مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

گزارش سریع
چهل و هفتم

استراتژی امنیت سایبری و اطلاعاتی دانمارک

Cyber and information security strategy Denmark

گزارش سریع

گزارش شماره ۴۷
شهریور ۱۴۰۱

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

استراتژی امنیت سایبری و اطلاعاتی دانمارک

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: دکتر الهه سوفسطائی
ناظر: عباس قنبری باغستان

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

فهرست

سخن نخست

سخن نخست

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

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

سیدابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

مقدمه

مقدمه

همانند دیگر کشورهای جهان، فناوری در دانمارک با سرعت بالایی در حال پیشرفت می‌باشد. علاوه بر این، استفاده و وابستگی شهروندان، ادارات و شرکت‌های دانمارک به تکنولوژی، اینترنت و خدمات ارائه شده توسط آنها روز به روز در حال افزایش است.

در حال حاضر دانمارک به یکی از دیجیتالی‌ترین کشورها در جهان تبدیل شده است؛ جایی که استفاده از تکنولوژی در رسیدگی به امورات دولتی و توسعهٔ مشاغل خصوصی و رقابت بین آنها حائز اهمیت می‌باشد.

شهروندان نه تنها به استفاده از تکنولوژی برای انجام مشاغل خود و ارتباط با مقامات دولتی عادت کرده‌اند بلکه به امنیت این فضا نیز اعتماد کامل دارند.

احساس امنیت و اعتماد برای پیشرفت و توسعهٔ صنعت دیجیتال حیاتی است. حفاظت از داده‌ها در برابر حملات خارجی و ایجاد حس امنیت و اعتماد نیز از مسائلی است که باید به آن توجه شود.

دولت هم اکنون در حال تقویت پایه‌های امنیت سایبری و اطلاعاتی است و طی چند سال آینده۱/۵ میلیارد کرون (DKK 1.5

billion)در زمینه امنیت سایبری و حفاظت از اطلاعات[1] سرمایه‌گذاری خواهد کرد.

طی توافقنامه دفاعی ۲۰۱۸-۲۰۲۳ [2]، دولت و مقامات مربوطه زمینه‌های حفاظت اطلاعات در کشور دانمارک در برابر حملات سایبری را به طور قابل توجهی تقویت کردند. این امنیت به کمک استراتژی جدید امنیت ملی اطلاعات سایبری بیشتر از قبل تأمین می‌شود.

دولت ۲۵ طرح و۶ استراتژی هدفمند را برای پرداختن به مهمترین بخشهای امنیت سایبری و حفاظت از اطلاعات جهت افزایش انعطاف پذیری زیرساخت های فناوری دیجیتال[3] ، ارتقای سطح دانش و بهبود مهارت شهروندان و ادارات و تقویت هماهنگی و همکاری در این زمینه را راه‌اندازی خواهد کرد. این استراتژی، امنیت سایبری اطلاعات دانمارک را طی چهار سال آینده تضمین می کند.

امکان حذف حملات آسیب‌رسان سایبری وجود ندارد؛ اما به‌وسیله یک استراتژی مناسب و جدید برای آمادگی علیه حملات سایبری، دولت می‌تواند تضمین کند که شهروندان و شرکت‌ها از خدمات تکنولوژی به راحتی و در امنیت کامل استفاده کنند.

1. Cyber And Information And Security
2. 2018-2023 Defence Agreement
3. Technological resilience of digital infrastructure

بخش اول

بخش اول

نقـاط ضعف و قـوت تکنولوژی

دانمـارک یکـی از پیشـگامان عرصـهٔ دیجیتـال در دنیـا می‌باشـد. ایـن امـر هـم در مـورد مسـائل عمومـی صـدق مـی کنـد کـه بخـش اعظـم امـور شـهروندان و حتـی مشـاغل آنهـا بـه صـورت دیجیتـال در آمـده اسـت، و هـم در مـورد مشـاغل خصوصـی کـه بـه وسـیله آن مـی تـوان از موقعیـت هـای متعـدد به‌وجودآمـده بـرای توسـعه و ایجـاد موقعیـت هـای شـغلی جدیـد اسـتفاده کـرد. ایـن حجـم اسـتفاده از تکنولـوژی مزایـا و موقعیـت هـای بسـیار متنوعـی بـرای شـهروندان، شـرکت‌ها و کل جامعـه به‌وجـود مـی آورد. عـلاوه بـر بقیـه مـوارد، نـه تنهـا مـی تـوان توجه سـرمایه گـذاران خارجـی را بـه ایـن وسـیله جـذب کـرد؛ بلکـه مـی تـوان بـه رقابـت و پویایـی اعضـای جامعـه نیـز کمـک کـرد.

در طـول سـال هـای پیـش رو تحـولات در هـر دو بخـش عمومـی و خصوصـی ادامـه خواهنـد داشـت. توسـعه فنـاوری سـریع تـر خواهـد شـد و بـه دنبـال آن، اسـتفاده از فنـاوری نیـز گسـترده‌تر خواهـد شـد. ایـن اسـتفاده فقـط مربـوط بـه شـهروندان نمـی باشـد، بلکـه ادارات دولتـی نیـز بـه ایـن توسـعه کمـک می‌کننـد؛ زیـرا تجـارت دولـت رونـق پیـدا خواهـد کـرد.

با این حال گسترش استفاده از دیجیتال وابستگی به استفاده از تکنولوژی را افزایش می دهد و باعث آسیب پذیری بیشتر خواهد شد که می‌تواند به وقایعی نظیرخرابی سیستم های ICT [1]، نفوذ در اطلاعات محرمانه[2]، در دسترس بودن اطلاعات و از بین رفتن یکپارچگی آنها[3] بشود. چنین وقایعی می تواند نتیجه حملات سایبری یا نشر ناخواسته اطلاعات فرد باشند که در چنین شرایطی دولت در برابر تأمین امنیت لازم همگام با چالش های جدید مسئول می باشد.

دولت دانمارک در حوزه امنیت ملی سایبری و حفاظت و همچنین برای اطمینان از امنیت دیجیتال دانمارک، برنامه های جاه طلبانه ای را برای سال‌های آینده ارائه داده است. طی سال‌های پیش‌رو، دولت دانمارک با همکاری اداره‌هایی که برای بقای جامعه نقش حیاتی دارند، مانند بخش‌های انرژی، حمل و نقل، ارتباطات از راه دور، امور مالی، بهداشت و درمان و دریانوردی باید تلاش های خود را افزایش دهند تا از امنیت سایبری و اطلاعات در سراسر دانمارک اطمینان حاصل کند. این کار باید طی سال‌ها با همکاری و زحمات طیف‌های گسترده ای از جامعه انجام شود اما دولت به انجام سریع آن تأکید دارد؛ تهدید ها روز به روز افزایش می یابند و به همین دلیل اقدامات لازم برای تحکیم ساختار های حفاظتی نیز باید هر چه سریع تر شکل بگیرند.

مقامات در برابر تأمین امنیت لازم و همگام با چالش های جدید مسئول می باشند

1. ICT System Breakdowns
2. Breaches of Confidentiality
3. Accessibility and Integrity of Data

امنیت اطلاعات

امنیت اطلاعات اصطلاحی جامع است که به کلیه اقدامات جهت ایمن سازی اطلاعات با در نظر گرفتن محرمانه بودن آنها، تمامیت (تغییر داده‌ها) و قابلیت دسترسی گفته می‌شود. امنیت داده شامل سازماندهی اقدامات امنیتی ، تأثیر بر رفتار، پروسه های پردازش داده و مدیریت تأمین کننده‌ها است.

امنیت سایبری

امنیت سایبری شامل حفاظت در برابر نقض ایمنی ناشی از حمله به داده یا سیستم ها از طریق اتصال به شبکه یا سیستم خارجی است؛ بنابراین تمرکز امنیت سایبری بر آسیب پذیری بالقوه اتصال سیستم ها از جمله اتصال به اینترنت است.

بخش های حمل و نقل، ارتباطات از راه دور، امور مالی، بهداشت و درمان و دریانوردی باید تلاش های خود را برای تأمین امنیت سایبری و اطلاعاتی در سراسر دانمارک افزایش دهند. این کار باید بر اساس تلاش های ملی سال های اخیر که به افزایش سطح امنیت سایبری و اطلاعاتی کمک کرده است، باشد اما دولت اکنون در نظر دارد سرعت این روند را بیشتر کند. تهدیدها با سرعت بالایی در حال بیشتر شدن هستند و این امر مستلزم تقویت چشمگیرانه یا اقدامات برای پاسخ به این چالش ها است.

افزایش وابستگی و افزایش آسیب پذیری

هرچه ارتباطات بین افراد یک جامعه به وسیله تکنولوژی بیشتر از قبل می شود، حجم اطلاعات منتقل شده بین آنها نیز بیشتر از قبل می شود؛ در نتیجه عواقب و خطرات یک حمله سایبری در صورت وقوع سنگین تر می شود. شهروندان، سازمان ها و شرکت ها نیز هدف اصلی چنین اقداماتی هستند.

هنگامی که حادثه‌ای رخ می‌دهد، در ابتدا ممکن است یک موضوع امنیتی محدود و نسبتاً جزئی تلقی شود اما می‌تواند به سرعت در تمام ادارات، شرکت ها و بخش های مختلف گسترش یابد. علاوه بر آن، بسیاری از سازمان‌ها دارای سیستم‌های ICT بیش از حد پیچیده و گاهاً از دوران گذشته هستند که حفاظت از آن‌ها نیز پیچیده‌تر است. بنابراین حفاظت بسیاری از زیرساخت های سیستم‌های ICT توسط شرکت‌های خصوصی تأمین می‌شود. بسیاری از این شرکت‌ها قادر به تأمین امنیت ساختارهای زیربنایی دانمارک در این سطح نمی‌باشند؛ در نتیجه احتمال نشت اطلاعات و حملات سایبری افزایش می‌یابد و اطلاعات بقیه ساختار های جامعه نیز به راحتی می‌تواند پخش شود.

به عنوان اعضای یک جامعه، ما نه تنها باید از خود در برابر انواع حملات، بلکه در برابر خرابی سیستم، خرابی تأمین کننده[1]، نقض عمدی و غیر عمدی امنیت سایبری و اطلاعاتی[2] و به خطر انداختن اطلاعات شخصی محافظت کنیم.

«همانطور که سیستم‌ها و زیرساخت‌ها بیشتر با یکدیگر مشارکت می‌کنند، چالش‌های امنیتی مربوطه نیز پیچیده‌تر می‌شود.»

1. Supplier Failure
2. Intentional and Unintentional Breaches of Cyber and Information Security

آسیب پذیری های بیشتر فرهنگ امنیتی ناقص

فقدان مهارت و دانش امنیتی باعث ایجاد آسیب‌پذیری قابل توجهی می‌شود که شخص ثالثی میتواند از آن سوءاستفاده کند. رفتارهای امنیتی مدیران، کارمندان شرکت‌ها و ادارات در کسب سطح امنیتی مناسب بسیار حائز اهمیت است.

وابستگی شدید به زیرساخت های دیجیتال

زیرساخت های دیجیتال حیاتی یکی از الزامات برای انجام امور مختلف در بخش های خصوصی و عمومی می‌باشد. کمبود دسترسی، تعامل و اعتماد به زیرساخت های دیجیتال می‌تواند عواقب قابل توجهی برای جامعه به ارمغان بیاورد.

افزایش ارتباط میان دستگاه ها

تعداد دستگاه‌های متصل به اینترنت در حال افزایش است. این باعث به وجود آمدن موقعیت های جدید می‌شود ولی در کنار آن آسیب پذیری در برابر حملات را به دلیل وقوع بیشتر حوادث امنیتی را افزایش می‌دهد.

پیچیدگی زیاد در نمونه کارهای IT (IT portfolio)

بسیاری از سازمان‌های دولتی و خصوصی از سیستم‌های ICT پیچیده و گاهاً از تاریخ گذشته استفاده می‌کنند. گاهاً نرم‌افزار مورد استفاده به درستی مهیا نشده است و سیستم‌ها از سطح امنیتی مناسب نیز برخوردار نیستند.

حملات سایبری به راحتی قابل انجام هستند

دسترسی آسان ابزار های لازم برای هک کردن در اینترنت به معنای این است که هرکس که بخواهد یک سیستم را هک کند، می‌تواند به راحتی این کار را انجام بدهد.

یک تهدید احتمالی در حال تکامل

در سال های اخیر در کنار توسعه دیجیتال، روش های جدیدی برای حملات علیه کشورها، مشاغل و شهروندان توسط گروه‌های تحت حمایت دولت یا کشورهای خارجی به وجود آمده است. این یک چالش در سطح جهانی است که همه جوامع با آن روبرو هستند و انتظار می رود در سالهای پیش رو وضعیت بدتر هم بشود.

حملات سایبری اشکال مختلفی دارند که در آن شخصی سعی در ایجاد اختلال یا دسترسی غیرمجاز به داده ها، سیستم‌ها، شبکه‌های دیجیتالی یا خدمات دیجیتال دارند. برای نمونه می‌توان به حملات به مقامات عمومی یا وب سایت های تجاری یا حملات پیچیده تر در قالب تلاش برای دستیابی به اطلاعات محرمانه مشاغل و سازمان های عمومی، ایجاد خرابی و اختلال اشاره کرد.

تهدیدات سایبری و امنیت اطلاعات بر تمام بخش‌های جامعه تأثیر می‌گذارد. تاثیر آن بر قربانیان شامل از دست دادن سرمایه تا از دست دادن اطلاعات و داده های حیاتی تجارت فرد است. چنین حملاتی می‌توانند برای امنیت دولت مرکزی نیز مخرب باشند و منجر به از بین رفتن اعتماد مردم به دولت، خسارت مادی یا مالی قابل توجه و در موارد شدید از دست دادن زندگی شود. برای دولت

دانمـارک، ضـروری اسـت کـه بـه طـور مـداوم تـلاش هـای خـود را بـرای حفاظـت جامعـه در برابـر ایـن تهدیـدات انجـام دهـد.

