گزارش

مجمع ایرانی دفاع از حقیقت

Iranian Council For
Defending The Truth

دی ۱۴۰۰

امنیت سایبـــــری

بسم الله الرحمن الرحیم

فهرست

پیشگفتار ۱
مقدمه ۲
اخبار ۳

۱۶ گزارش: لزوم تغییر در نحوه عملکرد پنتاگون در خصوص هوش مصنوعی
۱۹ کارشناسان درب پشتی مستقر در شبکه آژانس‌های فدرال ایالات متحده را کشف کردند
۲۰ فیشرها برای جمع آوری اطلاعات بانکی و سایر مدارک هویتی خود را به جای فایزر جا می زنند
۲۱ یک باگ بلوتوث سبب خطا و مثبت شدن تست COVID-۱۹ می‌شود
۲۱ بایدن برترین مؤسسه پزشکی نظامی چین را در لیست سیاه کنترل صادرات قرار داد

۲۴ توییتر، متا و تیک تاک به دلیل محتوای ممنوعه در روسیه جریمه شدند
۲۵ رقابت‌های جنگی اوکراین شبکه برق این کشور را محک می‌زند

۲۸ گزارش: تحقیقات، جاسوس افزار پگاسوس در تلفن همسر جمال خاشقجی را به ماموران امارات متحده عربی مربوط می کند
۲۹ مرکز جدید کنترل و فرماندهی سایبری اسرائیل برای حفظ ایمنی حمل و نقل
۳۱ ارتش اسرائیل و ایالات متحده مانور مشترک امنیت سایبری را به پایان رساندند

۳۴ آموزش و پرورش باید بر امنیت سایبری توجه کند
۳۷ روندهای امنیتی برای سال ۲۰۲۲ - نیاز به استعدادها و مهاجرت ابری

Iranian Council For
Defending The Truth

پیشگفتار

۱

پیشگفتار

مجمع ایرانی دفاع از حقیقت مادام همه تلاش خود را انجام می‌دهد که با به کارگیری شبکه‌ای از نخبگان در حوزه‌های مختلف سیاسی و شناختی گامی در جهت جلوگیری از ایجاد سوءتفاهم بردارد. در همین خصوص ما در مجمع ایرانی دفاع از حقیقت رسالت خود میدانیم تا با تهیه دیدبان‌هایی از موضوعاتی که به عنوان کارویژه برای خود انتخاب کرده‌ایم، چشم اندازی از مسیر را ارائه داده و در صورت توان پیشنهاداتی نیز برای کاهش این سوءتفاهم‌ها در آنان جای دهیم. ناگفته نماد که این دیدبان خود بخشی از راه حل کاهش سوءتفاهم است.

مجمع ایرانی دفاع از حقیقت
میز مطالعات امنیت

Iranian Council For
Defending The Truth

مقدمه

۲

مقدمه

اطلاع از اخبار و وضعیت فضای سایبر در ایالات متحده این امکان را فراهم می‌سازد تا با مسائل و مشکلات این حوزه سریع‌تر آشنا شده و هم‌چنین پیش از این که کشور ما نیز به آن مصائب و دشواری‌ها دچار گردد، راهکارهای اصلاحی را پیش‌بینی نماییم. از طرفی، با توجه به این که در اظهارات عمومی و جلسات رسمی مقامات این کشور برخی از نقاط ضعف دشمن در زمینه سایبری و فناوری‌های نوین بیان می‌گردد و با توجه به این نکته که بخش سایبری ایران توانایی آن را دارد که در تقابل با ایالات متحده از همین ضعف‌ها بهره‌برداری کند و به دشمن ضربه بزند؛ فلذا می‌توانیم از نقاط ضعف حریف استفاده نماییم و زمین بازی را به نفع خود تغییر دهیم و در موضع آفندی قرار بگیریم.

این تذکر ضروری است که با توجه به پیشگامی کشور امریکا در عرصه تکنولوژی، بررسی پیشرفت‌ها و برنامه‌ریزی‌های کلان این کشور در زمینه فناوری پیش‌بینی مقصد نهایی مسیر تکنولوژی در آینده را ممکن می‌سازد.

در بولتنی که در اختیار دارید اهم اخبار و اتفاقات کلان حوزه سایبر، تکنولوژی و فناوری‌های نوین جمع‌آوری شده است تا مخاطبین و فعالین در این زمینه بتوانند نسبت به وضعیت ایالات متحده از نگاهی جامع، کلان و به‌روز برخوردار شوند.

دیدکلی

این شماره از گزارش امنیت سایبری ICDT، در چهار بخش تحت عناوین «ایالات متحده»، «سایبر بین‌الملل»، «محیط سایبری اسرائیل» و «گزارش‌های راهبردی» تنظیم شده است. بخش نخست هم‌چون گذشته به اخبار سایبری ایالات متحده می‌پردازد. قوانین و اقدامات اخیر امریکا بی‌شک تحولاتی را در سالهای آتی بر فضای جهانی سایبر به همراه خواهد داشت که توجه به آنها برای پیش‌بینی روندها حائز اهمیت است.

