مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

گزارش سریع
چهل و پنجم

استراتژی ملی امنیت سایبری در کانادا

National Cyber Security Strategy in Canada

بسم الله الرحمن الرحیم

گزارش سریع

گزارش شماره ۴۵
شهریور ۱۴۰۱

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

استراتژی امنیت ملی سایبری در کانادا

گزارش سریع که با عنوان Rapid Report شناخته می‌شود، نوعی گزارش کوتاه است که صرفاً برای اطلاع کلی از موضوع یا پدیده‌ای خاص در بازه زمانی محدود تهیه می‌شود. هدف عمده چنین گزارش‌هایی ایجاد تصویری اجمالی برای آشنایی ابتدایی سیاست‌گذاران و برنامه‌ریزان در موضوعات مورد علاقه آنان است.

تهیه شده در پژوهشگاه فضای مجازی
(گروه مطالعات بین‌الملل)

ترجمه: فرزانه اسکندریان
ناظر: عباس قنبری باغستان

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش خیابان ۱۶ غربی، پلاک ۲۰
تلفن: ۸۶۱۵۱۰۶۱-۰۲۱
کد پستی: ۱۵۱۵۶۷۴۳۱۱

فهرست

سخن نخست

سخن نخست

فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گستری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سیدابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

مقدمه

مقدمه

تقریباً هر کاری که کانادایی ها انجام می دهند، به نوعی تحت تأثیر فناوری است. ما به طور سرانه، نسبت به بقیه کشورهای جهان بیشترین زمان را به صورت آنلاین صرف می کنیم، یعنی هر کانادایی۴۳/۵ساعت در ماه را در فضای سایبری می‌گذرانند. ما تا حد زیادی به هم پیوسته و به شبکه سایبری متصل شده‌ایم، واقعیتی که کیفیت زندگی ما را بالا برده اما آسیب پذیری‌هایی را نیز ایجاد کرده است. ریسک دنیای سایبری از زنجیره های تأمین کسب و کار گرفته تا زیرساخت های مهمی که زیربنای اقتصاد و جامعه ما را تشکیل می‌دهد، چند برابر شده، سرعت گرفته و به طور فزاینده و مخربی در حال رشد است.

رالف گودل
وزیر امنیت عمومی و آمادگی اضطراری کانادا

شرکت‌های بزرگ، صنایع و متحدان و شرکای بین‌المللی ما درگیر چالش جهانی سایبری هستند. اما بسیاری دیگر با این چالش روبرو نیستندکه خود ریسکی قابل توجه و فرصتی از دست رفته را در این صنعت جهانی به سرعت در حال رشد نشان می‌دهد. گرچه آگاهی کامل از تهدیدات سایبری اهمیت دارد، اما سیاست امنیت سایبری کانادا را نمی‌توان با

ترس و واکنش های دفاعی هدایت کرد.

علاوه بر این، بررسی استراتژی امنیت سایبری فعلی با تأکید بر پتانسیل بزرگ افزایش نقش پیشتازی کانادا در این زمینه از نو آغاز شده است. ما از طریق همکاری با وزرای دفاع، نوآوری، زیرساخت‌ها، خدمات عمومی و هیئت خزانه‌داری، مستقیماً با کانادایی‌ها و ذینفعان اصلی مشورت کردیم که چگونه استراتژی جدید می‌تواند نیازهای امنیتی آنها را به بهترین وجه تأمین کند و در عین حال به آنها امکان دهد از فرصت‌های اقتصاد دیجیتال استفاده کنند. این استراتژی که بر اساس بیش از ۲۰۰۰ پیشنهاد ارسالی در مشاوره عمومی تنظیم شده است، به طور مستقیم شکاف‌ها و زمینه‌های بهبود شرایط فعلی امنیت سایبری کانادا را لحاظ کرده است.

اهداف اصلی این استراتژی در سرمایه‌گذاری های قابل توجه در بودجه ۲۰۱۸، به مبلغ بیش از ۵۰۰ میلیون دلار در طول پنج سال قابل مشاهده است. بودجه ۲۰۱۸ بزرگترین سرمایه گذاری منفرد کانادا در زمینه امنیت سایبری تاکنون بوده است که تعهد ما نسبت به ایمنی و امنیت در عصر دیجیتال را نشان می‌دهد.

از اقدامات جدید معرفی شده:

- تأمین وجه مرکز جدید امنیت سایبری کانادا برای حمایت از راهنمایی و همکاری بین سطوح مختلف دولت و شرکای بین‌المللی، ضمن تأمین منابع روشن و قابل اعتماد برای شهروندان و کسب و کارهای کانادایی؛
- ایجاد واحد ملی هماهنگی جرایم سایبری برای گسترش ظرفیت پلیس سواره‌نظام سلطنتی کانادا[1] برای بررسی جرایم سایبری، ایجاد مرکز هماهنگی برای شرکای داخلی و بین المللی؛

1. RCMP

• تأمین وجه در جهت تقویت نوآوری و رشد اقتصادی و توسعه استعدادهای سایبری در کانادا.

این استراتژی نقشه راهی برای پیشبرد امنیت سایبری کانادا است و برای دستیابی به اهداف و اولویت‌های کانادایی‌ها طراحی شده است. ما افتخار می‌کنیم که در این مسیر پیشگام هستیم.

بخش اول

بخش اول

خلاصه عملیات اجرایی

جایگاه کانادا در دنیای دیجیتال

دنیای ما با نوآوری دیجیتال متحول شده است.

فناوری‌های دیجیتال هر روز با ارائه پیشرفت‌هایی جدید، اکنون دیگر بخش جدایی‌ناپذیر از زندگی روزمره ما شده است. این فناوری‌ها از راه اندازی کسب و کارها و دسترسی به خدمات دولتی تا تعامل با دوستان و خانواده‌ها به ما کمک می کنند، و نه تنها ارتباط کانادایی ها را از ساحلی به ساحلی دیگر برقرار کرده، بلکه ما را نیز به یک شبکه جهانی پویا متصل می‌کنند.

این تازه اول کار است. پتانسیلی بی‌پایان برای جذب ایده‌های جدید و انقلابی وجود دارد. ما همچنان اوج تازه‌ای از نوآوری دیجیتال را شاهد خواهیم بودکه به نفع جوامع و سیاره ما به طور کلی است.

اهمیت امنیت سایبری

همچنان که از فناوری‌های دیجیتال برای مزایای فوق‌العاده آنها استقبال می‌کنیم، باید آغوش خود را در برابر تهدیدهای سایبری نیز باز کنیم .

مجرمان و سایر تهدیدکنندگان سایبری ـ که بسیاری از آنها در خارج از مرزهای ما فعالیت می‌کنند ـ از تحولات فناوری، خلأ امنیتی و آگاهی کم نسبت به امنیت سایبری سوءاستفاده می‌کنند و در تلاش هستند سیستم‌های سایبری را به خطر بیندازند. آنها اطلاعات شخصی و مالی، مالکیت معنوی و اسرار تجاری را می‌دزدند. آنها زیرساخت‌هایی را که ما برای خدمات ضروری و سبک زندگی خود به آنها متکی هستیم را مختل کرده و از بین می برند.

در سال ۲۰۱۰، دولت کانادا با نخستین «استراتژی امنیت سایبری کانادا» تلاشی ملی برای دفاع در برابر این تهدیدها را آغاز کرد. پیشرفت حاصل شده و دستاوردهای «استراتژی ۲۰۱۰» مبنای اقدامات آینده است.

رویکرد جدید ما ضرورت استفاده از فناوری‌های دیجیتال در سبک زندگی را منعکس می‌کند. ما می‌توانیم از طریق «استراتژی جدید امنیت سایبری»، با اعتماد به نفس بیشتری در عصر دیجیتال پیش رویم. این یک واقعیت است که امنیت سایبری، همراه نوآوری از رونق و شکوفایی محافظت می‌کند.

چشم‌انداز استراتژی ملی امنیت سایبری: امنیت و شکوفایی در عصر دیجیتال

امنیت سایبری قوی یکی از عناصر اساسی نوآوری و شکوفایی کانادا است. افراد، دولت ها و کسب و کارها همگی می‌خواهند به سیستم های سایبری که زیربنای زندگی روزمره آنها است، اعتماد داشته باشند. دولت کانادا آینده ای را در نظر دارد که در آن همه کانادایی ها نقشی فعال در شکل‌گیری و پایداری انعطاف سایبری داشته باشند.

دولت کانادا و شرکای آن برای تحقق چشم‌انداز ما حول سه محور همکاری خواهند کرد:

امنیت و انعطاف‌پذیری

ما از طریق اقدام مشترک با شرکا و افزایش قابلیت‌های امنیت سایبری، به شکل بهتری از کانادایی‌ها در برابر جرایم اینترنتی محافظت می کنیم، به تهدیدات در حال تحول واکنش نشان می‌دهیم و از سیستم‌های مهم بخش‌های دولتی و خصوصی دفاع می‌کنیم.