تهدیـدات سـایبری و امنیـت اطلاعـات بـر تمـام بخش‌هـای جامعـه تأثیـر می‌گـذارد

- بنیان‌های استراتژیک:

استراتژی ملی برای امنیت سایبری و اطلاعات ۲۰۱۵-۲۰۱۶

هـدف اولیـن اسـتراتژی ملـی امنیـت سـایبری و حفاظـت اطلاعـات دانمـارک درسـال هـای ۲۰۱۵ و ۲۰۱۶ ارتقـای سـطح امنیتـی و همچنیـن افزایـش سـطح آگاهـی شـهروندان و شـرکت‌ها از ایـن مفهـوم بـود. ایـن اسـتراتژی شـامل الزاماتـی بـرای اجـرای اسـتاندارد امنیـت بیـن المللـی ISO27001 و نظـارت سیسـتماتیک دولـت مرکـزی بـود.

مرکـز امنیـت سـایبری یـک واحـد بـرای ارزیابـی تهدیـد موجـود و یـک مرکـز مشـورتی بـرای امنیـت ICT ایجـاد کـرده اسـت. ظرفیـت پلیـس دانمـارک بـرای تحقیـق در رابطـه بـا امنیـت اطلاعـات افزایش یافتـه اسـت. مقامـات بازرگانـی دانمارکـی معیـار هایـی بـرای امنیـت دیجیتـال مخصوصـاً بـرای شـرکت هـای کوچـک و متوسـط تعییـن کرده‌انـد.

همچنیـن یـک هیئـت مشـاوره بازرگانـی[1] بـه منظـور گفت‌وگـو بـرای تقویـت چهارچوب‌هـای امنیـت اطلاعاتـی مشـاغل ایجـاد شـده در مـارس ۲۰۱۷ هیئـت مدیـره توصیـه هـای خـود را در مـورد چگونگـی

1. ICT(Virksomhedsrådet for it-sikkerhed)

تقویت امنیت ICT و تقویت کنترل اطلاعات به ویژه در کسب و کارهای کوچک و متوسط ارائه کرد.

همچنین این استراتژی تشخیص داد برای افزایش بهره‌وری، نیاز به بهبود سطح ارتباطات بین مؤسسات آموزشی و کارفرمایانی که فارغ التحصیلان این موسسات را استخدام می کنند، وجود دارد. بر این اساس، یک همکاری ایجاد شد و از جمله نتایج این همکاری به وجود آمده می توان به تولید یک برنامه کارشناسی حرفه ای جدید در حوزه امنیت سایبری و حفاظت از اطلاعات اشاره کرد.

بخش دوم

بخش دوم

تلاشـــی سیســـتماتیک و پایدار

چشـــم انـــداز و تـــلاش هـــای دولـــت بـــرای امنیـــت ســـایبری و حفاظـــت اطلاعـــات در دانمـــارک

شـهروندان، شـرکت هـا و ادارات بایـد بـا خطـرات دیجیتالی آشـنا باشـند و بتواننـد آن را مدیریـت کننـد، بـه گونـه ای کـه تمامـی افـراد دانمـارک بتواننـد از مزایـای تکنولـوژی اسـتفاده کننـد.

افزایـش اسـتفاده از تکنولـوژی در حوزه‌هـای اقتصـادی و اجتماعـی چالش‌هـای کامـلاً جدیـدی را در مـورد امنیـت اطلاعـات ایجـاد مـی کنـد و پیامدهـای منفـی نداشـتن یـک رویکـرد مناسـب و سـاختاری بـرای نظـارت بـر آن مـی توانـد بسـیار عمیـق باشـد؛ بـه همیـن دلیـل دولـت دانمـارک تمرکـز خـود را بـر روی ایـن زمینـه بیشـتر کـرده اسـت.

بـرای آن کـه جامعـه دانمـارک بتوانـد بـه ایـن امنیـت دسـت یابـد، بایـد زیرسـاخت هـای دیجیتالـی مـا در برابـر تهدیـدات سـایبری انعطاف‌پذیـر باشـد و شـهروندان، شـرکت‌ها و ادارات بـه طـور مـداوم اطلاعـات خـود را در ایـن راسـتا افزایـش دهنـد. ایـن موضـوع هـم مربـوط بـه متخصصـان امنیتـی اسـت کـه نیـاز بـه آنهـا طـی چنـد سـال آینـده افزایـش خواهـد یافـت و هـم افـرادی کـه بـه طـور خصوصـی کار می‌کننـد.

یک مسئولیت مشترک: ارتقای سطح امنیت سایبری و اطلاعات ملی یک مسئولیت مشترک است. دولت مرکزی مسئول حفاظت از امنیت ملی است. مشاغل و مقامات مسئول حفاظت از امنیت در سازمانهای خود هستند. علاوه بر این، همه شهروندان باید درک کنند که چگونه اعمال آنها می تواند بر امنیت دیجیتال خود و دیگران تأثیر بگذارد.

با استراتژی امنیت سایبری و اطلاعات دانمارک ۲۰۱۸-۲۰۲۱ دولت دانمارک گام بعدی را به سمت دانمارک دیجیتال امن تر برداشته است. تمرکز این استراتژی در حول سه زمینه زیر است:

- ❖ آمادگی فناوری؛
- ❖ افزایش آگاهی از امنیت سایبری بین شهروندان، شرکت ها و ادارات؛
- ❖ بهبود همکاری و هماهنگی بین مقامات مسئول.

به علاوه بسیاری از زیرساختهایی که برای جامعه نقش حیاتی دارند (برای مثال:انرژی، حمل و نقل، ارتباطات از راه دور، امور مالی، بهداشت و درمان و بخش دریایی و همچنین در سازمان های دولت مرکزی) توسط شرکت‌های خصوصی اداره می‌شوند. به همین دلیل، نیاز به همکاری نزدیکی بین بخش دولتی و بخش خصوصی و همچنین بین جامعه مدنی، پلیس و نیروهای مسلح وجود دارد دولت دانمارک ۲۵ طرح ویژه را برای تقویت امنیت سایبری و حفاظت اطلاعات آغاز کرده است. برخی از آنها بر اساس تلاش هایی است که قبلاً انجام شده، در حالی که برخی دیگر کاملاً جدید هستند.

دولت دانمارک ۲۵ طرح ویژه را برای تقویت امنیت سایبری و

حفاظت اطلاعات آغاز کرده است. برخی از آنها بر اساس تلاش هایی است که قبلاً انجام شده، در حالی که برخی دیگر کاملاً جدید هستند. این استراتژی همچنین جهت برقراری ارتباط بین تعدادی از فعالیت های مقطعی در ادارات مسئول امنیت سایبری و اطلاعاتی دانمارک انجام می شود.

بخشی از یک طرح گسترده تر

استراتژی امنیت سایبری و حفاظت اطلاعاتی دانمارک بخشی از یک طرح گسترده تر است. دولت تأکید زیادی بر امنیت سایبری کرده است و طبق توافقنامه دفاعی ۲۰۱۸-۲۰۲۳، سطح امنیت سایبری دانمارک با تزریق۱/۴ میلیارد DKK طی شش سال آینده به طور قابل توجهی تقویت خواهد شد. این شامل حفاظت بهتر در برابر حملات سایبری پیچیده با گسترش مرکز شبکه حسگر امنیت سایبری[1] برای مقامات و مشاغل خواهد بود. علاوه بر این، یک مرکز ملی وضعیت سایبری ایجاد خواهد شد. این مرکز که به طور شبانه روزی کار می‌کند، نمای کلی از وضعیت امنیت ملی را در برابر تهدیدات فعلی و احتمالی مهمترین شبکه های دیجیتالی دانمارک ارائه می دهد. همچنین مرکز امنیت سایبری، که یک مرجع ملی امنیت ICT است، به شرکت‌های خصوصی و ادارات دولتی مشاوره می‌دهد و از آنها پشتیبانی می‌کند. علاه بر اینها، با گسترش یافتن ظرفیت تحلیل سرویس های اطلاعات دفاعی دانمارک، توانایی نیروهای مسلح دانمارک برای انجام عملیات سایبری نظامی بهبود خواهد یافت.

1. Centre for Cyber Security's Sensor Network

دستورالعمل اتحادیه اروپا درباره امنیت شبکه ها و سیستم های اطلاعاتی دستورالعمل (NIS)

در حال حاضر دانمارک در حال انتقال دستورالعمل امنیت شبکه ها و سیستم های اطلاعاتی اتحادیه اروپا (دستورالعمل NIS) است. یکی از الزامات دستورالعمل این است که اپراتورهای خدماتی که برای عملکردها جامعه ضروری هستند و خدمات کلیدی ارائه می‌دهند، باید گام هایی را برای مدیریت امنیت شبکه ها و سیستم های اطلاعاتی مورد استفاده برای ارائه خدمات خود بردارند.

یکی دیگر از الزامات مندرج شده در این بخشنامه این است که اعضای آن باید یک استراتژی ملی برای امنیت شبکه ها و سیستم های اطلاعاتی تهیه کنند و این چیزی است که استراتژی امنیتی سایبری و اطلاعاتی دانمارک در نظر میگیرد.

مقررات عمومی حفاظت از دادهٔ اتحادیه اروپا

این آیین نامه از ۲۵ می ۲۰۱۸ به اجرا در می آید. این آیین نامه به همراه یک قانون محافظت از داده‌ی دیگر به طور همزمان به اجرا در می آید و تکمیل کننده سیستم حفاظتی پیشین برای داده های شخصی در دانمارک است.

امضا کنندگان توافق نامه دفاعی، بخشی از بودجه این توافق نامه را برای مقابله با چالش های سایبری پیش‌رو از طریق اقدامات اضافی، از جمله تحقیق و آموزش در این راستا اختصاص داده اند. این خود نشانگر این است که دانمارک برای چالش های پیش‌رو در حال برنامه ریزی است.

سرویس امنیت و اطلاعات دانمارک به عنوان یک مقام امنیت ملی، در حال برنامه ریزی برای افزایش همکاری با مقامات مربوطه و مشاغل خصوصی برای کمک به دانمارک در رفع تهدیدات امنیتی به بهترین شکل ممکن است. سرانجام در ژانویه ۲۰۱۸، دولت استراتژی خود را برای رشد دیجیتال دانمارک ارائه داد. هدف آن اطمینان حاصل کردن از تبدیل شدن دانمارک به یک کشور پیشرو در عرصه دیجیتال است. این استراتژی شامل تعدادی از ابتکارات با هدف ارتقای سطح امنیت ICT و نظارت بر تبادلات داده ها برای اطمینان از استفاده بهینه از امکانات جدید فن آوری است.

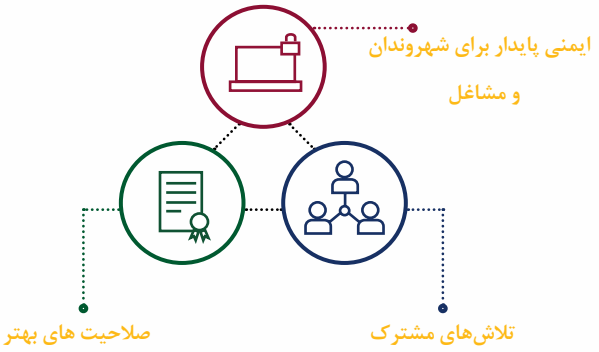
به موازات این، به عنوان بخشی از بخش عمومی مشترک استراتژی دیجیتال برای سال های ۲۰۱۶ تا ۲۰۲۰، توافق شده است که تلاش ها برای ارتقای امنیت اطلاعات شهرداری و منطقه ای باید بیشتر شوند. دولت بر اساس استراتژی امنیت سایبری و اطلاعاتی دانمارک با شهرداری‌ها و مناطق مربوطه در مورد ابتکارات بیشتر در این زمینه وارد گفت‌وگو خواهد شد.

بخش سوم

بخش سوم

معیارها

دولت دانمارک سه معیار مشخص برای تقویت امنیت و دیجیتالی شدن بیشتر کشور طی چهار سال آینده معرفی کرده است.



ایمنی پایدار برای شهروندان و مشاغل

دولت مرکزی با مشارکت ساختارهای مهم دیگر دارد آمادگی خود را برای رویارویی با تهدیدات پیش‌رو افزایش می دهند تا بتوانند از ساختار های اساسی جامعه در برابر حملات سایبری یا دیگر مهم

امنیتی اطلاعاتی محافظت کند.

تلاش‌های مشترک

این سبک مدیریت امنیتی مبتنی بر ریسک می باشد و باید تقسیم‌بندی مشخصی برای مسئولیت ها در زمینه امنیت سایبری و اطلاعاتی در ادارات و شرکت های پیش‌برنده عملکردهای حیاتی جامعه وجود داشته باشد.

صلاحیت های بهتر

شهروندان، شرکت ها و ادارات به دانش لازم دسترسی کافی دارند و باید خود را قادر به مواجه با چالش های امنیت سایبری و اطلاعاتی بکنند.

اقدامات

امنیت پایدار

۱-۱) ایجاد یک مرکز ملی وضعیت سایبری؛

۱-۲) به وجود آوردن حداقل شرایط لازم برای فعالیت مقامات در زمینه امنیت سایبری و اطلاعات؛

۱-۳) آغاز اقدامات نظارتی در حوزه سایبری؛

۱-۴) نظارت بر سیستمهای مهم ICT در دولت مرکزی؛

۱-۵)طراحی پورتال دیجیتال مشترک برای تهیه گزارش؛

۱-۶) ایجاد مرکز ملی رسیدگی به پرونده های مربوط به جرایم جنایی؛

۱-۷) تشکیل همکاری پیشرفته در زمینه جلوگیری از حملات مرتبط با ICT و اجرای آن در پاسخ به چنین حملاتی؛

۱-۸) امنیت بالاتر برای اسناد هویتی؛

۱-۹) بهبود اولویت بندی زیرساخت های ICT ملی ؛
۱-۱۰) ایجاد ارتباط امن در دولت مرکزی.

صلاحیت های بهتر

۲-۱) قضاوت دیجیتالی و صلاحیت های دیجیتالی که از طریق سیستم آموزشی به دست آمده است؛
۲-۲) پورتال آموزشی؛
۲-۳) تحقیق در مورد فناوری جدید؛
۲-۴) همکاری شرکتی برای افزایش امنیت ICT در جامعه تجاری دانمارک؛
۲-۵) همکاری در زمینه توسعه صلاحیت ها و پرورش فرهنگ امنیتی در دولت مرکزی؛
۲-۶) انگیزه جهت بهبود آگاهی برای شهروندان و مشاغل.

