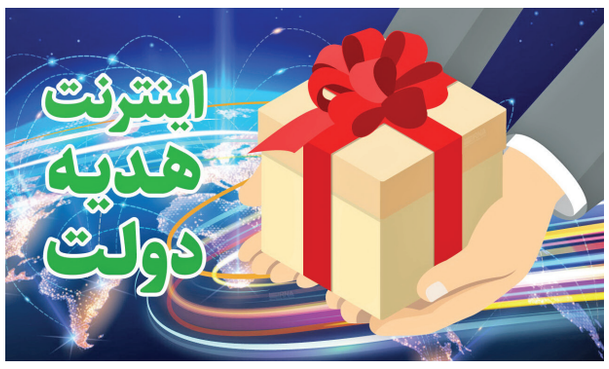
اخبار

۱۰ گیگ اینترنت رایگان برای هر نفر



وزیر ارتباطات و فناوری اطلاعات از فعال‌سازی بسته اینترنت هدیه رایگان دولت برای همه مردم در بستر پنجره ملی خدمات دولت هوشمند خبر داد.
عیسی زارع‌پور گفت: به منظور تحقق وعده دولت، کاربران می‌توانند با مراجعه به پنجره ملی خدمات دولت هوشمند این بسته را فعال کنند. وی درباره جزئیات این بسته اینترنتی یادآور شد: فعال‌سازی اینترنت رایگان هدیه دولت برای مردم در قالب ۱۰ گیگابایت اینترنت داخلی (معادل پنج گیگابایت اینترنت بین‌الملل) روی یکی از سیم‌کارت‌های هر فرد به انتخاب خود او انجام می‌شود. کاربران می‌توانند با مراجعه به پنجره ملی خدمات دولت هوشمند به آدرس my.gov.ir از این هدیه بهره‌مند شوند. وزیر ارتباطات و فناوری اطلاعات همچنین با انتشار پستی در شبکه اجتماعی ایرانی نوشت: افزایش قیمت بسته‌های اینترنتی که با هدف توسعه زیرساخت‌های ارتباطی انجام شد، مشمول ترافیک داخلی نیست و اپراتورها مکلف به اجرای آن هستند.

رونمایی از ۹ محصول فناورانه در نمایشگاه «ایران‌ساخت»

بازدیدکنندگان از یازدهمین دوره نمایشگاه «تجهیزات، مواد آزمایشگاهی و تست و آزمون پیشرفته ایران ساخت» امروز شاهد رونمایی از ۹ محصول فناورانه تست و آزمون جدید و ساخت بار اول خواهند بود.
یازدهمین دوره نمایشگاه تجهیزات، مواد آزمایشگاهی و تست و آزمون پیشرفته ایران ساخت امروز با حضور روح‌الله دهقانی فیروزآبادی معاون علمی، فناوری واقتصاد دانش‌بنیان رئیس جمهور و محمدعلی زلفی‌گل وزیر علوم، تحقیقات و فناوری افتتاح می‌شود.
به گزارش ایرنا، این نمایشگاه تا ۱۵ دی ماه در محل دائمی نمایشگاه‌های بین‌المللی تهران، میزبان شرکت‌های دانش‌بنیان، فناور، دانشگاه‌ها و مراکز تحقیقاتی و هیأت‌هایی از کشورهای خارجی خواهد بود. در این رویداد فناورانه، ۳۳۰ شرکت ایرانی بیش از ۱۰هزار و ۵۰۰ مدل محصول تولیدی خود را در معرض دید بازدیدکنندگان قرار می‌دهند. این محصولات که در سطوح مختلف فناورانه دسته‌بندی شده‌اند، نیازهای صنعت، تحقیقات، پژوهش و فناوری کشور را تأمین می‌کنند.
در این نمایشگاه محصولات و خدمات متنوعی از حوزه‌های گوناگون اعم از نفت، گاز و پتروشیمی، برق، الکترونیک، نرم‌افزار و شبیه‌ساز، عمران و ساختمان، مکانیک، شیمی و متالورژی، کشاورزی و محیط زیست، فیزیک پایه، تجهیزات عمومی آزمایشگاهی، تجهیزات و ماشین‌آلات در حوزه فناوری‌های راهبردی ارائه می‌شود. حوزه‌های مهندسی پزشکی و زیست مواد، مواد آزمایشگاه، تجهیزات آموزشی با فناوری مناسب، تجهیزات حوزه تست و آزمون صنعتی و ارائه‌کنندگان خدمات کالیبراسیون از دیگر موضوعات عرضه محصولات در این دوره از نمایشگاه ایران‌ساخت است.

