مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

گزارش سریع
چهل و هشتم

استراتژی امنیت سایبری ۲۰۲۰ استرالیا

Cyber Security Strategy
2020 Australia

بسم الله الرحمن الرحیم

گزارش سریع

گزارش شماره ۴۸
شهریور ۱۴۰۱

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

استراتژی امنیت سایبری کشورهای منتخب
دولت استرالیا
(استراتژی امنیت سایبری ۲۰۲۰ استرالیا)

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)

مترجم: 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 ۵
مقدمه ۹

بخش اول (استراتژی امنیت سایبری ۲۰۲۰ استرالیا: در یک نگاه) ۱۵

بخش دوم (بررسی اجمالی) ۲۱

بخش سوم (فضای تهدید) ۲۹

بخش چهارم (مشاوره) ۳۷

بخش پنجم (استراتژی ما) ۴۳

بخش ششم (پاسخ ما) ۴۹

بخش هفتم (برنامه علمی) ۸۹

بخش هشتم (اجرا و سنجش پیشرفت) ۱۰۱

جمع بندی ۱۰۹

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

اطمینـان از امنیـت آنلایـن اسـترالیایی‌ها مسـئولیتی مشـترک اسـت ـ همـه بایـد نقشـی داشـته باشـند. ایـن اسـتراتژی برنامـه مـا بـرای محافظت آنلایـن اسـترالیایی‌ها را تنظیـم می‌کنـد.

جهـان هرگـز ایـن چنیـن بـه هـم پیوسـته نبـوده اسـت؛ وابسـتگی مـا بـه اینترنـت بـرای رفـاه و تعییـن سـبک زندگـی نیـز هرگـز تـا ایـن حـد نبـوده اسـت. واکنـش اسـترالیا بـه بیمـاری همه‌گیـر کووید ـ ۱۹ اهمیـت ارتبـاط امـن آنلایـن را نشـان داد. ایـن پاندمیـک همچنیـن مقاومـت و عـزم اسـترالیایی‌ها بـرای همـکاری مشـترک در راسـتای یـک هـدف را نشـان می‌دهـد. مشـارکت ملـی میـان دولـت، کسـب‌وکارها و جامعـه نیـز بایـد در جهـت اطمینـان از امنیـت سـایبری اسـترالیا بـه کار گرفتـه شـود.

اسـترالیایی‌ها بـه درسـتی از فرصت‌هـای دنیـای دیجیتـال اسـتفاده می‌کننـد. بـا ایـن حـال، بـا افزایـش فرصت‌هـا، تهدیـدات سـایبری نیـز افزایـش می‌یابـد. فعـالان مجهـز و تحـت حمایـت پایـدار دولـت، زیرسـاخت‌های مهـم را هـدف قـرار داده و مالکیـت معنـوی مـا را می‌دزدنـد.

مجرمـان سـایبری نیـز صدمـات زیـادی وارد می‌کننـد، از هـر نقطـه دنیـا بـه سیسـتم نفـوذ می‌کننـد، پـول، هویـت و اطلاعـات شـهروندان بی‌خبـر

استرالیایی را می‌دزدند. آن‌ها از بحران کرونا برای هدف قرار دادن خانواده‌ها و کسب‌وکارها، از جمله امکانات تحقیقاتی سلامت و درمان، سوءاستفاده می‌کنند. آن‌ها در وب تاریک (دارک وب) مخفی شده‌اند تا مواد مخدر و سایر کالاهای غیرقانونی را قاچاق کنند و تصاویر نفرت‌انگیز از کودک آزاری را به اشتراک بگذارند. پاسخ ما باید جسورانه باشد تا به طور جدی این تهدید را برطرف کنیم.

این استراتژی موقعیت ما برای پاسخگویی به این تهدیدات در حال تحول را تعیین می‌کند. چشم‌انداز ما دنیای آنلاین امن‌تر برای استرالیایی‌ها، کسب‌وکار آن‌ها و خدمات ضروری است که همه ما به آن وابسته هستیم. ما همراه یکدیگر با اقدامات مکمل از سوی ادارات، کسب‌وکارها و جامعه به این هدف خواهیم رسید. دولت ائتلاف از طریق این استراتژی۱/۶۷میلیارد دلار در طول ده سال برای امنیت سایبری سرمایه‌گذاری خواهد کرد. این بزرگ‌ترین تعهد مالی برای تأمین امنیت سایبری است. ما توانایی‌های جدید دولت را توسعه خواهیم داد، در صنعت ایجاد انگیزه خواهیم کرد تا از خود و مشتریانشان محافظت کنند، نسبت به اقتصاد دیجیتال جلب اعتماد کرده و از امنیت آنلاین جامعه حمایت می‌کنیم.

این استراتژی به نفع همه استرالیایی‌ها خواهد بود. خانواده‌ها و کسب‌وکارها به مشاوره و راهنمایی قابل اعتماد در زمنیه امنیت سایبری دسترسی خواهند داشت. دولت ائتلاف به منظور مقابله با مجرمان سایبری، ارتقای اشتراک اطلاعات با صنعت در زمینه تهدیدات و حمایت از ابتکارات جدید برای رشد نیروی کار سایبری ماهر، ظرفیت اجرای قانون را افزایش خواهد داد. دولت در همکاری با مالکان زیرساخت‌های

حیاتی، حفاظت از سیستم‌های حیاتی که همه استرالیایی‌ها به آن وابسته هستند را تقویت می‌کند.

اما کار ما برای اطمینان از امنیت سایبری استرالیا در اینجا به پایان نمی‌رسد. این استراتژی این نکته را در نظر گرفته است که امنیت سایبری مؤثر به تلاش مستمر همه ما نیاز دارد. دولت ائتلاف به همکاری با صنعت، مردم و ادارات در ایالت‌ها و مناطق مختلف ادامه خواهد داد تا اطمینان حاصل شود که اقدامات مبتنی بر این استراتژی از بهبود وضعیت اقتصادی از طریق انعطاف‌پذیری قدرتمند سایبری پشتیبانی می‌کنند.

این استراتژی با کمک و اطلاعات بسیاری از استرالیایی‌ها که در مشاوره عمومی شرکت کردند، تهیه شده است. من می‌خواهم از آن‌ها و همچنین هیئت مشاوره صنعت به ریاست اندی پن، مدیر ارشد اجرایی تلسترا، به خاطر تعهد، اشتیاق و مشاوره دقیق، که برای تدوین این استراتژی نقشی اساسی داشته است، تشکر کنم.

پیتر داتون، نماینده مجلس

وزیر کشور

۶ آگوست ۲۰۲۰

بخش اول

بخش اول

استراتژی امنیت سایبری ۲۰۲۰استرالیا: دریک نگاه

چشم‌انداز

دنیای آنلاین امن‌تری برای استرالیایی‌ها، کسب‌وکار آن‌ها و خدمات ضروری که همه ما به آن وابسته هستیم.

رویکرد

این چشم‌انداز از طریق اقدامات مکمل از سوی ادارات، کسب‌وکارها و جامعه محقق خواهد شد.

تهدیدهای سایبری به سرعت در حال تکامل هستند:

- تهدیدات امنیت سایبری در حال افزایش است. کشورها و فعالان و خلاف‌کاران تحت حمایت آن‌ها با دسترسی به اطلاعات حساس و برای سود مالی از استرالیایی‌ها بهره‌برداری می‌کنند.
- مجرمان از وب تاریک برای خریدوفروش هویت‌های مسروقه، کالاهای غیرقانونی و اطلاعات برای استثمار کودکان استفاده می‌کنند و همچنین مرتکب جرایم دیگر می‌شوند.
- فناوری‌های رمزنگاری و ناشناسی هویت به مجرمان، تروریست‌ها و دیگران اجازه می‌دهد تا هویت و فعالیت‌های

خود را از دید سازمان‌های اجرای قانون مخفی کنند.

• مجرمان سایبری قصد دارند از این واقعیت که استرالیایی‌ها بیش از هر زمان دیگری به فضای سایبری متصل هستند، سوءاستفاده کنند.

مبنای استوار

این استراتژی مبتنی بر استراتژی امنیت سایبری سال ۲۰۱۶ است که ۲۳۰ میلیون دلار برای پیشبرد و محافظت منافع آنلاین استرالیا سرمایه‌گذاری کرد.

نکات مهم

این استراتژی برای دستیابی به چشم‌انداز پیش رو طی ۱/۶۷سال ۱.میلیارد دلار سرمایه‌گذاری خواهد کرد، که شامل موارد زیر می شود:

• محافظت و دفاع فعالانه از زیرساخت‌های حیاتی که همه استرالیایی‌ها به آن‌ها وابسته هستند، و شامل الزامات امنیت سایبری برای مالکان و اپراتورها می‌شود؛

• روش‌های جدید برای تحقیق و توقف جرایم سایبری، که شامل وب تاریک (دارک وب) می‌شود؛

• دفاع قوی‌تر از شبکه‌ها و داده‌های دولتی؛

• همکاری بیشتر برای ایجاد مهارت‌های سایبری در استرالیا؛

• افزایش سطح آگاهی موقعیتی و توسعه اشتراک اطلاعات از تهدیدات پیش رو؛

• مشارکت قوی‌تر با صنعت از طریق برنامه مشترک مرکز امنیت سایبری؛

- مشاوره به شرکت‌های کوچک و متوسط برای افزایش انعطاف‌پذیری سایبری خود؛
- ارائه راهنمایی شفاف برای کسب‌وکارها و مصرف‌کنندگان در مورد ایمن‌سازی دستگاه‌های اینترنت اشیا؛
- پاسخ‌گویی شبانه‌روزی خط تلفن مشاوره امنیت سایبری به شرکت‌های کوچک و متوسط و خانواده‌ها؛
- ارتقای آگاهی جامعه در مورد تهدیدات امنیت سایبری.

بخش دوم

بخش دوم

بررسی اجمالی

۱) چشم‌انداز دولت استرالیا، ایجاد جهان آنلاین امن‌تر برای استرالیایی‌ها، کسب‌وکار آن‌ها و خدمات ضروری است که همه ما به آن وابسته هستیم.

۲) مقیاس و پیچیدگی تهدیدات سایبری همچنان در حال افزایش است. استرالیایی‌ها به طور فزاینده‌ای به اینترنت و دستگاه‌های متصل به اینترنت که روزانه استفاده می‌کنیم، متکی هستند. اقتصاد دیجیتال آینده اقتصاد استرالیا را در دست خواهد داشت. تجربه ما با بیماری همه‌گیر کووید ـ ۱۹ و برجسته شدن میزان تعامل و کار آنلاین استرالیایی‌ها، اعتماد به اینترنت برای مراقبت‌های بهداشتی، کار در خانه، آموزش، سرگرمی و خرید آنلاین، این موضوع را بهتر نشان داد. اکنون بیش از هر زمان دیگری محافظت از استرالیایی‌ها در فضای آنلاین در برابر کسانی که به ما آسیب می‌رسانند، از اهمیت بیشتری برخوردار است.

۳) تجربه کووید ـ ۱۹ در استرالیا درس‌های دیگری نیز به همراه داشت. همان طور که ما ـ ادارات، کسب‌وکارها و جامعه ـ برای مبارزه با بیماری همه‌گیر به یکدیگر اعتماد کردیم، امنیت سایبری

نیز به ما وابسته است، و هرکدام باید نقش خود را بازی کنیم. همه ما ـ ادارات، کسب‌وکارها و جامعه ـ در ایجاد فضای امن‌تر سایبری در استرالیا نقشی داریم.

۴) امنیت سایبری به خانواده‌ها و کسب‌وکارها اجازه می‌دهد تا در اقتصاد دیجیتالی پیشرفت کنند، همان طور که حصارهای دور استخر آرامش خاطری را برای خانواده‌ها فراهم می‌کنند. امنیت سایبری باید بخشی اساسی و یکپارچه در زندگی روزمره باشد، به طوری که استرالیایی‌ها را قادر سازد با امنیت و اطمینان از مزایای اینترنت بهره‌مند شوند.

۵) دولت استرالیا از طریق این استراتژی، و با پشتیبانی از انعطاف‌پذیری سایبری کسب‌وکارها، به اشتراک گذاشتن اطلاعات در زمینه تهدیدهای سایبری، تعریف انتظارات روشن از نقش‌ها و تقویت مشارکت، در دنیای آنلاین اعتمادسازی می‌کند.

۶) دولت استرالیا با صنعت همکاری خواهد کرد تا از مهم‌ترین سیستم‌های ما در برابر تهدیدات پیچیده محافظت کند. به سازمان‌های اجرای قانون، توانایی بیشتری در محافظت از فضای آنلاین استرالیایی‌ها داده خواهد شد، دقیقاً مانند آنچه در دنیای فیزیکی وجود دارد. به این ترتیب، آن‌ها فعالیت‌های خلاف‌کارانه را در وب تاریک مورد هدف قرار خواهند داد. دولت استرالیا با استفاده از توانایی‌های حمله سایبری علیه مجرمان فرامرزی، مطابق با قوانین بین‌المللی، با فعالیت‌های غیرقانونی مقابله خواهد کرد. دولت استرالیا به تقویت دفاعی شبکه‌های خود در برابر تهدیدهای کشورهای پیشرفته و فعالان تحت حمایت ادارات ادامه خواهد داد.

۷) کسب‌وکارها باید به عنوان بخشی از اقتصاد دیجیتالی قدرتمند و شکوفا، هر جا که امکان دارد، محصولات و خدمات ایمن تولید کنند. مقررات داوطلبانه انتظارات امنیتی دولت استرالیا برای دستگاه‌های متصل به اینترنت که استرالیایی‌ها هر روز استفاده می‌کنند را تعیین می‌کند. دولت استرالیا با صنعت همکاری خواهد کرد تا تعهدات مربوط به امنیت سایبری صنعت را با اصلاحاتی قانونی در آینده مورد بررسی قرار دهد.
۸) دولت و کسب‌وکارهای بزرگ به شرکت‌های کوچک و متوسط کمک می‌کنند تا آگاهی و توانایی خود را در زمینه امنیت سایبری افزایش دهند. دولت استرالیا با کسب‌وکارهای بزرگ و ارائه دهندگان خدمات همکاری خواهد کرد تا به عنوان بخشی از «بسته‌های خدمات ایمن» (مانند مسدود کردن تهدیدها، آنتی ویروس و آموزش جهت آگاهی از امنیت سایبری) اطلاعات و ابزارهای امنیت سایبری را در اختیار شرکت‌های کوچک و متوسط قرار دهد. ادغام محصولات امنیت سایبری در سایر خدمات ارائه شده به محافظت از شرکت‌های کوچک و متوسط در مقیاس مناسب کمک خواهد کرد و تصدیق می‌کند که بسیاری از کسب‌وکارها نمی‌توانند از کارمندان اختصاصی حوزه امنیت سایبری استفاده کنند. ادارات برای شناسایی و رفع آسیب‌پذیری‌های فوری دست در دست هم با صاحبان زیرساخت‌های کلیدی همکاری‌های نزدیک خواهند داشت. «برنامه افزایش نیروی کار ملی امنیت سایبری» نیروی کار سایبری ماهر را توسعه می‌دهد که می‌تواند تهدیدات و چالش‌های جدید را برطرف کرده و مزایای تحولات

آنلاین اقتصاد جهانی را به حداکثر برساند.

۹) ادارات و صنعت نمی‌توانند همه ریسک‌های مربوط به امنیت سایبری را برطرف کنند ـ افراد نیز باید برای محافظت از خود گام‌هایی را بردارند. دولت استرالیا تلاش‌های خود را برای افزایش آگاهی از تهدیدات امنیت سایبری و توانمندسازی جامعه در رفتارهای آنلاین ایمن گسترش خواهد داد. دولت استرالیا برنامه‌ای برای آموزش آنلاین امنیت سایبری اختصاص داده است، مشاوره شبانه‌روزی تلفنی برای امنیت سایبری کسب‌وکارهای کوچک و متوسط و خانواده‌ها ارائه داده و بودجه جهت خدمات پشتیبانی از قربانیان را افزایش می‌دهد.

۱۰) این اقدامات امنیت اینترنت را برای همه استرالیایی‌ها افزایش خواهد داد. با اطمینان از اینکه دولت استرالیا می‌تواند با پیچیده‌ترین تهدیدات و رفتارهای غیرقانونی مقابله کند، کسب‌وکارها و جامعه نیز در معرض خطرات کمتری قرار خواهند گرفت و آسیب کمتری را متحمل می‌شوند. استرالیایی‌ها اطمینان بیشتری خواهند داشت که از سیستم‌های ضروری محافظت می‌شود. تجهیز صاحبان کسب‌وکارهای کوچک و جامعه به اطلاعات و ابزاری که برای محافظت از خود نیاز دارند، آن‌ها را تشویق خواهد کرد تا بیشتر از محصولات ایمن سایبری و تصمیم‌گیری‌های هوشمند سایبری استفاده کنند.

مبنای استوار

استراتژی امنیت سایبری سال ۲۰۱۶ برنامه دولت استرالیا برای پاسخ‌گویی به چالش‌های دوگانه عصر دیجیتال ـ پیشرفت و محافظت از

منافع آنلاین استرالیا ـ را ارائه کرده است. دولت استرالیا با سرمایه‌گذاری ۲۳۰ میلیون دلاری خود از استراتژی سال ۲۰۱۶ حمایت کرد.

بازخورد از کسب‌وکارها و جامعه نشان داد که استراتژی سال ۲۰۱۶ بنیان امنیت سایبری استرالیا را تقویت می‌کند، سرمایه‌گذاری بخش خصوصی را در صنعت امنیت سایبری داخلی تشویق می‌کند و استرالیا را پیشتاز امنیت سایبری منطقه‌ای معرفی می‌کند. دستاوردهای اصلی عبارتند از:

- افتتاح مرکز امنیت سایبری استرالیا؛[1]
- ایجاد مراکز مشترک امنیت سایبری[2] برای همکاری ادارات ایالت‌ها و مناطق مختلف و صنعت؛
- افزایش مهارت‌های سایبری و سرمایه‌گذاری‌های آموزشی؛
- نظارت شبانه‌روزی؛
- استخدام سفیر امور سایبری؛
- ایجاد شبکه رشد امنیت سایبری استرالیا[3] و مرکز تحقیقات مشارکتی در حوزه امنیت سایبری.

این استراتژی مبتنی بر اقداماتی است که از سال ۲۰۱۶ آغاز شد، از جمله مراکز مشترک امنیت سایبری و مرکز امنیت سایبری استرالیا.

«پالو آلتو نتورکز»، شرکت امنیت سایبری چند ملیتی آمریکایی: «استراتژی اختصاصی امنیت سایبری ۲۰۱۶ استرالیا با ارائه مجموعه‌ای از فعالیت‌های بخش‌های دولتی و خصوصی و واکنش به مسائل امنیت سایبری و چالش جرایم اینترنتی، کاتالیزوری برای تغییر بوده است.»

1. ACSC
2. JCSCs
3. AustCyber

بخش سوم

بخش سوم

فضـای تهدید

«سـاپین سـایبر»، شـرکت امنیـت سـایبری اسـترالیایی: «شـدت پیامدهـای حمـلات سـایبری بـه دلیـل اهمیـت بیشـتر سیسـتم‌های اطلاعاتـی در تجـارت و جامعـه، در حـال افزایـش اسـت.»

