیین تکلیف وضعیت ثبتی اراضی و ساختمانهای فاقد سند رسمی مستقر در واحد ثبتی حوزه ثبت ملک برازجان تصرفات مالکانه بلامعارض متقاضی آقای سعید خیری فرزند بزرگ بشماره شناسنامه ۷۴۷۸ صادره از دشتستان در ششدانگ یک قطعه زمین مزروعی به مساحت ۱۶۱۰.۱۴ مترمربع قسمتی از پلاک فرعی از ۷۴۸۹ اصلی واقع در اراضی روستای آبطویل خریداری از مالک رسمی محرز گردیده است. لذا به منظور اطلاع عموم مراتب در دو نوبت به فاصله ۱۵ روز آگهی می‌شود در صورتی که اشخاص نسبت به صدور سند مالکیت متقاضی اعتراضی داشته باشند می‌توانند از تاریخ انتشار اولین آگهی به مدت دو ماه اعتراض خود را به این اداره تسلیم و پس از اخذ رسید، ظرف مدت یک ماه از تاریخ تسلیم اعتراض، دادخواست خود را به مراجع قضایی تقدیم نمایند. بدیهی است در صورت انقضای مدت مذکور و عدم وصول اعتراض طبق مقررات سند مالکیت صادر خواهد شد.
تاریخ انتشار نوبت اول: ۱۴۰۵/۰۸/۱۲
تاریخ انتشار نوبت دوم: ۱۴۰۵/۰۸/۲۷
حمیدرضا باقرپور
رییس واحد ثبتی حوزه ثبت ملک برازجان

شناسه آگهی: ۲۳۱۷۰۵۶
اداره کل ثبت اسناد و املاک استان بوشهر
اداره ثبت اسناد و املاک حوزه ثبت ملک برازجان
هیات موضوع قانون تعیین تکلیف وضعیت ثبتی اراضی و ساختمانهای فاقد سند رسمی

آگهی موضوع ماده ۳ قانون و ماده ۱۳ آئین نامه قانون تعیین تکلیف وضعیت ثبتی و اراضی و ساختمانهای فاقد سند رسمی

برابر رای شماره ۱۴۰۵۶۰۳۲۴۰۰۲۰۰۶۸۵۶ هیات اول موضوع قانون تعیین تکلیف وضعیت ثبتی اراضی و ساختمانهای فاقد سند رسمی مستقر در واحد ثبتی حوزه ثبت ملک برازجان تصرفات مالکانه بلامعارض متقاضی خانم مریم حلقه سیمین فرزند اکبر بشماره شناسنامه ۳۵۱۰۴۲۵۲۴۳ صادره از دشتستان در ششدانگ یکباب ساختمان به مساحت ۱۳۰.۲۸ مترمربع قسمتی از پلاک فرعی از ۱۹۸۰ اصلی واقع در شهر برازجان خریداری از مالک رسمی محرز گردیده است. لذا به منظور اطلاع عموم مراتب در دو نوبت به فاصله ۱۵ روز آگهی می‌شود در صورتی که اشخاص نسبت به صدور سند مالکیت متقاضی اعتراضی داشته باشند می‌توانند از تاریخ انتشار اولین آگهی به مدت دو ماه اعتراض خود را به این اداره تسلیم و پس از اخذ رسید، ظرف مدت یک ماه از تاریخ تسلیم اعتراض، دادخواست خود را به مراجع قضایی تقدیم نمایند. بدیهی است در صورت انقضای مدت مذکور و عدم وصول اعتراض طبق مقررات سند مالکیت صادر خواهد شد.
تاریخ انتشار نوبت اول: ۱۴۰۵/۰۸/۱۲
تاریخ انتشار نوبت دوم: ۱۴۰۵/۰۸/۲۷
حمیدرضا باقرپور
رییس واحد ثبتی حوزه ثبت ملک برازجان

