رویداد

دستورالعمل جدید برای اینترنت موبایل

● **مهر:** معاون سازمان تنظیم مقررات ارتباطات از پیگیری برای تدوین دستورالعملی جدید در بخش اینترنت موبایل خبر داد. صادق عباسی‌شاهکوه با اعلام این خبر گفت: براساس آن، اپراتورها ملزم خواهند شد مصرف دیتای آزاد و پایان بسته اینترنت مشترکان را اعلام کنند. او ادامه داد: در حال پیگیری برای تدوین دستورالعملی جدید هستیم که براساس آن، آیین‌نامه‌ای تدوین شود تا اپراتورها ملزم شوند مصرف دیتای آزاد و پایان بسته اینترنت مشترکان را اعلام کنند. او افزود: بسیاری از کاربران و مشترکان موبایل از این موضوع اظهار نارضایتی کرده‌اند که به دلیل اطلاع‌رسانی‌نکردن اپراتورها برای پایان بسته‌های تخفیفی اینترنت، دچار ضرر و زیان بسیاری شده‌اند. او گفت: تعرفه مصرف آزاد اینترنت با نرخ بسته‌های اینترنتی، بسیار متفاوت است و عدم اعلام پایان بسته از سوی برخی اپراتورها سبب شده نرخ اینترنت از شارژ مشترک کم شود یا در پایان ماه در صورت‌حساب دوره‌ای مشترک، ارقام بالایی از اینترنت مصرف آزاد محاسبه شود. به گفته او، تاکنون دستورالعمل الزامی برای اپراتورها در زمینه اعلام پایان مصرف بسته‌های اینترنتی نداشته‌ایم. او گفت: بیشترین اعتراضات مطرح‌شده از سوی مشترکان مربوط به دو اپراتور ایرانسل و رایتل در این زمینه بوده است.

درخواست دریافت رنج جدید شماره

● **ایسنا:** معاون بازاریابی شرکت ارتباطات سیار ایران از درخواست این شرکت برای دریافت رنج جدید شماره خبر داد. محمدمهدی عطوفی با اعلام این خبر گفت: مدتی است درخواست رنج جدید شماره را به سازمان تنظیم مقررات ارتباطات ارسال کرده‌ایم و منتظریم در این زمینه تصمیم‌گیری شود. او درباره اینکه اکنون عدم ارائه سیم‌کارت با کدهای قدیمی در بازار موجب شده سیم‌کارت‌های قدیمی ازجمله کد یک به قیمتی بالغ بر ۱۰ برابر سیم‌کارت‌های کد جدید به فروش برسد، بیان کرد: به‌هرحال، در هرجامعه‌ای برخی اجناس دارای نوعی مطلوبیت هستند که ما نمی‌توانیم این مطلوبیت را از بین ببریم، چراکه در این زمینه مردم هستند که تصمیم می‌گیرند. او افزود: از نظر ما خدماتی که در هردو سیم‌کارت ارائه می‌شود، یکسان است، اما درنهایت، مردم هستند که برای خرید سیم‌کارت تصمیم می‌گیرند و دراین‌میان عده‌ای دوست دارند سیم‌کارت‌هایی با کدهای قدیمی‌تر یا شماره‌هایی که مناسباتی خاص را به ذهن آنها می‌رساند، خریداری کنند که این موضوع نیز جزئی از مناسبات بازار است.

برگزاری روز جهانی دختران و فناوری اطلاعات

● **شرق:** سازمان نظام صنفی رایانه‌ای تهران با همکاری دانشکده فنی‌وحرفه‌ای دکتر شریعتی، کمیته زنان در مهندسی IEEE بخش ایران و انجمن ملی زنان کارآفرین، برای اولین‌بار در ایران مراسم روز جهانی «دختران و فناوری اطلاعات و ارتباطات» را در کشور برگزار می‌کند. فریبا مهدیون، عضو هیأت‌مدیره سازمان نظام صنفی رایانه‌ای تهران و مدیر اجرایی مراسم روز جهانی دختران و ارتباطات و فناوری اطلاعات بیان کرد: با توجه به اهمیت نقش فناوری‌های ارتباطی و اطلاعاتی در تمام عرصه‌های زندگی و افزایش تخصص زنان در حوزه ارتباطات و فناوری اطلاعات به‌عنوان نیمی از جمعیت جهان، اتحادیه بین‌المللی مخابرات (ITU) به عنوان نهاد تخصصی سازمان‌ملل‌متحد در حوزه مخابرات و ارتباطات و فناوری اطلاعات، روز ۲۳ آوریل (سوم اردیبهشت) را به‌عنوان «روزجهانی دختران و فناوری اطلاعات و ارتباطات» نام‌گذاری کرده است.

