آکادمی الزامات فناوری اطلاعات و ارتباطات برای مدیران ارشد دولتی

سرفصل

۶

امنیت اطلاعات و حریم خصوصی
سازمان اینترنت و امنیت کره

UNITED NATIONS
APCICT - ESCAP

به نام خدا

آکادمی الزامات فناوری اطلاعات و ارتباطات برای مدیران

ارشد دولتی

سرفصل ۶:

امنیت اطلاعات و حریم خصوصی

سازمان اینترنت و امنیت کره

(ویرایش اول)

فهرست مطالب

فصل سوم: فعالیت‌های امنیت اطلاعات **۴۷**

آکادمی الزامات فناوری اطلاعات و ارتباطات برای مدیران ارشد دولتی

سرفصل ۶: امنیت اطلاعات و حریم خصوصی

سازمان اینترنت و امنیت کره

مسئولیت نظرها، اعداد و ارقام و برآوردهای این اثر به عهده نویسندگان است و لزوماً نباید بازتاب دیدگاه یا حامل تأییدیه سازمان ملل متحد تلقی شود.

عناوین به کار رفته و ارائه مطالب در اینجا متضمن بیان هیچ عقیده‌ای از دبیرخانه سازمان ملل متحد درباره وضعیت قانونی هر کشور، حوزه، شهر یا منطقه یا اختیارات آن یا دغدغه‌هایی در مورد محدود ساختن مرزهای آن نیست.

ذکر اسامی شرکت‌ها و محصولات تجاری متضمن تأیید سازمان ملل متحد نیست.

Contact:
United Nations Asian and Pacific Training Centre for Information
and Communication Technology for Development (UN-APCICT/ESCAP)
Bonbudong, 3rd Floor Songdo Techno Park
7-50 Songdo-dong, Yeonsu-gu, Incheon City
Republic of Korea

Tel: 82 32 245 1700-02
Fax: 82 32 245 7712
E-mail: info@unapcict.org
http://www.unapcict.org

ISBN: 978-89-959662-4-2 13560

Design and Layout: Scand-Media Corp., Ltd.
Printed in: Republic of Korea

پیشگفتار

جهانی که ما هم‌اکنون در آن زندگی می‌کنیم دارای ارتباطات درونی گسترده و تغییرات سریع است که عمدتاً ناشی از سرعت رشد و توسعه در فناوری اطلاعات و ارتباطات (فناوری‌های اطلاعاتی و ارتباطی[1]) است. همان‌طور که «مجمع اقتصاد جهانی»[2] به‌درستی بیان می‌کند، فناوری‌های اطلاعاتی و ارتباطی به‌عنوان یک «سیستم عصبی تجمیعی»[3] از طریق هوشمندی و راه‌حل‌های نوآورانه و انطباقی، تمام بافت‌های زندگی ما را به هم مرتبط و تحت تأثیر قرار داده است. در حقیقت فناوری‌های اطلاعاتی و ارتباطی ابزارهایی هستند که می‌توانند کمک بزرگی در حل چالش‌های اقتصادی، اجتماعی و محیطی باشند و توسعه فراگیر و پایدار را ترویج کنند.

دسترسی فزاینده به اطلاعات و دانش از طریق توسعه به کمک فناوری اطلاعات و ارتباطات، پتانسیل بهبود قابل‌ملاحظه معیشت به حاشیه رانده شده‌ها و فقرا را در برداشته و برابری جنسیتی را ترویج می‌کند. فناوری اطلاعات و ارتباطات می‌تواند به‌عنوان پل ارتباطی برای اتصال افراد از کشورها و بخش‌های مختلف (در یک منطقه و حتی فراتر) عمل کرده و ابزاری کارآمد، شفاف و قابل‌اعتماد و هم‌چنین سکویی برای ارتباط و همکاری را فراهم کند. فناوری اطلاعات و ارتباطات برای ارتباطی که تبادل کارآمد محصولات و خدمات را تسهیل می‌کند، ضروری است. موفقیت‌های زیادی در منطقه آسیا و اقیانوسیه ثبت شده‌اند که به‌عنوان مثال می‌توان از موارد زیر نام برد: ابتکارات دولت الکترونیکی دسترسی و کیفیت خدمات عمومی را بهبود داده‌اند، تلفن‌های همراه درآمدهای زیادی را از زوایای مختلف ایجاد می‌کنند، فرصت‌های شغلی برای زنان و صدای آسیب‌پذیرها، از طریق رسانه‌های اجتماعی، از همیشه بلندتر شده است.

با این وجود، شکاف دیجیتالی در آسیا و اقیانوسیه بسیار گسترده (نسبت به سایر نقاط جهان) است. در آمار رتبه‌بندی توسعه به کمک فناوری اطلاعات و ارتباطات، کشورهای این منطقه در سراسر این طیف قرار دارند که تأییدی است بر شکاف دیجیتالی عمیقی که در این نقاط وجود دارد. با وجود پیشرفت‌های قابل‌توجه فناوری و تعهدات بسیاری از بازیگران اصلی در منطقه، دسترسی به ارتباطات پایه هنوز برای همه تضمین شده نیست.

برای پر کردن شکاف‌های دیجیتالی، سیاست‌گذاران باید متعهد به درک بیشتر پتانسیل‌های فناوری اطلاعات و ارتباطات برای توسعه اقتصادی و اجتماعی فراگیر در منطقه باشند. در راستای این اهداف، مراکز آموزشی برای توسعه به کمک فناوری اطلاعات و ارتباطات در آسیا و اقیانوسیه (APCICT)[4]، به‌عنوان آموزشگاه‌های منطقه‌ای کمیسیون اقتصادی و اجتماعی سازمان ملل برای آسیا و

1- Information and Communication Technologies
2- World Economic Forum
3- Collective Nerve System
4- Asian and Pacific Training Centre for Information and Communication Technology

اقیانوسیه [1](UN/ESCAP)، با مأموریت و حکمی برای تقویت تلاش‌های ۶۲ کشور عضو ESCAP در استفاده از فناوری اطلاعات و ارتباطات در توسعه اجتماعی اقتصادی خود، از طریق توسعه ظرفیت‌های اجتماعی و نهادی، در این منطقه تشکیل شد. حکم APCICT در جواب به بیانیه اصول و برنامه عملیاتی اجلاس جهانی جامعه اطلاعاتی [2](WSIS)، مبنی بر اینکه هر شخص باید فرصت به‌دست آوردن مهارت‌ها و دانش ضروری برای درک، مشارکت فعال و بهره‌مندی کامل از جامعه اطلاعاتی و اقتصاد دانشی را داشته باشد، آماده شد.

به‌منظور رعایت بیشتر این دستورالعمل، APCICT یک برنامه درسی آموزشی جامع برای را توسعه به کمک فناوری اطلاعات و ارتباطات [3](ICTD) به نام آکادمی الزامات فناوری اطلاعات و ارتباطات برای مدیران ارشد دولتی توسعه داد. این برنامه در سال ۲۰۰۸ بر اساس تقاضای بالای کشورهای عضو، آغاز به کار کرد. آکادمی ۱۰ سرفصل مجزا و در عین حال مرتبط را که با هدف انتقال دانش و مهارت‌های ضروری به سیاست‌گذاران و هم‌چنین کمک به آن‌ها در برنامه‌ریزی و پیاده‌سازی کارآمدتر خلاقیت‌های فناوری اطلاعات و ارتباطات، طراحی کرد. استفاده گسترده از برنامه‌های آکادمی در سراسر آسیا و اقیانوسیه گواه و تأییدی بر مفادی است که در این سرفصل پوشش داده شده است.

ESCAP از تلاش‌های مداوم APCICT برای به‌روزرسانی و انتشار سرفصل‌های با کیفیت بالای یادگیری توسعه به کمک فناوری اطلاعات و ارتباطات، با توجه به تغییرات سریع در فناوری و بهره‌گیری از منافع دانش توسعه به کمک فناوری اطلاعات و ارتباطات برای ذی‌نفعان ملی و منطقه‌ای، استقبال می‌کند. به‌علاوه، ESCAP از طریق APCICT، استفاده، منطبق‌سازی و ترجمه، این سرفصل‌های آکادمی را به کشورهای مختلف ترویج می‌کند. امید است که با ارائه‌های مستمر کارگاه‌های آموزشی برای مسئولین دولتی در رده‌های مختلف، دانش لازم به آن‌ها انتقال یابد و درک آن‌ها از منافع فناوری اطلاعات و ارتباطات گسترش یافته و منجر به اقدامات مشخص برای رسیدن به اهداف توسعه در سطح ملی و منطقه‌ای گردد.

Noeleen Heyzer

معاون دبیر کل سازمان ملل متحد و دبیر اجرایی ESCAP

1- United Nations Economic and Social Commission for Asia and the Pacific
2- World Summit on the Information Society
3- Information and Communication Technology for Development

مقدمه

در تلاشی برای پوشش شکاف دیجیتالی، اهمیت توسعه منابع انسانی و ظرفیت‌های سازمانی برای استفاده از فناوری اطلاعات و ارتباطات را نمی‌توان دست‌کم گرفت. به خودی خود، فناوری‌های اطلاعاتی و ارتباطی صرفاً یک سری ابزار هستند، اما زمانی که افراد بدانند چگونه به‌طور مؤثر از آن‌ها استفاده کنند، به هدایت‌کننده و محرک ایجاد تحول تبدیل شده و تسریع روند توسعه اجتماعی، اقتصادی و تغییرات مثبت را به دنبال خواهند داشت. با در نظر گرفتن این چشم‌انداز، آکادمی الزامات فناوری اطلاعات و ارتباطات برای مدیران ارشد دولتی، توسعه داده شده است.

این آکادمی برنامه شاخصی از مرکز فناوری اطلاعات و ارتباطات برای توسعه آسیا و اقیانوسیه سازمان ملل است و برای تجهیز مقامات دولتی با دانش و مهارت طراحی شده و به‌طور کامل نفوذ فناوری اطلاعات و ارتباطات برای توسعه اجتماعی و اقتصادی را افزایش می‌دهد. آکادمی به هزاران مخاطب و صدها سازمان در سراسر آسیا و اقیانوسیه، از زمان شروع آن در سال ۲۰۰۸، رسیده است. آکادمی در ۲۰ کشور در منطقه آسیا و اقیانوسیه گسترش پیدا کرده و توسط تعداد زیادی از دولت‌ها به‌عنوان چارچوبی برای آموزش منابع انسانی پذیرفته شده است و هم‌چنین در برنامه درسی مؤسسات عالی و دانشگاه‌های منطقه، گنجانده شده است.

بخشی از تأثیرگذاری آکادمی به خاطر مفاد جامع و گستردگی عناوین پوشش داده شده توسط ۸ سرفصل آموزشی ابتدایی است. هم‌چنین توانایی آکادمی در پیکربندی برای انطباق با بافت‌های محلی و پرداختن به مسائل توسعه اجتماعی و اقتصادی در حال ظهور، نیز شایان توجه است. در سال ۲۰۱۱، در نتیجه تقاضای بسیار زیاد از جانب کشورهای آسیا و اقیانوسیه، APCICT با مشارکت با همکاران و شرکا، دو سرفصل آموزشی را که برای افزایش ظرفیت استفاده از فناوری اطلاعات و ارتباطات در مدیریت بحران و ریسک و تغییرات آب‌وهوا طراحی شده بود، توسعه داد.

در یک رویکرد مشارکتی با APCICT سرفصل‌های جدید آکادمی ۹، ۱۰و ۱۱ همانند سرفصل‌های ۱ تا ۸ در شیوه‌ای فراگیر و مشارکتی توسعه، پیاده‌سازی و تحویل داده شدند و به‌صورت نظام‌مند نظر یک گروه گسترده و استثنایی از ذی‌نفعان توسعه را به خود جلب کردند. کل آکادمی بر اساس موارد زیر تنظیم شده است: نیازهای ارزیابی از سراسر منطقه آسیا و اقیانوسیه؛ رایزنی با مقامات دولتی، اعضای جامعه بین‌المللی، دانشگاهیان و مربیان؛ تحقیق و تحلیل روی نقاط قوت و ضعف مواد آموزشی موجود؛ و یک فرآیند بررسی دقیق که از طریق کارگاه‌هایی که در سطح منطقه و زیرمجموعه‌ها، توسط APCICT سازمان‌دهی شده بود. این کارگاه‌های آموزشی فرصتی با ارزش را برای تبادل تجربه و دانش در بین استفاده‌کنندگان از آکادمی در کشورهای مختلف، فراهم می‌آورند. خروجی

و نتیجه آن نیز ۱۰ سرفصل جامع برنامه درسی آکادمی است که گستره مهمی از سرفصل‌های توسعه فناوری ارتباطات و اطلاعات (ICDT)[1] را پوشش داده و دلالت بر وجود نقطه نظرات فراوان و تفاوت‌های ظریف فعلی در سراسر منطقه است.

رویکرد فراگیر و مشترک APCICT برای توسعه آکادمی، شبکه‌ای از مشارکت‌های قوی به‌منظور تسهیل ارائه آموزش توسعه به کمک فناوری اطلاعات و ارتباطات به مقامات دولتی، سیاست‌گذاران، ذی‌نفعان توسعه در سراسر منطقه آسیا و اقیانوسیه و فراتر از آن، ایجاد کرده است. آکادمی به‌صورت مداوم به‌صورت یک چارچوب آموزشی در سطح ملی و منطقه‌ای (در کشورهای مختلف و با همکاری با APCICT و مؤسسات آموزشی و سازمان‌های ملی و بین‌المللی) مورد قبول و استفاده قرار می‌گیرد. این اصول به‌عنوان نیروی محرک و هدایت‌کننده در تعامل APCICT با شرکا در بهبود و به‌روزرسانی مفاد آکادمی و توسعه سرفصل‌های جدید برای پاسخ‌گویی به نیازها و رسیدن به مخاطبان جدید، مورد استفاده قرار می‌گیرند.

APCICT پلت‌فرم یادگیری از راه دور آنلاین (به نام «آکادمی مجازی APCICT»[2]) که امکان مطالعه و یادگیری مطالب به‌صورت فردی را فراهم می‌کند، به‌عنوان مکمل ارائه چهره به چهره برنامه‌های آکادمی را توسعه داده است. این آکادمی مجازی اطمینان حاصل می‌کند که سرفصل‌های آکادمی و مواد همراه، به‌سادگی قابل‌دسترسی برای دانلود، انتشار، سفارشی‌سازی و بومی‌سازی، هستند. آکادمی هم‌چنین به‌صورت DVD، برای کسانی که دسترسی محدود به اینترنت دارند، موجود است.

برای افزایش قابلیت دسترسی و ارتباط در زمینه‌های محلی، APCICT با همکاری شرکا توانسته‌اند تا این آکادمی‌ها را به زبان‌های مختلف در دسترس قرار دهند و برنامه‌ریزی برای ترجمه به زبان‌های دیگر نیز انجام شده است.

به‌طور مشخص، توسعه و ارائه آکادمی بدون تعهد، از خود گذشتگی و مشارکت فعال بسیاری از افراد و سازمان‌ها، امکان‌پذیر نمی‌بود. در این فرصت از تمام دولت‌ها، وزارتخانه‌ها، مؤسسات آموزشی و سازمان‌های منطقه‌ای و ملی که در توسعه این آکادمی‌ها مشارکت داشته‌اند، تشکر می‌شود. آن‌ها نه تنها ورودی‌های با ارزش را برای محتوای سرفصل‌ها ارائه داده‌اند، بلکه به حامیان آکادمی، در کشور و منطقه خود، تبدیل شده‌اند، اما مهم‌تر از آن، نقش عمده‌ای است که آکادمی‌ها در تبدیل شدن به جزء مهم چارچوب ملی و منطقه‌ای برای ایجاد ظرفیت‌های فناوری اطلاعات و ارتباطات برای برآوردن اهداف توسعه آینده اقتصادی-فرهنگی، بازی کرده‌اند.

1- Information and Communication Technology for Development
2- APCICT Virtual Academy

هم‌چنین تلاش قابل‌توجه بسیاری از مشارکت‌کنندگان که توسعه سرفصل ۲ را امکان‌پذیر کرده‌اند، قابل‌تقدیر است. به‌علاوه، از ۷۵۰۰ شرکت‌کننده که تا کنون ۸۰ کارگاه آکادمی که در ۲۰ کشور برگزار شده و مخاطبان دوره‌های آموزشی آنلاین، قدردانی می‌گردد. بینش ارزشمند و انتقادات و پیشنهادهای آن‌ها به آکادمی در ایجاد تأثیرگذاری پایدار کمک کرده است.

ما به‌طور صادقانه امیدواریم که این آکادمی‌ها در کاهش شکاف دانشی منابع انسانی فناوری اطلاعات و ارتباطات، رفع موانع قبول فناوری اطلاعات و ارتباطات و ترویج استفاده از فناوری اطلاعات و ارتباطات در شتاب توسعه اجتماعی-اقتصادی و دستیابی به اهداف توسعه هزاره سوم، کمک کند.

Hyeun- Suk Rhee
مدیر UN-APCICT/ESCAP

درباره مجموعه سرفصل‌ها

امروزه و در «عصر اطلاعات»[1]، دسترسی آسان به اطلاعات نحوه زندگی و کار ما را دچار تحول کرده است. «اقتصاد دیجیتالی»[2] که به‌عنوان «اقتصاد دانشی»[3]، «اقتصاد شبکه‌ای»[4] و «اقتصاد جدید»[5]، نیز اشاره می‌گردد، با یک تغییر از تولید کالاها به ایجاد ایده‌ها، مشخص شده است. این تأکیدی بر رشد نقش فناوری اطلاعات و ارتباطات (و حتی نقش مرکزی) در اقتصاد و اجتماع است.