هوشمندسازی خدمات دانشگاهی و استقرار حکمرانی داده‌محور در وزارت علوم

مدیر کل فناوری اطلاعات و هوشمندسازی وزارت علوم، تحقیقات و فناوری گفت: هوشمندسازی خدمات و استقرار حکمرانی داده‌محور از اولویت‌های وزارت علوم در سال ۱۴۰۵ است. محمدهادی زاهدی در گفت‌وگو با مهر با اشاره به اولویت‌های این وزارتخانه، استقرار نظام حکمرانی داده‌محور و تحقق آموزش عالی هوشمند را از مهم‌ترین برنامه‌های وزارت علوم عنوان کرد. وی اظهار کرد: یکی از موضوعاتی که طی یک سال گذشته در وزارت علوم در اولویت قرار گرفته، بحث استقرار نظام حکمرانی داده‌محور و تحقق آموزش عالی هوشمند است. مدیر کل فناوری اطلاعات و هوشمندسازی وزارت علوم با تأکید بر ضرورت توجه روسای دانشگاه‌ها به موضوع حکمرانی داده، افزود: انتظار ما از دانشگاه‌ها، به‌ویژه روسای دانشگاه‌ها، این است که حکمرانی داده را صرفاً یک موضوع مرتبط با فناوری اطلاعات ندانند، چراکه حکمرانی داده‌محور، موضوعی در سطح کلان مدیریتی و حکمرانی دانشگاه است و باید در بالاترین سطوح دانشگاه مورد توجه قرار گیرد. زاهدی با اشاره به برنامه‌های وزارت علوم برای سال ۱۴۰۵ گفت: یکی از اولویت‌های این وزارتخانه در سال جاری، هوشمندسازی خدمات است که هدف آن ارایه خدمات شفاف، سریع و تسهیل امور جامعه ذی‌نفعان دانشگاه‌هاست. وی ادامه داد: از همه مسوولان دانشگاه‌ها، از روسای دانشگاه‌ها گرفته تا حوزه‌های تحول و فناوری اطلاعات، انتظار داریم توجه ویژه‌ای به موضوع داده داشته باشند و در زمینه جمع‌آوری داده‌های برخط، اشتراک‌گذاری و به‌روزرسانی اطلاعات، همکاری و تعامل لازم را با مجموعه ستاد وزارت علوم انجام دهند. وی تأکید کرد: همکاری دانشگاه‌ها در این زمینه موجب می‌شود تصمیم‌گیری‌ها بر اساس اطلاعات دقیق، به‌روز و قابل اتکا انجام شود و تصمیم‌های اتخاذشده نه تنها زمینه‌ساز ایجاد چالش نباشند، بلکه به پیش‌بینی مسائل و یافتن راهکارهایی برای حل چالش‌های آموزش عالی کمک کنند.

دنیای فناوری

دایرکت اینستاگرام یک اپ جداگانه می‌شود

متا مشغول توسعه یک اپ پیام‌رسان جداگانه برای اینستاگرام است که احتمالا گستره پیام‌های مستقیم آن (دایرکت مسیج) را بیشتر می‌کند. به گزارش مهر به نقل از انگجت، این شرکت همچنین آزمایش «دایرکت»، اپ جداگانه‌ای که اینباکس اینستاگرام را به شکل یک برنامه جداگانه ارایه می‌کند اما نیازمند حساب کاربری در این شبکه اجتماعی نیست را آغاز می‌کند. متا در به‌روزرسانی جدید اعلام کرد هم‌اکنون «دایرکت» فقط در تایلند و ترکیه ارایه شده است. ظاهر این اپ در نگاه نخست شباهت زیادی به اینباکس اینستاگرام دارد. همچنین اپ مذکور ساختار تقریبا یکسانی دارد به‌طوری که اگر فرد با اطلاعات حساب اینستاگرام خود وارد شود، چت‌ها را از اپ اصلی نمایش می‌دهد. دایرکت همچنین همان ویژگی‌های شخصی‌سازی شده اینستاگرام مانند قابلیت تنظیم پس زمینه مخصوص برای تردهای جداگانه و ویژگی آپدیت استاتوس را دارد. هرچند کاربران اینستاگرام می‌توانند با استفاده از اطلاعات حساب‌های کاربری فعلی خود وارد دایرکت شوند اما این اپ در واقع نیازمند اطلاعات ورود اینستاگرام نیست. کاربران می‌توانند به‌طور مستقیم و از طریق آدرس ایمیل یا شماره موبایل نیز در اپ دایرکت وارد شوند و همچنین به دوستانشان پیام دهند. البته به نظر می‌رسد ارسال پیام بدون اتصال اپ به حساب کاربری اینستاگرام چندان راحت نباشد. متا عنوان کرده کاربرانی که بدون اطلاعات ورود اینستاگرام وارد این اپ می‌شوند باید مخاطبان را از طریق نام کاربری‌شان در اینستاگرام یا کد QR وارد کنند تا بتوانند با آنها ارتباط برقرار کنند. شرکت مادر اینستاگرام اعلام کرده برخی از ویژگی‌های ایمنی این اپ را به دایرکت نیز آورده است. اپ مذکور به افراد اجازه نمی‌دهد بدون حساب کاربری که از قبل به مخاطبانشان متصل نیست، چت را آغاز کنند. همچنین والدین می‌توانند از طریق ویژگی‌های مخصوص کنترل والدین، افرادی که با فرزند نوجوانشان چت می‌کنند و مدت زمانی که آنها در اپ می‌گذرانند را رصد کنند. در کنار این موارد متا مدعی است از فناوری برای ردیابی و مقابله با تعاملات احتمالا نامناسب با کاربران جوان استفاده می‌کند اما درباره ماهیت دقیق این فناوری توضیحی نداده است.