بیومتریک جایگزین رمز عبور

نهال شیوا: با عرضه تلفن‌های هوشمند آیفون S5 اپل به بازار، کمتر کسی متوجه ورود بی‌سروصدای بشر به عصر بیومتریک شد. اپل با خرید شرکت AuthenTec در سال ۲۰۱۲ به این فناوری دست یافت. ازسوی‌دیگر نیز سامسونگ در اقدامی رقابتی، نسخه‌های خود را از این فناوری در گوشی‌های گلکسی S5 و گوشی‌های S6 که به‌زودی به بازار ارائه می‌شود، روانه بازار کرد.

شرکت مخابراتی Qualcomm نیز متعهد شده است به‌زودی حسگرهای سه‌بُعدی اثرانگشت را در محصولات خود تعبیه کند. با این روند، به‌نظر می‌رسد این فناوری در گوشی‌های هوشمند، در دو سال آینده، به‌طور فزاینده‌ای استانداردتر شود.

بانک‌های RBS و NatWest به‌تازگی اعلام کرده‌اند مشتریانشان به‌زودی می‌توانند از طریق Touch ID (احراز هویت از طریق لمس اثرانگشت) کارهای بانکی خود را انجام دهند. اما «جان کریسلر»، هکر آلمانی با نام مستعار «استارباگ» تسلیم این فناوری‌ها نشده است. او فقط چندروز پس از عرضه اپل به بازار، Touch ID آن را هک کرد و این کار را فقط با استفاده از کیتی که شامل یک اسکنر، یک پرینتر و اندکی چسب و اسکن تکرار آخرین اثر انگشتی که صفحه شیشه‌ای آیفون را لمس کرده بود، انجام داد. او سپس در ماه سپتامبر با استفاده از عکس‌های وزیر دفاع آلمان که در یک نشست خبری از فاصله سه متری گرفته شده بود، اثر انگشت این وزیر را بازآفرینی کرد. استارباگ معتقد است حفاظت مناسب، نیازمند یک احراز هویت دوعاملی است که براساس دو مؤلفه کاملا مستقل از یکی از سه روش: رمز عبور- اطلاعاتی، کارت‌های هوشمند شخصی و ویژگی‌های بیومتریک تعریف شده باشد.

این امنیت بر پایه آن اطلاعاتی که می‌دانید آنچه دارید و آنچه هستید، برقرار می‌شود. این هکر می‌گوید: دو روش از این سه روش می‌توانند یکدیگر را همپوشانی کنند، به‌طوری‌که می‌توان اطلاعات محرمانه یک روش روی دستگاه را از طریق روش دوم کشف کرد؛ مثلا اگر بتوانید از روی اثر انگشتی که روی تلفن جا مانده، یک انگشت جعلی بسازید این دو عامل در واقع به اندازه یک عامل ارزش دارند. آسیب‌پذیری در تشخیص اثر انگشت، موضوع محرمانه‌ای نیست و همین امر، موجب شده محققان به تلاش و رقابت برای یافتن یک جایگزین بیومتریک برای آن ادامه دهند. این امر با حسگرهایی که به‌وفور و ارزان تولید می‌شوند، تسریع شده است و اغلب، شاهد تولید نرم‌افزارهایی هستیم که شرکت‌های جنوب‌شرق آسیا با تکیه بر فناوری خدمات ابری عرضه می‌کنند. بارکلی، امسال احراز هویت رگ انگشت دست را برای مشتریان انگلیسی خود ارائه می‌کند. این فناوری را شرکت ژاپنی هیتاچی تولید کرده و در دستگاه‌های خودپرداز ژاپن و لهستان از آن استفاده می‌شود.