در نتیجه، دولت‌ها در سطح جهان، به‌صورت گسترده تمرکز خود را بر توسعه به کمک فناوری اطلاعات و ارتباطات افزایش داده‌اند. برای دولت‌ها، توسعه به کمک فناوری اطلاعات و ارتباطات نه تنها برای توسعه صنعت فناوری اطلاعات و ارتباطات یا بخش اقتصادی اهمیت دارد، بلکه شامل استفاده از فناوری اطلاعات و ارتباطات برای ایجاد رشد اقتصادی، اجتماعی و سیاسی نیز می‌گردد.

هرچند، در بین مشکلاتی که دولت‌ها در تنظیم سیاست‌های فناوری اطلاعات و ارتباطات با آن روبرو هستند، این است که سیاست‌گذاران اغلب با فناوری‌هایی که برای توسعه ملی به‌کار می‌گیرند، آشنایی لازم را ندارند. از آنجایی که نمی‌توان آنچه را که درک نمی‌شود تنظیم کرد، بسیاری از سیاست‌گذاران از سیاست‌گذاری در فناوری اطلاعات و ارتباطات کنار گذاشته شده‌اند. البته واگذاری کامل فناوری اطلاعات و ارتباطات به متخصصان فناوری نیز کار درستی نیست، زیرا این متخصصان فنی درک مناسبی از پیامدهای سیاست‌ها ندارند.

مجموعه سرفصل‌های آکادمی الزامات فناوری اطلاعات و ارتباطات برای مدیران ارشد دولتی توسط UN-APCICT/ESCAP برای آموزش و افزایش اطلاعات گروه‌های زیر توسعه داده شده است:

۱- سیاست‌گذاران در سطوح ملی و داخلی که مسئولیت سیاست‌گذاری فناوری اطلاعات و ارتباطات را بر عهده دارند؛

۲- مقامات دولتی که مسئولیت توسعه و پیاده‌سازی سیستم‌های مبتنی بر فناوری اطلاعات و ارتباطات را بر عهده دارند؛

۳- مدیران در بخش دولتی که به دنبال استخدام مدیران پروژه و به‌کارگیری ابزارهای فناوری اطلاعات و ارتباطات هستند.

مجموعه سرفصل‌ها، برای توسعه آشنایی با مسائل اساسی مرتبط با توسعه به کمک فناوری اطلاعات و ارتباطات از منظر فناوری و سیاست، هدف‌گذاری شده‌اند. در اینجا منظور توسعه یک

1- Information Age
2- Digital Economy
3- Knowledge Economy
4- Networked Economy
5- New Economy

راهنمای فناوری فناوری اطلاعات و ارتباطات نیست، بلکه ایجاد یک درک خوب از قابلیت‌های فناوری دیجیتال و اینکه فناوری به چه سمتی در حال حرکت است و چه چیزی را به سیاست‌گذاران پیشنهاد می‌کند، است. سرفصل‌هایی که در سرفصل‌ها پوشش داده شده، توسط تحلیل نیازهای آموزشی و بررسی سایر مفاد آموزشی در سطح جهان، تشخیص داده شده است.

سرفصل‌ها به نحوی طراحی شده‌اند که بتوانند به‌عنوان منبع خودخوان برای آموزش، توسط مخاطبان، مورد استفاده قرار گیرند. سرفصل‌ها به‌صورت مستقل و در عین حال مرتبط با یکدیگر، طراحی شده‌اند و سعی شده است که هر سرفصل به مباحث مطرح در سرفصل‌های دیگر مرتبط باشد. هدف بلند مدت این است که سرفصل‌ها به یک دوره آموزشی منسجم که بتوان برای آن‌ها گواهی و مدرک نیز صادر کرد، تبدیل شوند.

هر سرفصل با یک متن کوتاه در رابطه با اهداف سرفصل و اهداف یادگیری که مخاطبین و شرکت‌کنندگان می‌توانند پیشرفت خود را با توجه به آن ارزیابی کنند، شروع می‌گردد. مفاد سرفصل به دو قسمت تقسیم می‌گردد که شامل مطالعات موردی و تمرین‌ها برای کمک به درک مفاهیم کلیدی، می‌شود. تمرین‌ها می‌توانند به‌صورت فردی یا گروهی انجام گیرند. شکل‌ها و جداول برای درک بیشتر بعضی از جنبه‌ها در سرفصل‌ها ارائه شده‌اند. لیست مراجع و منابع آنلاین برای مطالعه بیشتر مخاطبان، در سرفصل‌ها ارائه شده است.

استفاده از توسعه به کمک فناوری اطلاعات و ارتباطات تا حد بسیار زیادی متنوع و گوناگون است، در نتیجه مطالعات موردی و مثال‌ها در داخل یک سرفصل یا در سرفصل‌های مختلف ممکن است متناقض به نظر برسد که البته دور از انتظار نیست. این‌ها شور و هیجان و چالش‌های این نظم نوین در حال ظهور و وعده‌های آن است، در حالی که تمام کشورها در حال جست‌وجو برای پتانسیل‌های فناوری اطلاعات و ارتباطات و ابزارهای توسعه آن هستند.

برای حمایت از مجموعه سرفصل آکادمی به فرمت چاپی، پلت‌فرم آموزش از راه دور آکادمی مجازی APCICT، با کلاس‌های مجازی و ارائه آموزش‌ها به فرمت ویدئو و نیز ارائه اسلایدها، فراهم شده و در دسترس مخاطبان قرار دارد: http://e-learning.unapcict.org.

به‌علاوه، APCICT یک قطب همکاری الکترونیکی را توسعه داده است. این یک سایت آنلاین اختصاص داده شده برای کارکنان و سیاست‌گذاران توسعه به کمک فناوری اطلاعات و ارتباطات است که برای افزودن تجربه یادگیری و آموزشی آن‌ها توسعه داده شده است. این قطب دسترسی به منابع دانشی، در جنبه‌های مختلف توسعه به کمک فناوری اطلاعات و ارتباطات را ایجاد و یک فضای تعاملی را برای به اشتراک گذاشتن دانش و تجربه و همکاری در پیشبرد توسعه به کمک فناوری اطلاعات و ارتباطات فراهم می‌کند.

سرفصل ۶

در عصر اطلاعات، اطلاعات سرمایه‌ای است که باید محافظت شود و سیاست‌گذاران باید بدانند که امنیت اطلاعات چیست و چگونه باید در مقابل نشت اطلاعات و قانون‌شکنی در مورد آن دست به اقدام بزنند. این سرفصل مروری را بر نیاز به امنیت اطلاعات، معضلات و روندهای مربوط به امنیت اطلاعات و فرآیند تدوین یک راهبرد امنیت اطلاعات ارائه می‌دهد.

اهداف سرفصل

اهداف این سرفصل عبارتند از:

۱- تشریح مفهوم امنیت اطلاعات، حریم خصوصی و مفاهیم مرتبط با آن‌ها
۲- توصیف تهدیدهای پیش روی امنیت اطلاعات و چگونگی مقابله با آن‌ها
۳- بحث پیرامون نیازمندی‌های برقراری و پیاده‌سازی خط‌مشی در امنیت اطلاعات و نیز چرخه حیات خط‌مشی امنیت اطلاعات و
۴- ارائه مروری بر استانداردهای امنیت اطلاعات و حفاظت از حریم خصوصی که توسط چند کشور و سازمان‌های بین‌المللی امنیت اطلاعات مورد استفاده قرار می‌گیرند.

نتایج حاصل از یادگیری

بعد از کار روی این سرفصل، خوانندگان باید بتوانند:

۱- امنیت اطلاعات، حریم خصوصی و مفاهیم مرتبط را تعریف کنند؛
۲- تهدیدات پیش روی امنیت اطلاعات را شناسایی کنند؛
۳- خط‌مشی موجود در امنیت اطلاعات را از حیث استانداردهای بین‌المللیِ امنیت اطلاعات و حفاظت از حریم خصوصی ارزیابی کنند؛ و
۴- توصیه‌هایی را در مورد خط‌مشی امنیت اطلاعات که برای محیط کار آن‌ها مناسب است تدوین یا ارائه کنند.

اختصارات

ASN.1	Abstract Syntax Notation One
APCERT	Asia-Pacific Computer Emergency Response Team
APCICT	Asian and Pacific Training Centre for Information and Communication Technology for Development
APDIP	Asia-Pacific Development Information Programme (UNDP)
APEC	Asia-Pacific Economic Cooperation
APT	Advanced Persistent Threat
ASEAN	Association of Southeast Asian Nations
BPM	Baseline Protection Manual
BSI	British Standards Institution
BSI	Bundesamt fűr Sicherheit in der Informationstechnik (Germany)
CAP	Certificate Authorizing Participant (CCRA)
CC	Common Criteria
CCP	Certificate Consuming Participant (CCRA)
CCRA	Common Criteria Recognition Arrangement
CECC	Council of Europe Convention on Cybercrime
CERT	Computer Emergency Response Team
CERT/CC	Computer Emergency Response Team Coordination Center
CIIP	Critical Information Infrastructure Protection (EU)
CISA	Certified Information Systems Auditor
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CM	Configuration Management
CSEA	Cyber Security Enhancement Act
CSIRT	Computer Security Incident Response Team
CTTF	Counter-Terrorism Task Force (APEC)
DDoS	Distributed Denial-of-Service
DID	Defense-In-Depth
DoS	Denial-of-Service
ECPA	Electronic Communications Privacy Act
EGC	European Government Computer Emergency Response Team
ENISA	European Network and Information Security Agency
ERM	Enterprise Risk Management
ESCAP	Economic and Social Commission for Asia and the Pacific (UN)
ESM	Enterprise Security Management
EU	European Union
FEMA	Federal Emergency Management Agency (USA)
FIRST	Forum of Incident Response and Security Teams
FISMA	Federal Information Security Management Act
FOI	Freedom of Information
GCA	Global Cybersecurity Agenda
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technology
IDS	Intrusion Detection System

IGF	Internet Governance Forum
IM	Instant-Messaging
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ISO/IEC	International Organization for Standardization and International Electrotechnical Commission
ISP	Internet Service Provider
ISP/NSP	Internet and Network Service Provider
IT	Information Technology
ITU	International Telecommunication Union
ITU-D	International Telecommunication Union – Development Sector
ITU-R	International Telecommunication Union – Radiocommunication Sector
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
KCC	Korea Communications Commission
KISA	Korea Internet & Security Agency
NIS	Network and Information Security
NISC	National Information Security Center (Japan)
NIST	National Institute of Standards and Technology (USA)
OECD	Organisation for Economic Co-operation and Development
OMB	Office of Management and Budget (USA)
OTP	One-Time Password
PC	Personal Computer
PIA	Privacy Impact Assessment
PP	Protection Profile
PSG	Permanent Stakeholders Group
RFID	Radio Frequency Identification
SAC	Security Assurance Component
SFR	Security Functional Requirement
SG	Study Group (ITU)
SME	Small and Medium Enterprise
ST	Security Target
TEL	Telecommunications and Information Working Group (APEC)
TOE	Target of Evaluation
TSF	TOE Security Functions
UK	United Kingdom
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNDP	United Nations Development Programme
US	United States
USA	United States of America
WPISP	Working Party on Information Security and Privacy (OECD)
WSIS	World Summit on the Information Society

لیست آیکن‌ها


مطالعه موردی


پرسش‌هایی برای تفکر


فعالیت


خودآزمایی

فصل اول

نیاز به امنیت اطلاعات

هدف این فصل عبارت است از:
- توضیح مفهوم اطلاعات و امنیت اطلاعات؛ و
- توصیف استانداردهایی که در فعالیت‌های امنیت اطلاعات به‌کار می‌روند.

زندگی انسان امروز تا حد زیادی متکی بر فناوری اطلاعات و ارتباطات[1] (ICT) است. این امر باعث می‌شود افراد، سازمان‌ها و کشورها در مقابل حملات به سیستم‌های اطلاعاتی، از قبیل هک، تروریسم سایبری، جرم‌های رایانه‌ای و مشابه آن‌ها آسیب‌پذیر باشند. تعداد کمی از سازمان‌ها و افراد برای مواجهه با چنین حملاتی مجهز هستند. دولت‌ها از طریق گسترش زیرساخت‌های اطلاعاتی-ارتباطی و برقراری سیستم‌هایی برای محافظت در مقابل تهدیدها در امنیت اطلاعات، نقش مهمی را در تضمین امنیت اطلاعات بازی می‌کنند.

۱-۱ مفاهیم مبنا در امنیت اطلاعات

اطلاعات چیست؟

به‌طور کلی، اطلاعات به‌عنوان نتیجه فعالیت ذهنی تعریف می‌شود؛ اطلاعات یک محصول ناملموس است که از طریق رسانه‌ها انتقال می‌یابد. در حوزه فناوری اطلاعات و ارتباطات، اطلاعات نتیجه پردازش، دستکاری و سازمان‌دهی داده‌هاست که به‌طور ساده مجموعه‌ای از حقایق هستند.

در حوزه امنیت اطلاعات، اطلاعات به‌عنوان یک "دارایی" تعریف می‌شود؛ چیزی که دارای ارزش است و بنابراین باید محافظت شود. در سرتاسر این کتاب، تعریف اطلاعات و امنیت اطلاعات موجود در ISO/IEC 27001:2005 مورداستفاده قرار می‌گیرد.

امروزه، ارزش منتسب به اطلاعات منعکس‌کننده انتقالی است که از جامعه مبتنی بر کشاورزی به جامعه صنعتی و نهایتاً به جامعه اطلاعات‌گرا رخ داده است. در جوامع مبتنی بر کشاورزی، زمین

1- Information and Communication Technology

مهم‌ترین دارایی بود و کشوری که بیشترین میزان تولید غلات را داشت دارای نفوذ رقابتی بود. در جوامع صنعتی، قدرت سرمایه، از قبیل داشتن ذخایر نفت، عاملی کلیدی در رقابت بود. در جامعه مبتنی بر اطلاعات و دانش، اطلاعات مهم‌ترین دارایی است و توانایی جمع‌آوری، تحلیل و استفاده از اطلاعات مزیتی رقابتی برای هر کشور محسوب می‌شود.

همان‌طور که دورنما از ارزش دارایی خالص به ارزش دارایی اطلاعاتی تغییر یافته است، اجماع رو به رشدی در موردنیاز به حفاظت از اطلاعات وجود دارد. اطلاعات به خودی خود دارای ارزش بیشتری از رسانه‌ای است که آن را در بر دارد. جدول ۱-۱ تفاوت‌های بین دارایی‌های اطلاعاتی و دارایی‌های ملموس را نشان می‌دهد.

جدول ۱-۱ مقایسه بین دارایی‌های اطلاعاتی و دارایی‌های ملموس

ویژگی‌ها	دارایی‌های اطلاعاتی	دارایی‌های ملموس
شکل- نگهداری	هیچ شکل فیزیکی ندارد و می‌تواند منعطف باشد	دارای شکل فیزیکی است
ارزش- تغییرپذیری	وقتی ترکیب و پردازش شود ارزش بیشتری به‌دست می‌دهد	کل ارزش برابر با مجموع ارزش همه دارایی‌هاست.
سهیم شدن	تولید نامحدود دارایی‌های اطلاعاتی امکان‌پذیر است و افراد می‌توانند ارزش را به اشتراک بگذارند.	تولید مجدد غیرممکن است؛ با تولید مجدد، ارزش دارایی کاهش می‌یابد.
رسانه‌ها- وابستگی	باید از طریق رسانه‌ها تحویل داده شود	می‌تواند به‌طور مستقل تحویل داده شود (به‌دلیل شکل فیزیکی آن‌ها)

همان‌طور که در جدول ۱-۱ نشان داده شده، دارایی‌های اطلاعاتی از ریشه با دارایی‌های ملموس تفاوت دارند؛ بنابراین، دارایی‌های اطلاعاتی در مقابل انواع مختلفی از مخاطرات آسیب‌پذیر هستند.

مخاطرات پیش‌روی دارایی‌های اطلاعاتی

همان‌طور که ارزش دارایی‌های اطلاعاتی بالا می‌رود، میل به دست‌یابی به اطلاعات و کنترل آن در میان افراد بیشتر می‌شود. گروه‌هایی تشکیل می‌شود تا از دارایی‌های امنیتی در جهت اهداف مختلف استفاده کنند و بعضی‌ها برای به‌دست آوردن دارایی‌های اطلاعاتی به هر وسیله ممکن تلاش

می‌کنند. دسته دوم شامل هک، تکثیر غیرمجاز، تخریب سیستم‌های اطلاعاتی از طریق ویروس‌های رایانه‌ای و دیگر روش‌ها است. این مخاطرات که ملازم با اطلاعاتی شدن هستند، در بخش ۲ از این سرفصل موردبحث قرار می‌گیرند.

جنبه‌های منفی محیط‌های اطلاعات‌گرا شامل موارد زیر هستند:

افزایش رفتارهای غیراخلاقی ناشی از گمنامی: فناوری اطلاعات و ارتباطات می‌تواند برای حفظ گمنامی استفاده شود و این قابلیت باعث ایجاد زمینه مناسب برای افرادی خاص جهت ارتکاب رفتارهای غیراخلاقی و مجرمانه، از قبیل اکتساب غیرقانونی اطلاعات می‌شود.

ایجاد تعارض درباره مالکیت و کنترل اطلاعات: با گسترش اطلاعاتی‌سازی، پیچیدگی‌های ایجاد شده در بحث مالکیت و کنترل اطلاعات افزایش یافته است. مثلاً، در حالی‌که دولت به‌دنبال ساخت پایگاه داده‌های اطلاعاتی از اشخاص تحت چتر دولت الکترونیکی است، بعضی از بخش‌ها در مورد امکان تجاوز به حریم خصوصی از طریق افشاسازی اطلاعات شخصی برای دیگران اظهار نگرانی می‌کنند.

شکاف‌های اطلاعاتی و ثروت بین طبقات و کشورها: اندازه دارایی‌های اطلاعاتی را می‌توان به‌عنوان یک ابزار سنجش ثروت در جوامع دانش/اطلاعات‌گرا دانست. کشورهای توسعه یافته دارای ظرفیت تولید اطلاعات بیشتر هستند و می‌توانند سود بیشتری از فروش اطلاعات به‌عنوان محصول کسب کنند. از طرف دیگر، کشورهایی که از حیث اطلاعات ضعیف هستند نیاز به سرمایه‌گذاری عظیمی دارند تا بتوانند به اطلاعات دسترسی داشته باشند.

