مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

گزارش سریع
چهل و سوم

استراتژی ملی امنیت سایبری در یونان

National Cyber Security Strategy in Greece

بسم الله الرحمن الرحیم

گزارش سریع

گزارش شماره ۴۳
شهریور ۱۴۰۱

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

استراتژی ملی امنیت سایبری در یونان

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

تهیه شده در پژوهشگاه فضای مجازی
(گروه مطالعات بین‌الملل)

ترجمه: مینا راستی
ناظر: عباس قنبری باغستان

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

فهرست

سخن نخست

سخن نخست

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

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

سیدابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

مقدمه

مقدمه

سند پیش رو، استراتژی ملی امنیت سایبری یونان را توضیح می‌دهد در حال حاضر، برنامه ریزی مرکزی دولت یونان در حوزه امنیت سایبری بر اساس این سند در حال توسعه است.

با توجه به اینکه استفاده از اینترنت و فناوری‌های اطلاعات و ارتباطات[1] در تمامی فعالیت های بخش دولتی و خصوصی در حال رشد است، لازم است بر ایجاد محیط آنلاین، زیرساخت ها و خدمات ایمن تأکید ویژه ای شود تا بدین طریق، اعتماد شهروندان افزایش یابد و آنها به سمت استفاده بیشتر از محصولات و خدمات دیجیتالی جدید سوق داده شوند. فراهم ساختن محیطی امن همراه با ترویج خدمات و محصولات جدید از یک طرف و حفظ حریم خصوصی و حقوق شهروندان در دنیای دیجیتال جدید از طرفی دیگر، شرایطی اساسی برای تقویت و ارتقای توسعه اقتصادی در یونان محسوب می‌شوند

استراتژی ملی امنیت سایبری، اصول اصلی ایجاد فضای آنلاین ایمن در یونان را فراهم و اهداف استراتژیک و چارچوب عملیاتی برای تحقق آنها را نیز تعیین می‌کند اهداف و اقدامات فردی برای دستیابی به این عوامل در ادامه با جزئیات شرح داده شده است.

1. ICTs

اجرای استراتژی ملی امنیت سایبری بر عهده سازمان ملی امنیت سایبری[1] است که با هدف ترمیم شکاف سازمانی و هماهنگی میان ذینفعان حوزه امنیت سایبری در یونان، چه در بخش دولتی و چه در بخش خصوصی، ایجاد شده است. به علاوه سازمان ملی امنیت سایبری در صورت لزوم و حداکثر هر سه سال یکبار، استراتژی ملی امنیت سایبری را ارزیابی، بازنگری و به روز خواهد کرد.

1. National Cyber Security Authority

بخش اول

بخش اول

معرفی

استفاده روز افزون از فناوری اطلاعات و ارتباطات امکان انتقال، پردازش و ذخیره‌سازی حجم گسترده‌ای از داده‌ها را فراهم می‌کند که جوامع امروزی بیش از پیش از آنها برای پیشرفت اقتصادی، اجتماعی، فناوری، فرهنگی و علمی خود بهره می‌برند. در عین حال، دسترسی گسترده به اینترنت امکان دستیابی مستقیم به این داده‌ها و تبادل اطلاعات را فراهم می‌کند، و بنابراین زندگی اجتماعی و اقتصادی را تا حد زیادی تغییر می دهد. اقتصاد، تجارت و کسب و کارها برای پیشرفت بیشتر خود بیش از پیش به زیرساخت‌های دیجیتال متکی هستند. مدیریت دولتی انتظار دارد که فناوری دیجیتال به ابزاری برای بهبود خدمات ارائه شده تبدیل شود و به استفاده منطقی از منابع اطلاعاتی منتج شود. دسترسی آزاد و رایگان به اینترنت و محرمانه بودن، یکپارچگی، امکان دسترسی و انعطاف پذیری سیستم‌های فناوری اطلاعات و ارتباطات زمینه‌ای برای رفاه، امنیت ملی و همچنین حفاظت از حقوق و آزادی های اساسی فراهم می‌کند.