متخصصان هیتاچی می‌گویند الگوی عروق در زمان جنینی شکل می‌گیرد و در سراسر عمر، ثابت می‌ماند. وقتی نور فروسرخ از انگشت می‌گذرد، بخشی از آن جذب هموگلوبین رگ‌ها می‌شود. ازاین‌رو اسکنر احراز هویت رگ هیتاچی می‌تواند هویت فرد را از طریق بررسی الگوی رگ تصدیق کند.

«استالر» استارت‌آپ انگلیسی با هیتاچی و BT روی راهکار پرداخت با اثر انگشت کار می‌کند و این کار را در چندین جشنواره موسیقی آزمایش کرده است. آنها نام این نوع پرداخت را «پرداخت انگشتی» (FingoPay) گذاشته‌اند. در این روش، کاربر انگشت را روی اسکنر قرار داده و چند رقم آخر کارت اعتباری خود را به فروشنده می‌گوید و به‌همین‌سادگی پرداخت به صورت زمان واقعی انجام می‌شود. روش‌های بیومتریک بسیار متنوعی به بازار عرضه شده‌اند که ازآن‌جمله می‌توان به Nymi اشاره کرد. این فناوری که توسط شرکت کانادایی «بیونیم» عرضه شده، دستبندی است که هویت کاربر را بر اساس پالس‌های الکتریکی ضربان قلب که کاملا منحصربه‌فرد است- تعیین می‌کند.

شرکت آلمانی Cognitec نیز پس از تمرکز اولیه بر فناوری اثر انگشت، اکنون روی تشخیص چهره کار می‌کند. مقامات این شرکت می‌گویند دراین‌زمینه قراردادی را با پلیس مرزی آلمان منعقد کرده‌اند. شرکت آمریکایی EyeLock در حال تولید اسکنرهای تجاری عنبیه موسوم به Myris است. این شرکت مدعی است که فقط «دی‌ان‌ای» احراز هویت دقیق‌تری از فرد ارائه می‌دهد. اما آنهایی که در زمینه فناوری‌های مالی کار می‌کنند معتقدند استفاده از چندین مورد از این اسکنرهای بیومتریک برای بانک‌ها و شرکت‌های اعتباری که قصد معرفی خودشان به مشتریان معمولی را دارند، مشکل‌زاست. دکتر «نیل کاستیگان»، رمزنگار ایرلندی و مدیرعامل شرکت سوئدی BehavioSec بر این باور است برای این شرکت‌ها بخش گران‌قیمت و دردسرساز درواقع به‌چالش‌کشیدن کاربر یا همان مشتری است.

به گفته او، پرسیدن یک‌سری سؤالات، ازجمله «اسم حیوان خانگی» یا «ماشین‌حساب را کجا می‌گذارید» برای کاربر اذیت‌کننده است. با هرگام از امنیت که از کاربر می‌خواهد کاری انجام دهد درواقع از تعداد پرداخت‌ها کم می‌شود. برخی از شرکت‌های فناورانه نیز روی تشخیص صدا برای احراز هویت‌های بانکی کار می‌کنند؛ چراکه خیلی برای مشتریان دردسرساز و دشوار نیست. گروهی از محققان نیز در تلاش برای کاشت ایمپلنت‌های بیومتریک هستند؛ مانند تراشه احراز هویت فرکانس رادیویی که زیر پوست کار گذاشته می‌شود یا خالکوبی‌های پاک‌شدنی که بتواند یک یا دو ماه دوام بیاورد. دولت‌ها و مؤسسات خصوصی بیشتر ترجیح می‌دهند از نظر امنیت زیاد سخت نگیرند و مشتریانشان را نیازارند.

یک جایگزین دیگر برای احراز هویت، بیومتریک رفتاری است؛ یعنی بررسی ژست و سرعتی که کاربر رمزعبور خود را به سیستم وارد می‌کند. وقتی Danske Bank تلاش داشت تایمری را به پلت‌فرم بانکداری الکترونیک خود معرفی کند، دریافت سرعتی که کاربر فرم آنلاین را پر می‌کند، می‌تواند در ۹۷/۴ درصد موارد یک کاربر واقعی را از یک متقلب مشخص کند. پیش‌بینی بسیاری از کارشناسان این است که بیومتریک، مرگ رمز عبور را رقم خواهد زد. برخی از کارشناسان بر این باورند ابزارهایی مانند کلید امنیتی فیزیکی HSBC و کارت‌های اعتباری دیگر پایشان لب گور است.