دانش‌بنیان

ترمیم پوست با کرم‌های دانش‌بنیان ایرانی

متخصصان یک شرکت دانش‌بنیان فعال در حوزه پزشکی بازساختی، موفق به تولید و تجاری‌سازی کرم‌هایی شدند که ترمیم پوست را سرعت می‌بخشد.
به گزارش روابط عمومی معاونت علمی، فناوری و اقتصاد دانش‌بنیان ریاست جمهوری، رضا صاحبی مدیرعامل این شرکت(نوژن) گفت: این کرم ترمیمی برای محافظت و درمان پوست بر پایه اگزوزوم‌های گیاهی، انسانی، جلبک‌ها و قارچ‌های دارویی تولید شده است و از سلول‌های خود افراد مشتق می‌شود یا بنیان گیاهی دارد.
وی با بیان اینکه این محصول روی داربست‌های زیستی سوار می‌شود تا پیام لازم مربوط به سنتز کلاژن و فاکتورهای رشدی مختلف را به لایه‌های عمیق‌تر برساند، افزود: از نظر ترمیمی برای زخم‌ها، اگزما و راش‌های پوستی و حتی برای مواردی مانند چین و چروک‌ها و آب‌رسانی بهتر و هدفمندتر قابل استفاده است.
صاحبی با یادآوری اینکه در حال حاضر ۷ نفر در مجموعه مشغول به فعالیت هستند، تصریح کرد: این محصول در حال حاضر در مسیر تجاری‌سازی قرار گرفته و کارآزمایی بالینی انجام شده و تأییدیه‌های ایزو نیز دریافت شده است. با دریافت مجوز تولید در سطح وسیع، این محصول می‌تواند تا پایان سال جاری به طور گسترده وارد بازار شود.

دیجیتال ترندز

۳/۸
میلیارد دلار
در سال ۲۰۲۲ میلادی درگزارشی عنوان شد مجرمان سایبری ۳٫۸میلیارد دلار رمزارز در دنیا به سرقت برده‌اند که حدود۱٫۷میلیارد دلار آن مربوط به گروه هکری لازاروس به عنوان یکی از پرکارترین گروه‌های هکری رمزارز جهان بود که در کره شمالی فعالیت دارند

خسارت ۸ تریلیون دلاری جرایم سایبری درسال ۲۰۲۳

گزارش

میتراجلیلی
خبرنگار

با به پایان رسیدن سال ۲۰۲۳ فعالان حوزه فناوری نگاهی به وضعیت امنیت سایبری جهان در این سال داشته‌اند تا شاید تلنگری برای شرکت‌ها و مؤسسات و کاربران عادی باشد که امنیت سایبری را در سال ۲۰۲۴ میلادی جدی‌تر بگیرند و با آگاهی بیشتری در فضای مجازی و اینترنت حضور یابند. هکرها همیشه در کمین طعمه‌ها هستند درحالی که بهترین راهکار و استراتژی برای ناکام گذاشتن آنها، رعایت چند گام ساده است.