بخش دوم تحت عنوان سایبر بین الملل، به فعالیت‌های روسیه در محیط سایبر متمرکز است. بخش سوم نیز تحولات سازمانی و ساختاری اسرائیل و اقدامات این کشور در عرصه سایبری را مورد بررسی قرار داده است. بخش پایانی نیز به دو گزارش راهبردی در زمینه آموزش الکترونیکی و تحلیل روندهای سایبری در سال آینده میلادی اختصاص یافته است.

Iranian Council For
Defending The Truth

اخبار

۳

ایالات متحده امریکا

گزارش: لزوم تغییر در نحوه عملکرد پنتاگون در خصوص هوش مصنوعی

متن ذیل ترجمه و تلخیصی از گزارش وب‌سایت Cyber Security Inteligence می‌باشد:

تغییرات سریع تکنولوژیکی و خودکارسازی سیستم‌ها ماهیت بسیاری از امور و کارها را به طرز چشمگیری تغییر خواهد داد و تمرکز این دگرگونی‌ها بر کاربردهای نظامی به ویژه در حوزه هوش مصنوعی (AI) است.

کارشناسان و نخبگان ایالات متحده وقتی صحبت از فناوری هوش مصنوعی به میان می‌آید، مبتنی بر این فرض که پیشقدم شدن در این حوزه یک مزیت بزرگ محسوب می‌شود، تلاش می‌کنند تا رهبری نظامی امریکا در حوزه‌های تکنولوژیک رقابتی با چین را توجیه نمایند.

در همین راستا، وزارت دفاع ایالات متحده (DoD) در حال بررسی تغییرات سازمانی به منظور ایجاد یک رویکرد یکپارچه تر در قبال داده ها و هوش مصنوعی است؛ از جمله ایجاد «منصب افسر ارشد داده و هوش مصنوعی» (CDAO).

از نظر کارشناسان رهبری تکنولوژیک مستلزم موثر بودن مدیریت داده و هوش مصنوعی است و تلاش‌های پنتاگون تا به امروز به طور گسترده در مقایسه با چین ناکافی تلقی می‌شود. به عنوان مثال، تصور می‌شود که ۱۵ مؤسسه جداگانه تحت مدیریت پنتاگون وجود دارد که روی فناوری‌های مرتبط با هوش مصنوعی، قابلیت‌های اصلی هوش مصنوعی یا برنامه‌های کاربردی سرمایه‌گذاری می‌کنند و از هوش مصنوعی در توسعه صنعتی استفاده می‌کنند. هرکدام از این موسسات دارای فرآیندها، داده‌ها، دستورالعمل‌ها و برنامه‌های جداگانه‌ای هستند. هماهنگی ساختاریافته کافی بین آنها یا نظارت از طریق یک "هاب هوش مصنوعی" مرکزی وجود ندارد و همین امر به تنهایی توانایی ایالات متحده را برای رهبری فناوری‌های جدید تضعیف می‌کند.

نظارت یکپارچه از طریق ایجاد یک CDAO توانمند می‌تواند به وزارت دفاع کمک کند تا مطمئن شود ابزارهای مورد نیاز برای تفوق داشتن را برخوردار است و صنعت دفاعی ایالات متحده هم‌چنان پیشتازی می‌کند.

پذیرش فناوری‌های نوظهور مستلزم آزمایش ساختارهای نهادی لازم برای استفاده از آنها است. ادغام دفتر JAIC ، CDO ، و دفاتر DDS تحت CDAO نشان دهنده یک لحظه بالقوه رشد سازمانی برای وزارت دفاع در مورد جدی گرفتن داده ها و فناوری های نوظهور است.

- CDO مسئول مدیریت و هماهنگی داده ها در سرتاسر وزارت دفاع است.
- JAIC برای کمک به وزارت دفاع در فعال کردن و پیاده سازی استفاده از هوش مصنوعی ایجاد شد.
- DDS یک تیم ویژه علم داده است که برای

رسیدگی به مسائل امنیتی و مربوط به داده‌ها و اطلاعات طراحی شده است.

پیش از این در سال ۲۰۲۱، JAIC یک منصب ذیل معاون وزیر دفاع شد. این مقام قبلاً به افسر ارشد اطلاعات گزارش می داد و به همین خاطر حدود وظایف این بخش نامشخص و مورد مناقشه بود. JAIC این اختیار را ندارد که سرویس‌های نظامی و سایر موسسات را مجبور به همکاری کند.

سازمان‌دهی مجدد پیشنهادی می‌تواند با موانع بوروکراتیکی روبرو شود که هدف رهبری یکپارچه بخش‌های هوش مصنوعی، داده‌ها و دیجیتال را تضعیف می‌کند. به عنوان مثال، این تشکیلات همچنین به این اختیار نیاز دارد که اجزای مختلف پنتاگون، به ویژه سرویس‌های نظامی منحصر به فرد را برای به اشتراک گذاشتن داده‌ها از پایگاه‌های داده‌ای که هرگز برای اشتراک‌گذاری طراحی نشده‌اند، مجبور کند.