مبارزه با نسل آتی بدافزارها

نسل بعدی حملات سایبری پیچیده‌تر خواهند شد، ردیابی آنها دشوارتر خواهد شد و امکان بیشتری برای ایجاد اثرات مخرب ناگفته بر سیستم‌های کامپیوتری خواهند یافت. ازاین‌رو، وزارت دفاع ایالات‌متحده کمک‌هزینه‌ای سه میلیون دلاری به گروهی از دانشمندان علوم کامپیوتری در دانشگاه یوتا و دانشگاه کالیفرنیا، ایروین داده است تا نرم‌افزاری بسازند که بتواند نقاط ضعفی را بیابد که یافتن‌شان با تکنولوژی‌های امروزی تقریبا ناممکن است. وظیفه این گروه، ساختن تحلیلگری است که بتواند حملات اصطلاحا الگوریتمی‌ای را خنثی کند که مجموعه قوانین یا محاسباتی را موردحمله قرار می‌دهند که کامپیوترها باید برای حل مشکلات‌شان به آنها مراجعه کنند. سازمان فناوری اطلاعات بر اساس گزارش ساینس‌دیلی گزارشی را منتشر کرده که در آن آمده است: حملات الگوریتمی آن‌قدر جدید و پیچیده‌اند که تنها هکرهای تحت استخدام دولت‌ها ممکن است از منبع لازم برای اجرایشان برخوردار باشند؛ البته شاید نه برای مدت طولانی. مت مایت، دانشیار علوم کامپیوتری در دانشگاه یوتا و یکی از سرپرستان این گروه می‌گوید: ارتش چشم به آینده دارد تا ببیند در حوزه امنیت سایبری چه چیز تازه‌ای در شُرُف شکل‌گیری است و این‌طور به‌نظر می‌رسد که حملات الگوریتمی در حال ظهورند. مایت در مورد وضعیت فعلی امنیت کامپیوتری می‌گوید: «درحال‌حاضر، درهای خانه باز است و دلیلی وجود ندارد که کسی نردبان بگذارد و از پنجره‌ای قفل‌نشده در روی بام به خانه راه یابد. اما وقتی تمام درهای طبقه پایین قفل باشد، مهاجمان نردبان تهیه می‌کنند. کل نسل بعدی نقاط ضعف امنیتی در همین خلاصه می‌شود». امروزه ضعف‌های نرم‌افزاری عموما ناشی از کار برنامه‌نویس‌هایی هستند که در هنگام نوشتن برنامه‌هایشان دچار خطا می‌شوند و هکرها هم از این خطاها بهره‌برداری می‌کنند. برای مثال، نرم‌افزار درونداد برنامه‌نویسی‌ای دریافت می‌کند که یک هکر آن را ساخته است و بدون اعتبارسنجی اولیه از آن استفاده می‌کند. این عمل می‌تواند منجر به ایجاد نقطه‌ضعفی شود که به هکر امکان دسترسی به کامپیوتر یا نشت اطلاعات را می‌دهد. حملات الگوریتمی نیازی به پیداکردن این نوع نقاط ضعف معمولی ندارند. برای مثال آنها می‌توانند مخفیانه این موضوع را بررسی کنند که هرالگوریتم چطور اجرا می‌شود یا هر کامپیوتر چه میزان انرژی مصرف می‌کند و از این اطلاعات برای گردآوری داده‌های محرمانه‌ای که کامپیوتر پردازش‌شان می‌کند، بهره می‌برد. حملات الگوریتمی همچنین می‌توانند با واداشتن کامپیوتر به استفاده بیش از حد از حافظه یا واداشتن واحد پردازش مرکزی آن به کار بیش از حد، کامپیوتر را از کار بیندازند. سورش ونکاتاسوبرامانیان، دانشیار علوم کامپیوتر و یکی از سرپرستان گروه تحقیقی مذکور، می‌گوید: «این حملات الگوریتمی به‌ویژه غیرمستقیم صورت می‌گیرند زیرا از نقطه‌ضعف‌هایی در نحوه کاربرد منابعی چون زمان و فضا در الگوریتم بهره می‌برند».