۱۱) امنیـت سـایبری مرکـز ثقـل انتقـال بـه جامعـه‌ای دیجیتـال اسـت. امنیـت سـایبری سـتون کلیـدی تأمیـن اقتصـاد دیجیتـال مطمئـن و قابـل اعتمـاد اسـت، بـه همـه مصرف‌کننـدگان اطمینـان می‌بخشـد و بـه کسـب‌وکارها امـکان رونـق و پیشـرفت می‌دهـد. جـذب سـریع و گسـترده فنـاوری دیجیتـال در خانواده‌هـا و کسـب‌وکارها بـه دنبـال بیمـاری همه‌گیـر کووید ـ ۱۹، نشـان‌دهنده اهمیـت فنـاوری دیجیتـال در اقتصـاد اسـت. میلیون‌هـا اسـترالیایی از خانـه بـا اپلیکیشـن‌های مختلـف کار می‌کننـد، و از خدمـات دیجیتالـی ضـروری ماننـد «تلهلث»[1] بهره‌منـد هسـتند. بسـیاری از کسـب‌وکارهای سـنتی بـرای نخسـتین بـار آنلایـن شـده‌اند. بـرای مثـال، درآمـد سـالانه صنعـت خریـد آنلایـن در مـارس ۲۰۲۰ نسـبت بـه مـدت مشـابه سـال قبـل ۲۱/۸ درصـد افزایـش داشـته اسـت.[2]

۱۲) بـرای اینکـه مزایـای تحـول دیجیتـال بـه حداکثـر برسـد،

1.Telehealth

۲. بانک ملی استرالیا (۲۰۲۰)، فهرست فروش خرده فروشی آنلاین در ماه مارس به این آدرس قابل دسترس است:
https://business.nab.com.au/wp-content/ uploads/05/2020/NAB-Online-Retail-Sales-Index-MAR20.pdf

استرالیایی‌ها باید تهدیدات همراه آن را نیز درک کرده و مرتفع کنند. فعالیت‌های مخرب سایبری یکی از مهم‌ترین تهدیدات پیش روی استرالیایی‌ها است. بین ۱ جولای ۲۰۱۹ و ۳۰ ژوئن ۲۰۲۰، مرکز امنیت سایبری استرالیا به ۲/۲۶۶ حادثه امنیت سایبری واکنش نشان داد و روزانه تقریبا ۶ حادثه سایبری را اقتصاد تا ۲۹ میلیارد دلار در سال، یا ۱/۹٪ از تولید ناخالص داخلی استرالیا، هزینه در بر داشته باشد.[1] به علاوه، تخمین زده می‌شود که یک وقفه چهار هفته‌ای در زیرساخت‌های دیجیتال ناشی از یک حمله سایبری می‌تواند ۳۰ میلیارد دلار (۱/۵٪ از تولید ناخالص داخلی استرالیا) هزینه در بر داشته باشد و به حدود ۱۶۳ هزار شغل آسیب وارد کند.[2]

۱۳) بیماری همه‌گیر کووید ـ ۱۹ماهیت متغیر تهدیدات سایبری را برجسته کرد. مجرمان سایبری فرصت‌طلب به سرعت روش‌های خود را با تعداد بیشتر شهروندان مشغول کار، مطالعه و ارتباط آنلاین تطبیق می‌دهند. بین ۱۰ تا ۲۶ مارس ۲۰۲۰، مرکز امنیت سایبری استرالیا بیش از ۴۵ گزارش مربوط به جرایم اینترنتی و حوادث امنیت سایبری با مضمون پاندمیک و کمیسیون رقابت و مصرف‌کننده استرالیا[3] نیز بیش از ۱۰۰ گزارش کلاهبرداری با موضوع کووید ـ ۱۹ دریافت کردند. این کمپین‌ها برای توزیع نرم‌افزار مخرب (بدافزار) یا برداشت اطلاعات شخصی و مالی از شهروندان بی‌خبر استرالیایی طراحی شده‌اند.

1. Frost & Sullivan (2018), Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World
2. https://www.austcyber.com/resource/digitaltrustreport2020
3. ACCC

حادثه سایبری

یک رویداد منفرد یا یک سری رویدادها که یکپارچگی، دسترسی یا محرمانه بودن اطلاعات دیجیتالی را تهدید کند.

«ای یو کلود»، ارائه دهنده خدمات زیرساخت به عنوان سرویس استرالیایی: "حملات ارزان قیمت و با فناوری سطح پایین مانند باج افزار، فیشینگ و بدافزار همچنان افزایش خواهد یافت و نیاز است تا دولت برای حمایت از مشاغل کوچک تا متوسط و شرکت‌های بزرگ استرالیا در مقابل مجرمان اینترنتی تأکید ویژه‌ای داشته باشد.»

خلافکاران سایبری

۱۴) طیف وسیعی از گروه‌های مختلف استرالیایی‌ها را مورد هدف قرار می‌دهند، که هر کدام قصد و پیچیدگی متفاوتی دارند.

- **کشورها و فعالان تحت حمایت آن‌ها** قصد دارند تا با دسترسی به اطلاعات اقتصادی، سیاسی، حقوقی، دفاعی و امنیتی، به منافع خود دست یابند. کشورها و فعالان تحت حمایت آن‌ها همچنین ممکن است در زمان صلح یا درگیری تأثیرات مخربی را علیه اهداف خود به جای بگذارند. آن‌ها بیشتر دشمنانی پیچیده، دارای منابع کافی و صبور هستند که اقداماتشان

می‌تواند بر امنیت ملی و رونق اقتصادی استرالیا تأثیر بگذارد.

• **مجرمان با انگیزه مالی** برای دستیابی به منافع مالی وارد سیستم‌ها شده و از اطلاعات سوءاستفاده می‌کنند، که تهدیدی اساسی برای منافع اقتصادی استرالیا و منطقه است. سندیکاهای جرایم سایبری فراملیتی که ابزارها و تکنیک‌های پیچیده سایبری را تولید می‌کنند، به اشتراک می گذارند، به فروش می‌رسانند و استفاده می‌کنند، مورد توجه ویژه قرار می‌گیرند. مجرمان همچنین از وب تاریک برای خریدوفروش هویت‌های مسروقه و کالاهای غیرقانونی، استثمار کودکان و همچنین ارتکاب جرایم دیگر استفاده می‌کنند.

• **گروه‌ها و افراد با انگیزه جلب توجه** در درجه نخست سعی دارند توجه افراد را به مسئله‌ای که وجود دارد جلب کنند. آن‌ها عموماً از توانایی و پیچیدگی کمتری برخوردار هستند، اما همچنان قادر هستند در صنعت و ادارات اخلال ایجاد کنند.

• **گروه‌های تروریستی و افراط‌گرایان** در استفاده از اینترنت برای برقراری ارتباط و جلب توجه مهارت دارند، اما به طور کلی از تکنیک‌ها و قابلیت‌های بسیار ابتدایی سایبری مانند فعالیت‌های حمله انکار سرویس، ربودن حساب‌های شبکه‌های اجتماعی و مخدوش کردن وب سایت‌ها استفاده می‌کنند. این گروه‌ها در حال حاضر تهدید سایبری نسبتاً کمی دارند.

۱۵) کشورهای بسیار پیچیده و بازیگران تحت حمایت آن‌ها همچنان ادارات و تأمین‌کنندگان زیرساخت‌های مهم را هدف قرار می‌دهند. دولت استرالیا یا نهادهای دولتی ایالتی و منطقه‌ای در

۳۵/۴٪ از حوادث سایبری منتهی به ۳۰ ژوئن ۲۰۲۰ مورد هدف قرار گرفته بودند (نمودار ۱ را ببینید). حدود ۳۵٪ از حملات سایبری، تأمین‌کنندگان زیرساخت‌های اساسی را تحت تأثیر قرار داد که خدمات اساسی از جمله مراقبت‌های بهداشتی، آموزشی، بانکی، آب، ارتباطات، حمل‌ونقل و انرژی را ارائه می‌دهند. یک حمله سایبری موفق علیه یکی از این خدمات می‌تواند پیامدهای قابل توجهی برای اقتصاد و زندگی استرالیا همراه داشته باشد. این گونه حمله در خارج از کشور رخ می‌دهد، همان طور که در سال ۲۰۱۵ حمله به تأسیسات برق اوکراین، در سال ۲۰۱۷ حملات «تریتون» به تأسیسات پتروشیمی سعودی‌ها و حملات «نات پتیا» و «واناکرای» در سال ۲۰۱۷ به خدمات مالی، حمل‌ونقل و بهداشت و درمان سراسر جهان رخ داد.

۱۶) در سال ۲۰۱۹، از هر سه بزرگسال استرالیایی یک نفر تحت تأثیر جرایم سایبری قرار گرفت.[1] به طور متوسط، ابزار «ریپورتر سایبر» مرکز امنیت سایبری استرالیا هر ۱۰ دقیقه یک گزارش از جرایم اینترنتی دریافت می‌کند. موانع پیش روی ورود به جرایم سایبری بسیار اندک هستند. بازارهای آنلاین زیرزمینی خدمات جرایم اینترنتی یا دسترسی به ابزارهای پیشرفته هک را ارائه می‌دهند که زمانی تنها در دسترس ادارات بود. مجرمان سایبری با حداقل تخصص فنی می‌توانند ابزارها و خدمات غیرقانونی را برای تولید جریان درآمد جایگزین خریداری کنند، پول‌شویی کنند یا از طرف دشمنان پیچیده‌تر به شبکه‌ها نفوذ کنند.

1. NortonLifeLock (2019 ,(2020 Cyber Safety Insights Report Global Results, available at .now.symassets.com/content/dam/norton/campaign/ NortonReport/2019/2020_ NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf?

فعالیت مخرب علیه شبکه های استرالیایی در سال ۲۰۲۰

تاریخ ۱۹ژوئن ۲۰۲۰، نخست وزیر اعلام کرد که عملیات پیچیده سایبری دولتی، سازمان‌های استرالیایی را مورد هدف قرار داده اند. این فعالیت طیف وسیعی از بخش‌ها در سازمان های استرالیایی، از جمله تمام سطوح دولتی، صنعتی، سازمان‌های سیاسی، ارائه دهندگان خدمات آموزش، مراقبت‌های بهداشتی و ضروری و دیگر زیر ساخت‌های حیاتی را مورد هدف قرار داده بود.

دولت استرالیا میداند که این اقدام به دلیل مقیاس و ماهیت اهداف و مهارت نفوذ آن، یک فعالیت پیچیده سایبری دولتی بوده است. مرکز امنیت سایبری استرالیا و وزارت کشور،مشاوره فنی دقیق تری را برای راهنمایی کسب و کارها و سازمان‌های استرالیایی جهت محافظت از خود منتشر کردند. این مشاوره در سایت cyber.gov.auدر دسترس است.

مجرمان اینترنتی با سوءاستفاده از بحران کووید-۱۹ کمپین های گسترده فیشینگ، ایمیل و پیامک را با موضوع کووید-۱۹ به را انداخته اند. این کمپین ها با هدف توزیع بدافزار یا جمع آوری اطلاعات شخصی از شهروندان بی خبر استرالیا هدایت می شود.

برای محافظت از استرالیایی‌ها، اداره سیگنال های دیجیتالی استرالیا از قابلیت‌های حمله سایبری علیه مجرمان خارجی از طریق کمپین های فیشینگ با مضمون کووید-۱۹ شکل گرفت و با موفقیت زیر ساخت های آن ها را غیر فعال کرد و دسترسی آن ها به اطلاعات سرقت شده را نیر مسدود کرد.

سازمان امنیت سایبری استرالیا همچنین با ارائه دهندگان عمده ارتباطات راه دور استرالیا و شرکت‌های مرورگر وب «گوگل» و مخرب در مرورگر وب و مسدود کردن آن ها برای کاربران تلفن بوده است. این واکنش نشان داد که چگونه همکاری نزدیک بین دولت و صنعت می تواند استرالیایی ها را از فعالیت های مخرب سایبری محافظت کند.

فعالیت سایبری مخرب در وب تاریک

وب تاریک بخشی از اینترنت است که به کاربران آن اجازه می دهد ناشناس بمانند. به راحتی قابل دسترسی نیست. وب تاریک فعالیت های غیر قانونی مانند سوءاستفاده جنسی کودکان، سرقت هویت، قاچاق مواد مخدر وسلاح گرم و برنامه ریزی برای حملات تروریستی را تسهیل می‌کند.

استفاده از فناوری های هویت ناشناس،ارتکاب جرایم سنگین و گسترده در حوزه های قضایی را آسان کرده است. همچنین، به مجرمان و سایر فعالان اجازه می دهد خارج از دید نیروهای قانون گذار فعالیت کنند. اگر سازمان های اجرای قانون ما بخواهند در کاهش جرایم سایبری موفق باقی بمانند، توانایی آن ها نیز در مقابله با حجم و ناشناس ماندن هویت فعالان در وب تاریک و فناوری های رمزنگاری شده باید افزایش یابد. دولت استرالیا به عنوان بخشی از این استراتژی، تلاش خواهد کرد تا اطمینان حاصل کند که نیروهای قانون گذار از قدرت و توانایی لازم برای بررسی و جلوگیری از جرایم اینترنتی، از جمله در وب تاریک برخوردار هستند.

فعالیت مخرب علیه شبکه‌های استرالیایی در سال ۲۰۲۰

تاریخ ۱۹ ژوئن ۲۰۲۰، نخ ست وزیر اعلام کرد که عملیات پیچیده سایبری دولتی، سازمان‌های ا سترالیایی را مورد هدف قرار داده‌اند. این فعالیت طیف وسیعی از بخش‌ها در سازمان‌های استرالیایی، از جمله تمام سطوح دولتی، صنعتی، سازمان‌های سیاسی، ارائه دهندگان خدمات آموزش، مراقبت‌های بهداشتی و ضروری و دیگر زیرساخت‌های حیاتی را مورد هدف قرار داده بود.

دولت ا سترالیا می‌داند که این اقدام به دلیل مقیاس و ماهیت اهداف و مهارت نفوذ آن، یک فعالیت پیچیده سایبری دولتی بوده است. مرکز امنیت سایبری استرالیا و وزارت کشور، مشاوره فنی دقیق‌تری را برای راهنمایی کسب‌وکارها و سازمان‌های استرالیایی جهت محافظت از خود منتشر کردند. این مشاوره در سایت cyber.gov.au در دسترس است.

مجرمان اینترنتی با سوءاستفاده از بحران کووید ـ ۱۹ کمپین‌های گسترده فیشینگ ایمیل و پیامک را با موضوع کووید ـ ۱۹ به راه انداخته‌اند. این کمپین‌ها با هدف توزیع بدافزار یا جمع‌آوری اطلاعات شخصی از شهروندان بی‌خبر استرالیایی هدایت می‌شود.

برای محافظت از ا سترالیایی‌ها، اداره سیگنال‌های دیجیتالی ا سترالیا [1] از قابلیت‌های حمله سایبری خود علیه مجرمان سایبری خارجی ا ستفاده کرد که خانواده‌ها و م شاغل ا سترالیایی را هدف قرار داده بودند. این حملات سایبری علیه مجرمان خارجی از طریق کمپین‌های فیشینگ با مضمون کووید ـ ۱۹ شکل گرفت و با موفقیت زیرساخت‌های آن‌ها را غیرفعال کرد و دسترسی آن‌ها به اطلاعات سرقت شده را نیز مسدود کرد.

سازمان امنیت سایبری ا سترالیا همچنین با ارائه دهندگان عمده ارتباطات راه دور ا سترالیا و شرکت‌های مرورگر وب «گوگل» و «مایکروسافت» همکاری نزدیک داشت تا مجرمان خارجی را مورد هدف قرار دهد. این اقدامات شامل نشان‌گذاری وب سایت‌های مخرب در مرورگر وب و مسدود کردن آن‌ها برای کاربران تلفن بوده است. این واکنش نشان داد که چگونه همکاری نزدیک بین دولت و صنعت می‌تواند استرالیایی‌ها را از فعالیت‌های مخرب سایبری محافظت کند.

فعالیت سایبری مخرب در وب تاریک

وب تاریک بخ شی از اینترنت ا ست که به کاربران آن اجازه می‌دهد نا شناس بمانند. به راحتی قابل د ستر سی نی ست. وب تاریک فعالیت‌های غیرقانونی مانند سوءاستفاده جنسی کودکان، سرقت هویت، قاچاق مواد مخدر و سلاح گرم و برنامه‌ریزی برای حملات تروریستی را تسهیل می‌کند.

ا ستفاده از فناوری‌های هویت نا شناس، ارتکاب جرایم سنگین و گ سترده در حوزه‌های ق ضایی را آ سان کرده ا ست. همچنین، به مجرمان و سایر فعالان اجازه می‌دهد خارج از دید نیروهای قانونگذار فعالیت کنند. اگر سازمان‌های اجرای قانون ما بخواهند در کاهش جرایم سایبری موفق باقی بمانند، تولنایی آن‌ها نیز در مقابله با حجم و نا شناس ملندن هویت فعالان در وب تاریک و فناوری‌های رمزنگاری شده باید افزایش یابد. دولت ا سترالیا، به عنوان بخ شی از این ا ستراتژی، تلاش خواهد کرد تا اطمینان حا صل کند که نیروهای قانونگذار از قدرت و تولنایی لازم برای برر سی و جلوگیری از جرایم اینترنتی، از جمله در وب تاریک برخوردار هستند.

1. ASD

بخش چهارم

بخش چهارم

مشاوره

۱۷) تاریخ ۶ سپتامبر ۲۰۱۹، دولت استرالیا مقاله‌ای را تحت عنوان «فراخوان دیدگاه» منتشر کرد؛ به این طریق، همه شهروندان استرالیایی فرصتی پیدا کردند تا در توسعه این استراتژی نظری دهند.

۱۸) دولت استرالیا ۲۱۵ پیشنهاد از طرف افراد و سازمان‌ها دریافت کرد که ۱۵۶ مورد به آدرس homeaffairs.gov.au/cybersecurity موجود است.

۱۹) دولت استرالیا همچنین با بیش از ۱۴۰۰ نفر از سراسر کشور در مشاوره‌های حضوری، از جمله کارگاه‌های آموزشی، میزگردها و جلسات دوجانبه دیدار کرد. همچنین گردهمایی‌های اختصاصی با حضور نمایندگان شرکت‌های بزرگ فناوری، دانشگاهی، آژانس‌های ایالتی و منطقه‌ای، ادارات محلی و صنایع دفاعی نیز برگزار شد.

۲۰) موضوعات کلیدی زیر در طی مراحل مشاوره مطرح شد:

- فضای تهدید وخیم‌تر شده است؛
- نقش‌ها و مسئولیت‌ها نیاز به شفاف‌سازی دارد؛
- مشارکت دولت و صنعت باید تقویت شود؛
- توسعه اشتراک دو طرفه اطلاعات ضروری است؛

• استانداردها و مقررات برای درک درست اصول ضروری است؛
جرایم سایبری از توانایی ما در پاسخگویی پیشی گرفته است؛
• بسیاری از تهدیدها را می‌توان در مقیاس بزرگ بررسی کرد؛
• رفتار انسان تقریباً همیشه بخشی از مشکل است؛
• استرالیا به متخصصان معتبر و ماهر حوزه امنیت سایبری نیاز دارد؛
•کسب‌وکارهای کوچک به ویژه آسیب‌پذیر هستند؛
• استرالیا باید به خصوص برای حادثه‌ای در مقیاس ملی آمادگی بیشتری داشته باشد؛
• فرصت‌های اقتصادی برای استرالیا وجود دارد؛
• شبکه اقدام مصرف‌کننده و ارتباطات استرالیا.