تلاش‌های مشترک

۳-۱) استراتژی‌های جانبی در سطح بخشی و واحدهای غیرمتمرکز امنیت سایبری؛
۳-۲) تلاش‌های میان بخشی برای حمایت از امنیت سایبری و اطلاعات در بخش‌های مهم؛
۳-۳) مدیریت تأمین کنندگان خدمات ICT برون سپاری شده؛
۳-۴) تقویت هماهنگی ملی؛
۳-۵) افزایش میزان مشارکت در همکاری های بین المللی؛
۳-۶) ارزیابی وضعیت فعلی امنیت سایبری و امنیت اطلاعات؛
۳-۷) نمای کلی اطلاعاتی که قابل محافظت است؛

۳,۸ معماری امنیت اطلاعات؛
۳,۹ تلاش ملی و بین المللی برای حفاظت از داده ها و محافظت از داده های شخصی.

امنیت پایدار برای شهروندان و مشاغل

دولت مرکزی با مشارکت ساختارهای مهم دیگر آمادگی خود را برای رویارویی با تهدیدات پیش رو افزایش می دهد تا بتواند از ساختار های اساسی جامعه در برابر حملات سایبری یا دیگر موارد مهم امنیتی اطلاعاتی محافظت کند.

به منظور محافظت از عملکردهای اساسی جامعه و محافظت از سیستم ها و داده های ضروری ICT، دولت دانمارک باید:

- یک دید کلی بهتر از تهدیدهای موجود برای جامعه ارائه دهد و بر سیستم ها و داده های حیاتی جامعه نظارت بیشتری داشته باشد؛
- سطح امنیت سایبری و ادارات دولتی را افزایش دهد؛
- مشاوره‌های ملی را افزایش دهد.

دولت دانمارک می‌خواهد خود را در برابر حملات سایبری مقاوم بسازد. آگاهی از تهدیدها، شناسایی آسیب ها و ارزیابی خطرات از جمله عوامل مهم در این زمینه هستند. هر شرکت و اداره مسئولیت رسیدگی به امنیت سایبری خود و تطبیق تلاش‌های خود با اساس

ارزیابی ریسک و تحلیل آسیب‌پذیری را بر عهده دارد. همچنین هر سازمانی در برابر اجرای صحیح اقدامات امنیتی لازم و حفاظت از سیستم ها و داده های ICT خود مسئول می‌باشد. این امر مستلزم آگاهی و بررسی تهدیدات احتمالی است. به همین دلیل، توانایی دولت دانمارک در شناسایی و مدیریت تهدیدهای اینترنتی باید تقویت شود.

سیستم نظارتی پیشرفته

به منظور محافظت از سیستم های ICT و داده های مهم جامعه، بسیار مهم است که مقامات مرکزی یک دید کامل نسبت به سیستم و داده‌هایی که نیاز به محافظت بیشتر دارند، داشته باشند و بر آنها نظارت بکنند. این نظارت به معنای آگاه کردن ادارات و شرکت‌هایی است که از خطرات موجود و همچنین کمک رسانی به آنها در معرض تهدید هستند. برای پایدار کردن این نظارت، دولت باید یک مرکز ملی وضعیت سایبری در مرکز امنیت سایبری ایجاد بکند. این مرکز به صورت شبانه‌روزی و با اپراتور اداره می شود و یک مرور کلی و مداوم بر وضعیت امنیت ملی، تهدیدات موجود و مهمترین شبکه های دیجیتال دانمارک می کند. این اطلاعات به دست آمده به اداره مدیریت بحران در پیشبرد وظیفه‌اش کمک شایانی می‌کند.

ادارات، در کنار بعضی از مشاغل، موظفاند گزارش حوادث سایبری را به مقامات دولتی مربوطه ارائه دهند. گزارش های ارائه شده توسط مقامات و مشاغل شرط لازم برای نشر اطلاعات و تجربیات و یک مرور کلی بر حوادث امنیتی ICT، انواع حوادث و پیامدهای حاصله از آنها است. به منظور تسهیل گزارش دهی، دولت دانمارک یک راه حل

دیجیتالی واحد برای گزارش وقایع امنیتی ICT ایجاد خواهد کرد. این راه حل همچنین باید بتواند اطلاعات مربوط به پیشگیری و رسیدگی حوادث را به خبرنگاران منتقل کند. یک راه حل دیجیتالی واحد از یک طرف از مشاغل و مقامات در گزارش دهی حوادث امنیتی مربوطه تا آنجا که ممکن است پشتیبانی می کند، و از طرف دیگر بینش دقیق‌تری از حوادث ICT مربوط به شرکت‌ها و ادارات ارائه می‌دهد.

افزایش تلاش های دولت در زمینه امنیت سایبری و اطلاعات

از سال ۲۰۱۶، مقامات دولت دانمارک موظف به رعایت الزامات استاندارد امنیتی بین المللی ISO27001 هستند که بهترین روش برای مدیریت امنیت اطلاعات است. آخرین پیگیری ها در مورد اجرای ISO27001 توسط مقامات دولتی نشان می دهد که قبل از پیاده‌سازی کامل ISO27001، اقدامات باید انجام شوند. به عنوان مثال ، مقامات باید ارزیابی چالش‌ها و ارزیابی مستمر تلاش های خود را بهبود بخشند. با این استراتژی، دولت تمرکز خود را بر تأمین حداقل سطح امنیت ICT لازم برای همه ادارات دولتی افزایش می دهد.

در آینده، همه ادارات دولتی موظف به تأمین حداقل الزامات در زمینه امنیت سایبری و حفاظت اطلاعات خواهند بود. این حداقل الزامات مربوط به جنبه های فنی و سازمانی است و از تأمین سطح بالای حفاظت در برابر حوادث سایبری اطمینان حاصل می کند. این امر باعث می شود که ادارات دولتی اقدامات خود را در زمینه

مدیریت امنیت اطلاعات در برابر چالش ها و بر اساس ISO 27001 بهبود بخشند، برنامه هایی برای مدیریت و توسعه نمونه کارهای ICT (از جمله مدیریت چالش های پیشین و حفاظت اطلاعات) را آماده سازند، به یک تصمیم مکتوب در مورد محصولات دستورالعمل در منطقه دست یابند و پیاده سازی فناوری لازم برای محافظت در برابر حملات را اجرایی کنند.

به منظور اطمینان از اجرای جامع ISO 27001 در سازمانهای دولتی مرکزی، دولت دانمارک در آینده هر شش ماه یکبار اقدامات سازمان را پیگیری خواهد کرد. دولت از مقاماتی که هنوز استاندارد را اجرا نکرده اند ، تقاضا خواهد کرد که شرح حالی از برنامه‌هایی که برای پیروی از استاندارد ها دارند، به دولت ارائه دهند.

پیشرفت تلاش های مشاوره ملی

مرکز امنیت سایبری که یک مرجع ملی امنیت ICT است، مسئول مشاوره ملی مرتبط با امنیت سایبری در بخش های دولتی و خصوصی است که به حوادث خاص نیز رسیدگی می‌کند.

توافقنامه های دفاعی ۲۰۱۸-۲۰۲۳ به طور قابل توجهی اقدامات این مرکز را از طریق مشاوره و هدایت های ویژه مخصوصاً در بخشهای پراهمیت تر، تقویت می کند.

در عین حال، ظرفیت مرکز برای شناسایی حوادث خاص تقویت خواهد شد. در کنار مشاوره‌های این مرکز، این افزایش ظرفیت به ادارات و شرکت‌های مسئول در برابر امنیت سایبری پس از حمله رخ داده در بخشهای مهم کمک خواهد کرد.

کار ادارات و شرکت ها در زمینه امنیت اطلاعات باید بر اساس ارزیابی چالش ها باشد که شامل ارزیابی چالش های تجاری و مالی با حفظ اهداف تجاری در صورت بروز حادثه ای از جمله حملات سایبری و اقدامات امنیتی مناسب برای کاهش خطر است. این ارزیابی به معنای پیش بینی سیستم های هر سازمان، از جمله بررسی طراحی فنی و آسیب پذیری آنها است. براساس اولویت بندی تعیین شده و بر اساس ارزیابی چالش ها، اقدامات مناسبی برای مقابله با آسیب پذیری های شناسایی شده صورت می گیرند.

بخش چهارم

بخش چهارم

اقدامات

امنیت پایدار

طرح ۱-۱
ایجاد یک مرکز ملی وضعیت سایبری

یک مرکز ملی وضعیت سایبری در مرکز امنیت سایبری ایجاد خواهد شد. این مرکز شبانه روز کار می کند و یک نمای کلی از وضعیت امنیتی از شبکه های دیجیتال موجود ارائه می دهد. مرکز، وضعیت نظارت فنی بر شبکه ها و منابع اطلاعاتی، رسانه ها و انجمن ها را انجام خواهد داد و اطلاعات مربوط به تهدیدهای جدید و حملات سایبری بالقوه در حال پیمایش را اسکن می کند. علاوه بر این، این مرکز به عنوان یک نقطه ارتباط ملی در برابر حوادث سایبری مرزی عمل خواهد کرد.

طرح ۲-۱
حداقل شرایط لازم برای فعالیت ادارات در زمینه امنیت سایبری و حفاظت اطلاعات

سطح مناسبی از حداقل نیازها برای کنترل امنیت سایبری در ادارت

دولتی باید تأمین شود. همه ادارت دولتی باید به اصول مندرج در استاندارد امنیت اطلاعات ISO27001 پایبند بوده و نسبت به تهیه گواهینامه مربوط اقدام کنند. اداراتی که استاندارد را به طور کامل اجرا نکرده اند، باید برنامه عملیاتی خود را به دولت ارائه دهند. علاوه بر این، ادارات باید یک تصمیم مکتوب در مورد استفاده از دستورالعمل های مربوط به امنیت سایبری بگیرند، نیاز به پیاده سازی فن‌آوری‌های از پیش آزمایش شده برای محافظت در برابر سوءاستفاده از امنیت اطلاعات را بررسی کنند و شرایط مندرج در استراتژی ICT را در دولت مرکزی فراهم کنند.

طرح ۳-۱
نظارت در حوزه سایبری

تغییرات سریع تهدیدات مستلزم انطباق قانون و همچنین تحولات فناوری برای رسیدگی به تهدیدات حاضر را به همراه دارد، به گونه ای که مرکز امنیت سایبری آمادگی بیشتری برای پاسخگویی به حملات سایبری علیه زیرساخت های مهم را دارد. وزارت دفاع دانمارک پیشنهادی را برای اصلاح قوانین در حوزه سایبری ارائه می دهد و بدین ترتیب مرکز امنیت سایبری قادر به شناسایی و جلوگیری از حملات سایبری بیشتری می‌شود و در کنار آن قدرت تحلیل مرکز بهبود می یابد.

طرح ۴-۱
نظارت بر سیستم های مهم ICT در دولت مرکزی

در نتیجه تغییرات گسترده تهدیدها، نیاز به گسترش نظارت فعال برای حفاظت از سیستم های حیاتی ICT دولت مرکزی وجود دارد. بر این

اساس، یک مرکز نظارت در آژانس خدمات ICT دولتی ایجاد خواهد شد که شبانه روز کار می کند. این طرح امکان نظارت ۲۴ ساعته بر سیستم های اداره شده توسط آژانس برای خدمات ICT دولتی را برای کلیه مشتریان آژانس خدمات ICT فراهم می کند. طرح به تدریج و تا سال ۲۰۲۰ به طور کامل پیاده سازی خواهد شد. اداراتی که سیستم های آنها زیر نظر آژانس خدمات اینترنتی دولتی نمی باشد، باید اقدامات لازم را جهت نظارت ۲۴ ساعته انجام دهند.

طرح ۵-۱
ایجاد پورتال دیجیتال مشترک برای تهیه گزارش

گزارش حوادث امنیتی باید یک موضوع ساده و آسان برای شرکت‌ها و ادارات باشد. به همین دلیل باید یک روش دیجیتالی مشترک برای گزارش حوادث امنیتی ایجاد بشود. در این روش، شرکت‌ها باید به حدی برسند که یک حادثه را در هر ماه گزارش کنند. علاوه بر آن، این روش باید امکان ارتباط اطلاعات عمل محور[1] در مورد پیشگیری و رسیدگی به حوادث را به گزارشگر مهیا کند. پورتال دیجیتال برای گزارش حوادث امنیتی از طریق VIRK.DK قابل دسترسی خواهد بود.

طرح ۶-۱
تشکیل مرکز ملی رسیدگی به جرایم ICT

به منظور اطمینان از تلاش مداوم و منسجم جهت مبارزه با جرایم بین المللی، یک مرکز ملی تحت نظارت پلیس دانمارک تأسیس می شود تا به گزارش جرایم بین المللی رسیدگی کند. این مرکز از پلیس جهت

1. Action-Oriented Information

اتخاذ داده ها در زمینه مبارزه و پیشگیری از جرم پشتیبانی خواهد کرد.

طرح ۱-۷
تشکیل همکاری پیشرفته در زمینه جلوگیری از حملات مرتبط با ICT و اجرای آن در پاسخ به چنین حملاتی

حملات مربوطه می توانند با فاصله زیادی بین مجرم و قربانی و با استفاده از روش‌هایی رخ دهند که برای روش هایی که جهت رویارویی با چنین حملاتی آزمایش شده‌اند را به چالش بکشند. بنابراین مهم است که ادارات مربوطه از ابزارها و ظرفیت های لازم برای جلوگیری از وقوع یا تشدید حملات برخوردار باشند. همکاری بین ادارات مسئول در منطقه باید به طور مداوم بهترین پایه ممکن را برای مبارزه با حملات مرتبط با ICT در همه زمان ها تضمین کند. برای این منظور، یک گروه کاری متشکل از وزارت دفاع و وزارت دادگستری ایجاد خواهد شد.

طرح ۱-۸
امنیت بالاتر برای اسناد هویتی

به عنوان یک جامعه، باید بتوانیم به اسناد هویتی که توسط ادارات دولتی ایجاد و صادر شده‌اند، اعتماد داشته باشیم. این برای اسناد هویتی فیزیکی و دیجیتالی مانند گذرنامه، گواهینامه رانندگی و امضای دیجیتالی ملی (NemID) صدق می کند. بدین منظور، نسبت به ایجاد انسجام بین ثبت سند هویت فیزیکی و صدور سند هویت دیجیتالی اقداماتی صورت می گیرند.

