FARAASAT NEWSLETTER

فراست

خبرنامه امنیت سایبری

شماره ۹۹/۱

- پرواز ابدی بوینگ ۷۳۷ اوکراینی از منظر سایبر الکترونیک
- چگونه از خودمان در شبکه‌های اجتماعی مراقبت کنیم
- اهمیت آموزش مداوم کارمندان در زمینه امنیت سایبری
- پیامدهای ویروس کرونا بر امنیت سایبری کشور
- سال۲۰۲۰ و تهدیدهای سایبری پیش رو

SOPHOS

SOPHOS XG Firewall

Xstream

محافظت از شبکه

هیچ چیز از دید سوفوس پنهان نیست. با کنترل تمامی بسته‌ها، سوفوس توانایی شناسایی و جلوگیری از پیچیده‌ترین حملات را داراست.

امنیت شبکه‌های بیسیم

شبکه‌های وایرلس یکی از هدف‌های محبوب هکرهاست. سوفوس با ایجاد یک شبکه وایرلس کد شده و امن اجازه ورود به هیچ هکری را نمی‌دهد.

محافظت از کاربران وب

زمانی که کاربران یک سازمان در وب مشغول کاوش هستند، عملا در یک جنگل وحشی گام برمی‌دارند. سوفوس در این جنگل محافظ کاربران شماست.

محافظت به روش طوفان شن

در نسل جدید UTMهای Sophos، شما یکی از قویترین ابزارهای شناسایی حملات را در اختیار دارید. این قابلیت با آنالیز رفتارهای مشکوک، جدیدترین بدافزارها را شناسایی و معدوم می کند. این روش یکی از بهترین روش‌ها برای جلوگیری از ورود باج‌افزارهاست.

امنیت ایمیل سرور

همه‌ی ما با حملات علیه ایمیل سرورها دست و پنجه نرم کرده‌ایم.با آسایش یک ایمیل سرور پاک را تجربه کنید. از این به بعد سوفوس با آنتی اسپم و آنتی ویروس و سایر امکانات امنیتی قدرتمند خود در مقابل این حملات قرار می‌گیرد.

محافظت از وب‌سرورها

وب سرورها طعمه‌هایی لذیذ برای هکرها هستند. از آنجا که معمولا وب‌سرورها در ناحیه DMZ قرار دارند، شناسایی، دسترسی و حمله به آن‌ها بسیار ساده‌تر است. سوفوس با شناسایی حملات تا لایه Application محافظی مطمئن برای وب‌سرورهای شماست.

---

www.ParsAvan.com

(۰۲۱) ۹۱۰۰۵۴۱۸

Sales@ParsAvan.com

axigen

ایمیل سرور اَکسیژن

امکان مهاجرت ساده

کلیه اطلاعات و فولدرهای کاربران از دیگر ایمیل سرورها از جمله Exchange و MDaemon در کمتر از چند دقیقه قابل انتقال است.

محیط کاربری جذاب آسان

بهره گیری از Webmail زیبای **فارسی** AJAX در کنار پشتیبانی از **تقویم هجری شمسی** و دارا بودن Outlok Connector محیط نرم افزار را بسیار جذاب و کاربر پسند نموده است.

پشتیبانی حرفه ای

کارشناسان فنی ۲۴ ساعته از تهران و رومانی به صورت تیکت و تلفنی پشتیبان شما هستند.

پایداری بسیار بالا

ایمیل سرور اَکسیژن علاوه بر بهینه بودن استفاده از منابع و پایداری عالی با دارا بودن قابلیت‌های Clustering و High Availability یک ایمیل سرور مطمئن و همیشه دسترسی برای شما خواهد بود.

امنیت فوق العاده بالا

در ایمیل سرور اَکسیژن از لایه ی امنیتی فوق العاده قوی استفاده شده است. علاوه بر این قابلیت تلفیق با آنتی ویروسهای تجاری و مشهور جهان از جمله Bitdefender ،Cyren و Kaspersky امکان پذیر می باشد.

مدیریت ساده

مدیریت تحت وب کاربرپسند همراه با امکانات و ویژگیهای فوق العاده از مشخصات اسیجن است. ضمن اینکه قابلیتهای گروهی زیاد موجود در اَکسیژن باعث شده تا این ایمیل سرور به عنوان جایگزین قدرتمند MS Exchange مطرح باشد.

نمایندگی رسمی در ایران

نام شرکت «پارس آوان رایان» به عنوان نماینده رسمی و انحصاری این ایمیل سرور در ایران و در سایت اَکسیژن www.axigen.com ثبت شده است. لایسنسها در کشور رومانی و بنام خریدار صادر می شوند و مشتریان می توانند از طعم لذت بخش استفاده از محصولات قانونی بهره مند گردند.

www.ParsAvan.com

(۰۲۱) ۹۱۰۰۵۴۱۸

Sales@ParsAvan.com

رسید مژده که ایّام غم نخواهد ماند چنان نماند چنین نیز هم نخواهد ماند

خوانندگان گرامی
سلام و درود

سال ۱۳۹۸ گذشت با خاطراتی تلخ و شیرین و در آستانه‌ی سالی قرار گرفتیم که زندگی نه تنها مردم کشور عزیزمان ایران بلکه کل مردم جهان متأثر از کرونا یک ویروس به احتمال زیاد ساخته‌ی دست بشر گردیده است، ویروسی که اگر چه هنوز منشاء آن رسما اعلام نشده اما شباهت‌های بسیاری با ویروس‌های کامپیوتری ساخته‌ی بشر با اهداف خاص همچون استاکس‌نت دارد.
از منشاء این ویروس هولناک که بگذریم این موضوع، علاوه بر روشن ساختن نیاز به تقویت بیشتر پدافندهای زیستی، لزوم توجه خاصی به فناوری اطلاعات به عنوان ابزاری مؤثر در جهت کمک به حل این چنین بحران‌هایی را بیش از پیش نمایانگر می‌کند. چه در زمینه‌ی هوش مصنوعی که چین از آن برای یافتن افراد مشکوک به ویروس بهره جست، چه برنامه‌های رایانه‌ای برای مدیریت و توزیع کمک‌های پزشکی، چه زیرساخت‌های لازم برای پرسنلی که به اجبار از منزل و به صورت دورکاری مشغول فعالیت می‌گردند.
اگر چه آغاز سال ۱۳۹۹ شمسی خوشآیند نیست ولیکن امیدواریم که با مدیریت صحیح و همکاری همه‌ی مردم فهیم کشورمان و در ذل رهنمودهای مقام معظم رهبری (مدظله) و با برچیده‌شدن هر چه سریعتر این ویروس منحوس سالی شاد و پر از برکت را برای کلیه هم‌میهنان و نیز مردم کل دنیا شاهد باشیم.

با احترام
محسن عزیزی‌پور
شرکت پارس آوان رایان

۹۹/۱

خبرنامه امنیت سایبری فراست

فهرست

لزوم آگاهی بخشی امنیت سایبری

لزوم آگاهی‌بخشی امنیت سایبری به کارکنان

لزوم آگاهی‌بخشی امنیت سایبری به کارکنان

شرکت‌ها و سازمان‌ها همیشه در معرض تهدیدهای سایبری قرار دارند و با گسترش خدمات سازمانی مبتنی بر اینترنت و فضاهای ابری، این تهدیدها پیشرفته‌تر نیز شده‌اند. امنیت سازمان به راحتی می‌تواند به واسطه عوامل مختلفی از جمله خطای انسانی به خطر بیافتد. بنابراین اگر کارکنان سازمان به اندازه کافی آگاه نبوده یا هشدارهای لازم را به موقع دریافت نکرده باشند می‌توانند باعث به خطر افتادن اطلاعات حیاتی سازمان شوند.

تهدیدهای حوزه سایبری همه‌گیر هستند و داده‌های هیچ فردی مخصوصاً شرکت‌ها و سازمان‌های تجاری نمی‌تواند از این قاعده مستثنی باشد. این موضوع دارای اهمیت است که با وجود سیاست‌های امنیتی سازمان در سطوح بالادستی و انجام اقدام‌های لازم برای بهبود زیرساخت‌های امنیتی، درصد بالایی از تخلفات امنیت سایبری و تهدیدهای آن برای سازمان به دلیل خطای نیروهای انسانی است. بنابراین اگر عامل انسانی به اندازه کافی آگاهی و مهارت‌های لازم را نداشته باشد می‌تواند شکاف قابل توجهی را در راهبرد دفاعی سازمان به وجود آورد.

چرا آگاهی‌بخشی در مورد امنیت سایبری در سازمان اینقدر مهم است؟

تحقیقات نشان می‌دهد ۹۵ درصد از تهدیدهای امنیت سایبری به دلیل خطای انسانی است. سازمان‌هایی که در حال حاضر می‌توانند اعلام کنند آماده دفاع در برابر حملات سایبری پیشرفته‌اند، اندک هستند. آمارها نشان می‌دهد که در طول یک سال گذشته، درصد بالایی از سازمان‌ها اعلام کرده‌اند که حداقل یک یا چند حمله و تهدید را تجربه کرده‌اند.

عامل انسانی یعنی همان کارمندان شما در سازمان، اولین حلقه در حوزه امنیت سایبر هستند و این حلقه از دید مهاجمان سایبری مخفی نمانده است. مجرمان سایبری می‌دانند که ساده‌ترین راه برای دسترسی به داده‌های شبکه‌های سازمانی ایمن یا سرقت داده‌های آنها، هدف قرار دادن افرادی است که امکان ورود به سیستم و اطلاعات مهم دیگر را دارند. بنابراین شرکت‌ها و سازمان‌ها نمی‌توانند از اهمیت اصلی آموزش کارکنان خود در مورد تهدیدها و شیوه‌های مواجهه با آن غافل شوند. از این‌رو باید بررسی شود کارمندان شرکت یا سازمان شما در برابر تهدیدهای سایبری، هکرهای مخرب یا کشورهایی که قصد سرقت داده‌ها، اطلاعات یا خدمات با ارزش دیگر را دارند، چقدر مقاوم بوده و از دانش کافی برخوردار هستند؟

مهمترین خطرهایی که می‌تواند امنیت سایبری سازمان را تهدید کند، روش‌ها و ابزارهایی مانند فیشینگ، بدافزارها، باج‌افزارها، مهندسی اجتماعی و استفاده از هوش مصنوعی در این روش‌ها است. بدون آگاهی‌بخشی و فرهنگ‌سازی در سازمان برای آگاهی از امنیت سایبری و مطلع کردن کارکنان از چگونگی امکان جاسوسی از سیستم‌ها، همه سیستم‌ها و اطلاعات با ارزش شما، با استفاده عمدی یا غیرعمدی از همان روش‌ها یا ابزارها با فریب کارمندان توسط مهاجمان، در معرض خطر خواهند بود.

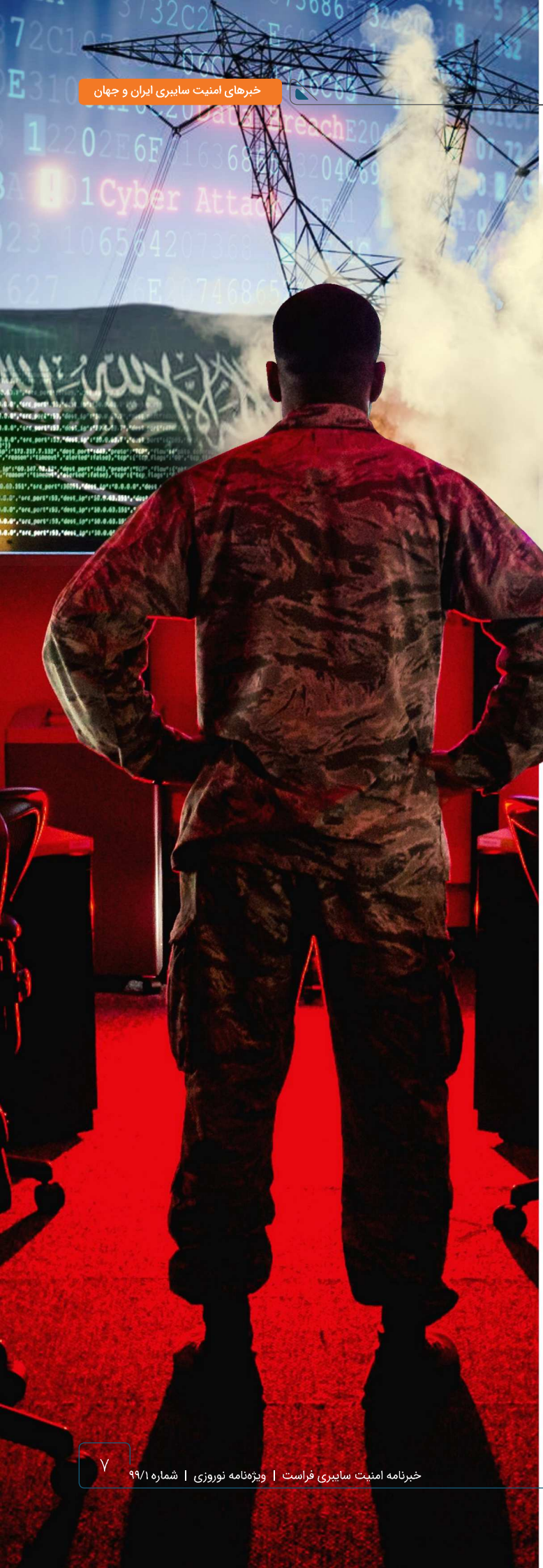
کدام طیف از کارمندان شما باید دوره‌های آگاهی‌بخشی و آموزش را بگذرانند؟

با توجه به این که کارمندان سازمان، اولین و اصلی‌ترین خط دفاعی شما در برابر این تهدیدها هستند، بنابراین هر کارمندی که به یک رایانه یا گوشی هوشمند مرتبط با کار خود در سازمان دسترسی داشته باشد باید آموزش‌ها و آگاهی‌بخشی‌ها را در خصوص امنیت سایبری ببیند.

با آگاهی‌بخشی و آموزش امنیت سایبری برای همه کارمندان می‌توان احتمال کلاهبرداری یا حمله اینترنتی را به کمترین سطح ممکن رساند.

خبرهای امنیت سایبری ایران و جهان

- امنیت سایبری ایران در سال ۹۸
- گزیده رخدادهای امنیت سایبری ایران در سال ۹۸
- گزیده اخبار امنیت سایبری جهان در سال ۹۸
- باگ‌های امنیتی محصولات سایبری در سال ۹۸



امنیت سایبری ایران در سال ۹۸

دروغ‌پراکنی سایبری بر ضد ایران، حمله به تأسیسات برق عربستان

در خردادماه ۹۸ موج تازه‌ای از اتهام‌ها بر ضد ایران، تحت عنوان حمله سایبری ایران به تأسیسات برق عربستان سعودی در پی قطع برق در برخی از مناطق این کشور به راه افتاد. همزمانی این خبر با اجلاس مکه و بیانیه‌ای که علیه جمهوری اسلامی ایران در این نشست منتشر شد، خوراک تبلیغاتی رسانه‌های معاند به خصوص یک کانال مجهول‌الهویه تلگرامی را فراهم کرد.

بر اساس شواهد به دست آمده در خبرگزاری‌های معتبر جهان، قطعی برق در عربستان سعودی، حتی اگر جنبه خرابکارانه نیز داشته باشد، ریشه سایبری ندارد و سند مستحکم و متقنی نیز در مورد دخالت ایران در اقدام‌های خرابکارانه فیزیکی نیز در این زمینه وجود ندارد؛ کما این که جمهوری اسلامی ایران، همواره به قوانین و هنجارهای بین‌المللی در زمینه احترام به حاکمیت کشورها، معتقد بوده و خود را ملزم به رعایت حقوق بشر در تمامی سطوح می‌داند. بر این موضوع نیز باید تأکید کرد که ایران برای پاسخ به اقدام‌های رژیم سعودی و هم‌پیمانان منطقه‌ای این کشور، راه‌حل‌های قانونی و متعارف بسیاری در دست دارد که اجرای هر کدام از آنها قطعاً سعودی‌ها را مستأصل خواهد کرد و همین مسأله، ایران را از به‌کارگیری راه‌حل‌های غیرمتعارف و خارج از شئون بین‌المللی بی‌نیاز خواهد کرد.

آمریکا آغازگر جنگ سایبری علیه ایران

در مهرماه ۹۸، محمد جواد ظریف وزیر امور خارجه کشورمان در گفتگو با شبکه خبری ان‌بی‌سی آمریکا در خصوص جنگ سایبری دو کشور و دخالت سایبری ایران در انتخابات آمریکا گفته است: «ما در امور داخلی کشور دیگری دخالت نمی‌کنیم اما جنگی سایبری بین ایران و آمریکا وجود دارد و در جریان است».

در جریان این مصاحبه، همچنین وزیر امور خارجه کشورمان گفته است: «ایالات متحده، این جنگ سایبری را با حمله به تأسیسات هسته‌ای ما با روش خطرناک و غیرمسئولانه‌ای آغاز کرد که می‌توانست جان میلیون‌ها انسان را بگیرد». آقای ظریف با اشاره به ویروس‌هایی که تأسیسات هسته‌ای ایران را هدف گرفته بودند، افزود: «استاکس‌نت، روز صفر و عملیات المپیک را به یاد بیاورید. لذا یک جنگ سایبری بین ایران و آمریکا وجود دارد و ایران درگیر آن است». وی همچنان تاکید کرده هر جنگی که ایالات متحده آغاز کند، قادر به پایان دادن به آن نخواهد بود.

انتشار آمار آلودگی سایبری ایران در بازه زمانی یکساله توسط مرکز ماهر

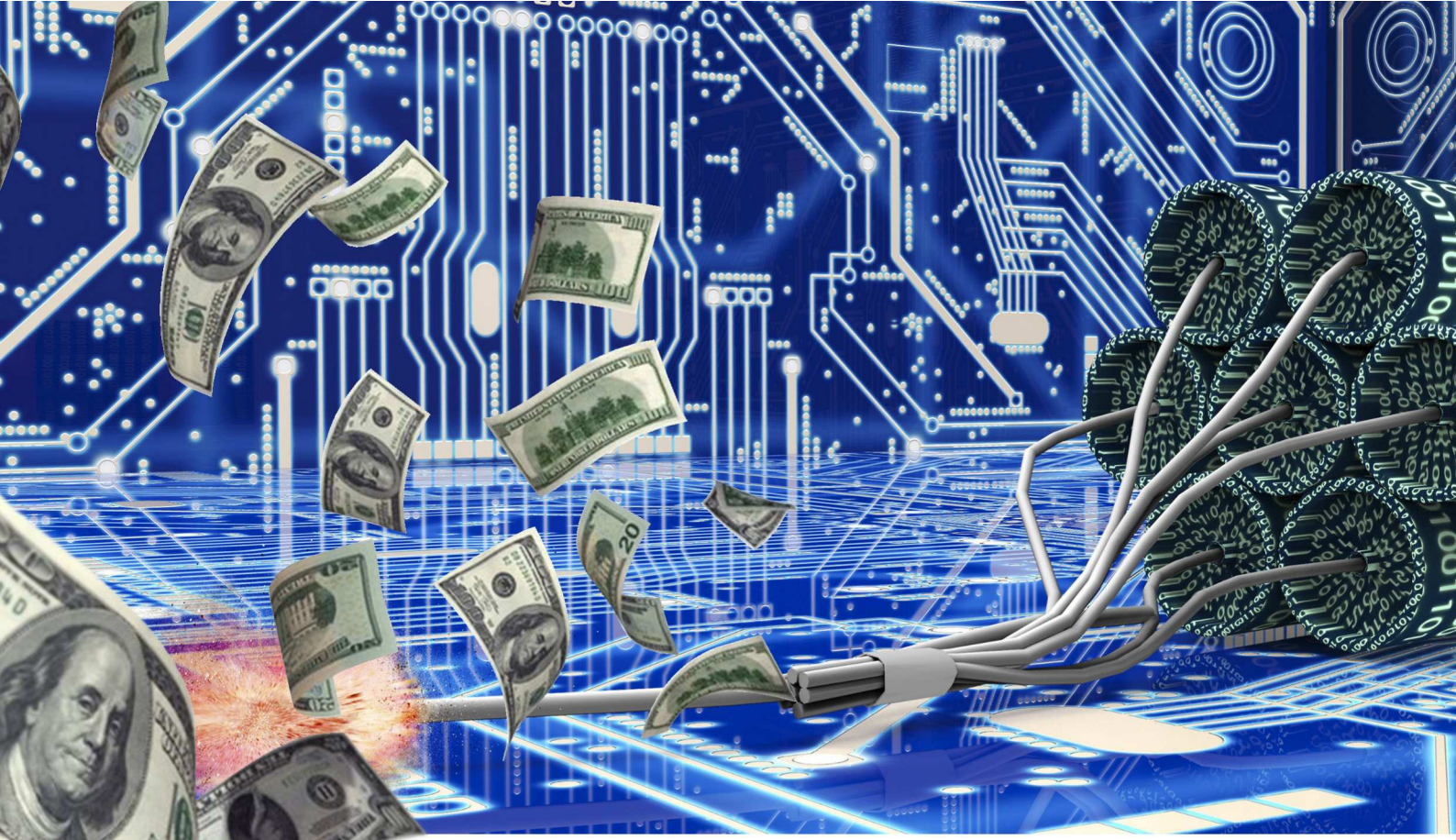
سامانه رصد ماهر وابسته به مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور، در گزارشی تعداد آدرس‌های اینترنتی آلوده کشور که در ۱۲ ماه منتهی به شهریور ۹۸ ثبت شده بودند را منتشر کرد.