سازماندهی مجدد ضروری به نظر می رسد زیرا نهادهای موجود تمرکزی برای هماهنگی مؤثر تلاش های پنتاگون ندارند.

سازماندهی مجدد پیشنهادی در نهایت بسته به میزان حمایتی که از سوی رهبری ارشد پنتاگون دریافت می‌کند، با موفقیت یا شکست مواجه خواهد شد. ایالات متحده توانایی فنی و مالی برای تبدیل شدن به یک رهبر جهانی در هوش مصنوعی را دارد، اما برای موفقیت باید اقدامات لازم را جهت پذیرش نوآوری‌های فنی انجام دهد.

avas

کارشناسان درب پشتی مستقر در شبکه آژانس‌های فدرال ایالات متحده را کشف کردند

یک کمیسیون دولت فدرال ایالات متحده مرتبط با حقوق بین‌الملل به واسطه یک درب پشتی هدف قرار گرفته است که طبق گزارش‌ها شبکه داخلی آن را به خطر انداخته است.

شرکت امنیتی Avast کشور چک طی گزارشی که هفته گذشته منتشر شد در این باره گفت: "این حمله می تواند افشای کامل شبکه و کنترل کامل یک سیستم را به همراه داشته باشد و بنابراین می تواند به عنوان اولین گام از یک حمله چند مرحله ای برای رخنه عمیق تر به سایر شبکه ها استفاده شود."

نام نهاد فدرال فاش نشد، اما گزارش‌های Ars Technica و The Record آن را به کمیسیون آزادی مذهبی بین‌المللی ایالات متحده (USCIRF) مرتبط می‌کند. Avast گفت که یافته های خود را در صورت عدم موفقیت تلاش هایش برای اطلاع رسانی مستقیم به آژانس در مورد نفوذ و از طریق کانال های دیگری که توسط دولت ایالات متحده ایجاد شده، علنی می کند.

در این مرحله، تنها "بخش هایی از پازل حمله" کشف شده است، و با توجه به ماهیت سیر دسترسی اولیه مورد استفاده برای رخنه به شبکه و توالی اقدامات پس از بهره برداری توسط بازیگر مجهولات بی‌پاسخ بسیاری باقی مانده اند.

آنچه مشخص است این است که این حمله در دو مرحله برای استقرار دو باینری مخرب انجام شده است، مرحله اول به طور بالقوه دشمن ناشناس را قادر می سازد تا ترافیک اینترنت را رهگیری کرده و کد مورد نظر خود را اجرا کند و به اپراتورها اجازه می دهد تا کنترل کامل بر سیستم های آلوده را در دست بگیرند. با سوء استفاده از WinDivert، یک ابزار قانونی ضبط بسته برای ویندوز، به این امر دست می یابد.

شباهت های این حمله با «عملیات امضای سرخ» در سال ۲۰۱۸ که سازمان های کره جنوبی را هدف قرار داده بود باعث شده تا تیم اطلاعاتی Avast Threat مشکوک شود که مهاجمان به کد منبع دومی دسترسی داشته اند یا خیر.

فیشرها برای جمع آوری اطلاعات بانکی و سایر مدارک هویتی خود را به جای فایزر جا می زنند

بین ۱۵ اوت تا ۱۳ دسامبر، شرکت حفاظت پستی INKY، ۴۱۰ ایمیل فیشینگ را شناسایی کرد که هویت برند Pfizer را در یک سری کلاهبرداری‌های RFQ جعل نمودند.

INKY خاطرنشان کرد که هکرها هم از روش‌های فنی سطح بالا و هم سطح پایین به منظور فرار از رادار ضد فیشینگ استفاده می‌کنند. روش فنی پیشرفته شامل دامنه‌های تازه ایجاد شده و رایگانی است که برای ارسال ایمیل‌های فیشینگ راه‌اندازی شده‌اند و باعث ایجاد دفاع اولیه از ایمیل نمی‌شوند. روش فنی سطح پایین یک پیوست ساده PDF بود که هیچ لینک مخرب یا بدافزاری در پیوست یا خود ایمیل وجود نداشت. این عناصر به صراحت طراحی شده‌اند تا آنالیزهای ضد فیشینگ را تحریک نکنند و شناسایی آنها دشوار شود.

ایمیل‌های فیشینگ خود از مجموعه‌ای از دامنه‌های گیج‌کننده سرچشمه می‌گیرند: pfizer-nl[.]com، pfizertenders[.]xyz، pfizerhtlinc[.]xyz، pfizer-bv[.]org، xyz.

این دامنه‌ها، به گونه‌ای طراحی شده‌اند که به نظر می‌رسد توسط Pfizer کنترل می‌شوند، همگی به‌طور صریح برای کلاهبرداری ایجاد شده و با نام Namecheap ثبت شده‌اند. این ثبت کننده دامنه، ارز دیجیتال را به عنوان پرداخت می پذیرد.