طرح ۹-۱
بهبود اولویت بندی زیرساخت های ICT ملی

لیستی جامع از ادارات و شرکتهای دارای زیرساخت دیجیتال تهیه می شود که کارکردهایی حیاتی برای جامعه دارند. شرکتها و مقامات کلیدی، همراه با هرگونه خدماتی دارای اهمیت سایبری در دانمارک شناسایی خواهند شد. شناسایی به همراه ارزیابی تهدید بالقوه، زمینه ای برای اولویت بندی بهتر فعالیت های مرکز نظارت امنیت سایبری و مقابله با حملات سایبری توسط ادارات و شرکت‌های مسئول این بخش ایجاد خواهد کرد.

طرح ۱۰-۱
برقراری ارتباط امن در دولت مرکزی

نیاز به دسترسی گسترده تر برای برقراری ارتباط ایمن بین ادارات وجود دارد. بر این اساس، استفاده از شبکه هایی با سطح امنیتی بالا برای برقراری ارتباط با یکدیگر در ادارات دولتی آسان تر خواهد شد و راه حلی برای ارتباط ایمن از طریق تلفن همراه نیز ارائه خواهد شد.

صلاحیت های بهتر

اقدامات

۱-۲) قضاوت دیجیتال و صلاحیت های دیجیتالی که از طریق سیستم آموزشی به دست آمده است

۲-۲) پورتال آموزشی

۲-۳) تحقیق در مورد فناوری جدید

۲-۴) مشارکت شرکتی برای افزایش امنیت ICT در جامعه تجاری دانمارک

۲-۵) همکاری در زمینه توسعه صلاحیت ها و پرورش فرهنگ امنیتی در دولت مرکزی

۲-۶) انگیزه های آگاهی بهبود یافته با هدف شهروندان و مشاغل

بخش پنجم

بخش پنجم

صلاحیت هـــای بهتر

شـهروندان، شـرکت‌ها و ادارات به دانش لازم دسترسـی کافی دارند و باید خـود را قـادر بـه مواجه با چالش هـای امنیت سـایبری و اطلاعاتی بکنند.

بـه منظـور حمایـت از بهبـود صلاحیـت هـا در بین شـهروندان، شـرکت‌ها و ادارت، دولـت دانمـارک:

- قضـاوت دیجیتـال و مهـارت هـای دیجیتالـی در کـودکان و جوانـان را بهبـود خواهد بخشـید؛
- سـطح آگاهی خود را از امنیت سـایبری در بین شـهروندان، شـرکت‌ها و ادارات دولتـی افزایش خواهد داد؛
- از بهبود دائمی دانش متخصصین در منطقه پشـتیبانی کمّی خواهد کرد؛
- از تلاش های مربوط به امنیت سـایبری و اطلاعاتی در شـرکت ها پشـتیبانی خواهدکرد؛

افزایـش دیجیتالـی شـدن و تغییـرات دائـم تهدیدهـا، نیـاز بـه آگاهی از امنیـت دیجیتـال و بهبـود مهارت‌هـای مربوطـه‌ی متخصصیـن، شـرکت‌ها و سـازمان‌ها جهـت رسـیدگی بـه تهدیـدات سـایبری و امنیـت اطلاعاتـی را افزایـش می‌دهـد.

سـرعت بالای توسـعهٔ فناوری در کنار تلاش کلاهبرداران برای سوءاستفاده

از ایـن فنـاوری هـا همـواره چالـش مهـم ایـن عرصـه بـوده اسـت. بـه همین دلیل، آگاه سـازی شـهروندان راجع به مشـکلات مربوط به امنیت سـایبری و حفاظـت از اطلاعـات بسـیار حائز اهمیت می باشـد تـا از امنیت شـهروندان و تجـارت هـا در ایـن فضـا اطمینان حاصـل کنیم.

قضـاوت دیجیتـال و صلاحیـت هـای دیجیتالـی به دسـت آمـده از سیسـتم آموزشی

بسـیاری از جوانـان دانـش کافـی در مـورد نحـوه محافظـت از خـود و دیگـران در اینترنـت را ندارنـد و یـا در مـورد شـخص ثالـث احتیاطـی نمی‌کننـد. در ایـن زمینـه، سیسـتم آموزشـی نقـش مهمـی بـرای مجهـز کـردن همـه کـودکان و جوانـان بـرای پیمایشـی ایمـن، مسـئولانه و اخلاقی هنـگام اسـتفاده از فنـاوری هـای ICT و رسـانه هـای جمعـی دارد.

بـر ایـن اسـاس، دولـت دانمـارک بـر امنیـت دیجیتالـی از دوران ابتدایی و متوسـطه و تـا پایـان فـارغ التحصیلـی تمرکـز خواهـد کـرد. باید به کـودکان و جوانـان بهتریـن فرصـت هـا بـرای پذیرفتـن امکانـات دیجیتالـی و داشـتن رویکـردی انتقـادی بـه عنـوان اعضـای یـک جامعـه دیجیتـال ارائـه شـود. کـودکان و جوانـان بایـد توانایـی تفکـر انتقـادی دربـاره محتـوای موجـود در اینترنـت را داشـته باشـند، بـه گونـه ای کـه نسـبت بـه تهدیـدات موجـود بـه خاطـر اخبـار جعلـی، رادیـکال سـازی، زورگویـی اینترنتـی، کلاهبـرداری آنلایـن و غیـره نگـران باشـند. آنهـا بایـد در موقعیتـی باشـند کـه بتواننـد بـه راحتـی در اینترنـت پیمایـش کننـد تـا از فرصـت هـای دیجیتالـی بـه روشـی ایمـن و مطمئـن اسـتفاده کننـد. عـلاوه بـر ایـن، آنهـا بایـد از قوانین و عواقـب مرتبـط بـا آنلایـن بـودن آگاه باشـند. بـه کـودکان

و جوانـان بایـد آمـوزش داده شـودکه از نظـر مهـارت دیجیتالـی صلاحیـت داشـته باشـند، مراکـز قـوی دیجیتالـی ایجـاد کننـد و عـلاوه بـر مهـارت هـای لازم مرتبـط بـا دیجیتالـی شـدن، معضـلات اخلاقـی را نیـز درک کننـد.

کـودکان و جوانـان بایـد توانایـی بهـره گیـری ایمـن و مطمئـن از امکانـات دیجیتـال را داشـته باشـند.

افزایش آگاهی از امنیت سایبری و اطلاعاتی

همـه شـهروندان، ادارات و شـرکت‌ها بایـد از تهدیـدات سـایبری آگاه باشـند. عـلاوه بـر ایـن، آنهـا بایـد بـه طـور مـداوم دانـش خـود را در مـورد چنیـن تهدیدهایـی و واکنـش خـود را بـه آنهـا بهبـود بخشـند. آنهـا همچنیـن بایـد از خطراتـی کـه خـود و دیگـران را در معرضشـان قـرار مـی دهنـد، آگاه باشـند.

بـه همیـن منظـور، دولـت یـک پلتفـرم اطلاعاتـی بـا هـدف شـهروندان، شـرکت‌ها و ادارات ایجـاد خواهـد کـرد. شـهروندان، شـرکت‌ها و ادارات دولتـی بایـد بتواننـد اطلاعـات و ابزارهـای مربـوط ، خـاص و مفیـدی را کـه بـه آنهـا امـکان محافظـت از خـود بـه بهتریـن شـکل را می‌دهـد، بیابنـد. تلاش‌هـای بـر پایـه اطلاعـات، بـه افزایـش آگاهـی در مـورد تهدیدهـا کمـک می‌کنـد، در حالـی کـه پورتـال اطلاعـات سـطح بالاتـری از دانـش را فراهـم مـی کنـد کـه افـراد را قـادر مـی سـازد بتواننـد اقدامـات محتاطانـه لازم را انجـام دهنـد.

همانطـور کـه تکنولـوژی توسـعه مـی یابـد، حفاظـت از اطلاعـات ادارات دولتـی بیـش از پیـش پیچیـده می‌شـود و تقاضـای صلاحیـت بهتـر

میان متخصصین این حیطه نیز گسترده تر می شود. در نتیجه دولت از تمامی حوزه های مرتبط دعوت می کند تا در این عرصه رقابتی و حفاظتی شرکت نمایند.

همچنین برای بهبود صلاحیت ها در دولت مرکزی، دولت دانمارک طرح‌های زیادی را آغاز خواهد کرد که هدفشان مدیران، کارمندان و متخصصین دولت مرکزی است. تعدادی از دوره های برگزار شده توسط آکادمی دیجیتال، که توسط دولت در پاییز ۲۰۱۷ به عنوان بخشی از استراتژی مدیریت ICT در دولت مرکزی ارائه شده است، بر رفتارهای آنلاین ایمن و امنیت سایبری و اطلاعاتی متمرکز خواهد بود.

دانش مربوط به فن آوری های جدید

علاوه بر نیاز به آگاهی بیشتر، نیاز به متخصصین امنیتی بیشتر جهت پشتیبانی از دیجیتالی شدن شرکت‌ها و ادارات دولتی به طور امن وجود دارد. این مهارت های تخصصی در عصر دیجیتال بسیار حیاتی هستند و برای حفظ امنیت سایبری و اطلاعات دانمارک بسیار مهم است.

دولت دانمارک از طریق تحقیقات هدفمند تر در مورد اهمیت فن آوری برای مقابله با آسیب‌های دیجیتالی، آگاهی بیشتری را برای بهترین اقدامات، مدل ها و ابزارهای ممکن جهت دستیابی به امنیت سایبری و اطلاعات ایجاد خواهد کرد. این امر توسط بودجه‌های تحقیقات استراتژیک برای تحقیق در مورد فرصت های جدید تکنولوژی امکان پذیر خواهد شد.

تقویت تلاش های سایبری و امنیت اطلاعات در جامعه تجاری

دولت از تثبیت عمومی شرایط امنیت سایبری در جامعه تجاری پشتیبانی خواهد کرد. در کشور دانمارک، شرکت‌ها از تحول دیجیتال استقبال کرده‌اند. گردش کار به طور خودکار انجام شده است، بایگانی‌های کاغذی و دفتر حساب‌ها دیجیتالی شده و وارد سیستم‌های ICT شده‌اند و فعالیت های فروش و بازاریابی بیشتر از طریق اینترنت انجام می‌شوند. این امر باعث رشد و رقابت بیشتر بین شرکت‌ها می‌شود، اما وابستگی به سیستم‌های دیجیتال این شرکت‌ها را در برابر حملات سایبری آسیب‌پذیرتر می‌کند. تحقیق در این موضوع باعث ارائهٔ دوره های مناسب‌تر درمؤسسات آموزشی می شود که در نتیجه باعث می شود در آینده نیروها و متخصصین کارآمدتری برای حفاظت تربیت شوند.

حمله های سایبری به شرکت‌های دانمارک رو به افزایش است. یک حملهٔ سایبری می تواند عواقب جدی‌ای برای شرکت داشته باشد. اما حملات، نقض و یا نشت داده‌ها، در بسیاری از شرکت‌های کوچک و متوسط نیز می تواند راهی برای گسترش حوادث باشد.

دولت اکنون تمرکز خود را بر تقویت امنیت سایبری در شرکت‌ها خواهد گذاشت. این وظیفه به طور مشترک با ذی‌نفعان جامعه تجاری انجام خواهد شد و مشارکتی برای تمرکز بیشتر بر امنیت ICT و مدیریت مسئولانهٔ داده‌ها در جامعه تجاری ایجاد خواهد کرد.

این مشارکت چارچوبی برای ارتقای امنیت ICT و مسئولیت‌پذیری مسئولین ایجاد می‌کند. این مشارکت، پیشگیری در اقدامات امنیتی

را افزایش می‌دهد و استفادهٔ تجاری از استانداردهای امنیتی بین‌المللی را ایجاد می کند. سرانجام، این مشارکت بر افزایش آگاهی ICT مشاوران اصلی شرکت‌ها متمرکز خواهد بود، به گونه‌ای که این مشاوران بتوانند امنیت ICT در شرکت‌های کوچک و متوسط دانمارکی را ارتقا دهند.

دولت با استراتژی خود برای رشد دیجیتالی دانمارک، تصمیم به حفظ هیئت مشاوره بازرگانی در زمینه امنیت[1] ICT گرفت، که مکرراً دولت و شرکت‌ها را به تقویت چارچوب‌های امنیتی ICT و بررسی داده‌ها تشویق می‌کند. این هیئت نقش مشاور برای مشارکت خواهد داشت، و قادر خواهد بود که پیشنهادهایی در مورد روش های خاص (کسب‌وکار) اطلاعاتی ارائه دهد.

در حال حاضر کمبود نیرو و متخصصین توانمند برای حفاظت از شرکت های دیجیتال در دانمارک وجود دارد. همانطور که تکنولوژی‌های پیشرفته و راهکارهای دیجیتالی بیشتر مورد استفاده قرار می‌گیرند،تقاضای شرکت ها برای مهندسین کامپیوتر،آمارشناس‌ها وبرق‌کارها و بقیه افراد دارای مهارت‌های مربوطه افزایش می‌یابد. به همین دلیل دولت یک طرح جدید راه‌اندازی کرده است تا علاقهٔ نیروهای جوان برای آموزش و شرکت در موضوع را برانگیزد. با این طرح دولت تضمین می کند که میزان افراد جوانی که یک دورهٔ آموزش مرتبط با این موضوع (در رشته های STEM) را به طور کامل می‌گذرانند،در طی ۱۰ سال آینده ۲۰ درصد افزایش پیدا خواهد کرد.

منبع: استراتژی های پیشرفت دانمارک، آپریل ۲۰۱۸

1. Virksomhedsrådet for It-sikkerhed: شورای امنیت فناوری اطلاعات

اقدامات برای صلاحیت بهتر

طرح ۱-۲
قضاوت دیجیتالی و صلاحیت‌های دیجیتالی به‌دست آمده از سیستم آموزشی

اقدامات مشترک در سراسر سیستم آموزشی با تمرکز بر افزایش آگاهی از چالش های امنیتی موجود برای کودکان، جوانان و معلمان شکل خواهند گرفت. برنامه های آموزشی مداوم برای افزایش آگاهی در زمینه امنیت سایبری و اطلاع رسانی برای معلمان، دانش آموزان و دانشجویان تدوین خواهد شد.