شبکه اقدامات ارتباطی مصرف‌کننده استرالیا: "کمیسیون رقابت و مصرف‌کننده استرالیا نگران تأثیر نامتناسبی است که کلاهبرداری و سایر جرایم اینترنتی بر مصرف‌کنندگان آسیب‌پذیر بر جای می‌گذارد؛ مانند افرادی که در استفاده از اینترنت مهارت لازم را ندارند، افراد مسن و افرادی که آشنایی کمتری با زبان انگلیسی دارند."

شبکه خدمات چند ملیتی «اکسنچر»: "همان طور که در مقوله بهداشت عمومی جمعیت‌های آسیب‌پذیری وجود دارد، ما همچنین شاهد اهداف آسیب‌پذیر در حوزه حملات امنیت سایبری نیز هستیم."

شرکت استرالیایی ارتباطات از راه دور «اپتوس»: "دولت باید مسئول اطمینان از اپراتورهای ارتباط از راه دور باشد، و اپراتورهای خدمات حیاتی نیز اقدامات لازم را برای حفاظت از شبکه‌ها و خدمات انجام می‌دهند."

هیئت مشاوره صنعت ما

۲۱) وزیر کشور همچنین هیئت مشاوره صنعت را برای ارائه مشاوره استراتژیک جهت حمایت از توسعه استراتژی امنیت سایبری ۲۰۲۰ استرالیا ایجاد کرد. اعضای هیئت:

- آقای اندرو پن، مدیرعامل شرکت «تلسترا»
- خانم کرستجن نیلسن، وزیر امنیت داخلی پیشین آمریکا
- آقای رابرت منسفیلد، مدیر «ووکس گروپ»
- خانم رابین دنهلم، مدیر شرکت «تسلا»
- آقای کریس دیبل، مدیر اجرایی «نورث‌روپ گرومن استرالیا»
- آقای درن کین، مدیر ارشد امنیت شرکت «ان بی ان»

۲۲) این هیئت بین نوامبر ۲۰۱۹ و ژوئیه ۲۰۲۰، سیزده بار جلسه داشت که شامل دیدار با وزیر کشور بود. این پنل بر اساس مضامین اصلی بازخورد مطرح شده در طی روند مشاوره عمومی، حدود ۱۲ مشکل اصلی را بیان کرد. گزارش نهایی توصیه‌هایی را در ۷ حوزه اصلی ارائه کرده که به آدرس homeaffairs.gov.au/cybersecurity در دسترس است.

۲۳) مطابق با توصیه‌های هیئت، این استراتژی سعی دارد تا نقش‌ها و مسئولیت‌های امنیت سایبری را به طور واضح در دولت، کسب‌وکارها و جامعه تنظیم کند که در بخش بعدی شرح داده شده است.

۲۴) با تکیه بر موفقیت پنل، «کمیته مشاوره دائمی صنعت» نیز برای اطمینان از نقش مداوم صنعت برای شکل‌دهی اقدامات کوتاه‌مدت و بلندمدت در این استراتژی تشکیل شده است.

اندرو پن، مدیر هیئت مشاوره صنعت و مدیر «تلسترا»: «اگر ما همچنان به سرمایه‌گذاری در زمینه دفاع سایبری ادامه دهیم، استرالیا به عنوان یک اقتصاد دیجیتالی رونق خواهد گرفت. اگر تلاش کنیم تا به طور کلی از خود در برابر جرایم سایبری محافظت کنیم، کسب‌وکارهای ما همچنان رقابتی خواهند بود، از زیرساخت‌های ملی ما محافظت می‌شود، امنیت نهادهای ما از جمله فرایند انتخابات دموکراتیک ما، که در سایر قسمت‌ها مورد سوءاستفاده سایبری قرار گرفته است، تحت حمایت قرار می‌گیرد و رفاه استرالیایی‌ها ارتقا می‌یابد. با اقدام سریع و قاطع می‌توان اطمینان حاصل کرد که مزایای این روند از هزینه آن بیشتر خواهد بود."

بخش پنجم

استراتژی ما

۲۵) استراتژی دولت استرالیا در نمودار ۲ نشان داده شده است. چشم‌انداز دولت استرالیا ایجاد یک جهان آنلاین با امنیت بیشتر برای استرالیایی‌ها، کسب‌وکار آن‌ها و خدمات اساسی است که همه ما به آن وابسته هستیم.

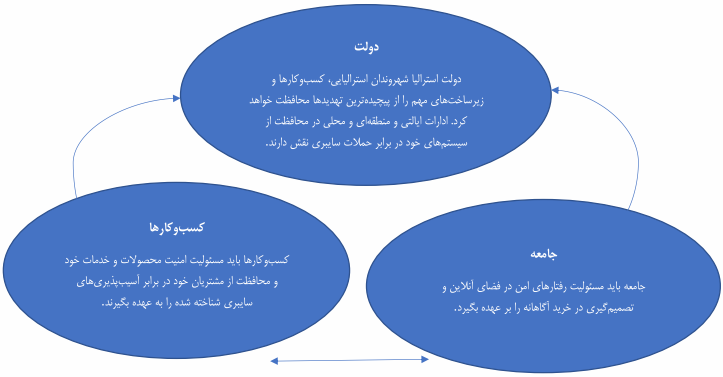
نمودار ۲. استراتژی ما

چشم‌انداز دنیای آنلاین امن‌تر برای استرالیایی‌ها، کسب‌وکار آن‌ها و خدمات ضروری که همه ما به آن وابسته هستیم		
موضوعات اصلی	موضوعات اصلی	موضوعات اصلی
• حفاظت از زیر ساخت‌های حیاتی، خدمات ضروری و داراییها • مبارزه با جرایم اینترنتی از جمله در وب تاریک	• بهبود امنیت پایه برای زیرساخت‌های حیاتی • ارتقای امنیت سایبری شرکت های کوچک و متوسط • ارائه محصولات و خدمات ایمن	• دسترسی و استفاده از راهنمایی‌ها و اطلاعات مربوط به امنیت سایبری • تصمیمات خرید آگاهانه • گزارش جرایم اینترنتی
• حفاظت از دامنه‌ها و شبکه های دولتی استرالیا • اشتراک اطلاعات مربوط به تهدیدات • تقویت مشارکت در امنیت سایبری • پشتیبانی از کسب‌وکارها برای دستیابی به استانداردهای امنیت سایبری • افزایش قابلیت‌های سایبری	• افزایش نیروی کار ماهر • انجام اقداماتی برای جلوگیری از فعالیت‌های مخرب در مقیاس بزرگ	• دسترسی به کمک و پشتیبانی در صورت لزوم

۲۶) ایـن چشـم‌انداز بـا اقـدام ادارات، کسـب‌وکارها و جامعـه محقـق خواهـد شـد، همـان طـور کـه در نمـودار ۳ نیـز نشـان داده شـده اسـت.

- دولـت اسـترالیا محافظـت از اسـترالیایی‌ها، کسـب‌وکارها و زیرسـاخت‌های مهـم را در مقابـل پیچیده‌تریـن تهدیدهـا تقویـت خواهـد کـرد. ادارات ایالتـی، منطقـه‌ای و محلـی نیـز در محافظـت از سیسـتم‌های خـود در برابـر حمـلات سـایبری نقـش دارنـد.
- مشـاغل بایـد مسـئولیت ایمن‌سـازی محصـولات و خدمـات خـود و محافظـت از مشـتریان خـود در برابـر آسـیب‌پذیری‌های سـایبری شـناخته شـده را بـه عهـده بگیرنـد.
- جامعـه نیـز بایـد مسـئولیت رفتارهـای ایمـن در فضـای آنلایـن و تصمیم‌گیـری خریـد آگاهانـه را بـه عهـده بگیـرد.

نمودار ۳: نقش‌ها و مسئولیت‌ها در حوزه امنیت سایبری



۲۷) ایـن رویکـرد اسـترالیا را قـادر می‌سـازد تـا از منابـع محـدود خـود

به بهترین نحو استفاده کند. دولت استرالیا ضمن اطمینان از انعطاف‌پذیری سایبری در اقتصاد کشور، بر تهدیدات مهم و پیچیده‌ترین فعالیت‌های سایبری تمرکز خواهد کرد. دولت استرالیا در جلوگیری و واکنش در برابر مجرمان پیچیده سایبری، از جمله از طریق قابلیت‌های سایبری دفاعی و تهاجمی خود، در بهترین سطح قرار دارد. ادارات ایالتی و منطقه‌ای نیز باید اطمینان حاصل کنند که شبکه‌های آن‌ها در برابر نفوذ سایبری آسیب‌پذیر نیستند.
۲۸) کسب‌وکارها باید همان گونه که مسئول ایمنی و کیفیت محصولاتشان هستند، مسئولیت افزایش امنیت سایبری خود را نیز بر عهده بگیرند. دولت استرالیا انتظار دارد که همه کسب‌وکارها این مهم را بپذیرند و در وهله اول نیز قانونی را در رابطه با زیرساخت‌های حیاتی و سیستم‌های دارای اهمیت ملی معرفی خواهد کرد. بسیاری از اقدامات در این استراتژی با ارائه مشاوره، ابزارهای عملی و سرمایه‌گذاری مشترک در نیروی کار ماهر، در راستای کمک به کسب‌وکارها برای بهره‌مندی از اقتصاد دیجیتال است.
۲۹) جامعه همیشه نقشی در حوزه امنیت سایبری بر عهده خواهد داشت. علی رغم اینکه ادارات و کسب‌وکارها بهترین تلاش‌های خود را به ثمر برسانند، استرالیایی‌ها باید بدانند که چگونه از خود در برابر تهدیدات سایبری محافظت کنند. این استراتژی با تمرکزی ویژه آگاهی جامعه نسبت به رفتارهای ایمن در فضای آنلاین را افزایش داده، دسترسی به خدمات پشتیبانی از قربانیان را ارتقا داده و اطلاعات لازم برای تصمیم‌گیری بهتر در خریدهای اینترنتی را در اختیار تمام شهروندان استرالیایی قرار می‌دهد.

۳۰) تمام بخش‌های مربوط به دولت، کسب‌وکار و جامعه در اجرای این استراتژی نقشی بر عهده دارند. اگرچه این استراتژی ابتکار عمل دولت استرالیا است، اما دولت استرالیا نقش اساسی ادارات ایالتی و منطقه‌ای، کسب‌وکارها، دانشگاه‌ها، شرکای بین‌المللی و جامعه در درک چشم‌انداز ایجاد دنیای آنلاین امن‌تر برای استرالیایی‌ها، کسب‌وکارها و خدمات اساسی که همه ما به آن وابسته هستیم را به رسمیت می‌شناسد. اجرای موفقیت‌آمیز این استراتژی وابسته به تلاش‌ها و اقدامات فردی و مشارکتی ادارات، کسب‌وکارها و جامعه است.

بخش ششم

بخش ششم

پاسخ ما

اقدامات ادارات دولتی

گروه صنعتی «ای آی گروپ»: «دولت نقش مهم رهبری را بر عهده دارد که شامل کمک به سازمان‌ها و جامعه برای کسب آگاهی کامل در فضای سایبری است.»

۳۱) دولت استرالیا در حال سرمایه‌گذاری بر روی توانایی‌های خود برای واکنش در برابر تهدیدهای رو به رشد پیش روی امنیت سایبری است. تاریخ ۳۰ ژوئن ۲۰۲۰، دولت استرالیا بسته ۱/۳۵ میلیارد دلاری آگاهی موقعیتی و پاسخگویی به وضعیت سایبری[1] را تصویب کرد. بسته آگاهی موقعیتی و پاسخ‌گویی به وضعیت سایبری اطمینان حاصل خواهد کرد که اداره سیگنال‌های دیجیتالی استرالیا، به عنوان آژانس عملیاتی امنیت سایبری استرالیا، می‌تواند تهدیدات سایبری بیشتری را شناسایی کند، فعالیت بیشتر مجرمان سایبری خارجی را مختل کند، با صنعت و دولت مشارکت بیشتری برقرار کند و از شهروندان بیشتر استرالیایی محافظت کند. این بخش به طور مفصل مجموعه کاملی از ابزارهایی که دولت استرالیا برای مقابله با تهدیدات امنیت سایبری استفاده خواهد کرد ـ از اقدامات

1. CESAR

داوطلبانـه و همـکاری تـا قانونگـذاری و قابلیت‌هـای طبقه‌بنـدی شـده ـ را توضیـح می‌دهـد.

همکاری با کسب‌وکارها

۳۲) دولـت اسـترالیا نقـش بسـیار مهمـی در امنیـت سـایبری دارد. ایـن مـورد بـه تنهایـی نمی‌توانـد از فضـای سـایبری بـه طـور کلـی محافظـت کنـد؛ بـا ایـن حـال، محیطـی را ایجـاد می‌کنـد کـه هـر کـس می‌دانـد چـه نقشـی را بایـد ایفـا کنـد و «قوانیـن مسـیر» چیسـت. در صـورت لـزوم نیـز قانونگـذاری صـورت می‌گیـرد. ایـن امـر بـه کسـب‌وکارها و جامعـه امـکان می‌دهـد تـا از انعطاف‌پذیـری بیشـتری در زمینـه امنیـت سـایبری ملـی برخـوردار شـوند و اسـترالیا بتوانـد از فرصت‌هـای روزافزون اقتصـاد دیجیتالـی بهره‌منـد شـود.

۳۳) دولـت اسـترالیا عـلاوه بـر ایجـاد سیاسـت‌هایی بـرای امنیـت بیشـتر اسـترالیا در فضـای آنلایـن، نقـش مهمـی در دفـاع فعالانـه از اسـترالیا در برابـر فعالیت‌هـای مخـرب و پیچیـده سـایبری بـر عهـده دارد. دولـت اسـترالیا بـرای دسـتیابی بـه ایـن هـدف، تلاش‌هـای امنیتـی سـایبری خـود را در بخش‌هایـی کـه بیشـترین تأثیـر را خواهـد داشـت، متمرکـز خواهـد کـرد. نخسـت بـرای کوتاه‌مـدت، تمرکـز بـر تعییـن انتظـارات بـرای زیرسـاخت‌های حیاتـی و سیسـتم‌های دارای اهمیـت ملـی (بـا جزئیـات بیشـتر در بخـش «اقدامـات کسـب‌وکارها») اسـت. در ایـن رونـد اطمینـان حاصـل می‌شـود کـه اسـترالیا بـرای مدیریـت تهدیدهایـی بـا بالاتریـن پیامدهـا، از سیاسـت‌ها و قابلیت‌هـای مناسـبی برخـوردار اسـت تـا از خدمـات اساسـی کـه همـه اسـترالیایی‌ها بـرای زندگـی بـه آن وابسـته‌اند، محافظـت شـود.

۳۴) اگرچه استرالیا در جلوگیری از وقوع یک حادثه فاجعه‌بار امنیت سایبری خوش شانس بوده است، اما ما در برابر حملات سایبری که در سایر نقاط جهان تجربه شده است، آسیب‌پذیر هستیم. حمایت از تداوم خدمات ضروری در برابر حملات مخل یا پیچیده وظیفه اساسی دولت است. قطعی خدمات ضروری مانند برق، آب یا حمل‌ونقل می‌تواند تأثیرات مخربی را در سراسر استرالیا فراتر از تجارت مورد هدف داشته باشد. اگرچه برای بالا بردن وضعیت کلی امنیت زیرساخت‌های حیاتی می‌توان کارهای بیشتری انجام داد (رجوع شود به بخش «تأمین خدمات ضروری»)، برخی از کشورها یا فعالان تحت حمایت دولت‌های کشورهای خارجی چنان پیشرفته هستند که حمله آن‌ها ممکن است فراتر از توانایی مالک شبکه مورد هدف، صرف نظر از اندازه، تخصص و تلاش آن باشد.

۳۵) دولت استرالیا باید آماده باشد تا در صورت نیاز به توانایی‌های منحصر به فرد خود، به ویژه در شرایط اضطراری، در جهت منافع ملی اقدام کند. دولت استرالیا از طریق مشورت با صاحبان زیرساخت‌ها و اپراتورهای حیاتی، متناسب با پیامدهای حمله سایبری پیچیده و فاجعه‌بار، اختیارات جدیدی را همراه سازوکارهای دفاعی و نظارتی مناسب ایجاد خواهد کرد. دولت با این اختیارات اطمینان حاصل خواهد کرد که می‌تواند به طور فعال از شبکه‌ها دفاع کند و به بخش خصوصی کمک کند تا در صورت حمله سایبری بهبود یابد. ماهیت این کمک به شرایط بستگی دارد اما می‌تواند شامل مشاوره تخصص، کمک مستقیم یا استفاده از ابزار طبقه‌بندی شده باشد. این امر احتمال خرابی

خدمات ضروری و تأثیر حملات سایبری به استرالیایی‌ها را کاهش خواهد داد.

۳۶) دولت استرالیا همچنین با کسب‌وکارها همکاری خواهد کرد تا تغییرات قانونی را در نظر بگیرد که حداقل سطح امنیت سایبری را در کل اقتصاد تعیین کند. این مشاوره گزینه‌های مختلف اصلاحات از جمله موارد زیر را در بر می‌

- نقش حریم خصوصی، مصرف‌کننده و قوانین محافظت از داده‌ها؛
- وظایف مدیران شرکت و سایر نهادهای تجاری؛
- تعهدات مربوط به تولیدکنندگان دستگاه‌های متصل به اینترنت.

این مشاوره روش‌های ساده‌سازی و کاهش هزینه‌های ایجاد حداقل خط مبنای آینده را بررسی می‌کند.

۳۷) دولت استرالیا ظرفیت خود را برای جلوگیری و یا واکنش به فعالیت‌های مخرب سایبری، از جمله در پاسخ به فعالان پیچیده، تقویت خواهد کرد. دولت استرالیا از طریق این استراتژی، ۶۲/۳ میلیون دلار در توانایی ملی برای آگاهی از موقعیت ملی سرمایه‌گذاری خواهد کرد تا دولت را قادر سازد تهدیدات سایبری پیش روی زیرساخت‌های مهم و سایر شبکه‌های دارای اولویت بالا را درک کرده و نسبت به آن واکنش نشان دهد. این امر با افزایش گزارش حوادث و اطلاعات تهدیدها تقریباً در زمان حقیقی از مهم‌ترین زیرساخت‌ها به عنوان بخشی از الزامات نظارتی آینده تکمیل خواهد شد. برای استفاده از منابع اطلاعات، دولت استرالیا پلتفرم مشترک تهدیدات را ارائه می‌دهد، به طوری که اپراتورهای مهم زیرساختی را قادر می‌سازد تا اطلاعات مربوط به فعالیت‌های مخرب سایبری را به سرعت با دولت و سایر ارائه دهندگان به

اشتراک بگذارند و تهدیدهای پیش رو را در صورت بروز مسدود کنند. این استراتژی ۱۱۸ میلیون دلار برای توسعه توانایی‌های علوم داده سرمایه‌گذاری خواهد کرد. دولت استرالیا با سرمایه‌گذاری ۶۶/۵ میلیون دلاری خود به بزرگترین تأمین‌کنندگان زیرساخت‌های مهم استرالیا در ارزیابی آسیب‌پذیری‌ها در جهت تقویت وضعیت امنیت سایبری کمک خواهد کرد. علاوه بر این، ۲۰/۲ میلیون دلار به آزمایشگاه‌های پیشرفته تحقیقاتی اختصاص می‌یابد تا بتوانیم تهدیدات مربوط به فناوری‌های زیربنایی سیستم‌های مهم زیرساختی استرالیا را بهتر درک کنیم، سیستم‌هایی که کسب‌وکارها و کاربران به طور فزاینده‌ای به آن‌ها وابسته هستند.