فیشرها برخی از ایمیل‌های جعلی Pfizer را از حساب‌های رایگان ایمیلی راه‌اندازی شده در Gmail، Outlook و Ziggo ارسال کردند.

اگرچه INKY نتوانست این کلاهبرداری را تا حل آن دنبال کند، ولی آنها شواهدی از دو نتیجه احتمالی دیده اند:

یا عامل تهدید اطلاعات بانکی و سایر اطلاعات اعتباری آنها را از طریق تبادل ایمیل یا از طریق تلفن جمع آوری کرده است، یا این که کلاهبرداران بدون آن که هرگز پولی پرداخت کنند، کالاهایی را خریده و دوباره آن را در بازار سیاه فروخته اند.

یک باگ بلوتوث سبب خطا و مثبت شدن تست COVID-۱۹ می‌شود

محققان از یک آسیب‌پذیری در تست خانگی معروف Ellume COVID-۱۹ که سبب آزمایش مثبت می‌شد پرده برداری کردند.

کیت آزمایش مورد بحث Ellume COVID-۱۹ Home Test بود، یک آزمایش آنتی ژنی که به طور خودسرانه انجام می شود.

این آزمایش با یک آنالایزر بلوتوث کار می کند و سبب کنارگذاشته شدن مراکز انجام تست می‌شود و نتیجه را از طریق برنامه موبایل Ellume در اختیار کاربر و مقامات بهداشتی قرار می دهد.

از آنجایی که دو نوع ترافیک ارسالی از بلوتوث دستگاه تست به دیوایس مصرف‌کنندگان، مسئول مثبت بودن آزمایش کرونا هستند، محققان اسکریپت های مخصوص ترافیک را نوشتند که نتیجه منفی را به مثبت تبدیل کرد.

حتی اگر آزمایش منفی بود، محققان اسکریپتهایی نوشتند که نتیجه را به مثبت تغییر می‌داد. در عمل، این بدان معنی است که هکرها می توانستند گواهی لازم برای شرکت در فعالیت های خاص در ایالات متحده و ورود به این کشور را برای خود مهندسی کنند.

بایدن برترین مؤسسه پزشکی نظامی چین را در لیست سیاه کنترل صادرات قرار داد

دولت بایدن اعلام کرد که به دلیل نگرانی فزاینده مبنی بر اینکه پکن از فناوری‌های پزشکی نوظهور و «سلاح‌های کنترل مغز» برای تقویت ارتش خود و سرکوب اقلیت‌های مسلمان در چین استفاده می‌کند، یکی از مراکز تحقیقاتی نظامی چین را به فهرست سیاه کنترل صادرات اضافه می‌کند.

آکادمی علوم پزشکی ارتش وابسته به PLA و تقریباً ده ها مؤسسه تحقیقاتی آن به لیست سیاه این نهاد اضافه شدند که صادرات فناوری آمریکا را بدون مجوز دولت ایالات متحده ممنوع می کند. این وزارتخانه گفت که استفاده چین از داده‌های بیولوژیکی و سلاح های به اصطلاح "کنترل مغز" انگیزه این ممنوعیت است.

آکادمی علوم پزشکی نظامی ممکن است به دلیل همکاری با CanSino Biologics برای تولید واکسن چینی کووید موسوم به Convidecia در سطح جهانی شناخته شود. این واکسنی است که چین به کشورهای در حال توسعه ارائه کرده است. وزارت خارجه و جامعه اطلاعاتی ایالات متحده مدتی است که گفته اند ارتش چین از فناوری پیشرفته برای سرکوب اویغورها و سایر اقلیت های مسلمان در استان سین کیانگ در شمال غربی این کشور استفاده کرده است.

هم چنین، مقامات چینی از نرم افزار تشخیص چهره بیومتریک برای نظارت جمعی بر ساکنان این استان استفاده کرده اند و نمونه های DNA را از مردم سین کیانگ بین سنین ۱۲ تا ۶۵ سال جمع آوری کرده اند.

در اقدامی جداگانه، فیس‌بوک - که اکنون با نام متا شناخته می‌شود - به حدود ۵۰۰۰۰ کاربر خود هشدار داد که ممکن است هدف نرم‌افزارهای نظارتی باشند و اعلام کرد که هفت سرویس تجاری با کاربری جاسوسی را از سایت‌های رسانه‌های اجتماعی خود حذف خواهد کرد. یکی از این سازمان‌ها و سرویس‌های ارائه دهنده در چین مستقر است.

سایبر بین‌الملل

توییتر، متا و تیک تاک به دلیل محتوای ممنوعه در روسیه جریمه شدند

دادگاه مسکو در آخرین اقدام از سلسله جرائم علیه شرکت‌های فناوری خارجی اعلام کرد که روسیه توییتر، متا -پلتفرم مالک فیس بوک- و تیک تاک را به دلیل عدم حذف محتوایی که دولت آن را غیرقانونی می داند جریمه کرده است.