اغلب هکرها امروزه از حملات الگوریتمی استفاده نمی‌کنند، زیرا این حملات پرهزینه و به‌شدت پیچیده‌اند و زمان زیادی می‌طلبند. بنابراین مهاجمان از راه ساده‌تر بهره می‌برند و از نقطه‌ضعف‌های موجود استفاده می‌کنند. این گروه، نرم‌افزاری تولید خواهد کرد که می‌تواند برنامه‌های کامپیوتر را مورد نظارت قرار دهد و ضعف‌های الگوریتمی یا «هات‌اسپات»های کد را ردگیری کند. این تحلیلگر روی نرم‌افزار شبیه‌سازی ریاضی انجام می‌دهد تا پیش‌بینی کند در صورت وقوع حمله چه اتفاقی خواهد افتاد. مایت می‌گوید: «این نرم‌افزار مانند نرم‌افزار بررسی صحت املای کلمات است، فقط وضعیت امنیت سایبری را بررسی می‌کند».

نگاه

کدگذاری داده‌ها با هزینه‌ای کمتر

● سنجش سالانه توسعه کدگذاری در کسب‌وکارها نشان می‌دهد تعداد شرکت‌هایی که راهبردی جامع در این زمینه دارند، اندکی افزایش یافته و شرکت‌های فعال در زمینه خرده‌فروشی و خدمات بهداشتی، بیشترین دستاورد را کسب کرده‌اند. بنابر نظرسنجی مؤسسه پانمان (Ponemon Institute) بعد از نفوذهای بزرگ هکری در سال ۲۰۱۴- که بیشترین تأثیر را بر خرده‌فروشی‌ها و خدمات بهداشتی برجای گذاشتند- شرکت‌ها بیش‌ازپیش به راهبردهای کدگذاری روی آورده‌اند هرچند اغلب آنان در راه‌اندازی این فناوری امنیتی مشکلات عمده‌ای داشته‌اند. بنا بر این تحقیق که با حمایت شرکت ثیلز ئی-سکیوریتی (Thales e-Security) انجام شده است، بیشتر از یک‌سوم شرکت‌ها، فناوری‌های کدگذاری را به‌طور گسترده راه‌اندازی کرده‌اند. در حالی که خدمات مالی در این صنعت منجر به توسعه کدگذاری در سال ۲۰۱۴ شد، بیشترین درصد دستاوردها در حوزه صنایع بهداشت، دارو و خرده‌فروشی حاصل شده است. براساس پایگاه سازمان فناوری اطلاعات ایران، ئی‌ویک در گزارشی می‌نویسد: براساس این تحقیق، به طور متوسط، ۳۶ درصد از شرکت‌ها از راهبرد کدگذاری کاملی در سراسر کسب‌وکار خود برخوردارند. اما شرکت‌های سه کشور در اجرای کدگذاری‌ها فعال‌تر بوده‌اند: در آلمان که به حفظ حریم شخصی حساس است، ۵۹ درصد از شرکت‌ها از راهبرد جامعی برخوردارند و این در حالی است که شرکت‌های آمریکایی و ژاپنی با ۴۳ و ۳۹ درصد در سطحی بالای حد متوسط قرار دارند. اما صرف هزینه برای کدگذاری در سال ۲۰۱۴ کاهش یافت. پول صرف‌شده، به منزله درصدی از بودجه امنیت آی‌تی، در سال ۲۰۱۴ به ۱۵/۷ درصد رسید و این در حالی است که در سال قبل از آن، این رقم ۱۸/۲درصد بود. درمجموع، هزینه مصروفه برای امنیت در سال ۲۰۱۴ اندکی کاهش یافت و به ۲/۹ درصد از کل بودجه آی‌تی رسید. این رقم در سال ۲۰۱۳ به میزان ۹/۹ درصد بود. بااین‌حال، هزینه صرف‌شده برای آی‌تی طی دهه گذشته، از سال ۲۰۰۵، به طور پیوسته افزایش یافته است. این رقم در سال ۲۰۰۵ معادل ۷/۵ درصد بود. بنابر نظراتی که پاسخ‌گویان به مؤسسه پانمان داده‌اند، مانع عمده در اجرای کدگذاری عبارت است از شناسایی جایی از شبکه که داده‌های حساس در آن قرار داده شده‌اند.