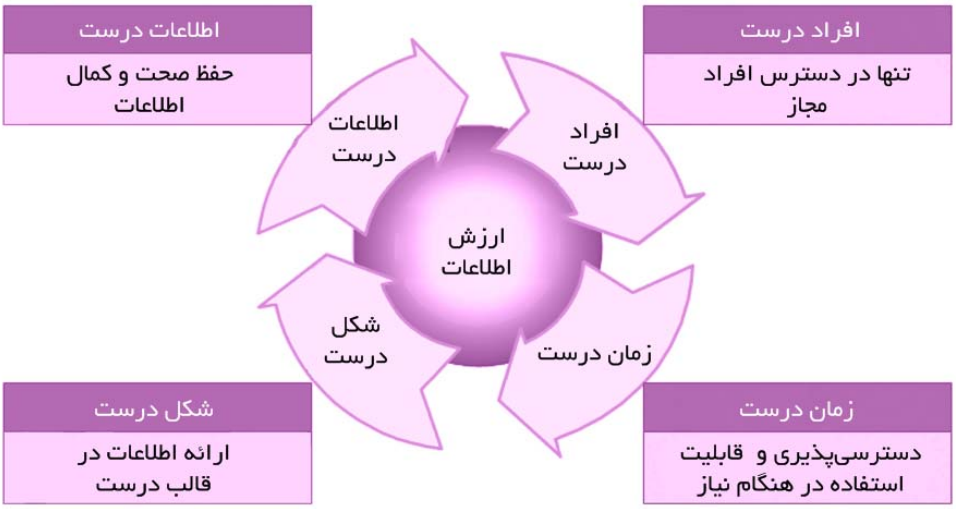
در معرض‌گذاری رو به رشد اطلاعات در نتیجه شبکه‌های پیشرفته: جامعه دانش/اطلاعات‌گرا یک جامعه شبکه‌ای است. کل دنیا همچون یک شبکه ساده به هم متصل شده است. این یعنی ضعف در یک قسمت از شبکه می‌تواند بر بقیه قسمت‌های شبکه اثر منفی داشته باشد.

امنیت اطلاعات چیست؟

در پاسخ به تلاش‌ها برای به‌دست آوردن اطلاعات از راه غیرقانونی، افراد در حال تلاش برای جلوگیری از ارتکاب جرم‌های مرتبط با اطلاعات یا به حداقل رساندن خسارت ناشی از چنین جرم‌هایی هستند. به این اقدامات امنیت اطلاعات گویند. به عبارت ساده، امنیت اطلاعات را می‌توان شناخت ارزش اطلاعات و حفاظت از آن دانست.

چهار مؤلفه اصلی در امنیت اطلاعات

در امنیت اطلاعات چهار مؤلفه اصلی وجود دارد که در زبان انگلیسی به 4R معروفند. این چهار مؤلفه عبارتند از: اطلاعات درست، افراد درست، زمان درست و شکل درست[1]. کنترل روی این چهار مؤلفه کاراترین راه برای نگهداری و کنترل ارزش اطلاعات است.



شکل ۱-۱ چهار مؤلفه اصلی امنیت اطلاعات

"اطلاعات درست" به دقیق و کامل بودن اطلاعات اشاره دارد که صحت اطلاعات را تضمین می‌کند.

"افراد درست" به این معنی است که اطلاعات فقط در دسترس افراد مجاز قرار می‌گیرد، در نتیجه محرمانگی اطلاعات تضمین می‌شود.

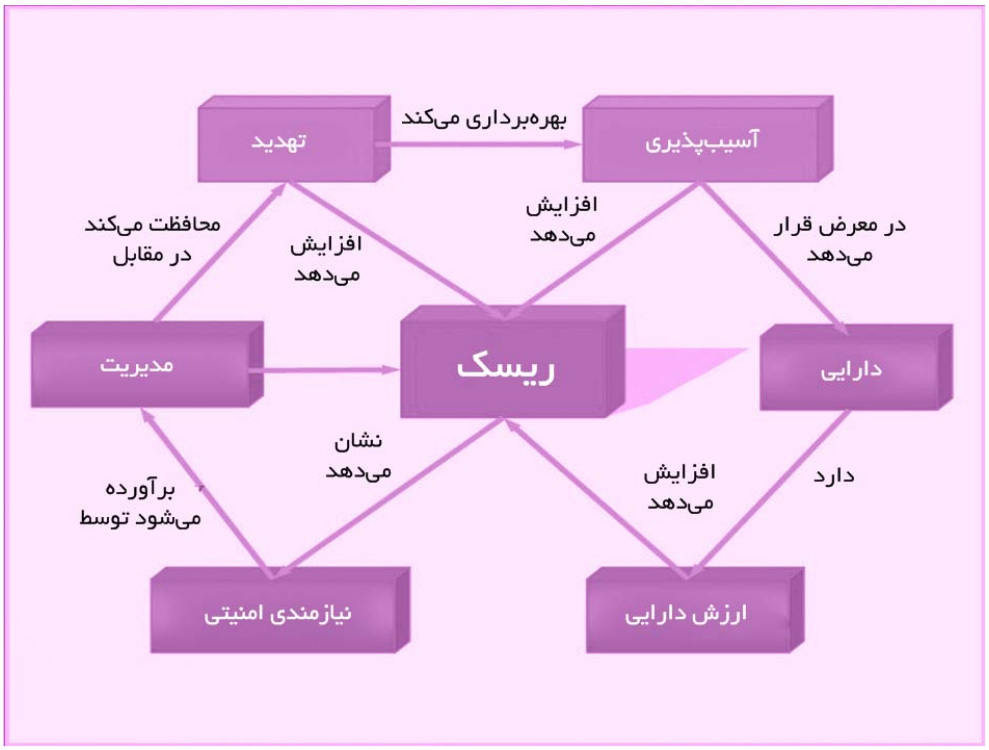
"زمان درست" به دسترسی‌پذیری اطلاعات و قابلیت استفاده آن هنگام نیاز از سوی یک موجودیت مجاز اشاره دارد. این امر دسترسی‌پذیری را تضمین می‌کند.

"شکل درست" مربوط به مهیا کردن اطلاعات در قالب درست است.

برای حفاظت از امنیت اطلاعات، مدل 4R را باید به‌طور صحیح به‌کار گرفت. این بدان معنی است که هنگام کار کردن با اطلاعات، محرمانگی، صحت و دسترسی‌پذیری باید در نظر گرفته شوند.

1- Right Information, Right People, Right Time and Right Form

همچنین، امنیت اطلاعات نیازمند یک درک صحیح از ارزش دارایی‌های اطلاعاتی و نیز آسیب‌پذیری‌ها و تهدیدهای پیش‌روی آن‌ها است. این مسئله مدیریت ریسک گفته می‌شود. شکل ۲-۱ همبستگی بین دارایی‌های اطلاعاتی و ریسک را نشان می‌دهد.



شکل ۲-۱ همبستگی بین ریسک و دارایی‌های اطلاعاتی

ریسک به‌وسیله ارزش، تهدیدها و آسیب‌پذیری‌های دارایی تعیین می‌شود. فرمول آن به این شکل زیر است:

ریسک= ƒ (ارزش دارایی، تهیدها، آسیب‌پذیری‌ها)

ریسک مستقیماً با ارزش، تهدیدها پیش‌رو و آسیب‌پذیری‌های دارایی متناسب است؛ بنابراین، ریسک می‌تواند با تغییر میزان ارزش، تهدیدها و آسیب‌پذیری‌های دارایی افزایش یا کاهش یابد. این کار را می‌توان از طریق مدیریت ریسک انجام داد.

روش‌های مدیریت ریسک عبارتند از:

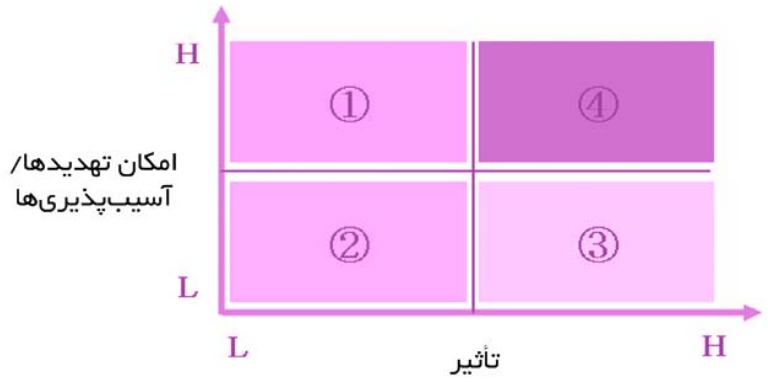
کاهش ریسک (تخفیف ریسک)[1]: این کار زمانی انجام می‌شود که احتمال تهدیدها/ آسیب‌پذیری‌ها بالاست ولی اثر آن‌ها کم است. این عمل شامل شناخت و درک تهدیدها و آسیب‌پذیری‌ها، تغییر یا کاهش آن‌ها و پیاده‌سازی اقدامات پیشگیرانه است. با این حال، کاهش ریسک مقدار ریسک را به "صفر" کاهش نمی‌دهد.

پذیرش ریسک[2]: این عمل زمانی انجام می‌شود که احتمال تهدیدها/ آسیب‌پذیری‌ها پایین و اثر محتمل آن‌ها جزئی و قابل قبول است.

انتقال ریسک[3]: اگر ریسک بیش از حد بالا باشد یا سازمان قادر به آماده‌سازی کنترل‌های لازم نباشد، ریسک را می‌توان به خارج از سازمان منتقل کرد. یک مثال می‌تواند اجرای یک قرارداد بیمه باشد.

دوری گزیدن از ریسک[4]: اگر احتمال رخداد تهدیدها و آسیب‌پذیری‌ها بسیار بالا باشند و اثر آن‌ها نیز بیش از حد زیاد باشد، بهترین کار دوری از ریسک است. این کار به‌عنوان مثال با برون‌سپاری تجهیزات و کارکنان پردازش داده‌ها انجام می‌گیرد.

شکل ۳-۱ نمایشی گرافیکی از این ۴ روش مدیریت ریسک را نشان می‌دهد. در این شکل، مستطیل شماره ۱ کاهش ریسک، شماره ۲ پذیرش ریسک، ۳ انتقال ریسک و ۴ دوری از ریسک هستند.



شکل ۳-۱ روش‌های مدیریت ریسک

نکته مهم در انتخاب روش مدیریت ریسکِ مناسب، اثربخشی هزینه است. تحلیل اثربخشی هزینه را باید پیش از تکمیل طرح برای کاهش، پذیرش، انتقال و دوری از ریسک انجام داد.

1- Risk Mitigation
2- Risk Acceptance
3- Risk Transference
4- Risk Avoidance

۲-۱ استانداردهایی برای فعالیت‌های امنیت اطلاعات

فعالیت‌های امنیت اطلاعات را نمی‌توان بدون بسیج کردن طرح‌های متحد اجرایی، فیزیکی و فنی انجام داد.

بسیاری از سازمان‌ها دارای استانداردهای توصیه شده‌ای برای فعالیت‌های امنیت اطلاعات هستند. به‌عنوان مثال می‌توان به سازمان بین‌المللی استانداردسازی[۱] و کمیسیون بین‌المللی الکتروتکنیک[۲] (ISO/IEC)، نیازمندی‌های امنیت اطلاعات و موارد ارزیابی مربوط به مدرک ممیز تأیید شده سیستم‌های اطلاعاتی[۳] (CISA) و مدرک متخصص تدوین شده امنیت سیستم‌های اطلاعاتی[۴] (CISSP) از مؤسسه ممیزی و کنترل سیستم‌های اطلاعاتی[۵] (ISACA) اشاره کرد. این استانداردها فعالیت‌های متحد و یکپارچه را در امنیت اطلاعات توصیه می‌کنند، از قبیل یک خط‌مشی امنیت اطلاعات، ساخت و اداره یک سازمان امنیت اطلاعات، مدیریت منابع انسانی، مدیریت امنیت فیزیکی، مدیریت امنیت فنی، ممیزی امنیتی و مدیریت تداوم کسب‌وکار.

جدول ۲-۱ فهرست استانداردهای مربوط به حوزه امنیت اطلاعات را نشان می‌دهد.

جدول ۲-۱ حوزه‌های امنیت اطلاعات و استانداردها و گواهی‌نامه‌ها

حوزه‌های امنیتی	ISO/IEC 27001	CISA	CISSP
اجرایی	▪ خط‌مشی امنیتی	▪ حاکمیت فناوری اطلاعات	▪ اقدامات مدیریت امنیت ▪ معماری‌ها و مدل‌های امنیتی
	▪ سازمان امنیت اطلاعات	▪ حاکمیت فناوری اطلاعات	
	▪ مدیریت دارایی	▪ حفاظت از دارایی‌های اطلاعاتی	▪ اقدامات مدیریت امنیت
	▪ امنیت منابع انسانی		

1- International Organization for Standardization
2- International Electrotechnical Commission
3- Certified Information Systems Auditor
4- Certified Information Systems Security Professional
5- Information Systems Audit and Control Association

	▪ مدیریت حوادث امنیت اطلاعات	▪ تداوم کسب‌وکار و بازیابی از فاجعه	▪برنامه‌ریزی تداوم کسب‌وکار و برنامه‌ریزی بازیابی از فاجعه
	▪ مدیریت تداوم کسب‌وکار	▪ تداوم کسب‌وکار و بازیابی از فاجعه	▪ برنامه‌ریزی تداوم کسب‌وکار و برنامه‌ریزی بازیابی از فاجعه
	▪ پیروی	▪ فرآیند ممیزی سیستم‌های اطلاعاتی	▪ قانون، بازرسی و مسائل اخلاقی
فیزیکی	▪ امنیت فیزیکی و محیطی		▪ امنیت فیزیکی
فنی	▪ مدیریت عملیات و ارتباطات	▪ مدیریت چرخه حیات سیستم‌ها و تولید	▪ رمزنگاری ▪ امنیت مخابرات و شبکه ▪ امنیت عملیات
	▪ کنترل دسترسی		
	▪ اکتساب سیستم‌های اطلاعاتی، توسعه و نگهداری	▪ تحویل و پشتیبانی از خدمات فناوری اطلاعات	

ISO/IEC 27001[۱] بر امنیت اجرایی تمرکز دارد؛ به‌ویژه بر مستندسازی و ممیزی عملکرد، به‌عنوان رفتار اجرایی، رعایت اصول راهنما و خط‌مشی‌ها و قانون تأکید دارد. تأییدها و اقدامات پیشگیرانه مستمر به‌وسیله مدیران اجریی الزامی است. از این رو، ISO/IEC 27001 سعی می‌کند تا نقاط ضعف سیستم‌های امنیتی، تجهیزات و مانند این‌ها را به طریق اجرایی مورد بررسی قرار دهد.

برعکس، در CISA که بر فعالیت‌های ممیزی و اقدامات کنترلی در سیستم‌های اطلاعاتی متمرکز گردیده است، هیچ اشاره‌ای به منابع انسانی یا امنیت فیزیکی نشده است. در نتیجه، نقش ممیزان و عملکرد فرآیندهای ممیزی بسیار مهم تلقی شده است.

اصولاً CISSP[۲] بر امنیت فنی تمرکز دارد و آرایش و کنترل تجهیزاتی همچون سرورها و رایانه‌ها را مورد تأکید قرار می‌دهد.

فعالیت

۱- سطح آگاهی از امنیت اطلاعات را در میان اعضای سازمان خود ارزیابی کنید.
۲- سازمان شما چه اقداماتی را در زمینه امنیت اطلاعات انجام می‌دهد؟ این اقدامات را بر اساس چهار روش در امنیت اطلاعات دسته‌بندی کنید.
۳- نمونه‌هایی از اقدامات امنیت اطلاعات را در حوزه‌های اجرایی، فیزیکی و فنی در سازمان خود یا دیگر سازمان‌ها در کشور خود شناسایی کنید.
شرکت‌کنندگان در دوره آموزشی می‌توانند این تمرینات را در گروه‌های کوچک انجام دهند. اگر شرکت‌کنندگان از کشورهای مختلف باشند، گروه‌های کوچک می‌توانند از یک کشور باشند.

خودآزمایی

۱- اطلاعات چه تفاوتی با دیگر دارایی‌ها دارد؟
۲- چرا امنیت اطلاعات برای سیاست‌گذاران یک نگرانی است؟
۳- راه‌های تضمین امنیت اطلاعات چیست؟ روش‌های مختلف پرداختن به امنیت اطلاعات را از همدیگر تفکیک کنید.
۴- موارد تمایز سه حوزه از امنیت اطلاعات (اجرایی، فیزیکی و فنی) را مشخص کنید.

فصل دوم

روندها و دستورالعمل‌های امنیت اطلاعات

اهداف این فصل عبارتند از:

- مروری بر تهدیدهای پیش‌روی امنیت اطلاعات؛ و
- توصیف اقدامات پیشگیرانه در برابر چنین تهدیدهایی.

۲-۱ انواع حملات سایبری

هک کردن

هک کردن به عمل به‌دست آوردن دسترسی به یک رایانه یا یک شبکه رایانه‌ای برای کسب اطلاعات یا تغییر آن بدون حق دسترسی قانونی گفته می‌شود.

هک کردن را می‌توان بسته به هدف هک به سه دسته تفریحی، مجرمانه یا سیاسی تفکیک کرد. هک تفریحی به تغییر غیرمجاز برنامه‌ها و داده‌ها که صرفاً برای ارضای کنجکاوی هکر انجام می‌شود گفته می‌شود. هک مجرمانه در کلاه‌برداری یا جاسوسی مورداستفاده قرار می‌گیرد. هک سیاسی به دست‌کاری سایت‌های وب برای پخش و انتشار غیرمجاز پیام‌های سیاسی اطلاق می‌شود[۳].

