خبرنامه مدیریتی سراج
مرکز نرم‌افزار و سرویس وخدمات سازمان فضای مجازی سراج

اخبار فناوری اطلاعات و ارتباطات

۸۵

هفته نامه | سال دوم | شماره هشتاد و پنجم | ۲۷ آذر ۱۳۹۵

قانون جدید روسیه: ۱۰ سال زندان برای نفوذگران و نویسندگان بدافزار

دولت روسیه پیش‌نویس لایحه‌ای را صادر کرد که در آن برای مجازات مهاجمان سایبری و توسعه‌دهندگان بدافزار که زیرساخت‌های روسیه را هدف قرار می‌دهند، حکم زندان در نظر گرفته شده است.

این لایحه روز چهارشنبه بر روی وب‌گاه دولت روسیه منتشر شد و تغییر و اصلاح در قانون و آیین کیفرخواست باررسی را پیشنهاد می‌داد. عنوان این مقاله «نفوذ غیرقانونی به زیرساخت‌های حیاتی دولت روسیه» است.

در این لایحه مجازات مختلفی برای عملیات مخرب از جمله ایجاد و توزیع برنامه‌های مخرب برای برانداختن، مسدود کردن و رونویسی داده‌ها از سامانه‌های روسی در نظر گرفته شده است.

زمانی‌که مظنون در بخشی از عملیات نفوذ نقش داشته باشد، مبلغی بین 7700 تا 15400 دلار جریمه شده و به 5 سال زندان محکوم خواهد شد حتی اگر این نفوذ بی‌اثر بوده و هیچ آسیبی بدنبال نداشته باشد. با این حال اگر حملات سایبری انجام‌شده، منجر به عواقب جدی در زیرساخت‌های روسیه شود، براساس این قانون اعضای شرکت‌کننده در این حمله به 10 سال زندان محکوم خواهند شد.

همچنین نفوذگرانی که به داده‌های حفاظت‌شده دسترسی غیرمجاز داشته باشند به پرداخت 31500 دلار جریمه و 5 سال کار اجباری و 6 سال حبس محکوم خواهند شد. این لایحه پس از امضا توسط رئیس جمهور روسیه، ولادیمیر پوتین، در یک دوره‌ی کوتاه مدت تدوین خواهد شد.

در وب‌گاه دولت روسیه آمده است: «فرصت گسترش برون‌مرزی داده، باعث استفاده‌ی غیرقانونی از داده‌ها با اهداف جغرافیایی، سیاسی، نظامی و تروریسی شده و امنیت بین‌المللی را در معرض خطر قرار داده است.» این قانون جدید که مجازات کیفری ویژه‌ای را برای نفوذگران در نظر گرفته، به مجلس دومای روسیه ارسال شده است.

این حرکت یک کار بسیار عالی است چرا که نفوذگران روسی در زمینه‌ی انواع بدافزار و تهدیدها از جمله بهره‌برداری از POS، تروجان‌های بانکی و کیت‌های بهره‌برداری پیشقدم هستند.

نفوذ به شبکه‌ی خبری رژیم صهیونیستی و پخش اذان

سه‌شنبه شب گروهی از نفوذگران، کنترل شبکه‌ی 2 رژیم صهیونیستی را که یک شبکه‌ی خبری است در دست گرفتند و اذان پخش کردند. نفوذگران می‌خواستند به یک لایحه‌ی بحث‌برانگیز اعتراض کنند. در این لایحه گفته شده که باید صدای اذان پخش‌شده از مساجد محدود شود.

نفوذگران ابتدا به شبکه‌ی همه‌پخشی تلویزیون رژیم صهیونیستی نفوذ کرده و پس از بدست آوردن دسترسی بر روی شبکه‌های ماهواره‌ای، در انتقال داده‌ی این شبکه اختلال ایجاد کردند. رسانه‌های رژیم صهیونیستی حدس می‌زنند این نفوذگر از عربستان سعودی باشد.

آبان ماه، پارلمان رژیم صهیونیستی لایحه‌ی مؤذن را تصویب کرد. براساس این لایحه رهبران مذهبی حق ندارند برای دعوت نمازگزاران و پخش اذان از بلندگو استفاده کنند. هدف دولت رژیم صهیونیستی از تصویب این لایحه محافظت از شهروندان در برابر سروصدا است. در حالی‌که این لایحه در درجه‌ی اول از آلودگی صوتی پیشگیری می‌کند ولی منتقدان معتقدند یک بند در این لایحه وجود دارد که مسلمانان را هدف قرار داده است. در این بند آمده است: «آزادی مذاهب نباید به کیفیت زندگی شهروندان خطری برساند یا با بیان عبارات تحریک‌آمیز افراد را به دین خاصی تشویق و ترغیب کند.» سیاستمداران عرب احمد تیبی و طالب ابو عرعر نیز در اعتراض به این لایحه‌ی رژیم صهیونیستی در صحن مجلس اذان گفتند. این لایحه تحت حمایت نتانیاهو نخست وزیر رژیم صهیونیستی نیز قرار گرفته است.