۳۸) این امر مستلزم مشارکت قوی بین کسب‌وکارها و ادارات است. برای حمایت از این مشارکت، دولت استرالیا سرمایه‌گذاری خود را در بخش امنیت سایبری در سیدنی، ملبورن، بریزبن، پرث و آدلاید افزایش می‌دهد و خدمات موجود برای شرکای ما را نیز گسترش می‌دهد. ادامه و گسترش فعالیت مراکز مشترک امنیت سایبری در دوران مشاوره و رایزنی عمومی به شدت مورد حمایت قرار گرفت. مراکز مشترک و توسعه یافته امنیت سایبری تعداد بیشتری از مأموران خدمات سایبری، از جمله از وزارت امور داخلی، را استخدام می‌کند. این مأموران حلقه مهمی را در ایجاد مشارکت‌های قوی و به اشتراک‌گذاری مشاوره‌های عملی در زمینه امنیت سایبری شکل خواهند داد.

۳۹) همه مراکز مشترک امنیت سایبری دارای امکانات طبقه‌بندی چند منظوره برای جای دادن طیف گسترده‌تری از قابلیت‌های

مرکز امنیت سایبری استرالیا و تعامل طبقه‌بندی شده با مجریان قانون و شرکای معتمد هستند. همچنین با ایجاد تیم‌های میان رشته‌ای از متخصصان که می‌توانند تخصص عملیاتی و فنی بیشتری را در سراسر کشور ارائه دهند، به تعداد کادر فنی نیز افزوده خواهد شد. مرکز امنیت سایبری استرالیا مکمل فعالیت کسب‌وکارهای خصوصی در حال رشد و حیاتی خواهد بود.

۴۰) اگرچه مبحث امنیت سایبری در درجه اول مسئولیت بخش آموزش عالی است، دولت استرالیا نیز ۱/۶ میلیون دلار برای افزایش امنیت سایبری دانشگاه‌های استرالیا سرمایه‌گذاری می‌کند. به این ترتیب، بودجه شبکه اشتراک اطلاعات، مدل‌سازی تهدید در کل بخش و مجمع ملی امنیت سایبری فراهم می‌شود. مجمع ملی امنیت سایبری استرالیا هر سال سه بار تشکیل می‌شود. تقویت دفاع جمعی دانشگاه‌ها در برابر تهدیدات آینده از برنامه مهارت‌های سایبری پشتیبانی می‌کند. دولت استرالیا از کاری که شبکه تحقیقات دانشگاهی استرالیا[1] برای اشتراک اطلاعات تهدید در بخش آموزش عالی انجام می‌دهد، استقبال می‌کند.

۴۱) دولت استرالیا از طریق همکاری نزدیک با کسب‌وکارها و با عملی کردن فرایندهای واکنش به تهدیدات، خود را برای پاسخ‌گویی به حوادث سایبری آماده خواهد کرد. برنامه تمرینی امنیت سایبری، تحت نظارت مراکز مشترک امنیت سایبری، اطمینان خواهد داد که کسب‌وکارها و ادارات استرالیا زودتر از موعد فرایند واکنش به حوادث سایبری را تمرین کرده و همیشه آمادگی و مقاومت خود را در مواجهه با اتفاقات پیشِ رو تقویت می‌کنند.

1. AARNet

دولت استرالیا با همکاری ادارات ایالتی و منطقه‌ای، کسب‌وکارهای موجود در دفترچه راهنمای پاسخ‌گویی به‌حوادث را به طور رسمی شناسایی کرده، که به «تنظیمات مدیریت حوادث سایبری» معروف است. این روند اطمینان می‌دهد که تمام بخش‌های جامعه استرالیا به طور واضح نقش‌ها و مسئولیت‌های مشخصی دارند و آگاه هستند که در صورت بروز حادثه سایبری یا موارد اضطراری چه باید بکنند.

بازخواست مجرمان اینترنتی

۴۲) مقابله با جرم به همان اندازه که در دنیای فیزیکی اهمیت دارد، در دنیای آنلاین نیز مهم است. مجرمان از هر جای دنیا می‌توانند با سهولت و در مقیاس بزرگ از اینترنت برای صدمه زدن به استرالیایی‌ها استفاده کنند. آژانس‌های اجرای قانون در سراسر استرالیا برای پاسخ‌گویی به مجرمان سایبری و جلوگیری از جرایم سایبری، باید با یکدیگر همکاری کنند. با استناد به موفقیت رویکردهای مقابله با تروریسم و استثمار کودکان، این استراتژی همچنین همکاری‌های بیشتر در سراسر استرالیا و با شرکای بین‌المللی را تشویق می‌کند. دولت استرالیا با ادارات ایالتی و منطقه‌ای همکاری خواهد کرد تا تلاش‌های ما را در اولویت قرار دهد و آژانس‌ها را به قابلیت‌های ایجاد تغییر مجهز کند. دولت استرالیا همچنین با سرمایه‌گذاری ۸۹/۹ میلیون دلاری توانایی پلیس فدرال استرالیا[1] را در تحقیق و تعقیب مجرمان اینترنتی تقویت خواهد کرد. این سرمایه‌گذاری پلیس فدرال استرالیا را قادر

1. AFP

می‌سازد تا تیم‌های توسعه هدف را با شرکای خود ایجاد کرده، توانایی‌های فنی سایبری را ایجاد کرده و ظرفیت عملیاتی را افزایش دهد. تخصص اطلاعات مالی مرکز تراکنش‌ها و تجزیه و تحلیل تراکنش‌های استرالیا برای هدف قرار دادن سود مجرمان اینترنتی مورد استفاده قرار خواهد گرفت. دولت استرالیا با تکیه بر توانایی مقابله با مجرمان سایبری خارجی سال ۲۰۱۹، همچنین توانایی مراکز مشترک امنیت سایبری را برای مقابله با فعالان جرایم اینترنتی در خارج از کشور گسترش خواهد داد.

۴۳) رمزنگاری روشی مهم برای محافظت از داده‌های تجاری و مصرف‌کننده است، اما استفاده روزافزون از وب تاریک و فناوری‌های رمزنگاری که به افراد اجازه می‌دهد در فضای آنلاین ناشناس بمانند، توانایی سازمان‌های اجرای قانون در محافظت از جامعه ما را به چالش می‌کشد. وب تاریک مجرمان سایبری را قادر می‌سازد تا استثمار و سوءاستفاده جنسی کودکان را ترویج کرده، هویت سرقت شده را به تجارت گذاشته، مواد مخدر قاچاق و سلاح گرم را پخش کرده و حملات تروریستی را طراحی کنند. این پلتفرم‌ها ارتکاب جرایم جدی را بیش از پیش آسان و آسان‌تر کرده است. قانون اصلاح ارتباطات و سایر قوانین که در سال ۲۰۱۸ ارائه شد، به آژانس‌های اجرای قانون و امنیت استرالیا در همکاری با صنعت و مقابله با تهدیدات جنایی و تروریستی آنلاین کمک کرده است. دولت استرالیا از طریق این استراتژی اطمینان حاصل خواهد کرد که آژانس‌های اجرای قانون از اختیارات قانونی و توانایی‌های فنی مناسبی برای جلوگیری، اختلال و شکست بهره‌برداری‌های جنایی

از فناوری‌ها و وب تاریک برخوردار هستند.

شناسایی تهدیدها

۴۴) سازمان‌های اجرای قانون در استرالیا برای شناسایی تهدیدهای جدید، پیش از آسیب به استرالیایی‌ها، و همچنین برای پاسخ‌گویی به تحولات فناوری با چالشی مداوم روبرو هستند. اداره سیگنال‌های استرالیا ۵۰۰ پرسنل اطلاعاتی و امنیتی سایبری دیگر را با هزینه ۴۶۹/۷ میلیون دلار طی ۱۰ سال استخدام خواهد کرد. دولت استرالیا ۳۸۵/۴ میلیون دلار در زمینه توانایی بخشی و افزایش قابلیت‌های اطلاعاتی سرمایه‌گذاری خواهد کرد. این اقدامات، علاوه بر واکنش به مجرمان اینترنتی و فعالان مخرب، اطمینان حاصل خواهد کرد که استرالیا رهبر جهانی توسعه رویکردهای جدید و نوآورانه است، به طوری که همه استرالیایی‌ها قادر خواهند بود با اطمینان از فناوری‌های جدید استفاده کنند و از مزایای اقتصاد دیجیتال بهره ببرند.

سیستم‌های دولتی

۴۵) ادارات نیز مسئولیت دارند که بر اساس الگو مدیریت کنند. ارائه بیشتر خدمات دولتی به صورت آنلاین زندگی استرالیایی‌ها را آسان می‌کند. با این حال، شهروندان باید اطمینان داشته باشند که داده‌های آن‌ها امنیت دارد، که این امر بر تأمین امنیت سیستم‌ها و داده‌های دولتی تأکید دارد. این استراتژی در طولانی مدت دولت استرالیا را بر آن می‌دارد تا دفاع از شبکه‌های بخش

عمومی را تقویت کند. اولویت نخست، متمرکز کردن مدیریت و عملکرد تعداد زیادی از شبکه‌ها، از جمله در نظر گرفتن مراکز امن است که توسط آژانس‌های دولتی استرالیا اداره می‌شوند. متمرکز کردن مدیریت می‌تواند تعداد اهداف در دسترس فعالان مخرب، مانند کشورها یا فعالان مورد حمایت آن‌ها را کاهش دهد و به دولت استرالیا اجازه دهد سرمایه‌گذاری امنیت سایبری خود را روی تعداد کمی از شبکه‌های امن‌تر متمرکز کند. مدل متمرکز برای ترویج نوآوری و سرعت در کنار توسعه اقتصاد طراحی خواهد شد.

۴۶) متمرکزسازی سیستم‌های امنیت سایبری در سراسر دولت همراه فعالیت آژانس‌های دولت استرالیا برای تقویت امنیت سایبری آن‌ها و اجرای استراتژی‌های هشت‌گانه مرکز امنیت سایبری استرالیا تکمیل خواهد شد. این فرایند با مشاوره و راهنمایی‌های مربوط به امنیت سایبری فنی مرکز امنیت سایبری استرالیا پشتیبانی خواهد شد. رویکرد ارتقای سیستم‌های دولتی در جهت کاهش ریسک آسیب و کمک به جلوگیری از متداول‌ترین تکنیک‌های مورد استفاده مجرمان سایبری طراحی شده است. آژانس‌های دولتی استرالیا همچنین تمرکز جدیدی بر سیاست‌ها و روش‌های مدیریت ریسک امنیت سایبری خواهند داشت. بندهای استاندارد امنیت سایبری در قراردادهای فناوری اطلاعات دولت استرالیا گنجانده خواهد شد.

ارتباط میان جرایم سایبری و سرقت هویت

بسیاری از تهدیدات سایبری به دلیل فعالیت مجرمانی است که با استفاده از اطلاعات هویتی جعلی یا سرقت شده، هویت خود را پنهان می‌کنند. اطلاعات شخصی سرقت شده از شهروندان بی‌خبر استرالیایی به طور گسترده‌ای در بازارهای وب تاریک در دسترس است و مجرمانی که قصد کلاهبرداری یا تسهیل اقدامات غیرقانونی را دارند، آن‌ها را در مقیاسی بسیار بزرگ خریداری می‌کنند و می‌فروشند. برای مثال، مجرمان با استفاده از هویت‌های مسروقه پول را از حساب‌های بانکی برداشت می‌کنند، وام می‌گیرند، درخواست کارت‌های اعتباری می‌دهند، یا مزایای دولتی را به نام شخصی دیگر مطالبه می‌کنند.

ارتقای امنیت سایبری با هویت‌های دیجیتالی قابل اعتماد

۴۷) برای کمک به محافظت از استرالیایی‌ها در برابر جرایم هویتی، برنامه هویت دیجیتال دولت استرالیا به مردم این امکان را می‌دهد تا از اعتبار هویت دیجیتال معتبر، مانند myGovID، برای دسترسی به خدمات آنلاین سازمان‌های دولتی و بخش خصوصی استفاده کنند. با اطمینان بیشتر سازمان‌ها به افرادی که به صورت آنلاین با آن‌ها سروکار دارند، دسترسی به خدمات آنلاین برای استرالیایی‌ها آسان‌تر و ایمن‌تر خواهد شد.

۴۸) با استفاده از شناسنامه‌های معتبر هویت دیجیتال برای دسترسی به چندین سرویس آنلاین افراد نیازی به تأیید مجدد هویت خود یا حفظ چندین رمز عبور نخواهند داشت. این روند میزان اطلاعات شخصی که باید با ارائه دهندگان خدمات آنلاین

به اشتراک گذاشته شود را کاهش می‌دهد و به جلوگیری از سرقت هویت و سایر اشکال جرایم اینترنتی کمک می‌کند.

۴۹) هویت‌های دیجیتالی باید با توجه به سوابق هویتی دولتی مانند گذرنامه، گواهینامه رانندگی و شناسنامه، و اسنادی که استرالیایی‌ها برای کمک به اثبات هویت خود استفاده می‌کنند، تأیید شوند. دولت استرالیا برای به‌روزرسانی استراتژی امنیت ملی هویت در جهت تقویت ترتیبات صدور و مدیریت این اسناد، حفظ ضمانت‌های محرمانه، و همچنین تقویت بیشتر نیروی دفاعی ما در برابر هویت و جرایم اینترنتی، با ایالت‌ها و نواحی مختلف همکاری خواهد کرد.

ارتباط بین‌المللی

۵۰) در آخر، ادارات وظیفه دارند از قوانین بین‌المللی موجود و رفتار مسئولانهٔ دولت در فضای مجازی حمایت کنند. استرالیا به تشویق جامعه بین‌الملل در مسئولیت‌پذیری آنلاین، از جمله با رعایت قوانین بین‌المللی موجود، قوانین داخلی و رفتار مسئول دولتی، ادامه خواهد داد. دولت استرالیا اطمینان حاصل خواهد کرد که استرالیا به عنوان هدفی نرم دیده نمی‌شود و در صورت صلاح دید به کشورها فراخوان می‌دهد. دولت استرالیا بیانیه‌های عمومی خود را با اقداماتی از طریق طیف وسیعی از پاسخ‌های هدفمند و قاطع در برابر نفوذ یا فعالیت غیرقابل قبول در راستای بیانیهٔ اصول استرالیا در زمینه بازدارندگی سایبری مطابقت می‌دهد:

ما تلاش می‌کنیم تا به طور فعال از حملات سایبری جلوگیری کنیم،

آسیب‌ها را به حداقل برسانیم و به فعالیت‌های مخرب سایبری که علیه منافع ملی ما است، واکنش نشان دهیم. ما ضمن ایجاد توازن در برابر ریسک، مانع حملات سایبری می‌شویم. اقدامات ما قانونی و مطابق با ارزش‌هایی است که ما می‌خواهیم آن را حفظ کنیم. بنابراین؛ متناسب، همیشه مطابق با بافت و به صورت مشارکتی خواهد بود. البته می‌توانیم انتخاب کنیم که واکنشی نشان ندهیم.

۵۱) اقدامات دولت استرالیا امنیت سایبری کشور را تقویت می‌کند. تعهدات و مشارکت‌های قوی‌تر، بهترین فرصت را برای ایجاد اختلال یا به حداقل رساندن حملات پیچیده به ما می‌دهد. تقویت نیروی انتظامی و قابلیت‌های اطلاعاتی بازدارندگی قوی‌تری را در برابر مجرمان سایبری ایجاد می‌کند. سیستم‌های دولتی که همه استرالیایی‌ها به آن اعتماد می‌کنند، مقاوم‌تر می‌شود. اقدامات مورد نیاز مشاغل بر اساس همین ابتکارات خواهد بود.

استراتژی مشارکت بین‌المللی در زمینه فناوری‌های حیاتی و سایبری استرالیا

دولت استرالیا فناوری‌های حیاتی را فناوری‌های فعلی و در حال توسعه تعریف می‌کند که به شکلی قابل توجه ظرفیت ارتقا و ایجاد ریسک برای منافع ملی (رفاه، انسجام اجتماعی یا امنیت ملی) را دارد. فناوری حیاتی و فضای سایبری به طور فزاینده‌ای به جنبه‌های مهم روابط بین‌الملل تبدیل می‌شود. این فناوری ذاتاً با رفاه و امنیت ملی، محافظت و ارتقای حقوق بشر و دموکراسی، ثبات بین‌المللی، رفاه اقتصاد جهانی و توسعه پایدار ما در ارتباط است.

دولت استرالیا در حال توسعهٔ استراتژی مشارکت بین‌المللی سایبری و فناوری‌های حیاتی است.

با توجه به استراتژی بین‌المللی مشارکت سایبری ۲۰۱۷، استراتژی بین‌المللی مشارکت سایبری و فناوری‌های حیاتی آتی چهارچوبی را برای هدایت مشارکت بین‌المللی استرالیا فراهم می‌کند. این چهارچوب تضمین کننده این است که فضای مجازی و تکنولوژی از اهداف ما برای امنیت، ایمنی و رفاه استرالیا، هند و اقیانوسیه و دنیا حمایت می‌کند. در جهت انجام این کار شرکا باید با ایجاد ظرفیت بین‌المللی و مقاومت در برابر تهدیدات امنیت سایبری، جرایم سایبری، آسیب‌های اینترنتی و دروغ پراکنی از دستیابی به اهداف امنیت سایبری ما حمایت کنند.

دولت استرالیا تمرکز بیشتری بر روی مشارکت بین‌المللیِ امنیت فناوری‌های حیاتی خواهد داشت. ماهیت زنجیره‌های تأمین جهانی به این معنی است که استرالیا باید در جهت اطمینان از دستکاری نشدن فناوری‌های حیاتی برای اهداف مخرب، اقدامات مشترکی را با کشورهای هم‌عقیده به انجام برساند.

همکاری با شرکای بین‌المللی

امنیت و مقاومت متحدان، شرکای منطقه‌ای و جامعه بین‌المللیِ وسیع‌تر برای تأمین امنیت ملی و رفاه استرالیا ضروری است.
استرالیا به حمایت و حفظ مکانیزم‌های بین‌المللی ایجاد ثبات و همکاری داوطلبانه با شرکا در جهت توقف و پاسخ به رفتارهای غیرقابل قبول در فضای سایبری متعهد می‌شود.

استرالیا به مجامعی مانند سازمان بین‌المللی استانداردسازی و اتحادیه بین‌المللی مخابرات کمک می‌کند. این مجامع استانداردهای بین‌المللی را توسعه داده و به ایجاد فضای سایبری امن‌تر برای همه کشورها کمک می‌کنند.

افزایش آگاهی و ظرفیت‌سازی به تضمین استفاده صلح آمیز از فناوری کمک می‌کند و در نهایت باعث افزایش مقاومت جمعی سایبری ما می‌شود و در نتیجه منافع مستقیمی را برای استرالیا به همراه می‌آورد. برخی از کشورها برای رسیدن به موارد ذیل به کمک نیاز دارند:

- بهبود امنیت زیرساخت‌های حیاتی فناوری اطلاعات و ارتباطات؛
- توسعه مهارت‌های فنی و قانونگذاری مناسب، چهارچوب‌های نظارتی و استراتژی‌ها برای انجام مسئولیت‌های کشور؛
- ایجاد ارتباط بین بخش امنیت فناوری اطلاعات و ارتباطات و استفاده از آن.

