رویداد

همکاری ایران و ویتنام برای اجرای پروژه فیبر نوری منازل

● **شرق:** نشست کاری مدیران مخابرات ایران و گروه مخابرات کشور ویتنام در راستای استفاده از تجارب مشترک دو کشور در حوزه فناوری (FTTH) در نمایشگاه تله‌کام برگزار شد. در این نشست، رسول سرائیان، مدیرعامل شرکت مخابرات ایران، با اشاره به برنامه‌های ایران برای اجرای پروژه دسترسی منازل به فیبر نوری بیان کرد: در راستای برقراری تعاملات دوسویه و بهره‌گیری از تجارب صنعت مخابرات ویتنام تیم مشارکتی در این زمینه تشکیل می‌شود. او بر ضرورت گسترش همکاری‌های دوجانبه در این مورد تأکید کرد و گفت: با مشارکت و هم‌افزایی توانمندی‌های مشترک می‌توانیم زمینه راه‌اندازی طرح (FTTH) را در ایران فراهم کنیم. در این نشست، هونگ تین، رئیس فناوری گروه مخابرات کشور ویتنام، بر لزوم تدوین توافق‌نامه همکاری درخصوص اجرای مشترک این پروژه تأکید کرد. براین اساس مقرر شد گروه کارشناسی برای عملیات مطالعاتی و اجرائی به صورت مشترک ایجاد شود. مدیرعامل شرکت مخابرات ایران بهترین مکان برای ایجاد یک سرمایه‌گذاری مشترک به منظور راه‌اندازی شبکه دسترسی فیبر نوری را مراکز دانشگاهی، مجتمع‌های تجاری و در نهایت منازل مسکونی عنوان کرد که به لحاظ تجاری و درآمدزایی در وضعیت مناسبی قرار دارند.

واگذاری تلفن ثابت به شیوه جدید

● **فارس:** مدیرعامل شرکت مخابرات استان تهران از راه‌حل جدید این شرکت برای کاهش صف انتظار دریافت تلفن ثابت خبر داد. علیرضا صیدی با اعلام این خبر گفت در شیوه جدید واگذاری، تمامی امکانات تلفن ثابت در بستر اینترنت با سرعت راه‌اندازی سریع‌تر به مشترکان ارائه می‌شود. او ادامه داد: با شیوه جدید واگذاری تلفن ثابت با استفاده از سرویس سیپ‌فون (SIP PHONE)، ارائه تمامی امکانات تلفن ثابت در بستر اینترنت به جای بستر سیم مسی امکان‌پذیر می‌شود. به گفته او، این روش دارای سرعت بیشتری در راه‌اندازی و واگذاری است و می‌تواند جایگزین روش فعلی واگذاری خط تلفن ثابت باشد. او افزود: در این مدل سرویس‌های در بستر اینترنت با حذف سیم مسی به صورت مستقیم اتصال به شبکه دیتا برقرار می‌شود. در این روش امکان استفاده از چند خط تلفن با شماره‌های متفاوت روی یک خط فراهم است.

سرمایه‌گذاری کشور برای جهانی‌شدن صنعت بازی

● **شرق:** نمایشگاه Tehran Game Convention با حضور سرمایه‌گذاران و شرکت‌های ناشر از سراسر دنیا در ایران برگزار می‌شود. براساس اعلام بنیاد ملی بازی‌های رایانه‌ای، کشور حمایت کامل بازی‌سازان داخلی را دارد و در هر گام از مشورت و نظرات تک‌تک بازی‌سازان داخلی یاری جسته است و می‌تواند نقطه عطفی در تاریخ صنعت نوپای بازی‌سازی باشد. طرح‌ریزی اقدامات اولیه برای برگزاری رویداد TGC براساس برنامه ملی بازی‌های رایانه‌ای مصوبه سال ۱۳۹۴ شورای‌عالی فضای مجازی، انجام شده و در این نمایشگاه که برای اولین‌بار قرار است ناشران، سرمایه‌گذاران و فعالان بین‌المللی را به ایران بیاورد، فرصت‌هایی در اختیار بازی‌سازان کشورمان قرار می‌گیرد تا خودشان را به بازارهای جهانی متصل کنند.