مسکو امسال طی سلسله اقداماتی که منتقدان آن را تلاشی از سوی مقامات روسی برای اعمال کنترل شدیدتر بر اینترنت توصیف می کنند، فشارها را بر شرکتهای بزرگ فناوری افزایش داده است؛ این اقدامات به گفته منتقدان تهدیدی برای سرکوب آزادی فردی و جمعی به شمار می‌آید.

دادگاه منطقه تاگانسکی مسکو اعلام کرد که پلتفرم‌های مِتا در سه پرونده اداری جداگانه به دلیل حذف نکردن محتوا در مجموع ۱۳ میلیون روبل (۱۷۶۹۲۶ دلار) جریمه شده است. به گفته خبرگزاری های روسی، توییتر در دو پرونده ۱۰ میلیون روبل جریمه شد، ضمن آن که TikTok ۴ میلیون روبل جریمه دریافت کرد.

رگولاتور ارتباطاتی Roskomnadzor اعلام کرده است که روسیه از ماه مارس سرعت توییتر را به دلیل پست‌های حاوی هرزه‌نگاری کودکان، اطلاعات سوءمصرف مواد مخدر، یا فراخوان افراد زیر سن قانونی به خودکشی به عنوان یک اقدام تنبیهی کاهش داده است.

رقابت‌های جنگی اوکراین شبکه برق این کشور را محک می‌زند

از آن جایی که تنش‌های ژئوپلیتیکی با روسیه همچنان در حال افزایش است، صدها کارشناس سایبری اوکراینی در یک تمرین واکنشی در مقیاس بزرگ علیه شبکه انرژی این کشور شرکت کرده‌اند.

رئیس‌جمهور پوتین روز جمعه یک سری درخواست‌های امنیتی صادر کرد، از جمله اینکه ناتو استقرار نیروها و تسلیحات را در مرزهای شرقی اوکراین با روسیه محدود کند و این کشور متعهد شود که هرگز به ائتلاف نظامی نپیوندد.

این کشور نسبت به وقوع بحران نظامی در منطقه در صورت عدم برآورده شدن خواسته هایش هشدار داد. روسیه در حال حاضر ۱۰۰۰۰۰ سرباز را در کنار موشک و توپخانه در سمت مرز خود جمع کرده است.

بسیاری از اوکراینی ها با نگرانی دسامبر ۲۰۱۵ و ۲۰۱۶ را به یاد می‌آورند که هکرهای مورد حمایت دولت روسیه شبکه برق را مختل کردند و صدها هزار نفر را برای چند ساعت در تاریکی و سرمای زمستان رها کردند.

در تمرین اخیر ۲۵۰ شرکت کننده و ۴۹ تیم به منظور جلوگیری از حمله احتمالی به یک توزیع کننده ساختگی انرژی با هم رقابت کردند. این تمرین چند ساعته که توانایی متخصصان صنعتی بخش خصوصی و شرکت‌کنندگان از دانشگاه‌ها و سایر موسسات را به نمایش گذاشت، بر سه عنصر کلیدی متمرکز بود: کشف آنچه اتفاق افتاده، بیرون راندن اخلالگران و اصلاح سیستم‌های آسیب‌دیده.

محیط سایبری اسرائیل

گزارش: تحقیقات، جاسوس افزار پگاسوس در تلفن همسر جمال خاشقجی را به ماموران امارات متحده عربی مربوط می کند

واشنگتن پست اولین بار در روز سه شنبه گزارش داد که ماموران امارات متحده عربی نرم افزار جاسوسی پگاسوس را ماه ها قبل از مرگ همسر جمال خاشقجی، در تلفن همراه وی بارگذاری کردند.

این نرم افزار توسط Citizen Lab کشف شد که به درخواست همسر خاشقجی، حنان الاتر، دستگاه را بررسی کرد.

به گفته محققان، ماموران پس از دستگیری او از فرودگاه دبی در آوریل ۲۰۱۸ و بازجویی از او، این نرم افزار جاسوسی را روی تلفن او قرار دادند. در بازجویی ها دو گوشی اندرویدی او را ضبط کردند.

واشنگتن پست برای اولین بار در ماه ژوئیه گزارش داد که حنان الاتر توسط نرم افزارهای جاسوسی Pegasus از طریق پیام های متنی هدف قرار گرفته است، اما محققان نمی توانند تشخیص دهند که آیا هک موفقیت آمیز بوده است یا خیر. بیل مارکزاک، محقق آزمایشگاه Citizen Lab به واشنگتن پست گفت: مشخص نیست که آیا نرم افزار جاسوسی راه اندازی شده توسط عوامل امارات بر روی تلفن نصب شده است یا خیر. با این حال، یافته‌های جدید اولین موردی است که مستقیماً یک آژانس دولتی امارات متحده عربی را به استفاده از جاسوس‌افزار بر روی یکی از نزدیکان خاشقجی در ماه‌های منتهی به قتل وی مرتبط می‌کند.