بر اساس این آمار، بیشترین باتنت‌ها در مردادماه ۹۸ و کمترین آنها نیز در آبان‌ماه سال ۹۷ رخ داده است. همچنین بیشترین آسیب‌پذیری‌ها مربوط به فروردین‌ماه ۹۸ و کمترین آسیب‌دیدگی در مردادماه رخ داده است. بیشترین آلودگی سایبری، مربوط به تهران و پس از آن اصفهان، گیلان و یزد است. این درحالی است که کمترین آدرس IP آلوده شناسایی شده، مربوط به استان کهگیلویه و بویراحمد با ۱۶۴ مورد IP آلوده است. در این زمینه، استان‌های خراسان جنوبی، سیستان و بلوچستان و زنجان هم در یک ماه اخیر منتهی به شهریور ۹۸، کمترین آدرس‌های IP آلوده را داشته‌اند.

افزایش ۳۰ برابری توان دفاع سایبری کشور

آذری جهرمی، وزیر ارتباطات کشورمان در حاشیه مراسمی که در اردیبهشت‌ماه امسال به مناسبت روز ملی شدن داده‌های دولتی برگزار شد، از سی‌برابر شدن توان دفاع سایبری کشور خبر داد. او گفته بر اساس برآوردهای انجام شده، هم اکنون ۷۰ درصد تجهیزات شبکه مخابراتی کشور به تجهیزات بومی مجهز شده و موفق شده‌ایم ۳۰ درصد از تجهیزات شبکه پهن باند موبایل را در کشور تولید کنیم. همچنین آذری‌جهرمی گفت که ۱۴۲ آزمایش برای راستی‌آزمایی استقلال شبکه ملی اطلاعات در صورت قطع اینترنت انجام شده که این آزمایش‌ها موفق بوده و ما برآورد می‌کنیم که در برابر تهدیدها می‌توانیم مقابله کنیم.

وی با بیان این که ظرفیت امنیت شبکه ملی اطلاعات ۳۰ برابر افزایش پیدا کرده است، تصریح کرد: «مصرف اینترنت داخلی از طریق شبکه ملی اطلاعات افزایش پیدا کرده‌است که ما شاهد ۸۰ برابر شدن کیفیت دسترسی به ارتباطات داخلی نسبت به سایت‌های خارجی هستیم».



گزیده رخدادهای امنیت سایبری ایران در سال ۹۸

حمله سایبری به سامانه‌های ارزی کشور

در اواخر شهریورماه ۹۸ بود که حمله سایبری به برخی وب سایت‌های عرضه کننده ارز دیجیتال کشور، از جمله سامانه ارزجو انجام شد. اگر چه متخصصان، سازوکارهایی که برای مقابله با این حملات در نظر داشتند را بر روی سامانه ارزجو پیاده‌سازی کردند اما تعداد حملات و گستردگی آنها به قدری بود که برای کاهش بار سرورها، از سرویس‌های تشخیص منابع حمله استفاده کردند. این حملات از نوع حملات گسترده DDoS لایه ۷ با ظرفیتی معادل ۲۰ برابر میانگین حملات در سطح جهان، به سایت ارزجو انجام شد.

در پی این حمله، سایت‌های excoino.com و avalpardakht.com نیز درگیر حملات DDoS شدند اما هیچکدام به قدرت حملاتی که به arzjoo.com انجام شد، نبود. البته این دو سایت نیز از خدمات ابری استفاده می‌کردند و مشکل خاصی برایشان به وجود نیامد. بیشتر این حملات، از کشورهای روسیه، اکراین و قزاقستان صورت پذیرفته بودند.

گسترده‌ترین حملات به زیرساخت‌های کشور

نیمه دوم بهمن‌ماه ۹۸ بود که گسترده‌ترین حمله تجربه شده در تاریخ ایران بر ضد زیرساخت‌های کشور انجام گرفت. به گفته مسئولان شرکت ارتباطات زیرساخت ایران، پیش از این تاکنون چنین حمله‌ای نظیر نداشته است.

حمید فتاحی، معاون وزیر ارتباطات و رئیس هیأت مدیره و مدیرعامل شرکت ارتباطات زیرساخت در پستی در توییتر اعلام کرد که هکرهای اجاره‌ای، گسترده‌ترین حمله تجربه شده در تاریخ ایران را علیه زیرساخت‌های کشور اجرا کردند. آنها از میلیونها مبدأ شبکه زیرساخت را هدف دادند و با حمله SYN flood با نرخ ۱۸۰ میلیون PPS به دنبال اختلال سراسری در شبکه اینترنت ایران هستند. وی همچنین اعلام کرد که به دلیل حمله جلوگیری از سرویس توزیع شده، اینترنت برخی اپراتورهای همراه و ثابت برای مدت یک ساعت با اختلال مواجه شد که با مداخله سپر دژفا و تلاش همکاران شرکت زیرساخت، اختلالات برطرف گردید.

خواندن افکار و امکان نقض محرمانگی افراد

تصور این که شخصی بتواند با استفاده از ابزار و فناوری، افکار شما را تشخیص دهد یا بتواند روی تصمیم‌گیری‌های مغز شما تأثیرگذار باشد واقعاً هراس‌انگیز است. با این وجود، فعلاً جای نگرانی نیست، چون هنوز تا آن زمان راه درازی باقی مانده است. امروزه خوانش مغز با دو روش تهاجمی و غیرتهاجمی انجام می‌گیرد. در روش تهاجمی، با استفاده از اعمال جراحی کوچکی بر روی مغز، ارتباط مستقیمی بین نورون‌های مغزی و الکترودهای دستگاه پزشکی برقرار می‌شود و از این طریق امکان دریافت سیگنال‌های الکتریکی از نورون‌ها و امکان ارسال سیگنال‌های محرک به آنها وجود دارد. در حال حاضر از این روش برای درمان معلولیت‌های جسمی و نقص عضو استفاده می‌شود و پیشرفت‌های خوبی را هم شاهد بوده‌ایم. این روش با توجه به نیاز به جراحی، تا حدی خطر دارد و به همین دلیل صرفاً اشخاصی که دارای معلولیت هستند خطر عوارض جراحی آن را می‌پذیرند.

در روش غیرتهاجمی، امواج خروجی از سطح جمجه فرد، یعنی از روی پوست سر با نصب حسگرهای EEG جذب می‌شود. امواج مغزی پس از جذب، مورد تحلیل قرار گرفته و با استفاده از روش‌های هوش مصنوعی مانند یادگیری ماشین تشخیص داده می‌شوند. البته روش غیرتهاجمی نسبت به روش‌های تهاجمی دقت پایین‌تری دارند و انتظار می‌رود در آینده با پیشرفت الگوریتم‌های هوش مصنوعی این دقت افزایش پیدا کند.

متلاشی شدن شبکه سایبری جاسوسی سیا توسط ایران

علی شمخانی، دبیر شورای عالی امنیت ملی کشورمان در خردادماه ۹۸، پیش از عزیمت به کشور روسیه برای حضور و سخنرانی در دهمین اجلاس بین‌المللی نمایندگان عالی امور امنیتی کشورهای جهان، در گفت‌وگو با خبرنگار خبرگزاری صداوسیما از کشف و نابودی یکی از پیچیده‌ترین شبکه‌های سایبری سازمان سیا که در حوزه جاسوسی سایبری به کار گرفته می‌شد، از سوی دستگاه‌های اطلاعاتی ایران خبر داد. وی افزود: «بخش مهمی از ظرفیت‌های عملیاتی سیا در کشورهای هدف آمریکا با کشف این شبکه از سوی دستگاه‌های اطلاعاتی ایران کاملاً نابود شد».

آقای شمخانی همچنین گفت: «با توجه به همکاری جاری میان ایران و بسیاری از کشورهای جهان در قالب ایجاد «شبکه ضدجاسوسی بین‌المللی» بر ضد آمریکا، ما اطلاعات شبکه کشف شده را که در چند کشور دیگر نیز فعال بود در اختیار شرکایمان قرار دادیم که منجر به شناسایی و فروپاشی شبکه افسران اطلاعاتی سیا و دستگیری تعدادی از جاسوسان و مجازات آنها در کشورهای مختلف شد». وی اظهار داشته که آمریکایی‌ها با اعتراف به پیروزی ایران، این اقدام ایران را « شکست مفتضحانه اطلاعاتی» نام‌گذاری کرده‌اند.

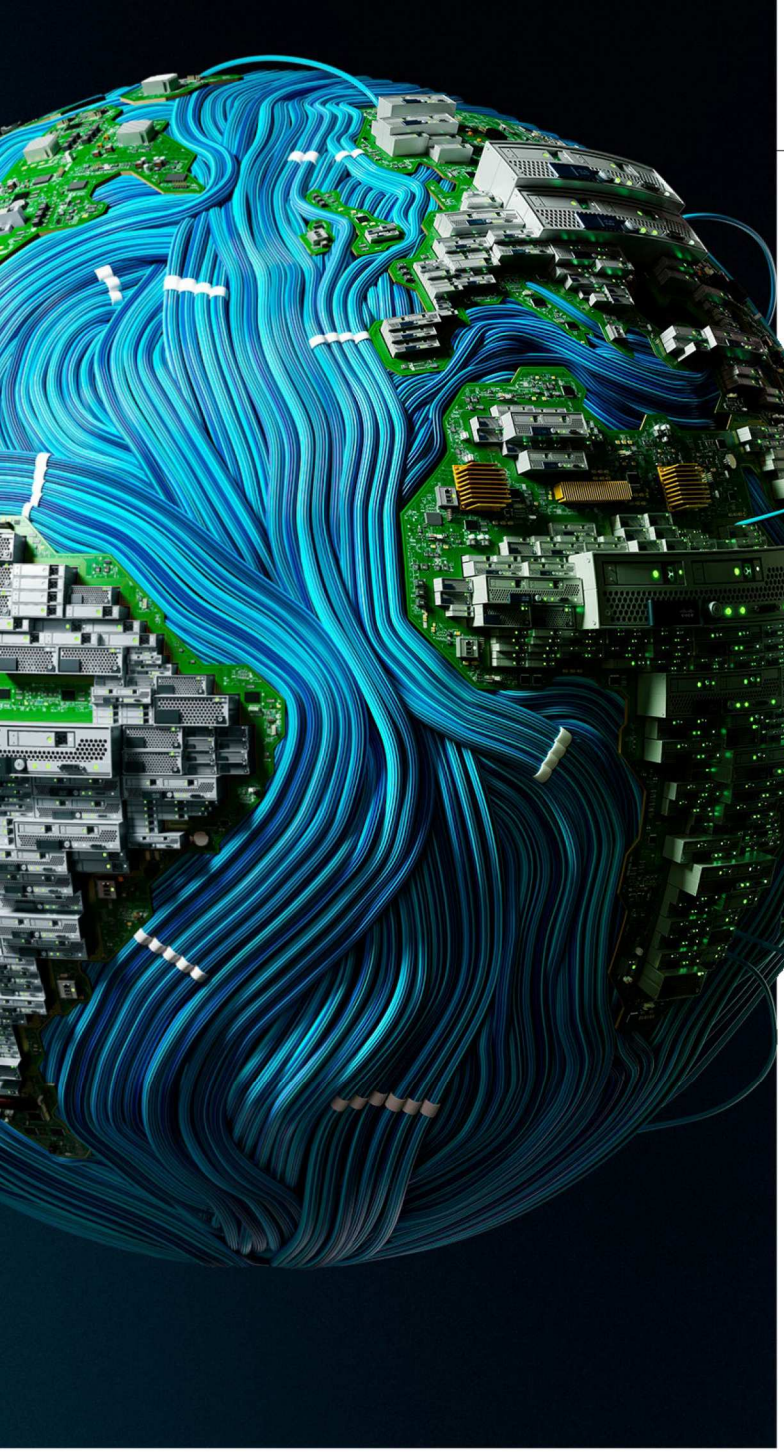
استفاده هکرها از ویروس کرونا برای سرقت اطلاعات افراد

پس از هشدار سازمان بهداشت جهانی در مورد ویروس کرونا و نگرانی عمومی از شیوع این ویروس در کشورهای دیگر، در بهمن‌ماه ۹۸ بود که لینک‌هایی حاوی خبرها یا ویدیوهایی درباره شیوع ویروس کرونا در قالب فایل‌هایی مانند فایل‌هایpdf و mp۴ منتشر شد که دارای بدافزار بودند. هکرها با استفاده از فضای نگرانی عمومی ایجاد شده، کاربران را ترغیب به باز کردن این فایل‌ها در رایانه یا تلفن همراه خود می‌کردند. سپس از طریق بدافزارهای نهفته در این فایل‌ها، به اطلاعات ذخیره شده در دستگاه کاربر دسترسی پیدا کرده یا آنها را مسدود، تخریب یا کپی می‌کردند.

کارشناسان امنیت سایبری هشدار داده‌اند که این لینک‌ها دارای کدی هستند که برای سرقت اطلاعات شخصی افراد ساخته شده است. بنابراین کاربران برای اجتناب از این بدافزارها، لازم است اطلاعات و خبرها را از منابع رسمی دریافت کرده و به پسوند فایل‌های دریافتی نیز توجه بیشتری کنند. گفتنی است ویروس کرونا نخستین‌بار ۱۲ دسامبر در شهر ووهان چین شناسایی شده است.

فاش شدن اطلاعات شخصی ۲۶۷ میلیون کاربر فیسبوک

در دی‌ماه ۹۸، باب دیاچنکو از محققان امنیت سایبری، در وب سایت Comparitech از وجود پایگاه داده‌ای خبر داد که در آن، اطلاعات بیش از ۲۶۷ میلیون نفر از کاربران شبکه اجتماعی فیسبوک شامل ID، شماره تلفن و نام آنها وجود داشت. چنین پایگاه داده‌ای امکان استفاده از این اطلاعات را برای ارسال پیام‌های هرزنامه و فیشینگ توسط مهاجمان فراهم می‌کند. در سال‌های اخیر، فیسبوک بارها با مشکلاتی در زمینه امنیت و حریم خصوصی کاربرانش مواجه شده است و این نخستین‌بار نیست که شاهد انتشار چنین خبرهایی درباره این شبکه اجتماعی پرمخاطب هستیم.

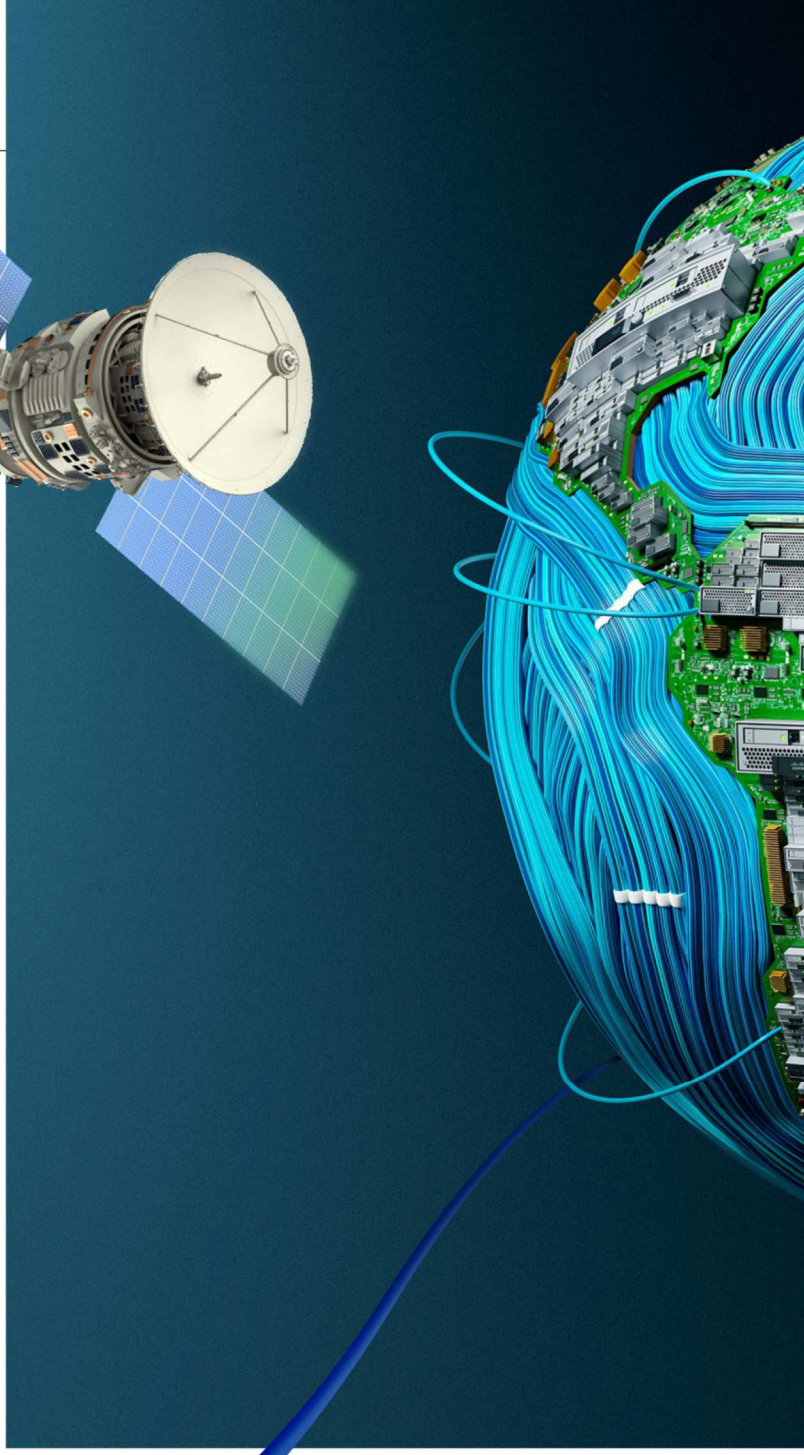


گزیده اخبار امنیت سایبری جهان در سال ۹۸

استفاده آمریکا از شرکت کریپتو برای جاسوسی از پیام‌های محرمانه و رمزنگاری کشورهای دیگر

بیش از ۱۲۰ کشور جهان در طول سال‌های زیادی از شرکت سوئیسی کریپتو که به Crypto AG شناخته می‌شود، تجهیزات و فناوری‌های رمزنگاری خریداری می‌کردند و هیچ کدام از این کشورها هم نمی‌دانستند که این شرکت در واقع تحت مالکیت محرمانه آژانس اطلاعاتی آمریکا موسوم به CIA قرار دارد. شرکت کریپتو در واقع طی یک قرارداد طبقه‌بندی شده با سازمان‌های اطلاعاتی آلمان غربی، به مالکیت CIA درآمده است. آژانس‌های اطلاعاتی، دستگاه‌های این شرکت را دستکاری می‌کردند تا با سوءاستفاده از آنها بتوانند پیام‌های رمزنگاری شده کشورهای دیگر را به آسانی رمزگشایی کنند؛ حتی پیام‌های محرمانه‌ای که میان جاسوس‌ها، دیپلمات‌ها، مقام‌های سیاسی و سربازهای این کشورها رد و بدل می‌شده است.