از آنجا که جامعه ما بیشتر و بیشتر به سیستم‌های اطلاعاتی و ارتباطی متکی می‌شود، لذا امنیت آنها به یکی از موضوعات اصلی در منافع ملی

1. Cyber Attacks

بدل شده است. در عین حال، محافظت از کاربران خدمات دیجیتال، به ویژه جوانان، به شکل فزاینده‌ای ضروری است. اصطلاح «امنیت سایبری» به تمام کارها و اقدامات مناسبی گفته می‌شود که برای اطمینان از حفاظت از فضای سایبری در برابر تهدیدهای مرتبط با فضای سایبری اتخاذ می‌شود. این تهدیدها می‌توانند به سیستم های متقابلاً وابسته فناوری اطلاعات و ارتباطات آسیب وارد کنند. استراتژی ملی امنیت سایبری، ابزاری برای ارتقای امنیت آنلاین از طریق اطمینان نسبت به یکپارچگی، امکان دسترسی و انعطاف‌پذیری زیرساخت‌های مهم و محرمانه بودن اطلاعات دیجیتالی منتقل شده است؛ به طوری که اصول جامعه باز، آزادی‌های اساسی و حقوق فردی نیز حفظ شود.

بخش دوم

بخش دوم

اصول و اهداف کلی

رشد و محافظت از خدمات و بازارهای دیجیتالی ستون اصلی حمایت از اقتصاد ملی است که مزیت رقابتی در سطح ملی و اروپایی را به همراه دارد. در حالی که تجربه یونان همچنان در رشد و سرمایه‌گذاری در بازارها، شبکه‌ها و خدمات دیجیتالی، چه در بخش دولتی و چه در بخش خصوصی ادامه دارد، ایجاد استراتژی ملی امنیت سایبری ضرورت محسوب می‌شود. اصول اصلی استراتژی ملی امنیت سایبری عبارتند از:

الف) توسعه و استقرار فضای سایبری امن و مقاوم که مطابق با قوانین، استانداردها و اقدامات مناسب ملی و بین‌المللی و متناسب با مقررات اتحادیه اروپا تنظیم خواهد شد که طبق آن شهروندان و ذی‌نفعان بخش دولتی و خصوصی می‌توانند فعال بوده و به طور ایمن تعامل داشته باشند. این تعامل باید بنا بر ارزش‌های حاکم بر قوانین باشد، مانند ارزشهایی که بر آزادی، عدالت و شفافیت دلالت کنند؛

ب) بهبود مستمر توانایی‌های ما برای محافظت در برابر حملات سایبری، با تأکید بر زیرساخت‌های حیاتی و حفاظت از تداوم عملیاتی؛

ج) محافظت نهادی از چارچوب ملی امنیت سایبری، برای رسیدگی مؤثر به حوادث حمله سایبری و به حداقل رساندن تأثیر تهدیدات فضای مجازی؛

د) توسعه فرهنگ قوی امنیت در شهروندان و بخش‌های دولتی و خصوصی، با استفاده از توانایی‌های مرتبط جامعه دانشگاهی و سایر ذی‌نفعان بخش دولتی و خصوصی؛

اهداف جداگانه استراتژی ملی امنیت سایبری را می‌توان به صورت زیر خلاصه کرد:

۱) ارتقای سطح پیشگیری، ارزیابی، تحلیل و جلوگیری از تهدیدات علیه امنیت سیستم‌ها و زیرساخت‌های فناوری اطلاعات و ارتباطات؛

۲) افزایش توانایی ذی‌نفعان بخش دولتی و خصوصی در جلوگیری و کنترل حوادث امنیتی سایبری و بهبود انعطاف‌پذیری و بازیابی سیستم های فناوری اطلاعات و ارتباطات پس از حمله سایبری؛

۳) ایجاد یک چارچوب هماهنگی و همکاری مؤثر با تعیین صلاحیت ها و نقش‌های فردی ذی‌نفعان مختلف بخش دولتی و خصوصی در اجرای استراتژی ملی امنیت سایبری؛

۴) اطمینان از مشارکت فعال یونان در اقدامات بین‌المللی امنیت سایبری و اقدامات سازمان‌های بین‌المللی در جهت افزایش امنیت ملی؛

۵) آگاهی کلیه نهادهای اجتماعی و آگاهی کاربران درباره استفاده ایمن از فضای سایبری؛

۶) تطابق مداوم چارچوب نهادی ملی با الزامات جدید فناوری و دستورالعمل‌های اتحادیه اروپا برای رسیدگی مؤثر به اعمال غیرقانونی مرتبط با فعالیت در فضای سایبری؛

۷) ارتقای نوآوری، تحقیق و توسعه در مسائل امنیتی و همکاری میان ذی‌نفعان؛

۸) استفاده از بهترین روش‌های بین‌المللی.