ظرفیت‌سازی برای همسایگانمان

دولت استرالیا تا کنون ۶۰ میلیون دلار برای حمایت از ایجاد ظرفیت سایبری در منطقه هند و اقیانوسیه هزینه کرده است تا بتواند فضای مجازی آزاد، رایگان و امن را به ارمغان بیاورد. این کار شامل یک برنامه هفت‌ساله، همکاری مجازی ۳۴ میلیون دلاری، همکاری با دولت، صنعت، جامعه مدنی و دانشگاهی در جهت افزایش مقاومت مجازی در کلِ محدوده امور مجازی می‌شود. برنامه همکاری مجازی اکنون نیز در تلاش است تا تأثیر فعالیت‌های مخرب مجازی را در دوران کووید ـ ۱۹ کاهش دهد.

استرالیا به طرح همکاری مجازی چهارساله ۱۴ میلیون دلاری استرالیا ـ پاپوآ گینه نو برای ارتقای چهارچوب‌های امنیت مجازی پاپوآ گینه نو و توانایی فنی و چهار ساله ۱۲/۷ میلیون دلاری مشارکت مجازی و فناوری‌های حیاتی استرالیا-هند نیز متعهد شده است.

اقدامات تجاری

بانک کامن ولث استرالیا: «در اقتصاد به هم پیوستهٔ ما، حمله به یک سازمان می‌تواند بر مشتریان و زنجیره‌های تأمین تأثیر بگذارد.»

۵۲) امنیت سایبری برای همه کسب‌وکارها مهم است. امکان دسترسی به اقتصاد دیجیتالی را فراهم می‌کند و از سودهایی که به سختی به دست آمده، مالکیت معنوی ارزشمند و اطلاعات حساس مشتری محافظت می‌کند. برخی از مشاغل امنیت مجازی را نسبت به بقیه جدی‌تر تلقی می‌کنند. با توجه به اینکه بیشتر داده‌ها و شبکه‌های استرالیا به بخش خصوصی تعلق دارد، تا زمانی که همه کسب‌وکارها برای محافظت از خود، زنجیره‌های تأمین‌شان و مشتری‌هایشان اقدامی نکنند، استرالیا امنیت نخواهد داشت.

ایمن‌سازی خدمات ضروری

۵۳) بهترین راه برای محافظت از استرالیایی‌ها در بهترین حالت، تأمین زیرساخت‌های حیاتی ما است. از طریق این استراتژی، دولت استرالیا با مالکان و اپراتورها همکاری خواهد کرد تا امنیت مجازی آن‌ها را ارتقا داده و با استفاده از ابزار دفاعی و تهاجمی از شبکه‌ها محافظت کند. این مسئله مطابق با بازخورد استراتژی در

مورد کار مشترک برای دفاع بهتر از زیرساخت‌های حیاتی است.

۵۴) دولت استرالیا نیاز به محافظت از زیرساخت‌های حیاتی ما را جدی گرفته و همواره برای آن اقدام کرده است. دولت استرالیا اصلاحاتی را در سال ۲۰۱۸ برای مدیریت تهدیدات بخش مخابرات و برخی از امکانات برق، آب، گاز و حمل‌ونقل انجام داده است. با این حال، فضای تهدید در حال بدتر شدن است. در واکنش به این موضوع، دولت استرالیا در حال توسعه چهارچوب نظارتی پیشرفته برای زیرساخت‌های حیاتی و سیستم‌های اساسی کشور است.

۵۵) چهارچوب پیشرفته باعث ارتقای امنیت و مقاومت در بخش‌های زیرساختی حیاتی، همراه با شناسایی بهتر و به اشتراک‌گذاری اطلاعات در مورد تهدیدها می‌شود تا زیرساخت‌های حیاتی استرالیا ـ تحت مالکیت یا اداره صنعت یا دولت ـ از مقاومت و امنیت بیشتری برخوردار شود. این رویکرد اقدامات پیش از حادثه را در همه جا در اولویت قرار می‌دهد.

۵۶) یک راه حل برای همه کارساز نیست. این چهارچوب ضمن شناسایی تفاوت بخش‌های خاص، اهداف مربوط به حمایت‌های مجازی، فیزیکی، پرسنلی و زنجیره تأمین را در همه بخش‌ها تعدیل می‌کند. به همین دلیل است که این چهارچوب بر اساس نتایج مبتنی بر اصول ایجاد می‌شود و با راهنمایی و مشاوره متناسب با ریسک‌ها و شرایط موجود در هر بخش پشتیبانی می‌شود. به دلیل ماهیت به هم پیوستهٔ بخش‌های زیرساخت حیاتی، حتی بخش‌های کامل نیز از این تغییرات بهره‌مند می‌شوند و باید شاهد ارتقا در زنجیره تأمین خود و شبکه‌ها و سیستم‌های وابسته

به خود باشند.

۵۷) ایـن چهارچـوب بـدون در نظـر گرفتـن توافـق مالکیـت، بـرای مالـکان و اپراتورهـای زیرسـاخت‌های حیاتـی مربوطـه اعمـال خواهـد شـد. همچنیـن شـرایط یکسـانی را بـرای مالـکان و اپراتورهـا فراهـم می‌کنـد و محیـط بـاز فعلـی سـرمایه‌گذاری اسـترالیا را حفـظ می‌کنـد تـا بـه مشـاغل اطمینـان دهـد کسـب‌وکارهایی کـه امنیـت را جـدی می‌گیرنـد، ضـرر مالـی نخواهنـد کـرد.

۵۸) چهارچـوب نظارتـی امنیتـی زیرسـاخت‌های پیشـرفتهٔ اسـترالیا تبییـن خواهـد کـرد کـه دارنـدگان زیرسـاخت بـرای بـرآورده کـردن حداقـل انتظـارات مـا از امنیـت مجـازی چـه کاری بایـد انجـام دهنـد. ایـن کارهـا عبارتنـد از:

- تعهـد امنیتـی مطمئـن و قابـل اجـرا بـرای نهادهـای زیرسـاختی حیاتـی تعییـن شـده؛
- افزایـش تعهـدات امنیـت مجازی بـرای نهادهای بسـیار مهم کشـور؛
- کمـک دولـت اسـترالیا بـه مشـاغل در واکنـش بـه قابـل توجه‌تریـن حمـلات سـایبری بـه سیسـتم‌های اسـترالیایی؛
- اقدامـات داوطلبانـه بـرای تقویـت مشـارکت بـا کسـب‌وکارهای در معـرض خطـر و حمایـت از ارتقـای امنیـت یـک نهـاد.

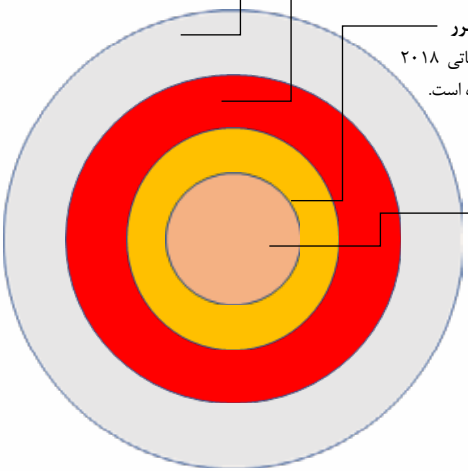
۵۹) چهارچـوب نظارتـی پیشـرفته بـه وسـیله اصلاحیه‌هـای مصوبـهٔ امنیـت زیرسـاخت‌های حیاتـی ۲۰۱۸ ارائـه می‌شـود.

محافظت از زیرساخت‌ها و سیستم‌های حیاتی کشور

اصلاحـات امنیتـی بخـش مخابـرات و مصوبـهٔ امنیـت زیرسـاخت‌های

حیاتی ۲۰۱۸ حفاظت از استرالیا را در برابر تهدیدات پیشِ روی بخش مخابرات و برخی از دارایی‌های برق، آب، گاز و حمل و نقل تقویت می‌کند.

دولت استرالیا با استفاده از این بنیان، بخش‌های حیاتی دیگری که استرالیایی‌ها مبتنی بر آن زندگی می‌کنند را نیز دربر می‌گیرد. به عنوان بخشی از این اصلاحات، دولت استرالیا تعهداتی را برای دارندگان این امکانات حیاتیِ زیرساختیِ مقرر از جمله تعهدات خاص سایبری دیگر برای محافظت از حیاتی‌ترین سیستم‌های ما معرفی خواهد کرد.



اصلاحات تأیید می‌کنند که اگرچه نهادها وظیفه دارند در جهت محافظت از خود و خدمات ارائه شدهٔشان اقدام کنند، اما دولت استرالیا موظف است درصورتی که بدون استفاده از ظرفیت‌های خاص دولتی، مدیریت تهدیدها یا پیامدها برای واحدها بیش از حد دشوار باشد، در جهت منافع ملی اقدام کند.

۶۰) از جهت دیگر کسب‌وکارهای کوچک و متوسط بیشتر در معرض تهدیدهای پیشِ روی امنیت سایبری هستند. نتیجهٔ حاصل از همفکری‌ها نشان می‌دهد که کسب‌وکارهای کوچک و متوسط اغلب منابع یا مهارت لازم برای دفاع را ندارند و هنگامی که مجرمان سایبری آن‌ها را هدف قرار می‌دهند، می‌توانند تأثیر زیادی بر جوامع منطقه‌ای داشته باشند. این استراتژی شامل برنامه پیوند و محافظت از امنیت سایبری ۸/۳ میلیون دلاری است که با مشاوره و پشتیبانی از منابع معتبر به کسب‌وکارهای کوچک و متوسط کمک می‌کند.

۶۱) دولت استرالیا آموزش‌های آنلاین و پشتیبانی شبانه‌روزی را برای کسب‌وکارهای کوچک و متوسط که نیاز به کمک یا مشاور امنیت سایبری دارند، ارائه می‌دهد. دولت و کسب‌وکارهای بزرگ به کسب‌وکارهای کوچک کمک می‌کنند تا امنیت سایبری خود را ارتقا داده و آگاهی خود را درباره امنیت سایبری افزایش دهند. دولت استرالیا کسب‌وکارهای بزرگ و خدمات‌دهندگان را به ارائه اطلاعات و ابزارهای امنیت سایبری تشویق می‌کند که به عنوان بخشی از «بستهٔ» خدمات امنیتی مانند آموزش جلوگیری از تهدیدات، آموزش آنتی ویروس و آگاهی از امنیت سایبری در اختیار

کسب‌وکارهای کوچک قرار می‌گیرد. ادغام محصولات امنیت سایبری در سایر خدمات ارائه شده به محافظت از کسب‌وکارهای کوچک و متوسط به بهترین حالت کمک می‌کند و ثابت می‌کند که بسیاری از کسب‌وکارها نمی‌توانند کارمندان مختص امنیت سایبری را استخدام کنند. همه این برنامه‌ها در وب سایت http://cyber.gov.au/ ارائه شده است. بنابراین کسب‌وکارهای کوچک و متوسط می‌توانند به سرعت کمک دولت استرالیا را دریافت کنند که به بهترین نحو نیازهای آن‌ها را برآورده می‌کند.

حمایت از کسب‌وکارهای کوچک و متوسط

دولت استرالیا حمایت از کسب‌وکارهای کوچک و متوسط را از طریق تعدادی از ابتکارات کلیدی در اولویت قرار خواهد داد:

- توسعه ۱۲/۳ میلیون دلاری خط تلفن اضطراری شبانه‌روزی مرکز امنیت سایبری استرالیا، ارائه مشاوره و کمک فنی امنیت مجازی را افزایش می‌دهد.
- برنامه پیوند و محافظت از امنیت مجازی ۸/۳ میلیون دلاری سازمان‌های مورد اعتماد را برای بالا بردن امنیت سایبری کسب‌وکارهای کوچک و متوسط در منطقه محلی خود مجهز می‌سازد.
- استقرار کارمندان کمک‌رسان در مراکز مشترک امنیت مجازی از کسب‌وکارهای کوچک و متوسط پشتیبانی می‌کند.
- پشتیبانی از گسترش تکنولوژی جلوگیری از تهدید، مانع از آن خواهد شد که تهدیدات مجازی مخرب شناخته شده به مشتریان و مشاغل استرالیایی آسیب برساند.

- راهنمای امنیت سایبری کسب‌وکارهای کوچک و متوسطِ مرکز امنیت سایبری استرالیا، مشاوره‌ای متناسب با محافظت در برابر رایج‌ترین حوادث امنیت مجازی را ارائه می‌دهد.
- راهنماهای گام‌به‌گام و سریع مرکز امنیت سایبری استرالیا آموزش‌های عملی را با کمک وسایل آموزشی بصری در اختیار می‌گذارند و اقدامات مختصری را که کسب‌وکارهای کوچک و متوسط می‌توانند برای محافظت از خود انجام دهند را ارائه می‌دهد.
- برنامه مرکز امنیت سایبری استرالیا Stay Smart Online بهترین مشاوره در زمینه امنیت سایبری را ترویج می‌دهد و کسب‌وکارها را به محافظت آنلاین از خود ترغیب می‌کند.
- ابزارهای منتشر شده در cyber.gov.au به کسب‌وکارهای کوچک و متوسط کمک می‌کند تا آگاهی در مورد امنیت مجازی را در بین کارکنان خود افزایش دهند.
- برنامه آموزشی آنلاین امنیت مجازی اختصاصی در وب سایت cyber.gov.au به تقویت مهارت کسب‌وکارهای کوچک و متوسط و کارمندان کمک خواهد کرد.
- اجرای قانون، توانایی شناسایی و ایجاد اختلال برای مجرمان سایبری که کسب‌وکارهای استرالیایی را هدف قرار می‌دهند، توسعه خواهد داد.

مایکروسافت: «امروزه حملات فزاینده سایبری مجرمان پیشرفته، تمام بخش‌های سازمان‌ها، از شرکت‌های بزرگ گرفته تا نانوایی محلی را تهدید می‌کند. سازمان‌ها در هر اندازه باید اقدامات لازم

برای محدود کردن خطرات ناشی از این تهدیدها را انجام دهند.»

۶۲) کسب‌وکارهای خاص می‌توانند با مسدود کردن خودکار محتوای مخربِ شناخته شده، میزان تهدیدات وارد شده را کاهش دهند. این راه حل با پردازش و نتیجه‌گیری سریع از استرالیایی‌ها و کسب‌وکارهای استرالیایی محافظت می‌کند. در طول دوره این استراتژی، دولت استرالیا از کسب‌وکارها برای حمایت از فناوری جلوگیری از تهدیدات، پشتیبانی خواهد کرد که می‌تواند به طور خودکار از شهروندان و کسب‌وکارها در برابر بدافزارها و تروجان‌ها محافظت کند. دولت استرالیا همچنین بررسی خواهد کرد که چگونه می‌تواند به خدمات‌دهندگان مخابرات که این فناوری را ارائه می‌دهند، خدمات قانونی و هر کمک دیگری ارائه دهد. به عنوان بخشی از این ابتکار، دولت استرالیا ۱۲/۵ میلیون دلار برای مرکز امنیت سایبری سرمایه‌گذاری خواهد کرد تا اطلاعات مربوط به وب سایت‌های مخرب شناخته شده، بدافزارها، کمپین‌های فیشینگ و کلاهبرداران آنلاین را به بزرگترین خدمات‌دهندگان مخابرات استرالیا ارائه دهد تا توانایی خدمات‌دهندگان در جلوگیری از تهدیدات را به طور گسترده افزایش دهد. این بودجه از مشارکت صنعتی، پژوهش و توسعه توانایی‌های جدید برای شناسایی و جلوگیری از تهدیدها در مقیاسی وسیع پشتیبانی کرده و حجم تهدیدات مجازی که استرالیایی‌ها را تحت تأثیر قرار می‌دهد، کاهش داده تا آن‌ها بتوانند بر اداره کسب‌وکارها و اقتصاد خود تمرکز کنند.

ابتکار «کلینر پایپز»

در ماه مه سال ۲۰۲۰، تلسترا اختراع خود را با عنوان «کلینر پایپز»

معرفی کرد. این اختراع فیلترینگ سامانه نام دامنه «تلسترا» را ارتقا می‌دهد تا ارتباط میلیون‌ها بدافزار را به طور خودکار مسدود کند؛ چراکه هر هفته تلاش می‌کنند تا از زیرساخت‌های «تلسترا» عبور کنند. «تلسترا» به مدت ۱۲ ماه این طرح را از جمله در مسدود کردن نفوذ و کنترل باتنت‌ها و بدافزارها و توقف دانلود تروجان‌های مدیریت از راه دور، بکدورها و تروجان‌های بانکی آزمایش کرده است. «کلینر پایپز» اختراعات مشابه متمرکز بر کاهش پیامک‌های مخرب و تماس‌های کلاهبرداری را کامل می‌کند. در حال حاضر «تلسترا» از دسترسی ماهانه بیش از نیم میلیون مکالمه کلاهبرداری به مشتریان جلوگیری می‌کند. دولت استرالیا در حال همکاری با مشاغل است تا از اجرای خدمات بیشتر برای استرالیایی‌ها پشتیبانی کند.

ایمن‌سازی محصولات و خدمات

۶۳) استرالیایی‌ها بسیار بیشتر از قبل به اینترنت متصل می‌شوند. تخمین زده می‌شود که تا سال ۲۰۳۰ بیش از ۲۱ میلیارد دستگاه‌های اینترنت اشیا در سطح جهان به اینترنت متصل شوند که بیشترین تخمین‌ها بیش از ۶۴ میلیارد دستگاه[1] را پیش‌بینی می‌کند. دستگاه‌ها شامل این موارد می‌شود: وسایل شخصی مانند ساعت‌های هوشمند، یخچال‌ها و ناظران کودک، ابزارهای پزشکی مانند ضربان سازهای قلب و دستگاه‌های اندازه‌گیری گلوکز خون و دستگاه‌های صنعتی که بازده کسب‌وکار را افزایش می‌دهد.
۶۴) دولت استرالیا برای حمایت از مشاغل در انجام اقدامات حفاظتی از خود و مشتریان، آیین‌نامه کار داوطلبانه را منتشر می‌کند: امنیت

1. t5onNLioferLock (2020), The future of IoT: 10 predictions about the Internet of Things, available at https://us.norton.com/internetsecurity-iot- -5predictions-for-the-future-of-iot.html; Business Insider (2020), A look at examples of IoT devices and their business applications in 2020, available at https://www.businessinsider.com/internet-of-things-devices-examples?r=AU&IR=T

اینترنت اشیا برای مشتریان در جهت آگاهی مشاغل در مورد ویژگی‌های امنیت مجازی مورد انتظار از دستگاه‌های متصل به اینترنت در استرالیا، ۱۳ اصل در آیین‌نامه کار داوطلبانه، اهمیت حمایت از مشتریان را به تولیدکنندگان نشان می‌دهد. تصویب آیین‌نامه کار همراه با راهنمای تولید شده توسط مرکز امنیت سایبری استرالیا، با افزایش تعداد محصولات ایمنی موجود برای خرید، به استرالیایی‌ها و کسب‌وکارهای کوچک و بزرگ خدمات می‌رساند. دولت استرالیا اطلاعاتی را در مورد مواردی که باید هنگام خرید دستگاه‌های اینترنت اشیا در نظر بگیرند، در اختیار مشتریان قرار خواهد داد.

۶۵) همانند کارهای انجام شده در انگلستان، دولت استرالیا برای ترغیب به طراحی ایمن، شفافیت و استقلال و یکپارچگی در سرمایه‌گذاری، خرید و امنیت اصول زنجیره تأمین را برای تصمیم‌گیرندگان و تأمین‌کنندگان به طور مشترک طراحی می‌کند. دولت استرالیا این اصول را در شیوه‌های تصمیم‌گیری، حمایت از رقابت و تنوع در بازار، ایجاد خواهد کرد. دولت استرالیا برای به‌روز نگه داشتن راهنماها همگام با پیشرفت تکنولوژی و تهدیدها، همچنان بر ابتکارات موجود دولتی که نوآوری در تحقیق و توسعه امنیت سایبری خودکفا را فراهم می‌کند، نظارت کرده و بر اساس آن‌ها اقدام می‌کند. ابتکار «آوس سایبر» برای اطمینان از تجاری‌سازی و سنجش ظرفیت‌های امنیت سایبری که نیازهای کشور ما را پشتیبانی می‌کند، از موقعیت خوبی برخوردار است.