نوآوری سایبری

دولت فدرال با حمایت از تحقیقات پیشرفته، ارتقای نوآوری دیجیتال و توسعه مهارت‌ها و دانش سایبری، کانادا را رهبر جهانی امنیت سایبری معرفی کرده است.

رهبری و همکاری

دولت فدرال از طریق همکاری نزدیک با ایالت‌ها، ناحیه‌ها و بخش خصوصی، برای پیشبرد امنیت سایبری در کانادا نقش رهبری را بر عهده خواهد گرفت و از طریق هماهنگی با متحدان، در جهت ایجاد فضای بین المللی امنیت سایبری به نفع کانادا تلاش خواهد کرد.

رویکرد دولت کانادا در محیط پویای امنیت سایبری، ریشه در تعهد پایدار نسبت به موارد زیر خواهد داشت:

- حفاظت از ایمنی و امنیت کانادایی‌ها و زیرساخت‌های حیاتی ما؛
- ارتقا و محافظت از حقوق و آزادی‌های آنلاین؛

- ترویج امنیت سایبری در کسب و کار، رشد و شکوفایی اقتصادی؛
- همکاری و پشتیبانی از هماهنگی برای تقویت انعطاف پذیری سایبری کانادا در حوزه های قضایی و بخش های مختلف دولتی و خصوصی؛
- سازگاری کنشگرایانه با تغییرات در فضای امنیت سایبری و ظهور فناوری جدید؛

محدوده استراتژی

دامنه این استراتژی با کاری آغاز می‌شود که دولت کانادا در حال انجام آن است. این روند شامل تلاش‌های جاری و آتی در راستای محافظت از سیستم‌های دولت کانادا، گسترش شبکه مشارکت برای کمک به محافظت از زیرساخت های حیاتی و کمک به کانادایی‌ها برای امنیت آنلاین است. با این وجود، رویکرد جدید کانادا در فضای متنوع و پویاتر امنیت سایبری جهانی، گسترده‌تر و فراگیرتر خواهد بود. این سند به طور خلاصه عناصر اصلی محیط امنیت سایبری جهانی و برخی از راه‌های واکنش دولت کانادا به مجموعه‌ای از چالش‌ها و فرصت‌های جدید در فضای مجازی را بیان می‌کند.

اجرای استراتژی

با توجه به سرعت روزافزون تغییراتی که امروز شاهد آن هستیم، این استراتژی به عنوان اصلی‌ترین تلاش دولت برای تقویت امنیت سایبری در کانادا طراحی شده است. اقدامات دولت همراه تحولات خلاقانه فناوری و تغییرات پارادایمی رایج در جهان تکامل می‌یابد.

برنامه‌های عملیاتی امنیت سایبری این استراتژی را تکمیل می‌کنند. این

برنامه‌ها جزئیات ابتکارات ویژه‌ای را که دولت فدرال در طول زمان انجام خواهد داد و معیارهای واضح عملکرد و تعهد به گزارش نتایج به‌دست آمده را شرح می‌دهد. همچنین برنامه دولت برای همکاری با شرکای داخلی و خارجی برای دستیابی به چشم‌انداز خود نیز بیان می شود.

اجرای این استراتژی با سایر اقدامات مربوط به فضای سایبری دولت کانادا همسو می‌شود. این اقدامات شامل اختیار وزیر نهادهای دموکراتیک برای دفاع از روند انتخابات در برابر تهدیدات سایبری، سیاست خارجی کانادا در دستور کار بین المللی استفاده ارتش سایبری کانادا از فضای مجازی و «برنامه نوآوری و مهارت» می شود.

دولت کانادا برای نخستین استراتژی امنیت سایبری خود ۴۳۱/۵ میلیون دلار را برای مدت ۱۰ سال اختصاص داد که سه ستون اصلی دارد:

۱. امنیت سیستم‌های دولتی

به این طریق، دولت کانادا ظرفیت خود برای جلوگیری، شناسایی، واکنش و بازیابی پس از حملات سایبری را افزایش داده است. تعداد دفعات نفوذ به داده‌ها و اطلاعات از سال ۲۰۱۰ به طور پیوسته کاهش یافته است. این در حالی است که تعداد و پیچیدگی فعالیت‌های سایبری با حمایت‌های دولتی و غیر دولتی، علیه شبکه‌های دولتی کانادا افزایش داشته است.

۲. مشارکت برای تأمین امنیت سیستم‌های سایبری حیاتی خارج از دولت فدرال

قرارداد مشارکت با مالکان و متصدیان زیرساخت‌های مهم، بخش

خصوصی، ادارات ایالتی و مؤسسات منطقه‌ای کانادا منعقد شد. مرکز واکنش به حوادث سایبری کانادا[1] با بیش از ۱۳۰۰ سازمان که به طور منظم اخطارها و ارتباطات جدیدی را دریافت می‌کنند، عملیات خود را گسترش داده است.

۳. کمک به امنیت آنلاین کانادایی ها

دولت کانادا از طریق کمپین امنیت سایبری[2]، با اطلاع رسانی فعالیت ها و توسعه منابع هدفمند، از آگاهی نسبت به امنیت سایبری پشتیبانی کرده است. همچنین تلاش‌های انجام شده از طریق «استراتژی ۲۰۱۰» باعث بهبود ظرفیت پلیس سواره‌نظام سلطنتی کانادا و سازمان‌های اجرای قوانین در مبارزه با جرایم اینترنتی شدند که سرمایه‌گذاری‌های اولیه در زمینه اطلاعات مربوط به جرایم اینترنتی، تحقیقات و آموزش‌ها را شامل می‌شود.

1. CCIRC
2. Get Cyber Safe

بخش دوم

بخش دوم

معرفی

توسعه دستاوردهای کانادا در چشم‌انداز پویای فضای سایبری

امنیت سایبری چیست؟

امنیت سایبری به معنای حفاظت از اطلاعات دیجیتال و زیرساخت‌هایی است که داده‌ها در آن قرار دارد.

امنیت سایبری، زمانی حوزه متخصصان فنی بود، اما اکنون، همه ما در دنیای دیجیتال در امنیت سایبری فردی و جمعی خود نقشی داریم.

از حواشی به جریان اصلی

تا چند سال پیش غیرقابل تصور بود که فناوری دیجیتال در زندگی روزمره ما تا این حد ادغام شود. ما به فناوری‌های دیجیتالی همچون رسانه‌های اجتماعی، اپلیکیشن‌های کاربردی تلفن‌های هوشمند، خرید آنلاین، دستگاه‌های شبکه‌ای، فضای ابری و موارد دیگر، وابسته هستیم و این چیزی بیش از لذت شخصی است. فناوری‌های دیجیتالی از سیستم‌هایی که زیربنای اقتصاد و سبک زندگی ما هستند، جدایی‌ناپذیر می‌باشند. این سیستم‌های به هم وابسته شامل شبکه‌های ارتباطی است که سراسر کشور و سراسر جهان را به هم متصل می‌کند، یا همان انرژی

برای گرم کردن خانه‌ها و تأمین برق برای صنعت و سفرهای هوایی، ریلی و جاده‌ای است که ما هر روز از آنها استفاده می‌کنیم.

ما تمایل داریم که قابلیت اتصال را امری مسلّم بدانیم، بدون اینکه لحظه‌ای در پیامدهای آن تامل کنیم اما امنیت سایبری را نمی‌توان مسلم دانست. همانطور که مزایا و فرصت‌های فناوری‌ها همچنان در حال رشد است، تامین امنیت آنها نیز به شکل فزاینده‌ای اهمیت پیدا می‌کند.

ارزیابی چشم انداز در حال تغییر

دولت کانادا در سال ۲۰۱۶ اولین قدم را در جهت تدوین «استراتژی جدید امنیت سایبری» برداشت. «بازنگری سایبری» برای درک پیامدهای امنیت سایبری در کشور آغاز شد دولت کانادا نیز رویکرد جدیدی را ایجاد کرد که چالش‌ها و فرصت‌های پیش روی ما را منعکس می‌کرد.

روند «بازنگری سایبری» تهدیدهای در حال تحول در فضای مجازی را مورد ارزیابی قرار می دهد تا راه‌هایی که امنیت سایبری محرک رونق اقتصادی است را درک و کشف کرده و نقش مناسب فدرال را در عصر دیجیتالی تعیین کند. «بازنگری سایبری» شامل تعامل عمیق در جمعیت امنیت سایبری دولت فدرال، ارزیابی عملکرد در راستای «استراتژی ۲۰۱۰» و همچنین نخستین مشاوره عمومی کانادا درباره امنیت سایبری می‌شود. دولت کانادا از کارشناسان، ذی‌فعان اصلی و شهروندان ایده و مشاوره گرفته است.