هر ثانیه ۲۵۵هزار دلار خسارت

طبق گزارش مؤسسه Cybersecurity Ventures به عنوان یکی از مؤسسات پیشرو در جهان که اقتصاد سایبری جهانی را پوشش می‌دهد و یک منبع قابل اعتماد برای حقایق و ارقام امنیت سایبری است، جرایم اینترنتی در سال ۲۰۲۳ حدود ۸ تریلیون دلار برای جهان هزینه داشته است.
این رقم به معنای خسارت ماهانه ۶۶۷ میلیارد دلاری برای جهان است و این عدد در هر هفته به ۱۵۴ میلیارد دلار و روزانه به ۲۱٫۹ میلیارد دلار می‌رسد. این اختلال در تحقیقات پزشکی و همچنین آسیب به شهرت شرکت‌ها و مؤسسات کوچک و بزرگ می‌شود.
در این گزارش آمده است که بیش از نیمی از حملات سایبری علیه کسب‌وکارهای کوچک تا متوسط (SMB) انجام می‌شود که ۶۰ درصد آنها در نتیجه این حملات، در عرض شش ماه پس از نقض داده‌ها یا هک شدن، از کار می‌افتند و از گردونه خارج می شو ند .
این آمار تنها اعداد و رقم‌هایی روی کاغذ نیست وهریک از آنها می‌تواند بر زندگی چندین عدد بدان معناست که جهان درهر ساعت ۹۱۳ میلیون دلار در نتیجه حملات سایبری ضرر می‌کند و این رقم در هر دقیقه به ۱۵٫۲ میلیون دلار و در هر ثانیه به ۲۵۵۰۰۰ دلار می‌رسد.
همچنین طبق این گزارش، انتظار می‌رود میزان خسارت جرایم سایبری در جهان تا سال ۲۰۲۵ به ۱۰٫۵ تریلیون دلار در سال برسد، در حالی که این رقم در سال ۲۰۱۵، حدود ۳ تریلیون دلار بود؛ همین روند روبه رشد نشان می‌دهد که کاربران تا چه حد در مقابل هکرها و حربه‌های جدید آنها آسیب‌پذیرتر شده‌اند.
هزینه‌های جرایم سایبری شامل آسیب و تخریب داده‌ها، سرقت پول، کاهش بهره‌وری، سرقت مالکیت معنوی، سرقت اطلاعات شخصی و مالی، اختلاس، کلاهبرداری، اختلال در روند عادی کسب و کار پس از حمله، خانواده تأثیرگذار باشد و اقتصاد شرکت‌ها و مؤسسات و حتی کشورها را با چالش‌های جدی مواجه سازد.
به همین دلیل هم فعالان حوزه سایبری دائم نسبت به رعایت موارد امنیت سایبری هشدار می‌دهند.

تیغ حملات سایبری برگردن آموزش و تحقیقات

در سال ۲۰۲۳ مؤسسات دیگری هم در زمینه وضعیت امنیت سایبری جهان تحقیق وپژوهش داشته‌اند. یکی از این مؤسسات، چک پوینت (Check Point Research) است که در تازه‌ترین گزارش خود یادآور شده است میانگین هفتگی حملات سایبری جهانی با بالاترین تعداد در ۲ سال گذشته به اوج خود رسیده و رشد سالانه ۸ درصدی را نشان می‌دهد.
طبق این گزارش، در ماه‌های پایانی ۲۰۲۳، میانگین تعداد حملات به ازای هر سازمان در هفته به ۱۲۵۸ عدد رسیده است که بالاترین تعداد در ۲ سال گذشته محسوب می‌شود و اگر بخواهیم میزان حملات در صنایع گوناگون را با یکدیگر مقایسه کنیم، باید گفت که میزان حملات سایبری به مؤسسات آموزشی و تحقیقاتی در صدر فهرست قرار دارد. در طول سه‌ماهه دوم ۲۰۲۳، بخش آموزش و تحقیق با میانگین ۲۱۷۹ حمله به هر سازمان در هفته، بیشترین تعداد حملات را تجربه کرد.
بخش دولتی/نظامی با میانگین ۱۷۷۲ حمله در هفته در جایگاه دوم قرار گرفت که نشان دهنده افزایش ۹ درصدی نسبت به دوره مشابه در سال گذشته است.
بخش مراقبت‌های بهداشتی با میانگین ۱۷۴۴ حمله در هفته هم نشان‌دهنده افزایش قابل توجه ۳۰ درصدی نسبت به سال ۲۰۲۲ است.