اخیراً، هک کردن بیش از گذشته در تروریسم سایبری و جنگ‌های سایبری نمود داشته است که این تهدیدی عمده برای امنیت ملی است. روند جدید دیگر نشان‌دهنده این است که گروه‌های هک سایت‌های اصلی مربوط به منافع ملی را نشانه می‌گیرند که اطلاعات بسیار حساسی را شامل می‌شوند.

کادر ۱- مثال‌هایی از هک‌های مجرمانه و تفریحی

سال ۲۰۱۱ عصر جدیدی را در حملات برجسته هدفمند هویدا کرد که شامل هک شدن RSA، یک ارائه‌کننده راه‌حل‌های امنیتی؛ هک شدن لاکهید مارتین[1]، بزرگ‌ترین پیمان‌کار دفاعی در ایالات متحده؛ هک شدن آزمایشگاه ملی اوک ریج[2]، یک آزمایشگاه تحقیقاتی مربوط به وزارت نیروی ایالات متحده؛ و هک کردن صندوق بین‌المللی پول (IMF)، یک نهاد خاص بین‌المللی در سازمان ملل. سازمان‌های نظامی، مالی، دولتی و

1- Lockheed Martin
2- Oak Ridge National Laboratory

دیگر انواع سازمان‌ها با دارایی‌های فکری، طرح‌ها و منابع مالی در معرض خطر هستند.
لولزسک[1] که یک گروه هکر رایانه‌ای است، اخیراً با پذیرفتن مسئولیت چندین حمله برجسته از جمله سرقت حساب‌های کاربری از شرکت سونی پیکچرز[2] در سال ۲۰۱۱ سرخط خبرها را به خود اختصاص داده است. لولزسک همچنین به ایستگاه‌های رادیویی غیرانتفاعی، مجلس سنای ایالات متحده، CIA، نهادهای وابسته به FBI و دیگر اهداف نفوذ کرد. این گروه همچنین به‌خاطر پیام‌های طنزآمیزی که پس از انجام حملاتش ارسال می‌کند معروف است. بعضی از کارشناسان امنیتی لولزسک را به‌خاطر جلب توجه به سمت سیستم‌های نا امن تحسین کرده‌اند، در حالی‌که بقیه به جهت افشاسازی اطلاعات شخصی افراد و شرکت‌ها ابراز نگرانی می‌کنند.

منبع:

Sophos, Security Threat Report Mid-Year 2011(2011); and Wikipedia, "LulzSec", http://en.wikipedia.org/ /LulzSec

انکار خدمات[3] و انکار توزیع شده خدمات[4]

انکار خدمات (DoS) باعث انجام عملی بر یک رایانه یا یک شبکه رایانه‌ای می‌شود که منجر به مختل شدن یا ناتوان شدن فرآیندها، سیستم‌ها و منابع در پاسخ‌گویی مناسب و کافی می‌گردد. انکار خدمات توزیع شده (DDoS) زمانی رخ می‌دهد که چندین وسیله از مجموعه محل‌های پراکنده به‌طور همزمان در حمله DoS شرکت می‌کنند.

ترافیک خاص یا نوع بهره‌برداری از آسیب‌پذیری‌ها که باعث ناتوانی هدف یا اهداف در پاسخگویی می‌شود معمولاً برای DoS و DDoS یکسان است. منابع توزیع شده‌ای که درگیر در حمله هستند، اغلب دفاع را در برابر حمله دشوارتر ساخته و عموماً در مقابل اهداف بزرگ‌تر و سریع‌تر موفق‌تر عمل می‌کنند[۴].

سایت‌های اینترنتی در کره از حمله DDoS رنج می‌برند

در چهارم مارس سال ۲۰۱۱، کدهای مخرب رایانه‌ای یک حمله DDoS را روی سایت‌های اینترنتی در دفتر ریاست جمهوری و دیگر مؤسسات مهم در جمهوری کره اجرا کردند که باعث تعطیلی موقت بعضی از آن‌ها شد. به‌دنبال حمله DDoS، جمهوری کره سطح هشدار سایبری را بالا برد و این عمل باعث مسدود کردن دسترسی به سرورها و رایانه‌های آسیب‌دیده گشت. کمیسیون ارتباطات کره (KCC)، مرجع تنظیم مخابرات کشور، سومین هشدار سطح بالا را صادر کرد.
صفحه وب کمیسیون خدمات مالی که مرجع تعیین مقررات مالی کشور است، برای مدت کوتاهی در صبح دچار

1- LulzSec
2- Sony Pictures
3- Denial-of-Service
4- Distributed Denial-of-Service

اضافه بار شد و یک سیستم معاملات سهام آنلاینِ متعلق به یک بنگاه محلی برای چندین دقیقه به‌وسیله این هجوم متوقف گردید. آن‌ها عملکرد خود را بازیافتند و هیچ خسارت دیگری گزارش داده نشد. سایت اینترنتی دفتر ریاست جمهوری نیز به‌وسیله یک حمله DDoS مورد هجوم واقع شد، اما هیچ خسارتی به‌وجود نیامد.

این حمله DDoS همچنین سایت‌های اینترنتی وزارت اتحاد[1]، وزارت دفاع، مجلس ملی، مراکز نظامی، نیروهای ایالات متحده در کره، مؤسسات مالی مهم محلی، شرکت‌های اوراق بهادار، پورتال‌های اینترنتی و دیگر نهادهای دولتی مورد هدف قرار داد.

مهاجمان دو سایت اینترنتی کره‌ای را که مختص اشتراک‌گذاری فایل به‌طور همتا به همتا بودند هک کرده و کدهای مخرب را در فایل‌ها جایگذاری کردند، به‌طوری‌که این کدها می‌توانستند به رایانه‌های شخصی دانلود شده و حملات سایبری عظیمی را راه‌اندازی کنند.

برآورد شد که بین ۴,۳۰۰ الی ۱۱,۰۰۰ رایانه شخصی به‌وسیله بدافزارهای این حمله DDoS آلوده شدند. در پاسخ به این حمله، یک شرکت امنیتی نرم‌افزارهای رایگانی را برای درمان توزیع کرد.

منبع:

Yonhap News Agency, “S. Korean Web sites suffer DDoS attack”, 4 March 2011, http://english.yonhapnews.co.kr/national/2011/03/04/36/0301000000AEN20110304007200315F.HTML.

کدهای مخرب

کدهای مخرب[2] برنامه‌هایی هستند که در هنگام اجرا باعث ایجاد خسارت به یک سیستم می‌شوند. ویروس‌ها، کرم‌ها و اسب‌های تروا[3] انواعی از کدهای مخرب هستند.

ویروس[4] **رایانه‌ای**، برنامه‌ای رایانه‌ای یا کد برنامه‌نویسی است که از طریق تکثیر خودش در هنگام کپی شدن در برنامه‌ای دیگر، بخش بوت یا سندی در رایانه، به سیستم‌های رایانه‌ای خسارت وارد می‌کند.

یک کرم[5]، ویروسی خود-تکثیر است که فایل‌ها را تغییر نمی‌دهد بلکه در حافظه فعال می‌ماند و قسمت‌هایی از سیستم عامل را که خودکار بوده و معمولاً برای کاربر غیرقابل‌رؤیت است استفاده می‌کند. تکثیر غیرقابل‌کنترل آن‌ها منابع سیستم را مصرف می‌کند و باعث کندی یا توقف دیگر وظایف می‌گردد. معمولاً تنها هنگامی حضور کرم‌ها تشخیص داده می‌شود که این اتفاق رخ بدهد.

اسب تروا، برنامه‌ای است که به نظر مفید یا بی‌خطر می‌رسد، اما در واقع، کارکردی مخرب دارد، از قبیل خارج کردن برنامه‌های پنهان یا اسکریپت‌های دستوری از حالت بارگذاری که این امر موجب می‌شود سیستم در مقابل تجاوز آسیب‌پذیر شود.

1- Unification Ministry
2- Malicious code
3-Trojan horses
4- Virus
5- Worm

ایران: کرم استاکس‌نت ظهور عصر جدیدی از جنگ‌های سایبری را خبر می‌دهد

در ماه ژوئن سال ۲۰۱۰، کرم استاکس‌نت روی رایانه‌هایی در ایران به‌وسیله یک شرکت امنیتی بلاروسی کشف گردید. این کرم بیش از ۱۰۰,۰۰۰ سیستم رایانه‌ای را در سراسر جهان آلوده کرده بود که بیشتر آن‌ها در ایران بودند.

لس‌آنجلس تایمز گزارش می‌دهد "استاکس‌نت به‌عنوان پیچیده‌ترین سلاح سایبری که تا کنون به‌کار گرفته شده است، شناخته می‌شود و این به‌دلیل شیوه موزیانه‌ای است که در آن به‌کار رفته و این اعتقاد وجود دارد که به‌طور سری تجهیزات خاص مورداستفاده در برنامه هسته‌ای ایران را هدف قرار داده است."

کد مورد نظر برای حمله به سیستم‌های Siemens Simatic WinCC SCADA طراحی شده بود. سیستم‌های زیمنس برای مدیریت خطوط لوله در تأسیسات متعدد، نیروگاه‌های هسته‌ای و تجهیزات خدماتی و تولیدی مختلف مورداستفاده قرار می‌گیرند. اگرچه کرم استاکس‌نت تعداد زیادی از سیستم‌ها را آلوده کرد، بسیاری بر این باورند که این کرم، مخصوصاً برای هدف قرار دادن تأسیسات هسته‌ای ایران ساخته شد. خالق این کرم هنوز ناشناخته است.

منبع:

Ken Dilanian, “Iran’s nuclear program and a new era of cyber war”, Los Angeles Times, 17 January 2011, http://articles.latimes.com/2011/jan/17/world/la-fg-iran-cyber-war-20110117; Kim Zetter, “Iran: Computer Malware Sabotaged Uranium Centrifuges”, Wired, 29 November 2010,http://www.wired.com/threatlevel/2010/11/stuxnet-sabotage-centrifuges/; and Wikipedia, “Stuxnet”, http://en.wikipedia.org/wiki/Stuxnet.

مهندسی اجتماعی

واژه "مهندسی اجتماعی[1]" به مجموعه‌ای از تکنیک‌ها اشاره دارد که برای فریب دادن افراد، جهت فاش کردن اطلاعات محرمانه‌شان، مورداستفاده قرار می‌گیرد. اگرچه روش کار به کلاه‌برداری از راه جلب اعتماد یا یک تقلب ساده شباهت دارد، این واژه معمولاً در مورد اعمال حیله‌گری برای جمع‌آوری اطلاعات یا دسترسی به سیستم به‌کار گرفته می‌شود. در بیشتر موارد، مهاجم هرگز با قربانی رو در رو نمی‌شود.

فیشینگ[2]، یعنی عمل دزدیدن اطلاعات شخصی از طریق اینترنت با هدف ارتکاب کلاه‌برداری مالی، مثالی از مهندسی اجتماعی است. فیشینگ به یک فعالیت مجرمانه چشمگیر در اینترنت تبدیل شده است.

1- Social engineering
2- Phishing

بانک سوئدی با بزرگ‌ترین سرقت آنلاین مورد حمله واقع می‌شود

در نوزدهم ماه ژانویه سال ۲۰۰۷، بانک سوئدی نوردیا[1] با حمله فیشینگ مورد هجوم قرار گرفت. این حمله با یک اسب تروای سفارشی شروع شد که به نام بانک به بعضی از مشتریانش ارسال گردید. فروشنده مشتریان را تشویق می‌کرد که یک برنامه "مبارزه به اسپم" را دانلود کنند. کاربرانی که فایل ضمیمه را با نام "raking.zip" یا raking.exe دانلود کردند به‌وسیله اسب تروایی که از سوی بعضی شرکت‌های امنیتی به نام "haxdoor.ki" نیز شناخته می‌شود، آلوده شدند.

معمولاً haxdoor برنامه‌های ثبت‌کننده کلید[2] را برای ثبت دنباله کلیدهای فشرده شده نصب می‌کند و خودش را با استفاده از یک rootkit پنهان می‌کند. قسمت داده نوع ki. از این اسب تروا هنگامی فعال می‌شد که کاربران اقدام به وارد شدن به سایت بانکداری الکترونیکی نوردیا می‌کردند. کاربران به یک صفحه ورود جعلی هدایت می‌شدند، جایی‌که آن‌ها اطلاعات مهم ورود (log-in)، از قبیل شماره ورود را وارد می‌کردند. پس از اینکه کاربر اطلاعات را وارد می‌کرد، پیام خطایی ظاهر می‌شد و به آن‌ها اطلاع می‌داد که سایت با مشکلات فنی مواجه است. آنگاه تبهکاران اطلاعات برداشت شده مشتریان را در سایت اینترنتی واقعی نوردیا مورداستفاده قرار می‌دادند تا پول را از حساب مشتریان بردارند.

مشتریان نوردیا به‌مدت ۹ ماه به‌وسیله ایمیلی که شامل اسب تروا سفارشی بود مورد هدف قرار گرفتند. گفته شد که دویست و پنجاه مشتری این بانک، با خسارتی در مجموع بین هفت تا هشت میلیون کرونای سوئد (۷۳۰۰ الی ۸۳۰۰ دلار آمریکا در سال ۲۰۰۷) قربانی این حمله شدند.

این مورد ثابت کرد که حملات سایبری حتی می‌توانند شرکت‌های مالی با حفاظت سطح بالای امنیتی را نیز تحت تأثیر قرار دهند.

منبع:

Tom Espiner, “Swedish bank hit by ‘biggest ever’ online heist”, ZDNet.co.uk(19 January 2007),http://news .zdnet.co.uk/security/0,1000000189,39285547,00.htm.

هرزنامه[3]

هرزنامه یک پیام الکترونیکی حجیم، ناخواسته و تجاری است که از طریق سرویس‌های ارتباطی همچون ایمیل تحویل داده می‌شود. هرزنامه رسانه‌ای با هزینه کم و مؤثر جهت تبلیغات است. اخیراً، هرزنامه برای پخش کدهای مخرب یا ربودن اطلاعات شخصی مورداستفاده قرار می‌گیرد. گهگاه، این نوع از هرزنامه از طریق رایانه‌های شخصی قربانی که در بیشتر مواقع با کدهای مخرب آلوده شده‌اند ارسال می‌گردد.

1- Nordia
2- Keylogger
3- Spam

APT

تهدید ماندگار پیشرفته[1] (APT) حمله‌ای در شبکه است که در آن یک شخص غیرمجاز دسترسی به شبکه را به‌دست آورده و در آنجا برای مدت طولانی به‌طور مخفیانه باقی می‌ماند. قصد یک حمله APT به‌جای وارد کردن خسارت به شبکه یا سازمان، دزدیدن داده‌ها است[۵].

حملات APT سازمان‌هایی را هدف قرار می‌دهند که در بخش‌هایی با اطلاعات با ارزش، همچون دفاع ملی، تولید و بخش‌های مالی فعال هستند.

یک مهاجم APT برای دسترسی به شبکه از طریق ابزارهای مجاز، اغلب از "ماهیگیری با نیزه" استفاده می‌کند که نوعی مهندسی اجتماعی است. هنگامی‌که دسترسی محقق شد، مهاجم یک "در پشتی" را ایجاد می‌کند.

گام بعدی جمع‌آوری اطلاعات معتبر از کاربران (مخصوصاً حساب‌های مدیریتی) و گردش در شبکه برای نصب درهای پشتی بیشتر است. درهای پشتی به مهاجم اجازه می‌دهند تا ابزارهای سودمند جعلی را نصب کرده و یک "زیرساخت شبح‌گونه" را برای توزیع بدافزارها ایجاد کند که به‌سادگی قابل‌رؤیت نیست.

RSA با حملات تهدید پایدار پیشرفته هدف قرار می‌گیرد

در ماه مارس سال ۲۰۱۱، RSA که بخش امنیتی EMS است، اعلام کرد که هدف یک حمله قرار گرفته و اطلاعات مربوط به محصولات احراز هویت دو عامله SecurID این مؤسسه توسط مهاجمان به سرقت رفته است. تحقیقات نشان داد که حمله در دسته APT قرار می‌گیرد. تهدیدهای APT چالشی عمده برای همه شرکت‌های بزرگ هستند. برای شناسایی APT ها، سازمان‌ها باید فناوری‌هایی را به‌کار گیرند که نه تنها همه تهدیدهای بالقوه را از طریق تحلیل رفتار شناسایی کنند، بلکه قادر باشند همه عناصر مشکوک را در یک محیط مجازی آزمایش نمایند.

احراز هویت دو عامله روشی ارجح در مهیا کردن امنیت قوی‌تر در مقایسه با روش استفاده از نام کاربری و رمز عبور است. یکی از رایج‌ترین روش‌های احراز هویت دو عامله استفاده از یک زنجیره کلید یا توکن است که کدی تصادفی را مهیا می‌کند و کاربران باید این کد را علاوه بر نام کاربری و رمز عبور وارد کنند تا احراز هویت شده و دسترسی به سایت یا برنامه کاربردی ایجاد شود.

RSA یک فراهم‌کننده پیشرو محصولات احراز هویت دو عامله است و زنجیره کلیدها یا توکن‌های آن عملاً فراگیر شده‌اند. با وجود میلیون‌ها مشتری که برای فراهم آمدن احراز هویت اضافی و حفاظت حساب‌ها از دسترسی غیرمجاز به RSA متکی هستند، اکنون آزاردهنده است که هکرهای بدخواه کلیدهای لازم برای دور زدن آن حفاظت را در اختیار دارند.