تصویب، اجرا و نظارت بر استراتژی ملی امنیت سایبری در ایجاد یک قانون قدرتمند، با سطح بالایی از امنیت و انعطاف‌پذیری در برابر تهدیدات سایبری، با احترام به حریم خصوصی، حقوق فردی و اجتماعی همراه خواهد بود. علاوه بر این، خدمات الکترونیکی با کیفیت به شهروندان و کسب‌وکارها ارائه می‌شود. این خدمات در عین حال همچون اهرمی برای رشد اقتصاد و کسب‌وکارها همراه تنظیم قوانین مشترک برای همه ذی‌نفعان دخیل عمل می‌کنند.

بخش سوم

بخش سوم

چهارچوب عملیاتی ـ اهداف استراتژیک

استراتژی ملی امنیت سایبری از دو مرحله جداگانه تشکیل شده است که شامل توسعه و اجرای استراتژی در مرحله نخستین و ارزیابی و بررسی آن در مرحله دوم می‌شود. این مراحل چرخه مداوم استراتژی ملی را تعیین می‌کنند؛ بدین معنا که استراتژی ملی ابتدا تدوین و اجرا می شود، سپس براساس شاخص‌های ارزیابی از پیش تعیین شده ارزیابی می‌شود و در صورت لزوم اصلاح و به روز می شود.

ذی‌نفعان به دو سطح استراتژیک و عملیاتی تقسیم می‌شوند. سازمان ملی امنیت سایبری که طبق فرمان ریاست جمهوری ۲۰۱۷/۸۲ [1] در دبیرخانه عمومی سیاستگذاری دیجیتال وزارت ارتباطات دوربرد و رسانه‌های سیاست دیجیتال تأسیس شده و فعالیت می‌کند، در سطح بالاتر سیاسی و دولتی ذی‌نفع است. این سازمان با صلاحیت‌های گسترده‌ای که دارد، استراتژی ملی امنیت سایبری را نظارت و اجرا کرده و مسئولیت کلی آن را بر عهده دارد. سازمان ملی امنیت سایبری می‌تواند وظایف خود را با مشارکت یک نهاد / انجمن مشورت ملی اجرا کند، که در آن ذی‌نفعان بخش دولتی و خصوصی با همکاری نزدیک با تیم ملی واکنش اضطراری رایانه‌ای [2] می‌توانند شرکت کنند. این سازمان در چارچوب مسئولیت‌های

1. A117
2. CERT

خود، فعالیت‌های ذی‌نفعان را برای دستیابی به اقدامات و اهداف استراتژیک نظارت، هماهنگی و ارزیابی خواهد کرد. سطح عملیاتی از میان موارد دیگر، شامل تیم های واکنش به اتفاقات مربوط به امنیت رایانه‌ای[1] می‌شود که همچنین به عنوان تیم های واکنش اضطراری رایانه‌ای در بخش دولتی و خصوصی شناخته می‌شود که مسئولیت رسیدگی به حوادث سایبری (دفاع سایبری) را بر اساس صلاحیت‌های خود بر عهده دارند.

چارچوب اقدامات لازم برای اجرای استراتژی ملی امنیت سایبری در زیر تعریف شده است:

۳-۱- تعیین ذی‌نفعان شرکت کننده در استراتژی ملی امنیت سایبری

استراتژی ملی عمدتاً وابسته به ذی‌نفعانی است که در عملکرد روان جامعه حیاتی هستند.

بنابراین ضروری است تا ذی‌نفعان دولتی و خصوصی مرتبط با این موضوع به طور صریح تعیین شوند، چرا که به توسعه و اجرای استراتژی ملی کمک می‌کنند

۳-۲ -تعریف زیرساخت‌های حیاتی

تعریف و ثبت زیرساخت‌های حیاتی (هم در بخش دولتی و هم در بخش خصوصی) و وابستگی متقابل آنها.