وزارت دفاع اوکراین: نفوذگران تلاش می‌کنند وب‌گاه ما را از کار بیندازند

اخیراً اوکراین هدف نفوذگران ناشناخته قرار گرفته و مقامات محلی اوکراین می‌گویند مهاجمان در تلاش هستند تا به وب‌گاه وزارت دفاع این کشور نفوذ کنند.

در گزارشی از رویترز آمده است، اسناد مقامات اوکراین نشان می‌دهد که حملات متعدد منع سرویس توزیع‌شده علیه وب‌گاه وزارت دفاع این کشور اتفاق افتاده است. مقامات اوکراینی معتقدند مهاجمان می‌خواهند باعث اختلال در این وب‌گاه شده و از انتشار اطلاعیه‌ها برای مردم جلوگیری کنند.

سخنگوی وزارت دفاع اوکراین در اسنادی نشان داد که این وب‌گاه چندین بار در طول چند ماه گذشته، هدف حمله قرار گرفته است ولی مشخص نیست چند حمله مؤثر بوده و شدت هر یک از حملات چقدر بوده است. جزئیاتی از اینکه چه تعداد از حملات منع سرویس توزیع‌شده موفق بوده نیز ارائه نشده است.

در حال حاضر مشخص نیست چه گروهی پشت این حملات قرار دارند ولی به گفته‌ی سخنگوی این وزارت‌خانه، وب‌گاه عملکرد عادی خود را داشته و بررسی‌ها در دست انجام است.

باتوجه به اینکه در این وب‌گاه قرار بوده اطلاعیه‌های مربوط به درگیری‌های جدایی‌طلبان روسیه منتشر شود، به نظر می‌رسد این حملات، کارِ نفوذگران روسی باشد. هرچند این مسئله هنوز تأیید نشده است.

در طرف دیگر نیز مقامات روسی ادعا می‌کنند از برنامه‌ای مطلع شده‌اند که طی این برنامه قرار است سرویس‌های اطلاعاتی کشورهای خارجی، مؤسسات مالی روسیه را هدف قرار دهند. روسیه نیز در خصوص این ادعا توضیحات دقیقی ارائه نکرده است.

در حمله به وب‌گاه‌های روسی کاملاً مشخص بود که کارگزارها بر روی سرویس میزبانی کشور اوکراین در هلند قرار دارند. با این حال شرکت اوکراینی این ادعا را رد کرد و توضیح داد که کارگزارهای هلند را بررسی کرده و شواهدی مبنی بر حمله به وب‌گاه‌های روسی کشف نکرده است.

امنیت سایبری در تأسیسات هسته‌ای: آیا داعش نیروگاه‌های هسته‌ای اروپا را هدف قرار خواهد داد؟

کارشناسان در اجلاس صنعت هسته‌ای توضیح دادند چگونه می‌توان در تأسیسات هسته‌ای خطر بروز حملات سایبری را کاهش داد. در اجلاس صنعت هسته‌ای که اوایل امسال برگزار شد، کارشناسان اعلام کردند که تعداد حملات سایبری علیه برنامه‌های هسته‌ای رو به افزایش است. نفوذگران روز به روز پیچیده‌تر و ماهرتر می‌شوند و می‌توانند تأثیرات مخربی بر روی شبکه‌ها و تأسیسات هسته‌ای داشته باشند.

این موضوع بسیار ضروری است که کسب‌وکارها، دولت‌ها و تنظیم‌کنندگان امنیت در حوزه‌ی صنعت را در اولویت قرار دهند. کارشناسان در اجلاس صنعت هسته‌ای تأکید کردند که نفوذگران زیرساخت‌های هسته‌ای را هدف قرار داده‌اند چرا که با آسیب رساندن به آن باعث هرج‌ومرج و آشوب زیادی می‌شوند.