1- advanced persistent threat

RSA به مشتریانش تضمین داد که اطلاعاتی که استخراج شده بود حمله مستقیم موفقی را به هیچ‌کدام از مشتریان SecurID موجب نمی‌شود. با این حال، این اطلاعات به‌طور بالقوه می‌توانست برای کاهش اثربخشی یک پیاده‌سازی کنونی از احراز هویت دو عامله، به‌عنوان قسمتی از یک حمله وسیع‌تر مورداستفاده قرار گیرد.
لاک‌هید-مارتین، یکی از مشتریان RSA، پس از این واقعه هک شد و گمان می‌رود که این کار توسط همان هکر انجام شده است (مورد مطالعاتی بالا را ببینید).

منبع:

Tony Bradley, "RSA SecurID Hack Shows Danger of APTs", PCWorld, 19 Mach 2011, http://www .pcworld.com/businesscenter/article/222555/rsa_securid_hack_shows_danger_of_apts.html; and Warwick Ashford, "RSA hit by advanced persistent threat attacks", Computer Weekly, 18 March 2011, http://www.computerweekly.com/Articles/2011/ 03/18/245974/RSA-hit-by-advanced-persistent-threat-attacks.htm.

۲-۲ روندها در تهدیدهای پیش‌روی امنیت اطلاعات[۶]

یک فعالیت مهم در حفاظت از امنیت اطلاعات تحلیل روندهای موجود در تهدیدهای امنیتی است. این یعنی جست‌وجوی الگوهای تهدید در طول زمان به‌منظور شناسایی روش‌هایی که با استفاده از آن‌ها، این الگوها تغییر و توسعه یافته، در جهت‌های دیگر تغییر مسیر داده یا انتقال می‌یابند. این فعالیت تکراری جمع‌آوری و مرتبط کردن اطلاعات و بهبود مشخصات حوادث به این منظور انجام می‌شود که تهدیدهای محتمل و ممکن را پیش‌بینی کرده و پاسخ‌های مناسب در برابر این تهدیدها را آماده کند.

سازمان‌هایی که تحلیل روندهای مربوط به تهدیدهای امنیتی را انجام می‌دهند گزارش‌های مربوط به آن را به اشتراک می‌گذارند عبارتند از:

- رایانه‌های (http://www.cert.org/cert/)
- Symantec (http://www.symantec.com/business/theme.jsp?themeid=threatreport)
- IBM (http://xforce.iss.net/)

در ادامه، روندهایی که در تهدیدهای پیش‌روی امنیت اطلاعات گزارش شده است تشریح می‌شوند.

خودکارسازی ابزارهای حمله[۷]

نفوذگران اکنون از ابزارهای خودکاری استفاده می‌کنند که به آن‌ها اجازه می‌دهد به‌آسانی و سریع اطلاعات هزاران میزبان را در اینترنت به‌دست آورند. شبکه‌ها را می‌توان از محلی دور اسکن کرده و با استفاده از ابزارهای خودکار میزبان‌هایی را که دارای ضعفی مشخص هستند شناسایی کرد. نفوذگران ممکن است اطلاعات را برای استفاده در آینده دسته‌بندی کنند، آن‌ها را با نفوذگران دیگر به

اشتراک گذارند یا بلافاصله حمله می‌کنند. بعضی از ابزارها (مانند Cain & Abel) دنباله‌ای از حملات کوچک را برای یک هدف کلی خودکارسازی می‌کنند. مثلاً، نفوذگران می‌توانند از یک بوینده بسته‌ها[1] برای به‌دست آوردن رمزهای عبور مسیریاب‌ها و فایروال‌ها استفاده کنند، به فایروال وارد شده تا فیلترها را غیرفعال نمایند و سپس از یک سرویس فایل در شبکه برای خواندن داده‌ها روی سرور استفاده کنند.

دشواری در تشخیص ابزارهای حمله

بعضی از ابزارهای حمله از الگوهایی برای حمله استفاده می‌کنند که با ابزارهای تشخیص موجود قابل‌شناسایی نیستند. به‌عنوان مثال، تکنیک‌های ضد دادگاهی برای پوشاندن یا پنهان کردن ماهیت ابزارهای حمله مورداستفاده قرار می‌گیرند. ابزارهای چندریختی هر زمانی که استفاده می‌شوند، شکل را تغییر می‌دهند. بعضی از این ابزارها از پروتکل‌های رایج همچون HTTP استفاده می‌کنند که تمایز دادن آن‌ها را از ترافیک مجاز در شبکه دشوار می‌سازد[۸]. کرم نرم‌افزار MSN Messenger مثالی خوب از این نوع است. یک کرم در نرم‌افزار کلاینت پیام‌دهی سریع MSN Messenger، فایلی را که برای آلوده کردن سیستم‌ها طراحی شده به فهرست تماس‌های موجود در دفترچه آدرس کاربر آلوده شده می‌فرستد و قبل از آن پیام هشداری به آن‌ها می‌فرستند مبنی بر اینکه آن‌ها به‌زودی قرار است فایلی را دریافت کنند. رفتار یک کاربر واقعی در سیستم پیام‌دهی سریع تقلید می‌شود و این یک زنگ خطر است[۹].

کشف سریع‌تر آسیب‌پذیری‌ها

هر ساله تعداد آسیب‌پذیری‌هایی که به‌تازگی در محصولات نرم‌افزاری کشف شده‌اند و در گزارش مرکز هماهنگی تیم پاسخ اضطراری در رایانه‌ها[2] (CERT/CC) وارد می‌شوند، بیش از دو برابر می‌شود و این مسئله هماهنگی و به‌روز بودن مدیران سیستم‌ها را با ترمیم‌ها دچار مشکل می‌کند. نفوذگران از این موضوع آگاهی دارند و از آن سوءاستفاده می‌کنند[۱۰]. بعضی از نفوذگران یک حمله روز صفر یا ساعت صفر را پیاده می‌کنند و آن تهدیدی رایانه‌ای است که از نقاط آسیب‌پذیری از برنامه‌های کاربردی بهره‌برداری می‌کند که برای آن‌ها هیچ ترمیم یا حفاظتی وجود ندارد، چون هنوز به‌وسیله مدیران سیستم کشف نشده‌اند[۱۱].

1- Packet Sniffer
2- Computer Emergency Response Team Coordination Center

افزایش تهدید نامتقارن و همگرایی روش‌های حمله

یک تهدید نامتقارن شرایطی است که در آن یک مهاجم در موقعیت برتری نسبت به مدافع باشد. تعداد تهدیدهای نامتقارن با خودکارسازی اجرای تهدیدها و پیچیده شدن ابزارهای حمله افزایش می‌یابد.

همگرایی روش‌های حمله به معنی ادغام روش‌های متنوع حمله به‌وسیله مهاجم در جهت ایجاد شبکه‌های سراسری است که از فعالیت‌های بدخواهانه هماهنگ پشتیبانی می‌کند. به‌عنوان مثال، Zbot که تحت عنوان Zeus نیز شناخته می‌شود، یک بسته بدافزاری است که همواره برای فروش در دسترس است و در فوروم‌های زیرزمینی نیز ردوبدل می‌شود. این بسته شامل یک سازنده است که می‌تواند یک ربات اجراشونده و فایل‌های سرور وب (PHP، تصاویر و قالب‌های SQL) را برای استفاده به‌عنوان سرور فرمان و کنترل تولید کند. اگرچه Zbot یک در پشتی عام است که اجازه کنترل کامل را به‌وسیله یک کاربر غیرمجاز از راه دور می‌دهد، کارکرد اصلی کسب منافع مالی است – مانند سرقت اطلاعات ورودی در مواردی نظیر FTP، ایمیل، بانکداری الکترونیکی و سایر رمزهای عبور آنلاین[۱۲].

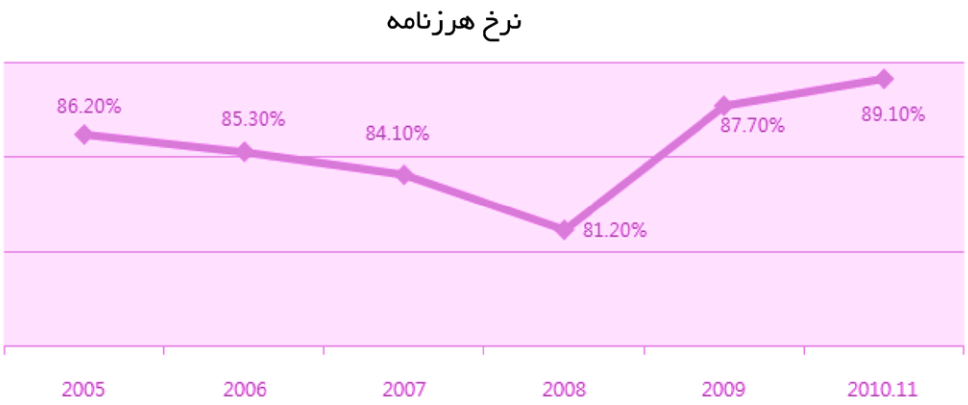
افزایش تهدید از سوی حملات زیرساختی

حملات زیرساختی، حملاتی هستند که مؤلفه‌های کلیدی اینترنت را به‌طور وسیع تحت تأثیر قرار می‌دهد. این نوع حملات به‌خاطر تعداد زیاد سازمان‌ها و کاربران در اینترنت وابستگی رو به افزایش آن‌ها به اینترنت برای انجام کارهای روزمره آن‌ها یک نگرانی بزرگ ایجاد می‌کنند. حملات زیرساختی منجر به حمله DoS، به مخاطره افتادن اطلاعات حساس، پخش شدن اطلاعات نادرست و انحراف چشم‌گیر منابع از دیگر وظایف می‌شوند.

باتنت[1] مثالی از یک حمله زیرساختی است. واژه "باتنت" به گروهی از رایانه‌های آلوده شده اشاره دارد که به‌وسیله یک "سرور کنترل فرمان" از راه دور کنترل می‌شود. رایانه‌های آلوده شده کرم‌ها و اسب‌های تروا را در سراسر سیستم‌های شبکه پراکنده می‌کنند.

هرزنامه‌ها به‌دلیل استفاده از باتنت‌ها سریعاً در حال افزایش هستند. هرزنامه پیام‌های حجیم ناخواسته‌ای است که می‌تواند از طریق ایمیل، پیام‌های سریع، موتورهای جست‌وجو، وبلاگ‌ها و حتی تلفن‌های همراه ارسال شود. شکل ۱-۲ روند موجود در حجم هرزنامه‌ها را نشان می‌دهد.

1 -Botnet



شکل ۱-۲ آمار مربوط به هرزنامه‌ها

منبع: **Symantec MessageLabs**.

مقابله با بات‌نت

برای کاهش خسارات ناشی از بات‌نت، اتحادیه مخابرات بین‌الملل (ITU) ترکیبی از خطمشی، فناوری و روش‌شناسی اجتماعی را توصیه می‌کند.

خطمشی: قوانین و مقررات مؤثر ضد هرزنامه و جرم‌های سایبری

- ظرفیت‌سازی در میان ذی‌نفعان خطمشی‌ها
- چارچوب جامع برای همکاری‌ها و کمک‌های بین‌المللی
- سازگاری بین جرم‌های سایبری و قوانین مربوط به حریم خصوصی
- چارچوبی برای اعمال قانون محلی کاهش جرم‌های سایبری و بات‌نت

فناوری: ابزارها و تکنیک‌هایی برای شناسایی و جمع‌آوری اطلاعات پیرامون بات‌نت‌های فعال

- اقدامات موفق در امنیت اطلاعات و حریم خصوصی در جهت کاهش فعالیت بات‌نت‌ها
- اقدامات موفق در ثبت اسناد جهت کاهش فعالیت بات‌نت‌ها
- ظرفیت‌سازی برای ارائه‌کنندگان تجارت الکترونیکی و تبادلات آنلاین

اجتماعی: اقدامات آموزشی در مقیاس وسیع در مورد ایمنی و امنیت اینترنت

- تسهیل دستیابی به فناوری اطلاعات و ارتباطات امن برای کاربران

جعبه ابزار PTF ITU SPAM بسته‌ای جامع برای کمک به برنامه‌ریزان خطمشی‌ها، واضعان مقررات و شرکت‌ها در تنظیم خطمشی‌ها و بازیابی اعتماد به ایمیل است. همچنین، این جعبه ابزار اشتراک اطلاعات را بین کشورها برای جلوگیری از مشکلات بین‌المللی توصیه می‌کند.

تغییرات در مقاصد حملات

سابقاً حملات به رایانه‌ها و شبکه‌ها به‌خاطر کنجکاوی یا برای ارضای شخصی انجام می‌گرفت؛ اما امروزه، مقصود معمولاً پول، سودجویی و خرابه‌کاری است. از این گذشته، این نوع از حملات تنها بخش کوچکی از طیف وسیع جرم‌های سایبری را نشان می‌دهد.

جرم سایبری به تخریب، انقطاع یا اختلال عمدی جریان داده‌ها یا اطلاعات دیجیتال با دلایل سیاسی، اقتصادی، مذهبی یا ایدئولوژیک گفته می‌شود. رایج‌ترین جرم‌ها عبارتند از: هک کردن، DoS، کدهای مخرب و مهندسی اجتماعی. اخیراً، جرم سایبری به‌عنوان قسمتی از تروریسم سایبری و جنگ سایبری در نظر گرفته می‌شود که آثار منفی بر امنیت ملی دارد.

جدول ۱-۲ در زیر نشان می‌دهد که ارتکاب‌گران جرم‌های سایبری چه مبالغی به‌دست می‌آورند.

جدول ۱-۲ میزان درآمد از جرم‌های سایبری

مورد	دامنه مبلغ (به دلار آمریکا)
اطلاعات کارت اعتباری	0.07-100
اطلاعات حساب بانکی	10-900
حساب‌های کاربری ایمیل	1-18
ابزارهای حمله	5-650
آدرس‌های ایمیل	1/MB-20/MB
کپی نوار مغناطیسی کارت اعتباری	0.50-120
هویت‌های کامل	0.50-20
کلاه‌برداری از طریق میزبانی	10-150
شل‌اسکریپت‌ها	2-7
سرویس‌های پرداخت پول نقد	200-500 (۵۰٪ -۷۰٪ از کل مقدار)

منبع: Symantec, Internet Security Threat Report Volume 16 (2011), http://www.symantec.com/business/threatreport/topic.jsp?id=fraud_activity_trends&aid=underground_economy_servers

۳-۲ بهبود امنیت

با توجه به روندهای موجود در تهدیدهای امنیتی و فناوری‌های حمله، دفاع مستحکم نیازمند استراتژی منعطفی است که اجازه تطابق با تغییرات محیطی را بدهد. همچنین نیاز به خط‌مشی‌ها و رویه‌های معین، استفاده از فناوری‌های امنیتی مناسب و هشیاری پیوسته وجود دارد.

شروع یک برنامه بهبود امنیت با تعیین وضعیت فعلی امنیتی مفید است. اجزای یکپارچه با یک برنامه امنیتی، خط‌مشی‌ها و رویه‌های مستند شده و همچنین فناوری‌هایی هستند که از پیاده‌سازی آن‌ها پشتیبانی می‌کنند.

امنیت اجرایی

امنیت اجرایی از یک استراتژی امنیت اطلاعات، خط‌مشی و اصول راهنما تشکیل شده است. **استراتژی امنیت اطلاعات**[1] سمت و سوی تمام فعالیت‌های امنیت اطلاعات را مشخص می‌کند. **خط‌مشی امنیت اطلاعات**[2] طرحی سطح بالا و مستند شده برای امنیت اطلاعات در سراسر سازمان است. این طرح چارچوبی را برای اتخاذ تصمیم‌های خاص، همچون طرح امنیت اجرایی و فیزیکی مهیا می‌کند.

به دلیل اینکه خط‌مشی امنیت اطلاعات باید دید دراز مدت داشته باشد، باید از محتویات مربوط به فناوری‌های خاص دوری گزیند و توسعه برنامه‌های مؤثر در تداوم کسب‌وکار را در برگیرند.

اصول راهنمای امنیت اطلاعات[3] باید با توجه به استراتژی و خط‌مشی امنیت اطلاعات تدوین شود. این اصول راهنما باید مقرراتی را برای هر حوزه مرتبط با امنیت اطلاعات تعیین کند. چون اصول راهنما باید جامع بوده و در سطح ملی گستردگی داشته باشد، باید توسط دولت توسعه داده شده و برای برگزاری تحویل سازمان‌ها شوند.

استانداردهای امنیت اطلاعات[4] باید به‌طور تخصصی و خاص تعیین گردند به‌گونه‌ای که بتوانند در همه حوزه‌های امنیت اطلاعات به‌کار گرفته شوند. برای هر کشور خوب است که پس از تحلیل استانداردهای امنیتی اجرایی، فنی و فیزیکی که به‌طور فراگیر در سراسر دنیا استفاده می‌شوند، استانداردهای خودش را توسعه دهد. استانداردها باید برای محیط‌های فناوری اطلاعات و ارتباطات متعارف مناسب باشند.

1- Information Security Strategy
2- Information Security Policy
3- Information Security Guidelines
4- Information Security Standards

استراتژی، خط‌مشی و اصول راهنمای امنیت اطلاعات یک کشور باید از قوانین مرتبط پیروی کنند. دامنه پوشش آن‌ها باید در داخل مرزهای قوانین ملی و بین‌المللی باشد.

عملکرد و فرآیند امنیت اطلاعات

هنگامی‌که استراتژی، خط‌مشی و اصول راهنمای امنیت اطلاعات تدوین شد، رویه‌های عملیاتی و فرآیندهای امنیت اطلاعات باید تعریف شوند. چون این افراد هستند که مرتکب حملات به اطلاعات می‌شوند یا اطلاعات داخلی را نشت می‌دهند، مدیریت منابع انسانی مهم‌ترین عامل در عملکرد امنیت اطلاعات است. از این رو، به موارد زیر نیاز است:

۱- برنامه‌های آموزشی و تربیتی امنیت اطلاعات: روش‌های زیادی برای بهبود سطح امنیت اطلاعات یک سازمان وجود دارند، اما آموزش و تربیت اساسی‌ترین فعالیت‌ها هستند. اعضای یک سازمان باید نیاز به امنیت اطلاعات را درک کنند و مهارت‌های لازم را از طریق آموزش و تربیت به‌دست آوردند. با این وجود، مهم است که برنامه‌های متنوعی را برای به حدبیشتر رسانیدن مشارکت اعضا تدارک ببینیم چون برنامه‌های آموزشی و تربیتی استاندارد امنیت اطلاعات ممکن است اثربخشی لازم را نداشته باشند.