طرح ۲-۲
پورتال اطلاعات

پورتال اطلاعاتی ایجاد خواهد شد که ارائه دهندهٔ خدماتی نظیر مشاوره‌های قابل دسترسی، ابزارهای خاص برای شهروندان، شرکت‌ها و ادارات راجع به امنیت سایبری و حفاظت از داده ها، و همچنین اطلاعاتی در مورد چگونگی انطباق با قوانین فعلی است. محتوای پورتال به طور منظم به‌روزرسانی می شود.

طرح ۳-۲:
تحقیق در مورد فناوری جدید

دولت دانمارک بودجه بیشتری را برای تحقیقات فناوری اختصاص خواهد داد ، از جمله بودجه پروژه (RESEaRCh2025team

foRSK2025): «امکانات جدید فناوری» تحت نظر صندوق نوآوری دانمارک. این اقدامات تحقیقاتی بر آگاهی در مورد مدل‌ها و ساخت ابزارهای جدید برای ارزیابی تهدیدات، تقویت دانش زیرساخت ها در برابر حملات و همچنین اطلاعاتی است که می توانند به بهبود توانایی ادارات و شرکت‌ها در شناسایی مهاجمان کمک کنند.

طرح ۴-۲

مشارکت برای افزایش امنیت ICT در بین شرکت های دانمارک

دولت دانمارک می خواهد امنیت ICT و مدیریت داده ها را در بین شرکت های دانمارک بهبود بخشد و به کمک آن، امنیت ICT به یکی از نقاط قوت دانمارک تبدیل شود. برای دستیابی به این هدف، مشارکت در بخش‌های دولتی و خصوصی ضروری خواهد بود. علاوه بر آن مستلزم گفتگوی نزدیک و تبادل دانش بین عوامل مختلف است که هر یک می توانند به نوع خود امنیت ICT و مدیریت داده ها را با مراقبت کامل پشتیبانی کنند. بر این اساس، دولت دانمارک اقداماتی را برای همکاری بین بخش دولتی و خصوصی از طریق افزایش مشارکت در حوزهٔ امنیت فناوری اطلاعاتی و مدیریت همراه با مسئولیت پذیری داده ها به عهده خواهد گرفت. هیئت مشاوره بازرگانی دولت دانمارک می خواهد امنیت ICT و مدیریت داده ها را در بین شرکت های دانمارک بهبود بخشد و به کمک آن امنیت ICT به یکی از نقاط قوت دانمارک تبدیل شود. برای دستیابی به این هدف، مشارکت در بخش‌های دولتی و خصوصی ضروری خواهد بود. علاوه بر آن، این مستلزم گفتگوی نزدیک و تبادل دانش

بین عوامل مختلف است که هر یک می‌توانند به نوع خود امنیت ICT و مدیریت همراه با مسئولیت‌پذیری داده‌ها را پشتیبانی کنند. بر این اساس، دولت دانمارک اقداماتی را برای همکاری بین بخش دولتی و خصوصی از طریق افزایش مشارکت در حوزهٔ امنیت فناوری اطلاعاتی و مدیریت همراه با مسئولیت پذیری داده ها به عهده خواهد گرفت. هیئت مشاوره بازرگانی در زمینه امنیت (ICT Virksomhedsrådet for it-sikkerhed) ادامه خواهد داشت.

طرح ۵-۲
همکاری برای توسعه صلاحیت ها و پرورش فرهنگ امنیت در دولت مرکزی

تقاضا برای صلاحیت امنیت سایبری و اطلاعاتی هم میان متخصصان و کابران عمومی بیشتر خواهد شد؛ بنابراین دولت دانمارک از همه احزاب مربوطه دعوت می کند تا در توسعه صلاحیت های زمینه، مشارکت کنند. علاوه بر این، تعدادی طرح برای توسعه صلاحیت های کارمندان دولت آغاز خواهد شد. کارمندان باید برای توسعه صنعت دیجیتال به سطح امنیتی قابل قبولی مجهز شوند.

طرح۶-۲
انگیزه های بهبود آگاهی برای شهروندان و مشاغل

افزایش آگاهی شهروندان و شرکت‌ها به منظور افزایش ایمنی در اینترنت باید به طور منظم انجام شود. افزایش آگاهی ملی همراه با تلاش‌های هدفمند برای شهروندان و شرکت‌ها هنگام رویارویی با

چالش های دیجیتال، همراه با تهدیدات محلی با هدف شرکت‌ها یا گروه های خاص کارمندان در بخش دولتی راه اندازی خواهند شد. از ذینفعان خصوصی و عمومی دعوت می‌شود تا در اجرای این طرح‌ها همکاری کنند.

تلاش مشترک

اقدامات

۳-۱ استراتژی‌های فرعی در سطح بخشی و واحدهای غیرمتمرکز امنیت سایبری؛

۳-۲ تلاش‌های میان بخشی برای حمایت از امنیت سایبری و اطلاعات در بخش‌های مهم؛

۳-۳ مدیریت تأمین‌کنندگان خدمات ICT برون سپاری شده؛

۳-۴ تقویت هماهنگی ملی؛

۳-۵ افزایش میزان مشارکت در همکاری‌های بین المللی؛

۳-۶ ارزیابی وضعیت فعلی امنیت سایبری و امنیت اطلاعات؛

۳-۷ نمای کلی اطلاعاتی که قابل محافظت است؛

۳-۸ معماری امنیت اطلاعات؛

۳-۹ تلاش ملی و بین المللی برای حفاظت از اخلاق داده‌ها و محافظت از داده‌های شخص.

بخش ششم

بخش ششم

تلاش‌های مشترک

این سبک مدیریت امنیتی مبتنی بر ریسک می باشد و باید تقسیم‌بندی مشخصی برای مسئولیت ها در زمینهٔ امنیت سایبری و اطلاعاتی در ادارات و شرکت های پیش‌برندهٔ عملکردهای حیاتی جامعه وجود داشته باشد.

به منظور تضمین تلاش های مشترک در امنیت سایبری و اطلاعاتی، دولت دانمارک بایستی:

- اقداماتی را برای حمایت از کار در زمینه امنیت سایبری و اطلاعات در بخشهای مهم راه اندازی کند؛
- تقاضای بیشتری از مدیریت ادارات در زمینه تأمین کنندگان سیستم های خود که برای جامعه از اهمیت حیاتی برخوردار هستند را داشته باشد؛
- تقویت هماهنگی استراتژیک در سطح ملی؛
- افزایش میزان مشارکت دانمارک در همکاری های بین المللی در این زمینه.

وظایف امنیت سایبری و حفاظت اطلاعاتی توسط طیف وسیعی از ادارات انجام می شود که هرکدام نقش های متفاوتی را بر عهده دارند. تحول مداوم دیجیتال و وابستگی رو به رشد به آن در جامعه، نیاز به هماهنگی بیشتر بین ادارات این حوزه را افزایش می‌دهد. این امر به سطح بالاتری از ادغام مرکزی و استراتژیک اقدامات و ابتکارات در سطح ملی نیاز دارد.

ماهیت چالش های امنیتی بدان معنی است که امروزه امنیت سایبری و اطلاعاتی باید کانون اصلی همه مدیران چه در بخش دولتی و چه در بخش خصوصی باشد. در عین حال، امنیت سایبری و اطلاعاتی در دانمارک نه تنها به اقدامات دولت مرکزی بلکه به تلاش بخش‌هایی که از اهمیت حیاتی در جامعه برخوردارند، بستگی دارد. به همین دلیل، حمایت از اقدامات سایبری و امنیت اطلاعات از طریق افزایش تبادل تجربیات و هماهنگی بین آنها در دولت مرکزی، در بخش‌های خصوصی و در ارتباط با شهروندان و شرکت‌ها لازم است. این کار، به جای در نظر گرفتن مشکلات صرفاً به عنوان یک چالش، به افزایش سطح امنیت دانمارک و تمرکز بر امنیت سایبری و اطلاعاتی به عنوان یک فرصت استراتژیک جهت رشد و شکوفایی بیشتر کمک می‌کند.

تقویت تلاش‌ها در بخش‌های حیاتی

به منظور حفظ امنیت سایبری و اطلاعاتی در دانمارک، تمرکز بخش‌هایی در جامعه که از اهمیت حیاتی برخوردار هستند، بسیار مهم است. بنابراین دولت طرح‌هایی را برای بهبود تلاش‌ها و تمرکز این بخش‌های حیاتی در زمینهٔ امنیت سایبری و اطلاعاتی آغاز خواهد کرد.

متغیر بودن سطح بلوغ و نیازها در بخشهای منفرد به این معنی

است که تلاش‌ها باید متناسب با نیاز بخش‌های مختلف باشد. واحدهای اختصاصی امنیت سایبری و اطلاعاتی برای کمک به ارزیابی تهدیدها، تقویت نظارت، استقرار سیستم‌های امنیتی و توسعه صلاحیت‌ها، و مشاوره و متغیر بودن سطح بلوغ و نیازها در بخش‌های منفرد به این معنی است که تلاش‌ها باید متناسب با نیازبخش‌های مختلف باشد. واحدهای اختصاصی امنیت سایبری و اطلاعاتی برای کمک به ارزیابی تهدیدها، تقویت نظارت، استقرار سیستم‌های امنیتی و توسعه صلاحیت‌ها و مشاوره و راهنمایی ادارات و شرکت‌های فعال در این بخش‌ها ایجاد خواهند شد.

استراتژی های خاص مربوط به بخش

بخش‌های ویژه در حوزهٔ امنیت سایبری و اطلاعاتی در دانمارک باید برنامهٔ مشخصی مربوط به امنیت سایبری و اطلاعاتی که قصد دارند در بخش‌های مربوط به خود اجرا کنند، داشته باشند. به این ترتیب، این بخش‌ها باید استراتژی‌های مخصوص بخش‌ها[1] را بر اساس شرایط خاصی در هر بخش مورد نظر تهیه کنند. هنگام تهیه این استراتژی‌ها، بخش‌ها باید ذی‌نفعان مربوطه را در کار خود مشارکت دهند.

انرژی

تأمین انرژی پایدار شرط لازم برای یک جامعهٔ با عملکرد خوب است. بنابراین، عدم امنیت در بخش انرژی، باعث آسیب‌پذیری کل جامعه می‌شود. با افزایش دیجیتالی شدن، آسیب‌پذیری بخش انرژی از توربین‌های بادی گرفته تا لوازم خانگی، در برابر تهدیدات سایبری به سرعت در حال رشد است.

1. sector specific strategies

امنیت سایبری و اطلاعاتی در دانمارک به اقدامات بخش‌هایی که اهمیت حیاتی برای جامعه دارند، وابسته است

در آینده، تأمین کنندگان تجهیزات دیجیتالی، نرم افزارها و یا ناظرین آن نقش مهمی در تأمین انرژی خواهند داشت. علاوه بر آن، در حال حاضر وابستگی بیشتری به کنترل مبادله انرژی تأسیسات دیجیتالی با کشورهای همسایه و تنظیم نوسانات تولید انرژی از انرژی خورشیدی و بادی وجود دارد. به همین دلیل، قوانینی برای برنامه های احتمالی در بخش های برق و گاز، از جمله موارد خاص احتمالی ICT وضع شده است، به طوری که تهدیدات، آسیب پذیری ها و خطرات جدید را می توان در مراحل اولیه شناسایی و مدیریت کرد. استراتژی های بخش انرژی باید در چارچوب موجود و بر اساس اقداماتی که قبلاً انجام شده اند، باشند.

وزارت انرژی ، تأسیسات و اقلیم دانمارک مسئول تهیه یک استراتژی فرعی برای امنیت سایبری و اطلاعات در بخش انرژی است که حداکثر تا پایان سال ۲۰۱۸ تکمیل شود.

مراقبت از سلامت

یکی از ویژگی‌های بخش مراقبت از سلامت ثبت اطلاعات خصوصی مربوط به سوابق پزشکی، الزامات اسناد و استفاده از دستگاه‌های پزشکی و دیجیتال و... است. این امر بخش بهداشت و درمان را به یک هدف بالقوه برای جرایم سایبری نفوذ یکی از ویژگی‌های بخش مراقبت از سلامت ثبت اطلاعات خصوصی مربوط به سوابق پزشکی، الزامات اسناد و استفاده از دستگاه‌های پزشکی و دیجیتال و... است. این امر بخش بهداشت و درمان را به یک هدف بالقوه برای جرایم سایبری نفوذ اشخاص ثالث به سیستم ها و داده‌های شخصی تبدیل می کند. همکاری گسترده در زمینه درمان بیمار و بخش مراقبت‌های

بهداشتی، همراه با به اشتراک گذاری داده‌های بیمار بین ذینفعان درگیر، خطر حمله مجرمان سایبری به «ضعیف ترین حلقه» را به همراه دارد، مگر اینکه همه ذینفعان از الزامات امنیتی لازم پیروی کنند. بر این اساس، هدف این استراتژی تقویت امنیت سایبری و اطلاعات در بخش بهداشت و درمان برای پیش بینی، جلوگیری، شناسایی و مقابله با حملات سایبری و ادامهٔ اقدامات استراتژیک سلامت دیجیتال در سال ۲۰۱۸-۲۰۲۲ است،که در آن یک انجمن سیاسی سایبری اولویت بر امنیت سایبری در همه زمینه های بخش بهداشت و درمان دارد.

وزارت بهداشت مسئول تهیه یک استراتژی فرعی برای امنیت سایبری و اطلاعات در بخش انرژی است که حداکثر تا پایان سال ۲۰۱۸ تکمیل شود.