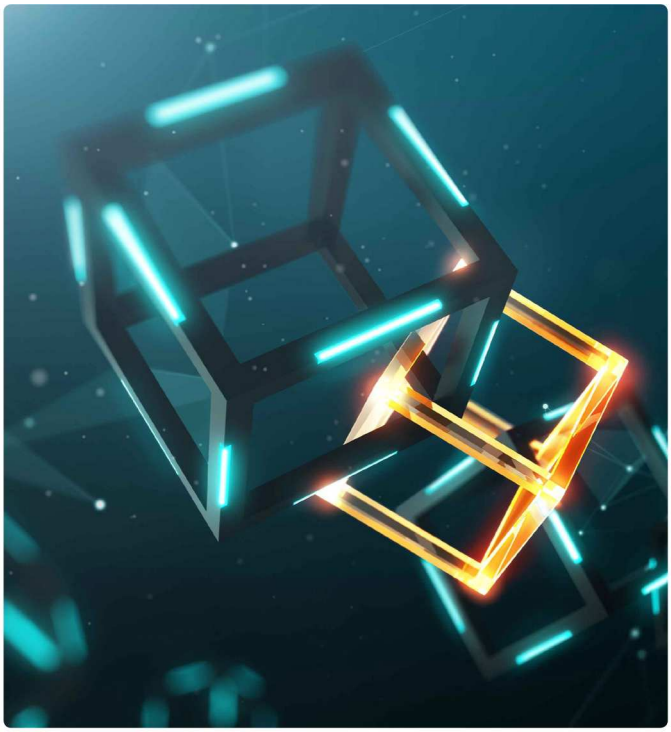
اسناد محرمانه نشان می‌دهد ایالات متحده با همکاری کریپتو از کشورها هزینه دریافت می‌کردند و هم زمان، اطلاعات‌شان را نیز سرقت می‌کردند. بنابراین این کشورها مجوز خواندن محرمانه‌ترین ارتباط‌های خود را حداقل به دو کشور می‌دادند. در این میان، رقبای آمریکا مانند روسیه و چین به دلیل نگرانی و شک عمیقی که از ارتباط با مقام‌های غربی داشتند هرگز مشتری این شرکت سوئیسی نبوده‌اند.



گسترش حملات باج‌افزاری در بین کاربران خانگی

بررسی‌ها نشان دهنده افزایش چشم‌گیر حملات باج‌افزاری در بین کاربران خانگی است. از عمده دلایل گسترش این حملات می‌توان به کلیک بر روی لینک‌های آلوده، دریافت فایل‌های اجرایی مخرب، کرک‌ها و نرم‌افزارهای فعال‌ساز و همچنین ماکروهای آلوده موجود در فایل‌های محصولات ادوبی و آفیس با پسوندهای pdf, doc, ppt و ... توسط کاربران ناآگاه اشاره کرد. برای جلوگیری از آلوده شدن رایانه‌های شخصی و کاربران خانگی و همچنین کاهش آسیب‌های ناشی از حملات باج‌افزاری توصیه می‌شود موارد زیر مورد توجه قرار گیرد:

- تهیه نسخه‌های پشتیبان از اطلاعات ارزشمند و نگهداری آنها به صورت آفلاین
- باز نکردن پیام‌های مشکوک در محیط‌های مختلف از جمله ایمیل، پیام‌رسان‌ها و شبکه‌های اجتماعی
- دانلود نکردن فایل‌های اجرایی از منابع ناشناس، به ویژه کرک نرم‌افزارها خصوصاً فعال‌سازهای ویندوز و محصولات آفیس
- به‌روز نگه داشتن سیستم عامل و آنتی‌ویروس‌ها
- توجه به علایم آلودگی باج افزار از قبیل تغییر پسوند فایل‌ها، پیغام باج‌خواهی، کاهش محسوس سرعت سیستم عامل و سایر موارد اینچنینی.



استفاده از بلاک‌چین برای مقابله با خبرهای دروغین

با آن که فناوری بلاک‌چین از زمان ظهور خود تا به حال هیاهوی خبری زیادی به راه انداخته و انتظارات بیشماری را برای ما ایجاد کرده است اما عملاً تاکنون دستاورد قابل توجهی نداشته و به قولی هنوز در مرحله سرخوردگی به سر می‌برد. هم اکنون به جز چند نمونه محدود در حوزه حمل‌ونقل، کاربرد بیشتری را نمی‌توان برای این فناوری پیدا کرد. البته این سرخوردگی بلاک‌چین به این معنا نیست که شکست خورده است بلکه به دنبال بلوغ اهداف و ادعاهای خود در سرویس‌های مالی، تجارت الکترونیک و بازارهای دیگر است.

از نظر تحلیل‌گران و متخصصان بازار، بلاک‌چین تا پنج سال آینده به بسیاری از اهداف خود در زمینه اشتراک داده و تجارت خواهد رسید. یکی از کاربردهای احتمالی بلاک‌چین که انتظار می‌رود به حقیقت بپیوندد، مقابله با خبرهای دروغین و فناوری Deep Fake- است. پیش‌بینی می‌شود تا سال ۲۰۲۳ میلادی حدود ۳۰ درصد از خبرها و محتواهای ویدیویی در سطح جهان، توسط بلاک‌چین اعتبارسنجی خواهد شد. ردگیری و اثبات منشأ این اخبار از کاربردهای کلیدی است که محققان برای بلاک‌چین متصور شده‌اند.

طراحی کابل USB امنیتی برای حفاظت از لپ‌تاپ در برابر سرقت

تصور کنید در یک محیط عمومی مشغول انجام فعالیت‌های حساس کاری و بانکی خود با لپ‌تاپ هستید و ناگهان لپ‌تاپ شما به سرقت می‌رود. در این حال قفل و رمزنگاری‌های سیستم عامل و لپ‌تاپ شما کمکی به شما برای محفوظ ماندن اطلاعات‌تان نخواهد کرد و ممکن است کل زندگی دیجیتالی شما در دسترس سارقان قرار گیرد.

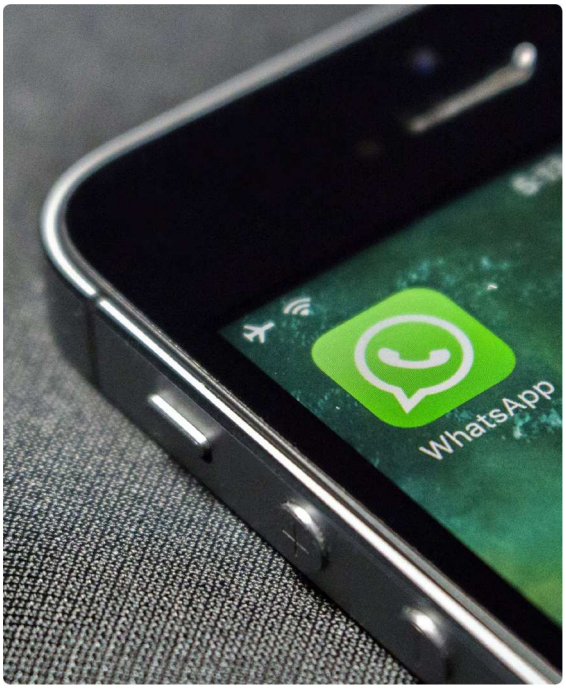
یکی از برنامه‌نویسان اهل سان‌فرانسیسکو به نام مایکل آلتفیلد، راهکار سخت‌افزاری بسیار ساده و کم‌هزینه‌ای را برای حل این مشکل طراحی کرده است. او که نام نوآوری خود را BusKill گذاشته است از قوانین‌نویسی بخش مدیریت نرم‌افزار سیستم عامل لینوکس در موقع خارج شدن قطعه سخت‌افزاری USB استفاده کرده است. در این روش، درایو USB به کابلی متصل می‌شود که یک سر آن به وسیله گیره به لباس شخص وصل می‌شود و در صورت سرقت لپ‌تاپ، قطع کابل بین لباس کاربر و لپ‌تاپ، دستگاه را قفل یا خاموش می‌کند. آلتفیلد این راه‌حل را به خاطر سفرهای زیاد خود و اجبار استفاده از لپ‌تاپ در محیط‌های عمومی طراحی کرده است.

امکان دزدی اطلاعات گوشی در ایستگاه‌های شارژ مکان‌های عمومی

وقتی باتری گوشی شما رو به اتمام است و قصد دارید به ایستگاه‌های شارژ موجود در مکان‌های عمومی مراجعه کنید باید به این نکته توجه داشته باشید که امکان ارسال بدافزار یا دزدی اطلاعات شما از طریق این ایستگاه‌های شارژ وجود دارد.

با توجه به افزایش زیاد گوشی‌های هوشمند و استفاده عموم از کابل‌های USB که همزمان برای شارژ و انتقال داده استفاده می‌شود محققان امنیتی روشی را برای تغییر اتصال USB یافته‌اند که همزمان با شارژ، اطلاعاتی را نیز از گوشی قربانی دریافت خواهد کرد. این روش حمله به گوشی‌های هوشمند، Juice Jacking نامیده می‌شود. در طول سال‌های گذشته، چندین روش حمله هکرها به گوشی‌های هوشمند کشف شده که به عنوان مثال می‌توان به یک تیم تحقیقاتی اشاره کرد که در سال ۲۰۱۶ توانستند بدافزار پیشرفته‌ای را در ایستگاه شارژی تعبیه کنند که قابلیت ضبط فیلم از نمایشگر گوشی را حین اتصال به شارژ داشته باشد. این عملیات با نام Video Jacking شناخته می‌شود. به تازگی نیز پیش‌بینی شده است که هکرها می‌توانند در برخی از ایستگاه‌های شارژ نمونه دارای بدافزار خود را در کنار سایر شارژرها قرار دهند تا بدون جلب توجه اقدام به دزدی اطلاعات کنند. کاربران می‌توانند برای امنیت بیشتر، از کابل‌های USB مخصوصی استفاده کنند که تنها وظیفه انتقال انرژی را بر عهده داشته و پین و اتصالات لازم برای انتقال داده را ندارند. استفاده از پاوربانک هم شیوه امنی برای شارژ در مکان‌های عمومی است.

هک گوشی بعضی از مقام‌های دولتی جهان از طریق اپلیکیشن موبایل واتساپ



منابع خبری رویترز با استناد به تحقیقاتی که در فیسبوک در اوایل سال ۲۰۱۹ میلادی انجام شده است، می‌گویند گوشی‌های تلفن همراه مقام‌های عالی‌رتبه دولتی و نظامی شماری از کشورهای متحد با آمریکا، توسط ابزار خاصی هک شده‌اند. این ابزار خاص که از طریق برنامه کاربردی واتساپ (WhatsApp) به گوشی قربانیان نفوذ کرده است، اطلاعات مقامات عالی‌رتبه حداقل بیست کشور در پنج قاره جهان که همگی آنها از متحدان آمریکا محسوب می‌شدند را مورد هجوم خود قرار داده است. تحقیقات نشان می‌دهد قربانیان بیشتر در ایالات متحده آمریکا و برخی دیگر نیز در امارات متحده عربی، بحرین، مکزیک، پاکستان و هند حضور دارند که به شکلی گسترده مورد حمله نفوذگران قرار گرفته‌اند.

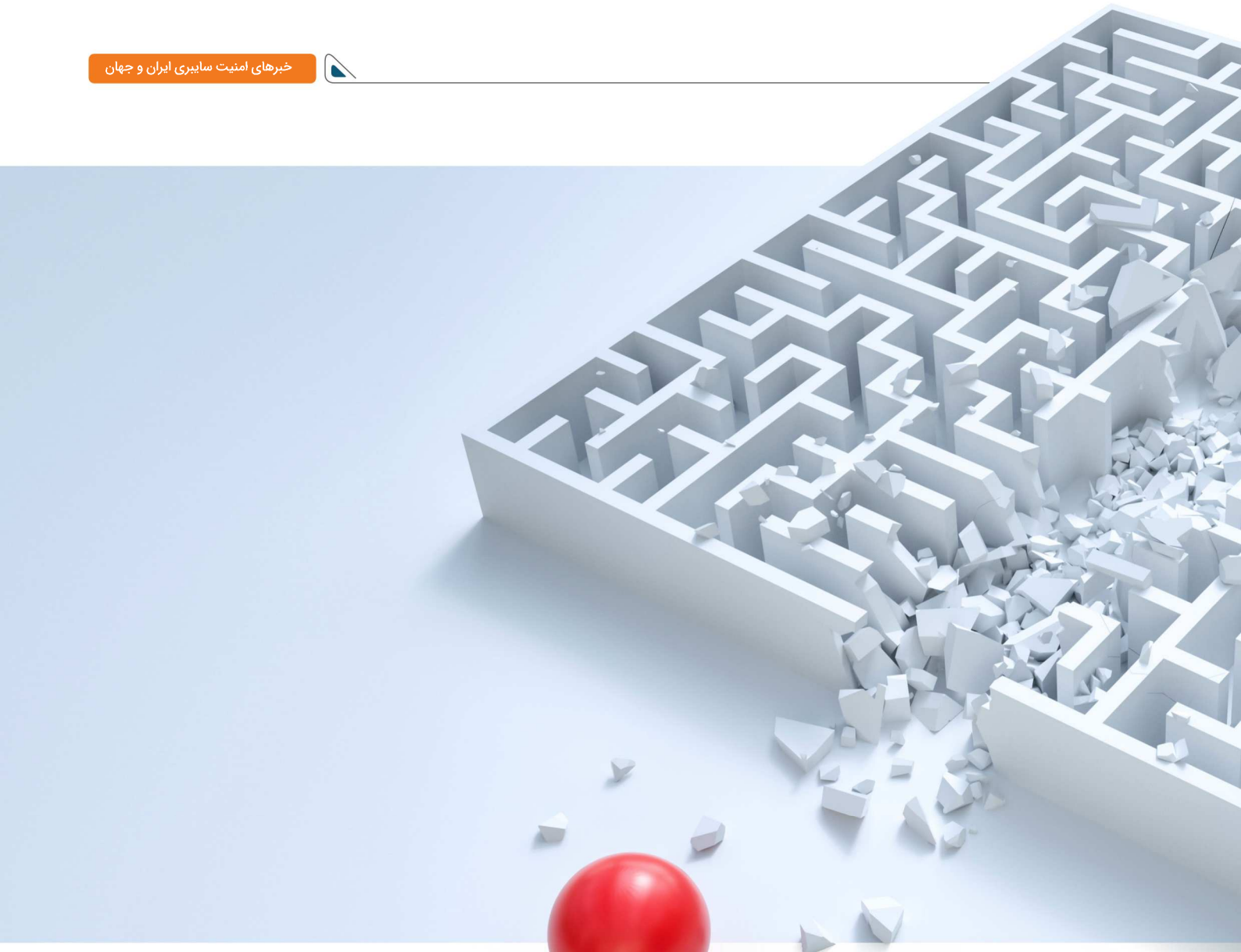
نمایندگان واتساپ معتقدند که NSO Group که یک شرکت اسرائیلی است، عامل اصلی این هک بزرگ می‌باشد. آنها می‌گویند این شرکت اسرائیلی، پلتفرم هک ویژه‌ای تولید کرده و به فروش رسانده است که از طریق آن افراد سودجو توانسته‌اند نفوذپذیری خاصی در واتساپ پیدا کنند. این نفوذپذیری با فعال‌سازی تماس صوتی در واتساپ صورت می‌گیرد و فارغ از این که قربانی به تماس صوتی خود پاسخ بدهد یا ندهد، تلفن هوشمند او به بدافزار جاسوسی و هک آلوده می‌شود.

باگ‌های امنیتی محصولات سایبری در سال ۹۸

وجود آسیب‌پذیری روز صفر در تمامی نسخه‌های phpMyAdmin

در ماه ژوئن سال ۲۰۱۹ شواهد و جزییات کاملی از یک آسیب‌پذیری رفع نشده روز صفر در نرم‌افزار phpMyAdmin، توسط یک محقق امنیت سایبری منتشر گردید. نرم‌افزار phpMyAdmin یک ابزار مدیریتی رایگان و متن‌باز برای پایگاه‌های داده MySQL و MariaDB است که به طور گسترده برای مدیریت پایگاه‌های داده وب سایت‌هایی که با WordPress، Joomla و بسیاری دیگر از بسترهای مدیریت محتوا ساخته شده‌اند، استفاده می‌شود.

این آسیب‌پذیری با شناسه CVE-۲۰۱۹-۱۲۹۲۲ ثبت شده و قابل رهگیری است و از نظر شدت، متوسط رتبه‌بندی شده است؛ اما نباید نسبت به آن بی‌تفاوت هم بود زیرا مهاجم جز دانستن URL سرور قربانی، نیاز به اطلاعات دیگری مانند نام پایگاه داده ندارد و سوءاستفاده از آن راحت است. این نقص، تمامی نسخه‌های phpMyAdmin تا ۴/۹/۰/۱ را که آخرین نسخه از این نرم‌افزار تاکنون است را تحت تأثیر قرار می‌دهد. همچنین این نقص در phpMyAdmin alpha۱-۵/۰/۰ که در ماه جولای سال ۲۰۱۹ منتشر شده است نیز وجود دارد.



کشف ۸ آسیب‌پذیری خطرناک در نرم‌افزار Foxit PDF Reader

۸ آسیب‌پذیری خطرناک در نرم‌افزار Foxit Reader که ابزاری برای خواندن و ویرایش سندهای PDFاست، کشف شده است. این باگ‌ها که البته هم‌اکنون برطرف شده‌اند، بر روی نسخه ویندوز این برنامه وجود داشتند و منجر به اجرای کد دلخواه از راه دور توسط مهاجم می‌شدند. از آنجایی که محبوبیت این ابزار در حدی است که طبق ادعای شرکت تولید کننده این برنامه، در سال گذشته ۴۷۵ میلیون کاربر از آن استفاده کرده‌اند، بنابراین سیستم‌های بسیاری در معرض خطر قرار داشته‌اند. از این‌رو، به کاربران اکیداً توصیه شده که نرم‌افزار خود را هر چه سریعتر به‌روزرسانی کرده و آن را به نسخه ۹/۷ ارتقا دهند.

این آسیب‌پذیری بسیار خطرناک که با کدCVE-۲۰۱۹-۵۰۳۱ ثبت شده است، دارای امتیاز ۸/۸ از ۱۰، طبق امتیازدهی CVSS است. بر اساس گفته کارشناسان امنیتی، مهاجم برای بهره‌برداری از این آسیب‌پذیری کافی است یک فایل آلوده را برای کاربر فرستاده و کاربر نیز فایل را اجرا کند. لازم به ذکر است که در سال گذشته، بیش از ۱۰۰ آسیب‌پذیری توسط شرکت Foxit Software برطرف شدند که بیشتر آنها شامل اجرای کد از راه دور با مخاطره بالا بوده‌اند.

آسیب‌پذیری امنیتی در آنتی‌ویروس McAfee و امکان تزریق کد دلخواه و افزایش سطح دسترسی در ویندوز توسط مهاجمان

در تاریخ ۵ آگوست سال ۲۰۱۹ میلادی، یک آسیب‌پذیری امنیتی در آنتی‌ویروس McAfee با شناسه "CVE-۲۰۱۹-۳۶۴۸" ثبت شده است. مهاجم برای اکسپلویت کردن و سوءاستفاده از این آسیب‌پذیری که توسط آزمایشگاه‌های SafeBreach در تمام نسخه‌های McAfee شناسایی شده است باید سطح دسترسی مدیر سیستم را داشته باشد.

مهاجم می‌تواند از آسیب‌پذیری مذکور برای دور زدن سازوکارهای حفاظتی McAfee و دستیابی به پایداری آن از طریق بارگیری چندین سرویس که به عنوان "NT AUTHORITY\SYSTEM" اجرا می‌شوند، استفاده کند. این آسیب‌پذیری به مهاجمان امکان بارگذاری و اجرای پی‌لودهای مخرب را با استفاده از چندین سرویس، به صورت مداوم و در چارچوب فرایندهای McAfee می‌دهد.

شرکت McAfee این آسیب‌پذیری را در تمام نسخه‌های آنتی‌ویروس خود برطرف کرده و از کاربران نیز خواسته است تا نسخه R۲۲.۱۶/۰ را جهت رفع این آسیب‌پذیری نصب کنند. در این آسیب‌پذیری و در نسخه کلاینت ویندوز آنتی‌ویروس McAfee، مهاجمان می‌توانستند کد دلخواه خود را اجرا کرده و به امتیازات SYSTEMدسترسی پیدا کنند.