نگاهی اجمالی بر امنیت سایبری: مزایای بک آپ

ژاکلین صاحب کسب و کار کوچکی است و کارهای دستی را از طریق

یک فروشگاه آنلاین به فروش می‌رساند. روزی ژاکلین از مشتری ایمیلی دریافت می‌کند که از بستهٔ شکسته شده شکایت دارد. مشتری تصویری از محصول را ضمیمه می‌کند اما وقتی ژاکلین پیوست را باز می‌کند، متوجه می شود که رایانه قفل شده است. پیامی ظاهر می شود که نشان می دهد تنها در صورت پرداخت وجه ۱۰۰۰ دلاری به مجرم، قفل رایانه وی باز خواهد شد.

خوشبختانه ژاکلین به طور منظم از رایانه خود بک آپ می‌گیرد. او هارد دیسک خود را پاک می‌کند، بدافزاری را که از طریق پیوست ایمیل دریافت شده بود از بین می‌رود و نسخه پشتیبان او این امکان را می‌دهد تا به تمام اسناد خود دسترسی پیدا کند.

پاسخ ما

«استراتژی جدید امنیت سایبری» چشم‌اندازهای «ارزیابی سایبری» را منعکس می‌کند. همچنین نشان می‌دهد که با افزایش پیچیدگی و حجم تهدیدات سایبری، پتانسیل بسیار زیادی در کانادا برای نوآوری دیجیتال و تخصص در زمینه امنیت سایبری وجود دارد. این برنامه به گونه‌ای طراحی شده است که می تواند فضای سایبری دائما در حال تغییر را در برداشته و با آن سازگار باشد.

«استراتژی ملی امنیت سایبری» در پاسخ به تهدیدات در حال تحول، فرصت های نوظهور و نیاز به اقدام مشترک سه هدف را تعیین می‌کند:

۱) سیستم های امن و انعطاف پذیر کانادایی؛
۲) زیست بوم سایبری مبتکرانه و سازگار؛
۳) رهبری و همکاری موثر.

دولت فدرال تلاش برای دستیابی به این اهداف را در دورانی هدایت می‌کند که امنیت سایبری نه تنها یک ضرورت بلکه یک مزیت رقابتی برای کانادا است.

نگاهی اجمالی بر امنیت سایبری: هوش گذرواژه

کریستین راحتی فضای ابری را دوست دارد. او یک حساب مرکزی به صورت آنلاین ایجاد کرده است که از طریق رایانه، تلفن هوشمند، ردیاب تناسب اندام و حتی سیستم امنیت خانه‌اش همه چیز را مدیریت می‌کند. حساب‌های ایمیل و شبکه‌های اجتماعی وی از طریق ابر به هم متصل هستند، عکس‌ها و فیلم‌های او به طور خودکار بارگذاری می‌شوند و هرگونه به‌روزرسانی تقویم در همه دستگاه‌های وی نمایان می‌شود.

کریستین همیشه از همان رمز عبور استفاده می‌کند تا به خاطر سپردن آن برای او آسان باشد. هنگامی که وی از نفوذ به داده‌ها و اطلاعات مربوط به حساب ایمیل خود با خبر می‌شود، به این نکته پی می‌برد که دسترسی به حساب ابری وی با استفاده از رمز ورود ایمیل برای دیگران امکان‌پذیر است. کریستین که نگران محافظت از حریم خصوصی و اطلاعاتش است، یک رمزعبور جدید و قوی ایجاد می‌کندکه برای سایر سرویس‌های آنلاین کمی متفاوت باشد.

ورودی دریافتی از روند «ارزیابی سایبری» جامع، پیچیده و خردمندانه بود. جامعه سایبری دولت فدرال کانادا، کارشناسان امنیت سایبری، رهبران کسب و کار، مقامات دولتی، مجریان قانون، دانشگاهیان و شهروندان نیز واکنش‌هایی را نشان دادند.

«ارزیابی سایبری» سه روند اصلی را نشان داد:

از تلاش‌ها در راستای اجرای قانون برای رسیدگی به جرایم سایبری ضمن محافظت از حریم خصوصی در فضای مجازی پشتیبانی می‌شود؛

- این آگاهی وجود دارد که امنیت سایبری برای محافظت از اطلاعات شخصی و به طور گسترده، حریم خصوصی، است. کانادایی‌ها از تلاش برای حفظ حریم خصوصی آنلاین خود پشتیبانی می‌کنند؛
- کانادایی‌ها اذعان می‌کنند که اجرای قانون مقابله با جرایم اینترنتی با چالش‌هایی روبرو است و نگران افزایش تهدید جرایم اینترنتی برای افراد، سازمان‌های بخش دولتی و خصوصی و ادارات هستند.

ارتقای دانش و مهارت‌های امنیت سایبری ضرورت بالایی دارد.

- دانش و مهارت‌های بهتری در زمینه امنیت سایبری مورد نیاز است. گستره این امر از فرزندان تا افراد مسن و از صاحبان کسب و کارهای کوچک و متوسط تا سازمان‌های اجرای قوانین و مدیران شرکت‌ها صدق می‌کند.
- سازمان ها، از جمله دولت فدرال، با کمبود استعداد در زمینه امنیت سایبری در جذب و حفظ افراد در راستای ارتقای امنیت سایبری خود و مقابله با تهدیدات سایبری با دشواری روبرو می شوند.

رهبری قدرتمند فدرال در حوزه امنیت سایبری ضرورت دارد.

- شرکای خارجی نقطه کانونی قابل اعتماد رهبری دولت فدرال را در زمینه امنیت سایبری لازم دارند.
- شرکا خواستار پیام‌رسانی، مشاوره و راهنمایی مداوم از طرف دولت

کانادا هستند.

• سازمان‌ها برای روشن شدن الزامات و انتظارات در جهت بهبود امنیت سایبری خود، نیاز به استانداردها یا قوانین مربوط به امنیت سایبری در کانادا دارند.

• ذی‌نفعان می‌خواهند رهبری فدرال را در امنیت سایبری در جهت تقویت همکاری ملی، جذب سرمایه‌گذاری، تسهیل به اشتراک‌گذاری اطلاعات و حفاظت از حقوق و آزادی‌ها، مشاهده کنند.

بخش سوم

بخش سوم

امنیت و انعطاف پذیری

بافت استراتژیک: تکامل تهدید سایبری

تهدیداتی که در فضای مجازی با آن روبرو هستیم، پیچیده بوده و به سرعت در حال تحول هستند. دولت‌ها، کسب و کارها، سازمان‌ها و کانادایی‌ها در این زمینه آسیب‌پذیر هستند. با توجه به اینکه هر ساله بخش حائز اهمیتی از اقتصاد و خدمات ضروری ما به صورت آنلاین انجام می‌شوند، ریسک بالایی متوجه آنها است.

جرایم سایبری و تهدیدات پیشرفته سایبری

مجرمان سایبری بسیار متنوع هستند و اهداف مختلف و طیف گسترده ای از تکنیک‌ها را دارند. فعالان اقدامات مخرب سایبری شامل هکرهای فردی و تهدیدات داخلی، شبکه‌های جنایی، دولت‌ها، سازمان‌های تروریستی و بازیگران تحت حمایت دولت هستند. درک حملات سایبری پیچیده غالباً از نظر فنی چالش برانگیز است و برای این کار تخصص قابل توجهی لازم است.

هر سازمان یا فردی می‌تواند قربانی جرایم سایبری شود. قربانیان ممکن است به صورت جداگانه مورد هدف قرار بگیرند یا بخشی از یک

کمپین باشند که میلیون‌ها کاربر اینترنت را تحت تأثیر قرار دهند. از آنجا که کانادایی ها اطلاعات بیشتری را به صورت آنلاین به اشتراک می گذارند، بنابراین اهداف جذابی برای مجرمان سایبری محسوب می شوند. توانایی سازمان های مجری قانون کانادا در محافظت از کانادایی‌ها در برابر مجرمان سایبری که ممکن است در هر کجای دنیا باشند، چالشی رو به رشد است.