موفق‌ترین حمله‌ی سایبری در این حوزه مربوط به بدافزاری است که دستگاه‌های غنی‌سازی و تولید اورانیوم در ایران را هدف قرار داده بود. این بدافزار استاکس‌نت نام داشت و قادر بود کنترل چرخش سانتریفیوژها را در دست گرفته و باعث درهم شکسته شدن آن‌ها شود. علاوه بر تأسیسات هسته‌ای، حمله به وب‌گاه صنایع بزرگ نیز بسیار نگران‌کننده است. به‌عنوان مثال در حمله‌ی سایبری به شبکه‌ی برق اوکراین، برق هزاران خانوار قطع شد. نفوذگران از برنامه‌ای با نام BlackEnergy بهره برده بودند که سامانه‌های کنترل صنعتی را هدف قرار داده بود. به گزارش وزارت امنیت داخلی آمریکا، بخش‌های انرژی تنها 5 الی 6 درصد از تولید ناخالص آمریکا را تشکیل می‌دهد ولی نزدیک به 32 درصد از حملات سایبری، این زیرساخت‌ها را هدف قرار داده‌اند.

مهر ماه بود که یوکیا آمانو، مدیرکل آژانس بین‌المللی انرژی اتمی اعلام کرد که یک نیروگاه هسته‌ای در آلمان حدود دو سه سال پیش هدف حمله‌ی سایبری قرار گرفته است. هرچند این اولین حمله‌ی سایبری به نیروگاه‌های هسته‌ای نبود که به‌طور عمومی منتشر می‌شد. در حال حاضر 3 حمله‌ی شناخته‌شده به نیروگاه‌های هسته‌ای به‌طور عمومی اعلام شده است:

- حمله به تأسیسات هسته‌ای Monju (ژاپن در سال 2014)
- حمله به تأسیسات آب و هسته‌ای کره در سال 2014
- حمله به تأسیسات Gundremmingen آلمان در سال 2016

غول‌های دنیای فناوری برای حذف محتوای تروریستی متحد می‌شوند

برخی از بزرگ‌ترین شرکت‌های فناوری در حوزه‌ی وب دور هم جمع شدند تا با همکاری یکدیگر از انتشار محتوای برخط تروریستی جلوگیری کنند.

روز دوشنبه در یک نامه‌ی رسمی مشترک، شرکت‌های فیس‌بوک، مایکروسافت و توییتر متعهد شدند تا یک پایگاه داده‌ای مشترک از اثرانگشت دیجیتال منحصر بفرد متشکل از مقادیر درهم‌سازی برای شناسایی محتوای تروریستی توسعه دهند. ایده‌ی اصلی این است که این پایگاه داده، دسترسی به محتوا و اِعمال سیاست‌ها را سریع و آسان می‌کند.

در این بیانیه آمده است: «ما متعهد می‌شویم زمانی‌که تصاویر و ویدئوهای تروریستی را که از روی سرویس‌های خود حذف می‌کنیم، مقدار درهم‌سازی آن را در پایگاه داده به اشتراک بگذاریم. هر یک از شرکت‌های متعهد می‌توانند مقدار درهم‌سازی هر محتوای تروریستی بر روی هر بستری را به این پایگاه داده اضافه کند. شرکت‌های دیگر نیز می‌توانند از این پایگاه داده استفاده کرده و محتوای تروریستی را شناسایی کرده و این محتوا را از روی سرویس خود حذف کنند.»

در مرحله‌ی اول هر شرکت باید به‌طور مستقل تصمیم بگیرد که چه تصویر یا ویدئویی محتوای تروریستی دارد. علاوه بر این هر شرکت زمانی‌که انطباقی بین محتوای خود و مقدار درهم‌سازی در پایگاه داده پیدا کرد، باید براساس سیاست‌های خود تصمیم بگیرد که این محتوا را حذف کند یا خیر. در آینده این طرح می‌تواند با حضور شرکت‌های فناوری دیگر، توسعه یابد.

همچنین این شرکت‌ها اشاره کردند که هیچ‌گونه اطلاعات شناسایی شخصی به اشتراک گذاشته نخواهد شد چرا که این شرکت‌ها به ایده‌ی آزادی بیان پایبند هستند و می‌خواهند با حضور شرکت‌ها و سرمایه‌گذاران علاقه‌مند به این حوزه، این پروژه بیش از پیش پیشرفت کند.

امروزه بر هیچ کسی پوشیده نیست که گروه‌های تروریستی همچون داعش از بسترهایی مانند توییتر و یوتیوب برای انتشار پیام‌های خود، عضوگیری و سازمان‌دهی نیروها استفاده می‌کنند و در حال رشد هستند.