کشف ۱۸ آسیب‌پذیری منجر به حملات اجرای کد از راه دور در نرم‌افزارهای Cisco

شرکت Cisco که یکی از بزرگترین تولیدکنندگان تجهیزات نرم‌افزاری و سخت‌افزاری شبکه است، با توجه به پیشرفت روزافزون حوزه فناوری اطلاعات و به موازات آن افزایش چشمگیر تهدیدهای سایبری در سطح جهان و همچنین آسیب‌پذیری‌های موجود در تجهیزات فناورانه می‌تواند موجب به خطر افتادن اطلاعات کاربران شود. از این‌رو بخش‌های مختلف شرکت سیسکو به صورت مداوم و حتی چندین مرتبه در ماه نیز اقدام به ارایه آسیب‌پذیری‌های کشف شده در سرویس‌ها و تجهیزات این شرکت کرده و راه‌حل‌هایی را برای رفع این آسیب‌پذیری‌ها ارایه می‌کنند.

در سالی که گذشت، سیسکو برای چندین محصول امنیتی خود از جمله Cisco ASA، FMC و FTD به‌روزرسانی‌هایی را منتشر کرد تا بتواند ۱۸ آسیب‌پذیری شناخته شده در محصولاتش را برطرف کند. شرکت سیسکو تمامی این ۱۸ آسیب‌پذیری را خطرناک و با سطح مخاطره بالا اعلام کرده است. بهره‌برداری موفق از این آسیب‌پذیری‌ها می‌تواند منجر به کسب دسترسی بدون مجوز به سیستم‌های مجهز به نرم‌افزار آسیب‌پذیر سیسکو شود.

گسترش حملات دسترسی غیرمجاز بر روی سرویس دهنده‌های MS SQL Server در داخل کشور

در سالی که گذشت، مرکز ماهر هشدارهایی را در خصوص افزایش حملات به سرویس دهنده‌های SQL_Server بر روی پورت ۱۴۳۳ اعلام کرد. رصد حسگرهای این مرکز حاکی از گسترش آلودگی احتمالی سرورها در داخل کشور و فعالیت آنها به عنوان مهاجمان جدید در این حملات بود. اولین پیک حمله، در اوایل شهریورماه ۹۸ ثبت شد و دومین پیک حملات نیز در اواخر مهر و اوایل آبان‌ماه ثبت گردید.

در این حمله مهاجم، شبکه هدف را برای یافتن سرورهای SQL Server با کلمه عبور ضعیف اسکن کرده و با به کارگیری حمله Brute-force اقدام به ورود به سیستم می‌کرد. در ادامه نیز مهاجم با ایجاد برخی Jobها در SQL Server، فرمان‌های مختلفی را اجرا کرده یا بدافزارهایی را به سیستم منتقل می‌کرد. بدافزارهای منتقل شده در این روش می‌توانند هر نوع بدافزاری باشند. مهاجم با این حمله گسترده در پی یافتن سیستم‌های آسیب‌پذیر در شبکه‌های مختلف همچون سرورهای دارای کلمه عبور ضعیف است. برای جلوگیری از نفوذ مهاجمین از طریق این حملات بر روی سرور SQL Server در سازمان نکات زیر توصیه شده است:

- از قرارگیری این سرورها به صورت نامحدود بر بستر اینترنت اکیداً خودداری شود.
- از کلمه عبور مطمئن و مقاوم در برابر حملات حدس زدن کلمه عبور برای حساب‌های کاربری SQL Server استفاده شود.
- در صورتی که SQL Server در اینترنت قرار دارد، علاوه بر انجام موارد بالا لازم است:
- فهرست SQL Server Agent Jobها، جهت شناسایی موارد ایجاد شده احتمالی توسط مهاجمان بررسی شود.
- با توجه به احتمال آلودگی، بررسی دقیقی بر روی سیستم عامل از نظر وجود ردپای نفوذ مهاجمین و آلودگی احتمالی انجام شود.

مقالات امنیت سایبری

- پـرواز ابدی بـوینگ ۷۳۷ اوکـراینی از منظر سایبـر الکترونیک
- چـگونه از خـودمان در شبکه‌های اجتماعی مراقبت کنیم
- اهمیت آموزش مداوم کارمندان در زمینه امنیت سایبری
- در فضای مجـازی با آرامش و امنیت خـاطر زندگی کنیم
- پیامد های ویروس کرونا بر امنیت سایبری کشور

پرواز ابدی بوینگ ۷۳۷ اوکراینی از منظر سایبر الکترونیک

بعد از سقوط هواپیمای اوکراینی بر فراز آسمان کشورمان، فرضیه‌ها و نظرات بسیاری در خصوص این فاجعه تأسف‌برانگیز مطرح شد که بخشی از آنها نیز در حوزه سایبری بوده است. به عنوان نمونه، این احتمال مطرح است که شلیک موشک از طرف سامانه پدافندی کشورمان به دلیل اشتباه در تشخیص هواپیمای مسافربری با یک شیء متخاصم صورت گرفته است. بیان موضوعاتی از این دست ما را برآن داشت که این مسأله را از جنبه امنیت سایبری و سایبر الکترونیک (جنگ الکترونیک - جنگال) بررسی کنیم.

با نگاهی گذرا به تاریخچه پدافندی و ظهور و بلوغ آن در طول سال‌های متمادی بهتر می‌توانیم ابعاد این حادثه را بیان کنیم.
نیاز به پدافند هوایی، زمانی توسط کشورهای شرق احساس شد که توان رزم هوایی با دشمن غربی خود را نداشتند. به همین دلیل جهت حفظ دارایی‌های سرزمینی خود مجبور به استفاده از علوم روز برای دفاع در مقابل تهدیدهای هوایی به عنوان میدان سوم جنگ شدند .تجهیزات پدافند هوایی در ابتدا بسیار ساده بود ولی به مرور با پیشرفت تجهیزات و با قدرتمند شدن سیستم‌های پدافندی شرق که با استفاده از راداء، دشمن را شناسایی کرده و توسط توپ‌ها یا موشک‌های مختلف، پرتابه‌ها و هواپیماهای جنگی دشمن را رهگیری و منهدم می‌کردند، غرب متحمل خسارت‌های زیادی در این خصوص شد.

این موضوع، غرب را بر آن داشت تا به این عدم موازنه پایان داده و برتری خود را در میدان جنگ هوایی دوباره به دست آورد. از این‌رو بر سامانه‌های پدافندی شرق متمرکز شد و در پی کشف حفره‌ها و آسیب پذیری‌های موجود در سامانه‌های پدافندی شرق جهت دور زدن (Bypass) آنها تلاش‌های بسیاری را انجام داد.

نتیجه این تلاش‌ها، تولید هواپیماهایی مجهز به ابزارهای ویژه با هدف ایجاد اختلال و اشتباه در عملکرد سامانه‌های پدافندی کشورها بود. هواپیمای Rivet joint از گروه هواپیماهای RC-۱۳۵ نمونه‌ای از چنین اقدام‌هایی محسوب می‌شود. هواپیماهای RC-۱۳۵ که محصول کشور ایالات متحده آمریکا است در دهه ۱۹۶۰ میلادی در انواع مختلفی تولید شده و به تدریج ارتقا یافت. این هواپیما با بدنه جذب کننده امواج، از ویژگی غیرقابل رهگیری بودن برخوردار است و می‌تواند امواج راداری دشمن را دریافت کرده و با استفاده از تجهیزات و فناوری‌های داخل هواپیما آنها را تجزیه و تحلیل کند. همچنین بر روی بال‌های این هواپیما رادارهای مختلفی با امکان تولید امواج در فرکانس‌های مختلف تعبیه شده است. بررسی کادر پروازی هواپیما، خود نشان دهنده امکانات و فناوری‌های موجود در آن جهت ایجاد تشخیص اشتباه و انهدام سامانه پدافندی قربانی است.

بنابراین بر اساس آن چه به طور مختصر بیان شد و شواهد موجود، کاملاً مشخص است که حمله سایبر الکترونیک به هواپیمای اوکراینی و سامانه پدافندی ایران، احتمالی بسیار بدیهی بوده و قابل بررسی بیشتری است .احتمال انجام این حمله در دو سطح زیر قابل بررسی است:

حمله فریب سامانه پدافندی (اجرای سوتر)

بـر اسـاس قوانین بین‌المللی در هر پرواز مسـافربری، لیسـت پـرواز به تمامی سـامانه‌های پدافندی داخلـی و خارجی در کریـدور هوایـی مبـدأ به مقصد ارسـال می‌شـود. هواپیمـای مسـافربری در نزدیکی هر سـامانه پدافنـدی، اقدام به معرفـی خـود به آن سـامانه پدافنـدی می‌کند. همچنین سیسـتم ترنسـپوندر هواپیما به صورت پی‌درپی مشـخصات خـود را ارسـال می‌کنـد تـا در هر صورت، امکان اشـتباه از کاربر انسـانی گرفته شـود. در حمله سـوتر، سـامانه پدافندی بـر اسـاس بازخورد جعلی از امواج ارسـالی دچار تشـخیص اشـتباه می‌شـود. در خصـوص هواپیمای اوکراینـی، به دو صورت امکان حمله سـوتر وجود داشـته اسـت:

- بازخـورد امـواج ارسـالی از سـامانه پدافنـدی به جـای این که از طـرف هواپیمای مسـافربری داده شـود با خاموش شـدن سیسـتم ترنسـپوندر هواپیما توسـط هواپیمای جاسوسـی ریوت جوینت، به عنوان موشـک کروز تشخیص داده شـده اسـت. بـه گفته سـردار حاجـی زاده، فرمانـده نیروی هوافضای سـپاه نیـز چندین مورد موشـک کروز در سـامانه‌های پدافندی کشـورمان مشـاهده شـده و به اپراتورها اخطار شـلیک موشـک داده شـده بود.
- هواپیمـای مسـافربری از قبـل دسـتکاری شـده و زمـان بازخورد بـه امـواج راداری سـامانه پدافندی کشـور، خود را موشـک کروز معرفی کرده اسـت (همین هواپیما مدتی قبل در اسـرائیل لندینگ داشـته اسـت). در صورت صحت چنیـن فرضیـه‌ای، «موضـوع ارایـه گواهینامه‌های امنیتی نرم‌افزارهای هواپیما توسـط شـرکت بوئینگ یا اسـتفاده از آسـیب پذیری‌هـای روز صفـر در نرم‌افزارهـای شـرکت بوئینـگ، بـه پنتاگون مطرح می‌شـود که برای شـرکتی در آسـتانه ورشکسـتگی همچون بوییـنـگ فاجعه‌بـار خواهد بود.

حمله قطع سرویس هات‌لاین سامانه پدافندی

سامانه‌های پدافندی عموماً به صورت رینگ‌هایی با مرکزیت پایتخت یا مراکز حیاتی کشور در انواع رادارهای پیش اخطار، رادارهای پیش اخطار دور برد، رادارهای شناسایی و رادارهای شناسایی و پدافند، از نزدیکترین لبه مرزی کشور به سمت مرکز رینگ‌ها استقرار می‌یابند.

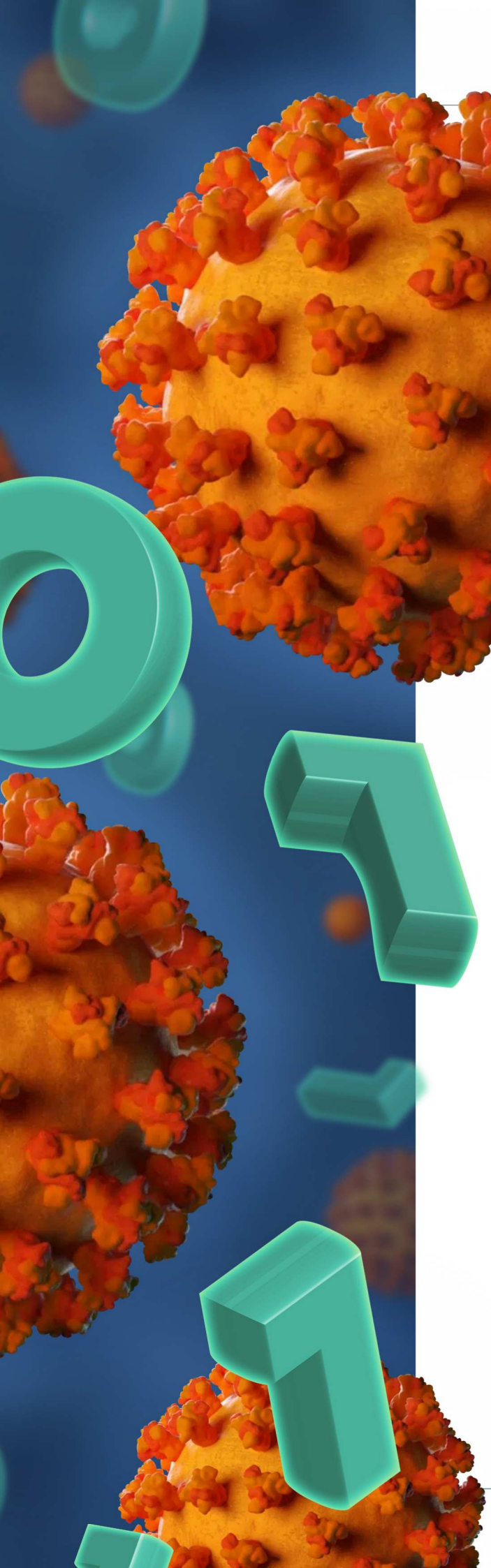
این سامانه‌ها به صورت سلسله مراتبی با یکدیگر در ارتباط هستند و جهت اخذ دستور نهایی، به صورت هات‌لاین با فرماندهی ارشد ارتباط مستقیم دارند. این ارتباط از این جهت هات‌لاین نامیده می‌شود که بدون واسطه در کوتاهترین زمان و زیرساختی امن با پایداری بالا، خدمات ارتباطی را فراهم می‌کند تا گزارش‌دهی و ابلاغ تصمیم‌هایی همچون فرمان شلیک در کوتاهترین زمان ممکن و بالاترین سطح امنیت انجام شود .

در جریان هواپیمای اوکراینی، سامانه پدافندی کشورمان در حساس‌ترین زمان تصمیم‌گیری، ارتباط خود را با مرکز فرماندهی از دست داده (قطع سرویس هات‌لاین) و به ناچار، تصمیم به شلیک موشک بر اساس تشخیص اپراتور سامانه پدافندی انجام گرفته است.

نتیجه‌گیری

آن چه بیان شد خلاصه‌ای از عملیات پیچیده و جامع احتمالی آمریکا و اسرائیل غاصب بر ضد جمهوری اسلامی ایران است که منجر به سقوط هواپیمای اوکراینی و کشته شدن تعداد زیادی از هموطنان‌مان گردید؛ عملیاتی که تاکنون بارها در مخاصمات رویداده در سطح جهان نیز تکرار شده است. برای نمونه، در حمله اسرائیل به تأسیسات هسته‌ای سوریه در سال ۲۰۰۷، به وسیله عملیات پیچیده فریب و استفاده از اجرای حمله سوتر، اسرائیل توانست بدون دادن هیچ‌گونه تلفاتی تأسیسات هسته‌ای سوریه را در منطقه دیرالزور بمباران کرده و پدافند هوایی سوریه نیز نتواند هیچ عکس‌العملی از خود نشان دهد. انهدام هواپیمای مالزیایی بر اساس اشتباه پدافند روسیه در جریان مناقشات بین اوکراین و روسیه هم نمونه دیگری از اجرای حملات فریب پدافندی است.

بررسی سناریو های احتمالی در موضوع‌هایی غیر از موضوع سایبر الکترونیک، خارج از بحث این نوشتار است اما تجربه نشان داده است ایالات متحده آمریکا با همراهی اسرائیل متجاوز در انجام عملیات‌های سری و خرابکارانه، از تمام توان خود در همه سطوح قابل انجام و بهره‌گیری از همکاری متحدان منطقه‌ای خویش استفاده می‌کند. مصداق بارز چنین حملاتی به کشورمان، حمله استاکس‌نت به سانتریفیوژهای آبشار غنی‌سازی ۲۰ درصدی در سال ۱۳۹۱ است که توسط آژانس امنیت ملی آمریکا (NSA)، گواهینامه‌ها و آسیب پذیری‌های روز صفر مایکروسافت و اسکادای شرکت زیمنس و با همکاری اسرائیل و چند کشور اروپایی انجام شد.



پیامدهای ویروس کرونا بر امنیت سایبری کشور

با همه‌گیر شدن ویروس کرونا در سطح جهان، مطالب بسیار زیادی را در جامعه، رسانه‌ها و فضای مجازی درباره این ویروس خطرناک شنیده یا می‌خوانیم. ویروسی که اگر چه اولین بار در شهر ووهان چین مشاهده شد ولی با فاصله زمانی نسبتاً کوتاهی توانست بیش از یکصد و چهل کشور را تحت الشعاع پیامدهای مخرب خود قرار داده و حتی جان تعداد زیادی از انسان‌ها را هم در گوشه و کنار جهان و همچنین کشور عزیزمان بگیرد.

کرونا ویروس که منشأ شکل‌گیری و پیدایش آن هنوز در شک و شبه است و تعدادی از سیاست‌مداران کشورهای مختلف از آن با عنوان «سلاح سایبری» و جنگ بیولوژیکی آمریکا بر ضد سایر کشورهای متخاصم این دولت یاد می‌کنند؛ با وجود توصیه‌های مداوم بهداشتی به شهروندان، متأسفانه تأثیر بسیار زیادی بر جامعه ایرانی گذاشته و موجب تغییر زندگی شهرنشینی برای مدت چند ماه‌ای خواهد شد که تبعات آن کماکان در ماه‌های پس از فروکش کردن آن نیز همچنان پابرجا می‌ماند. این ویروس علاوه بر زندگی شهری، روال‌های کاری و خدمات کسب و کارهای زیادی، از سازمان‌های دولتی گرفته تا شرکت‌های کوچک خصوصی و مشاغل سطح جامعه را از روند عادی خود خارج کرد.

ویروس کرونا موجب توجه جدی‌تر به اهمیت فضای مجازی برای بقای خدمات سازمانی و مفهوم «سازمان الکترونیک» هم شد. همزمان با افزایش کاربرد فضای مجازی در خدمات سنتی سازمانی و دورکاری تعدادی از کارکنان مشاغل دولتی و خصوصی، چالش‌های امنیتی نیز به تبع آن افزایش خواهد یافت. در این مقاله، به بررسی مهمترین تهدیدها و چالش‌های امنیت سایبری این ویروس که امکان مواجه شدن شرکت‌ها و سازمان‌ها با آنها وجود دارد، خواهیم پرداخت.

۱.دسترسی به خدمات سازمانی از راه دور

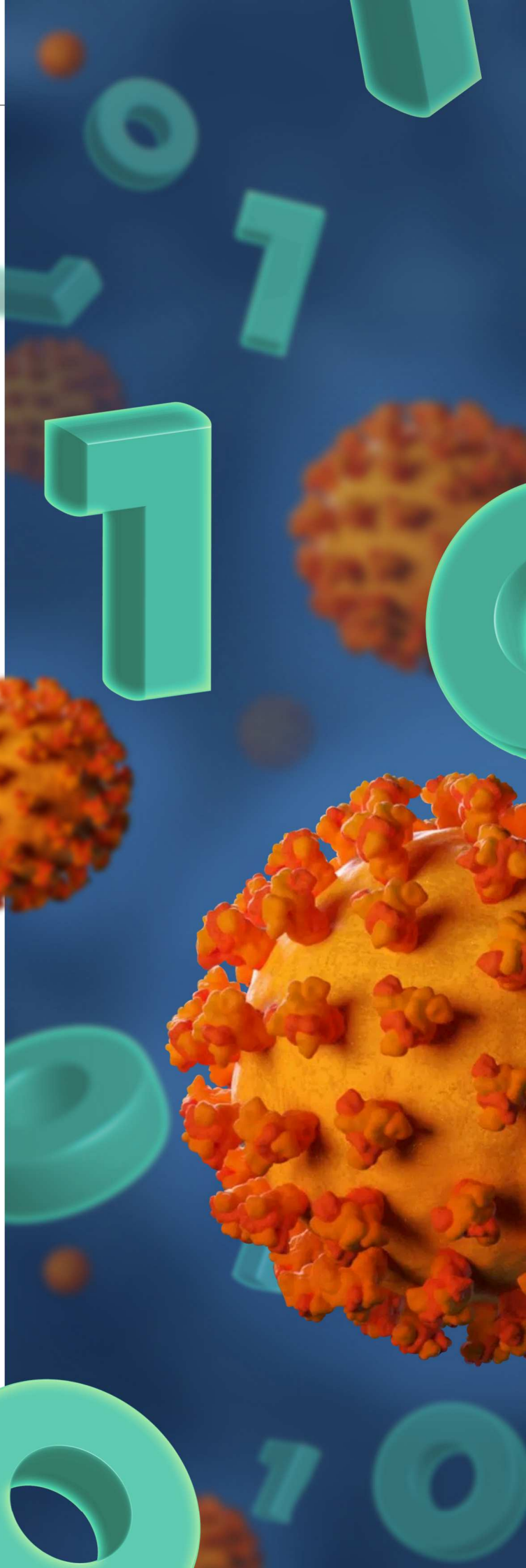
با تصمیم مدیران دولتی و خصوصی مبنی بر دورکاری کارمندانی که امکان دور کار شدن آنها میسر است، تعدادی از کارکنان این فرصت را پیدا کردند که وظایف کاری‌شان را از طریق منازل خود انجام دهند. چنین کاری در گام اول، احتیاج به باز کردن دسترسی آنها از طریق فایروال‌ها و مجازشماری آنها بر اساس سازوکارهای امنیتی یا سرویس‌دهی مورد استفاده است. قاعدتاً با انجام این کار، کنترل‌های مرسوم احراز هویت سازمانی ضعیف‌تر از قبل شده و امکان اتصال و استفاده سایر افراد غیرمجاز هم فراهم می‌شود.