مرکز جدید کنترل و فرماندهی سایبری اسرائیل برای حفظ ایمنی حمل و نقل

پیشرفت‌های تکنولوژیک در حوزه حمل‌ونقل هوشمند تهدیدات پیچیده‌ای را در زمینه سایبری به دنبال دارد. وزارت حمل و نقل و ایمنی راه اسرائیل تشکیل مرکز کنترل و فرماندهی ملی تهدیدات سایبری در حوزه حمل و نقل (مرکز عملیات امنیتی - SOC) را به پایان رسانده است.

این مرکز توسط سازمان هوانوردی اسرائیل اداره خواهد شد که در حال حاضر یک مرکز فرماندهی و کنترل سایبری در فرودگاه بن گوریون دارد. به گفته وزارت حمل و نقل، انتظار می رود نظارت بر تمام نهادهای حمل و نقل زیر یک سقف، امکان شناسایی و نظارت بهتر حملات را فراهم کند.

این مرکز در کنار مقابله با حملات سایبری به شناسایی آسیب‌پذیری‌ها و مقابله با آن‌ها می‌پردازد. در زمره ماموریت های این مرکز نظارت بر عملکرد چراغ های راهنمایی و زیرساخت های جاده ای، شرکت های حمل و نقل عمومی بزرگ، بنادر و همچنین نظارت بر عملکرد راه آهن اسرائیل، راه آهن سبک و غیره خواهد بود.

2021
CYBERDOME
VI

ارتش اسرائیل و ایالات متحده مانور مشترک امنیت سایبری را به پایان رساندند

بخش مشترک دفاع سایبری (JCDD) نیروهای دفاعی اسرائیل (IDF) و فرماندهی سایبری ایالات متحده ششمین مانور سالانه امنیت سایبری خود را با نام Cyberdome در یکی از تاسیسات سایبری ایالات متحده به پایان رساندند.

این رزمایش سناریوهای نبرد در حوزه سایبری را شبیه سازی کرد تا آمادگی هر دو کشور برای تهدیدات سایبری رو به رشد را بهبود بخشد.

این رزمایش توسط اداره خدمات کامپیوتری ارتش اسرائیل و با همکاری فرماندهی سایبری ارتش ایالات متحده رهبری شد. به گزارش وب سایت ارتش اسرائیل، این مانور در مرکز فرماندهی سایبری در ایالات متحده برگزار شد و توسط ارتش اسرائیل به عنوان تجلی همکاری استراتژیک ضروری و بزرگ میان دو ارتش توصیف شد.

DEAL
INCOME
CHARGE
REPORTS
BUDGET
4/4
3/4
2/4
1/4
ANALYSIS
UPDATE

گزارش‌های راهبردی

آموزش و پرورش باید بر امنیت سایبری توجه کند

تغییر به سمت یادگیری آنلاین، که با همه گیری کووید۱۹- تسریع گردیده، تأثیر زیادی بر سازمان‌های آموزشی در سراسر جهان داشته است؛ چه آن دسته سازمان‌های آموزشی که به طور کامل به یادگیری آنلاین روی آورده‌اند چه آن دسته موسسات آموزشی که از رویکرد یادگیری ترکیبی استفاده می‌کنند. آنچه واضح است آن است که آموزش الکترونیکی ادامه خواهد یافت.

حفاظت از مؤسسات آموزشی به دلیل حجم بالای دستگاه‌های مدیریت نشده و کاربرانی که به شبکه‌های آنها متصل می شوند، شدیداً چالش برانگیز هستند. این امر حفاظت از داده های شخصی دانش آموزان، سوابق کارمندان، داده های محرمانه، نتایج تحقیقات و سایر دارایی های معنوی را پیچیده می کند.

به گفته شرکت مشاوره وکتور استرالیا، این واقعیت که دانشگاه‌ها و مؤسسات آموزشی به طور فزاینده داده‌های حساس را با شرکای صنعتی و دولت‌ها به اشتراک می‌گذارند، آنها را هدف بالقوه مهاجمان قرار می‌دهد. مؤسسات آموزشی باید خدمات زیادی را به ذینفعان متعددی ارائه دهند و با مجموعه داده های بزرگ و بدون ساختار سروکار دارند؛ به همین خاطر هدف مطلوبی برای هکرها محسوب می‌شوند. علاوه بر این، پذیرش سریع فناوری آموزشی به این معنی است که ارائه دهندگان خدمات آموزشی در معرض خطرات بیشتری در ارتباط با امنیت سایبری قرار گرفته اند.

با این که ارائه دهندگان آموزش الکترونیک از قوانین حفاظت از داده ها، مانند GDPR اتحادیه اروپا یا CCPA کالیفرنیا پیروی می کنند، ولی باز هم برای موسسات ضروری است که کنترل کاملی بر داده های خود داشته باشند. از جمله توانایی تصمیم گیری در مورد نحوه و مکان ذخیره داده های خود.