نسخه جدید iOS فیس آی‌دی را به آیفون دوئو می‌آورد

به نظر می‌رسد اپل راه‌حلی برای باز کردن قفل آیفون دوئو با فیس آی‌دی یافته است. به گزارش مهر به نقل از انگجت، فقدان «فیس آی‌دی» یکی از گله‌های اصلی کاربران درباره آیفون دوئو است. اکنون شایعات نشان می‌دهد این شرکت احتمالا قابلیت True Depth دوربین را در دومین نسل آیفون تاشو در سال آینده استفاده کند. اکنون به نظر می‌رسد اپل راه‌حلی سریع‌تر برای برطرف کردن این شکایات پیدا کرده است. دومین نسخه بتا iOS۲۷.۳ برای توسعه‌دهندگان یک آپشن تازه برای باز کردن آیفون دوئو با قابلیت شناسایی چهره با کمک دوربین سلفی ارایه کرده است. قابلیت مذکور «باز کردن قفل با دوربین جلویی» نامیده می‌شود و می‌توان آن را از طریق بخش Touch ID&Passcode در بخش تنظیمات فعال کرد. وب‌سایت خبری انگجت فعال شدن این ویژگی روی یک آیفون دوئو با نسخه بتا مذکور را تایید می‌کند اما نحوه عملکرد آن عجیب است. دوئو برخلاف آیفون‌های مدرن دوربین True Depth با حسگرهای عمیق که فیس آی‌دی برای نقشه‌بندی سه‌بعدی صورت استفاده می‌کند را ندارد. در عوض دوربین‌های معمولی در نمایشگرهای داخلی و خارجی دستگاه به کار رفته‌اند که احتمالا به همین دلیل دستگاه برای باز شدن به تاچ‌آی‌دی متکی است. ویژگی جدید که در نسخه بتا iOS۲۷.۳ ارایه شده این امر را شفاف نشان می‌دهد. در صفحه راه‌اندازی این قابلیت به کاربران هشدار داده می‌شود که این ویژگی استفاده را آسان‌تر می‌کند، اما به اندازه تاچ‌آی یا فیس آی‌دی امن نیست. هنوز برای اظهار نظر قطعی زود است، اما آزمایش‌های این وب‌سایت نشان می‌دهد که این قابلیت عملکرد نسبتا قابل قبولی دارد. این ویژگی سریع‌تر از تاچ‌آی‌دی قفل گوشی را باز می‌کند و نتوانسته است با نشان دادن عکس چهره کاربر به دوربین، فریب بخورد. همچنین به نظر می‌رسد این قابلیت در شرایطی با نور کم نیز کار می‌کند، هرچند در تاریکی مطلق عملکردی ندارد. البته اپل باید محدودیت‌هایی وضع کند تا مجرمان نتوانند از این ویژگی برای دستکاری آیفون‌های افراد بدون رضایت شان سواستفاده کنند. قابلیت مذکور فقط با دور زدن قفل صفحه کار می‌کند و فرد نمی‌تواند قفل اپ‌ها را باز کند، رمز وی را نشان دهد از اپل پی با صورت فرد استفاده کند. ویژگی تاچ‌آی‌دی همچنان برای انجام فعالیت‌های حساس‌تر مورد نیاز است. عدم استفاده از موبایل به مدت بیش از ۴۵ دقیقه نیز به‌طور موقت باز کردن قفل دستگاه با دوربین سلفی را غیرفعال می‌کند.

وب‌سایت‌ها برای سرقت رمزارز از کاربران آیفون آلوده شدند

یک محقق امنیتی روز دوشنبه ۱۶ نوامبر مدعی شد که برخی از پربازدیدترین وب‌سایت‌های جهان، از جمله وب‌سایت‌های سلزفورس، سی‌ان‌ان، اکوئیفکس، اچ‌اس‌بی‌سی، زوم و ایکیا برای سرقت رمزارزها از کاربران گوشی‌های آیفون، به کد مخرب آلوده شده‌اند. به گزارش ایسنا، اسکات هلم، محقق امنیتی گفت: جاوا اسکریپت مخرب، بازدیدکنندگان وب‌سایت‌های ۱۷۸ سازمان در بخش‌های مختلف را از طریق پلت‌فرم بهینه‌سازی وب‌سایت Optimizely، هدف قرار گرفت. این اسکریپت‌ها آدرس‌های پرداخت رمزارزها را با کیف پول مهاجم جایگزین کرده، شماره کارت‌ها را هنگامی که کاربران جزییات کارت اعتباری را وارد می‌کردند، کپی کرده و کوکی‌ها و اسکرین‌شات‌ها را به سرقت برده و کد سوءاستفاده را در دستگاه‌های iOS قرار می‌دهند. شرکت امنیت سایبری «هودسون راک» (HudsonRock) همچنین اعلام کرد شواهدی پیدا کرده است که نشان می‌دهد این وب‌سایت‌ها، کد مخربی را برای بازدیدکنندگان خود توزیع کرده‌اند. طبق گزارش رویترز، اینکه این کد در هر مورد با موفقیت استفاده شده است یا گستردگی هک‌های حاصل از این شیوه فعلا مشخص نیست. شرکت سلزفورس اعلام کرد که در حال بررسی تغییرات غیرمجاز اسکریپت Optimizely بوده و برای احتیاط آنها را غیرفعال کرده است. اکوئیفکس نیز این مشکل را بررسی و استفاده از Optimizely را متوقف کرد. این شرکت اعلام کرد که شواهدی دال بر هرگونه آلودگی در سیستم‌های خود پیدا نکرده است.