جرایم سایبری اغلب برای سود مالی انجام می‌شود. برای مثال ایمیل‌های فیشینگ که به نظر می‌رسد از مؤسسات مالی ارسال شده‌اند، می‌توانند شهروندان را فریب دهند تا اطلاعات بانکی خود را ارائه دهند. از باج افزارها نیز می‌توان برای رمزگذاری پرونده ها در یک دستگاه یا سیستم استفاده کرد، به طوری که دسترسی به سیستم محدود می‌شود و ایجادکننده آن برای برداشتن محدودیت درخواست باج می‌کند. نفوذ به سیستم داده‌ها می‌تواند منجر به سرقت اطلاعات شخصی و مالی (مانند شماره های بیمه اجتماعی، اطلاعات کارت اعتباری) از پایگاه‌های اینترنتی سازمان‌ها شود و متعاقباً به دلیل فعالیت‌هایی مانند کلاهبرداری، سرقت هویت یا اخاذی در بازارهای جنایی فروخته شود.

مجرمان سایبری همچنین می‌توانند برای مقاصد مختلف، که گاهی اوقات «هکتیویسم» نامیده می‌شوند، به افشای تخلف، اعتراض برای شرمسار کردن می‌پردازند. آنها همچنین برای اینکه مهارت خود را در هک کردن نشان دهند و معروف شوند، دست به چنین اقداماتی می‌زنند.

در مقیاس بزرگتر، دولت‌ها و بازیگران تحت حمایت دولت می‌توانند مالکیت معنوی یا استراتژی‌های محرمانه کسب و کار را سرقت کنند تا برای اقتصاد خودشان مزیت رقابتی به ارمغان بیاورند.

برخی از کشورها نیز در حال توسعهٔ ابزارهای پیشرفته سایبری با اهداف خصمانه هستند. اگر تهدیدی متوجه سیستم‌های رایانه‌ای زیربنای سیستم‌های دولتی، زیرساخت‌های مهم و نهادهای دموکراتیک شود، امنیت ملی و امنیت عمومی کانادا را با ریسک روبرو خواهد شد.
سازمان های تروریستی همچنین علاقه‌مند به دستیابی به ابزارهای پیشرفته سایبری برای انجام حملات هستند.

تأثیر رو به رشد

روند رو به رشد دسترسی به ابزارهای مخرب سایبری و افزایش نرخ جرایم اینترنتی، تهدیدی واقعی پیش روی رفاه اقتصادی کانادا محسوب می‌شوند. علاوه بر این، از آنجا که می‌توان زیرساخت‌های مهم کانادا را از راه دور کنترل و خدمات ضروری را به صورت آنلاین مدیریت کرد، حوادث سایبری امکان به خطر انداختن امنیت ملی و عمومی را دارند.
قربانیان جرایم سایبری برای بازیابی سیستم‌های خود فوراً با هزینه های مادی روبرو می‌شوند. آنها همچنین برای جایگزینی یا به روزرسانی سیستم‌های سایبری باید هزینه های بی شمار اعتباری و طولانی مدتی را متحمل شوند. از آنجا که شرکت‌های استارت آپ آسیب‌پذیرتر هستند، از دست دادن مالکیت معنوی نیز تخریب مالی را برای کسب و کارها به هر اندازه ای به همراه دارد.
حوادث سایبری همچنین می‌تواند عمیقاً بی‌ثبات کننده باشد. آنها می‌توانند اعتماد به تجارت الکترونیکی و نهادهای دولتی را در مردم از بین ببرند. اگر مردم احساس کنند امنیت یا حریم خصوصی آنها در معرض خطر است، در استفاده مستمر از فناوری‌های دیجیتال دچار ابهام می‌شوند.

اینترنت اشیا (IOT) به اشیا و دستگاه‌هایی گفته می‌شود که برای برقراری ارتباط با یکدیگر و ارائه خدمات کارآمدتر و سفارشی‌تر به اینترنت متصل هستند. اینترنت اشیا به سرعت در حال رشد است و انتظار می‌رود تا سال ۲۰۲۰ بیش از ۲۵ میلیارد دستگاه به اینترنت متصل شوند.

نگاهی اجمالی بر امنیت سایبری: ایمیل‌های اسکم یا کلاهبرداری

فصل مالیات است و محسن اخیراً مالیات خود را به صورت آنلاین ثبت می‌کند. چند روز بعد، او ایمیلی را از شخصی که ادعا می‌کند مامور مالیاتی است، دریافت می‌کند و به او می‌گوید اطلاعاتی در پرونده وی وجود ندارد. او برای تکمیل پرونده محسن، فوراً اطلاعات شخصی از جمله آدرس و شماره بیمه اجتماعی او را درخواست می‌کند. در این ایمیل آمده است که عدم ارائه این اطلاعات می‌تواند منجر به مجازات‌های شدید و حتی زندان شود. محسن در مورد ایمیل مشکوک است و بنابراین قبل از ارائه اطلاعات، وب سایت آژانس درآمد کانادا[1] را بررسی می‌کند. در این وب‌سایت آمده است که آژانس درآمد کانادا هرگز با ارسال نامه‌های الکترونیکی از افراد نمی‌خواهد اطلاعات شخصی یا مالی را افشا کنند. او با نادیده گرفتن ایمیل از توصیه‌های آژانس درآمد کانادا پیروی می‌کند.

اتصال دستگاه‌ها به اینترنت در را به سوی ریسک‌های جدید امنیت سایبری باز می‌کند. از شکاف های امنیت سایبری می‌توان برای ایجاد اختلال در خدمات از طریق کمپین‌های حمله توزیع شده انکار از سرویس[2] یا ورود به سیستم‌های گسترده‌تر یا داده‌های خصوصی استفاده کرد. در اکتبر ۲۰۱۶ از میلیون‌ها دستگاه ناامن برای تحت فشار قرار دادن

1. CRA
2. DDoS

سرورهای «داین»، یک شرکت زیرساخت اینترنتی، استفاده شد، طوری که وب‌سایت ها و خدمات آنلاین معروف در سطح بین‌المللی آفلاین شدند. هرچه نوآوری دیجیتال بیشتر جلو برود و فناوری‌های جدید توسعه یابد، ماهیت تهدیدات سایبری دائما تغییر خواهد کرد.

برای مثال، فناوری‌های متصل به اینترنت به طور فزاینده‌ای محبوب هستند، از ترموستات و دستگاه‌های مراقبت‌های بهداشتی مانند ضربان‌ساز قلب گرفته تا ماشین و سیستم هایی که زیرساخت ها و خدمات حیاتی ما را اجرا می کنند. دستگاه های متصل بدون امنیت سایبری کافی، در معرض هک شدن آن هم در مقیاسی بی‌سابقه هستند. به همین ترتیب، بسیاری از کانادایی ها برای ایمن سازی ارتباطات و داده های آنلاین خود به رمزگذاری تکیه می کنند. ورود محاسبات کوانتومی باعث تضعیف امنیت رمزگذاری سنتی می شود و این امر مستلزم آن است که کانادایی ها راه‌حل‌های بهتری در اختیار داشته باشند. به منظور همگام شدن با این تغییرات، اتخاذ نگرشی آینده‌نگرانه و انعطاف‌پذیر در حوزه امنیت سایبری ضروری است.

نگاهی اجمالی بر امنیت سایبری: انعطاف‌پذیری از طریق به اشتراک گذاری اطلاعات

بوئم ژان در دپارتمان فناوری اطلاعات یک مؤسسه مالی بزرگ کار می‌کند. وی اخیراً متوجه شده است که چندین بار تلاش کرده‌اند تا سیستم را هک کنند. با وجود اینکه این تلاش ناموفق بوده است، اما او تصمیم می‌گیرد اطلاعات فنی را برای تجزیه و تحلیل به مرکز پاسخگویی حوادث سایبری کانادا[1] ارسال کند. بوئم می‌دانست که

1. CCIRC

مرکز پاسخگویی حوادث سایبری کانادا برای گزارش حوادث سایبری به سازمان‌های مهم زیرساختی متکی است تا بتوانند روندها و تهدیدها را به سایر بخش‌ها و شرکای بین‌المللی اطلاع دهند. او قدردانی می‌کند که آنها با همکاری یکدیگر امنیت سایبری سازمان‌هایی که کانادایی‌ها به آن اعتماد دارند را افزایش می‌دهند.

مشاوره عمومی درباره امنیت سایبری

آنچه که شنیدیم

«چالش شماره ۱ سایبری کانادا این است که تخلفات، جرایم، اختلال در خدمات ضروری و از بین بردن دارایی های شرکت‌ها و کشورها، آسیب زیادی به اقتصاد و جامعه وارد می‌کنند.»

«حریم خصوصی و امنیت یک بازی با جمع صفر نیست و ما می‌توانیم هر دو را داشته باشیم. بدون حریم خصوصی هیچ امنیتی وجود ندارد. و آزادی نیز به امنیت و حریم خصوصی نیاز دارد.»