حمل و نقل

حمایت از زیرساخت‌های مهم در بخش حمل و نقل توسط سیستم‌های ICT رو به افزایش است که امکان نظارت و کنترل از راه دور یا خودکار را فراهم می کند. با افزایش دیجیتالی شدن، تهدیدات علیه سیستم‌های که دارای سیستم‌های حمل و نقل با درجه تحرک بالا و جریان‌های ترافیکی امن هستند، نیز افزایش می یابد. استراتژی فرعی امنیت سایبری و اطلاعات کل بخش حمل و نقل را پوشش می دهد. با این حال، مناطقی که بیشترین وابستگی را به شبکه و سیستم‌های اطلاعاتی دارند، هواپیمایی و تا حدی راه آهن است. بنابراین، این مناطق به ویژه در معرض تهدیدات سایبری و امنیت اطلاعات قرار دارند. این زیراستراتژی، نمای کلی از چالش‌های

بخش حمل و نقل را به دلیل افزایش استفاده از سیستم‌های کنترل الکترونیکی و تبادل خودکار داده‌ها ارائه می دهد. به همین ترتیب، زیراستراتژی مبنای اولویت بندی کلی کار در زمینه امنیت سایبری و اطلاعاتی در بخش حمل و نقل قرار خواهد گرفت و تا حدی بر اطمینان از حفظ عملکردهای حمل و نقل که برای جامعه از اهمیت اساسی برخوردار است و بخشی دیگر بر ایمنی مسافران متمرکز است.

وزارت حمل و نقل، ساختمان و مسکن مسئول تهیه یک استراتژی فرعی برای امنیت سایبری و اطلاعات در بخش حمل و نقل است که حداکثر تا پایان سال ۲۰۱۸ تکمیل می شود.

مخابرات

ویژگی اصلی بخش ارتباطات از راه دور این است که شبکه ارتباط از راه دور یکی از مهمترین عناصر زیرساخت ICT جامعه ما است. بر این اساس، هنگام تهیه پیش نویس بر اساس قانون امنیت شبکه ها و سیستم‌های اطلاعاتی، دولت دانمارک تمرکز خود را بر این امر تأمین کرد که ارائه دهندگان ارتباطات از راه دور امنیت اطلاعات را بالا نگه دارند. به عنوان یکی از این عناصر، ارائه‌دهندگان ارتباطات از راه دور باید از دسترسی، یکپارچگی و محرمانه بودن در شبکه های مخابراتی خود اطمینان حاصل کنند و باید یک برنامه احتیاطی داشته باشند که در صورت تحت تأثیر قرار گرفتن شبکه‌های مربوطه، عملکرد را در برابر حوادث و بلایای طبیعی و یا حملات سایبری تا حد ممکن تضمین کنند.

وزارت حمل‌ونقل، ساخت و ساز و مسکن مسئول تهیه یک استراتژی فرعی برای امنیت سایبری و اطلاعات در بخش انرژی است که حداکثر تا

پایان سال ۲۰۱۸ تکمیل شود.

بخش مالی

در بخش مالی بخشی به نام FSOR [1] ایجاد شده است. یکی از اهداف این مجمع اطمینان از هماهنگی تلاش مشترک در زمینه امنیت سایبری و حفاظت اطلاعات است. علاوه بر این ، دستورالعمل NIS تا ماه می سال ۲۰۱۸ به قوانین مالی دانمارک نیز خواهد پیوست. استراتژی مکمل شامل انتقال دستورالعمل NIS و توسعهٔ حیطهٔ کاری FSOR در کنار اجرای ابتکارات خاص است. براساس آسیب پذیری های بخش فعلی، این طرح ها به مقاومت بیشتر در برابر حملات سایبری و در نتیجه بهبود امنیت سایبری در بخش مالی کمک خواهند کرد. وزارت صنعت، تجارت و امور مالی مسئول تهیه یک استراتژی فرعی برای امنیت سایبری و اطلاعات در بخش انرژی است که حداکثر تا پایان سال ۲۰۱۸ تکمیل شود.

بخش دریایی

مسئولیت بخش دریایی تأمین امنیت در حوزهٔ ناوبری آب های دانمارک و امنیت کشتی های ثبت شده با عنوان پرچم دانمارک، همراه با خدمه آنها است. امنیت سایبری برای کشتی ها شامل خدماتی مانند نظارت بر ترافیک، هشدارها و اطلاعات ناوبری (NAVTEX ، AIS)، سیستم‌های مورد استفاده کشتی‌ها و نرم افزارهایی برای کارکرد کشتی، از جمله نرم افزارهای پیشرانه و ناوبری است. این استراتژی اجرای دستورالعمل‌های NIS را تکمیل می‌کند. براساس آسیب پذیری های بخش، این طرح‌ها به مقاومت بیشتر در برابر حملات سایبری و در نتیجه بهبود

1. Financial Sector Forum for Operational Robustness : مجمع بخش مالی برای مقاومت عملیاتی

امنیت سایبری در بخش دریایی کمک خواهد کرد. وزارت صنعت، تجارت و امور مالی مسئول تهیه یک استراتژی فرعی برای امنیت سایبری و اطلاعات در بخش انرژی است که حداکثر تا پایان سال ۲۰۱۸ تکمیل شود.

تأمین آب آشامیدنی

از آنجایی که تأمین آب آشامیدنی به هیچ شبکه و سیستم‌های اطلاعاتی وابسته نیست، لذا هیچ استراتژی جداگانه ای برای بخش تأمین آب آشامیدنی تهیه نخواهد شد. با توجه به اینکه همه شرکت های خدماتی می توانند به صورت دستی اداره شوند، با این حال مقامات شهرداری موظفاند برنامه ای برای تأمین آب آشامیدنی آماده کنند. نمی توان تکذیب کرد که با گذشت زمان و تغییر در عملکرد شرکت های آب و برق، وابستگی به کنترل ICT تأمین آب آشامیدنی بیشتر می‌شود، لذا وزارت محیط زیست و غذا به طور منظم ارزیابی می‌کند که تدوین یک استراتژی فرعی برای تأمین آب آشامیدنی لازم است یا نه.

کمیسیون اروپا یک بسته جامع امنیت سایبری را ارائه داده است که هدف کلی آن دستیابی به مقاومت، بازدارندگی و دفاع برای محافظت از اروپا در برابر تهدیدات سایبری است که در عین حال اعتماد شهروندان اروپایی را برای استفاده از روش های دیجیتالی افزایش می دهد. بسته امنیت سایبری در راستای پیشرفت‌های حاصل شده از استراتژی امنیت سایبری اتحادیه اروپا در سال ۲۰۱۳ است که در آن بخشنامه امنیت شبکه و اطلاعات (بخشنامه NIS) یکی از عناصر کلیدی بود. بسته امنیت سایبری کمیسیون اروپا شامل

اقدامـات گسـترده، از جملـه یـک آییـن نامه پیشـنهادی بـرای افزایش وظیفـه آژانـس امنیت سـایبری اتحادیـه اروپـا (ENISA)، و همچنین یـک چارچـوب بـرای صـدور گواهینامه امنیت سـایبری اسـت.

سیستم های (DNS) و خدمات دیجیتالی

دسـتورالعمل NIS بـرای ارائـه دهنـدگان DNS و مدیـران آن و همچنین ارائه‌دهنـدگان برخـی خدمـات دیجیتـال، از جملـه خدمـات رایانـش ابـری،[1] جهـت مدیریـت خطـرات مرتبط با امنیت سـرویس‌های خود و گـزارش آن‌ها، الزاماتـی را اعمـال خواهـد کـرد. ایـن الزامـات از طریـق قوانین جدیـد وزارت صنعت، تجارت و امور مالی در مورد امنیت شـبکه‌ها و سیسـتم‌های اطلاعاتی در رابطـه بـا سیسـتم‌های نـام دامنـه و خدمـات دیجیتالـی اجرا خواهد شـد.

مدیریت تأمین کنندگان خدمات مهم ICT

بخـش عمـده ای از سیسـتم هـای ICT حیاتـی ادارات دانمـارک توسـط ارائه‌دهندگان شـخصی اداره می شـود. این امر مقامات دولتی را موظف می‌کند تا از سـطح امنیتی ارائه دهندگان خدمات، تطبیق اطلاعات و داده ها با قوانین و رعایت حقوق شـهروندان در مورد داده های شـخصی اطمینان حاصل کنند.

بـر ایـن اسـاس، دولـت در قراردادهـای آینـده الزامـات سـختگیرانه‌تری را بـرای کلیـه ادارات دولتـی و سیسـتم هـای حیاتـی ICT در زمینـه تأمیـن کننـدگان بخـش خصوصی در راسـتای مقـررات امنیتی انجام خواهـد داد. در آخـر، دولـت در صورت مجاز دانسـتن این امر در شـرایط اسـتثنایی، صلاحیت دولـت مرکـزی را بـرای تصاحـب سیسـتم‌های اصلـی ICT کـه از طـرف یک مرجـع دولتـی اداره می‌شـوند، مـورد بررسـی قرار خواهـد داد.

1. Cloud Computing Services

همکاری بیشتر و بهبود هماهنگی ملی

اصل مسئولیت پذیری بخشی[1] به این معنی است که در صورت وقوع یک حادثهٔ جدی، بخش معیّنی مسئولیت خاصی نیز بر عهده دارد. این مسئولیت شامل برنامه‌ریزی برای حفظ و ادامه کار در صورت وقوع حادثه است. در نتیجه، مسئولیت امنیت سایبری و اطلاعاتی و محافظت از زیرساختهای حیاتی ما، بین ادارات مسئول بخش‌های مهم، یعنی بخش حمل و نقل، بخش بهداشت و درمان و بخش مالی تقسیم می شود. توافقنامه دفاعی ۲۰۱۸-۲۰۲۳ توانایی مرکز امنیت سایبری را در کمک به ادارات دولت مرکزی مسئول در برابر بخش‌های مختلف را به طور قابل توجه‌ای بهبود می‌بخشد.

تقسیم مسئولیت‌ها بین بخش‌ها باعث می‌شود که ابتکارات، خصوصیات و پیشرفت هر بخش متناسب با امنیت سایبری و اطلاعاتی در نظر گرفته شده باشد. علاوه بر این، مسئولیت یک بخش به هماهنگی هم بین وزارتخانه‌های مربوطه و هم بین ادارات مسئول منجر می‌شود. بسیار مهم است که دولت مرکزی چارچوب کلی استراتژیک را برای امنیت سایبری و اطلاعات تعیین کند و از اقدامات مربوطه در این زمینه در بخشهای حیاتی پشتیبانی کند. برای حمایت و کمک به بخشهای خاص و اطمینان از امنیت سایبری و اطلاعاتی مناسب، یک گروه ویژه موقت متشکل از شرکت‌کنندگان آژانس دیجیتالی‌سازی، مرکز امنیت سایبری و امنیت دانمارک و سرویس اطلاعاتی تشکیل خواهد شد.

برای تطبیق اقدامات سایبری و امنیت اطلاعاتی با تغییرات مداوم و سریع تهدیدات، تقویت هماهنگی ملی میان بخشی در این زمینه

1. Principle of Sectoral Responsibility

ضروری است. به همین دلیل، دولت کمیته راهبری ملی امنیت سایبری و اطلاعاتی را ایجاد خواهد کرد؛ لذا هماهنگی و اشتراک دانش بیشتر در منطقه، انسجام بین اقدامات در بخش‌های منفرد و رویکردهای استراتژیک کلی در زمینه امنیت سایبری و اطلاعات را بهبود می‌بخشد.

علاوه بر این، دولت قصد دارد به همکاری خود با کارشناسان بخش دولتی و خصوصی ادامه دهد و در نتیجه این امر، مجمع گفتگوی امنیت اطلاعات[1] به یک هیئت مشورتی تبدیل خواهد شد که نقش آن‌ها تأمین ورودی و پیگیری استراتژی سایبری خواهد بود.

افزایش مشارکت و همکاری های بین المللی

در سال های آینده، حوزه سایبری در اتحادیه اروپا از اولویت اصلی برخوردار خواهد بود و کمیسیون اروپا نیز از جمله موارد دیگر است که یک بسته سایبری جامع را پیشنهاد داده‌اند. امنیت سایبری به اهمیتی دست خواهد یافت که بخشهای مختلفی از جمله سیاست‌های صنعتی، امنیت انرژی و امنیت تأمین(security of supply)، ارتباطات از راه دور، دفاع، قانون و همچنین دیجیتالی‌سازی در بخش‌های دولتی و خصوصی را شامل خواهد شد. بر این اساس، دولت مایل است همکاری دانمارک را در در مجامع بین‌المللی افزایش دهد. هدف دولت دانمارک این است که در سطح اتحادیه اروپا، NATO و سازمان ملل، بحث‌هایی که مربوط به امنیت سایبری و کنترل اینترنت صورت میگیرد و مستقیماً بر شهروندان دانمارکی، شرکت‌ها و ادارات دولتی تأثیر می‌گذارد، بهتر دیده شود.

1. Dialogforum for Informationssikkerhed

دولت همچنین مایل است سفیر فناوری دانمارک را در زمینه فضای مجازی برای گفتگوهایی با موضوع امنیت سایبری و اطلاعاتی با شرکت‌های بزرگ فناوری چند ملیتی و به طور کلی صنعت فناوری، از جمله اخلاق داده‌ها و محافظت از داده‌ها، وارد صحنه کند. به‌علاوه، دولت مایل است دیپلماسی سایبری را با هماهنگ کردن اقدامات سایبری در وزارت امور خارجه تثبیت کند. هدف از هماهنگی این عملکرد افزایش میزان مشارکت دانمارک در همکاری های بین المللی در زمینه امنیت سایبری است.

علاوه بر این، اقدامی برای تقویت کنترل صادرات تجهیزات، جهت نظارت بر فضای مجازی صورت خواهد گرفت. در اینجا تمرکز بر اطمینان از وضوح مقررات و راهنمایی‌های بهتر از سوی ادارات خواهد بود، به گونه ای که شرکت‌های دانمارکی جرئت لازم برای تمرکز بر صادرات را پیدا کنند و از این طریق صنعت سایبری دانمارک را توسعه دهند که همچنین می تواند به تقویت دفاع سایبری دانمارک نیز کمک کند.

اقدامات

تلاش‌های مشترک

طرح۱-۳

استراتژی‌های بخشی و واحدهای غیرمجاز امنیت سایبری

به منظور تقویت توانایی‌های غیرمتمرکز و قوی در حوزه امنیت سایبری و اطلاعاتی، برای هر یک از بخش‌های مهم یک واحد ایجاد خواهد شد. این واحدها به ارزیابی تهدیدها در سطح بخشی، نظارت، تمرینات جهت آمادگی، استقرار سیستم‌های امنیتی، اشتراک دانش تجربه، دستورالعمل‌ها

و غیره کمک خواهند کرد. به‌علاوه، در سال ۲۰۱۸ استراتژی خاص هر بخش برای هر بخش مهم در ادامه استراتژی ملی آماده خواهد شد.