به عنوان مثال، در نرم‌افزار آموزشی پرکاربرد Moodle LMS و Moodle Workplace، مدیران می‌توانند نقش‌های کاربری متفاوتی را تعریف کنند و مجوزها یا «قابلیت‌هایی» را به‌طور انبوه به آن‌ها اختصاص دهند، و اطمینان حاصل کنند که تنها کاربرانی که نقش‌های «معتمد» دارند (مثلا معلم، مدیر، کارفرمان) به داده های خاصی دسترسی داشته باشند – در حالی که سایر کاربران مانند «دانشجویان» این امکان را ندارند.

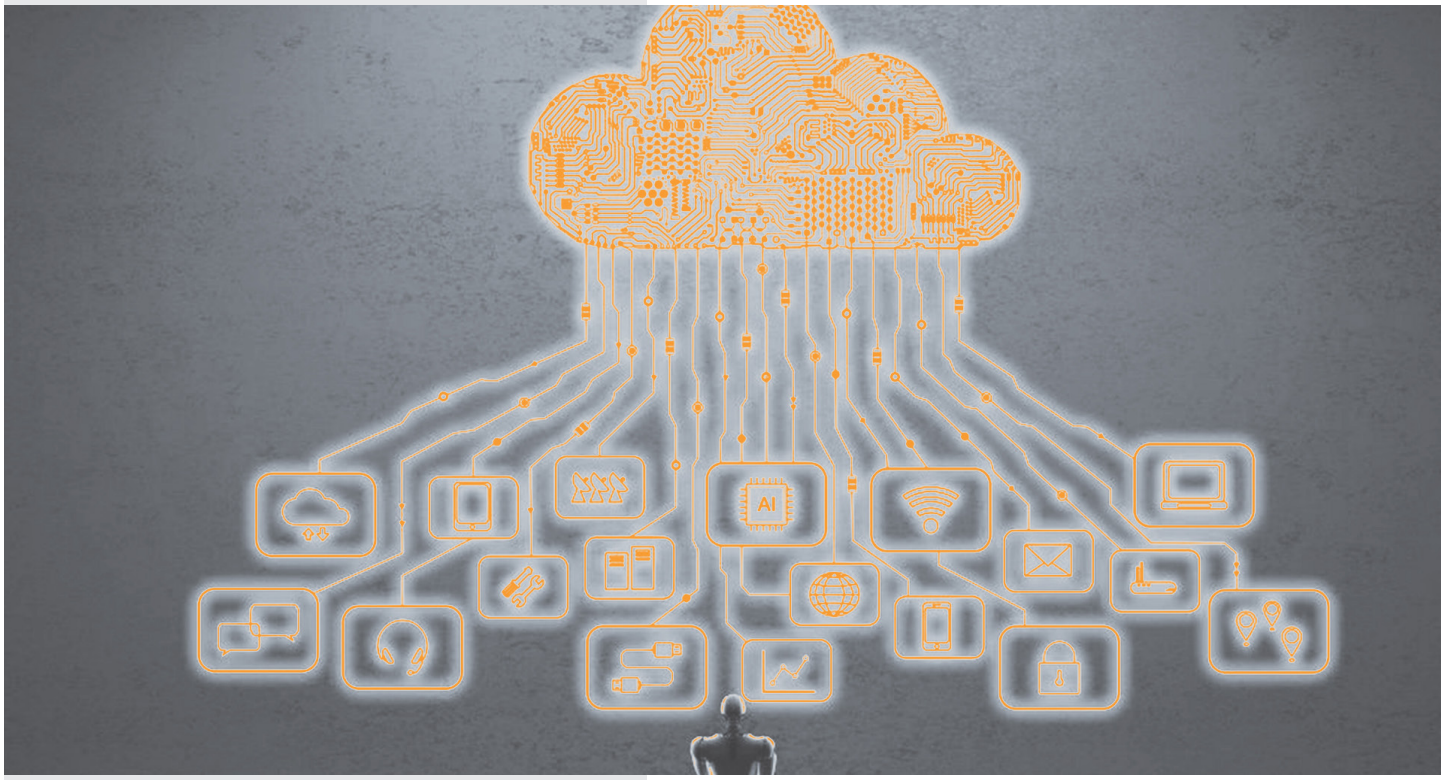
علاوه بر نگرانی‌های مربوط به حفظ حریم خصوصی داده‌ها، با وجود زبان‌آموزان و کارکنانی که از دستگاه‌های شخصی برای ورود از راه دور استفاده می کنند، به خطر افتادن کاربر و باج‌افزار

دو مـورد از رایج‌تریـن مسـائل امنیـت سـایبری بـرای ارائه‌دهنـدگان آمـوزش عالـی هسـتند. روشـی کـه تیم‌هـای فنـاوری اطلاعـات در مؤسسـات آموزشـی بـا ایـن مسـائل برخـورد می‌کننـد، ماننـد حمـلات فیشـینگ یـا تهدیـد بـه انتشـار داده‌هـای خصوصـی که هکرهـا بـه آنهـا دسترسـی دارنـد، بایـد شـامل فعـال کـردن احـراز هویـت چنـد عاملـی در سیسـتم مدیریـت یادگیـری (LMS) آنهـا باشـد، از جملـه رمزگـذاری داده‌ها یـا انجـام منظـم پشـتیبان گیـری.