«مجری قانون در کانادا باید منابع جرایم اینترنتی خود را متمرکز کند. ایجاد یک مرکز، کار را برای کسب و کارها آسان‌تر خواهد کرد. به این ترتیب، هنگامی که سیستم‌هایشان به خطر می‌افتد، آنها می‌دانند با چه کسی تماس بگیرن. این مرکز همچنین برای تحقیقات و پاسخگویی به جرایم اینترنتی در سراسر حوزه‌های قضایی کمک می‌کند.»

سیستم‌های امن و انعطاف‌پذیر کانادایی

ما از طریق همکاری مشترک با شرکا و افزایش قابلیت‌های امنیت سایبری، به شکل بهتری از کانادایی‌ها در برابر جرایم اینترنتی محافظت خواهیم

کرد، به تهدیدات در حال توسعه پاسخ خواهیم داد و از سیستم‌های حیاتی دولتی و بخش خصوصی دفاع خواهیم کرد.

دولت کانادا برای محافظت از حریم خصوصی اطلاعات کانادایی ها که در اختیار ادارات و آژانس‌های دولت فدرال است، محافظت می‌کند و در راستای محرمانگی، یکپارچگی و دسترسی کانادایی‌ها به خدمات حیاتی، امنیت سایبری را حفظ کرده و توسعه می بخشد.

دولت کانادا ظرفیت اجرای قانون را برای پاسخگویی به جرایم اینترنتی افزایش می‌دهد. این برنامه از هماهنگی میان آژانس‌های اجرای قانون و شرکای فدرال، ایالتی و بین‌المللی پشتیبانی خواهد کرد. دولت ظرفیت تحقیقات درباره جرایم اینترنتی را ارتقا داده و گزارش جرایم اینترنتی را برای کانادایی‌ها آسان‌تر می‌کند.

سازمان‌های کوچک و متوسط اغلب دانش و منابع لازم برای اجرای سیستم‌های امنیتی سایبری را ندارند، حتی اگر انجام این کار مزیت رقابتی داشته باشد. بنابراین، دولت کانادا از این سازمان‌ها پشتیبانی می‌کند و امنیت سایبری را بیشتر در دسترس قرار می دهد.

دولت کانادا در پاسخ به تهدیدهای سایبری و افزایش پیچیدگی آنها، در نظر دارد که چگونه می‌توان از قابلیت های پیشرفته سایبری خود برای دفاع از شبکه های حیاتی در کانادا و بازدارندگی تهدیدات سایبری خارجی استفاده کرد.

برخی از سیستم‌های سایبری ـ مانند شبکه‌های برق، شبکه‌های ارتباطی یا مؤسسات مالی ـ آنقدر مهم هستند که هرگونه اختلال می‌تواند عواقب جدی برای امنیت عمومی و امنیت ملی به همراه داشته باشد. دولت فدرال برای کمک به تعریف الزامات محافظت از زیرساخت دیجیتال، با ایالت ها، ناحیه ها و بخش خصوصی همکاری خواهد کرد.

بخش چهارم

بخش چهارم

نوآوری سایبری

بافت استراتژیک: گسترش مرزهای امنیت سایبری

نوآوری دیجیتال در قرن ۲۱ به موتور رشد اقتصادی تبدیل شده است. امنیت سایبری نه تنها برای محافظت از منابع نوآوری دیجیتالی کانادا ضروری است، بلکه خود به منبعی برای نوآوری تبدیل شده است.

افق‌های جدید فناوری و توسعه کسب‌وکار

امنیت سایبری به طور فزاینده‌ای ابتکار و فعالیت اقتصادی را در کانادا به ارمغان می آورد. این روند در حال حاضر ۱/۷میلیارد دلار به تولید ناخالص داخلی کانادا کمک می کند و بیش از ۱۱ هزار شغل پردرآمد را نیز شامل می شود. با پیش بینی رشد ۶۶ درصدی صنعت امنیت سایبری در سال ۲۰۲۱، هزاران شغل جدید برای کانادایی ها در سال های آینده ایجاد می شود. دولت، دانشگاهیان و اعضای بخش خصوصی می‌توانند با هم همکاری کنند تا فرصت های جدیدی ایجاد شود. آنها همچنین می توانند سرمایه‌گذاری کرده و تحقیق و توسعه پیشرفته را تقویت کنند.

1. International Data Corporation (IDC) Canada, "2016 Canadian ICT Predictions and Forecast: Digital Transformation and Disruption," December 2015
Information and Communications Technology Council (ICTC), "Critical Infrastructure in a Hyperconnected Economy," August 2016.
2. Research and Markets, "Cyber Security Market – Global Forecast to 2021," August 2016.

کانادا در حال حاضر در زمینه تحقیق و توسعه امنیت سایبری پیشرو است. پیشرفت در تحقیقات مربوط به امنیت سایبری نه تنها برای شرکت‌های امنیت سایبری کانادا بلکه برای کل اقتصاد مفید است. دولت در حمایت از تحقیقات پیشرفته و کمک به شرکت‌های نوآور در توسعه فناوری‌ها و ارائه خدمات امنیت سایبری در بازارهای جهانی نقشی مهم دارد.

نگاهی اجمالی بر امنیت سایبری: مهارت‌ها در عصر دیجیتالی

مارک در جست‌وجوی اردوهای تابستانی برای دخترانش است. او دنبال اردویی است که به آنها اجازه می‌دهد در حالی که مهارت‌های جدیدی را فرا می‌گیرند، موضوع متفاوتی را امتحان کنند. او برنامه‌ای را پیدا کرد که برای کمک به کودکان در توسعه مهارت‌های اساسی برنامه‌نویسی طراحی شده، که به آنها ابزارهای لازم برای ساخت وب سایت ها و توسعه برنامه‌های خود را می‌دهد. دختران مارک، با تشویق پدر در اردوگاه ثبت نام می‌کنند و دری به سوی دنیایی با سرگرمی جدید و مهارت مهیج برایشان باز می‌شود.

بهره گیری از مزایای فناوری دیجیتال

مشارکت دولت کانادا در زندگی دیجیتال رفاه و مزایای بی‌نظیری را به ارمغان آورده و دروازه‌ای جدید را به جهان گشوده است. ادارات، کسب و کارها و سایر سازمان‌ها با استحکام امنیت پلتفرم‌ها، محصولات و خدمات آنلاین در محافظت از این مزایا، نقشی اساسی دارند.

قدرت امنیت سایبری به اندازه ضعیف‌ترین رشته آن است. بنگاه‌های

کوچک و متوسط و در واقع بسیاری از سازمان ها در کانادا، با تضمین امنیت سیستم ها و شبکه های خود مانند دیگر همتایان خود با چالش های مشابهی روبرو هستند و این در حالی است که این کار را باید با تخصص و منابع کمتر انجام دهند. ادارات می‌توانند با ارائه مشاوره و راهنمایی و افزایش دسترسی به اطلاعات و ابزارهای امنیت سایبری به اصلاح این عدم تقارن کمک کنند. این روند به سازمان های کانادایی در بخشهای دولتی و خصوصی کمک می کند تا فناوریهای دیجیتال را با موفقیت اجرا کنند.

نگاهی اجمالی بر امنیت سایبری: افزایش بازدهی ارائه خدمات

استوارت وقتی فهمید که می‌تواند بدون نیاز به یادآوری رمز ورود دیگر، به حساب برنامه بازنشستگی خود دسترسی پیدا کند، خیالش آسوده شد. تنها کاری که او باید انجام دهد این است که به صفحه ورود به سیستم برنامه بازنشستگی کانادا برود، روی لوگوی مربوط به بانک خود کلیک کرده و اطلاعات خود را وارد کند. او از نام کاربری و رمز عبور مشابه بانکی آنلاین خود استفاده می‌کند، زیرا بانک او شریک سیستم ورود به خدمات آنلاین دولت کانادا است. او واقعاً این مزیت را دوست دارد و از آنجا که به اقدامات امنیتی بانک خود اعتماد دارد، می‌داند که از اطلاعاتش محافظت می شود. همانطور که پسرش دیوید مرتباً به او می‌گوید، تا زمانی که وای فای امن و شبکه ای با رمز عبور استفاده کند، اطلاعات بانکی وی ایمن‌تر خواهد بود. ظاهراً هکرها می‌توانند از طریق سیستم بدون امنیت وای فای، برای مثال در کافی شاپ یا فرودگاه، ترافیک را رهگیری کنند.

دانش فردی، از سواد دیجیتال تا مهارت های مربوط به برنامه نویسی و کاهش تهدیدات سایبری، نقش مهمی را در امنیت سایبری بازی می‌کند. اقداماتی که در جوامع، مدارس و مؤسسات دوره متوسطه کانادا اتخاذ شده است، کانادایی‌ها را به مهارت‌های عصر دیجیتال مجهز می‌کند. دولت کانادا با کمک سرمایه گذاری‌های طولانی مدت سهم خود را ایفا کرده و به همه شهروندان کانادایی کمک می‌کند تا تحصیلات و تجربه کاری لازم را برای مشارکت در اقتصاد دیجیتالی به طور فزاینده کسب کنند.