۶۶) مشتریان در تصمیم‌گیری در مورد محصولات و خدماتی که خریداری می‌کنند، نقش مهمی را در ترغیب کسب‌وکارها برای ایجاد امنیت مجازی محصولاتشان ایفا می‌کنند. دولت استرالیا به ارزیابی آگاهی مشتریان از اطلاعات لازم برای انتخاب آگاهانه امنیت مجازی هنگام خرید محصولات و خدمات ادامه خواهد داد. اگر مشاوره و راهنمایی داوطلبانه مانند آیین‌نامه کار برای ایجاد تغییر کافی نباشد، شاید لازم باشد اقدام دیگری در نظر گرفته شود. دولت استرالیا با همکاری مشاغل و شرکای بین‌المللی، بهترین گروه ویژهٔ تنظیم مقررات برای امنیت مجازی را ایجاد می‌کند تا با اطمینان از وجود امنیت مجازی در محصولات دیجیتالی، خدمات و زنجیره‌های تأمین، گزینه‌هایی را برای حمایت بهتر از مشتریان در نظر بگیرد. این کار نشان‌دهنده انتظارات جامعه از ایمنی محصول و خطر گسترش آسیب‌پذیری‌ها به دلیل افزایش ارتباط بین دستگاه‌ها است.

آموزش نیروی کار سایبری ماهر

۶۷) نیروی کار قوی و متخصصان ماهر در زمینه امنیت سایبری راه‌گشای اصلی اقتصاد و امنیت دیجیتالی استرالیا هستند. برای حمایت از مشاغل در انجام این اقدامات، این استراتژی شامل برنامهٔ رشد نیروی کار ملی امنیت سایبری است که به کسب‌وکارها و دانشگاه‌ها کمک خواهد کرد تا نیروی کار ماهر سایبری آینده را آموزش دهند. رشد مهارت‌های کانال ارتباطی امنیت مجازی تضمین خواهد کرد که کلیه صاحبان زیرساخت‌ها و اپراتورها و

مشاغل مهم دسترسی بیشتری به متخصصان ماهر امنیت مجازی با مهارت‌های مناسب برای پاسخ‌گویی به درخواست‌ها را داشته باشند. این روند مکمل مراحلی است که دولت استرالیا پیش‌تر برای سرمایه‌گذاری در حمایت از رشد نیروی سایبری انجام داده است.
۶۸) فرصت‌های بزرگتری در اختیار استرالیایی‌هایی قرار می‌گیرد که به دنبال آموزش تخصصی امنیت سایبری در سطح جهانی هستند. صندوق نوآوری مشارکت در مهارت‌های سایبری از برنامه رشد نیروی کار ملی امنیت سایبری با ۲۶/۵ میلیون دلار پشتیبانی می‌کند، که کسب‌وکارها و دانشگاه‌ها را برای یافتن راه‌های جدید و نوآورانه در جهت بهبود مهارت‌های امنیت سایبری به همکاری با یکدیگر ترغیب می‌کند. فعالیت‌هایی که در صندوق مورد قبول واقع می‌شوند، عبارتند از:

- بورس تحصیلی؛
- دوره‌های کارآموزی، یا دوره‌های به سبک کارآموزی در آموزش عالی؛
- توسعه و ارائه دوره‌های تخصصی امنیت سایبری برای افراد حرفه‌ای؛
- ابتکارات بازآموزی، برای کمک به متخصصان حاضر در سایر رشته‌ها در جهت فعالیت‌های مربوط به امنیت سایبری؛
- آموزش یا توسعه حرفه‌ای برای مدرسان و مدیرعاملان از طریق مشارکت عملی یا مبادله با صنعت ؛
- کارآموزی، شغل سازمانی، تبادلات تجربه کاری و کارکنان؛
- پلتفرم‌های آموزش دیجیتال و دانشجویان که خدمات امنیت سایبری ارائه می‌دهند ؛
- هر ایده خلاقانه دیگری برای برآورده کردن نیازهای کسب‌وکارها؛

۶۹) برنامه افزایش نیروی کار امنیت سایبری درصدد است تا مهارت‌های امنیت سایبری را در تمام مراحل آموزش از جمله مقطع مبتدی، متوسطه و عالی افزایش دهد. این امر باعث الهام بخشیدن به نسل بعدی متخصصان امنیت سایبری و مدرسان می‌شود تا امنیت مجازی را در کلاس‌های درس خود بگنجانند. مرکز امنیت سایبری استرالیا برنامه‌های آموزشی، مهارتی، یادگیری، مربیگری و برنامه‌های آماده‌سازی خود از جمله برنامه‌های تخصصی برای زنانی که نقش کمرنگ‌تری در این بخش دارند را توسعه خواهد داد. دولت استرالیا نیز بر مبنای نمونه‌های بین‌المللی، قصد دارد با بهترین روش با مشاغل و دانشگاه‌ها برای ایجاد دوره‌های دانشگاهی در تأمین نیازهای کارفرمایان همکاری کند. این همکاری با در نظر گرفتن این موضوع که چگونه امنیت سایبری می‌تواند برای همیشه در سایر رشته‌ها مانند مهندسی و علوم داده‌ها گنجانده شود، صورت می‌پذیرد. تقویت ارتباطات بین دولت، مشاغل و بخش آموزشی به خصوص به دلیل سرعت تحول در امنیت سایبری از اهمیت زیادی برخوردار است. امنیت سایبری بسیار سریع‌تر از سایر حوزه‌ها توسعه می‌یابد، زیرا تکنولوژی تحول می‌یابد و مجرمان سایبری تاکتیک‌های خود را متناسب با آن تطبیق می‌دهند.

۷۰) کسب‌وکارها و جامعه باید به صنعت امنیت سایبری اعتماد داشته باشند. دولتِ استرالیا با همکاری کسب‌وکارها به بهترین نحو به ارتقای حرفهٔ امنیت سایبری و اطمینان از وجود معیارهای مشخص رسمی برای کارکنان و ثبات بیشتر در بازار برای مشتریان

ادامـه خواهـد داد. ایـن موضـوع در میان‌مـدت و بلندمـدت شـامل بررسـی وجـود نیـاز بـه چهارچوب‌هـای اعتباربخشـی امنیـت سـایبری می‌شـود، از جملـه نحـوه برنامه‌ریـزی بـا سـایر چهارچوب‌هـای مجـوز و اعتبارسـنجی حرفـه‌ای موجـود. بـرای ایجـاد هماهنگـی در بخـش امنیـت مجـازی، ایـن امـر می‌توانـد بـا شـرایط صلاحیـت تخصصـی بـرای حفـظ اعتبـار همـراه باشـد. دولـت اسـترالیا بـه واسـطه تعامـل نزدیـک بـا شـرکای بین‌المللـی بـرای آگاهـی از ارزش ایـن کار و بهتریـن راه بـرای ارائـه و حفـظ ایـن چهارچوب‌هـا در بخـش امنیـت سـایبری، بـا کسـب‌وکارها و شـرکای بین‌المللـی همـکاری خواهـد کـرد.

«آوسـت سـایبر»: «رقابـت جهانـی بخـش امنیـت مجـازی اسـترالیا، در نهایـت موفقیـت آینـده هـرگونـه صنعتـی را در اقتصـاد ملـی تضمیـن مـی کنـد»

بخش امنیت سایبری فرصت‌های مختلفی را ارائه می‌دهد

امنیـت سـایبری یکـی از بخش‌هـای بـا رشـد سـریع در اسـترالیا و جهـان اسـت. اثـر مسـتقیم اقتصـادی آن در سـال‌های ۲۰۱۹-۲۰۲۰ بـا اسـتخدام ۱۹/۴۷۵ نفـر[1]، ۱۵/۷ میلیـارد دلار ارزیابـی شـده اسـت. پیشـرفت سـریع فنـاوری و فضـای تهدیـد در حـال پیشـرفت، تقاضـا را در بخـش امنیـت سـایبری افزایـش می‌دهـد. «آوسـت سـایبر» پیش‌بینـی می‌کنـد تـا سـال ۲۰۲۶ تقریبـاً ۱۷۰۰۰ شـغل جدیـد مـورد نیـاز خواهـد بـود.[2]

فعالیـت دیجیتالـی در سـال‌های ۲۰-۲۰۱۰ بـه طـور مسـتقیم در ایـن زمینـه سـهیم بـود: ۳۱۷ میلیـارد دلار تولیـد ناخالـص بـه اقتصـاد اسـترالیا و

1. AustCyber (2020), Australia's Digital Trust Report 2020, available at https://www.austcyber.com/resource/digitaltrustreport2020
2. AustCyber (2019), Australia's Cyber Security Competitiveness Plan: 2019 Update, available at https://www.austcyber.com/resource/austr alias-cyber-security-sector-competitiveness-plan2019-

۱۰۵ میلیارد دلار (۵/۵٪) به تولید ناخالص داخلی استرالیا کمک کرده و ۵۲۷/۷۲۶ شغل برای اقتصاد استرالیا به ارمغان آورده است.

کار از هر جا

فضای سایبری محدود به جغرافیا نیست. کار در امنیت سایبری به این معنی است که شما مجبور نیستید در حوزه جغرافیایی واحد محدود شوید. فرصت‌هایی برای کسب‌وکارهای امنیت سایبری استرالیا وجود دارد تا راهکارهای خود را به خریداران خارج از کشور بفروشند و توجه سرمایه‌گذاران جهانی را به خود جلب کنند. امنیت مجازی امکان رشد و نوآوری در اقتصاد دیجیتالی را فراهم می‌کند که برای رونق اقتصادی استرالیا و بازیابی از کووید ـ ۱۹ بسیار مهم؛ است زیرا افراد و کسب‌وکارهای بیشتری به صورت آنلاین برای تهیه و ارائه خدمات و کالاها اقدام می‌کنند.

دستمزدهای رقابتی

طرح رقابت‌پذیری در بخش امنیت سایبری «آوست سایبر» حاکی از آن است که دستمزد در کلِ حرفهٔ امنیت سایبری بالا است. این دستمزد با میانگین ۱۲۰۰۰ دلار برای کارمند امنیت سایبری، یعنی بیش از دستمزد یک کارمند فناوری اطلاعات است. سمت‌های مدیریت و رهبری و اشخاصی که سیستم‌های سایبری را طراحی کرده و می‌سازند با میانگین ۲۰۰۰۰ دلار دستمزد، بیشتر از عموم کارمندان فناوری اطلاعات دستمزد می‌گیرند.

نیازی به تخصص در فناوری اطلاعات نیست

یکی از بزرگترین تصورات غلط در مورد حرفهٔ امنیت سایبری لزومِ داشتن پیش‌زمینه در فناوری اطلاعات است. امنیت مجازی بخش گسترده‌ای است که شامل نقش‌های فنی، سیاست‌گذاری، مدیریت ریسک، بازاریابی، مشارکت و موارد دیگر می‌شود. دوره‌های آموزشی مربوط به امنیت مجازی در هر شهر و استانی وجود دارد و بیش از ۸۵۰ دوره در سراسر استرالیا در دسترس است. اطلاعات بیشتر در مورد دوره‌های امنیت سایبری در وب سایت زیر موجود است: www. austcyber.com/educate/ career-paths-and-opportunities

ظرفیت‌های خودکفایی به نفع همه ماست

با توجه به اینکه کووید ـ ۱۹ تمرکز را بر ریسک وابستگی بیش از حد به بازارهای واحد جلب کرده است، اهمیت به تنوع و اطمینان بازار در زنجیره‌های تأمین بیش از هر زمان دیگری حائز اهمیت است.

این مسئله فرصت‌های تجاری برای ظرفیت سایبری خودکفای استرالیا را فراهم می‌کند. در پی همه‌گیری کووید ـ ۱۹، دولت استرالیا به همکاری با صنعت و دانشگاهیان برای ترغیب توسعه ظرفیت‌ها و شرکت‌های مجازی جدید خودکفا در کشور ادامه خواهد داد. مرکز تحقیقات مشارکتی امنیت سایبری با انجام تحقیقات قابل استناد و مبتکرانه برای ایجاد توانایی و ظرفیت امنیت سایبری در استرالیا به طور خاصی برای ایفای نقش اساسی در اجرای این استراتژی در کمک به ادارات و سهامداران اصلی ایجاد شده است.

آیا علاقه‌مند به کار در حوزه امنیت سایبری هستید؟

اداره سیگنال‌های دیجیتالی استرالیا سازمانی بزرگ در استرالیا است که مسئول سه مأموریت مهم، یعنی جمع آوری اطلاعات سیگنال‌ها، اقدامات سایبری تهاجمی و تقویت امنیت سایبری استرالیا است.

اداره سیگنال‌های دیجیتالی استرالیا تقریباً در همه رشته‌ها فرصت‌های شغلی سطح مبتدی را از طریق برنامه عالی خود ارائه می‌دهد. اداره سیگنال‌های دیجیتالی استرالیا دوره کارآموزی را از طریق برنامه کارآموز دیجیتالی دولت استرالیا برای کسانی که به دنبال حرفه‌ای جدید و جالب هستند ارائه می‌دهد. از جمله برای دانشجویانی که در حال تحصیل هستند، یا دیپلم سال ۱۲ خود را به پایان رسانده‌اند، افرادی که در «سی آی تی» یا «تیف» تحصیل می‌کنند و افراد علاقه‌مند به فناوری اطلاعات.

اطلاعات بیشتر در این زمینه در سایت زیر موجود است: www.asd.gov.au/careers

اقدامات انجمن

شرکت «سیسکو»: «داشتن مشتری آگاه و آموزش‌دیده در مورد فضای تهدیدات مجازی می‌تواند ثمربخش‌ترین برنامه‌ای باشد که دولت اجرا کرده است.»

۷۱) بیشتر اتفاقات امنیت سایبری عامل خطای انسانی دارد. به معنی اینکه بسیار مهم است که همه استرالیایی‌ها بدانند چگونه در اینترنت ایمن باشند، مخصوصاً به دلیل اینکه استفاده از فناوری‌های نو برای همه راحت نیست. این استراتژی با فراهم

آوردن ابزارهایی برای انجام این کار به روشی امن، استرالیایی‌ها را در این امر توانمند می‌سازد.

۷۲) استرالیایی‌ها برای امنیت آنلاین چندین کار را باید انجام دهند. مرکز امنیت سایبری استرالیا به ارائه مشاوره و راهنمایی در زمینه امنیت سایبری به بهترین نحو از طریق فروشگاه اینترنتی جامع cyber.gov.au ادامه خواهد داد. این وب سایت کلیه اطلاعات مورد نیاز اشخاص را از طریق اطلاعات جامعی که افراد باید درباره امنیت سایبری بدانند، فراهم می‌کند و در قالب یک شالودهٔ فوق‌العاده برای اقدامات بعدی در جهت ایجاد انعطاف‌پذیری حوزه امنیت سایبری در جامعه عمل می‌کند. دستیابی و به کارگیری این اطلاعات اقدامی است که جامعه می‌تواند برای افزایش امنیت سایبری خود انجام دهد. علاوه بر این، تخصص امنیت سایبری در بخش خصوصی در حال توسعه است که می‌تواند به حفظ امنیت آنلاین در طیف وسیعی از خدمات مانند ارائه نرم‌افزار ضد ویروس برای مشاوره و پاسخ جزئی امنیت سایبری کمک کند.

۷۳) از طریق این استراتژی، دولت استرالیا بر اساس توصیه‌های موجود اطمینان حاصل خواهد کرد که پیام‌های مربوط به امنیت سایبری بیشتر به استرالیایی‌ها می‌رسد. دولت استرالیا در فعالیت جدید افزایش آگاهی عمومی، که با هماهنگی کمپین‌های مربوط به ایمنی آنلاین ارائه می‌شود، سرمایه‌گذاری خواهد کرد (مطالعه موردی زیر را ببینید). دولت استرالیا برنامه جامع آموزش امنیت مجازی آنلاین را نیز برای مشاغل کوچک، افراد مسن و خانواده‌های استرالیایی ارائه می‌دهد که از طریق cyber.gov.au قابل دسترس است.

تفاوت بین ایمنی آنلاین و امنیت سایبری چیست؟

با توجه به اینکه استرالیایی‌ها وقت بیشتری را در اینترنت می‌گذرانند، باید در برابر تهدیدات سایبری و محتوای غیرقانونی و آسیب‌رسان از خود محافظت کنند. امنیت سایبری شامل کمک به استرالیایی‌ها برای ایمنی آنلاین به وسیله محافظت از داده‌ها، اطلاعات، دستگاه‌ها و شبکه‌های ارتباطی در برابر عملگران مخرب است. مرکز امنیت سایبری استرالیا از طریق وبسایت cyber.gov.au، هاب اصلی ارتباط با مردم در زمینه امنیت سایبری است. ایمنی آنلاین شامل محافظت از افراد، خانواده‌ها و جوامع در برابر محتوای آسیب‌رسان و عملکردهایی مانند آسیب رایانه‌ای، سوءاستفاده از تصاویر و محتوای غیرقانونی و آسیب‌رسان آنلاین است. وبسایت esafety.gov.au، مرکز اصلی ارتباط با مردم در حوزه ایمنی آنلاین است. با بیشتر شدن افراد آنلاین در استرالیا بر اثر کووید- ۱۹، دولت استرالیا ۱۰ میلیون دلار دیگر برای پیشرفت تحقیقات ایمنی اینترنتی و تیم‌های پشتیبانی سرمایه‌گذاری کرده است تا در صورت مواجهه با محتوا و عملکردهای آسیب‌رسان به صورت آنلاین، به مردم استرالیا کمک کنند. دولت استرالیا نیاز به ارائه مشاوره صریح و ساده در مورد چگونگی امنیت و ایمنی آنلاین را تصدیق می‌کند. به دلیل این استراتژی، ادارات دولت استرالیا برای ارائه مشاوره صریح در مورد ایمنی آنلاین و امنیت مجازی همکاری نزدیک خواهند داشت. دولت استرالیا همچنین تعامل با دولت را برای کسب‌وکارهای مشتاق به ایمنی آنلاین و امنیت مجازی آسان می‌کند.

۷۴) هر استرالیایی که به مشاوره یا پشتیبانی امنیت سایبری نیاز دارد، باید هرچه سریع‌تر با متخصصان تماس بگیرد. یکی از روش‌های اصلی برای دسترسی به کمک امنیت سایبری، تماس با خط تلفن شبانه‌روزی مرکز امنیت سایبری استرالیا است. اقدامات اولیه می‌توانند از وقوع حادثه جلوگیری کنند یا اگر حادثه‌ای رخ داده باشد، میزان آسیب را کاهش دهد. مرکز امنیت سایبری استرالیا بودجه بیشتری دریافت خواهد کرد؛ بنابراین این خط تلفن می‌تواند خدمات بیشتری ارائه دهد و ظرفیت خود را افزایش دهد.