روز شنبه کمیسیون اروپا اعلام کرد بدنبال راهی برای تشخیص هرچه سریع‌تر محتوای ترویستی برخط و برانداختن چنین محتوایی است.

نگرانی فرانسه از نفوذهای سایبری و تشکیل ارتش دفاعی

فرانسه روز دوشنبه تشکیل ارتش جنگ سایبری خود را اعلام کرد. این ارتش در پاسخ به افزایش تهدیدات سایبری در آمریکا و اروپا توسط نفوذگران روسی تشکیل شده است. وزیر دفاع فرانسه، نفوذ در جنگ سایبری را به نبرد هواپیمایی در جنگ‌های اوایل قرن 20 تشبیه کرد.

لو درین، وزیر دفاع فرانسه در رونمایی از دکترین جدید در شمال‌غرب فرانسه گفت: «منطقه‌ی جنگ جدیدی به نام میدان سایبری پدید آمده است و ما برای حفظ هنر نظامی و جنگی خود باید به‌طور جدی در روش‌های خود تجدیدنظر کنیم.»

درین گفت یک نفوذ سایبری می‌تواند یک عملیات جنگی باشد و باید پاسخی متناسب به آن داده شود. او در ادامه گفت: «قابلیت‌های تهاجمی سایبری باید به ما اجازه دهد بتوانیم به سامانه‌ها و شبکه‌های دشمنان نفوذ کنیم، سرویس‌های آن‌ها را به حالت تعلیق درآوریم و حملات آن‌ها را به‌طور موقت یا دائمی خنثی کنیم.»

ارتش جدید فرانسه قرار است علاوه بر شناسایی نفوذگران خارجی به تشخیص آسیب‌پذیری در زیرساخت‌های فناوری اطلاعات سازمان‌های نظامی مانند هواپیماهای بدون سرنشین کمک کند.

درین گفت واحد دفاع سایبری فرانسه از ماه بعد شروع به کار خواهد کرد و تا سال 2019 سازمانی از 2600 متخصص را تشکیل خواهد داد.

علاوه بر حمله‌ی سایبری به زیرساخت شبکه‌های کامپیوتری دولت، آژانس‌های اطلاعاتی نگران گسترش تبلیغات و اطلاعات غلط و گمراه‌کننده توسط نفوذگران هستند.

مسکو اتهامات مربوط به دخالت روسیه در انتخابات آمریکا را رد کرده است. روسیه می‌گوید در افشای رایانامه‌های هیلاری کلینتون توسط ویکی‌لیکس در پویش حمایت از ترامپ نقشی نداشته است.

نگرانی‌های آمریکا در خصوص نفوذهای سایبری توسط روسیه در بسیاری از کشورهای اروپای غربی به‌ویژه کشورهای بالتیک که مرز مشترک با روسیه دارند، به اشتراک گذاشته شده است.

در طرف دیگر ماجرا، در حمله‌ی سایبری به تأسیسات هسته‌ای ایران در سال 2010 تصور می‌شد که دولت‌های آمریکا و رژیم صهیونیستی پشت بدافزار استاکس‌نت باشند ولی هیچ یک از این کشورها به این حمله‌ی سایبری عظیم اعتراف نکردند. جمعه‌ی گذشته نیز روسیه اعلام کرد از برنامه‌ای مطلع شده که طی آن سرویس‌های اطلاعاتی خارجی قرار است مؤسسات مالی روسیه را هدف قرار دهند.

باراک اوباما: حملات احتمالی روسیه به انتخابات آمریکا به‌طور کامل بررسی شود

در آخرین ماه‌های ریاست جمهوری، باراک اوباما به آژانس اطلاعاتی آمریکا دستور داده تا مرور کاملی بر روی نتایج انتخابات ریاست جمهوری داشته باشند. بسیاری از جمله حزب دموکرات معتقدند که در انتخابات تقلبی صورت گرفته است.

آژانس اطلاعاتی آمریکا در حملات پیش از انتخابات، روسیه را مقصر اصلی می‌دانست. سخنگوی کاخ سفید گفت: «رئیس جمهور در اوایل این هفته دستور دادند تا الگوی حملات رخداده در چرخه‌ی انتخابات ریاست جمهوری مورد بررسی قرار گیرد.»

باراک اوباما پیش از اتمام ریاست جمهوری خود، گزارش کاملی در این خصوص می‌خواهد. رئیس جمهور منتخب، دونالد ترامپ نیز کاخ سفید را در ژانویه 2017 تحویل خواهد گرفت. اوباما باید نتایج این بررسی را پیش از ترک کاخ سفید به کنگره تحویل دهد.