علم و فناوری کوانتوم امکان پردازش و اطمینان از اطلاعات را با سرعت و امنیت بیشتری فراهم می‌کند. دستگاه‌های کوانتومی می توانند مزایای منحصر به فردی را در زمینه‌های مختلف، از جمله کمک به درک چگونگی روند گسترش بیماری‌ها یا بهبود درمان‌های پزشکی ارائه دهند. گرچه کوانتوم می تواند اطلاعات را ایمن کرده و فناوری را به مرزهای جدیدی برساند، اما با این حال ممکن است استفاده از آن اشکال مختلف رمزگذاری که امروزه برای محافظت از سیستم‌ها و برنامه‌ها در کانادا و سراسر جهان استفاده می شود، را با ریسک هایی مواجه کند.

تلاش‌های صورت گرفته همراه شناخت فرصت‌ها و چالش‌های محاسبات کوانتومی، پایگاه تخصصی و قوی را در محاسبات کوانتومی در کانادا ایجاد کرده است، مانند آنچه در انستیتوی محاسبات کوانتومی در دانشگاه واترلو دیده می‌شود.

پیشرفت مهارت‌ها و دانش قرن بیست و یکم

تقاضا برای متخصصان واجد شرایط امنیت سایبری در حال افزایش

است. کمبود متخصصان واجد شرایط در جهان، فرصتی فوری و رو به رشد را پیش روی نیروی کار با تحصیلات عالی کانادا قرار می‌دهد. ما می توانیم دانشجویان بیشتری را ترغیب کنیم که به سمت رشته‌های علوم، فناوری، مهندسی و ریاضیات بروند. ما می توانیم فارغ التحصیلان رشته های علوم، فناوری، مهندسی و ریاضیات و همچنین سایر رشته ها (مانند روانشناسی، جامعه‌شناسی یا مدیریت) را به کسب تخصص در مهارت‌های مورد نیاز برای مشاغل امنیت سایبری تشویق کنیم. جذب استعداد چند رشته ای از داخل و از خارج کشور، برای دولت‌ها و مشاغل کانادا ضروری است و اطمینان می‌دهد که شرکت های کانادایی با گسترش استفاده از فناوری دیجیتال قادر به رشد و نوآوری ایمن نیز هستند.

با ادامه تکامل محیط امنیت سایبری، دائماً به اطلاعات معتبر و به روز نیاز داریم. آمار و تحقیقات در زمینه امنیت سایبری دیدگاه دقیق‌تری را از موضوعات سایبری کشورمان در بستر جهانی ارائه می دهد. دانشگاهیان، محققان و سیاست‌گذاران می‌توانند از این اطلاعات برای درک گرایش‌ها، مدیریت ریسک، اطلاع رسانی برای سرمایه‌گذاری‌های آینده و در صورت لزوم تنظیم روش‌ها استفاده کنند.

مشاوره عمومی درباره امنیت سایبری

آنچه شنیدیم

«ما باید اطمینان حاصل کنیم که شرکت ها استارتاپ و نوآوری که در کانادا شکل گرفته اند، در کانادا می‌مانند.»

«دولت فدرال می‌تواند در این زمینه نقشی منحصر به فرد داشته باشد که کسب وکارها کانادا را مکانی بدانند که می‌توانند در یک فضای

امن سایبری رشد کنند.»

«تعداد کمی ارتباط استراتژیک اطلاعات امنیت سایبری را درک می‌کنند. شما نمی‌توانید آنچه را که نمی‌سنجید، مدیریت کنید.»

زیست‌بوم سایبری مبتکرانه و سازگار

دولت فدرال با حمایت از تحقیقات پیشرفته، ارتقای نوآوری دیجیتال و توسعه مهارت‌ها و دانش سایبری، کانادا را به عنوان رهبر جهانی امنیت سایبری معرفی می‌کند.

دولت کانادا برای جذب سرمایه‌گذاری و پیشرفت در تحقیق و توسعه سایبری با شرکای خود همکاری خواهد کرد. دولت بر زمینه‌های جدید، مانند محاسبات کوانتومی و فناوری‌های بلاکچین تمرکز خواهد کرد. دولت فدرال با اعلام بودجه ۲۰۱۷ و ایجاد استراتژی هوش مصنوعی پان کانادایی برای توسعه تحقیقات و استعدادها، در حال پیشرفت در این زمینه است.

ما با هم در میان اقدامات و نوآوری‌ها جستجو خواهیم کرد تا اطمینان حاصل کنیم که شرکت‌های کانادایی می‌توانند محصولات خود را به بازار جهانی ارائه دهند. دولت ابتکارات جدید را در راستای ایجاد تقاضای داخلی برای فناوری‌ها و خدمات امنیت سایبری بررسی خواهد کرد.

دولت کانادا ایده‌های جدید را بررسی خواهد کرد تا کسب و کارها و همه شهروندان کانادایی از امنیت سایبری بیشتر بهره‌مند شوند. دولت فدرال پیشتر برای بهبود مهارت‌های دیجیتالی، مانند آموزش کدنویسی به کودکان، سرمایه‌گذاری کرده است.

همکاری مشترک میان ادارات، دانشگاه‌ها و بخش خصوصی برای رفع

شکاف مهارت‌های سایبری ضروری است. حال حاضر، برداشتن این قدم ها به ما امکان می‌دهد تا نیروی کار آینده را بسازیم، نیرویی که به حمایت از امنیت سایبری و شکوفایی آینده کانادا کمک کند.

کیفیت اطلاعاتی که در اختیار ما است، توانایی ما در درک روندهای سایبری را شکل می دهد. دولت فدرال از تحقیقات و آمارهای کانادایی برای بهبود درک جمعی ما از تهدیدات و فرصت های سایبری پشتیبانی خواهد کرد.

بخش پنجم

بخش پنجم

رهبـری و همکاری

بافت استراتژیک: همکاری در راستای درک مزایای زندگی دیجیتال

ایـن عوامـل امـروزه بـه کیفیـت زندگـی مـا کمـک مـی‌کننـد و در مقابله بـا چالـش‌هـای آینـده نقـش مهمـی دارند. همـه مـا مسـئولیت امنیـت این فنـاوری‌هـا را بـر عهـده داریـم. از طریق اسـتراتژی ملـی امنیت سـایبری، دولت کانـادا راه هـای همـکاری در ایـن راسـتا را پیش مـی برد.

ارتقای مبنای امنیت سایبری در کانادا

اکثریـت قریـب بـه اتفاق سیسـتم های دیجیتالـی کانادا متعلق بـه افراد و سـازمان هـای خـارج از دولـت فدرال اسـت. از افرادی که تنهـا از چند فناوری اسـتفاده مـی‌کننـد تا کسـب و کارهای دارای فـن آوری های مبتنـی بر دنیای آنلایـن، بسـیاری نمی داننـد که می توانند هدف تهدیدهای سـایبری باشـند. در نتیجـه، اقدامـات لازم بـرای محافظـت از خود و غلبه بر حوادث سـایبری را انجـام نمـی دهند، حتی کسـانی که اهمیت امنیت اطلاعات خود را تشـخیص مـی دهند تشـخیص اقدامـات مقرون به صرفـه و مؤثر بـرای محافظت از خود را دشـوار می پندارند.

دولت کانادا به منظور کمک به سازمان‌ها و کانادایی‌ها برای درک ارزش امنیت سایبری و حمایت از تلاش‌ها برای بالا بردن سطح امنیت سایبری در کانادا، نقش رهبری را بر عهده دارد و همراه همکاری با شرکا و متحدان بین‌المللی تلاش های داخلی را تکمیل خواهد کرد. این تلاش‌ها در راستای کاهش تهدید مجرمان اینترنتی و همچنین نمایندگان دولتی می‌باشد که به دنبال این هستند که به ما آسیب برسانند.

علاوه بر این، دولت فدرال برای موفقیت امنیت سایبری ملی تلاش می کند. دستیابی به این هدف شامل افزایش و رشد قابلیت های امنیت سایبری در دولت و صنعت است. این امر مستلزم حمایت از تحقیق و توسعه پیشرفته در کانادا است و طیف وسیعی از سازمان ها و کسب و کارهای مختلف را پوشش می دهد که اقدامات ضروری امنیت سایبری را اعمال نمی کنند. رهبران بخش خصوصی نقشی اصلی را بازی می کنند، زیرا تلاشی مشترک مورد نیاز است تا اطمینان حاصل شود که بیشتر کانادایی ها برای جلوگیری و پاسخگویی به تهدیدات سایبری مجهز هستند.