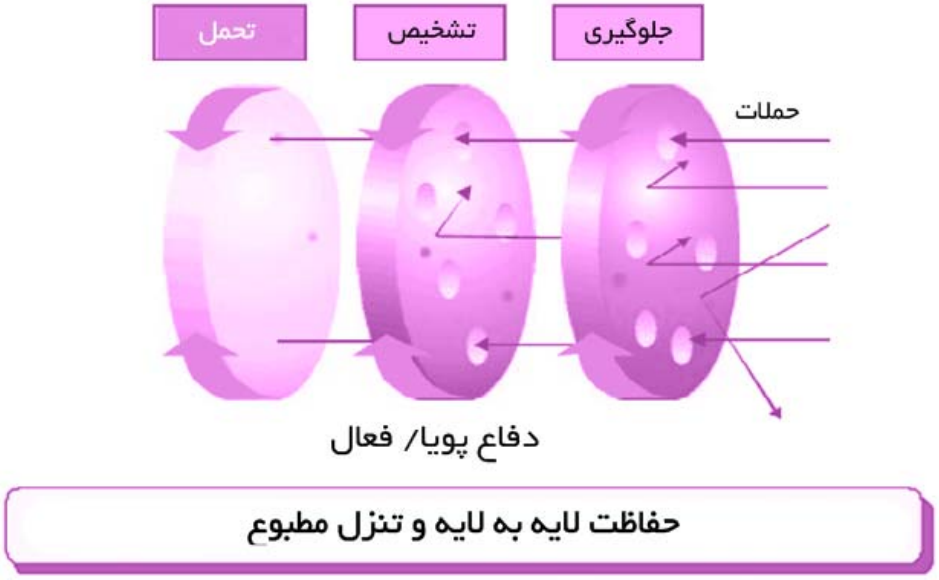
۲- تقویت ترویج از طریق رویدادهای گوناگون: مشارکت کارمندان در پیاده‌سازی موفق استراتژی، خط‌مشی و اصول راهنمای امنیت اطلاعات مهم است. امنیت اطلاعات را باید از طریق فعالیت‌های متنوع روزمره در میان کارمندان ترویج داد.

۳- ایمن‌سازی حمایت مالی: اگرچه ممکن است سطح آگاهی از امنیت اطلاعات در میان کارمندان بالا بوده و آن‌ها تمایل زیادی برای حفظ امنیت اطلاعات داشته باشند، تضمین امنیت اطلاعات بدون جلب حمایت سطوح بالای سازمان امکان‌پذیر نیست. حمایت مدیر عامل و مدیر فناوری اطلاعات سازمان باید کسب شود.

امنیت تکنولوژیک

فناوری‌های متعددی برای کمک به سازمان‌ها جهت ایمن‌سازی سیستم‌های اطلاعاتیشان در مقابل نفوذگران ابداع شده‌اند. این فناوری‌ها به حفاظت از سیستم‌ها و اطلاعات در مقابل حملات، تشخیص فعالیت‌های غیرعادی و مشکوک و پاسخ به رویدادهایی که بر امنیت تأثیر می‌گذارند، کمک می‌کنند.

امروزه، سیستم‌های امنیتی بر اساس مدل دفاع در عمق[1] (DID) طراحی و ساخته شده‌اند که ما را به‌سوی مدیریت متحد فناوری‌های درگیر رهنمون می‌کند. این مدل با دفاع در محیط که صرفاً یک لایه از دفاع را در مقابل همه تهدیدها دارد، متفاوت است. مدل DID از جلوگیری[2]، تشخیص[3] و تحمل[4] تشکیل شده است و تهدیدها در هر مرحله از آن کاهش می‌یابد (شکل ۲-۲ را ببینید).



شکل ۲-۲ مدل دفاع در عمق (DID)

منبع: Defense Science Board Task Force, Protecting the Homeland: Defensive Information Operations 2000 Summer Study Volume II (Washington, D.C., 2001), p. 5, http://www.carlisle.army.mil/DIME/documents/dio.pdf.

فناوری جلوگیری

فناوری‌های جلوگیری در سطح ذخیره‌سازی یا سیستم در مقابل نفوذگران و تهدیدها حفاظت به عمل می‌آورند. این فناوری‌ها عبارتند از:

۱- رمزنگاری[5]: که به آن رمزگذاری[6] هم گفته می‌شود، فرآیند ترجمه اطلاعات از یک فرم اصلی (به نام متن ساده) به یک فرم کدگذاری شده و غیرقابل فهم (به نام متن رمز) است.

1- Defense-In-Depth
2- Prevention
3- Detection
4- Tolerance
5- Cryptography
6- Encryption

رمزگشایی[1] به فرآیندی گفته می‌شود که متن رمز را دریافت کرده و آن را مجدداً به متن ساده تبدیل می‌کند. رمزنگاری برای حفاظت برنامه‌های کاربردی بسیاری مورداستفاده قرار می‌گیرد. اطلاعات بیشتر در مورد رمزگذاری و فناوری‌های مرتبط (IPSec، VPN، SSL، SSH، OTP و ...) در صفحات وب زیر در دسترس هستند:

- IETF RFC (http://www.ietf.org/rfc.html)
- RSA Laboratories' Frequently Asked Questions About Today's Cryptography (http://www.rsa.com/rsalabs/node.asp?id=2152)

۲- رمزهای عبور یک‌بار مصرف[2] (OTP): همان‌طور که از نام آن پیداست رمزهای عبور یک‌بار مصرف را تنها یک‌بار می‌توان استفاده کرد. رمزهای عبور ایستا را راحت‌تر می‌توان از طریق گم شدن، استراق سمع رمز عبور، شکستن رمزهای عبور با حمله وحشیانه و مانند آن‌ها به‌دست آورد. این ریسک را می‌توان تا حد زیادی با تغییر مرتب رمزهای عبور، آن‌چنان‌که در رمزهای عبور یک‌بار مصرف انجام می‌شود، کاهش داد. به همین دلیل، رمزهای عبور یک‌بار مصرف برای ایمن‌سازی تراکنش‌های مالی الکترونیکی همچون بانکداری آنلاین مورداستفاده قرار می‌گیرند.

۳- فایروال‌ها: مقداری از جریان ترافیک بین شبکه‌های رایانه‌ای با سطوح مختلف اعتماد، توسط فایروال کنترل می‌شود، مثلاً بین اینترنت که یک منطقه بدون اعتماد است و یک شبکه داخلی که منطقه‌ای با اعتماد بیشتر است. منطقه‌ای با سطح اعتماد میانه که بین اینترنت و شبکه‌های داخلی مورد اعتماد واقع می‌شود، اغلب به‌عنوان "شبکه محیطی" یا منطقه غیرنظامی خوانده می‌شود.

۴- ابزار تحلیل آسیب‌پذیری: به‌دلیل افزایش تعداد روش‌های حمله و آسیب‌پذیری‌هایی که در برنامه‌های کاربردی رایج وجود دارد، ارزیابی دوره‌ای آسیب‌پذیری‌های یک سیستم ضروری است. در امنیت رایانه‌ها، یک آسیب‌پذیری ضعفی است که به یک مهاجم اجازه می‌دهد تا حریم سیستم را نقض کند. آسیب‌پذیری‌ها ممکن است ناشی از رمزهای عبور ضعیف، اشکالات در نرم‌افزار، ویروس رایانه‌ای، تزریق کد اسکریپت، تزریق در SQL[3] یا بدافزار باشد. ابزارهای تحلیل آسیب‌پذیری این آسیب‌پذیری‌ها را تشخیص می‌دهند. این ابزارها به‌سادگی از طریق آنلاین در دسترس هستند و شرکت‌هایی وجود دارند که سرویس‌های تحلیلی را مهیا می‌کنند. با این حال، ابزارهایی که در اینترنت به‌طور رایگان در اختیار هستند می‌توانند مورد سوءاستفاده نفوذگران قرار گیرند. برای اطلاعات بیشتر به پیوندهای زیر مراجعه کنید.

- Secunia Vulnerability Archive (http://secunia.com/advisories)
- SecurityFocus Vulnerability Archive (http://www.securityfocus.com/bid)
- Top 100 Network Security Tools (http://sectools.org)

1- Decryption
2- One-Time Passwords
3- SQL Injection

- VUPEN Security Research – Discovered Vulnerability (http://www.vupen.com/english/research.php)

ابزارهای تحلیل آسیب‌پذیری شبکه، آسیب‌پذیری‌های منابع شبکه را همچون مسیریاب‌ها، فایروال‌ها و سرورها تحلیل می‌کنند.

ابزار تحلیل آسیب‌پذیری سرور، آسیب‌پذیری‌هایی همچون رمزهای عبور ضعیف، پیکربندی ضعیف و خطاهای مجوز دسترسی به فایل در سیستم داخلی را مورد تحلیل قرار می‌دهد. ابزار تحلیل آسیب‌پذیری سرور نتایج به نسبت دقیق‌تری در مقایسه با ابزارهای تحلیل آسیب‌پذیری شبکه ارائه می‌دهد، چون این ابزار بسیاری از آسیب‌پذیری‌ها را در سیستم داخلی تحلیل می‌کند.

ابزار تحلیل آسیب‌پذیری وب، آسیب‌پذیری‌های برنامه‌های کاربردی وب را همچون XSS و تزریق SQL از طریق وب تحلیل می‌کند. برای اطلاعات بیشتر می‌توانید به پروژه امنیت برنامه‌های کاربردی مبتنی بر وب باز رجوع کنید:

http://www.owasp.org/index.php/Top_10_2010

فناوری تشخیص

فناوری تشخیص برای تشخیص و ردگیری حالت‌های غیرعادی و نفوذ به شبکه‌ها یا سیستم‌های مهم مورداستفاده قرار می‌گیرد. فناوری تشخیص این موارد را در بر می‌گیرد:

۱- ضد ویروس[1]: یک ضد ویروس برنامه‌ای رایانه‌ای است که برای شناسایی، خنثی‌سازی یا حذف کدهای مخرب، شامل کرم‌ها، حملات فیشینگ، روت‌کیت، اسب‌های تروا و دیگر بدافزارها به‌کار می‌رود[۱۳].

۲- سیستم‌های تشخیص نفوذ[2] (IDS): یک سیستم تشخیص نفوذ اطلاعات را از نواحی مختلف در یک رایانه یا شبکه جمع‌آوری و تحلیل می‌کند تا رخنه‌های امنیتی ممکن را شناسایی نماید. کارکرد تشخیص نفوذ شامل تحلیل الگوهای فعالیت غیرعادی در جهت تشخیص الگوهای حمله است.

۳- سیستم‌های جلوگیری از نفوذ[3] (IPS): جلوگیری از نفوذ سعی دارد تهدیدهای بالقوه را قبل از اینکه در حملات استفاده شوند شناسایی کرده و پاسخ مناسب را به آن‌ها بدهد. یک سیستم جلوگیری از نفوذ، بر ترافیک شبکه نظارت کرده و در مقابل تهدیدهای بالقوه، با توجه به یک مجموعه قوانین تدوین شده به‌وسیله مدیر شبکه، اقدامات فوری را انجام می‌دهد. مثلاً، یک IPS می‌تواند ترافیک ورودی از یک آدرس IP مشکوک را مسدود کند[۱۴].

1- Antivirus
2- Intrusion Detection System
3- Intrusion Prevention System

فناوری یکپارچه‌سازی

فناوری یکپارچه‌سازی عملکردهای مهم همچون پیش‌بینی، تشخیص و ردگیری نفوذها را برای امنیت اطلاعات مربوط به دارایی‌های اصلی یکپارچه می‌کند. فناوری یکپارچه‌سازی شامل این موارد است:

۱- مدیریت امنیت سازمانی[1] (ESM): سیستم مدیریت امنیت سازمانی یک راه‌حل امنیت اطلاعات همچون IDS یا IPS را بر اساس یک خط‌مشی پایدار کنترل و اداره می‌کند. این سیستم به‌عنوان یک استراتژی برای جبران ضعف‌های دیگر راه‌حل‌ها، با استفاده از مزایای هر راه‌حل امنیت اطلاعات و بیشینه‌سازی اثربخشی امنیت اطلاعات تحت یک خط‌مشی پایدار، مورداستفاده قرار می‌گیرد.

انواع مدیریت امنیت سازمانی که می‌توانند فناوری‌های موجود امنیتی را به‌طور ترکیبی مدیریت کنند، اخیراً به‌دلیل کمبود منابع انسانی در کار کردن با فناوری‌های امنیتی، افزایش حملات ارتقا یافته همچون ترکیب روش‌های حمله متنوع و ظهور حملاتی که تشخیص آن‌ها دشوار است، به‌وجود آمده‌اند. با مدیریت امنیت سازمانی کارایی مدیریت بیشتر شده و اقدامات پیشگیرانه فعال انجام می‌شوند.

۲- مدیریت ریسک سازمانی[2] (ERM): سیستمی است که به پیش‌بینی همه ریسک‌های مرتبط با سازمان، از جمله حیطه‌های خارج از امنیت اطلاعات کمک کرده و به‌طور خودکار اقدامات پیشگیرانه را شکل می‌دهد. استفاده از مدیریت ریسک سازمانی برای حفاظت از اطلاعات مستلزم این است که هدف از مدیریت ریسک و طراحی برای توسعه سیستم مشخص شود. بیشتر سازمان‌ها با بهره‌گیری از شرکت‌های حرفه‌ای مشاور در زمینه امنیت، مدیریت ریسک سازمانی خود را ساخته و بهینه می‌کنند.

پرسش‌هایی برای تفکر

۱- سازمان شما در مقابل کدام تهدیدهای امنیت اطلاعات آسیب‌پذیر است؟ چرا؟

۲- چه راه‌حل‌هایی با استفاده از فناوری برای امنیت اطلاعات در سازمان شما موجود است؟

۳- آیا سازمان شما دارای خط‌مشی امنیتی، استراتژی و اصول راهنما است؟ اگر بله، آیا این موارد با توجه به تهدیدهایی که سازمان شما در مقابل آن‌ها آسیب‌پذیر است کفایت می‌کند؟ اگر هیچ‌کدام وجود ندارد، برای تدوین این موارد در سازمان خود چه توصیه‌هایی دارید؟

۴- موارد تمایز سه حوزه از امنیت اطلاعات (اجرایی، فیزیکی و فنی) را مشخص کنید.

1- Enterprise Security Management
2- Enterprise Risk Management

خودآزمایی

۱- چرا تحلیل روندهای مربوط به تهدیدهای امنیت اطلاعات مهم است؟

۲- چرا مدیریت منابع انسانی مهم‌ترین عامل در عملکرد امنیت اطلاعات است؟ فعالیت‌های کلیدی در مدیریت منابع انسانی برای امنیت اطلاعات چیست؟

۳- مدل دفاع در عمق را در امنیت مبتنی بر فناوری شرح دهید. این مدل چگونه عمل می‌کند؟

فصل سوم

فعالیت‌های امنیت اطلاعات

اهداف این فصل عبارتند از:

- ارائه نمونه‌هایی از فعالیت‌های امنیت اطلاعات در کشورهای مختلف به‌عنوان راهنمایی برای سیاست‌گذاری در امنیت اطلاعات؛
- تأکید بر همکاری بین‌المللی در پیاده‌سازی خط‌مشی‌های امنیت اطلاعات

۳-۱ فعالیت‌های امنیت اطلاعات در سطح ملی

استراتژی امنیت اطلاعات در کشور ایالات متحده آمریکا

پس از حملات تروریستی در ۱۱ سپتامبر سال ۲۰۰۱ (9/11)، دولت ایالات متحده آمریکا وزارت امنیت ملی را بنا نهاد تا امنیت ملی را نه تنها در برابر تهدیدهای فیزیکی بلکه در مقابل تهدیدهای سایبری نیز تقویت کند. ایالات متحده آمریکا از طریق سیستم متصدی امنیت اطلاعات، فعالیت‌های جامع و مؤثری برای امنیت اطلاعات پیاده‌سازی می‌کند. استراتژی امنیت اطلاعات این کشور شامل استراتژی ملی برای امنیت ملی، استراتژی ملی برای امنیت فیزیکیِ زیرساخت‌های حیاتی و دارایی‌های کلیدی و استراتژی ملی برای فضای سایبری امن است.

استراتژی ملی برای فضای سایبری امن[۱۵] نگرش به فضای سایبری و حفاظت از زیرساخت‌ها و دارایی‌های حیاتی را تعیین می‌کند. این استراتژی اهداف و فعالیت‌های خاص را برای جلوگیری از حملات سایبری به زیرساخت‌ها و دارایی‌های حیاتی تعریف می‌کند. پنج اولویت ملی که در *استراتژی ملی برای فضای سایبری امن* تعریف شده‌اند عبارتند از:

- ✓ سیستم ملی پاسخ‌گویی امنیت سایبری
- ✓ برنامه ملی کاهش آسیب‌پذیری و تهدید در امنیت سایبری
- ✓ برنامه ملی آموزش و آگاهی در امنیت سایبری
- ✓ ایمن‌سازی فضای سایبری دولت
- ✓ همکاری امنیت ملی و امنیت سایبری بین‌المللی

خط‌مشی امنیت سایبری در ایالات متحده آمریکا به‌طور پیوسته در حال تکامل است تا با چالش‌های متنوع مقابله کند، اما شکاف‌های حیاتی هنوز باقی مانده‌اند، از جمله حفاظت ناقص از زیرساخت دیجیتال، از قبیل شبکه‌های برق و شبکه‌های مالی که برای امنیت ملی حیاتی هستند. رئیس جمهور باراک اوباما، پس از رسیدن به قدرت، فضای سایبری را یک دارایی ملی استراتژیک اعلام کرد و خواستار بازبینی کامل خط‌مشی مربوط به فضای سایبری شد. در ماه می سال ۲۰۱۱، کاخ سفید استراتژی بین‌المللی خود را برای فضای سایبری منتشر کرد- تلاشی برای ارسال پیام به متحدان و دشمنان در مورد این‌که ایالات متحده آمریکا چه انتظاراتی دارد و طرح‌های این کشور برای این رسانه نوظهور چیست. خط‌مشی کنونی ایالات متحده آمریکا در فضای سایبری مسئولیت‌ها را بین وزارت دفاع و وزارت امنیت ملی تقسیم می‌کند که اولی دامنه‌های با پسوند ".mil" و دومی دامنه‌های با پسوند ".gov" را اداره می‌کنند. همچنین، دولت ایالات متحده آمریکا تلاش‌هایی داشته تا رویکرد منسجمی را در حفاظت از دارایی‌های دیجیتال در خارج از دولت حفظ کند و در بیشتر موارد، متکی بر مشارکت داوطلبانه صنعت بخش خصوصی است.