احتمال افزایش هک‌شدن بانک‌ها

● **فارس:** مدیران شبکه تبادل پیام‌های بانکی سوییفت هشدار داده‌اند در تابستان گذشته سه بانک مشتری آنها هک شده‌اند و حملات سایبری به بانک‌ها رو به افزایش است. براساس گزارش رویترز، این شبکه به بانک‌ها امکان می‌دهد تا دستوراتی را برای پرداخت چندین تریلیون دلار به طور روزانه ارسال کنند.

درحالی‌که تصور نمی‌شد شبکه یادشده دارای مشکلات جدی امنیتی باشد، اما حالا مشخص شده سوییفت هم از دست‌اندازی هکرها در امان نیست. سرقت ۸۱ میلیون دلار از بانک مرکزی بنگلادش در ماه فوریه با سوءاستفاده از سوییفت، اعتماد به این شبکه تبادل پیام‌های بین بانکی را به طور جدی خدشه‌دار کرد و حالا مشخص شده بانک‌ها خود باید با استفاده از سرویس‌ها و نرم‌افزارهای امنیتی به فکر تأمین امنیتشان باشند. سوییفت روز دوشنبه مجموعه‌ای از دستورات امنیتی اجباری را نیز در واکنش به حملات به مشتریان خود منتشر کرده و انتظار می‌رود از این طریق امنیت مشتریان در برابر هجوم‌های سایبری بیشتر شود.

کنترل‌های ضروری سالانه‌ای که سوییفت به مشتریان خود تحمیل کرده به ۱۶ مورد رسیده و قرار است در سال ۲۰۱۸ تحقیقات و بررسی‌هایی در این زمینه صورت گیرد و در صورت رعایت‌نکردن استانداردهای ضروری تصمیمات مقتضی گرفته خواهد شد. این احتمال وجود دارد که سوییفت حتی رابطه خود را با بانک‌های متخلف قطع کند.

دبیر شورای‌عالی فضای مجازی:

حمله سایبری به مراکز پتروشیمی به اثبات نرسید

اخیرا چند آتش‌سوزی در مراکز مختلف پتروشیمی و صنعتی، خسارات زیادی در کشور به بار آورد و باعث شد منشأ این آتش‌سوزی‌ها در هاله‌ای از ابهام قرار گیرد. سیدهادی سجادی، معاون امنیت سازمان فناوری اطلاعات ایران در همان زمان از احتمال سایبری‌بودن منشأ این آتش‌سوزی‌ها در مراکز پتروشیمی خبر داده و گفته بود: «با توجه به گمانه‌زنی‌ها درباره منشأ تهدیدات سایبری در آتش‌سوزی‌های اخیر تأسیسات صنعتی کشور، مرکز ملی فضای مجازی بررسی این موضوع را در دستور کار دارد». سجادی افزوده بود: «مرکز ملی فضای مجازی به عنوان مرکز هماهنگی برای تقسیم کار ملی در فضای مجازی، همه نوع تهدیدات محتمل را بررسی می‌کند و این کار را با کمک تمامی نهادهای فعال مرتبط با نهادهای امنیتی انجام می‌دهد. گروه‌های فعال در حوزه امنیت، نسبت به پایش و کنترل اوضاع اقدام کرده‌اند، اما تاکنون هیچ نشانه‌ای مبنی بر منشأ تهدیدات سایبری این رخدادها دیده نشده است». او بیان کرده بود: «اگر نتیجه این بررسی‌ها به وجود نشانه‌ای ختم شود حتما به نهادهای فعال مرتبط با نهادهای امنیتی برای بررسی موضوع شامل مرکز افتا (مرکز راهبردی امنیت فضای تبادل اطلاعات ریاست‌جمهوری)، پلیس فتا، سازمان پدافند غیرعامل و مرکز ماهر مأموریت داده می‌شود». به گزارش فارس، اکنون دبیر شورای عالی فضای مجازی با اعلام نتایج بررسی تیم‌های اعزامی ویژه به محل آتش‌سوزی‌های اخیر گفته است: «موضوعی دال بر حمله سایبری در حوادث اخیر به اثبات نرسید». ابوالحسن فیروزآبادی درباره نتایج ارزیابی تیم‌های ویژه این شورا برای بررسی منشأ سایبری آتش‌سوزی‌های اشاره‌شده، بیان کرده است: «تیم‌های ویژه در تاریخ مقرر گزارش خود را به شورا ارائه دادند و این گزارش را به مسئولان منعکس کردیم، اما موضوعی که ثابت کند براساس حمله سایبری حادثه‌ای اتفاق افتاده به اثبات نرسید». او افزوده است: «به‌این‌ترتیب موضوع احتمال حملات سایبری در آتش‌سوزی‌های اخیر با رد حمله سایبری به پایان رسید. اما حین بازدیدهایی که این تیم‌های ویژه از مناطق حادثه‌دیده داشتند، اشکالاتی ملاحظه شد که امیدواریم این اشکالات رفع شود». گرچه این رویداد از سوی شورای عالی فضای مجازی تأیید نشد، اما به گفته کارشناسان، حملات سایبری که منجر به بروز خسارات در دنیای فیزیکی می‌شوند، دیگر یک رؤیا یا موضوع فیلم سینمایی نیستند و امروزه، نمونه‌های متعددی وجود دارد که در آن حملات سایبری، به بروز خسارات مالی منجر شده‌اند. یکی از بارزترین این حملات، حمله سایبری سال ۲۰۱۰ به تأسیسات هسته‌ای نطنز بود که منجر به ازکارافتادن تعدادی از سانتریفیوژها شد. حمله به کارخانه فولاد آلمان در سال ۲۰۱۴، حمله به شبکه برق ترکیه در سال ۲۰۱۵ که سبب خاموشی نیمی از ترکیه شد، حمله سال گذشته به شبکه برق اوکراین که عامل خاموشی گسترده در این کشور شد و اتهام آن به روسیه نسبت داده شد، انفجار سال ۲۰۰۸ در خطوط انتقال نفت ترکیه که در آن احتمال حمله سایبری وجود داشت و نمونه‌های دیگری از این دست، نشان از آن دارند که احتمال بروز آتش‌سوزی در صنایع پتروشیمی ایران به علت بروز یک حمله سایبری، دیگر صحبتی دور از واقعیت نیست. نکته مهم دیگر این است که وزارت نفت ایران نیز از جمله اهدافی بوده که گاهی با حمله سایبری دشمنان مواجه شده است؛ برای نمونه در سال گذشته رئیس پلیس فتای ناجا، از حمله هکرهای آمریکایی به وزارت نفت خبر داد و گفت: «مرکز فوریت‌های واکنش به حملات سایبری که در پلیس فتا فعال است، موفق شد حمله هکرها به وزارت نفت را خنثی کند». شایان ذکر است این حمله سایبری، بدون واردکردن خسارت فیزیکی در همان ابتدای کار، خنثی شد.