فناوری بلاکچین امکان ایجاد دفتر کل یا گزارش آنلاین را فراهم می کند. بلاکچین غالباً با ارزهای مجازی شناخته شده است، اما چندین کاربرد دیگر نیز دارد. می‌توان از آن برای ارائه خدمات عمومی مانند صدور گذرنامه، ایجاد سوابق قرارداد یا اسناد حقوقی و پردازش پرداخت برای خدمات ارائه شده استفاده کرد. این فناوری با کاهش زمان پردازش برای فعالیت ها، میزان کارایی را بهبود می بخشد و خطر تقلب را کاهش می دهد، زیرا هیچ یک از طرفین نمی تواند سوابقی را اصلاح، حذف یا ضمیمه کند.

دولت کانادا از پتانسیل بلاکچین در ارائه خدمات ایمن و مزایای اقتصادی

و اجتماعی گسترده تر آگاه است. اطمینان از کاربرد هوشمند فناوری های بلاکچین در کانادا نیاز به رویکرد مشترک و تلاش جمعی دارد.

پیشتازی و رهبری امنیت سایبری فدرال در محیطی پویا

دولت کانادا در موقعیت منحصر به فردی برای ایفای نقش رهبری در حوزه امنیت سایبری قرار دارد. این امر برآمده از روابط گسترده با بخش‌های خصوصی و دولتی، سابقه همکاری با ایالت‌ها، مناطق و مقامات بین المللی در زمینه طیف وسیعی از مسائل مربوط به امنیت سایبری و تخصص و توانایی‌های پیشرفته امنیت سایبری است.

رهبری فدرال در حوزه امنیت سایبری از طریق «استراتژی ۲۰۱۰» و اقدامات مربوط به آن شکل گرفت. با این وجود، در فضای امنیت سایبری امروز دولت فدرال باید برای تقویت امنیت سایبری کانادا همکاری با شرکا را تعمیق بخشد. اقدامات هماهنگ و یکپارچه همه طرف‌ها برای ایجاد انعطاف‌پذیری سایبری در کانادا لازم است.

ایجاد نقطه کانونی روشن برای امنیت سایبری در دولت فدرال یکی از راه‌هایی است که دولت از آن طریق توانایی رهبری خود را نشان می دهد و در عین حال ظرفیت خود را برای همکاری با شرکا نیز افزایش می دهد. همچنین، دولت اطمینان حاصل خواهد کرد که شرکایش مشاوره و راهنمایی واحدی درباره امنیت سایبری دریافت می‌کنند و می‌دانند برای رسیدگی به کجا مراجعه کنند.

شهرهای هوشمند به منظور ارتقای کیفیت زندگی از فناوری های دیجیتالی استفاده می‌کنند و خدمات را برای ساکنان شهر به شکل کارامدتر، مقرون به صرفه تر و مسئولانه تری ارائه می دهند. برای مثال، چراغ‌های

راهنمایی «هوشمند» برای بهبود جریان ترافیک زمان را اندازه گیری و تنظیم می کنند، و سیستم‌های فاضلاب «هوشمند» نیز نشتی را تشخیص می دهند و جریان آب را در زمان واقعی کنترل می کنند.

دولت فدرال به منظور تسریع در توسعه شهرهای هوشمند در کانادا، طرح «چالش شهرهای هوشمند» را در بودجه ۲۰۱۷ اعلام کرد.

دولت فدرال سرمایه گذاری هوشمندانه ای در زمینه امنیت سایبری انجام خواهد داد، ضمن اینکه از شرکای خود در بخش خصوصی و سایر حوزه های قضایی نیز حمایت می‌کند تا همین کار را انجام دهند. سازمان های بخش خصوصی در کانادا قابلیت امنیت سایبری در سطح جهانی را دارا هستند که بهره گیری از مزایای آن می تواند به نفع همه بخش‌های اقتصاد کانادا باشد. همچنین مدارس و مؤسسات دوره متوسطه دارای ایده‌های عالی و رهبری قوی هستند. این امر در شکل گیری آینده امنیت سایبری در کانادا نقش مهمی خواهد داشت.

دولت کانادا تلاش خواهد کرد تا در راستای توسعه مهارت های سایبری، پیشبرد راه حل های جدید و تقویت امنیت سایبری پلی بر روی تلاش های ملی بزند. ما از این نظر برای جهانیان الگو خواهیم بود که از طریق «استراتژی ملی امنیت سایبری» منسجم و منطقی به چه اهدافی می توان رسید.

نگاهی اجمالی بر امنیت سایبری: همکاری در راستای حل مشکلات امنیت سایبری

آگوستین دعوت نامه ای برای شرکت در جشنواره سالانه هفته برنامه نویسان در مرکز واکنش به حوادث سایبری کانادا دریافت کرد. وی سال گذشته در این جشنواره شرکت کرده بود و از همکاری با متخصصان و

دانشگاهیان حوزه سایبری کانادا و دیگر کشورها برای حل مشکلات امنیت سایبری لذت برد. آگوستین پس از شرکت در این جشنواره هنگامی که سر کار بازگشت به این نکته پی برده بود که مهارت‌ها و ارتباطاتی حرفه‌ای را به دست آورده است. در رویداد سال گذشته، تیم او نمونه های نخستین ابزارهای مرکز واکنش به حوادث سایبری را برای تجزیه و تحلیل خودکار بدافزار و باج‌افزار مبتنی بر تلفن همراه مورد آزمایش قرار داد و همچنین نحوه استفاده از رمزگذاری در چنین دستگاه هایی را توسط مهاجمان مورد بررسی قرار داد. این حقیقت برای او خوشایند آمده که کاری که آنها انجام دادند، می‌تواند منفعتی واقعی داشته باشد و تیم او پس از این رویداد قادر است ابزاری که روی آن کار کرده اند را به سازمان های خود بازگرداند تا پیشرفت بیشتری حاصل شود.

مشاوره عمومی درباره امنیت سایبری

آنچه شنیدیم

«دولت کانادا می تواند با ایجاد، اتخاذ و الگوبرداری بهترین شیوه‌ها در زمینه امنیت سایبری و تلاش برای انتقال این دانش به بخش خصوصی، پیشتاز باشد و نقش رهبری را ایفا کند.»

«به منظور تصویب قوانین و مقررات مدرن و رهبری در شناسایی، اولویت بندی، تأیید و انتشار آخرین استانداردهای بین‌المللی فناوری امنیت سایبری، حاکمیت متمرکزتر و برنامه ریزی استراتژیک مورد نیاز است.»

«ما در مجموع نیاز به ایجاد یک چارچوب مؤثر برای حکومت امنیت سایبری و پوشش اصول، نقش‌ها و مسئولیت‌ها در دولت و در بخش‌های دولتی و خصوصی داریم.»

رهبری، مدیریت و همکاری مؤثر

دولت فدرال از طریق همکاری نزدیک با ایالت‌ها، ناحیه‌ها و بخش خصوصی، برای پیشبرد امنیت سایبری در کانادا نقش رهبری را بر عهده خواهد گرفت و با هماهنگی با متحدان، در جهت ایجاد فضای بین‌المللی امنیت سایبری به نفع کانادا تلاش خواهد کرد.

دولت کانادا در پاسخ به درخواست‌های مربوط به رهبری قاطع فدرال، با ایجاد یک نقطه کانونی روشن برای مشاوره معتبر، راهنمایی و پاسخ به حوادث سایبری، نحوه کار و همکاری با شرکای خارجی و سهامداران را ساده می‌کند. این رویکرد اشتراک اطلاعات را توسعه می‌بخشد و دستیابی به پشتیبانی مورد نیاز را برای بخش خصوصی آسان می‌کند.

دولت کانادا به آگاهی عمومی و تلاش در زمینه تعامل، نیرو می‌بخشد و مجامع جدیدی را برای همکاری ایجاد خواهد کرد. دولت فدرال با بخشی از ذی‌نفعان کانادایی مشورت و همکاری خواهد کرد تا اطمینان حاصل شود که ما با هم امنیت سایبری را در کانادا تقویت می‌کنیم.

دولت فدرال با مشارکت ایالت‌ها، ناحیه‌ها و بخش خصوصی، توسعه طرحی ملی برای جلوگیری، کاهش و واکنش به حوادث سایبری را هدایت می کند، برنامه ای که هماهنگی کارآمد و اقدامات موثر را تضمین می‌کند.

دولت کانادا برای پیشبرد منافع کانادا با شرکای بین المللی خود همکاری خواهد کرد. این همکاری شامل حمایت از یک اینترنت باز، رایگان و امن و تقویت همکاری بین‌المللی برای مبارزه با جرایم اینترنتی است.