طرح ۳-۱ a: استراتژی امنیت سایبری و اطلاعاتی برای بخش انرژی

طرح ۳-۱ b: استراتژی امنیت سایبری و اطلاعاتی در بخش مراقبت‌های بهداشتی

طرح ۳-۱ c: استراتژی امنیت سایبری و اطلاعاتی برای بخش حمل‌ونقل

طرح ۳-۱ d: استراتژی امنیت سایبری و اطلاعاتی برای بخش ارتباطات از راه دور

طرح ۳-۱ e: استراتژی امنیت سایبری و اطلاعاتی برای بخش مالی

طرح ۳-۱ f: استراتژی امنیت سایبری و اطلاعاتی برای بخش دریایی

طرح ۳-۲
تلاش‌های بین بخشی برای حمایت از امنیت سایبری و اطلاعاتی بخش‌های مهم

یک کارگروه بین وزارتخانه‌ای با کمک متخصصین مرکز امنیت سایبری، آژانس دیجیتالی‌سازی و سرویس امنیتی و اطلاعاتی دانمارک ایجاد خواهد شد. در مرحله انتقال، و با استفاده از راهنمایی و اقدامات مشترک، گروه ویژه به بخش‌های مهم در طراحی استراتژی‌های بخشی خود، ایجاد واحدهای غیرمتمرکز امنیت سایبری و تبادل تجربه و همچنین تهیه دستورالعمل برای اقدامات و ایجاد برنامه های احتمالی کمک می‌کند.

طرح ۳-۳
مدیریت تأمین کنندگان خدمات خارجی ICT

به منظور ارتقای سطح امنیت ICT و تأمین امنیت سیستم‌های مهم

ICT در ادارات دولتی، الزامات سختگیرانه تری برای کلیه ادارات دولتی در قراردادهای آینده در مورد اقدامات امنیتی لازم و مقررات مدیریتی برای مقررات تأمین‌کنندگان بخش خصوصی ادارات معرفی می‌شود.

طرح ۳-۴
تقویت هماهنگی ملی

هماهنگی استراتژیک حوزه امنیت سایبری و اطلاعات باید بیشتر شود. به همین منظور، یک کمیته راهبری ملی برای امنیت سایبری و اطلاعاتی ایجاد خواهد شد. این گروه راهنما وظیفه پیگیری پیاده سازی استراتژی‌های امنیت سایبری و اطلاعاتی، شروع هرگونه طرح و آنالیز مکمل و بحث و گفتگو در مورد سیاست‌های ملی دانمارک در مورد امنیت اطلاعات را دارد. انجمن گفتگوی امنیت اطلاعات (تالار گفتگو برای اطلاع رسانی Sikkerhed) به یک هیئت مشاوره متشکل از متخصصانی تبدیل خواهد شد که نقش آنها تأمین ورودی و پیگیری استراتژی‌های سایبری و سایر طرح‌های مربوطه به آن خواهد بود.

طرح ۳-۵
تقویت همکاری بین المللی

دولت با ارسال دو بیانیه‌ی سایبری به نمایندگی اتحادیه اروپا در بروکسل، مشارکت دانمارک را در سطح بین المللی تقویت خواهد کرد که به محافظت از منافع دانمارک کمک خواهد کرد. دولت همچنین اختیارات مربوط به سفیر فناوری دانمارک در سیلیکون ولی (Silicon Valley) را با مشاور متخصصی در زمینه امنیت سایبری و اطلاعاتی گسترش خواهد داد، همان‌گونه که با انتصاب یک هماهنگ‌کننده بین‌المللی سایبری در وزارت امور خارجه دانمارک تلاش های دیپلماسی سایبری خود را تقویت

مـی کنـد. عـلاوه بـر این، دانمـارک بـرای مقابله بـا تهدیدهای چنـد جانبه در هلسـینکی با مرکز دفاع سـایبری تعاونی ناتو در تالین و مراکز اروپا مشـارکت خواهـد داشـت. در آخر، اقدامات دانمـارک در زمینه کنترل صـادرات فناوری هـای نظـارت بـر فضـای مجـازی[1] بهبـود خواهـد یافـت تا بـه حضـور تجاری دانمـارک در ایـن منطقـه کمـک کنـد و از سوءاسـتفاده شـخص ثالـث بـرای جاسوسـی از کشـور جلوگیری شود.

طرح ۳-۶
ارزیابی وضعیت امنیت سایبری و اطلاعاتی

بـرای بررسـی تاثیـرات طرح‌هـای اجـرا شـده، نیاز بـه آنالیز متنـاوب ملی از وضعیـت سـایبری و امنیـت اطلاعات اسـت. آنالیز دوره ای ملی گسـتردگی و عمـق وضعیـت امنیت سـایبری و اطلاعاتـی دانمارک را بررسـی می کند. در آن تهدیدهـا، خطـرات، سـطح حفاظـت، طرح‌هـای اجرا شـده، سـازماندهی و هماهنگـی بیـن بخش‌ها و... بررسـی خواهند شـد.

طرح ۳-۷
نمای کلی از اطلاعاتی که ارزش محافظت دارند

بـه منظـور محافظـت از اطلاعـات دارای اهمیـت برای امنیـت ملی و بهبود بررسـی خطرات امنیت اطلاعاتی، طرح‌هایـی برای مروری اجمالی بر اطلاعاتی کـه ارزش حفاظـت دارنـد، اجرا خواهند شـد. این بررسـی بـرای تعیین طبقه بنـدی سـطوح خـاص و امنیت سـطح دولـت و همچنیـن به طور کلـی از نظر اهمیـت اطلاعـات مـورد نظر بـرای جامعه مـورد اسـتفاده قرار خواهـد گرفت.

طرح ۳-۸
معماری امنیت اطلاعات

به منظور حمایت از ادارات در گسـترش دسـتاوردهای وابسـته به ICT که

1. Export Controls on Cyber-Surveillance Technologies

می توانند محرمانه بودن، یکپارچگی، دسترسی و انعطاف‌پذیری سیستم‌ها و خدمات پشتیبانی را تضمین کنند، یک ساختار امنیتی مشترک برای عموم ایجاد می شود که شامل اصول، استانداردها، مؤلفه‌های مشترک و رهنمودها است.

طرح ۹-۳

اقدامات ملی و بین المللی برای حفظ داده ها و محافظت از داده های شخصی

دولت دانمارک با توجه به پردازش داده ها توسط شرکت‌های دانمارکی، طرح‌های مربوط به داده‌ها را در سطح ملی و بین‌المللی مطرح می‌کند. در سطح ملی، راهنمایی‌های مربوط به تجارت برای قوانین حاکم بر مسئولیت، مالکیت و حقوق در ارتباط با استفاده از داده‌ها تهیه می شود. به‌علاوه، یک گروه متخصص شامل نمایندگانی از جامعه تجاری دانمارک با وظیفه توصیه‌هایی برای نظارت داده‌ها تهیه کند. دولت همچنین استراتژی جداگانه‌ای برای موارد حفاظت از اطلاعات شخصی شهروندان دانمارکی آغاز خواهد کرد. در سطح بین‌المللی، دولت موضوع داده و حفاظت از داده را جزو زمینه‌های اصلی سفیر فناوری دانمارک در سیلیکون ولی (Silicon Valley) می‌داند که این به عنوان گامی در جهت افزایش گفتگو با شرکت‌های بزرگ فناوری چند ملیتی است.

بخش هفتم


پیوست: مسئولیت ها و نقش های مربوط به ادارت
در زمینه امنیت سایبری
و اطلاعاتی

بخش هفتم

پیوست: مسئولیت ها و نقش های مربوط به ادارات در زمینه امنیت سایبری و اطلاعاتی

کار امنیت سایبری و اطلاعاتی بر پایهٔ اصل مسئولیت‌بخشی سازمان یافته است. این بدان معنی است که بخشی که مسئولیت روزانه دارد نیز در صورت بروز حادثه ای جدی مسئول خواهد بود. این امر با توجه به آمادگی روزانه ، در صورت وقوع یک حادثه متداوم و در مواقع بهبود پس از یک حادثه، اعمال می‌شود.

اصل مسئولیت بخشی اداراتی که مسئولیت روزانه دارند، در صورت بروز یک حادثهٔ جدی مسئول می‌باشند.

اصل شباهت رویه‌ها و مسئولیت‌هایی که در طول عملیات‌های روزانه اعمال می شوند، تا آنجا که ممکن است در سیستم مدیریت بحران نیز اعمال می شوند.

اصل انحصار وظایف واکنش اضطراری باید تا آنجا که ممکن است، به صورت موضعی به شهروندان آسیب‌دیده نزدیک شود و بر این اساس در پایین‌ترین سطح سازمانی مدیریت شود.

اصل همکاری ادارات مسئولیت جداگانه‌ای جهت هماهنگی با سایر ادارات و سازمان‌ها برای برنامه‌ریزی، پاسخ مناسب و مدیریت

بحران دارد.

اصل احتیاط در شرایطی که اطلاعات نامشخص یا ناقص است، آمادگی باید خیلی زیاد باشد نه خیلی کم. علاوه بر این، باید بتوان به راحتی و به سرعت سطح آمادگی اضطراری را کاهش داد تا از اتلاف منابع جلوگیری شود.

علاوه بر بقیه موارد، اصل مسئولیت بخشی بر این موارد دلالت دارد:

۱) همه ادارات باید پاسخگوی شرایط اضطراری در حیطه اختیارات خود باشند؛

۲) مسئولیت مخصوص هر بخش شامل کلیه عملکردها و خدمات حیاتی مورد نیاز قانون از نظر سیاسی یا اداری می‌باشد

۳) برنامه‌ریزی برای واکنش اضطراری ادارات باید بر اساس یک روند ارزیابی مداوم و منظم چالش‌ها باشد، که مدیریت مسئولیت کلی آن را بر عهده می‌گیرد؛

۴) ادارت عمومی باید تهدیدات بخش خود به طور منظم کنترل کنند.

۱ مسئولیت ها و نقش های امنیت سایبری و اطلاعاتی در حوادث مهم

۱-۱) حوادث درون بخشی

نهاد (ادارات، شرکت‌ها و سازمان‌ها) که مسئولیت روزانه یک سرویس یا عملکرد معین را دارند، در صورت بروز حادثه سایبری نیز همچنان این مسئولیت را بر عهده دارند. در این راستا نهاد باید اطمینان حاصل کند که از هر تأمین‌کننده عملیاتی[1] کمک

1. Operational Supplier

می‌گیرد. علاوهٔ بر این، نهاد می‌تواند از واحدهای امنیت سایبری غیرمتمرکز نیز کمک بگیرد. نهاد مسئول درخواست این کمک و مدیریت اولیه‌ی حوادث است. علاوه بر آن، بسته به وسعت حادثه، نهاد مسئول گزارش دادن حادثه به همه مقامات ذیصلاح و به مرکز امنیت سایبری دانمارک است. در آخر، نهاد مسئول همهٔ ارتباطات خارجی مربوط به حادثه است.

۲-۱) حوادث مهم میان‌بخشی

در ارتباط با حوادث مهم سایبری که چندین بخش را تحت تأثیر قرار می‌دهند، ستاد عملیاتی ملی (NOST، که اعضای دائمی آن شامل پلیس ملی دانمارک، سرویس امنیت و اطلاعات دانمارک و سرویس اطلاعاتی دفاعی دانمارک / مرکز امنیت سایبری می‌باشد) ممکن است وارد عمل شود.

با این حال، در این شرایط اصل مسئولیت بخشی همچنان به قوت خود باقی است، به این معنی که این ادارات مسئول بخشهای مربوطه هستند و باید اطمینان حاصل کنند که یک ارزیابی کلی بر حادثه انجام می شود و گزارش این موضوع را به ادارات مربوطه، از جمله مرکز امنیت سایبری (و در صورت وجود به واحد ستاد عملیاتی ملی) ارائه دهند؛ همانطور که مسئولیت مدیریت حادثه و عواقب آن به عهده ادارات، شرکت‌ها و سازمان های آسیب دیده است. بسته به دامنه و ماهیت حادثه، مرکز امنیت سایبری می‌تواند به نهادهای آسیب دیده کمک کند. به عنوان مثال، مرکز امنیت سایبری ممکن است تحقیقات فنی در مورد حملات سایبری را با هدف متوقف

کردن حادثهٔ به خصوص و همچنین تعیین استراتژی‌های حمله انجام دهد، به گونه ای که بتوان از بروز حادثهٔ مشابه جلوگیری کرد. این تحقیقات با همکاری نزدیک نهاد آسیب‌دیده انجام خواهد گرفت.

در اکثر حملات سایبری مهم، هم به تحقیقات کلی و هم به تحقیقات فنی و امنیتیICT نیاز خواهد بود. به همین منظور، برقراری همکاری نزدیک بین پلیس (از جمله سرویس امنیت و اطلاعات دانمارک) و مرکز امنیت سایبری شکل خواهد گرفت. این همکاری شامل توجیهی متقابل (mutual a briefing) در صورت وقوع حوادث بزرگ سایبری است. به همین ترتیب، اقدامات منسجم معمولاً در ارتباط با حوادث خاص صورت می‌گیرند.

۳-۱) ارتباطات

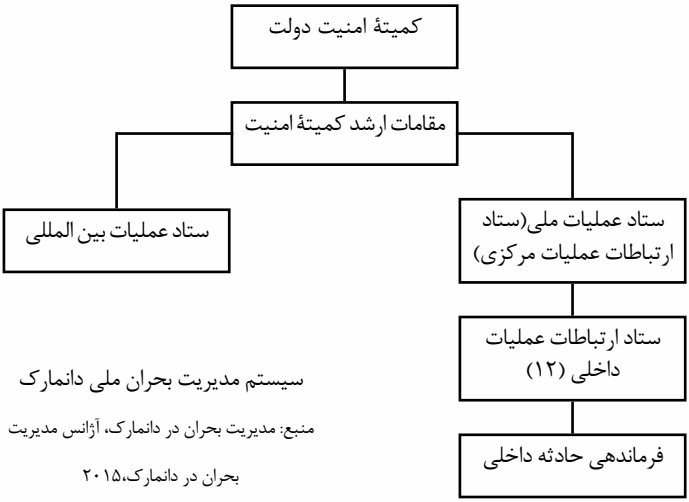
به عنوان یک قاعده کلی، ارتباطات خارجی در ارتباط با حوادث جزئی‌ای که چندین بخش را درگیر نمی‌کنند، توسط ادارهٔ مسئول در برابر بخش مربوطه مدیریت خواهد شد. ارتباطات مربوط به تهدیدات سایبری و گزارش وضعیت فعلی و همچنین سایر ارتباطات بحران در ارتباط با حوادث سایبری به عهده مرکز امنیت سایبری دانمارک با همکاری ادارهٔ مسئول در برابر بخش مربوطه است.