۳-۳- ارزیابی ریسک در سطح ملی

تهیه مطالعه ارزیابی ریسک در سطح ملی به دنبال روش علمی و فناوری است

1. CSIRTs

کـه بـه طور خلاصه باید بر اسـاس شناسـایی، تحلیـل و ارزیابی تأثیر ریسـک اسـتوار باشـد و به تعیین برنامه‌ای بـرای حفاظت از زیرسـاخت‌های حیاتی در هـر بخـش یـا برای هـر ذی‌نفع منتج شـود. این مطالعه که هر سـه سـال یک بـار بازنگری می‌شـود، تمـام تهدیدات احتمالی بـه ویژه تهدیدهـای مربوط به اقدامـات مخـرب (بـرای مثـال جرایم سـایبری، حملات سـایبری) و همچنین ریسـک‌های مربـوط بـه پدیده‌هـای طبیعـی، نقـص فنـی یـا نقـص عملکرد و خطـای انسـانی را در نظـر خواهد گرفت. تهدیدات ناشـی از وابسـتگی متقابل سیسـتم‌های اطلاعاتـی و ارتباطی ذی‌نفعان شـرکت‌کننده در اسـتراتژی ملی نیـز مـورد بررسـی قـرار خواهد گرفـت. این در حالی اسـت که میزان و شـدت تأثیرات در سـطح ملی بیشـتر بررسـی خواهد شـد.

۴-۳-ثبت و توسعه چارچوب سازمانی فعلی

مرحلـه اصلـی توسـعه و اجـرای اسـتراتژی ملـی شـامل ثبـت و ارزیابـی چارچوب سـازمانی فعلی و سـاختارهای موجود برای تحقق اهداف اسـتراتژی ملی اسـت:

- قانونگـذاری، نقش‌هـا و صلاحیت‌هـای ذی‌نفعـان مرتبـط بـا امنیـت سـایبری (بـرای مثال، پـردازش اطلاعات شـخصی، ارتباطـات الکترونیکی، حفظ محرمانگی ارتباطات، یکپارچگی و در دسـترس بودن شـبکه و غیره)؛
- اقدامـات نظارتـی، ویـژه هـر بخـش (برای مثـال بانکـداری) و تأثیـر آنها تاکنـون در بهبـود امنیـت سـایبری (بـرای مثـال قانونگـذاری هـاو نقـش شـنودی بانـک مرکـزی یونان)؛
- سـاختارها، ذی‌نفعـان و خدمـات بخـش دولتـی یـا خصوصـی بـا نقـش عملیاتـی در حفاظـت از امنیـت سـایبری (بـرای مثـال تیـم هـای واکنش به

حوادث امنیت رایانه ای[۵]؛

• برنامه‌های اضطراری موجود مانند «Xenokrates»، «Egnatia» و غیره؛

• مقررات اتحادیه اروپا و سایر دستورالعمل‌ها و مقررات بین‌المللی درباره امنیت شبکه و اطلاعات و امنیت زیرساخت‌های حیاتی.

ثبت و ارزیابی دقیق کارایی چارچوب سازمانی موجود و ساختارهای مربوط باعث می‌شود نقاطی تشخیص داده شود که به اندازه کافی پوشش داده نشده‌اند یا همپوشانی دارند. اما همچنین بخش‌هایی که نیاز به بهبود و هماهنگی مؤثرتر دارند نیز شناسایی می شوند. نتیجه این اقدام، تصویب قانون مورد نیاز با توجه به آزادی‌های اساسی و حقوق فردی و حقوق بین‌الملل، مطابق با اوضاع کلی اجتماعی و سیاسی و همچنین الزامات استراتژی ملی امنیت سایبری برای رسیدن به اهداف خواهد بود.

استراتژی ملی نسبیت خود را نه تنها در چارچوب سازمانی موجود، بلکه در سایر استراتژی‌ها در سطح ملی یا بین‌المللی (برای مثال مقررات ملی امنیت، استراتژی ملی نظامی، استراتژی دولت الکترونیکی و غیره) منعکس می‌کند. همچنین، با الزامات مقررات و دستورالعمل‌های مربوط در اتحادیه اروپا (به ویژه با بخشنامه ۱۱۴۸/۲۰۱۶ پارلمان اروپا و شورای ۶ ژوئیه ۲۰۱۶، درباره اقدامات مربوط در جهت ایجاد سطح بالایی از امنیت شبکه و سیستم‌های اطلاعاتی[1] به طور مشترک در سراسر اتحادیه اروپا) هماهنگ است.