> در ماه‌های پایانی ۲۰۲۳ میانگین تعداد حملات به ازای هر سازمان در هفته به ۱۲۵۸ عدد رسیده است که بالاترین تعداد در ۲ سال گذشته محسوب می‌شود باید گفت که میزان حملات سایبری به مؤسسات آموزشی و تحقیقاتی در صدر فهرست قرار دارد

سرقت ۲میلیارد دلار رمزارز

علاوه بر صنایع، مؤسسات تحقیقاتی و بخش نظامی و تحقیقاتی، رمزارزها هم در سال ۲۰۲۳ میلادی بسیار مورد توجه هکرها قرار داشته‌اند به گونه‌ای که وب سایت De.FI از سرقت حدود ۲میلیارد دلار ارز دیجیتال در سال ۲۰۲۳ توسط مجرمان سایبری طی چندین حمله سایبری خبر داد؛ هرچند مقایسه این رقم با سال ۲۰۲۰ نشان از روند نزولی هک ارزهای دیجیتال در دنیا دارد.
در سال ۲۰۲۲ میلادی درگزارشی عنوان شد مجرمان سایبری ۳٫۸میلیارد دلار رمزارز در دنیا به سرقت برده‌اند که حدود۱٫۷میلیارد دلار آن مربوط به گروه هکری لازاروس به عنوان یکی از پرکارترین گروه‌های هکری رمزارز جهان بود که در کره شمالی فعالیت دارند.
در سال ۲۰۲۱ هم هکرها طی حمله‌های سایبری مختلف رقمی حدود ۳٫۳میلیارد دلار ارز دیجیتال سرقت کردند.

یک سناریوی ۳٫۵تریلیون دلاری

میزان نگرانی از بغرنج شدن وضعیت امنیت سایبری، شرکت های بیمه بزرگ جهان را بر آن داشته تا به شبیه‌سازی حمله‌های بزرگ سایبری در جهان و تخمین زدن میزان خسارات ناشی از آنها در جهان بپردازند و نسبت به آنها هشدار دهند. در همین راستا شرکت بیمه لویدز لندن (Insurance giant Lloyd) به عنوان یکی از غول‌های صنعت بیمه جهان در تازه‌ترین گزارش خود، هشدار داده است که اقتصاد جهانی ممکن است ۳٫۵ تریلیون دلار در نتیجه یک حمله سایبری بزرگ و با هدف قرار گرفتن سیستم‌های پرداخت در دنیا، از دست بدهد.
درواقع این شرکت بزرگ بیمه با توجه به روند روبه رشد حملات سایبری در جهان یک شبکه حمله سایبری فرضی همه‌جانبه را متصور شده که می‌تواند حدود ۳٫۵ تریلیون دلار برای اقتصاد جهان هزینه در بر داشته باشد.
حادثه لویدز شامل شبکه‌ای از حملات سایبری فرضی و بی‌سابقه جداگانه است که همگی به یکباره روی می‌دهند و بر سیستم‌های مستقل متعددی که زیرساخت‌های بازار مالی را تشکیل می دهند، تأثیر می‌گذارند.
در این سناریوی تحقیقاتی آمده است: مهاجمین در طول به‌روزرسانی‌های معمول نرم‌افزار، کدهای مخرب را در بخش‌های مهم نرم‌افزار مورد استفاده صنعت خدمات مالی برای تأیید تراکنش‌ها و تأیید پرداخت‌ها نصب می‌کنند.
این به‌روزرسانی به ده‌ها هزار شبکه شریک و مشتری ارسال می‌شود و همزمان به همگی آنها نفوذ می‌کند.
این موضوع به مهاجمان اجازه می‌دهد با ایجاد یک در پشتی نفوذ بزرگی را آغاز کنند، به این ترتیب مشتریان برای پرداخت هزینه کالاها دچار مشکل می‌شوند و خدماتی همچون وام‌دهی و تسویه وام‌ها در بانک‌ها متوقف می‌شود.
طبق این سناریو، هکرها با تغییر داده‌های در اختیار، می‌توانند وجوه را به شبکه‌ای از حساب‌های تحت کنترل خود هدایت کنند.
درواقع این تحقیق، سناریوهای فرضی (اما قابل قبول) را بررسی می‌کند و به این نتیجه می‌رسد که چنین حمله‌ای بیشترین آسیب را به امریکا و پس از آن چین و ژاپن وارد خواهد کرد.