لازم به ذکر است که کارکنان، معمولاً ضعیف‌ترین حلقه در زنجیره امنیت سایبری به شمار می‌روند. آنها اغلب کلمه‌های عبور بسیار ضعیفی را انتخاب کرده و توجه چندانی به رعایت الزام‌های امنیت اطلاعات سازمانی ندارند. دسترسی از راه دور به خدمات و زیرساخت‌های سازمانی موجب خواهد شد که سامانه‌ها به راحتی در برابر حملات مربوط به حدس کلمه‌های عبور کاربران آسیب پذیرتر شده و امکان نشت اطلاعات سازمانی برای نفوذگران سایبری بیشتر از قبل فراهم شود.

۲.اتصال های شبکه ای محافظت نشده

چالش مهم دیگری که این مسأله برای شرکت‌ها و سازمان‌ها در آینده به دنبال خواهد داشت، این است که کارکنان که قبلاً از طریق سیستم‌های گاهاً هاردنینگ شده و شبکه‌های محافظت شده به سامانه‌های سازمانی متصل می‌شدند اینک با لپ‌تاپ‌ها، تبلت‌ها و رایانه‌های شخصی که هیچ‌گونه وصله امنیتی سیستم عامل و نرم‌افزارها بر روی آنها نصب نشده است، از قید تمامی محدودیت‌های قبلی عبور کرده و امکان اتصال به سامانه‌ها و تجهیزات سازمانی را پیدا می‌کنند. چنین موضوعی موجب تضعیف شدید امنیت سایبری خواهد شد.

در بیشتر وقت‌ها نیز رایانه خانگی کارکنان، حتی نرم‌افزار ضدویروس لایسنس‌دار به‌روز شده‌ای هم ندارد. از این بدتر اینکه ممکن است کارمندان از گوشی‌های هوشمند خود برای اتصال به سامانه‌های سازمانی استفاده کنند که بالطبع بر مشکلات موجود به شدت خواهد افزود. متأسفانه از آنجا که بیشتر شرکت‌ها و سازمان‌ها خط‌مشی‌ها و رویه‌های امنیتی مناسب و کافی نداشته و کاربران هم حداقل آموزش‌های امنیتی را ندیده‌اند، چنین مواردی می‌تواند منجر به مشکلات بسیار جدی برای آنها شود. از سوی دیگر باید در نظر داشت که کنترل دستگاه‌های متصل به شبکه‌ها و سرویس‌های سازمانی در شرایط حاد فعلی، تا حدودی برای کارشناسان امنیت سایبری که حالا ممکن است خودشان نیز دورکار شده باشند، بسیار سخت است.



۳.دسترسی به اطلاعات محرمانه و طبقه بندی شده سازمانی

از دیگر چالش‌های این ویروس در حوزه امنیت سایبری می‌توان به استفاده سایر اعضای خانواده از رایانه‌ای اشاره کرد که کارکنان به منظور انجام فعالیت‌های دورکاری روزانه‌شان از آن استفاده می‌کنند. از آنجا که کنترل‌ها و الزام‌های امنیت سازمانی بر روی رایانه‌های شخصی و در منزل کارکنان به دلیل شخصی بودن‌شان قابل اعمال نیستند، نظارت بر فعالیت‌های آنها سخت‌تر از همیشه خواهد بود.

معمولاً سیستم خانگی کارکنان، دیگر پس از عدم استفاده از آن پس از مدت زمانی، قفل نخواهد شد. بنابراین امکان دسترسی به سامانه‌های سازمانی که کارکنان عادت خارج شدن از آنها را هم پس از اتمام فعالیت‌های کاری‌شان ندارند، توسط سایر اعضای خانواده وجود دارد. این موضوع می‌تواند موجب دسترسی افراد غیرمجاز به اطلاعات سازمانی و حتی مشاهده مستندات طبقه‌بندی شده و محرمانه توسط آنها شود. باید توجه داشت که نشت ناخواسته اطلاعات، از مهمترین مواردی است که در طول چند سال اخیر، شرکت‌ها و سازمان‌ها به شدت با آن مواجه بوده‌اند و ضررهای هنگفتی را نیز به کسب و کارها وارد کرده است.

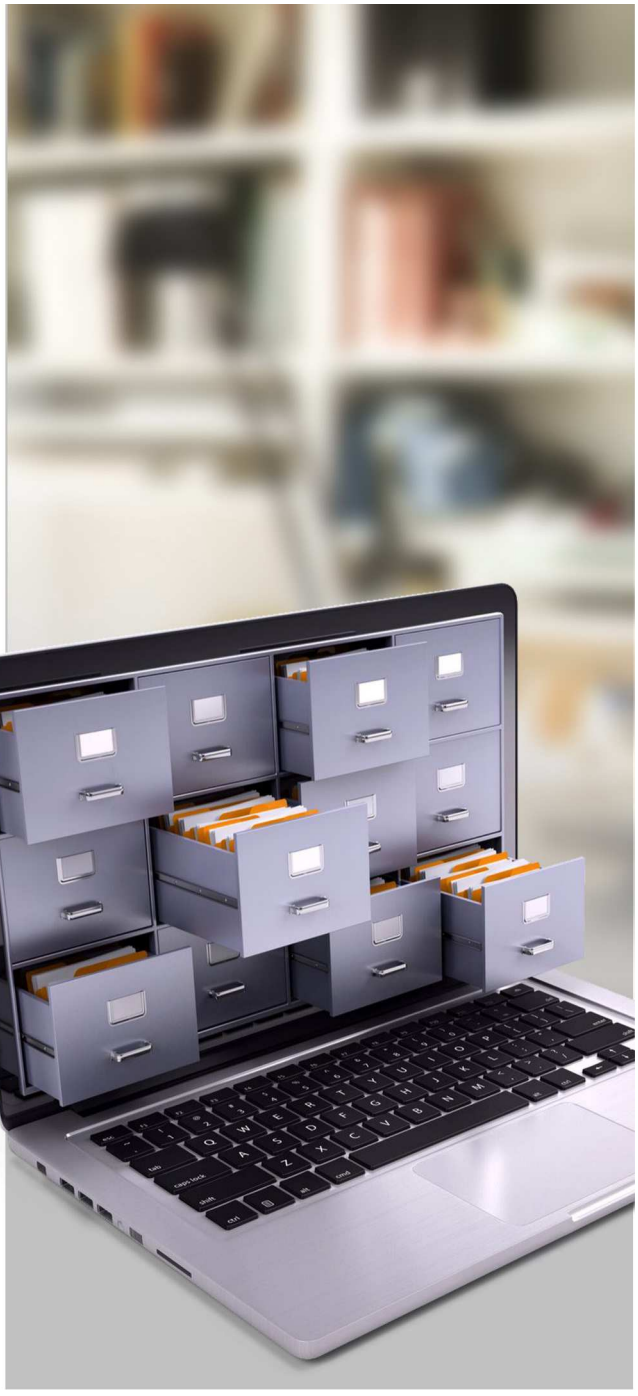
۴.آلودگی بدافزاری بیشتر شبکه های سازمانی

در بیشتر شرکت‌ها و سازمان‌ها پورت‌های USB و درگاه‌های انتقال فایل، به منظور کنترل امنیت نقاط انتهایی و جلوگیری از آلودگی بدافزاری توسط کارکنان بسته شده است. باید توجه داشت که روش‌های رایج جابه‌جایی فایل‌ها و انتقال آنها از شبکه امن سازمانی به رایانه خانگی کارکنان و همچنین برعکس می‌تواند آلودگی بیشتر شبکه‌های سازمانی را در پی داشته باشد. کاربران معمولاً از رسانه‌های ذخیره‌سازی قابل حمل شخصی (USB) یا ایمیل غیرسازمانی برای انتقال اطلاعات و فایل‌ها استفاده می‌کنند. آنها اغلب عادت به اسکن این رسانه‌ها توسط نرم‌افزارهای آنتی‌ویروس (که حالا دیگر ممکن است اصلاً برای روی سیستم هم نصب نباشند) در هنگام اتصال‌شان به سیستم‌ها نداشته و پیوست ایمیل‌های دریافتی را نیز بدون اسکن کردن باز می‌کنند.

چالش مهمی که این موضوع می‌تواند برای شرکت‌ها و سازمان‌ها علاوه بر بازکردن درگاه‌های انتقال فایل و نیاز به کنترل شدیدتر آلودگی‌های بدافزاری در پی آن به دنبال داشته باشد این است که همان‌طور که قبلاً گفته شد، بیشتر رایانه‌های خانگی کارکنان فاقد نرم‌افزار آنتی‌ویروس به‌روز شده لایسنس‌دار هستند. بنابراین چنین کاری موجب خواهد شد که در هنگام انتقال فایل‌ها از روی رسانه‌های ذخیره‌ساز شخصی که معمولاً نیز با غیرفعال کردن اسکن خودکار آنتی‌ویروس سازمانی توسط کارکنان کم‌حوصله و عجول انجام می‌شود، شاهد آلودگی بیشتر شبکه سازمانی به انواع و اقسام بدافزارها و باج‌افزارها باشیم.

۵.ذخیره مستندات محرمانه سازمانی بر روی سیستم های شخصی

تهدید دیگر ویروس کرونا بر امنیت سایبری، اتصال کارکنان به سامانه‌های سازمانی و دسترسی آنها از منزل به منظور انجام وظایف کاری‌شان است که می‌تواند موجب ذخیره فایل‌های محرمانه و طبقه‌بندی شده سازمانی بر روی رایانه‌های شخصی کارمندان شود. فقدان یا رویه‌های امحای ضعیف فایل‌های دیجیتالی و دارایی‌های اطلاعاتی نیز ممکن است منجر به ایجاد امکان دسترسی افراد غیرمجاز به این اطلاعات و افشای ناخواسته آنها شود.



۶.اعمال مجوزدهی فراتر از سطح نیاز کارکنان

مسأله دیگر می‌تواند دادن مجوزهای دسترسی به کارکنان برای انجام وظایف کاری‌شان، بیشتر از سطح نیاز آنها باشد. کاربران ممکن است در انجام فعالیت‌های‌شان از راه دور با مشکلاتی مواجه شوند که راهبران سامانه‌ها، سرویس‌ها و شبکه‌ها مجبور به افزایش سطوح دسترسی آنها به منظور رفع مشکلات جاری شوند. چنین امری منجر به دسترسی غیرمجاز افراد به بخش‌هایی از سامانه‌ها و منابع شبکه‌ای خواهد شد که تا پیش از این، هرگز امکان دسترسی به آنها را نداشتند.

۷.مهندسی اجتماعی کارشناسان پشتیبانی

تهدید بسیار جدی دیگری که در کشورمان متأسفانه در چند سال اخیر همواره روند صعودی داشته است، فریب و مهندسی اجتماعی کارکنان به منظور تخلیه اطلاعاتی آنها یا به دست آوردن امکان دسترسی غیرمجاز به سامانه‌ها و تجهیزات سازمانی است. به طبع افزایش خدمات دورکاری سازمانی، این تهدید نیز همچنان به رشد بالای خود ادامه خواهد داد. کارشناسان میز خدمت و بخش‌های پشتیبانی از راه دور، در معرض بیشتر این حمله قرار دارند و می‌بایست آموزش‌های کافی برای شناخت و مقابله با این حمله به صورت مداوم به آنها داده شود.

ارسال اس‌ام اس‌های فیشینگ (حمله اسمیشینگ)، فیشینگ تلفنی (حمله ویشینگ) و همچنین طراحی وب سایت‌های مشابه با سایت‌های خدمات‌رسان بهداشتی و بانکی به منظور دریافت کمک‌های مردمی (حمله فیشینگ) هر چند که با راه‌اندازی رمز یک‌بار مصرف کاهش چشم‌گیری داشته است اما همچنان مخاطرات خاص خود را دارد. چنین حملاتی امروزه در قالب تخلیه اطلاعاتی کارکنان و به دست آوردن اطلاعات سازمانی انجام شده و می‌توانند شرکت‌ها و سازمان‌ها را با مخاطرات زیادی مواجه سازند. این حملات ممکن است به منظور دستیابی به اطلاعات حساب کاربری و کلمه عبور کارمندان و همچنین آگاهی از روش‌های اتصال آنها به سامانه‌های سازمانی نیز صورت پذیرند. شناخت این حملات به دلیل تسلط بالای نفوذگر بر روش حمله مورد استفاده خود، برای بیشتر کارکنان سخت است و امکان مقابله با آن نیز از طریق سازوکارهای امنیتی فعلی وجود ندارد. افزایش آگاهی کارکنان با روش‌های مختلف این حمله، ضرورتی است که می‌بایست به صورت جدی به آن پرداخته شود.

۸.ارسال بدافزار به کارکنان

یکی دیگر از چالش‌های ویروس کرونا بر حوزه امنیت سایبری، ارسال انواع و اقسام بدافزارها به ایمیل کارکنان در قالب لینک به وب سایت‌های خبری و اطلاع از آخرین اخبار مرتبط با این ویروس و همچنین عکس‌های ارسالی در ایمیل کارکنان و فریب آنها جهت کلیک کردن بر روی این لینک‌ها یا باز کردن فایل‌های پیوست آلوده ایمیل‌ها است. ایمیل‌هایی که با عناوین جعلی و در قالب نهادهای معتبری همچون سازمان بهداشت جهانی برای کاربران بسیاری ارسال شده‌اند، موجب وسیعی از آلودگی را در سطح جهان به دنبال داشته‌اند. شبکه‌های اجتماعی و پیام‌رسان‌های برخط نیز می‌توانند بر این موج آلودگی‌های بدافزاری افزوده و کاربران بیشتری را با مخاطرات مواجه سازند. طراحی پروفایلی مشابه با افراد مشهور و مسئولین دولتی در ستاد ملی مبارزه با ویروس کرونا، موجب گمراهی بیشتر کاربران و آلودگی زیادتر سیستم‌های رایانه‌ای که حالا علاوه بر فعالیت‌های شخصی از آنها برای انجام فعالیت‌های سازمانی هم استفاده می‌شود، خواهد شد.

۹.اتصال اینترانت به اینترنت

جداسازی شبکه‌های سازمانی از اینترنت به صورت فیزیکی، یکی از موارد مطرح امنیت اطلاعات سازمانی در سال‌های اخیر بوده است. با دورکاری کارکنان، ممکن است بعضی از شرکت‌ها و سازمان‌ها مجبور به دسترسی کارکنان به سرویس‌های سازمانی از طریق بستر ناامن اینترنت شوند.

۱۰.ایجاد اختلال در روند تداوم کسب و کار سازمان

عدم نیاز به حضور کارکنان در محیط‌های کاری به دلیل جلوگیری از شیوع ویروس کرونا و انجام فعالیت‌های سازمانی به صورت دورکاری؛ از آنجا که دیگر امکان حضور افراد در محیط‌های سازمانی وجود نداشته یا سخت‌تر شده است به خصوص برای افراد بیمار، چنانچه مشکلی برای سرویس‌های سازمان‌ها پیش آید یا شهروندان در بهره‌گیری از خدمات سازمانی با مشکل خاصی مواجه شوند می‌تواند موجب طولانی‌تر شدن زمان رفع مشکل شده و شرکت‌ها و سازمان‌ها را در ارایه خدمات با مخاطرات جدی مواجه سازد.

مستندسازی ضعیف، به خصوص در بین کارشناسان فنی شرکت‌ها و سازمان‌ها و همچنین عدم وجود نظارت‌های کافی و جدی برای انجام این کار؛ موجب تضعیف رویه‌های کسب و کاری خواهد شد و بر دامنه رفع مشکلات، به ویژه در چنین زمان‌های بحرانی به شدت خواهد افزود.

۱۱.نفوذ به سامانه‌های آسیب پذیر

چالش بعدی که مدیران سازمان‌ها با آن مواجه هستند، اجبار به قراردادن سامانه‌ها و تجهیزاتی در اینترنت به دلیل شرایط موجود کشور و قابلیت دسترسی از راه دور کارکنان به آنها هستند که معمولاً دارای آسیب پذیری‌های برطرف نشده فراوانی هستند. شرکت‌ها و سازمان‌ها در بیشتر موارد، انجام آزمون‌های نفوذپذیری را به منظور یافتن نقاط آسیب پذیر سامانه‌ها، تجهیزات و شبکه خود انجام نداده و آسیب پذیری‌های برطرف نشده حیاتی زیادی در آنها وجود دارد.

این مسأله می‌تواند موضوع جذابی برای نفوذگران سایبری بوده و موجب بهره‌برداری از این آسیب پذیری‌ها و امکان دسترسی به اطلاعات سازمانی شود. تغییر، تخریب و افشای غیرمجاز داده‌ها و اطلاعات از نمونه پیامدهای مخربی هستند که به طور معمول سازمان‌ها در چنین مواقعی با آنها مواجه خواهند بود.

نتیجه گیری

ویروس کرونا، ناخواسته جامعه ایرانی را تحت تأثیر پیامدهای ناخوشایندی قرار داده و ضررهای هنگفتی را به بسیاری از کسب و کارها به خصوص مشاغل کوچک وارد کرده است. در این بین، به دلیل جلوگیری از شیوع گسترده بیماری از طریق محیط‌های کاری، کارکنان بسیاری از سازمان‌ها و شرکت‌ها ملزم به دورکاری شده‌اند. از آنجا که وضعیت امنیت سایبری در کشورمان و آگاهی بخشی‌های امنیت سایبری به کارکنان در جایگاه چندان مطلوبی قرار ندارد و حوادث امنیت اطلاعات سال‌های اخیر نیز بر این نکته صحه گذاشته است، پیش‌بینی می‌شود که روند مخاطرات سایبری سازمانی در چند ماه اخیر به شدت افزایش یابد. از این‌رو اتخاذ کنترل‌های امنیتی توسط شرکت‌ها و سازمان‌ها، با پیش‌بینی تهدیدات و مخاطراتی که به تعدادی از مهمترین آنها در این مقاله اشاره شد می‌تواند به مدیران سازمانی در گذار این بحران میکروبی کمک کرده و آن را تبدیل به فاجعه سایبری برای آنها نسازد.