1. NIS Directive

۳-۵- برنامه ملی رویدادهای پیش‌بینی نشده فضای سایبری

تدوین برنامه ملی رویدادهای پیش‌بینی‌نشده فضای سایبری که ساختارها و اقدامات مربوط به مقابله با حوادث قابل توجه را در سیستم های اطلاعاتی و ارتباطی حیاتی ذی‌نفعان شرکت‌کننده در استراتژی ملی امنیت سایبری تعیین کند و پذیرش مجدد خدماتی که ذی‌نفعان به جامعه ارائه می‌دهند.

اهداف اصلی برنامه ملی امنیت سایبری شامل تعیین و تشریح معیارهای مورد استفاده است تا یک حادثه بحرانی تلقی شود. این اهداف همچنین شامل تعیین فرایندها و اقدامات مهم برای مقابله با چنین حوادثی و تعیین نقش‌ها و صلاحیت‌های ذی‌نفعان مختلف که هرکدام حادثه خاصی را مدیریت می‌کنند نیز می‌شود.

۳-۶- تعیین الزامات اساسی امنیتی

همه ذی‌نفعان دخیل در استراتژی ملی امنیت سایبری موظفند تمام اقدامات فنی و سازمانی که عملکرد ایمن و یکپارچه سیستم‌های اطلاعاتی و ارتباطی آنها را تضمین می‌کند و تأثیر حادثه امنیتی را به حداقل می رسانند، را به انجام برسانند. این اقدامات شامل موارد پیشگیرانه است اما همچنین اقدامات مربوط به رسیدگی به حوادث امنیتی را نیز شامل می‌شود.

سازمان ملی امنیت سایبری (برای مثال بر اساس اقدامات قانونی) حداقل الزامات امنیتی و اقدامات فنی و سازمانی مربوطه را بر اساس ارزیابی ریسک در سطح ملی تعیین می‌کند که ذی‌نفعان نیز باید برای دستیابی به سطح اساسی و مشترک امنیتی آنها را اجرا کنند.

ایجاد حداقل سطح مشترک و هماهنگ در الزامات و اقدامات میان ذی‌نفعان که در حین اجرا، ارزیابی و بررسی دقیق اپلیکیشن مناسب اعمال خواهد شد، به طور ویژه قابل توجه است.

به علاوه، این روند توانایی ذی‌نفعان در تبادل اطلاعات را افزایش خواهد داد؛ زیرا «زبان مشترکی» ایجاد خواهد کرد و همچنین، گزارش‌دهی از حوادث امنیتی و اجرای اقدامات رایج امنیتی را نیز تسهیل می‌کند.

۷-۳- رسیدگی به حوادث امنیتی

در صورت بروز حادثه امنیت سایبری، ذی‌نفعان شرکت‌کننده در استراتژی ملی باید آماده واکنش مؤثر باشند. آگاهی از جزئیات فنی حوادثی که ذینفعان موظف به رسیدگی آنها هستند، تحلیل آنها و انتشار دانش لازم، به همه شرکت کنندگان کمک می کند تا خود را بهتر برای مقابله با حادثه امنیتی آماده کنند همچنین عملیات اصلاحی را با توجه به اقدامات امنیتی انجام دهند، به طوری که خطر تکرار حادثه به حداقل برسد. به این ترتیب، آمادگی و توانایی رسیدگی به حوادث امنیتی و متعاقبا بازیابی پس از آن در سطح ملی افزایش می‌یابد. علاوه بر این، مدیریت حوادث اضطراری مطابق با برنامه ملی رویدادهای پیش‌بینی نشده فضای سایبری محقق می‌شود.