مصائب سایبری کلینتون ادامه دارد

اعتراف به ضعف و آسیب‌پذیری زیرساخت‌های آمریکا

کلینتون در نشستی محرمانه، به آسیب‌پذیری زیرساخت‌های آمریکایی در برابر نفوذهای امنیتی اشاره کرده است. به‌تازگی اسنادی منتشر شده که نشان می‌دهد هیلاری کلینتون در جلسه‌ای محرمانه، درباره آسیب‌پذیری شبکه‌های دولتی هشدار داده است. این نشست محرمانه، دقیقا یک روز قبل از انتشار خبری برگزار شده که در آن مشخص می‌شود در ایمیل‌های کلینتون، مباحث فوق‌محرمانه امنیتی وجود داشته است. به گزارش سایبربان، در یکی از ایمیل‌های اعضای ستاد انتخاباتی کلینتون که به‌تازگی هکرها به آن نفوذ کرده‌اند، فایل صوتی این جلسه محرمانه یافت شده که حاوی پاسخ‌های کلینتون به برخی پرسش‌ها درباره موضوعات امنیتی است. در این فایل صوتی، کلینتون در پاسخ به سوالی درباره جمع‌آوری اطلاعات و نفوذ به شبکه‌های دولتی آمریکایی گفت: «ایالات متحده آمریکا در معرض خطر نفوذ امنیتی قرار دارد و این تهدیدات، هم از جانب دولت‌های مختلف احساس می‌شود و هم از سوی گروه‌های مختلف تروریستی، متوجه ما خواهد شد». همچنین کلینتون، نسبت به این موضوع نیز هشدار داد که چالش‌های امنیت سایبری، قطعا به معضلی بزرگ برای رئیس‌جمهور آینده آمریکا تبدیل می‌شود. او در بخشی از صحبت‌های خودش دراین‌باره گفت: «بخش‌های مختلف دولت ما مانند وزارت دفاع، آژانس امنیت ملی و سازمان اطلاعات مرکزی آمریکا به اندازه کافی پیچیده نیستند؛ بنابراین مجبوریم خود را در تمامی زمینه‌ها ارتقا بدهیم. ما همواره در معرض تهدیدات سایبری از جانب کشورهایی نظیر چین، روسیه، ایران و حتی کره شمالی هستیم، اما موضوعی که من را نگران می‌کند، تهدیداتی است که از جانب بازیگران غیردولتی متوجه ما می‌شود». نکته تأمل‌برانگیز در صحبت‌های هر دو نامزد انتخابات ریاست‌جمهوری آمریکا این است که هر دوی این افراد، مکررا تهدیدات امنیتی و خصوصا امنیت سایبری را یکی از معضلات جدی پیش‌روی آمریکا قلمداد می‌کنند و بر پیدا کردن راهکاری مناسب برای مقابله با آن تأکید می‌کنند، اما ظاهرا هیچ‌کدام از آنها، درک روشنی از طبقه‌بندی اطلاعات ندارند و به‌راحتی اسرار دولتی در آمریکا را که دولت میلیاردها دلار برای مخفی‌سازی آنها هزینه کرده است، برملا می‌کنند. پیش از این نیز دونالد ترامپ، صحبت‌هایی درباره ارتباط داعش با آمریکا بیان کرده بود که با واکنش مقامات امنیتی آمریکایی مواجه شده بود و آنها را وادار کرده بود برای ترامپ، جلسه توجیه امنیتی برگزار کنند. البته این موضوع برای دونالد ترامپ که صرفا یک تاجر است و حتی یک روز سابقه حضور در عرصه سیاست را هم ندارد، موضوعی طبیعی است، اما از کلینتون که سال‌ها حضور در عرصه‌های مختلف سیاسی آمریکا را تجربه کرده، بعید به نظر می‌رسد و اشتباهی فاحش به حساب می‌آید.