در زمان ارس

از نرم افزار های رمز


ل ایمیل
گذاری استفاده کنید

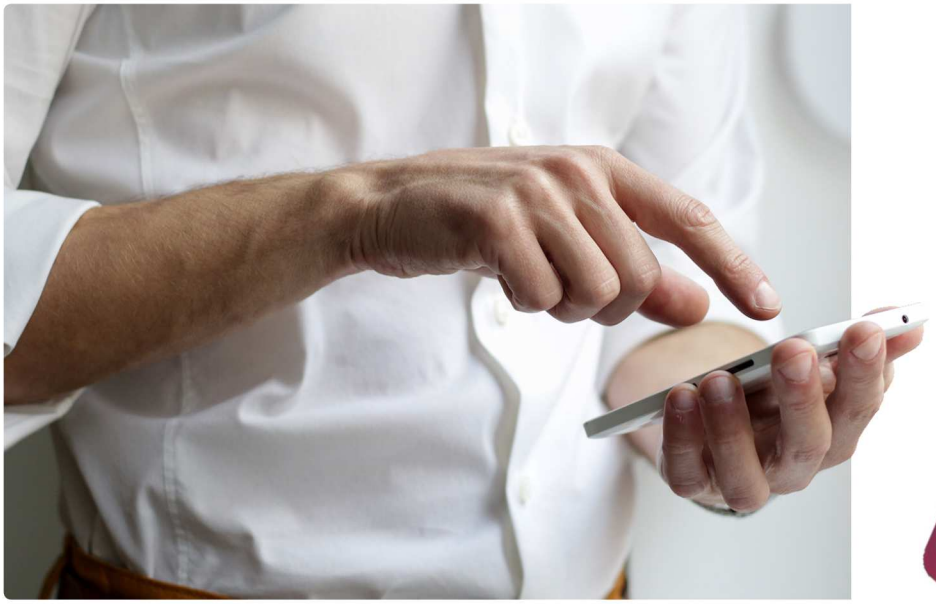
چگونه از خودمان در شبکه‌های اجتماعی مراقبت کنیم؟

ظهور فناوری‌های نوین ارتباطی و استقبال شگفت‌انگیز مردم از شبکه‌های اجتماعی آنلاین، موج جدیدی از حمله‌های سایبری را برای کاربران به همراه داشته است. در این میان، امنیت کاربران به علت هویت و ارتباط‌های مجازی افراد در شبکه‌های اجتماعی، به نوبه خود دارای اهمیت بسیار زیادی است که حتی لازم است به صورت ملی و چه بسا فراملی نیز مورد توجه قرار گیرد.

امروزه دسترسی مداوم و لحظه‌ای به شبکه‌های اجتماعی مجازی از طریق تلفن همراه و رایانه‌ها، اولویت مهمی برای بیشتر کاربران به شمار می‌رود. بر اساس آماری هم که از سوی مؤسسه‌های رسمی آمارسنجی کشور ارایه می‌شود، بیش از پیش بر این نکته تأکید دارند و در گزارش‌های خود از ساعت‌های حضور طولانی شهروندان در این شبکه‌ها (۵ تا ۹ ساعت در روز!) سخن به میان می‌آورند. خلق مفهومی با عنوان «معتاد شبکه اجتماعی» از دستاوردهای زندگی بشر در عصر فناوری است.

از بزرگترین و پرعضوترین شبکه‌های اجتماعی جهان می‌توان به فیسبوک اشاره کرد که دارای ۵۰۰ میلیون کاربر، یعنی حدود ۱ نفر از هر ۱۳ نفر روی کره زمین است. نیمی از اعضای این شبکه اجتماعی، به صورت روزانه وارد سایت آن شده و ۴۸ درصد نیز که سنی بین ۱۸ تا ۳۴ سال دارند، به محض بیدار شدن از خواب، صفحه‌های شخصی خود در فیس‌بوک را توسط گوشی‌های هوشمندشان چک می‌کنند.

اگر چه دریافت به‌روزرسانی‌های مستمر از دوستان فیسبوک، توییتر، اینستاگرام و سایر شبکه‌های اجتماعی و همچنین اشتراک‌گذاری خبرها و عکس‌های لحظه‌ای از خودتان یا موضوع‌های مورد علاقه‌تان، موضوع جالبی است اما توصیه ما به کاربران این است که از شبکه‌های اجتماعی، به خصوص پیام‌رسان‌های غیربومی و خارجی استفاده نکنند. در صورتی که مجبور به استفاده از این شبکه‌ها هستید، در ادامه حتماً به نکته‌های امنیتی توجه کنید تا ناخواسته در دام حمله‌های سایبری نیافتید.

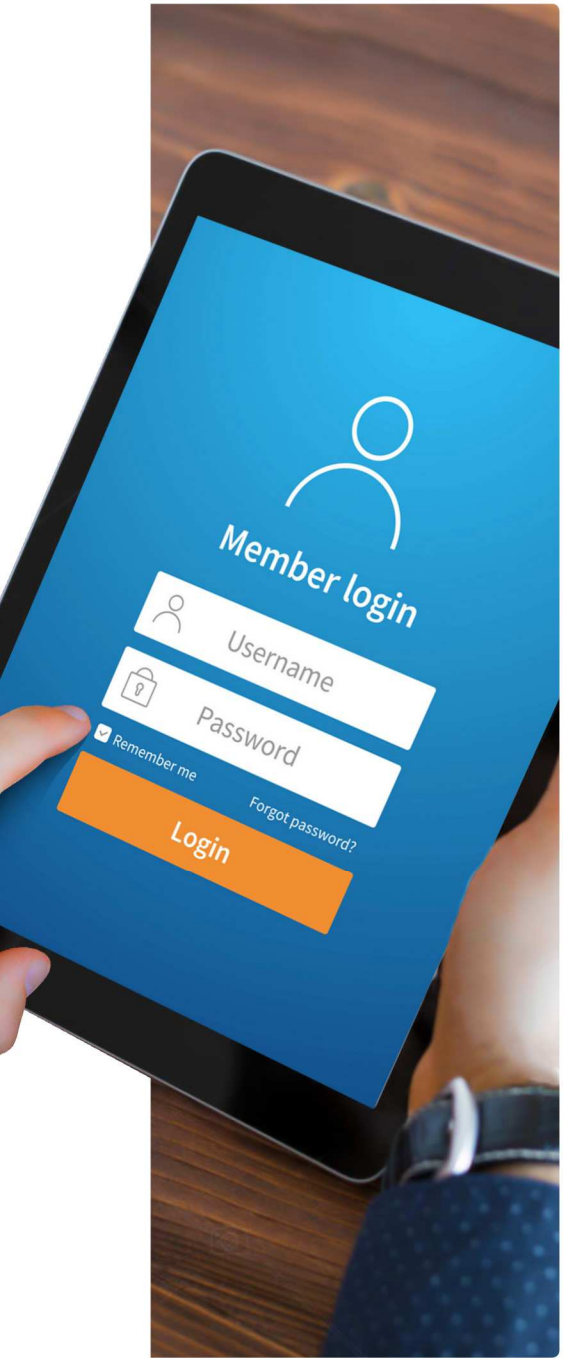


اشتراک مجازی جدید

مهمتریـن خطری که همیشـه در شـبکه‌های اجتماعی شـما را تهدید می‌کند، کوشـش برای متقاعـد کردن‌تان به منظـور تکمیـل یـک فرم اینترنتی یـا ثبت نام در یك اشـتراك مجازی جدید بـا فریب به دسـت آوردن امتیازهای خـاص اسـت. ایـن کار که با هدف دسترسـی به شـماره حسـاب بانکی، تلفن، ایمیـل و رمز عبور آن، مشـخصات شـما، خانواده یا دوسـتان‌تان انجام می‌شـود می‌تواند اطلاعات حسـاس شـما را در اختیار کلاهبردارها قرار داده تـا برای دسـتیابی به اهداف شـوم خود، از آنهـا بهره ببرند.

فراموشی رمز عبور

روش دیگری که کلاهبردارها از آن بهره‌های فراوانی می‌برند، اسـتفاده از گزینه فراموشـی رمز عبور حسـاب‌های کاربـری اسـت. کلاهبردارهـا با جسـتجوی افـراد خـاص و پس از بررسـی علاقمندی‌هـا، زمینه‌هـای مطالعه و سـایر اطلاعـات مفیـدی کـه در خصـوص شـخصیت آن فـرد می‌توانند به دسـت آورنـد و یا مهمتـر از همه، با طـرح دوسـتی و سـؤال از کاربـر هنـگام گفتگوهای اینترنتی، پاسـخ سـؤال‌های امنیتـی او را به دسـت آورده و اقـدام بـه تغییر کلمه عبور حسـاب آن شـخص می‌کنند. این مسـأله تاکنون ده‌هـا بار در شـبکه-های اجتماعی بـه وقوع پیوسـته و افراد بی‌شـماری حسـاب‌های کاربـری خـود را راحت از دسـت داده‌اند.



مرا به خاطر بسپار

لازم اسـت بدانیـد که رمزهـای عبوری که با اسـتفاده از گزینـه «مـرا بـه خاطـر بسـپار» ذخیـره می‌شـوند، در کوکی‌هـای مرورگرهـا یـا برنامه‌هـای کاربـردی شـبکه‌های اجتماعـی، ذخیـره شـده و کلاهبردارهـا بـا دزدیـدن ایـن کوکی‌هـا توسـط حمله‌هـای XSS می‌تواننـد کلمـه عبـور شـما را به دسـت آورنـد. پس هرگـز ایـن گزینه را بـه خصوص هنگامی کـه از رایانه در مکان‌هـای عمومـی و سیسـتم‌های اشـتراکی اسـتفاده می‌کنیـد، انتخـاب نکنیـد.

اعلام رمز عبور

اعضای شبکه‌های اجتماعی همواره با خطراتی همچون اعلام ناخودآگاه رمز عبور حساب کاربری توسط روش هوشمندانه مهندسی اجتماعی یا ترغیب به کلیک بر روی صفحه‌های ورودی دروغینی که مشابه با وب سایت شبکه‌های اجتماعی طراحی شده‌اند، روبرو هستند. در این روش، کلاهبردارها یک نام بسیار مشابه با دامنه وب سایت شبکه اجتماعی خاصی را ثبت کرده و با طراحی صفحه‌ای همانند صفحه اصلی ورودی همان سایت، به روش‌های مختلف از کاربر می‌خواهند که وارد شبکه اجتماعی مورد نظر شود. هدف کلاهبردارها از انجام این فریب زیرکانه، یافتن نام کاربری و کلمه عبور افراد، جهت تحقق هدف‌های بعدی خودشان است.

نصب برنامه‌های مخرب

بیشتر وقت‌ها، کلاهبردارها برنامه‌های مخربی را که عموماً تروجان هستند با عنوان نرم‌افزار یا فایل‌های جالبی که علاقمندان زیادی دارند، در شبکه‌های اجتماعی منتشر می‌کنند. این برنامه‌ها که معمولاً حجم کم و نصب بسیار آسانی دارند می‌توانند اطلاعاتی همچون رمزهای عبور، عکس‌های موجود در آلبوم تصاویر گوشی، حروف تایپ شده بر روی صفحه کلید و موارد مشابهی را تشخیص داده و آنها را به پست الکترونیک خاصی که قبلاً در برنامه مخرب مشخص شده، ارسال کنند.

این تروجان‌ها اغلب همراه فایل‌های اسکرین‌سیور، ویدیو یا عکس در اختیار کاربران قرار گرفته که فرد پس از کلیک بر روی فایل اصلی، همزمان برنامه مخرب را نیز اجرا می‌کند. از قابلیت‌های جدید این بدافزارها، دزدین اطلاعات حساب کاربری است که با آن، صفحه‌های اجتماعی خود را در این شبکه‌های آنلاین ایجاد کرده‌اید.

ایجاد پروفایلی مشابه پروفایل کاربری شما

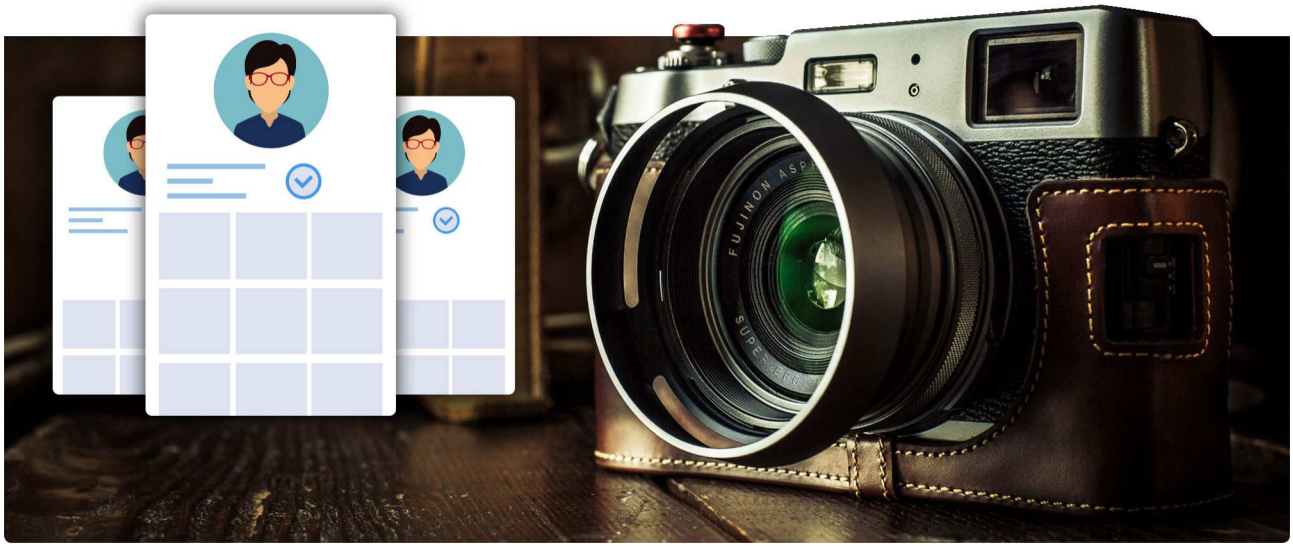
سارقان اطلاعات ممکن است با سر زدن به حساب کاربری شما در شبکه‌های اجتماعی و سرقت عکس‌های شخصی‌تان، از عکس-های شما برای ساخت پروفایل خودشان استفاده کنند. در این صورت، همزمان چند نفر پروفایلی مشابه شما را خواهند داشت. در چنین مواردی، هکرها ممکن است با حساب کاربری مشابه شما برای دوستان‌تان پیام‌هایی بفرستند که شما هرگز به آنها چنین پیام‌هایی نخواهید فرستاد!

مسدود کردن افراد مزاحم

اگر چه شبکه‌های اجتماعی، پیدا کردن دوست و در تماس بودن با افرادی که دوست‌شان دارید را برای شما بسیار ساده کرده‌اند اما این شبکه‌های دوست‌یابی سریع، گاهی موجب آشنایی با افرادی می‌شود که هدفی جز آزار و اذیت شما نداشته و با ارسال مداوم پیام‌های مزاحمت، باعث رنجش خاطرتان می‌شوند. در چنین مواقعی می‌توانید فرد مزاحم را از درون همان وب سایت یا برنامه کاربردی شبکه اجتماعی، مسدود کرده و برقراری ارتباط را برای او دشوارتر کنید. اگر چه فرد مزاحمی که شما آن را مسدود کرده‌اید، هیچ وقت از اقدام شما مطلع نمی‌شود ولی ممکن است پس از مسدود شدن، با ایجاد یک حساب کاربری جدید، باز هم اقدام به مزاحمت شما کند که در این صورت یا باید از خیر آن حساب کاربری گذشته و کاربری جدیدی برای خودتان ایجاد کنید یا دوباره حساب کاربری شخص مزاحم را مسدود کنید!

رعایت حریم خصوصی

از مهمترین چالش‌های پیش‌روی دست‌اندرکاران شبکه‌های اجتماعی و کارشناسان امنیت فناوری اطلاعات، حفظ حریم شخصی کاربران در فضای مجازی است. هر چند وقت یک‌بار، مدیران شبکه‌های اجتماعی به منظور سیاست‌های امنیتی بیشتر، در سرورها، برنامه‌های کاربردی و صفحه‌های وب سایت‌شان تغییرهایی را اعمال کرده و با انتشار اطلاعیه‌ای از کاربران می‌خواهند که تنظیمات حریم خصوصی خود را دوباره انجام دهند یا برنامه‌های خاصی که توسط کاربران آن شبکه استفاده می‌شود را به‌روزرسانی کنند. در صفحه تنظیمات حریم خصوصی، معمولاً تعریف‌هایی همچون مشخص کردن افرادی که اجازه جستجو و پیدا کردن کاربر در شبکه اجتماعی، ارسال درخواست دوستی یا پیام برای او، مشاهده لیست دوستان وی و غیره را دارند، وجود دارد. لازم است کاربران، این سطح دسترسی‌ها را با دقت کامل کرده و حتی برای مواردی هم که به اشتراک می‌گذارند آنها را اعمال کنند.



صفحه اجتماعی نه آلبوم عکس شخصی

یکی از موضوع‌های مهمی که متأسفانه بعضی از کاربران آن را رعایت نکرده و توجه چندانی به آن ندارند، اشتباه گرفتن صفحه‌شان در شبکه‌های اجتماعی با آلبوم عکس خصوصی‌شان است که می‌تواند موجب نقض حریم خصوصی آنها شود. کاربران در هنگام اشتراک‌گذاری عکس‌ها و ویدیوهای‌شان باید به این نکته توجه کنند که اگر چه ممکن است با خصوصی کردن صفحه‌شان فقط دسترسی آنهایی که خودشان می‌خواهند را به صفحه‌شان امکان‌پذیر کنند اما این موضوع زیاد مسأله ویژه‌ای نیست و همچنان امکان دسترسی به این عکس‌ها و مشاهده‌شان توسط سایرین وجود دارد.

استفاده از فیلترشکن‌ها

با مسدودی و فیلترینگ وب سایت‌ها و نرم‌افزارهای شبکه‌های اجتماعی غیربومی، همچنان بعضی کاربران برای سر زدن به صفحه-های خود در این شبکه‌ها از فیلترشکن‌ها کمک می‌گیرند. استفاده از نرم‌افزارهای فیلترشکن علاوه بر این که مطابق با قانون جرایم رایانه‌ای کشورمان جرم محسوب می‌شود، می‌تواند مخاطره‌های امنیتی جدی را نیز برای کاربران استفاده کننده در پی داشته باشد. همان‌طور که در زبان فارسی ضرب‌المثلی داریم که می‌گوید «گربه برای رضای خدا موش نمی‌گیرد»، این نرم‌افزارها هم اگر چه در ظاهر امکان دسترسی شما به وب سایت‌های مسدود شده و دور زدن فیلترینگ را فراهم می‌کنند ولی همزمان اقدام به سرقت اطلاعات گوشی تلفن همراه یا رایانه شما نیز می‌کنند.

حمله فیشینگ

از دیگر مخاطره‌هایی که کاربران در شبکه‌های اجتماعی به شدت با آن مواجه هستند، «فیشینگ» است. حمله فیشینگ برای تمامی افراد نوعی تهدید سایبری جدی به شمار می‌آید. احتمالاً افراد زیادی با این حمله آشنایی ندارند و این در حالی است که بیشتر وقت آنها صرف گشت‌وگذار در شبکه‌های اجتماعی شده و زمان کمتری را برای آگاهی از خبرهای مربوط به حمله‌های سایبری اختصاص می‌دهند. واقعیت این است که اگر دایماً با استفاده از زبان و ابزارهای مختلف نسبت به حملات فیشینگ آگاهی‌سازی نکنیم، هشدارها در رابطه با این چنین حمله‌هایی جدی گرفته نخواهند شد.

پیشنهاد آخر

هرگز فراموش نکنید که سهل‌انگاری در شبکه‌های اجتماعی، آسیب‌های جدی به حریم خصوصی شما، خانواده و حتی دوستان‌تان وارد خواهد کرد. پس بیشتر مراقب باشیم!

اهمیت آموزش مداوم کارمندان در زمینه امنیت سایبری

وجود همیشگی جرایم سایبری

اگر کارمندی نتواند در وهله اول تهدید را تشخیص دهد، چگونه می‌تواند آن را گزارش داده یا با آن مقابله کند؟ ما باید بدانیم که پیشرفت‌های فناورانه، هر چه انسان‌های دنیای امروزی را به هم متصل‌تر کرده و دستیابی به خدمات سازمانی را برای کارکنان و شهروندان سهل‌الوصول‌تر می‌کند، روش‌های هک کردن و حملات سایبری نیز پیشرفته‌تر می‌شود. در واقع، یک دلیل مهم برای لزوم آگاهی‌بخشی مداوم این است که همیشه جرایم سایبری وجود خواهند داشت.