در حین رسیدگی به حوادث امنیتی، تیم‌های واکنش به حوادث امنیت رایانه‌ای نقشی مهم دارند. وظیفه اصلی آنها هماهنگی اقدامات در هنگام مدیریت حادثه توسط ذی‌نفعان درگیر، براساس نقش‌ها، صلاحیت‌ها و فرایندهای از پیش تعیین شده و بر اساس قابلیت‌های ارتباطی و عملیاتی در سطح ملی است. تیم‌های پاسخگویی دیگری نیز وجود دارند

کـه از پیـش فعالیـت خـود را آغـاز کرده‌انـد یا ممکن اسـت با توجـه به بحث امنیـت رایانـه‌ای در هـر بخـش ایجـاد شـوند. عـلاوه بـر ایـن، هدف تیـم ملی واکنـش اضطراری رایانه‌ای، بهینه‌سـازی سـطح پیشـگیری، ارزیابـی و تحلیل تهدیدات ذی‌نفعان شـرکت کننده در اسـتراتژی ملی اسـت. تیم ملی واکنش اضطـراری رایانـه‌ای، بـا همـکاری سـایر تیم هـای واکنـش به حـوادث امنیت رایانـه‌ای/ تیـم ملـی واکنش اضطـراری رایانه‌ای فعال در یونان و سـایر تیم‌های واکنـش بـه حـوادث امنیت رایانـه‌ای/ تیم ملـی واکنش اضطـراری رایانـه ای که شـبکه همـکاری بـا آنها ایجاد شـده اسـت، دائماً در سـطح ملـی و بین‌المللی تهدیـدات و آسـیب‌پذیری‌های سیسـتم‌های اطلاعاتـی و ارتباطـی را کنتـرل می‌کنـد، آنهـا را براسـاس خصوصیـات هر کشـور تحلیـل و ارزیابـی می‌کند و ذی‌نفعـان را مطلـع می‌سـازد تـا آمادگی آنها بـرای برخورد با حـوادث امنیتی افزایـش یابد.

۸-۳- اجرای تمرینات آمادگی ملی

اجـرای تمرینـات آمادگـی ملـی ابـزاری قابـل توجـه بـرای ارزیابـی میزان آمادگـی ذی‌نفعـان شـرکت‌کننده و تشـخیص نقـاط ضعـف و آسـیب‌پذیری سیسـتم اسـت. شـبیه سـازی حـوادث امنیتـی فرصتـی فراهـم می‌کنـد تـا بـه ایـن مـوارد، از طریـق اجـرای اقدامـات امنیتـی و برنامه‌هـای پیش‌نویـس شـده از مـوارد احتمالـی در شـرایط مشـابه حوادث واقعی رسـیدگی شـود، به طـوری کـه ذی‌نفعـان می توانند نسـبت بـه ارتقا و به روزرسـانی‌هـای مربوطه اقـدام کننـد. به عـلاوه، چنیـن تمریناتی تبـادل اطلاعات و دانـش و همکاری بیـن ذی‌نفعـان شـرکت‌کننده را افزایـش می‌دهـد. در همیـن حـال، فرهنـگ همـکاری را نیـز برای افزایش سـطح امنیت سـایبری در یونـان تقویت می‌کنند.

تمرینات آمادگی در فواصل منظم انجام می‌شود. سازمان ملی امنیت سایبری این تمرینات را نظارت می‌کند. اجرای تمرینات نیز بر اساس جدول زمانی مشخص، نقش‌ها، سناریوها و اهداف صورت می‌پذیرد. نتایج این تمرینات و به ویژه دانش به دست آمده باید در اختیار ذی‌نفعان دست اندر کار در تمرینات و همچنین سایر ذی‌نفعان ذی‌صلاح قرار گیرد. مشارکت یونان در سایر تمرینات آمادگی اتحادیه اروپا و حوزه‌های‌بین المللی نیز پیگیری می‌شود.

۹-۳- آگاهی شهروند ـ کاربر

آگاهی از تهدیدات و آسیب‌پذیری های مربوط به امنیت سایبری و تأثیر اجتماعی آنها از اهمیتی کلیدی برخوردار است. آگاهی مناسب و هدفمند ـ کمپین‌های آموزشی، هم برای کاربران ذی‌نفع شرکت‌کننده در استراتژی ملی امنیت سایبری و هم برای شهروندان به طور کلی ـ کمک می‌کند میزان دانش نسبت به خطرات محیط آنلاین افزایش یابد تا بتوان در برابر تهدیدات رایج مقاومت نمود. انتظار می‌رود که این موضوع در نهایت سطح امنیت سایبری در یونان را افزایش دهد.