۷۵) از طریق این استراتژی ، دولت استرالیا حمایت از قربانیان جرایم اینترنتی را در اولویت قرار می‌دهد. گزارش حوادث سایبری به وب سایت ReportCyber روشی مهم برای افراد جامعه است که به ما کمک می‌کند تا بدانیم میزان آسیب مجرمان اینترنتی به استرالیایی‌ها تا چه حد است. قربانی شدن در یک جرم سایبری می‌تواند آسیب‌زا باشد، اما با کمک درست می‌توان تأثیر آن را کاهش داد. راه دیگر برای کمک گرفتن از طریق شناسه رایگان و خدمات پشتیبانی جرایم سایبری «آی دی کر»[1] است. «آی دی کر» قادر است به آسیب‌دیدگان جرایم سایبری در مواقع لزوم پشتیبانی درخور و فعالانه ارائه کند. این استراتژی بودجه بیشتری را برای خدمات پشتیبانی از قربانیان فراهم می‌کند تا به تعداد بیشتری از افرادی که به کمک آن‌ها نیاز دارند، کمک کند. با انجام اقدامات فوق، دولت، کسب‌وکارها و جامعه، دنیای آنلاین امن‌تری را برای استرالیایی‌ها، کسب‌وکار آنها و خدمات ضروری که همه ما به آن وابسته هستیم، ایجاد می‌کنند.

1. IDCARE

کار این استراتژی در اینجا به پایان نمی‌رسد

دولت و کسب و کارها دارای منابع محدودی هستند. اقدامات اشاره شده در این استراتژی، مهم ترین موارد را دربرمی گیرند. فناوری دائماً در حال تغییر است. اقداماتی که برای بهبود امنیت در دنیای آنلاین امروز طراحی شده‌اند، ممکن است به سرعت از فناوری‌های جدید، سیستم‌ها، نرم‌افزارها و برنامه‌ها عقب بمانند.

بنابراین، استرالیا نمی‌تواند فراموش کند، به خصوص اینکه فناوری و تهدیدها همچنان در حال پیشرفت هستند. دولت استرالیا به فعالیت خود با کسب و کارها و جامعه ادامه خواهد داد تا اطمینان حاصل شود که همه همچنان به ایجاد یک دنیای آنلاین امن‌تر برای استرالیایی‌ها، کسب‌وکارهای آنها و خدمات اساسی که همه ما به آن وابسته هستیم، ادامه می‌دهند.

کمیته مشاوران دائمی صنعت (رجوع شود به «اجرا و سنجش پیشرفت») نقشی اساسی در مشاوره وزیر برای اقدامات خاص به عنوان بخشی از این استراتژی در بلندمدت بازی می‌دهد. وزیر به طور دوره‌ای برنامه اقدام این استراتژی را به‌روز می‌کند (در صفحات بعدی) و اقدامات مربوط به افزایش مستمر امنیت سایبری استرالیا را به دولت و جامعه استرالیا گزارش می‌دهد.

چگونه می توانم در فضای مجازی امن بمانم؟

حریم خصوصی

مراقب باشید که چه چیزی را با چه کسی به اشتراک می گذارید.

کلمات عبور

برای امنیت از کلمات عبور قوی استفاده کنید.

پیام رسانی مشکوک

با هرگونه پیام غیرمنتظره با احتیاط رفتار کنید.

گشت و گذار اینترنتی امن

از بدافزار خودداری کنید ـ سایت های معتبر را باز کنید.

امور مالی و پرداخت های آنلاین

جزئیات مالی را از نگاه های کنجکاو دور نگه دارید.

تبلت ها و موبایل ها

هنگام استفاده از وای‌فای رایگان مراقب باشید.

بک آپ و حفاظت

برای حفظ ایمنی بک آپ بگیرید و به روز رسانی کنید.

گزارشات

با گزارش کلاهبرداری همه را در امان نگه دارید.

بخش هفتم

بخش ششم

برنامــه علمی

ابتکار	شرح	چه کسانی سود می برند؟
اقدامات ادارات		
در شرایط اضطرار ملی از زیرساخت‌های مهم محافظت کنید	-دولت استرالیا قوانین جدیدی را وضع خواهد کرد تا از عبور سریع استرالیا از وضعیت اضطراری سایبری اطمینان حاصل کند. این روند شامل ارائه راهنمایی منطقی و متناسب به کسب‌وکارها برای به حداقل رساندن تأثیر حادثه و اقدام مستقیم برای محافظت از سیستم‌ها در مواقع اضطراری است.	- زیرساخت‌ها و سیستم‌های مهم ملی استرالیا در صورت وقوع یک حادثه سایبری قابل توجه، قادر خواهند بود به سرعت بهبود یابند. - همه مشاغل و شهروندان از خدمات ضروری که در اسرع وقت محافظت یا بازیابی می شوند، بهره مند می شوند.
روش‌های پاسخ‌گویی به حوادث را توسعه دهید	-دولت استرالیا ۱۰/۰ میلیون دلار برای برنامه تمرین گسترده ملی سرمایه گذاری خواهد کرد که سازمان‌های مشترک المنافع و دولت را با سازمان‌های بخش خصوصی برای برنامه‌ریزی و آماده‌سازی برای حوادث امنیت سایبری گردهم می‌آورد. -دولت استرالیا همچنین برای گسترش فرایندهای استاندارد مربوط به حوادث امنیت سایبری، با ایالت‌ها و مناطق همکاری خواهد کرد تا به طور رسمی مشارکت‌های تجاری را در پاسخ‌گویی به حادثه‌ای بزرگ شناسایی و برنامه‌ریزی کند.	- زیرساخت‌ها و کسب‌وکارهای حیاتی استرالیا در روند واکنش ملی به حوادث، ایفای نقش کرده و توانایی بهبودی از آنها را توسعه می‌بخشند. - خدمات اساسی که استرالیایی‌ها هر روز به آن اعتماد می‌کنند، در صورت وقوع حادثه قابل توجه سایبری به سرعت بازیابی می‌شوند.

ابتکار	شرح	چه کسانی سود می برند؟
تقویت قابلیت های اجرای قانون، از جمله در دارک وب	-دولت استرالیا ۱۲۴/۹ میلیون دلار برای تقویت توانایی‌های مقابله با جرایم سایبری در بخش اجرای قانون سرمایه‌گذاری خواهد کرد. این مورد شامل سرمایه‌گذاری ۸۹/۹ میلیون دلاری در پلیس فدرال استرالیا برای ایجاد تیم‌های توسعه هدف و تقویت توانایی آن برای پیگیری مجرمان سایبری است. این کار با استفاده از گزارش‌های مرکز تراکنش‌ها و تجربه اطلاعات تخصصی مالی مرکز تحلیل، برای هدف قرار دادن منافع مجرمان سایبری تکمیل خواهد شد. دولت استرالیا اطمینان حاصل خواهد کرد که از اختیارات و توانایی‌های مناسب برای کشف، هدف قرار دادن، تحقیق و اخلال در جرایم سایبری، از جمله در دارک وب برخوردار است. -دولت استرالیا بیش از ۳۱/۶ میلیون دلار سرمایه‌گذاری خواهد کرد تا توانایی مرکز امنیت سایبری استرالیا را برای مقابله با مجرمان سایبری در خارج از کشور و ارائه مشاوره و کمک فنی به سازمان‌های اجرای قانون مشترک المنافع، ادارات و مناطق در شناسایی مجرمان سایبری، گسترش دهد. این مبلغ به ۴۰/۰ میلیون دلار دولت استرالیا برای مقابله با مجرمان سایبری خارجی اضافه می‌شود. این ابتکارات به صورت ترکیبی دولت را قادر می‌سازد تا به جنگ عوامل خارجی بپردازد که استرالیایی‌ها را مورد هدف قرار می دهند.	-بامنصرف شدن مجرمان اینترنتی از هدف قرار دادن استرالیایی‌ها، هزینه‌های جرایم اینترنتی کاهش یافته واقتصاد استرالیا تقویت خواهد شد. - استرالیایی‌ها در برابر جرایم سایبری به شکل بهتری محافظت می شوند.

ابتکار	شرح	چه کسانی سود می برند؟
فناوری اطلاعات حکومت استرالیا را تقویت کنید	-دولت استرالیا با تمرکز بر مدیریت و عملکرد شبکه‌های خود، از جمله با در نظر گرفتن مراکز امن، دفاع از شبکه‌های خود را تقویت می‌کند این تمرکز به دنبال کاهش فرصت برای عوامل مخرب برای هدف قرار دادن آژانس‌های کوچکتر با فناوری اطلاعات با امنیت کمتر است و فرصت‌های تمرکز سرمایه‌گذاری امنیت سایبری دولت استرالیا را افزایش می‌دهد. بندهای استاندارد امنیت سایبری در قراردادهای فناوری اطلاعات دولت وجود خواهد داشت. آژانس های دولتی استرالیا همچنین تمرکز جدیدی بر سیاست ها و فرایندهای مدیریت ریسک های امنیت سایبری خواهند داشت.	- سیستم‌های فناوری اطلاعات دولتی، به عنوان سیستم هایی با اهمیت ملی، ایمن تر خواهند بود. - کسب‌وکارها و شهروندان از امنیت بیشتر داده‌های خود اطمینان خواهند داشت.
اشتراک اطلاعات در زمینه تهدید را توسعه دهید	دولت استرالیا ۳۵/۳ میلیون دلار از طریق مرکز امنیت سایبری سرمایه‌گذاری خواهد کرد تا پورتال اشتراکی جدید همراه پلتفرم چند بعدی دسته بندی تهدیدات ارائه دهد. -دولت استرالیا همچنین ۱/۶ میلیون دلار برای افزایش امنیت سایبری دانشگاه‌های استرالیا سرمایه‌گذاری کرده است. این مبلغ شبکه اشتراک اطلاعات در زمینه تهدید، مدل‌سازی تهدیدات در بخش‌های مختلف و مجمع ملی امنیت سایبری را تأمین مالی خواهد کرد که سالانه سه بار برگزار می‌شود.	- زیرساخت‌ها و کسب‌وکارهای حیاتی استرالیا دسترسی به اطلاعات در زمینه تهدیدها را گسترش می‌دهند و به آنها این امکان را می دهند تا به شکلی بهتر برای تهدیدات سایبری آماده شوند و در برابر آنها مقابله کنند. - فعالیت‌های مخرب سایبری با پیچیدگی کم، قبل از ورود به سیستم‌های کسب‌وکارها و خانوارها متوقف خواهند شد.

ابتکار	شرح	چه کسانی سود می برند؟
قوانین بین‌المللی و موازین مربوط به مسئولیت خود را رعایت کنید	-دولت استرالیا با تحمیل عواقب شدیدتر برای افرادی که برخلاف قوانین بین‌المللی موجود و موازین مورد توافق منافع ملی استرالیا عمل می‌کنند، از فعالیت مجرمانه جلوگیری خواهد کرد.	- دولت‌های مخرب و فعالان تحت حمایت آنها از هدف قرار دادن زیرساخت‌های مهم استرالیا و سیستم‌های دارای اهمیت ملی تحذیر می شوند. - به طور کلی استرالیا کمتر مورد هدف فعالیت‌های سایبری مخرب دولتی قرار خواهد گرفت، که منجر به کاهش هزینه‌ها و حفظ امنیت و حاکمیتمان خواهد شد.
مشارکت‌های امنیت سایبری را تقویت کنید	-دولت استرالیا ۶۷/۹ میلیون دلار برای گسترش برنامه مراکز مشترک امنیت سایبری سرمایه‌گذاری خواهد کرد. طیف گسترده ای از کارکنان و ظرفیت‌های مراکز مشترک امنیت سایبری در جهت افزایش همکاری و حمایت از ادارات ایالتی، منطقه‌ای و محلی، شرکای صنعت و دانشگاه‌ها در سراسر کشور در دسترس خواهد بود. دولت استرالیا ۸/۲ میلیون دلار سرمایه‌گذاری خواهد کرد تا دفتر وزارت کشور در مراکز مشترک امنیت سایبری تأسیس شود و رویکرد کلی حکومت در زمینه امنیت سایبری از این طریق ارائه شود.	-زیرساخت‌های مهم استرالیا، مشاغل و آژانس‌های دولتی برای بهبود اقدامات امنیتی سایبری خود به یک مجمع مشترک دسترسی خواهند داشت.
تعهدات امنیت سایبری را برای کسب و کارهای استرالیایی واضح بیان کنید	-مطابق با نظر هیئت مشاوره صنعت و بازخورد ذی‌نفعان، دولت استرالیا با کسب‌وکارها در زمینه تغییرات احتمالی قوانین همکاری خواهد کرد که تعهدات مربوط به کسب‌وکارهای غیر زیرساختی مهم برای محافظت از خود و مشتریان در برابر تهدیدات امنیت سایبری را واضح بیان می‌کند. در این مشاوره چندین گزینه برای اصلاح، از جمله نقش حریم خصوصی، قوانین حمایت از حقوق مصرف‌کننده، و وظایف مدیران شرکت مورد بررسی قرار خواهد گرفت.	- کسب‌وکارهای استرالیایی به روشنی خواهند دانست که برای محافظت از خود و مشتریانشان چه کاری باید انجام دهند. - اعتماد مصرف‌کنندگان به امنیت محصولات و خدمات افزایش خواهد یافت.

ابتکار	شرح	چه کسانی سود می برند؟
جلوتر از منحنی فناوری باشید	-دولت استرالیا ۱۱۸/۰ میلیون دلار برای گسترش توانایی های علوم‌داده‌ای خود سرمایه‌گذاری خواهد کرد، تا اطمینان حاصل کند که استرالیا در خط مقدم پیشرفت‌های فناوری در امنیت سایبری باقی مانده است.	-با جلوتر رفتن از منحنی تکنولوژی می‌توان از توانایی استرالیا در تقابل با تهدیدات سایبری نوظهور و بهبود مقاومت ملی و ایجاد فرصت‌های اقتصادی برای کسب‌وکارهای امنیت سایبری استرالیا اطمینان حاصل کرد.
اقدامات کسب و کارها		
امنیت پایه زیرساخت های حیاتی را توسعه دهید	-دولت استرالیا حداقل ملزومات امنیت سایبری را برای اپراتورهای دارای زیرساخت‌های حیاتی و سیستم‌های دارای اهمیت ملی اجرا خواهد کرد. دولت استرالیا همچنین نحوه گزارش دهی تهدیدات نافرجام و ریسک‌های خنثی شده را برای قرار گرفتن در یک بازه مطلوب، اصلاح خواهد کرد. برای نیل به این هدف و به عنوان بخشی از تعهدات انتخاباتی دولت استرالیا، مرکز امنیت سایبری کشور ۶۶/۵ میلیون دلار برای کمک به بزرگترین تأمین‌کنندگان زیرساخت‌های مهم استرالیا جهت ارزیابی شبکه‌های خود از نظر آسیب پذیری و تقویت وضعیت امنیت سایبری دریافت خواهد کرد. -دولت استرالیا همچنین ۶۲/۳ میلیون دلار سرمایه‌گذاری خواهد کرد تا شهروندان نسبت به وضعیت کنونی آگاهی داشته باشند تا از این طریق مرکز امنیت سایبری استرالیا بتواند تهدیدات سایبری را در مقیاس ملی درک کرده و پاسخ دهد.	- زیرساخت‌ها و سیستم‌های مهم استرالیا از امنیت بیشتری برخوردار خواهند بود. - کسب‌وکارها و شهروندانی که به زیرساخت‌های مهم وابسته هستند، از ادامه دسترسی به خدمات ضروری بهره مند می‌شوند.

ابتکار	شرح	چه کسانی سود می برند؟
امنیت سایبری کسب و کارهای کوچک و متوسط را ارتقا دهید	-برنامه ۸/۳ میلیون دلاری ارتباط و محافظت از امنیت سایبری، سازمان‌های معتبری مانند اتاق بازرگانی و انجمن‌های تجاری را برای ارتقای امنیت سایبری کسب‌وکارهای کوچک و متوسط در منطقه خود تجهیز خواهد کرد.	-اقتصاد استرالیا از طریق توسعه امنیت سایبری کسب‌وکارهای کوچک و متوسط مستحکم‌تر و انعطاف‌پذیرتر خواهد شد.
اینترنت اشیای امن‌تری فراهم کنید	-دولت استرالیا قانون عملی داوطلبانه امنیت اینترنت اشیا را منتشر می‌کند که باعث می شود دستگاه‌های مورد استفاده خانوارها و کسب‌وکارها از امنیت سایبری بیشتری برخوردار شوند.	- محصولات اینترنت اشیا در استرالیا امنیت سایبری را بهبود داده و هزینه‌های کشور را که هم اکنون تحت تأثیر آسیب‌پذیری دستگاه‌ها است، کاهش می‌دهد. - مصرف‌کنندگان دسترسی بیشتری به دستگاه‌های ایمن اینترنت اشیا خواهند داشت، و در نتیجه کمتر در معرض فعالیت‌های مخرب سایبری قرار خواهند گرفت.
نیروی کار ماهر را رشد دهید	برنامه رشد نیروی کار ملی امنیت سایبری ۵۰/۰ میلیون دلاری نیروی انسانی ماهر، قابل اعتماد و آماده به کار را در کسب و کارها و ادارات تربیت می کند. چهار عنصر زیر در این برنامه گنجانده شده است: -صندوق نوآوری مشارکت ۲۶/۵ میلیون دلاری فرصت‌های جدیدی را برای کسب و کارها و دانشگاه‌ها برای مشارکت در پروژه‌هایِ مهارت نوآورانه ایجاد می کندکه مستقیماً نیازهای مهارتی کارفرمایان را برآورده‌می‌کنند -مرکز امنیت سایبری استرالیا ۶/۳ میلیون دلار برای رشد برنامه‌های آموزشی، مهارتی،	- زیرساخت‌ها و کسب‌وکارهای حیاتی استرالیا با تقویت اقدامات امنیت سایبری خود، به متخصصان ماهر امنیت سایبری دسترسی بیشتری خواهند داشت. - استرالیایی‌ها فرصت‌های جدیدی برای آموزش شغلی در کلاس جهانی امنیت سایبری خواهند داشت.

ابتکار	شرح	چه کسانی سود می برند؟
نیروی کار ماهر را رشد دهید	تمرینی، و مربیگری از جمله برای برنامه های ویژه زنان، دریافت خواهد کرد. -دولت استرالیا ۱۴/۹ میلیون دلار در «کوئستاکون» سرمایه‌گذاری خواهد کرد و کمک می‌کند تا چالش‌ها و دوره‌آموزش معلمان را که دانش آموزان ابتدایی، متوسطه و عالی را برای حرفه امنیت سایبری آماده می‌کنند، طراحی کند. همچنین، ۲/۵ میلیون دلار به جمع آوری اطلاعات بیشتر در مورد کمبود مهارت‌های امنیت سایبری اختصاص خواهد یافت. -برنامه رشد نیروی کار امنیت سایبری، مکمل برنامه ۴۰/۰ میلیون دلاری سرمایه‌گذاری دولت استرالیا به عنوان بخشی از تعهد انتخاباتی خود برای رشد نیروی کار دفاع سایبری است. شخص وزیر کار، مهارت، کسب و کارهای کوچک و خانوادگی این ابتکارات را با صلاحیت‌های آموزش سریع برای بخش فناوری ارتباطات و اطلاعات اعلام خواهد کرد تا نیروی کار استرالیا را به مهارت‌های سایبری‌وامنیت‌دیجیتال،بیشترمجهزکند.	
تهدیدها را به طور خودکار مسدود کنید	-در طول عمر این استراتژی، دولت استرالیا از کسب‌وکارها پشتیبانی خواهد کرد تا فناوری‌های مسدود کردن تهدید را که می‌تواند به طور خودکار شهروندان را در برابر تهدیدات سایبری مخرب محافظت کند، به کار گیرند. دولت استرالیا در نظر خواهد داشت که چگونه می‌تواند قطعیت قانونی را در اختیار ارائه‌دهندگان ارتباطات از راه دور این فناوری قرار دهد.	-کسب‌وکارها و خانواده‌های استرالیایی از مزایای خنثی سازی زود هنگام ریسک‌های سایبری بهره‌مند خواهند شد.