سرمایه‌گذاری درست

خسارت‌های وارده از یک حادثه سایبری به سازمان می‌تواند برای تجارت آن بسیار گران تمام شود. از دست دادن اعتبار نزد مشتریان و سرمایه‌گذارن، سرقت سایبری مالکیت معنوی سازمان، اختلال در عملیات‌ها و فرایندهای کاری، سرقت اطلاعات شخصی سرمایه‌گذاران، کارکنان یا مشتریان سازمان از جمله این موارد است. با سرمایه‌گذاری در بخش آگاهی‌بخشی و آموزش امنیت سایبری، در واقع سازمان سرمایه‌گذاری پرسود درازمدتی خواهد داشت و در مقابل مخاطرات سایبری تا حدود بسیار زیادی بیمه خواهد شد.

اعتماد به نفس کارکنان

عامل مهم دیگری که از آگاهی‌بخشی مداوم کارکنان سازمان حاصل می‌شود، ایجاد یک اعتماد به نفس مناسب در کارکنان سازمان است. درصد زیادی از مردم با شنیدن خبرهای مربوط به سرقت داده‌ها و حملات سایبری احساس استرس می‌کنند. به‌روز نگهداشتن کارکنان سازمان از آخرین اطلاعات و فنون انجام حملات سایبری و روش‌های مقابله با آنها به کاهش اضطراب ناشی از عدم آگاهی از خطرات سایبری کمک خواهد کرد. علاوه بر کاهش استرس، آموزش‌های آگاهی‌بخش سازمان باعث از بین رفتن رفتارهای مخاطره‌آمیز و فرهنگ‌سازی بهترین اقدام‌های امنیتی در سازمان‌های سراسر کشور خواهد شد.

وجود همیشگی جرایم سایبری رضایت مشتریان و سهامداران

عامل دیگر در اهمیت آموزش مداوم کارکنان، رضایت مشتریان و سهامداران است. با سرمایه‌گذاری در آموزش‌های آگاهی‌بخش کارکنان در زمینه امنیت سایبری، مشتریان و سهامداران سازمان می‌توانند اطمینان حاصل کنند که شریک تجاری آنها آگاهی‌های ضروری را راجع به مخاطرات امنیتی ناشی از کار با داده‌ها دارد. همچنین به مرور، سرمایه‌گذاران می‌توانند به جایگاه و ارزش کنترل‌های سایبری و اهمیت سرمایه‌گذاری در آن بیشتر پی ببرند.

امنیت اطلاعات و برنامه‌های سفارشی سازمان

هر سازمان در راستای سیاست‌های تجاری خود، برنامه‌ها و اطلاعاتش را بومی یا سفارشی می‌کند. آگاهی‌بخشی به کارکنان سازمان در خصوص تهدیدهای سایبری می‌تواند عامل به‌سزایی برای امن نگهداشتن اطلاعات باارزش و سفارشی سازمان باشد.

نتیجه‌گیری

با تأکید بر امنیت سایبری به عنوان اولویت در سازمان و آگاهی‌بخشی و آموزش کارکنان، علاوه بر این که کارکنان آگاهی لازم جهت مقابله با تهدیدها را به دست می‌آورند، به مرور می‌تواند موجب افزایش فرهنگ سازمانی در حوزه مقابله با تهدیدهای سایبری شود. از سوی دیگر، کارکنان برای استفاده از فناوری‌های ایمن و رعایت خط‌مشی‌ها و رویه‌های امنیتی سازمان، رغبت و مشارکت بیشتری نیز خواهند داشت.

در فضای مجازی با آرامش و امنیت خاطر زندگی کنیم

هر روزه بر تعداد رایانه‌های شخصی و گوشی‌های هوشمند افزوده می‌شود. متناسب با این امر، آمار و اخبار حکایت از نوآوری بیشتر مهاجمان و مجرمان سایبری در حوزه جرایم سایبری دارد. برای این که از سیستم‌های خود در برابر آسیب‌هایی همچون سرقت اطلاعات و صدمه به سخت‌افزار، نرم‌افزار و اطلاعات ایمن باشیم باید به نکات بیشتری دقت کرده و امنیت بیشتری را در فضای مجازی خود فراهم کنیم.

ما در این مقاله، نکات امنیتی مهم و در عین حال ساده و کم هزینه‌ای که می‌تواند امنیت آنلاین شما را بهبود بخشد، بیان کرده‌ایم. پس با ما همراه باشید!

نکته اول:
حضور خود در فضای مجازی را جدی بگیرید

باید درک کنید که شما می‌توانید طعمه خوبی برای مجرمان سایبری باشید. کلاهبرداران سایبری، بیشتر حملات خود را به صورت خودکار انجام می‌دهند و شما نیز می‌توانید یکی از اهداف این حملات خودکار باشید. توجه داشته باشید که هر چه دارایی‌های بیشتری در فضای مجازی داشته باشید، بیشتر هم در معرض خطر هستید. این دارایی‌ها دیگر فقط پول نیست. اطلاعات شخصی، خانوادگی، حقوقی و تجاری نیز دارایی‌های مهمی محسوب می‌شوند.

نکته دوم:
مبانی خرید ایمن در فضای سایبر را در نظر بگیرید

هرگز از دستگاه غیرشخصی و سرویس‌های شبکه‌ای عمومی مانند اینترنت رایگان اماکن عمومی جهت انجام خرید آنلاین استفاده نکنید. اطمینان پیدا کنید که فقط خودتان امکان استفاد از کارت اعتباری خود را دارید. حملات فیشینگ، درصد این اطمینان را در هنگام استفاده از شبکه‌های عمومی پایین می‌آورند.

نکته سوم:
پیشنهادهای دوستی در فضای مجازی را با حساسیت بیشتری بررسی کنید.

مجرمان سایبری غالباً برای دوستی با شما پروفایل‌های جعلی ایجاد می‌کنند و هدفشان به دست آوردن اطلاعات محرمانه در مورد شما یا شرکتی است که برایشان کار می‌کنید. این کار که مهندسی اجتماعی نامیده می‌شود، بیشترین میزان موفقیت را در بین روش‌های مجرمانه دارد. پس مراقب درخواست‌های دوستی باشید. به هیچ دوستی در فضای مجازی اعتماد نکنید مگر این که در زندگی واقعی شما وجود داشته و کاملاً هم به او اطمینان دارید.

نکته چهارم:
از اتصال حافظه‌های جانبی ناشناس مانند فلش مموری یا هارد اکسترنال به دستگاه‌هایتان خودداری کنید.

مراقب حافظه‌های جانبی که به رایانه خود وصل می‌کنید باشید. مثلا یک USB که منبع آن برای شما مشخص نیست می‌تواند به بدافزارهایی آلوده باشد که حتی در برابر پارتیشن‌بندی هم مقاومت کند. گاهی کنجکاوی شما ممکن است عاملی برای سوءاستفاده از شما شود.

نکته پنجم:
شما هنوز هم به یک آنتی‌ویروس خوب و قدرتمند نیاز دارید.

با کمی تحقیق، آنتی‌ویروسی را که قدرتمند بوده و مورد اطمینان‌تان است، انتخاب و نصب کنید. به این نکته توجه داشته باشید که صرف هزینه برای آنتی‌ویروس بهتر از تهیه رایگان آن است. هرگز فراموش نکنید که آنتی‌ویروس، هنوز هم بسیار ضروری است.

نکته ششم:
حساب‌های بانکی خود را مرتب چک کنید.

صورت حساب‌های بانکی خود را به صورت هفتگی و منظم بررسی کنید. برای این کار می‌توانید از نرم‌افزارهای بانکداری آنلاین استفاده نمایید. به دنبال فعالیت‌های مشکوک در حساب خود باشید و در صورت برخورد با مورد مشکوکی حتماً به بانک اطلاع داده و کلمه عبور حساب را سریعاً تغییر دهید. بدافزارهای مالی در کمین حساب‌های شما هستند.

نکته هشتم:
رایانه یا گوشی هوشمند خود را مثل کمد خودتان تمیز و مرتب کنید.

همان‌طور وسایلی را که استفاده نمی‌کنید، از وسایل مورد استفاده روزمره خود خارج می‌کنید تا کمد شما مرتب بماند، برنامه‌های کاربردی هم که در شش‌ماه گذشته از آنها استفاده‌ای نکرده‌اید را پاک کنید. برنامه‌های قدیمی همیشه مکانی برای سرک کشیدن مجرمان سایبری هستند.

نکته هفتم:
برای رایانه، لپ‌تاپ و گوشی هوشمند خود قفل صفحه تنظیم کنید.

هرگز رایانه شخصی، لپ‌تاپ، گوشی هوشمند یا تب‌لت خود را قفل نکرده رها نکنید. به این طریق، ورود هر شخصی را به سیستم خود سخت کنید. تنظیم کلمه ورود و قفل، زمان زیادی از شما نمی‌گیرد؛ شاید فقط در حد ۲-۳ دقیقه.

نکته نهم:
حساب‌های اینترنتی خود را مدیریت کنید.

لیست حساب‌های اینترنتی خود را تهیه کنید. دقت کنید تا برای همه حساب‌های‌تان کلمه عبور قوی در نظر گرفته باشید. حساب‌های اینترنتی که در ماه‌های اخیر از آنها استفاده نکرده‌اید را حذف کنید. این شفافیت حساب‌ها همچنین حس خوبی به شما می‌دهد.

نکته دهم:
مراقب اهداف و انگیزه‌های پنهانی لینک‌های پیوندی پیشنهادی باشید.

مجرمان سایبری اغلب پروفایل‌های جعلی در شبکه‌های اجتماعی ایجاد می‌کنند تا به این طریق بتوانند به جزییات اطلاعات سایر اشخاص دسترسی پیدا کنند؛ جزییاتی که بعداً می‌توانند از آنها استفاده کنند. اطلاعات مربوط به مطالعات شما، نام کارفرمایان یا حتی لینک‌هایی که به آن مراجعه می‌کنید را جمع‌آوری کرده و از آنها استفاده می‌کنند.

نکته یازدهم:
نرم‌افزارهای خود را به‌روزرسانی کنید.

با به‌روزرسانی سیستم عامل و برنامه‌های خود می‌توانید از ۸۵٪ حمله‌های سایبری هدفمند جلوگیری کنید. اگر هم وقت و حوصله به‌روزرسانی مداوم برنامه‌های خود را ندارید می‌توانید از نرم‌افزارهایی که در مقابل حملات سایبری، سیستم شما را تا حد زیادی ایمن نگه می‌دارند استفاده کنید.

نکته دوازدهم:
کلمه‌های عبور خود را متفاوت انتخاب کنید.

یکی از نکات کلیدی که همه متخصصان امنیت سایبری ارایه می‌دهند استفاده نکردن از رمز عبورهای تکراری و قابل حدس است. یعنی برای حساب‌های متفاوت، رمزهای متفاوت تعیین کنید. البته فکر نکنید که انتخاب رمزهایی مثل "password۱۲۳" و "passwords۱۲۳۴" به این معنی است که رمزهای متفاوت خوبی انتخاب کرده‌اید باید تفاوت را کمی بیشتر کنید. شاید فکر کنید رمزی مثل (c. *٪ ۷ :wQ، ۲۸ {T ^ ۷) حتما رمز خوبی است ولی باز هم باید بگویم که از این چنین رمزها هم استفاده نکنید چرا که نمی‌توانید به خاطر بسپارید.

نکته سیزدهم
باج‌افزارها یکی از بزرگترین تهدیدهای سایبری محسوب می‌شوند.

باج‌افزارها دسترسی به سیستم شما را محدود می‌کنند. آنها می‌توانند داده‌های شما را رمزنگاری کرده و رایانه شخصی یا لپ‌تاپ شما را قفل کنند. سپس برای برداشتن محدودیت و رمزگشایی از فایل‌هایتان، از خود شما باج می‌خواهند. نکات زیر را برای محافظت از خود در برابر باج‌افزارها در نظر بگیرید:

- از داده‌های خود به طور مکرر و در چندین مکان پشتیبان بگیرید.
- اطلاعات حیاتی خود را فقط در رایانه خود نگهداری نکنید.
- ایمیل‌های ناشناس خود را باز نکنید.
- بر روی لینک‌های پیوندی موجود در ایمیل‌هایی که فرستنده ناشناس دارند، کلیک نکنید.
- سیستم عامل و برنامه‌های خود را همیشه به‌روز نگه دارید.
- از یک آنتی‌ویروس خوب و مطمئن استفاده کنید.
- لایه‌های امنیتی خود را افزایش دهید تا اگر حمله‌ای به وسیله آنتی‌ویروس قابل دفع نبود، در لایه‌های بعدی مهار شود.

نکته چهاردم:
دسترسی نداشتن به مکان‌های ناامن، خطر هک شدن را از بین نمی‌برد.

بسیاری از مردم فکر می‌کنند که چون به مکان‌های ناامن دسترسی ندارند، به برنامه‌های امنیتی هم احتیاجی ندارند.

در این خصوص به چند نکته باید توجه داشت:

- اول این که حتی وب سایت‌های قانونی هم می‌توانند به خطر بیافتند.
- دوم این که حملات زیادی وجود دارد که حتی اگر شما بر روی چیزی کلیک نکرده باشید و یا داده‌های مشکوکی را دانلود نکرده باشید، باز هم برای شما اتفاق میافتد.
- سوم این که حتی اگر شما کارشناس امنیت سایبر هم باشید، باز هم حفره‌های آسیب پذیر زیادی وجود دارد که مهاجمان می‌توانند از آنها سوءاستفاده کنند تا به شما برسند.

ایمن بودن از این حملات، کاملاً شبیه رانندگی اتومبیل شما است. ممکن است شما راننده محتاط و قانونمندی باشید و به تمامی خطرات احتمالی توجه کنید ولی آیا همیشه می‌توانید پیش‌بینی کنید که رانندگان دیگر، چه رفتاری دارند و چقدر قوانین را رعایت می‌کنند؟

در نهایت باید بگویم که نگران نباشید و فکر نکنید که شما گزینه خوبی برای هک شدن هستید ولی همیشه تا می توانید نکات امنیتی را رعایت کنید.

گزارش و مصاحبه

سال ۲۰۲۰ و تهدیدهای سایبری پیش رو

سال ۲۰۲۰ و تهدیدهای سایبری پیش رو

سال ۲۰۲۰ میلادی، با ادامه مناقشات داخلی آمریکا بر سر موضوع استیضاح رئیس جمهور این کشور و انتخابات پیش رو شروع شد. ادامه جاه‌طلبی‌ها و ماجراجویی‌های ایالات متحده و شخص رئیس جمهور فعلی آمریکا در منطقه غرب آسیا که با ترور و به شهادت رساندن سردار سلیمانی، عالی‌رتبه‌ترین فرمانده نظامی برون مرزی ایران به اوج خود رسید، وضعیت این منطقه راهبردی و بالطبع کل دنیا را دستخوش تغییر و اضطرار کرده است.

این موارد بر فضای مجازی نیز بی‌تأثیر نبوده و تحولات بسیاری را در این محیط رقم زده است. در این مدت، ایران از دفع چند حمله سایبری گسترده به زیرساخت‌های حیاتی خود خبر می‌دهد و ایالات متحده نیز مدعی حملات سایبری ایران به سازمان‌های خود از جمله پایگاه‌های اینترنتی دولتی شده است. با توجه به این که جهان غرب و علی‌الخصوص آمریکا می‌داند شروع جنگ تمام عیار در غرب آسیا، کل منطقه را به آتش کشیده و اقتصاد و تولید را در کل جهان فلج می‌کند، بنابراین بدیهی است که دامنه چنین دشمنی‌هایی به جنگ‌های سرد و روانی و همچنین جنگ سایبری کشیده خواهد شد.

فضای سایبر با دو ویژگی گمنامی و عدم استناد خود، فضای مناسبی را برای ضربه زدن و مسئولیت‌ناپذیری دولت‌های متخاصم به وجود آورده است و دولت‌ها برای نیل به اهدافشان در فضای سایبر، از ایجاد گروه‌های سازمان‌یافته هکری بی‌نیاز نیستند. گاه چندین کشور با یک هدف واحد، هر کدام بخشی از وظایف محوله را در رسیدن به آن در این فضا بر عهده می‌گیرند.

بر اساس پیش‌بینی کارشناسان فراست، تهدیدهای فضای سایبری؛ بیشتر با تغییر جهت‌شان در سال ۲۰۲۰ کماکان ادامه پیدا خواهند کرد و اصل تهدیدها نیز همچنان به قوت خود باقی خواهد ماند. عدم انتشار Owasp Top ۱۰ جدید هم مؤید این نظر است که سال پیش رو، تغییرات کلیدی را در نوع تهدیدهای موجود بر ضد وب سایت‌ها رغم نخواهد زد. آن چه در ادامه می‌خوانید، پیش‌بینی تهدیدهای امنیتی در سال ۲۰۲۰ است که در دپارتمان فراست انجام شده است.

تغییر جهت حملات باج‌افزاری به سمت مراکز و سازمان‌های کوچک و محلی

سازمان‌ها و مراکز دولتی کوچک و محلی (مثل شهرداری‌ها و مراکز بهداشت و درمانی) معمولاً به دلیل محدودیت بودجه‌ای که برای‌شان در نظر گرفته می‌شود، نرم‌افزارهای امنیتی محدودی داشته و در عین حال اطلاعات خوبی هم برای باج‌افزارها می‌توانند داشته باشند. در مقایسه با نهادها و سازمان‌های دولتی بزرگتر با منابع مالی بیشتر، در این نهادهای محلی دانش و پشتیبانی فنی محدود، منجر به استفاده از زیرساخت‌های منسوخ و امنیت پایین می‌شود. همه این عناصر خطرناک، منجر به قربانی شدن این سازمان‌ها و مراکز حتی در ابتدایی‌ترین حملات باج‌افزاری خواهند شد. پیش‌بینی می‌شود در سال ۲۰۲۰، حملات باج‌افزاری بیشتری را نسبت به سال‌های گذشته به سمت چنین سازمان‌هایی شاهد باشیم.

قرارهای مجرمانه سایبری در اتاق‌های تاریک اینترنتی

با وجود قوانینی که برای اتاق‌ها و تالارهای گفتگو گذاشته شده است ولی همچنان تالارهای گفتگو به خصوص در وب تاریک، محل مناسبی برای دورهمی مجرمان سایبری و رد و بدل کردن اطلاعات، پیشنهادهای هکری و سفارش کار نفوذگری است. همان‌طور که در تالارهای گفتگو، هماهنگی‌ها و پیام‌های خصوصی یا تبلیغات در بازارهای آنی انجام می‌شود، این محیط یک مکان اصلی برای مجرمان سایبری نیز محسوب می‌شود. با توجه به رشد فزاینده اتاق‌های گفتگو از طریق سایت‌ها و شبکه‌های اجتماعی، دور زدن قوانین و رسیدن به اهداف مجرمانه بسیار رشد داشته است و پیش‌بینی می‌شود اگر در سال ۲۰۲۰ قوانین و کنترل سایبری جدیدی در این خصوص انجام نشود، همچنان قرارهای مجرمانه در این اتاق‌ها ادامه و رشد یافته و شرکت‌ها حملات سازمان‌یافته‌تر گروهی بیشتری را با ابزارهای نسبتاً قدرتمند تجربه کنند.

در معرض تهدید بیشتر قرار گرفتن داده‌های سازمانی ذخیره شده در فضاهای ابری

از آنجا که سازمان‌ها به طور فزاینده‌ای داده‌ها و بار پردازشی خود را به ابرها منتقل می‌کنند می‌توان انتظار داشت که مجرمان سایبری، بیش از پیش ارایه‌دهندگان خدمات ابری را مورد هدف خود قرار دهند. سازمان‌ها همان‌طور که به دنبال امنیت بیشتر بر روی داده‌های داخلی خود هستند، به امنیت داده‌ها و اطلاعات خود در محیط ابری هم توجه داشته و به ارایه‌دهندگان چنین خدماتی فشار می‌آورند که امنیت بیشتری را برای‌شان فراهم کنند. قاعدتاً سازمان‌هایی که با داده‌های حساسی سروکار دارند، طعمه وسوسه‌انگیزی برای مجرمان سایبری خواهند بود. پیش‌بینی می‌شود که در سال ۲۰۲۰، حملات مجرمانه به منظور سرقت و افشای داده‌های سازمانی موجود در فضای ابری بیشتر از قبل ادامه یابد.