رئیس امنیت داخلی آمریکا در مورد عواقب حمله‌ی روسیه به انتخابات آمریکا گفت: «اگر ما به این حملات روسیه پاسخ ندهیم، عواقب آن ادامه داشته و آن‌ها دموکراسی ما را هدف قرار خواهند داد.»

این اطلاعیه پس از آن منتشر شد که حزب دموکرات کاخ سفید را مجبور کرد تا جزئیات نفوذ و اطلاعات گمراه‌کننده در انتخابات ریاست جمهوری را منتشر کند. در همین حال، ترامپ نیز گفته که متقاعد نشده که دولت روسیه پشت این حملات سایبری بوده باشد.

مهر ماه بود که وزارت امنیت داخلی و سازمان اطلاعات آمریکا رسماً در خصوص نفوذ به حساب‌های حزب دموکرات، روسیه را مقصر اصلی اعلام کردند ولی روسیه تمامی این اتهامات را رد کرد.

نفوذگران روسی رایانامه‌های خصوصی کلینتون را به سرقت بردند که این اطلاعات چند روز بعد، درست چند هفته قبل از انتخابات توسط ویکی‌لیکس منتشر شد. با این وجود، ارائه‌ی گزارش کاملی از نفوذ در جریان انتخابات توسط اوباما، ممکن است در دولت بعدی چالش‌های بزرگی را بوجود آورد.

نفوذ به شهرهای هوشمند اروپایی

برنامه‌ریزان شهری در اروپا از فناوری‌های مختلفی بهره می‌برند تا سرویس‌های مختلفی را به شروندان ارائه دهند. در سرویس‌های شهر هوشمند، سنسورهایی متصل به اینترنت به وسایلی همچون اتوبوس‌ها، دوچرخه‌های اجاره‌ای، پارکینگ متصل می‌شود و در ادامه از طریق یک برنامه یا پیامک هزینه آن پرداخت می‌شود. اما به دلیل فرهنگ غنی نفوذ در اروپا سازندگان و نفوذگران هر روزه با هم در جدال هستند. بسیاری از افراد می‌دانند که چگونه به این سرویس‌ها نفوذ کنند. مثلاً با روش بسیار ساده‌ای همچون پخش تکراری می‌توان هزینه‌ی یک سرویس را پرداخت نکرد. در ادامه مثال‌های زیادی را خواهید دید.

در یک شهرستان در منطقه بنلوکس، سرویس پرداخت پارکینگی وجود دارد که رسید پارکینگ را چاپ کرده و بر روی شیشه یا داشبورد ماشین نمایش می‌دهد. نفوذگران می‌توانند برنامه‌ای بسازند که این رسیدهای پارکینگ را رونویسی کند. این برنامه به‌طور خودکار مکان ماشین را شناسایی کرده و فهرستی از پارکینگ‌های نزدیک را به او نشان می‌دهد. این برنامه در ادامه نیز یک رسید پارکینگ معتبر به قربانی نشان خواهد داد.

یکی دیگر از شهرستان‌های بنلوکس از یک سامانه‌ی مبتنی بر پیامک برای توزیع بلیط‌های یک‌ساعته برای سامانه‌ی حمل‌ونقل استفاده می‌کند. برخلاف رسیدهای پارکینگ، این بلیط‌های پیامکی حاوی یک شناسه‌ی منحصربفرد هستند و به راحتی نمی‌توان آن‌ها را رونویسی کرد. اما نفوذگران می‌توانند یک برنامه‌ی مبتنی بر وب ایجاد کنند که بلیط‌ها را به‌اشتراک بگذارند. یک کاربر اگر اولین بلیط خود را خریداری کرده و 20 دقیقه برای حمل‌ونقل از آن استفاده کند، در این بلیط هنوز 40 دقیقه باقی مانده است. با استفاده از این برنامه این 40 دقیقه می‌تواند بین افراد دیگر توزیع شود. در پایان هر ماه، هر مشترک صورتحسابی را از این برنامه برای بلیط‌های توزیع‌شده دریافت می‌کند (پرداخت آن از طریق بیت‌کوین باید انجام شود). این سامانه یک روش شسته رفته‌ی کوچک است که در آن اعتبار استفاده‌نشده برای برنامه باقی می‌ماند.

خبرنامه مدیریتی اخبار فناوری اطلاعات و ارتباطات
مرکز نرم‌افزار و سرویس و خدمات سازمان فضای مجازی سراج
شماره ۸۵ | ۲۷ آذر ۱۳۹۵