بخش ششم

بخش ششم

واژه نامـه کتاب

اپ / اپلیکیشن

اپلیکیشـن، برنامه‌ای اسـت که کاربر در دسـتگاه تلفن همراه خود بارگیری می‌کند (برای مثال، اپلیکیشـن ردیابی تناسـب اندام).

هوش مصنوعی

زیرمجموعه علوم کامپیوتر مربوط به توسـعه برنامه‌های رایانه‌ای هوشـمند اسـت کـه مـی‌تواند مشـکلات را حل کنـد، از تجربه بیامـوزد، زبـان را بفهمد، صحنـه‌هـای بصـری را تفسـیر کنـد و به طـور کلی، رفتاری داشـته باشـد که در صورت مشـاهده در انسـان، هوشـمندانه تلقی شود.

بلاکچین

بلاکچین پایگاه داده فقط نوشـتنی اسـت که در شـبکه‌ای از رایانه های به هم پیوسـته توزیع شـده اسـت که از رمزنگاری (رمزگذاری و رمزگشـایی رایانه ای اطلاعـات) بـرای ایجـاد گـزارش عمومی تراکنش‌ها اسـتفاده می‌کنـد که قابل تغییـر و دسـتکاری نیسـتند. فنـاوری بلاکچیـن شـفاف، ایمـن و غیرمتمرکز

است، به این معنی که هیچ تغییری در سوابق عمومی از سوی مرکز نمی‌تواند ایجاد شود.

پردازش ابری

امکان دسترسی به تمام نرم‌افزارها، داده ها و منابع مورد نیاز از طریق شبکه رایانه‌ای به جای مدل سنتی فراهم می‌شود. در مدل سنتی، اطلاعات در رایانه کاربر ذخیره می‌شوند.

زیرساخت حیاتی

فرایندها، سیستم‌ها، امکانات، فناوری‌ها، شبکه‌ها، دارایی‌ها و خدمات ضروری برای سلامت، ایمنی، امنیت یا رفاه اقتصادی کانادایی ها و عملکرد مؤثر دولت.

زیرساخت های حیاتی می توانند در ایالت ها، ناحیه ها و مرزهای ملی مستقل یا بهم پیوسته و وابسته به یکدیگر باشند. اختلال در زیرساخت‌های حیاتی می‌تواند از دست دادن فاجعه بار زندگی، اثرات نامطلوب اقتصادی و آسیب قابل توجه به اعتماد عمومی را به همراه داشته باشد.

حمله سایبری

حمله‌ای که شامل استفاده غیرمجاز، دستکاری، قطع یا تخریب یا دسترسی به اطلاعات الکترونیکی یا دستگاه های الکترونیکی یا سیستم های رایانه ای و شبکه های مورد استفاده برای پردازش، انتقال یا ذخیره اطلاعات باشد.

حادثه سایبری

هرگونه تلاش غیرمجاز، چه موفق و چه غیرموفق، برای دستیابی، اصلاح، تخریب، حذف یا از دسترس خارج کردن شبکه های رایانه‌ای یا منابع سیستم.

امنیت سایبری

حفاظت از اطلاعات دیجیتالی و همچنین یکپارچگی زیرساخت‌ها و انتقال اطلاعات دیجیتالی. به طور ویژه، امنیت سایبری شامل مجموعه ای از فناوری‌ها، فرایندها، روش ها و اقدامات واکنشی و اصلاحی است که برای محافظت از شبکه ها، رایانه ها، برنامه ها و داده ها در برابر حمله، آسیب یا دسترسی غیر مجاز طراحی شده است تا از محرمانه بودن، یکپارچگی و دسترسی اطمینان حاصل شود.

تهدید سایبری

عامل تهدید، که از طریق اینترنت، به منظور بهره برداری از شبکه و اطلاعات داخل آن از نقطه ضعف محصول استفاده می کند.

جرایم اینترنتی

جرمی که مستقیماً یا از طریق سیستم پردازش داده یا شبکه رایانه‌ای صورت می‌گیرد. رایانه یا داده‌های آن ممکن است هدف جرم باشد یا رایانه ممکن است ابزاری باشد که جرم با آن انجام شده است.

فضای سایبری

دنیای الکترونیکی که توسط شبکه‌های به هم پیوسته فناوری اطلاعات و اطلاعات موجود در آن شبکه‌ها ایجاد شده است. این فضا جهانی است که بیش از ۳ میلیارد نفر برای تبادل ایده، خدمات و دوستی با یکدیگر در ارتباط هستند.

نفوذ به داده‌ها

افشای غیرمجاز اطلاعاتی که امنیت، رازداری یا یکپارچگی اطلاعات قابل شناسایی شخصی را به خطر می اندازد.

انکار سرویس توزیع شده (DDOS)

نوعی حمله انکار سرویس که در آن مهاجم با استفاده از یک کد مخرب نصب شده بر روی رایانه‌های مختلف به یک هدف واحد حمله می‌کند.

تجارت الکترونیک

خرید و فروش اطلاعات، محصولات و خدمات از طریق اینترنت.

رمزگذاری

رمزگذاری رشته ای است که شامل اصول، ابزارها و روش‌های تبدیل داده ها به منظور پنهان کردن محتوای اطلاعات، جلوگیری از اصلاح غیرقابل شناسایی و یا جلوگیری از استفاده غیر مجاز از آن می‌شود. تبدیل اطلاعات به فرم جدید محافظت شده را رمزگذاری می نامند. تبدیل اطلاعات به شکل اصلی آن رمزگشایی است.

هکر

شخصی که از رایانه و اینترنت برای دسترسی به رایانه ها و سرورها بدون اجازه استفاده می‌کند.

تهدید داخلی

تهدیدی مخرب برای سازمان از سوی افراد درون سازمان، مانند کارمندان فعلی، کارمندان سابق، پیمانکاران یا همکاران بازرگانی که اطلاعات داخلی مربوط به شیوه‌های امنیتی سازمان، داده‌ها و سیستم‌های رایانه‌ای را در اختیار دارند.

مالکیت معنوی (IP)

طبق گفته سازمان جهانی مالکیت معنوی، مالکیت معنوی ابداع ذهن است. مالکیت معنوی شامل اختراعات، آثار ادبی و هنری، طرح‌ها و نمادها و نام‌ها و تصاویر مورد استفاده در تجارت است.

اینترنت اشیا

اتصال از طریق اینترنت دستگاه‌های محاسباتی اشیای روزمره، به طوری که آنها را قادر به ارسال و دریافت داده می‌کند.

نرم‌افزار مخرب / بدافزار

نرم‌افزار مخرب که بدون رضایت مالک برای نفوذ یا آسیب رساندن به سیستم رایانه ای طراحی شده است. انواع رایج بدافزارها شامل ویروس‌های رایانه‌ای، کرم‌ها، تروجان‌ها، جاسوس افزارها و بدافزار تبلیغاتی است.

محاسبات کوانتومی

رایانه کوانتومی می‌تواند تعداد زیادی از محاسبات را به طور همزمان پردازش کند. در حالی که یک رایانه کلاسیک با یک و صفر کار می‌کند، یک رایانه کوانتومی این مزیت را خواهد داشت که از یک، صفر و «همپوشانی» یک و صفر استفاده کند.

کامپیوتر کوانتومی برخی از کارهای دشوار که مدت‌هاست برای رایانه‌های کلاسیک غیرممکن تصور می‌شد را به سرعت و با کارآیی بالا انجام می‌دهد.

باج افزار

نرم‌افزاری که شما را از دسترسی به پرونده‌هایتان تا پرداخت باج منع می‌کند.

شهرهای هوشمند

شهرهای هوشمند از فناوری‌های دیجیتالی برای ارتقای کیفیت زندگی استفاده می‌کنند تا خدمات موثرتر، مقرون به‌صرفه‌تر و مسئولانه‌تری به ساکنان شهری ارائه دهند.

اسپیر فیشینگ، فیشینگ

استفاده از ایمیل‌های جعلی برای ترغیب افراد درون سازمانی به فاش کردن نام کاربری یا رمزهای عبور. بر خلاف فیشینگ که شامل ارسال حجم زیادی از ایمیل است، اسپیر فیشینگ در مقیاس کوچک و با هدف مشخص صورت می‌گیرد.

csri.majazi.ir

حوزه فضای مجازی به اندازه انقلاب اسلامی اهمیت دارد. این فضا مثل یک رودخانه پر از آب و خروشان است که می آید و دائماً هم بر آب آن افزوده و خروشان تر می شود. اگر ما بر این رودخانه تدبیر کنیم و برنامه داشته باشیم، زه‌کشی کنیم و هدایت کنیم این رودخانه را تا به سد بریزد، می‌شود فرصت. اگر رهایش کنیم و برنامه‌ای برای آن نداشته باشیم می‌شود یک تهدید.

csri.majazi.ir