سدی مقابل هکرها با چند راهکار ساده

بسیاری ادعا می‌کنند که حملات سایبری رخ خواهند داد و هیچ راهی برای اجتناب از آنها وجود ندارد بنابراین تنها کاری که باید انجام شود، سرمایه‌گذاری در فناوری‌هایی است که حمله را پس از نفوذ به شبکه، شناسایی کرده و آسیب را کاهش می‌دهند اما محققان معتقدند این بهترین راهکار نیست و باید راهکار پیشگیری را به جای شناسایی انتخاب کرد. با محافظت مؤسسات و کاربران در برابر حمله‌های سایبری، نه‌تنها می‌توان حملات را مسدود کرد، بلکه می‌توان مانع آنها شد.
آموزش و آگاهی: آموزش و آگاهی سایبری یکی از مهم‌ترین راهکارها برای مقابله با هکرها و قربانی نشدن است.
آموزش مکرر و آگاهی‌رسانی می‌تواند به کاربران کمک کند که کمتر در دام مجرمان سایبری بیفتند .
مؤسسات باید به کارکنان خودآموزش دهند که هرگز روی لینک‌های ناشناس کلیک نکنند چراکه ممکن است حاوی فایل‌های مخرب باشند و با این کار عملاً همه اطلاعات و داده‌های شخصی، علمی و مالی خود را تقدیم هکرها کنند.
افراد باید آموزش ببینند که قبل از دانلود هر نرم‌افزاری از امن بودن آن اطمینان حاصل کنند و این بارگذاری را تنها از فروشگاه‌های معتبر انجام د هند .
همچنین کاربران باید مراقب باشند و هرگز یک USB ناشناخته را به رایانه خود متصل نکنند چراکه ممکن است حاوی بدافزارها یا باج‌افزارهایی باشد که آنها را به دردسر بیندازد.
توجه به آپدیت‌ها: یکی دیگر از مهم‌ترین موارد امنیتی، توجه به آپدیت‌های نرم‌افزارها و سیستم‌های عامل است.
به روز نگه داشتن رایانه‌ها و سرورها و اعمال وصله‌های امنیتی، بویژه مواردی که برچسب حیاتی دارند، می‌تواند به محدود کردن آسیب‌پذیری سازمان‌ها در برابر حملات سایبری کمک کند.
کاربران باید نرم‌افزار خود را به‌روز نگه دارند چراکه مهاجمان گاه یک نقطه ورودی در برنامه‌ها و نرم‌افزارها پیدا و از این آسیب‌پذیری‌ها استفاده می کنند .
برخی از توسعه دهندگان، فعالانه به دنبال یافتن آسیب‌پذیری‌های جدید و اصلاح آنها هستند بنابراین همیشه باید از به‌روزرسانی‌ها استقبال شود.
تقویت احراز هویت کاربر: مجرمان سایبری معمولاً از پروتکل دسکتاپ از راه دور (RDP) و ابزارهای مشابه برای دسترسی به سیستم‌های یک سازمان و سرقت داده‌ها استفاده می کنند .
مهاجم می‌تواند پس از ورود به دستگاه، باج‌افزار را روی دستگاه اجرا کند، درحالی که کاربر با احراز هویت قوی می‌تواند سدی مقابل این حمله باج‌افزاری ایجاد کند.
احراز هویت چند عاملی می‌تواند به کاربران کمک کند تا طعمه هکرها نشوند.