اقدامات، مکانیسم‌ها و روش‌های مربوط به آگاهیِ کاربر ـ شهروند، به مخاطب بستگی دارد. سازمان ملی امنیت سایبری نظارت بر طراحی، سازماندهی و اجرای برنامه آگاهیِ کاربر ـ شهروند را بر عهده دارد که به طور مشخص شامل کمپین‌های اطلاعاتی شهروندان (برای مثال از طریق وزارت آموزش و پرورش در دوره ابتدایی و متوسطه)، فعالیت‌های آموزشی (برای مثال در همکاری با مؤسسات دانشگاهی) برای مدیران و کاربران سیستم‌های اطلاعاتی و ارتباطی ذی‌نفعان، تبلیغات از طریق وب سایت‌ها و غیره می‌شود.

۱۰-۳- مکانیسم های قابل اعتماد در تبادل اطلاعات

تبادل اطلاعات، به جز تبادل اجباری ذکر شده اطلاعات در بند ۳,۶بین ذی‌نفعان خصوصی شرکت‌کننده در استراتژی ملی امنیت سایبری و نهادهای نظارتی آنها در بخش دولتی و با سازمان ملی امنیت سایبری، برای اجرای این مهم از اهمیت ویژه‌ای برخوردار است. ذی‌نفعان خصوصی تشویق می‌شوند که اطلاعات مربوط به سیستم‌های اطلاعاتی و ارتباطی اجرا شده، سیاست‌های امنیتی اتخاذ شده و تهدیدها و حوادث امنیتی را به تبادل بگذارند. به همین ترتیب، ذی‌نفعان بخش دولتی نیز تشویق می‌شوند تا اطلاعات جمع‌آوری شده را تبادل کنند که به طور بالقوه ممکن است سطح مطلوب امنیت سایبری را به خطر بیندازد. با همبستگی این اطلاعات می‌توان توسعه تهدیدات مربوط به امنیت سایبری کشور را تجزیه و تحلیل کرد.

تهیه چنین سازوکارهایی برای تبادل مطمئن اطلاعات در چارچوب اعتماد متقابل و احترام نسبت به نقش‌ها و صلاحیت‌های مهم ذی‌نفعان شرکت‌کننده در استراتژی ملی امنیت سایبری ضروری است.

در این مرحله و احتمالاً، در مرحله بعد، امکان بررسی توسعه مشارکت‌های بخش دولتی و خصوصی وجود دارد که براساس یک دامنه عملیاتی مشترک ایجاد خواهد شد. به علاوه، از نقش‌های کاملاً مشخصی برای دستیابی به اهداف مشترک استفاده می‌شود.

۱۱-۳-پشتیبانی‌ازبرنامه‌های‌تحقیق‌وتوسعه‌وبرنامه‌های‌آموزشی‌دانشگاهی

حمایت قابل توجه دولت از تلاش جامعه دانشگاهی برای مشارکت در برنامه‌های تحقیق و توسعه ملی، برنامه های اتحادیه اروپا یا سایر برنامه های

بین‌المللی و انطباق برنامه درسی با موضوعات مربوط به استراتژی ملی امنیت سایبری، پارامتری اساسی برای تقویت سطح امنیت سایبری در یونان است؛ به ویژه هنگامی که در نظر بگیریم این موضوع زمینه‌ای از فناوری‌های پیشرفته و دانش تخصصی است که به طور مداوم در حال پیشرفت است.