افزایش حملات به پرداخت‌های موبایلی و نرم‌افزارهای سازمانی موبایلی

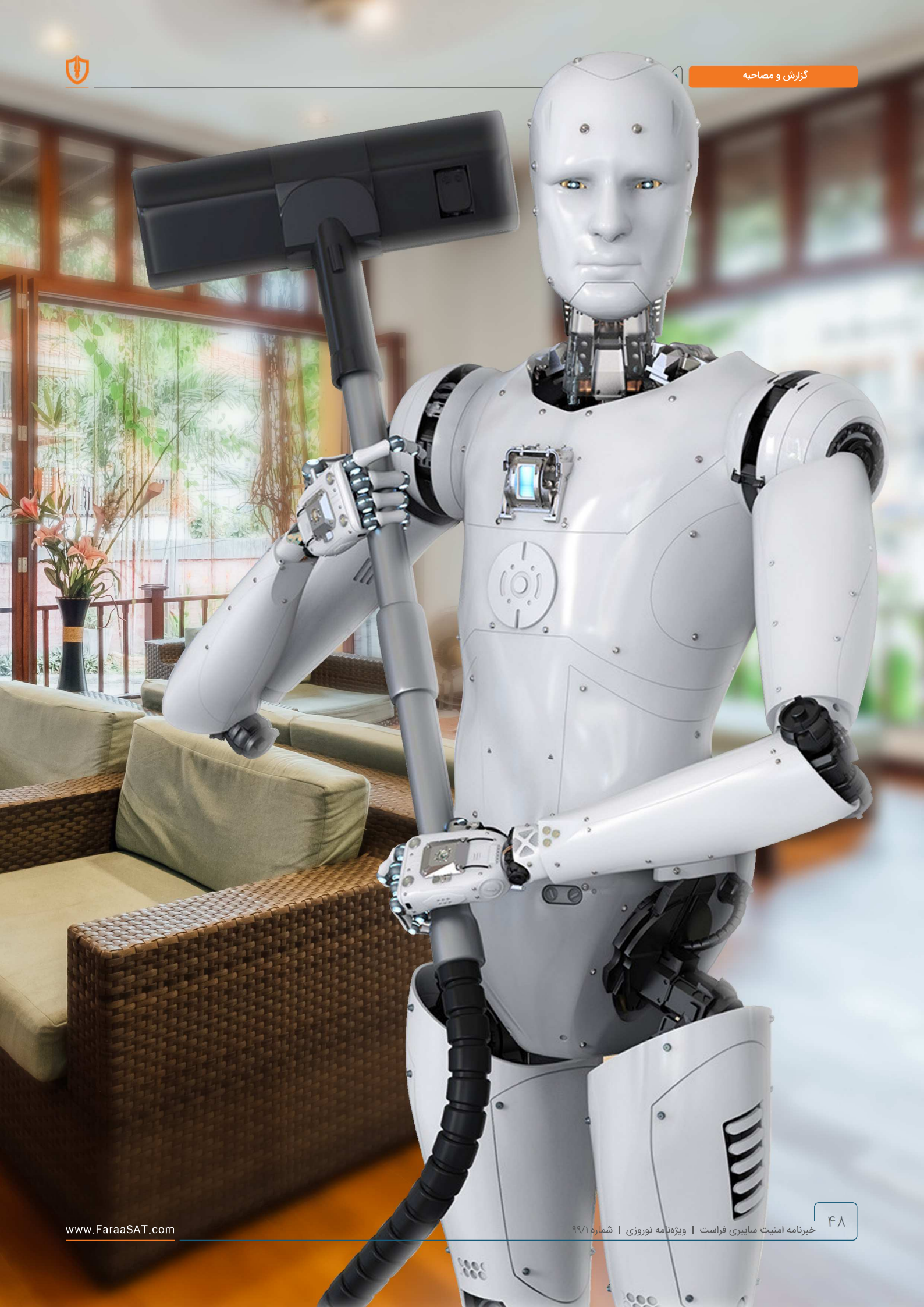
توسعه روزافزون کاربرد موبایل برای انجام بهتر و سریعتر امور شخصی و سازمانی، گسترش استفاده از آنها را برای انجام فرایندهای مالی و کسب‌وکار سازمانی در پی داشته است. چنین موضوعی از دید هکرها و نفوذگران سایبری هم پنهان نمانده است. پیش‌بینی می‌شود در سال ۲۰۲۰، افزایش چشم‌گیری را در حملات به فرایندهای مالی در پلتفرم‌های موبایلی و بهره‌برداری از آسیب پذیری‌های نرم افزارهای سازمانی در گوشی تلفن همراه و نیز BYOD شاهد باشیم.

افزایش تسویه حساب‌های سیاسی در فضای مجازی

نزدیک به دو دهه است که فضای سایبر به عنوان چهارمین میدان نبرد، مورد توجه دولت‌ها در بعد نظامی قرار گرفته است. این میدان نبرد، صرفاً برای انجام دشمنی‌ها و جنگ‌های سایبری مورد استفاده قرار نگرفته و در دهه اخیر، از این فضا به عنوان مکمل فضای سیاسی داخلی در درگیری‌ها و رقابت‌های سیاسی دولت‌ها و ملت‌ها استفاده می‌شود. مصداق بارز چنین کاربردهایی، در بعد اجتماعی، رقابت‌های انتخاباتی، شایعه پراکنی‌ها، ایجاد فضای آشوب و ناامیدی در جوامع مختلف و در نهایت بحران سیاسی ناشی از ایجاد نارضایتی عمومی است. در بعد فنی نیز حملات سازمان‌یافته از سوی کشورهای متخاصم جهت دستکاری و تقلب در سامانه‌های تعیین کننده نتایج سیاسی یک کشور مانند انتخابات، از مصادیق کاربردهای فضای سایبر در مسایل سیاسی به شمار می‌رود. پیش‌بینی می‌شود در سال ۲۰۲۰ و با توجه به در پیش رو بودن انتخابات آتی در آمریکا شاهد گسترش حملاتی از این نوع باشیم.

کاربردهای هوش مصنوعی؛ روی دیگر سکه

علوم مرتبط با فضای سایبر مانند سایر علوم، از کاربردهای هوش مصنوعی بهره می‌برند. در امنیت فضای سایبری، با دو رویکرد متفاوت از کاربرد هوش مصنوعی مواجه هستیم. در این فضا از الگوریتم‌های هوش مصنوعی برای اهداف امنیتی و حتی ضدامنیتی استفاده می‌شود. آن چه در سال ۲۰۲۰ پیش‌بینی می‌شود، افزایش رقابت بین شرکت‌های امنیتی و جامعه هکری جهانی در استفاده از هوش مصنوعی در رسیدن به اهداف‌شان است.



حمله مجرمان سایبری از طریق زنجیره‌های تأمین

حمله زنجیره تأمین که به آن حمله زنجیره‌ای یا شخص سوم نیز گفته می‌شود، هنگامی رخ می‌دهد که شخص یا گروه هکری (عموماً دولتی) از طریق دسترسی‌های یک پیمانکار یا تأمین کننده خارجی به سیستم‌های سازمانی نفوذ کند. حمله Target ۲۰۱۳ و بدافزار استاکس‌نت که در سال ۲۰۱۰ کشف شدند، از طریق ارایه‌دهندگان شخص سوم آسیب پذیر آغاز شده‌اند.

اشخاص سوم معمولاً به سیستم‌های مهم سازمان‌ها دسترسی دارند. بسیاری از پیمانکاران و تأمین کنندگان خدمات و محصولات، دارای برنامه‌ها و فرایندهای امنیت سایبری ضعیفی هستند که آنها را به هدفی غنی برای مجرمان سایبری تبدیل کرده است. بنابراین حملات زنجیره تأمین همواره در فرکانس و پیچیدگی، گسترده‌تر شده و رو به رشد هستند و اگر شرکت‌ها سیاست‌های امنیتی و حریم خصوصی همگی تأمین کنندگان خود را ارزیابی نکنند، قاعدتاً به درک درستی از ماهیت مخاطرات خود نرسیده‌اند. پیش‌بینی می‌شود در سال ۲۰۲۰ میلادی همچنان حملات زنجیره تأمین، به رشد روز افزون خود ادامه دهند.

اینترنت اشیاء

آسانی در استفاده از تجهیزات سخت‌افزاری و پلتفرم‌های نرم‌افزاری لازم برای پیاده‌سازی اینترنت اشیاء، موجب افزایش کاربردهای این فناوری در زندگی روزمره انسان‌ها شده است. در این مسیر اما آن چه که کمتر از آسایش و رفاه مصرف کنندگان مورد توجه تولیدکنندگان و خدمات دهندگان قرار گرفته است، امن‌سازی بستر ارتباطی تجهیزات به کارگیری شده، علاوه بر امن‌سازی محصولات تولیدی بوده است. بعد از شبکه‌های اجتماعی، اینترنت اشیاء بهترین مکان برای پیاده‌سازی بات‌نت‌ها محسوب می‌شود. با این وجود، حوزه عملکرد بات‌نت‌ها در اینترنت اشیاء بسیار گسترده‌تر از شبکه‌های اجتماعی است. در صورت نفوذ هکرها به تجهیزات IoT، آنها قادر خواهند بود تجهیزات موجود را جهت انجام عملکردهای فیزیکی کنترل کنند که تصور این موضوع هم می‌تواند به شدت برای شبکه‌های کنترل صنعتی وحشتناک باشد. در حال حاضر، خانواده بدافزارهای Mirai جدید، تهدیدی جدی برای استفاده از اینترنت اشیاء محسوب می‌شوند. در سال ۲۰۲۰ با گسترش استفاده از اینترنت اشیاء، به دلیل فراهم شدن بستر لازم برای فعالیت بات‌نت‌ها، تهدیدهای ناشی از آنها نیز کماکان بیشتر خواهد شد. بنابراین انتظار می‌رود در این سال با افزایش حملاتی در این حوزه روبرو باشیم.

افزایش حملات بدافزاری به دستگاه‌های پزشکی؛ تهدیدی برای جان و سلامت انسان‌ها

در گذشته، تولیدکنندگان دستگاه‌ها و تجهیزات پزشکی از سیستم عامل‌های اختصاصی یا ویژگی‌های خاصی برای تولید چنین تجهیزاتی استفاده می‌کردند که امکان هک شدن آنها را برای مجرمان سایبری سخت‌تر و تا حدودی محدودتر می‌کرد. در حال حاضر، به دلیل تنوع بسیار زیاد دستگاه‌های پزشکی و نیز افزایش نیاز بیماران و بیمارستان‌ها به دستگاه‌های جدید و به‌روز تشخیصی و بالینی، تولیدکنندگان در حال ساخت دستگاه‌های پزشکی ارزان‌تر و در دسترس‌تر بوده و سیستم عامل‌ها نیز عمومی‌تر شده‌اند. این مسأله، دستگاه‌ها و تجهیزات پزشکی را به طعمه مناسبی برای هکرها و حملات باج‌افزاری تبدیل کرده است.

به دلیل ماهیت حساس و بحرانی تجهیزات پزشکی که با جان انسان‌ها سروکار دارد، مجرمان سایبری تقریباً مطمئن هستند که قربانیان حملات این حوزه، حتماً اقدام به پرداخت هزینه‌های مورد نظر آنها به ویژه باج‌افزارها خواهند کرد. بنابراین پیش‌بینی می‌شود در سال ۲۰۲۰ میلادی، دستگاه‌های پزشکی گزینه بسیار مناسبی برای مجرمان سایبری بوده و اگر راهبرد مستند و منظمی برای امنیت بیشتر در این حوزه به کار گرفته نشود تجهیزات ناامن پزشکی، آسیب‌های جدی و بسیار مخاطره‌آمیزی را برای بهداشت و سلامت عده زیادی از شهروندان به رقم خواهند آورد.

سوءاستفاده از بهداشت و سلامت

مجرمان سایبری مدام به دنبال به دست آوردن منابع مالی بیشتری هستند. از این‌رو، شرکت‌های بیمه خدمات درمانی و ارایه-دهندگان خدمات بهداشتی به دلیل این که با منابع پولی زیادی در ارتباط هستند می‌توانند اهداف خوبی برای حمله‌های سایبری باشند. مجرمان سایبری با استفاده از وب سایت‌های جعلی ارایه‌دهنده خدمات یا پیامک‌های دروغین با ادعاهای کاذب و مطالبات تکراری، به دنبال کلاهبرداری بیشتر هم از شرکت‌های بیمه‌ای و ارایه‌دهندگان خدمات بهداشتی و درمانی و هم از مصرف کنندگان از همه جا بی‌خبر هستند. در حوزه خدمات بهداشتی، همان‌طور که شرکت‌ها مجبور به نوآوری در ابزارهای بهداشتی به منظور نجات جان انسان‌ها و بهبود سلامتی آنها هستند باید برای حفظ امنیت سایبری خود نیز هزینه کنند. بنابراین اگر بودجه کافی برای بهبود امنیت‌شان صرف نکنند، با تهدیدهای بیشتری هم در آینده مواجه خواهند بود.

در حوزه بیمه خدمات درمانی نیز مردم ناگزیر از روی آوردن به بیمه‌های خدمات درمانی بوده و نیاز به استفاده از خدمات بیمه‌ای هر روز بیشتر هم می‌شود که با رشد بیمه‌گذاران و شعب آنها مواجه خواهیم بود. بنابراین پیش‌بینی می‌شود در سال ۲۰۲۰، هم شرکت‌های بیمه‌ای و هم شرکت‌های ارایه‌دهنده خدمات بهداشتی با تهدیدهای بیشتری از جانب بدافزارها و باج‌افزارها روبرو باشند.

زنگ تفریح

کاریکاتور

اینفوگرافی

داستان


مدیـر :
چکار داری می کنی؟
کارمنـد:
در حال مانیتورینگ و پایش امنیتی
فضای ذخیـره سـازی ابـری شرکتـم

باج‌افزار چگونه کار می‌کند؟

باج افزارها به سرعت در حال رشدند!

باج افزارها هر روز با شتاب بیشتری رشد می کنند و اخیراً در حوزه تهدیدات سایبری، کانون توجه قرار گرفته اند. FBI اعلام کرده است که حملات باج افزاری در سال ۲۰۱۶ بیش از یک میلیارد دلار خسارت به بار آورده است.

باج افزار چیست؟

باج افزار نوعی نرم افزار مخرب است که به هکر این امکان را می دهد که دسترسی شخص یا شرکتی را به اطلاعات حیاتی اش محدود کرده و برای از بین بردن این محدودیت، پرداخت مبلغی(معمولاً بیت کوین) را تقاضا می کند.

۲۰۹ میلیون دلار مقدار مبلغی که در سال ۲۰۱۶ به مجرمان سایبری که از باج افزار استفاده کردند، پرداخت شد

۱ میلیارد دلار مقدار مبلغی که FBI به عنوان ضررهای ناشی از حملات باج افزاری در سال ۲۰۱۶ تخمین می زند

٪ ۷۲

درصد شرکت هایی که تحت تأثیر حمله باج افزاری، حداقل تا ۲ روز پس از حمله نمی توانند به داده های خود دسترسی داشته باشند

٪ ۳۲

درصد شرکت‌هایی که دسترسی به داده‌های خود را برای ۵ روز یا بیشتر از دست داده‌اند

مدت زمانی که معمولاً از زمان حمله تا تقاضای وجه طول می کشد

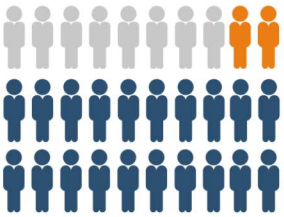
۱۵ دقیقه

۱۰ تا ۵۰ میلیون دلار

برآورد درآمد ماهانه از باج‌افزار برای مجرمان سایبری

٪ ۸۶

حملات هایی که ۲ نفر یا تعداد بیشتری از کارمندان را تحت تأثیر قرار داده اند



٪ ۴۷

حمله هایی که بیش از **۲۰ کارمند** را تحت تأثیر قرار داده اند

۱۷ هزار دلار

مبلغی که مرکز پزشکی وابسته به پروتستان در هالیوود در سال ۲۰۱۶ برای دسترسی دوباره به داده های خود پرداخت تا کسب و کار خود را به حالت معمول بازگرداند

۱۰ هزار دلار

مبلغی که این بیمارستان به دلیل ناتوانی در انجام سی تی اسکن بیماران خود در هر روز از دست می داد.

بیشتر مراقب باشیم!

مهندسی اجتماعی روشی پیشرفته برای نفوذ به شبکه سازمانی و سرقت اطلاعات است.

Bitdefender

آنتی ویروس سازمانی
بیت‌دیفندر

رهبری در مبارزه با بدافزارها

با امکاناتی نظیر آنتی ویروس، آنتی فیشینگ، دیواره آتش، ضد باج افزار و...

امنیت جامع و همه جانبه

امنیت در محیط های متنوع امروزی، نظیر بستر های مجازی،
فیزیکی و نیز دستگاه های هوشمند همراه

مدیریت یکپارچه

ابزار مدیریت امنیت GravityZone امکان نظارت و محافظت از
بستر های مختلف در شبکه های سازمانی را فراهم می کند

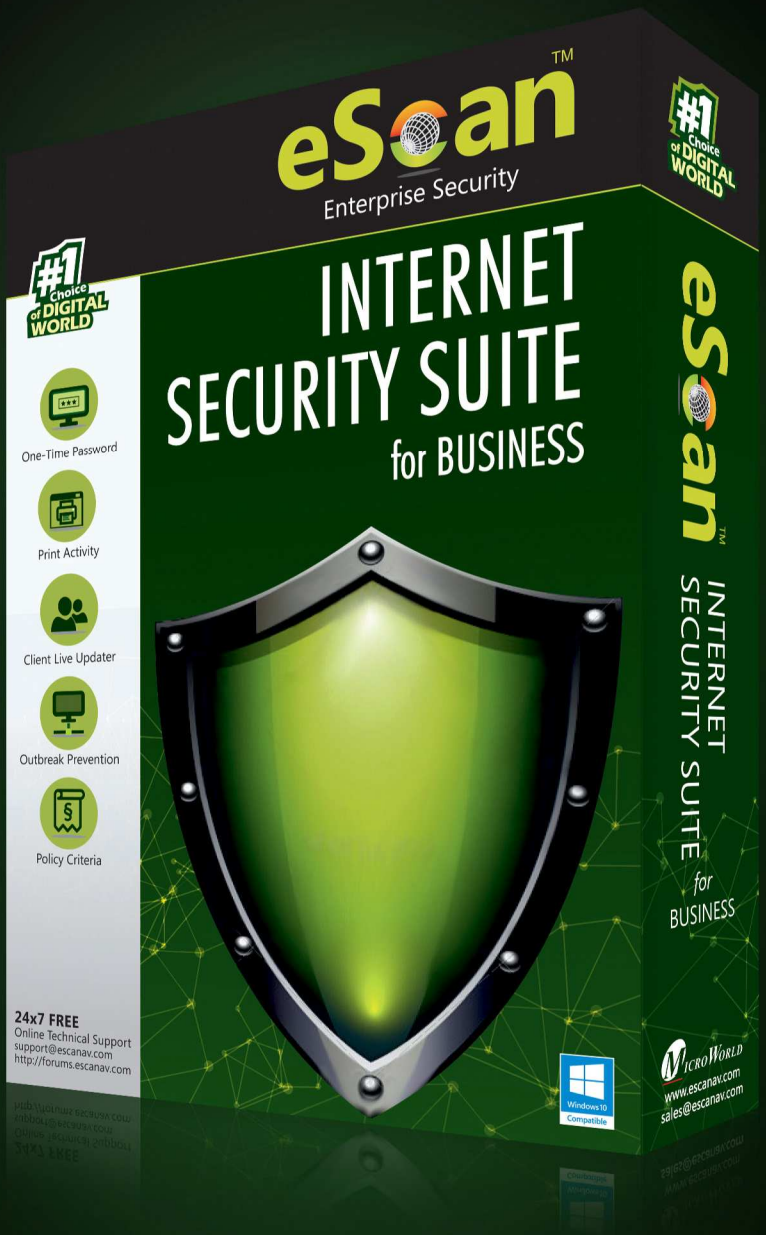
ساختار منحصر بفرد

ساختار GravityZone امکان مقیاس پذیری را به آسانی فراهم آورده
و قادر است امنیت شبکه را با هر تعداد سیستم، تامین نماید.

www.ParsAvan.com
(۰۲۱) ۹۱۰۰۵۴۱۸
Sales@ParsAvan.com

eScan™

آنتی ویروس سازمانی ای اسکن



www.eScaniran.com

۰۹۳۸ ۹۰۹ ۴۱۴۱ 24

۰۲۱-۹۱۰۰۵۴۱۸