سخت کردن قوانین مربوط به امنیت اطلاعات

قانون بهبود فضای سایبری سال ۲۰۰۲ (CSEA)[۱۶] تشکیل‌دهنده فصل دوم از قانون امنیت ملی است. این قانون اصلاحیه‌هایی را برای محکومیت‌های تعیین شده در بعضی جرائم رایانه‌ای، استثناهای مربوط به افشا در حالت اضطراری، استثناهای مربوط به حسن نیت، ممنوعیت تبلیغات غیرقانونی در اینترنت و حفاظت از حریم خصوصی و غیره ارائه می‌کند.

استثناهای مربوط به افشا در حالت اضطراری: قبل از حوادث یازده سپتامبر، قانون حریم خصوصی ارتباطات الکترونیکی[1] (ECPA) ارائه‌کنندگان خدمات ارتباطی الکترونیکی (از قبیل ارائه‌کنندگان خدمات اینترنتی یا ارائه‌دهندگان خدمات اینترنتی) را از افشای ارتباطات کاربران (از قبیل پست صوتی، رایانامه‌ها و ضمایم) منع می‌کرد. استثناهای مربوط به افشا در حالت اضطراری به ارائه‌دهندگان خدمات اینترنتی اجازه می‌داد تا محتویات یک رایانامه یا یک ارتباط الکترونیکی را بدون حکم قضایی، با توجه به قانون مبارزه با تروریسم که بعد از یازده سپتامبر ۲۰۰۱ تصویب شد، در اختیار مراجع قانونی قرار دهند. مقررات مربوط به موارد استثنایی در موقعیت‌های اضطراری در قانون بهبود فضای سایبری تقویت شده‌اند. سازمان‌های دولتی که محتوای مشکوک دریافت می‌کنند ملزم هستند ظرف ۹۰ روز پس از افشای اطلاعات، موارد مربوط به تاریخ افشا، طرف‌های درگیر، اطلاعات مربوط به افشا و تعداد متقاضیان مربوطه و نیز تعداد ارتباطات را به دادستان کل گزارش دهند.

1- Electronic Communications Privacy Act

استثناهای مربوط به حسن نیت: قانون بهبود فضای سایبری در صورتی‌که استراق سمع به‌وسیله مالک یا متصدی رایانه درخواست شود، معافیت از اتهامات جنایی و مدنی را تصریح می‌کند.

ممنوعیت تبلیغ اینترنتی لوازم غیرقانونی: قانون حریم خصوصی ارتباطات الکترونیکی تولید، توزیع، تملک و تبلیغ آنلاین لوازم سیمی، شفاهی یا الکترونیکی مورداستفاده در رهگیری ارتباطات را ممنوع می‌کند. ابزارهای استراق سمع الکترونیکی را می‌توان تبلیغ کرد. اما آگهی‌دهنده باید از محتویات تبلیغ آگاهی داشته باشد.

افزایش مجازات برای جرائم رایانه‌ای: تحت قانون تقلب و سوءاستفاده‌های رایانه‌ای در ایالات متحده آمریکا، دسترسی عمدی به یک رایانه و ایجاد خسارت به آن، بدون کسب اجازه، غیرقانونی تلقی می‌شود. قبل از یازده سپتامبر، هر شخصی که مرتکب این جرم شناخته می‌شد باید به حبس کمتر از پنج سال در صورت اولین ارتکاب جرم و کمتر از ۱۰ سال در صورت دومین ارتکاب محکوم می‌شد. پس از یازده سپتامبر، مجازات برای این جرائم بازنگری شده و کمتر از ۱۰ سال برای اولین ارتکاب و کمتر از ۲۰ سال برای دومین ارتکاب تعیین شدند. بندهای اضافی در قانون بهبود فضای سایبری قید می‌کند که یک مجرم را می‌توان به حبس کمتر از ۲۰ سال محکوم کرد اگر مجرم باعث جراحت جدی بدنی شده یا تصمیم به ایجاد آن داشته باشد؛ او را می‌توان به حبس ابد محکوم کرد اگر باعث مرگ کسی شده یا تصمیم به انجام آن داشته باشد.

معافیت مسئولیت معاونان: قانون حریم خصوصی ارتباطات الکترونیکی، ارائه‌کنندگان خدمات ارتباطی را که در ردگیری ارتباطات کمک کرده یا اطلاعات را برای مراجع اعمال قانون فراهم می‌کنند، از اتهامات کیفری معاف می‌کند.

قانون مدیریت امنیت اطلاعات فدرال (FISMA)[۱۷] فصل سوم از قانون دولت الکترونیکی ۲۰۰۲ را تشکیل می‌دهد. این قانون مدون اهمیت امنیت اطلاعات را در منافع اقتصادی و امنیت ملی ایالات متحده آمریکا باز می‌شناسد. به‌علاوه، این قانون ادارات دولتی فدرال را ملزم می‌کند یک برنامه را در کل اداره، جهت فراهم آوردن امنیت برای اطلاعات و سیستم‌های اطلاعاتی که عملکرد و دارایی‌های آن اداره را پشتیبانی می‌کنند، توسعه داده، مستند کرده و پیاده‌سازی کنند. این برنامه شامل عملکرد و دارایی‌هایی نیز است که به‌وسیله دیگر ادارات، پیمان‌کاران یا منابع دیگر مدیریت می‌شوند. این قانون، همچنین خواستار افزایش تلاش‌ها جهت حفاظت از امنیت اطلاعات برای همه شهروندان، ادارات امنیت ملی و مراجع اعمال قانون می‌شود.

اهداف اصلی مدیریت امنیت اطلاعات فدرال عبارتند از: ۱) فراهم آوردن چارچوبی جامع برای تقویت کارایی اقدامات کنترلی امنیت اطلاعات در عملیات و دارایی‌ها؛ ۲) توسعه اقدامات کنترلی و طرح‌های نگهداری مناسب برای حفاظت از اطلاعات/سیستم‌های اطلاعاتی و فراهم آوردن سازوکاری برای تقویت مدیریت برنامه‌های امنیت اطلاعات.

قانون مدیریت امنیت اطلاعات فدرال چارچوب لازم را برای ایمن‌سازی فناوری اطلاعات دولت فدرال فراهم می‌کند. تمام ادارات و سازمان‌های دولتی باید نیازمندی‌ها را پیاده‌سازی کرده و هر ساله گزارشی را در مورد اثربخشی برنامه‌های امنیت اطلاعات و حریم خصوصی به اداره مدیریت و بودجه[1] (OMB) و کنگره ارائه کنند. اداره مدیریت و بودجه از این اطلاعات استفاده می‌کند تا به ارزیابی عملکرد برنامه‌های امنیت اطلاعات و حریم خصوصی در سطح سازمانی و دولتی کمک کند، گزارش امنیتی سالانه خود را برای ارائه به کنگره تدوین کند، در بهبود و حفظ عملکرد کافی و مناسب سازمان‌ها یاری رساند و به توسعه کارت امتیازی دولت الکترونیکی، تحت فهرست کارهای مدیریتی رئیس جمهور کمک کند.

استراتژی امنیت اطلاعات در اتحادیه اروپا

در ابلاغیه ماه می سال ۲۰۰۶[۱۸]، کمیسیون اروپا استراتژی جدید اتحادیه اروپا (EU) را برای امنیت اطلاعات توصیف کرد که متشکل از تعدادی از اقدامات وابسته به هم از سوی ذی‌نفعان بسیاری بود. این اقدامات شامل تدوین یک چارچوب قانون‌گذاری برای ارتباطات الکترونیکی در سال ۲۰۰۲، اعلام اقدامات i2010 برای ایجاد انجمن اطلاعات اروپا و تأسیس سازمان امنیت شبکه و اطلاعات اروپا (ENISA)[2] در سال ۲۰۰۴ بودند. با توجه به این ابلاغیه، این اقدامات رویکردی سه شاخه را در معضلات امنیتی در انجمن اطلاعات منعکس می‌کرد که در بردارنده اقدامات خاص مربوط به امنیت شبکه و اطلاعات، چارچوب قانون‌گذاری برای ارتباطات الکترونیکی (که شامل معضلات مربوط به حریم خصوصی و امنیت داده‌ها است) و مبارزه علیه جرائم سایبری می‌باشد.

این ابلاغیه حملات به سیستم‌های اطلاعاتی، افزایش به‌کارگیری دستگاه‌های همراه، ظهور "هوش فراگیر" و بهبود سطح آگاهی کاربران را به‌عنوان مهم‌ترین معضلات امنیتی مطرح می‌کند که کمیسیون اروپا قصد دارد از طریق گفت‌وگو، مشارکت و تفویض اختیار مورد ملاحظه قرار دهد. این استراتژی‌ها در ابلاغیه توصیف شده‌اند (کادر ۲ را ببینید).

کادر ۲- گفت‌وگوی بین چندین ذی‌نفع در کمیسیون اروپا

کمیسیون تعدادی از اقدامات را پیشنهاد می‌دهد که برای برقراری یک گفت‌وگوی باز و فراگیر بین چند ذی‌نفع طراحی شده‌اند:

- به‌کارگیری محک‌زنی برای خط‌مشی‌های ملی مربوط به امنیت شبکه و اطلاعات، برای کمک به شناسایی مؤثرترین اقدامات به‌گونه‌ای که بتوانند بعد از آن در مقیاسی وسیع در سراسر اتحادیه اروپا

1- Office of Management and Budget
2- European Network and Information Security Agency

به‌کار گرفته شوند. به‌ویژه، این عمل بهترین اقدامات را برای بهبود آگاهی شرکت‌های کوچک و متوسط[1] (SME) و شهروندان از مخاطرات و چالش‌های مربوط به امنیت شبکه و اطلاعات شناسایی می‌کند.

- یک مباحثه ساخت‌یافته بین چند ذی‌نفع درباره اینکه چگونه می‌توان به بهترین شکل از ابزارهای قانون‌گذاری موجود بهره‌برداری کرد. این مباحثه در متن کنفرانس‌ها و سمینارها سازمان‌دهی می‌شود.

مشارکت

سیاست‌گذاری اثربخش مستلزم درک صحیح از ماهیت چالش‌هایی که باید با آن‌ها مقابله شود و نیز داده‌های آماری و اقتصادی قابل‌اتکا و بهنگام است. از این رو، کمیسیون از سازمان امنیت شبکه و اطلاعات اروپا می‌خواهد که:

- مشارکت مبتنی بر اعتماد را با دولت‌های عضو و ذی‌نفعان به وجود آورد تا چارچوب مناسب برای جمع‌آوری داده‌ها توسعه یابد؛ و
- امکان‌سنجی یک سیستم تسهیم اطلاعات و هشداردهی در اروپا را بررسی کند تا پاسخ‌گویی مؤثر به تهدیدها را ممکن سازد. این سیستم شامل پورتالی چندزبانه اروپایی برای فراهم آوردن اطلاعات مناسب پیرامون تهدیدها، ریسک‌ها و هشدارها است.

به‌طور موازی، کمیسیون از دولت‌های عضو، بخش خصوصی و جامعه تحقیقاتی دعوت می‌کند تا مشارکتی را برای تضمین دسترسی‌پذیری داده‌های مربوط به صنعت امنیت فناوری اطلاعات و ارتباطات پایه‌گذاری کنند.

تفویض اختیار

اختیار دادن به ذی‌نفعان یک پیش‌نیاز برای ارتقای آگاهی از نیازها و ریسک‌های امنیتی است. به این منظور، دولت‌های عضو دعوت می‌شوند تا:

- به‌طور فعالانه در فعالیت‌های محک‌زنی پیشنهاد شده برای خط‌مشی‌های ملی شرکت کنند؛
- با همکاری سازمان امنیت شبکه و اطلاعات اروپا، فعالیت‌های تبلیغاتی آگاهانه را درباره مزایای به‌کارگیری فناوری‌ها، اقدامات و رفتارهای مؤثر امنیتی ترویج دهند.
- از گسترش خدمات دولت الکترونیکی در جهت ترویج خدمات امنیتی خوب بهره‌گیری کنند؛ و
- توسعه برنامه‌های امنیت شبکه و اطلاعات را به‌عنوان قسمتی از برنامه تحصیلی آموزش عالی ترغیب کنند.

ذی‌نفعان بخش خصوصی نیز تشویق می‌شوند تا اقداماتی را در جهت اهداف زیر انجام دهند:

- تعریف مسئولیت‌ها برای تولیدکنندگان نرم‌افزار و ارائه‌دهندگان خدمات اینترنتی در رابطه با تدارک سطوح مناسب و قابل ممیزی امنیت؛

1- Small And Medium Enterprises

- ترویج تنوع، باز بودن، تعامل‌پذیری چندمحیطی، قابلیت استفاده و رقابت به‌عنوان محرک‌های کلیدی برای امنیت و ترغیب به‌کارگیری محصولات و خدمات ارتقادهنده امنیت برای مبارزه با سرقت هویت و دیگر حملات متجاوز به حریم خصوصی
- اشاعه اقدامات امنیتی مفید برای متصدیان شبکه، ارائه‌کنندگان خدمات و شرکت‌های کوچک و متوسط؛
- ترویج برنامه‌های آموزشی در بخش خصوصی برای کارمندان، جهت فراهم کردن دانش و مهارت‌های لازم برای پیاده‌سازی اقدامات امنیتی؛
- کار کردن با هدف رسیدن به الگوها و روندهای ذکر شده در گواهی‌های امنیتی برای محصولات، فرآیندها و خدمات که نیازهای خاص اتحادیه اروپا را در نظر می‌گیرد؛ و
- درگیر کردن بخش بیمه در توسعه ابزارها و روش‌های مدیریت ریسک.

منبع:

Abridged from Europa, "Strategy for a secure information society (2006 communication)", European Commission, http://europa.eu/legislation_summaries/information_society/internet/l24153a_en.htm

در ماه مارس سال ۲۰۰۹، کمیسیون ابلاغیه‌ای را در مورد حفاظت از زیرساخت‌های اطلاعاتی حیاتی[1] (CIIP) به‌عنوان "محافظت از اروپا در مقابل حملات و اختلالات سایبری با مقیاس بزرگ: بهبود آمادگی، امنیت و انعطاف‌پذیری"[۱۹] پذیرفت. این ابلاغیه طرحی را تنظیم می‌کند (طرح اقدام حفاظت از زیرساخت‌های اطلاعاتی حیاتی) تا امنیت و انعطاف‌پذیری زیرساخت‌های حیاتی فناوری اطلاعات و ارتباطات را تقویت کند. هدف این طرح ترغیب و حمایت از توسعه سطح بالایی از قابلیت‌های آمادگی، امنیت و انعطاف‌پذیری، هم در سطح ملی و هم در سطح اروپا بود. این رویکرد به‌وسیله مجمع در سال ۲۰۰۹ در حد گسترده‌ای تأیید شد[۲۰]. طرح اقدام حفاظت از زیرساخت‌های اطلاعاتی حیاتی در پنج محور بنا نهاده شد: ۱) آمادگی و پیش‌گیری؛ ۲) تشخیص و پاسخ؛ ۳) مقابله و بازیابی؛ ۴) همکاری بین‌المللی؛ و ۵) معیارهایی برای زیرساخت‌های حیاتی اروپا در حوزه فناوری اطلاعات و ارتباطات. طرح اقدام حفاظت از زیرساخت‌های اطلاعاتی حیاتی کارهایی را که باید تحت هر محور توسط کمیسیون، دولت‌ها یا صنایع عضو، تحت حمایت سازمان امنیت شبکه و اطلاعات اروپا انجام شوند، مشخص می‌کند.

دستور کار دیجیتال برای اروپا[۲۱] (DAE) که در ماه می ۲۰۱۰ به‌کار گرفته شد و نتایج مرتبط با مجمع[۲۲] بر این درک مشترک تأکید کردند که اعتماد و امنیت پیش‌نیازهایی بنیادی برای ارتقای فناوری اطلاعات و ارتباطات هستند و بنابراین، برای دست‌یابی به اهداف بُعد "رشد هوشمند"

1- Critical Information Infrastructure Protection

در استراتژی ۲۰۲۰ اروپا[۲۳] موردنیاز هستند. دستور کار دیجیتال برای اروپا نیاز به همه ذی‌نفعان را برای الحاق نیروها، در تلاشی کُل‌نگر برای تضمین امنیت و انعطاف‌پذیری زیرساخت‌های فناوری اطلاعات و ارتباطات مورد تأکید قرار می‌دهد. برای رسیدن به این مقصود، دستور کار دیجیتال برای اروپا به نیاز به تمرکز بر پیش‌گیری، آمادگی و آگاهی و نیز توسعه سازوکارهای مؤثر و هماهنگ شده جهت پاسخ‌گویی به شکل‌های جدید و رو به پیشرفت حملات سایبری و جرائم سایبری اهمیت زیادی می‌دهد. این رویکرد تضمین می‌کند که هر دو بُعد پیشگیرانه و واکنش‌گرانه از این چالش باید به اقتضای خود در نظر گرفته شوند.