چرا اطلاعات ۵۰۰ میلیون کاربر یاهو هک شد؟

یاهو رسما اعلام کرد که در سال ۲۰۱۴ قربانی هک گسترده‌ای شده است. اما حدودا بعد از دو سال و پس از فروش این اطلاعات در بازار سیاه رسما به این حمله اعتراف کرده است. اطلاعاتی از جمله نام‌ها، آدرس ایمیل، شماره تلفن و سؤالات امنیتی از شبکه شرکت یاهو در سال ۲۰۱۴ دزدیده شده است. رمز عبورها هم البته به صورت مخدوش‌شده دزدیده شده که باعث می‌شود هکرها نتوانند بلافاصله از آنها استفاده کنند. همچنین شرکت یاهو بر این باور است که اطلاعات مالی دست‌نخورده باقی مانده است. این شرکت، هک را در بیانیه‌ای در پنجشنبه‌شب تأیید کرد. اما این بیانیه و اطلاعیه‌ای که در جمعه صبح به مشتریان ارسال شد، سؤالات زیادی را ایجاد کردند. به گزارش زومیت، مهم‌ترین سؤالات درباره این است که چرا این اطلاع‌رسانی این‌قدر دیر انجام شده است. چون زمان هک مربوط به دو سال پیش بوده و این اطلاعات حدود دو ماه پیش در دارک وب (Dark Web) از سوی کاربری به نام Peace of Mind فروخته شد، کاربری که پیش از این اطلاعاتی از سایت‌های مای‌اسپیس (MySpace) و لینکدین (LinkedIn) به فروش گذاشته بود. جرمایاه گراسمن، مدیر بخش استراتژی امنیت شرکت سنتینل‌وان (SentinelOne) می‌گوید: «ما درحالی‌که می‌دانیم این اطلاعات در سال ۲۰۱۴ دزدیده شده، اما نمی‌دانیم یاهو چه زمانی از این هک آگاه شده است. این بخش مهمی از داستان است». گراسمن که تا سال ۲۰۱۱ مسئول بخش امنیت دپارتمان مهندسی یاهو بوده، می‌گوید این ادعای یاهو که هکرها از پشتیبان دولتی برخوردار بوده‌اند، نیازمند تحقیق بیشتری است. او در ادامه گفته است: «هکرهای دولتی هیچ‌وقت چنین اطلاعاتی را در بازار سیاه به فروش نمی‌رسانند، کاری که هکر یاهو انجام داده است. این هک به احتمال قریب به یقین فقط با انگیزه‌های مالی انجام شده است، پس احتمال اینکه او از پشتیبانی دولتی برخوردار بوده بسیار کم است. اگر هم چنین باشد، پس باید داستان درباره دو نفوذ جداگانه از سوی دو تیم مختلف باشد». کریس هادسن مدیر بخش اطلاعات امنیت اروپا، آفریقا و خاورمیانه شرکت امنیتی زسکالر با این گفته‌ها موافق است و در پی آن بیان کرده: «بدون هیچ‌گونه اطلاع‌رسانی درباره نحوه این هک، ادعای یاهو مبنی بر دولتی‌بودن هکرها اصلا اثبات‌شدنی نیست. این ادعای یاهو بیشتر برای منحرف‌کردن افکار عمومی به نظر می‌رسد و با توجه به اطلاع‌رسانی‌نکردن دقیق نمی‌توان به طور قطع نظر داد». در ضمن معلوم نیست تا چه حد رمزهای عبور، از هک نجات یافته‌اند. اما یاهو اذعان کرده رمزها به صورت مخدوش‌شده به دست هکرها رسیده است. این شرکت تأکید کرده است که قسمت اعظمی از رمزهای عبور از سوی الگوریتمی به نام بی‌کریپت (bcrypt) مخدوش شده است. این روش باعث می‌شود حتی رمزهای یکسان به صورت مخلوطی از کاراکترها در دیتابیس ذخیره شوند. این‌گونه بسیاری از افراد هم که رمزهای بسیار آسانی انتخاب کرده‌اند، از هک آسیب‌پذیر نخواهند بود. اما معلوم نیست آن درصد اندک که شامل این رمزنگاری نبوده‌اند چه تضمینی خواهند داشت. این حمله باعث شده مفیدبودن به‌دست‌آوردن رمز به وسیله سؤال‌های امنیتی زیر سؤال برود، چرا که به‌راحتی با چند سؤال ساده درباره نام مادر یا شهر تولد، هکر می‌تواند رمز قربانی را به دست آورد. یاهو تمام این سؤال‌ها را رمزنگاری نکرده، پس تعدادی از این سؤالات به‌راحتی در دسترس هکرها قرار گرفته است. یک سؤال دیگر که بعد از این هک بی‌جواب مانده است: تکلیف ادغام چندین‌میلیارددلاری یاهو با ورایزون (Verizon) چه خواهد شد؟ کوین کانینگهام، مؤسس و رئیس شرکت سیل‌پوینت (SailPoint) دراین‌باره می‌گوید: «به احتمال زیاد ورایزون با توجه به این قضیه قیمت‌گذاری کرده است. ادغام شرکت‌ها با روندی بسیار طولانی و دقیق صورت می‌گیرد. شرکت‌ها معمولا با تحقیقی مفصل به چنین پیشنهاداتی دست می‌زنند. ورایزون با توجه به تعداد زیاد کاربران یاهو از ریسک چنین ادغامی از قبل خبر داشته است. این سؤال که آیا این خبر بر قیمت‌گذاری تأثیر می‌گذارد یا نه بستگی به بررسی دقیق در زمینه کنترل امنیت یاهو دارد. این هک نه‌تنها باید نگرانی در زمینه امنیت شبکه را بالا ببرد بلکه دولت را هم باید نگران کند. چون دیده‌ایم در هک‌هایی مانند لینکدین (LinkedIn)، دراپ‌باکس (DropBox) و بسیاری از موارد دیگر با استفاده از این اطلاعات، اعتبار شهروندان زیادی زیر سؤال می‌رود». اما برای کاربران این سؤالات اصلا اهمیتی ندارد. تنها توصیه‌ای که در این موقعیت می‌توان به کاربران یاهو کرد این است: پسورد حساب کاربری یاهو و سؤالات امنیتی خود را هرچه‌زودتر تغییر دهند، همچنین پسورد جاهای دیگری که این اطلاعات را در آن استفاده کرده‌اند. در نهایت آنها باید از این پسوردها در هیچ حساب کاربری دیگری استفاده نکنند. چون یاهو یک سرویس ایمیل بزرگ محسوب می‌شود، یک مشکل دیگر هم وجود دارد. هر حساب کاربری که با ایمیل یاهو باز شده است، باید هرچه‌زودتر رمز آن حساب تغییر یابد.