بسـط یـک ذهنیـت امنیتـی در کل سـازمان ، کلیـد کاهـش خطـرات امنیـت سـایبری در مؤسسـات آموزشـی اسـت.

برخـی از ابتکاراتـی کـه مؤسسـات آموزشـی مـی تواننـد بـرای کار بـر روی ایـن طـرز فکـر امنیتـی در سـطح سازمانشـان اجـرا کننـد عبارتنـد از: کمپیـن هـای داخلی شـناخت فیشـینگ ، آمـوزش اجتنـاب از رفتارهـای مخاطـره آمیـز سـایبری و آمـوزش اولیـه حفاظـت از داده هـا اسـت.

اگـر همـه اینهـا از طریـق سیسـتم مدیریـت یادگیـری خـود مؤسسـه ارائـه شـود، بـه کاربـران کمـک مـی کنـد ایـن آمـوزش هـا را در متـن امـر بیاموزنـد و ابزارهـای حفـظ حریـم خصوصـی را کـه پلتفـرم خودشـان ارائـه مـی دهـد درک کننـد.


AI

روندهای امنیتی برای سال ۲۰۲۲ - نیاز به استعدادها و مهاجرت ابری

۱۲ ماه پرتلاطم در امنیت سایبری با چندین نقض بزرگ ظرف یک سال اخیر همراه بوده است.

ما شاهد حمله مخرب باج افزاری به Colonial Pipeline بودیم، یکی از پرمخاطب ترین داستان های امنیتی سال. این حمله باعث تعطیلی یک خط لوله به طول ۵۵۰۰ مایل در سواحل شرقی ایالات متحده شد و نگرانی ها در مورد خطرات مربوط به زیرساخت های حیاتی و زنجیره های تامین جهانی را تشدید کرد.

در ماه می، شاهد بودیم «بایدن» فرمان اجرایی را امضا کرد که برای مقابله مستقیم با مسائل امنیت سایبری کشور، از جمله امنیت زنجیره تامین، طراحی شده بود و شاید مهم‌ترین دستور اجرایی بود که از سازمان‌های دولتی اتخاذ رویکرد "اعتماد صفر" (zero trust) را طلب می نمود.

همچنین سال ۲۰۲۱، سال ارزهای دیجیتال، فناوری دیپ‌فیک و رشد کلاهبرداری‌ها و شیادی‌های مرتبط با همه‌گیری بود.

هنگامی که به ۱۲ ماه آینده این صنعت نگاه می کنیم، روی دو روند برای سال ۲۰۲۲ تمرکز می کنیم.

۱. کمبود استعداد

مایکروسافت اخیراً اعلام کرد با کالج‌های محلی در سراسر ایالات متحده برای ارائه منابع رایگان به منظور پایان دادن به کمبود متخصصان امنیت سایبری تا سال ۲۰۲۵، همکاری خواهد کرد. سوال این است که آیا این کمبود استعدادهای در دسترس بر صنعت امنیت در سال آینده یا پس از آن تأثیر خواهد گذاشت و بخش فناوری چگونه می‌تواند به تسکین آن کمک کند.

در آینده نزدیک، کمبود استعداد همچنان یک مشکل عمده باقی خواهد ماند. لکن اگر حوادث امنیتی کمتری برای مدیریت وجود داشته باشد، نیاز کمتری به جذب استعدادهای جدید در این صنعت وجود دارد و تأثیر کمبود استعداد تا حد زیادی کاهش می یابد.

از آن جایی که کمبود نیروی انسانی متخصص به این زودی ها از بین نمی رود، بنابراین باید راهکارهای مورد استفاده برای مقابله با تهدیدات به صورت کنترل و هدایت خودکار ماشینی سوق پیدا کنند.

۲. کوچ به فضای ابری

در حالی که مدتی پیش سایر صنایع، فرایندهای خود را به فضای ابری منتقل کردند، تردیدهایی برای دور شدن از عملیات های نرم افزاری در محل برای رهبران امنیتی وجود داشت. به دلیل گسترش انجام دورکاری توسط کارمندان و افزایش تهدیدات پیچیده سایبری، رهبران امنیتی دیگر نمی‌توانند برای حفاظت از رایانه‌ها و شبکه‌ها به سیستم‌های قدیمی وابسته باشند بلکه می‌بایست راه‌حل‌های متناسب با فضای رایانش ابری را اتخاذ نمایند.

اما آنچه مردم و کسب‌وکارها را به سمت فضای ابری سوق می‌دهد، احساس نیاز به امنیت است.

ICDT.IR