۱۲-۳- همکاری در سطح بین‌المللی

با توجه به اینکه فضای سایبری و اینترنت فضای جهانی اطلاعات است، مقابله با تهدیدات و آسیب‌پذیری های سیستم‌های اطلاعاتی و ارتباطی به یک تلاش جهانی تبدیل شده است که نیاز به همکاری در سطح ملی دارد. بنابراین، مهم است که یونان در همه همکاری‌های بین‌المللی در زمینه امنیت فضای سایبری در چارچوب اهداف موجود سیاست خارجی این کشور و دستورالعمل‌های اتخاذ آنها مطابق با قوانین قابل اجرا، به طور فعالانه شرکت کند. به طور دقیق تر همکاری سیستمی با کشورهایی که استراتژی مشابهی را در این زمینه اتخاذ کرده‌اند و انتخاب آنها با گزینه‌های مربوط به یونان در این مورد سازگار است، لازم می باشد. هدف این همکاری تبادل تجربیات و بهترین روش‌ها و تعیین پتانسیل توسعه مشترک ابزارهای مناسب برای رسیدگی به تهدیدها و چالش‌های مربوط به امنیت فضای سایبری خواهد بود. علاوه بر این، سهم یونان در تدوین و اجرای تصمیمات مربوط که در سازمان‌های بین‌المللی تصویب شده و یونان به آنها تعلق دارد مورد استفاده قرار خواهد گرفت. این سهم با هدف تقویت امنیت سایبری در بیشترین حد ممکن در سطح ملی و با ایجاد هماهنگی بین مکانیسم‌های مذاکره و اقدام چندجانبه بین‌المللی

مشابه، البته با در نظر گرفتن استقلال در تصمیم گیری در سطح ملی اجرا خواهد شد.

۱۳-۳- ارزیابی و بازنگری استراتژی ملی

سازمان ملی امنیت سایبری بر اجرای اهداف راهبردی استراتژی امنیت ملی سایبری با هدف ارزیابی و احیاناً تجدید نظر در استراتژی‌ها نظارت می‌کند. ارزیابی استراتژی بر اساس یک روش از پیش تعیین شده است که از شاخص های کارایی کمی و کیفی بر اساس استانداردهای بین‌المللی استفاده می‌کند و با گزارشی پایان می‌یابد که اقدامات ویژه توسعه را در یک جدول زمانی از پیش تعیین شده پیشنهاد می‌کند. سازمان ملی امنیت سایبری برای اتخاذ بهترین روش‌ها استانداردهای بین‌المللی را نظارت می‌کند که برای اجرای آن به ذی‌نفعان ذی‌صلاح نشان داده می‌شود. در طی این مرحله، مشارکت کلیه ذی‌نفعان در استراتژی ملی ضروری است که در چارچوب صلاحیت‌های سازمانی و اداری خود شرکت کنند.

بخش چهارم

بخش چهارم

نتیجـــه گیری

اســتراتژی ملــی امنیــت ســایبری بــر اســاس چارچــوب اقــدام فــوق تدویــن خواهــد شــد که همچنین شــرایطی را برای اجرای چشــم انــداز ملی ما بــرای ســطح مطلوب امنیت ســایبری ایجــاد می‌کند (به بخــش ۳ مراجعه کنید). اجــرای مــوارد ذکــر شــده مســتلزم تقویت همــکاری بیــن بخش هــای دولتی و خصوصــی اســت کــه بــه نظــر می‌رســد بــرای موفقیــت کل ایــن کار ضروری باشــد، امــا بــه ویــژه بــا توجه به درجــه بلوغ و تجربه کم، بســیار دشــوار اســت. بــا ایــن حــال، مزایای چنین همــکاری برای دولــت و اداره عمومی، شــهروندان و ســطح خدمــات امنیتــی ارائــه شــده و همچنیــن بــرای بخــش خصوصــی (ارائه‌دهندگان خدمات باند پهـــن کسب‌وکارهای خصوصی) چندبرابر خواهدبود.

csri.majazi.ir

حـوزه فضـای مجـازی بـه انـدازه انقـلاب اسـلامی اهمیـت دارد. ایـن فضـا مثـل یـک رودخانـه پـر از آب و خروشـان اسـت کـه مـی آیـد و دائمـاً هـم بـر آب آن افـزوده و خروشـان تـر مـی شـود. اگـر مـا بـر ایـن رودخانـه تدبیـر کنیـم و برنامـه داشـته باشـیم، زه‌کشـی کنیـم و هدایـت کنیـم ایـن رودخانـه را تـا بـه سـد بریـزد، می‌شـود فرصـت. اگـر رهایـش کنیـم و برنامـه‌ای بـرای آن نداشـته باشـیم می‌شـود یـک تهدید.

csri.majazi.ir