در صورت بروز حادثه ای مهم و بین بخشی، ارتباطات باید هماهنگ باشند. این هماهنگی به عهده سازمان ستاد ارتباطات عملیاتی مرکزی (DCOK)[1] تحت نظارت ستاد عملیاتی ملی (NOST)[2] است.

DCOK مسئول اطمینان حاصل کردن از پخش سریع اخبار مربوط به عموم مردم، از جمله رسانه ها است. DCOK همچنین وظیفه ایجاد

1. Central Operational Communication Staff
2. the National Operative Stthe

واحدهای موقت را بر عهده دارد که عموم مردم می توانند اطلاعات بیشتری در مورد حوادث به دست آورند.



سیستم مدیریت بحران ملی دانمارک

منبع: مدیریت بحران در دانمارک، آژانس مدیریت بحران در دانمارک،۲۰۱۵

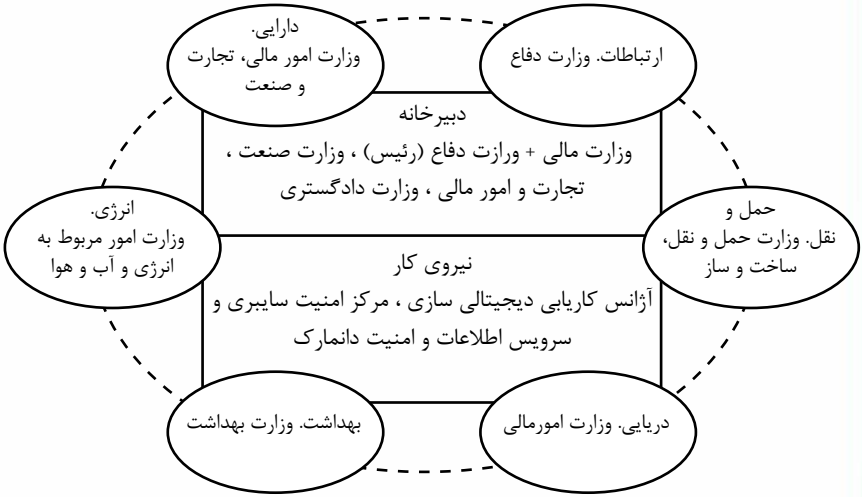
۴-۱) ترمیم بعد از وقوع یک حادثه سایبری

به عنوان یک قاعده کلی ، نهاد تحت تأثیر (اداره ، شرکت و یا سازمان) مسئول ترمیم عملکرد تجاری و همچنین عملکرد ICT بر پایهٔ برنامه پاسخگویی به حوادث است. نهاد مربوطه ممکن است توسط فروشندگان دولتی یا خصوصی در این زمینه و همچنین از واحدهای غیرمتمرکز امنیت سایبری در بخش‌های مختلف پشتیبانی شوند.

۲) هماهنگی مداوم

اقدامات جاری در زمینه امنیت سایبری و حفاظت اطلاعاتی باید با ادارات مربوطه هماهنگ شوند و این امر منوط به اشتراک‌گذاری اطلاعات است. به همین منظور، تعدادی طرح برای حمایت از اقدامات بخش‌ها، ادارات و شرکت‌ها پیشنهاد خواهند شد. این طرح‌ها همچنین هماهنگی ملی را در این زمینه، به ویژه در پیشگیری امنیت ICT تضمین می‌کنند.

این استراتژی بر این ضرورت تأکید می کند که بخشهای دارای اهمیت حیاتی برای جامعه باید یک واحد امنیت سایبری و اطلاعاتی مخصوص به خود ایجاد کنند که بتواند در برابر تهدیدها، ارزیابی آسیب‌پذیری، تمرینات پاسخ اضطراری، تأمین امنیت، اشتراک دانش، دستورالعمل‌ها و غیره پاسخگو باشد.



کمیته راهبری برای پیگیری هماهنگی استراتژی ملی سایبری و اطلاعات

مرکز امنیت سایبری

مرکز امنیت سایبری مرجع ملی امنیت فناوری اطلاعات است که وظایف پیشگیرانه و تخفیف دهنده از جمله خدمات مشاوره‌ای را برعهده دارد. زیرساخت های امنیتی و سرویس امنیت اینترنتی می توانند در شناسایی و هشدار حملات سایبری به ادارات و شرکت‌های عضو این سرویس کمک کنند. مرکز امنیت سایبری به ادارات و شرکت‌های مربوطه در مورد تهدیدات سایبری به خصوص هشدار می‌دهد. این مرکز همچنین از وضعیت ملی و بخش های خاص و گزارش تهیه شده تهدیدات را ارزیابی می‌کند.

پلیس

سرویس امنیت و اطلاعات دانمارک مرجع امنیت ملی دانمارک است و به ادارات دولتی و شرکت‌های خصوصی در زمینه‌های امنیتی، از جمله امنیت اطلاعاتی و همچنین امنیت جسمی، مشاوره می دهد و کمک می‌کند.

آژانس دیجیتالی سازی

آژانس دیجیتالی‌سازی از امنیت اطلاعات در بخش دولتی پشتیبانی می‌کند و مسئول وظایف اطلاعاتی مربوط به شهروندان است. این آژانس همچنین مسئول هماهنگی بین اجرای استراتژی و وزارت دفاع است.

ادارهٔ تجارت دانمارک

اداره‌ی تجارت اطلاعات دانمارک، دستورالعمل ها و ابزارهایی را برای بهبود اقدامات شرکت‌ها به‌وسیله‌ی امنیت ICT و پردازش مسئولانه داده‌ها می‌بخشد.

به منظور تقویت هماهنگی و اجرای استراتژی‌ها، کمیتهٔ ملی هدایت امنیت سایبری و اطلاعاتی جهت ایجاد هماهنگی بین اقدامات در بخش‌های مختلف تشکیل خواهد شد. نیاز به استراتژی‌های مخصوص هر بخش و واحدهای مخصوص امنیت سایبری و اطلاعاتی در هر بخش، هماهنگی به صورت مقطعی در هر بخش و همچنین بین بخش‌ها را تضمین می‌کند. گروهی متشکل از نمایندگان آژانس دیجیتالی‌سازی دانمارک[1]، مرکز امنیت سایبری و سرویس اطلاعاتی و امنیتی دانمارک تشکیل خواهد شد. گروه ویژه‌ای که با مشاوره و اقدامات مشترک به هر بخش در تشکیل واحدهای امنیت سایبری و اطلاعاتی و تهیه استراتژی‌های مخصوص هر بخش کمک خواهد کرد.

سرویس امنیت اطلاعاتی دانمارک، مرجع امنیت ملی و ICT زیر نظر وزارت دادگستری عمل می‌کنند

۳) نهادهای دولتی با مسئولیت میان بخشی در زمینه امنیت سایبری و اطلاعاتی

اقدامات مربوط به امنیت سایبری ادارات عمومی از طریق همکاری، اطلاع‌رسانی، راهنمایی و مشاوره از ارگان‌های دولتی به صورت میان‌بخشی پشتیبانی می شود. ادارات دولتی باید کمک‌های مورد نظر خود را درخواست کنند.

1. Danish Agency for Digitization

۱-۳ مرکز امنیت سایبری

مرکز امنیت سایبری در سال ۲۰۱۲ برای اطمینان از محافظت بهتر در برابر حملات سایبری و غیره بنا شد. با توجه به قانون دفاع سرویس اطلاعاتی دانمارک،[1] سرویس اطلاعات دفاعی دانمارک مقام ملی امنیت ICT است۱ و این سرویس زیر نظر مرکز امنیت سایبری دانمارک اقدامات خود را انجام می‌دهد.

مرکز امنیت سایبری به ادارات دولتی در مورد زمینه های مختلف امنیت سایبری، به عنوان مثال در ارتباط با تهیه سیستم های جدید ICT مشاوره می‌دهد. این مرکز همچنین دستورالعمل هایی در مورد نحوه مدیریت چالش های مربوط به امنیت سایبری ارائه می‌دهد. واحد ارزیابی تهدیدات زیر نظارت مرکز امنیت سایبری گزارش های تهدیدات ملی را تهیه می‌کند.

با توجه به واکنش‌ها، ادارات دولتی می‌توانند جزو زیرساخت‌های مرکز و سرویس امنیت اینترنت شوند و ترافیک مضر ارتباطات مستمر اینترنتی ادارات را کنترل کنند. در صورت شناسایی مورد مشکوک به حمله سایبری، ادارات دولتی می‌توانند برای کمک با این سرویس ارتباط برقرار کنند، به عنوان مثال در قالب یک تیم پاسخ سریع در محل[2].

طبق تصمیم دولت، همه ادارات دولتی موظفند گزارشهای امنیت ICT حائز اهمیت را از طریق سیستم‌های ICT خود به مرکز امنیت سایبری گزارش دهند. به این ترتیب زیرساخت‌ها و سرویس‌های امنیت اینترنتی می‌توانند نظارتی جامع بر وضعیت امنیتی جاری دانمارک داشته باشند.

1. 24 Danish Defence Intelligence Service AC
2. An on-Site Rapid Response Team

مرکز امنیت سایبری مرتباً وضعیت و ارزیابی تهدیدات را گزارش می‌کند. گزارشات طبقه بندی نشده و ارزیابی تهدیدات از طریق وب سایت مرکز امنیت سایبری با آدرس www.cfcs.dk قابل دسترسی می‌باشند. تهدیدات، هشدارها و ارزیابی‌های طبقه‌بندی شده نیز مستقیماً به خود ادارات متضرر ارسال می‌شوند.

توافقنامه های دفاعی ۲۰۱۸-۲۰۲۳ اختیارات مرکز امنیت سایبری را برای کمک به ادارات مسئول به طور قابل توجهی افزایش می‌دهد. تقویت مرکز امنیت سایبری به معنای تقویت نقش‌های مشاوره‌ای و پیشگیرانهٔ این مرکز برای اخطار دادن به بخش‌ها حائز اهمیت است. این امر با تأسیس یک مرکز ملی جدید در زمینه فضای سایبری که ۲۴ ساعته اداره می‌شود، محقق خواهد شد. وظیفه این مرکز عملیاتی کردن اطلاعات به‌دست آمده از منابع اطلاعاتی، داده‌های گزارش شده و در کنار آن تهیه‌ی گزارش از وضعیت امنیتی جاری شبکه‌های دیجیتالی کلیدی خواهد بود.

۲-۳) سرویس امنیتی و اطلاعاتی دانمارک

طبق قانون سرویس اطلاعاتی و امنیتی دانمارک، سرویس امنیتی و اطلاعاتی دانمارک وظیفه دارد از تهدیدها و اقداماتی که برای دانمارک به عنوان یک کشور مستقل، دموکرات و ایمن خطرساز هستند، جلوگیری کند. مسئولیت های سرویس امنیتی و اطلاعاتی دانمارک شامل جرایم مندرج در قسمت ۱۲ (جرایم علیه امنیت ملی و استقلال ملی) و ۱۳ (جرایم علیه قانون اساسی دانمارک و علیه مقامات عالیه، تروریسم و غیره) است. منظور از جرایم، جرایمی است که مرتبط با

سیستم‌های اطلاعاتی و ارتباطی و یا استفاده از فناوری‌های اطلاعاتی و ارتباطی باشند. لذا سرویس امنیتی و اطلاعاتی دانمارک با شناسایی و مدیریت تهدیدات در اسرع وقت به مؤثرترین شکل ممکن در شناسایی و مدیریت تهدیدها سهیم خواهد بود.

به‌علاوه، سرویس امنیتی و اطلاعاتی دانمارک به عنوان یک مقام امنیت ملی، در مورد حفاظت فیزیکی از اطلاعات حساس پیشنهاداتی ارائه خواهد داد. این پیشنهادات در مورد نظارت بر کارکنانی است که دسترسی فیزیکی به اطلاعات و سیستم‌های اطلاعاتی و همچنین ارزیابی امنیتی و مجوزهای امنیتی دارند. در آخر، سرویس امنیت و اطلاعات دانمارک به عنوان مرجع امنیتی ICT زیر نظر وزارت دادگستری فعالیت می‌کند.

۳-۳) پلیس

بر اساس قانون پلیس، پلیس وظیفه دارد از جرایم کیفری پیشگیری کند و راجع به فعالیت‌های مجرمانه، از جمله جرائم مربوط به فناوری اطلاعات تحقیق و آنها را متوقف کند.

به منظور بهبود مدیریت جرایم ICT ، در سال ۲۰۱۴ پلیس ملی دانمارک یک مرکز ملی جرایم سایبری (NC3) ایجاد کرد. به استثنای وظایفی که توسط سرویس امنیتی و اطلاعاتی دانمارک کنترل می شوند، مرکز جرایم سایبری مسئول کلی تعیین اقدامات پلیس برای مقابله با جرائمی مرتبط با ICT است.

حوزهٔ قضایی پلیس شامل کلیهٔ جرایم کیفری در دانمارک است. این همچنین شامل اقداماتی که در خارج از دانمارک انجام

شده‌اند، می‌باشد به شرطی که این اقدامات استقلال دانمارک، امنیت ملی دانمارک یا قانون اساسی دانمارک را نقض کنند یا اگر هدف اعمال مجرمانه در خاک دانمارک قرار گرفته باشند.

علاوه بر آن، طبق قانون مدیریت بحران، پلیس مسئولیت کلیهٔ اقدامات برای واکنش نشان دادن به خسارات عمده‌ای که نیاز به هشدار و غیره دارند را بر عهده دارد.

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