بازار

راهنمای خرید لپ‌تاپ‌هایی با قیمت ۴ میلیون تومان

● حدود قیمتی چهار میلیون تومان بودجه‌ای است که با آن می‌توان لپ‌تاپ‌هایی با کارایی و البته ارزش خرید بالا را در بازار یافت. چه بخواهید یک لپ‌تاپ مناسب برای بازی خریداری کنید، چه هدف شما بیشتر تماشای فیلم و مصرف محتوا باشد و چه عمر شارژ و قابلیت حمل برایتان مهم باشد، در این محدوده قیمتی می‌توانید گزینه‌های خوبی را پیدا کنید.

لپ‌تاپ‌های بازی و چندرسانه‌ای

به گزارش فارنت، لپ‌تاپ‌های این دسته حداقل دارای پردازنده Core i7-6700HQ بوده و به لطف کارت گرافیک قدرتمند NVIDIA GeForce 960M می‌توانند از پس بازی‌های روز با وضوح 1080p و تنظیمات متوسط یا بالا بربیایند. تفاوت اصلی در مدل‌های معرفی‌شده وضوح صفحه نمایش، طراحی بدنه، دوام شارژ باتری و نوع حافظه است. لپ‌تاپ‌هایی مانند ASUS N501VW، لنوو آیدیاپد و ایسر اسپایر جزء بهترین‌ها در این بخش هستند. لپ‌تاپ N501VW ایسوس، همچنین در یک نسخه دیگر با ۵۱۲ گیگابایت حافظه SSD PCIe x4 نیز در بازار موجود است که نه‌تنها سرعت بالاتری دارد، بلکه از عمر شارژ بسیار بهتری نیز برخوردار است. این نسخه با قیمتی نزدیک به چهارمیلیون‌و ۹۰۰ هزار تومان فروخته می‌شود.

لپ‌تاپ‌های با عمر شارژ بالا و قابلیت حمل مناسب

اپل مک‌بوک‌ایر ۱۳ اینچی یکی از این لپ‌تاپ‌هاست. مک‌بوک‌ایر سال‌هاست به عنوان بهترین لپ‌تاپ برای خبرنگاران و کاربرانی که دائم در حال جابه‌جایی هستند شناخته می‌شود. عمر شارژ عالی، کیبورد فوق‌العاده، وزن کم و سرعت بالا از مهم‌ترین دلایلی است که این لپ‌تاپ را هنوز هم بین بهترین‌ها نگه داشته است. همچنین ایسوس ذن‌بوک را نیز شاید بتوان تنها اولترابوک بازار دانست که به لطف پردازنده گرافیکی مناسب GeForce 940M برای بازی‌ها نیز تا حد زیادی مناسب است. هارد دیسک معمولی در کنار SSD نیز آن را هرچه بیشتر به گزینه‌ای بین یک اولترابوک و یک لپ‌تاپ مالتی‌مدیا شبیه کرده است. البته از معایب آن می‌توان به هارد دیسک کُند نسبت به SSD در دیگر لپ‌تاپ‌ها، سنگین‌تربودن و دوام شارژ پایین اشاره کرد. اپل مک‌بوک ۱۲اینچی برای افرادی طراحی شده که فوق‌العاده به جابه‌جایی و وزن پایین اهمیت داده و حاضرند عملکرد را فدای راحتی و زیبایی کنند. مهم‌ترین مزیت این لپ‌تاپ، فوق‌العاده سبک و باریک، زیبایی و بلندگوهای قدرتمند است.