ابتکار	شرح	چه کسانی سود می برند؟
تهدیدها را به طور خودکار مسدود کنید	دولت استرالیا همچنین ۱۲/۵ میلیون دلار در گزینه‌های اصلاحی و استراتژیک جدید، سرمایه‌گذاری خواهد کرد. این بودجه از مشارکت صنعت در زمینه تحقیق و توسعه قابلیت‌های جدید برای شناسایی و جلوگیری از تهدیدات در مقیاس وسیع و برای جلوگیری از آسیب رسیدن به میلیون‌ها استرالیایی در فعالیت‌های مخرب سایبری، پشتیبانی خواهد کرد.	
اقدامات جامعه		
به راهنمایی ها و اطلاعات مربوط به امنیت سایبری دسترسی پیدا کنید	دولت استرالیا انتظار دارد که جامعه طبق توصیه‌های عملی مرکز امنیت سایبری در زمینه امنیت آنلاین عمل کند. براساس این استراتژی، دولت استرالیا به افزایش آگاهی در مورد ریسک امنیت سایبری ادامه خواهد داد. دولت استرالیا ۴/۹ میلیون دلار در پویش آگاه‌سازی عمومی برای افزایش آگاهی استرالیایی‌های آسیب‌پذیر سرمایه‌گذاری خواهد کرد. دولت استرالیا با کسب‌وکارهای بزرگ مانند بانک‌ها و ارائه‌دهندگان خدمات اینترنت همکاری خواهد کرد تا اطمینان حاصل کند که کسب‌وکارهای کوچک و متوسط در روند عادی کار خود به اطلاعات امنیت سایبری دسترسی دارند. دولت استرالیا ابزارهایی را توسعه می‌دهد که کسب‌وکارهای کوچک و متوسط می توانند برای بالا بردن سطح آگاهی نسبت به امنیت سایبری کارکنان خود از آنها استفاده کنند. دولت استرالیا کسب‌وکارهای بزرگ را تشویق می‌کند تا مجموعه ابزارها را به عنوان بخشی از بسته	- آگاهی بیشتر جامعه کاهش هزینه فعالیت‌های مخرب سایبری برای کسب‌وکارها و تقویت اقتصاد استرالیا را به همراه خواهد داشت. - آگاهی بیشتر جامعه باعث کاهش اثر جرایم سایبری بر خانواده‌های استرالیایی می‌شود و خانواده‌ها را از آسیب محافظت می‌کند

ابتکار	شرح	چه کسانی سود می برند؟
به راهنمایی‌ها و اطلاعات مربوط به امنیت سایبری دسترسی پیدا کنید	ایمن خدمات، در اختیار کسب‌وکارهای کوچک قرار دهند. مرکز امنیت ملی سایبری آموزش آنلاین امنیت سایبری را به کسب‌وکارهای کوچک و متوسط، استرالیایی‌های مسن و خانواده‌ها ارائه می‌دهد. این اقدام همچنین سرمایه ۱۰/۰ میلیون دلاری دولت استرالیا برای تقویت تحقیقات امنیت سایبری و تیم‌های پشتیبانی را تکمیل می‌کند تا در صورت مواجهه با محتوا و رفتارهای مضر به صورت آنلاین، از این طریق به استرالیایی‌ها کمک‌رسانی شود.	
در صورت لزوم به کمک و پشتیبانی دسترسی پیدا کنید	همه استرالیایی‌هایی که از نحوه حضور امن در فضای سایبری اطلاع ندارند و همچنین آنهایی که قربانی جرایم سایبری شده‌اند، باید از کمک و پشتیبانی برخوردار شوند. دولت استرالیا ۵۸/۳ میلیون دلار برای افزایش کانال‌های تعامل با مشتری و ۱۲/۳ میلیون دلار برای گسترش مرکز خدمات امنیت سایبری دائمی در کسب‌وکارهای کوچک و متوسط و خانواده‌ها، سرمایه‌گذاری خواهد کرد. این امر ارائه مشاوره امنیت سایبری و کمک فنی به تمام استرالیایی‌ها را بهبود می‌بخشد، ابزار گزارش حادثه «ریپورترسایبر» را توسعه می‌بخشد، و منابع آنلاین اضافی و مشاوره و اطلاعات عملی و ویژه‌ای را برای همه استرالیایی‌ها فراهم می‌کند این روند همچنین سرمایه ۲۶/۰ میلیون دلاری دولت استرالیا برای حمایت از مرکز امنیت ملی سایبری در جهت گسترش کمک به کسب‌وکارهای کوچک و بزرگ و جامعه را تکمیل می‌کند	قربانیان جرایم اینترنتی، از جمله کسب‌وکارهای کوچک و بزرگ، دسترسی بیشتری به خدمات پشتیبانی خواهند داشت.

ابتکار	شرح	چه کسانی سود می برند؟
در صورت لزوم به کمک و پشتیبانی دسترسی پیدا کنید	دولت استرالیا همچنین ۶/۱ میلیون دلار برای تقویت خدمات به قربانیان جرایم سایبری کمک خواهد کرد.	
به هنگام خرید، با اطلاعات کافی تصمیم گیری کنید	همه مصرف‌کنندگان هنگام خرید دستگاه‌های دیجیتال نیاز به تصمیم‌گیری هوشمندانه در زمینه امنیت سایبری دارند. از طریق این استراتژی، دولت استرالیا میزان اطلاعات موجود برای مصرف‌کنندگان در مورد آنچه را که هنگام خرید یک محصول باید جستجو کنند، افزایش می‌دهد. این اطلاعات در وبسایت cyber.gov.au در دسترس خواهد بود. دولت استرالیا در درازمدت، بررسی خواهد کرد که آیا برای اطلاع‌رسانی به مصرف‌کنندگان، مانند برچسب‌گذاری محصولات امنیت سایبری، به مراحل دیگری نیاز است یا خیر.	مصرف‌کنندگان هنگام خرید دستگاه دیجیتال می‌دانند که باید دنبال‌کدام ویژگی‌های امنیت سایبری باشند.

بخش هشتم

بخش هشتم

اجرا و سنجش پیشرفت

۷۶) دولت استرالیا اهمیت اجرا و ارزیابی راهبردی قوی را برای این استراتژی به رسمیت می‌شناسد.

۷۷) وزیر کشور مسئولیت اصلی ارائه این استراتژی را با پشتیبانی سایر وزرا در صورت لزوم بر عهده دارد. هیئت استراتژی امنیت سایبری، به رهبری یک مقام ارشد امور داخلی، مسئول اجرای روزمره این استراتژی خواهد بود.

۷۸) کمیته مشاوره صنعت نیز برای هدایت اجرای این استراتژی تشکیل خواهد شد. کمیته مشاوره صنعت درباره راه‌های مقابله با چالش‌های امنیت سایبری استرالیا مشاوره مداوم خواهد داد و مستقیماً به وزیر کشور گزارش می‌دهد. این کمیته گزارش‌هایی عمومی درباره پیشرفت این استراتژی ارائه می‌دهد. این روند به موفقیت هیئت مشاوره صنعت است که در تهیه این استراتژی کمک کرده است، می‌افزاید.

ابتکار	چگونه دولت استرالیا موفقیت را می‌سنجد؟
اقدامات ادارات	
در شرایط اضطراری ملی از زیرساخت‌های مهم محافظت کنید	- اقدامات لازم برای پاسخگویی به موقع و مؤثر دولت استرالیا در برابر رخدادهای امنیت سایبری شکل گرفته است. - تهدیدات پیش روی زیرساخت‌های حیاتی و سیستم‌های دارای اهمیت ملی بیشتر به چشم می‌آید، و اطلاعات تقریباً در زمان حقیقی برای کسانی که برای دفاع فعال از شبکه‌ها به آن نیاز دارند، در دسترس است.
روش‌های پاسخگویی به حوادث را توسعه دهید	- تنظیمات به‌روزشده مدیریت حوادث سایبری خلاصه‌ای از نحوه افزایش آمادگی ادارات و کسب‌وکارها برای پاسخگویی جمعی به یک حادثه مهم ملی را خلاصه می‌کند - آژانس‌های دولتی و سازمان‌های بخش خصوصی، میزان آمادگی و مقاومت خود را تقویت کرده‌اند.
تقویت قابلیت‌های اجرای قانون، از جمله در دارک وب	- از طریق قابلیت های بهبودیافته و هماهنگی های بیشتر، پلیس فدرال استرالیا، کمیسیون اطلاعات جنایی استرالیا و مرکز امنیت سایبری اهداف جرایم سایبری بیشتری را شناسایی و خنثی می‌کنند - آژانس‌ها قدرت کشف، مورد هدف قرار دادن، تحقیق و خنثی‌سازی جرایم سایبری را دارند. - واکنش به جرایم آنلاین میان دولت استرالیا، ادارات و مناطق هماهنگ شده است.
فناوری اطلاعات دولت استرالیا را تقویت کنید	-متمرکز شدن شبکه های فناوری اطلاعات دولت استرالیا دفاع در برابر فعالیت‌های مخرب را آسان می‌کند
اشتراک اطلاعات در حوزه تهدیدات را توسعه دهید	- دولت و کسب‌وکارها تهدیدات سایبری را تقریباً در زمان حقیقی شناسایی می‌کنند - جریان اطلاعات دو طرفه امنیت سایبری افزایش یافته است.

ابتکار	چگونه دولت استرالیا موفقیت را می‌سنجد؟
قوانین بین‌المللی موجود و هنجارهای رفتار مسئولانهٔ دولت در فضای سایبری را تقویت کنید	- پاسخ استرالیا به رفتارهای غیرقابل قبول در فضای سایبری، با قوانین بین‌المللی و هنجارهای مربوط به رفتار مسئولانهٔ دولت در فضای مجازی همسو است. - استراتژی جدید روابط بین‌المللی در حوزه سایبری و فناوری حیاتی به اجرا درآمده است.
مشارکت ها را در زمینه امنیت سایبری را تقویت کنید	-داده‌های به دست آمده از بررسی تجربه مشتری، مشارکت مؤثر بین کسب‌وکارها و دولت را نشان می‌دهد.
تعهدات امنیت سایبری را برای کسب‌وکارهای استرالیایی به وضوح بیان کنید	-به منظور روشن‌سازی تعهدات امنیت سایبری برای کسب‌وکارها استرالیایی، مشاوره‌ای درباره اصلاحات احتمالی آینده ارائه می‌شود.
جلوتر از منحنی فناوری باشید	-دولت استرالیا توانایی تحقیق مستقل برای ارزیابی آسیب‌پذیری‌های فناوری نوظهور را دارد.
اقدامات کسب‌وکارها	
امنیت پایه زیرساخت‌های حیاتی را توسعه دهید	- الزامات واضح امنیت سایبری برای تأمین‌کنندگان زیرساخت‌های مهم بدون در نظر گرفتن تنظیمات مالکیت وجود دارد. - دولت در زمان حقیقی به اطلاعات مربوط به حوادث امنیتی سایبری و تهدیداتی که در لحظات آخر خنثی شده‌اند، دسترسی دارد. - ارائه‌دهندگان زیرساخت‌های حیاتی برای توسعه امنیت سایبری خود پشتیبانی می‌شوند.

ابتکار	چگونه دولت استرالیا موفقیت را می‌سنجد؟
امنیت سایبری کسب‌وکارهای کوچک و متوسط را ارتقا دهید	-تعداد فزاینده ای از کسب‌وکارهای کوچک در حال توسعه اقدامات مربوط به امنیت سایبری خود هستند.
اینترنت اشیای امن‌تری ایجاد کنید	-کسب‌وکارها درک بهتری از بهترین روش‌ها برای کنترل‌های امنیتی اینترنت اشیا دارند.
نیروی کار ماهر را رشد دهید	- داده‌های نظرسنجی نشان‌دهنده افزایش در دسترس بودن کارمندان امنیت سایبری آماده به کار است. - کسب‌وکارها و دانشگاه‌ها برنامه‌های ابتکاری را برای تأمین نیازهای بومی توسعه می‌دهند. - بیشتر دانش آموزان مقاطع ابتدایی، راهنمایی و متوسطه برای فعالیت در زمینه امنیت سایبری انگیزه می‌گیرند
تهدیدها را به طور خودکار مسدود کنید	-از آسیب‌های سایبری به استرالیایی ها جلوگیری می‌شود.
به راهنمایی‌ها و اطلاعات مربوط به امنیت سایبری دسترسی پیدا کنید	- معیارهای تغییر دستیابی و رفتار در پویش های آگاه‌سازی نشان می‌دهد که راهنمایی مؤثری ارائه شده است. - کمیته مدیران آژانس ایمنی آنلاین، بر تعدادی از پویش‌ها نظارت می‌کند
در صورت لزوم کمک و پشتیبانی بخواهید	- افزایش دسترسی و کیفیت خدمات پشتیبانی برای قربانیان جرایم اینترنتی. - افزایش دسترسی به مشاوره و مساعدت امنیت سایبری برای همه استرالیایی‌ها، از جمله از طریق پشتیبانی شبانه‌روزی مرکز امنیت سایبری استرالیا.

ابتکار	چگونه دولت استرالیا موفقیت را می‌سنجد؟
به‌هنگام خرید، با اطلاعات کافی تصمیم گیری کنید	-آگاهی جامعه از نحوه خرید محصولات و خدمات دیجیتالی ایمن.
جرایم سایبری را گزارش دهید	-افزایش درک تأثیرات جرایم سایبری بر جامعه.

جمع بندی

جمع‌بندی

پیوست الف: تعهدات مالی استراتژی امنیت سایبری ۲۰۲۰

اقدام	هزینه
ارتقای آگاهی و واکنش متناسب با موقعیت در فضای سایبری	۱/۳۵۰/۰ میلیون دلار
کمک به تأمین‌کنندگان مهم زیرساخت‌ها	۶۶/۵ میلیون دلار
برنامه گسترش یافته تمرین ملی	۱۰/۰ میلیون دلار
مراکز مشترک تغییر شکل یافته امنیت سایبری	۶۷/۹ میلیون دلار
ارتقای تعامل با مشتری	۵۸/۳ میلیون دلار
گسترش مرکز خدمات امنیت سایبری، برای مشاغل کوچک و خانواده‌ها	۱۲/۳ میلیون دلار
گسترش و توسعه اختلال در جرایم سایبری خارج از کشور	۳۱/۶ میلیون دلار
ارتقای پلتفرم به اشتراک‌گذاری تهدیدات سایبری	۳۵/۳ میلیون دلار
بازدارنده‌های استراتژیکی جدید	۱۲/۵ میلیون دلار
گسترش قابلیت‌های علوم داده	۱۱۸/۰ میلیون دلار
قابلیت جدید آگاهی از وضعیت ملی	۶۲/۳ میلیون دلار
آزمایشگاه‌های تحقیقات فناوری‌های نوظهور	۲۰/۲ میلیون دلار

اقدام	هزینه
پرسنل اداره سیگنال‌های استرالیا	۴۶۹/۷ میلیون دلار
قابلیت‌های اطلاعاتی و مدیریت برنامه	۳۸۵/۴ میلیون دلار
تقویت توانایی مقابله با جرایم اینترنتی استرالیا	۱۶۴/۹ میلیون دلار
تقویت قابلیت‌های اجرای قانون	۱۲۴/۹ میلیون دلار
ایجاد توانایی مقابله با مجرمان سایبری خارجی در مرکز امنیت سایبری استرالیا	۴۰/۰ میلیون دلار
رشد مهارت‌ها در استرالیا	۹۰/۲ میلیون دلار
صندوق نوآوری مشارکت مهارت‌ها	۲۶/۵ میلیون دلار
برنامه‌های آموزشی و تمرینی مرکز امنیت سایبری استرالیا	۶/۳ میلیون دلار
جمع‌آوری داده‌ها	۲/۵ میلیون دلار
ارتقای مهارت‌های سایبری برای دانش آموزان و معلمان	۱۴/۹ میلیون دلار
نیروی کار دفاعی سایبری را رشد دهید	۴۰/۰ میلیون دلار
پشتیبانی از شرکت‌های کوچک و متوسط و استرالیایی‌های آسیب‌پذیر	۶۳/۴ میلیون دلار
گسترش پشتیبانی مرکز امنیت سایبری استرالیا از شرکت‌های کوچک و متوسط	۲۶/۰ میلیون دلار
مشاوره و کمک «برنامه اتصال و محافظت» به کسب‌وکارهای کوچک و متوسط از منابع معتبر	۸/۳ میلیون دلار
گسترش دسترسی صنعت و ظرفیت همکاری ملی	۸/۲ میلیون دلار
آگاهی خانواده‌های استرالیایی و کسب‌وکارهای کوچک از امنیت سایبری	۴/۹ میلیون دلار
تقویت تیم تحقیق و پشتیبانی «ای ـ سیفتی»	۱۰/۰ میلیون دلار

اقدام	هزینه
حمایت از قربانیان جرایم اینترنتی	۶/۱ میلیون دلار
افزایش امنیت سایبری دانشگاه‌ها	۱/۶ میلیون دلار
مجموع	**۱/۶۷۰/۰ میلیون دلار**

جمع مبلغ ممکن است به دلیل رند شدن دقیق نباشد.

برای اطلاعات بیشتر در زمینه امنیت سایبری به کجا می‌توانم مراجعه کنم؟

در صورت تهدید زندگی یا ریسک آسیب، لطفا با شماره تلفن ۰۰۰ تماس بگیرید.

در موارد غیر اضطراری، وبسایت cyber.gov.au مرجع مشاورهٔ به‌روز در زمینه امنیت سایبری است و منابع امنیتی سایبری را ارائه می‌دهد و می‌توانید حوادث زیر را در این وبسایت گزارش دهید:

- **سوءاستفاده سایبری ـ** اگر شخصی در فضای آنلاین از شما سوءاستفاده می‌کند، شما را مورد آزار و اذیت قرار می‌دهد یا شما را مخفیانه تعقیب می‌کند.
- **سوءاستفاده از تصاویر ـ** اگر شخصی تصاویر یا فیلم‌های خصوصی شما را به صورت آنلاین به اشتراک گذاشته یا تهدید به اشتراک‌گذاری می‌کند.
- **کلاهبرداری در خرید آنلاین یا کلاهبرداری در رابطه احساسی ـ** در صورتی که در ارسال پول یا کالا به یک شخص در فضای آنلاین فریب خوردید.

- **سرقت هویت** - اگر شخصی از اطلاعات شخصی یا شغلی شما استفاده کرده و به حساب‌های آنلاین شما دسترسی پیدا کرده باشد.

- **کلاهبرداری از طریق ایمیل ـ** اگر ایمیلی حاوی اطلاعات جعلی دریافت کرده‌اید که قصد فریب شما را دارد تا مبلغی را واریز کنید.

- کلاهبرداری‌اینترنتی ـ اگر روی پیوند فیشینگ کلیک کرده‌اید یا به کسی دسترسی از راه دور به رایانه یا دستگاه خود را داده‌اید و ممکن است از حساب‌های شما پول دریافت شود.

- **باج افزار یا بدافزار ـ** اگر به سیستم یا دستگاه‌های شما آسیب وارد شود و شخصی درخواست پول کند.

پس از تهیه گزارش، مرکز امنیت سایبری استرالیا اطمینان حاصل می‌کند که گزارش شما به دست همه ارگان‌های دولتی مربوطه و پلیس رسیده باشد.

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