اقدامات زیر که در دستور کار دیجیتال اعلان شدند، انجام گرفته‌اند:

- ✓ کمیسیون در سپتامبر ۲۰۱۰ طرح پیشنهادی را برای دستورالعمل مواجهه با حملات به سیستم‌های اطلاعاتی پذیرفت[۲۴]. هدف این طرح تقویت مبارزه علیه جرائم سایبری، از طریق نزدیک کردن نظام حقوق جزایی دولت‌های عضو و بهبود همکاری بین مراجع قضایی و دیگر مراجع ذی‌صلاح است. این طرح، همچنین قیودی را برای مواجهه با شکل‌های جدید حملات سایبری، به‌ویژه باتنت معرفی می‌کند.
- ✓ به‌عنوان مکمل، کمیسیون به‌طور همزمان طرح پیشنهادی[۲۵] را برای یک حکم جدید جهت تقویت و مدرنیزه کردن سازمان امنیت شبکه و اطلاعات اروپا به‌منظور ارتقای اعتماد و امنیت شبکه در دستور کار قرار داد. تقویت و مدرنیزه کردن سازمان امنیت شبکه و اطلاعات اروپا به اتحادیه اروپا، دولت‌های عضو و ذی‌نفعان بخش خصوصی کمک خواهد کرد قابلیت‌ها و آمادگی خود را برای جلوگیری، تشخیص و پاسخ به چالش‌های امنیت سایبری توسعه دهند.

شورای پیمان‌نامه اروپا درباره جرم سایبری

در سال ۲۰۰۱، اتحادیه اروپا رسماً تشکیل شورای پیمان‌نامه اروپا درباره جرم سایبری (CECC)[1] را اعلام کرد که "دستورالعمل‌هایی را برای همه دولت‌هایی وضع می‌کند که قصد توسعه قوانین در مقابل جرم سایبری دارند" و "چارچوبی را برای همکاری‌های بین‌المللی در این حوزه فراهم می‌کند." ۳۹ کشور اروپایی به همراه کانادا، ژاپن، آفریقای جنوبی و ایالات متحده آمریکا این معاهده را امضا کردند. این امر باعث شد تا شورای پیمان‌نامه اروپا درباره جرم سایبری که در ماه جولای ۲۰۰۴ به مرحله اجرا در آمد، "تنها معاهده الزام‌آور بین‌المللی درباره این موضع باشد که تا کنون اجرایی شده است"[۲۶].

1- Council of Europe Convention on Cybercrime

سازمان امنیت شبکه و اطلاعات اروپا[1] (ENISA)

سازمان امنیت شبکه و اطلاعات اروپا توسط پارلمان اروپا و شورای اتحادیه اروپا، در دهم ماه مارس ۲۰۰۴، "به‌منظور کمک به افزایش امنیت شبکه و اطلاعات در جامعه اتحادیه اروپا و برای ترویج فرهنگ استفاده امنیت شبکه و اطلاعات به سود شهروندان، مصرف‌کنندگان و سازمان‌های بخش عمومی و خصوصی" تأسیس شد.

دید گروه ذی‌نفعان دائمی برای سازمان امنیت شبکه و اطلاعات اروپا[۲۷] که در ماه می ۲۰۰۶ بیان شد، سازمان امنیت شبکه و اطلاعات اروپا را به‌عنوان یک قطب علمی در امنیت اطلاعات و شبکه، محلی برای هم‌اندیشی ذی‌نفعان امنیت شبکه و اطلاعات و محرکی برای آگاهی از امنیت اطلاعات برای همه شهروندان اتحادیه اروپا می‌بینند. برای این منظور اقدامات بلند مدت زیر برای سازمان امنیت شبکه و اطلاعات اروپا در دید گروه ذی‌نفعان دائمی تصریح شده است (شکل ۱-۳ را مشاهده کنید).

شکل ۱-۳ اقدامات بلند مدت برای سازمان امنیت شبکه و اطلاعات اروپا

منبع: Paul Dorey and Simon Perry, eds. The PSG Vision for ENISA (Permanent Stakeholders Group, 2006), http://www.enisa.europa.eu/about-enisa/structure-organization/psg/files/psg-vision.

1- European Network and Information Security Agency

۱- همکاری و هماهنگی بین مراجع ملی امنیت اطلاعات و شبکه در دولت‌های عضو

همکاری بین سازمان‌های ملی در حال حاضر بسیار کم است. با ارتقای حجم ارتباطات و همکاری بین سازمان‌های ملی، به‌ویژه با تسهیم بهترین اقدامات از طرف سازمان‌های پیشرو با آن‌هایی که هنوز در مرحله آغازین هستند، کارهای بسیار خوبی می‌توان انجام داد.

۲- همکاری با مؤسسات پژوهشی

هدف سازمان امنیت شبکه و اطلاعات اروپا باید هدایت تحقیقات پایه و توسعه فنی هدفمند باشد تا بر حوزه‌هایی با بیشترین مزیت برای مدیریت ریسک امنیتی واقعی در دنیای واقعی تمرکز داشته باشد. سازمان امنیت شبکه و اطلاعات اروپا نباید معضلات پژوهشی را از سوی خود تعریف کند، بلکه باید هم‌راستا با فرآیندها و اولویت‌های موجود از برنامه‌های موجود اقدام کند.

۳- همکاری با فروشندگان نرم‌افزار و سخت‌افزار

فروشندگان نرم‌افزار و سخت‌افزار، طبق تعریف رقیب هستند و برای آن‌ها دشوار است که بتوانند به‌راحتی بر سر اقدامات دوجانبه توافق داشته باشند. سازمان امنیت شبکه و اطلاعات اروپا می‌تواند عقاید بی‌طرفانه‌ای را ابراز کند و یک محل گردهمایی را برای بحث‌های حساس فراهم کند، در عین حال می‌تواند محیط مساعدی را برای مقابله با رفتارهای ضد رقابتی حفظ کند.

دید بلند مدت سازمان امنیت شبکه و اطلاعات اروپا به‌جای گسترش روندهای فزاینده امنیتی، باید بیشتر بر ایجاد فناوری‌های شبکه‌ای و اطلاعاتی قابل‌اعتمادی متمرکز باشد که در مقابل کرم‌ها و دیگر مشکلات مقاوم هستند. با ترویج تکنیک‌هایی برای توسعه معماری‌ها و نرم‌افزارهای درست، امن و قابل‌اعتماد می‌توان به این هدف نائل شد.

۴- شرکت در نهادهای تنظیم استاندارد

سازمان امنیت شبکه و اطلاعات اروپا باید با قصد شناسایی و جلب‌توجه همگانی به اقدامات پر ارزش، معضلات مربوط به امنیت شبکه و اطلاعات را در نهادهای تنظیم استاندارد دنبال کرده و نظارت کند، از جمله می‌تواند فعالیت‌های نهادهای گواهی‌دهنده و اعتبارسنجی در امنیت را پیگیری کند.

۵- شرکت در فرآیندهای قانون‌گذاری از طریق اعمال نفوذ و ابراز عقاید

سازمان امنیت شبکه و اطلاعات اروپا باید برای به‌دست آوردن موقعیت یک نهاد مشاوره مورد اعتماد تلاش کند تا نظراتش در فرآیند پیش‌نویسی و پیشنهاد کردن قوانین و دستورالعمل‌ها، در معضلات مربوط به امنیت شبکه و اطلاعات، موردپذیرش قرار گیرد.

۶- کار با سازمان‌های کاربر

اغلب، سازمان‌های کاربری به‌خوبی فروشندگان در نهادهای تنظیم‌کننده استاندارد و قانون‌گذاری در نظر گرفته نمی‌شوند. سازمان امنیت شبکه و اطلاعات اروپا می‌تواند بینشی را در مورد فعالیت‌های مربوط به استانداردها، برای گروه کاربران نهایی فراهم کرده و فرصتی برای اثرگذاری بر این فعالیت‌ها

به آن‌ها بدهد.

۷- شناسایی و ترویج بهترین اقدامات در دولت‌های عضو برای صنایع مرتبط با کاربر نهایی

سازمان امنیت شبکه و اطلاعات اروپا نه تنها باید از منافع کسب‌وکار حفاظت کند، بلکه باید اطمینان کاربر نهایی را در استفاده از اینترنت و رسانه‌های دیجیتال افزایش دهد.

۸- تلاش برای یافتن راه‌حل‌های فنی و سیاسی جهت مدیریت هویت

فقدان اطمینان به اینترنت مانع عمده‌ای در مقابل کسب‌وکارهای الکترونیکی مشتری‌گرا در مقیاس بزرگ است. وجود توانایی در بررسی دقیق هویت مالک یک سایت، یک آدرس رایانامه یا یک سرویس آنلاین، گامی بزرگ در نوسازی و افزایش اعتماد مشترک کاربران به اینترنت است. راه‌حل‌های فنی در این حوزه را باید در فرآیندهای منتج از صنعت جویا شد، اما سازمان امنیت شبکه و اطلاعات اروپا می‌تواند برای احراز هویت موجودیت‌های آنلاین، در راستای خط‌مشی‌های موجود در سطح اتحادیه اروپا عمل کند.

۹- متوازن کردن تلاش‌ها برای معضلات امنیتی "اطلاعات" و "شبکه"

سازمان امنیت شبکه و اطلاعات اروپا باید با بزرگ‌ترین شرکت‌های ارائه‌کننده خدمات اینترنت و شبکه مراوده داشته باشد تا به آن‌ها در شناسایی بهترین اقدامات، در جهت سودرسانی به کسب‌وکار و مشتریان در سراسر اروپا یاری رساند. این کار مهم است، چون شرکت‌های ارائه‌کننده خدمات اینترنت و شبکه می‌توانند نقشی کلیدی را در بهبود امنیت اینترنت، در مقیاس بزرگ ایفا کنند. در حال حاضر، همکاری و هماهنگی در فعالیت‌هایی که ارائه‌دهندگان خدمات اینترنتی انجام می‌دهند، مشاهده نمی‌شود.

منبع:

Abridged from Paul Dorey and Simon Perry, eds., The PSG Vision for ENISA (Permanent Stakeholders Group, 2006), http://www.enisa.europa.eu/about-enisa/structure-organization/psg/files/psg-vision.

سازمان امنیت شبکه و اطلاعات اروپا به‌عنوان نهادی تخصصی، به‌وسیله اتحادیه اروپا تأسیس شده تا وظایف بسیار فنی و علمی بخصوص را در حوزه امنیت اطلاعات انجام دهد. این نهاد به‌عنوان یک "سازمان عام‌المنفعه اروپایی" فعالیت می‌کند. همچنین، این سازمان به کمیسیون اروپا در فعالیت‌های آماده‌سازی فنی برای بهنگام‌رسانی و توسعه قوانین جامعه در حوزه امنیت شبکه و اطلاعات یاری می‌رساند.

وظایف اصلی سازمان امنیت شبکه و اطلاعات اروپا بر موارد زیر متمرکز شده‌اند:

- ✓ ارائه مشاوره و کمک به کمیسیون و دولت‌های عضو درباره امنیت اطلاعات و در مورد گفت‌وگوی آن‌ها با صنعت، به‌منظور رفع مشکلات مربوط به امنیت در محصولات سخت‌افزاری و نرم‌افزاری
- ✓ جمع‌آوری و تحلیل داده‌ها درباره رخدادهای امنیتی در اروپا و ریسک‌های نوظهور
- ✓ ترویج روش‌های ارزیابی ریسک و مدیریت ریسک به‌منظور ارتقای توانایی مواجهه با تهدیدها در امنیت اطلاعات
- ✓ بالا بردن آگاهی و همکاری بین اقدام‌کننده‌های مختلف در حوزه امنیت اطلاعات، به‌طور ویژه با توسعه مشارکت‌های بخش‌های عمومی و خصوصی با صنعت در این حوزه

استراتژی امنیت اطلاعات در کشور جمهوری کره

جمهوری کُره با موفقیت توانسته موقعیتی به‌عنوان یک پیشرو جهانی در فناوری اطلاعات و ارتباطات برای خود ایجاد کند. این کشور رتبه سوم را از لحاظ شاخص توسعه فناوری اطلاعات اتحادیه بین‌المللی مخابرات و رتبه ۱۵ را از لحاظ شاخص آماده‌سازی شبکه در مجمع جهانی اقتصاد دارا است. در حال حاضر، این کشور از رتبه بالایی در شاخص‌های اصلی فناوری اطلاعات برخوردار است.

جمهوری کره به‌سرعت به سمت عصر جامعه فراگیر حرکت کرد که از طریق پیشرفت جامعه اطلاعاتی و همگرایی فناوری اطلاعات و ارتباطات با صنعت، تغییرات انقلابی را در تمام جنبه‌های زندگی روزانه ایجاد می‌کند. با این حال، این حرکت آثار منفی را نیز از قبیل شکاف بین فرهنگ و فناوری و تجاوز به حریم خصوصی به‌دنبال داشت.

دولت کره در پاسخ به این آثار منفی، در ماه دسامبر ۲۰۰۶، استراتژی جامعی را با عنوان "استراتژی اساسی برای امنیت اطلاعات فراگیر" تصویب کرد. اهداف اصلی این استراتژی عبارت بودند از: تضمین اینکه مردم کره بتوانند به‌طور ایمن از خدمات فناوری اطلاعات و ارتباطات در همه حوزه‌ها، از جمله خدمات مالی، آموزشی و پزشکی استفاده کنند؛ و اینکه حریم خصوصی حفاظت شده و محیطی خوب برای استفاده از اطلاعات پیاده‌سازی شود. استراتژی بنیادین برای امنیت اطلاعات فراگیر مفهوم حفاظت اطلاعات را گسترش می‌دهد تا امنیت فراگیر، حریم خصوصی فراگیر، اعتماد فراگیر و پاکیزگی فراگیر را در برگیرد. همچنین با کار کردن از دورنمای محافظت از کاربر، این استراتژی نیاز به حفاظت اطلاعات را به‌عنوان یک توانمندساز و نه یک مانع در جامعه فراگیر در نظر می‌گیرد.

از اواسط دهه ۱۹۸۰ تا کنون، جمهوری کره طرح ملی اطلاعاتی‌سازی را دنبال کرده است و اکنون به نظر می‌رسد این کشور به دوره تثبیت رسیده است. اما امنیت اطلاعات به‌عنوان یک هدف ملی، موضوع نسبتاً جدیدی است که از اواسط دهه ۲۰۰۰ شروع شد. مطالعات در آن زمان نشان داد که سیستم‌های فناوری اطلاعات و ارتباطات در مقیاس‌های مالی و زیرساخت‌های مرتبط با آن‌ها و نیز

فعالیت‌های تحقیق و توسعه بسیار ضعیف بودند. از این رو، دولت کره تصمیم گرفت که زیرساخت‌های کلیدی فناوری اطلاعات و ارتباطات را به روش گام به گام، از طریق دنبال کردن یک طرح جامع پایه‌گذاری کند. در ماه جولای ۲۰۰۸، دولت طرح جامع میان مدت را برای امنیت اطلاعات اجرا کرد. این طرح از شش برنامه کاری به قرار زیر تشکیل شده است:

۱- بهبود توانایی کشور در اداره کردن حملات سایبری
۲- تقویت حفاظت از زیرساخت‌های اطلاعاتی حیاتی ملی
۳- تقویت سیستم‌های حفاظت از اطلاعات شخصی
۴- گسترش زیرساخت‌های امنیت اطلاعات
۵- افزایش رقابت‌پذیری در صنعت امنیت اطلاعات
۶- ایجاد فرهنگ امنیت اطلاعات

این شش برنامه کاری را باز هم می‌توان به ۱۸ وظیفه اصلی و ۷۳ وظیفه مشروح تجزیه کرد. تحت این طرح، دولت اهداف خود را در تشکیل یک جامعه فراگیر امن و مورد اعتماد با تضمین قابلیت اعتماد خدمات در دولت الکترونیکی، از بین بردن اضطراب شهروندان و به‌دست آوردن یکپارچگی در فعالیت‌های کسب‌وکار تشریح کرد.

در حالی‌که که دستگاه‌های همراه فراگیرتر شده و با ویژگی‌های جدیدتر و کاربردهای متنوع "هوشمندتر" می‌شوند، به‌گونه‌ای که کاربران می‌توانند خدمات گوناگون الکترونیکی را دریافت کنند، این محیط همراه جدید در معرض تهدیدهای امنیتی روزمره نیز هست. دولت کره در یک پاسخ پیش‌دستانه به این مشکلات و چالش‌ها، پلت‌فرم‌های مشارکتی متنوعی را برای انجام اقدامات پیشگیرانه در امنیت تلفن‌های هوشمند و همراه بنا نهاد و استراتژی امنیت اطلاعات موبایل را در دسامبر ۲۰۱۰ اعلان کرد. چشم‌انداز این استراتژی برای جمهوری کره این است که این کشور پیشرو در امنیت موبایل در دنیا باشد. آرمان‌های آن شامل بهبود کیفیت در سرویس‌ها و امنیت زیرساخت‌های موبایل در آینده؛ حفاظت از حریم خصوصی برای کاربران موبایل؛ و پیشرفت در زیرساخت‌های امنیتی موبایل است. در این استراتژی، سه حوزه موردتوجه و ۱۰ وظیفه اصلی وجود دارند (شکل ۲-۳ را مشاهده کنید).

شکل ۲-۳ استراتژی امنیت اطلاعات موبایل در جمهوری کره

استراتژی امنیت اطلاعات در ژاپن[۲۸]

ژاپن در راستای هدف کلان تبدیل شدن به یک "کشور پیشرفته در امنیت اطلاعات"[۲۹] یک مجموعه مشروح از اهداف، اصول و پروژه‌های پایه را در حوزه امنیت اطلاعات اعلام کرده است. شورای سیاست‌های امنیت اطلاعات و مرکز ملی امنیت اطلاعات (NISC)[1] دو سازمان اصلی هستند که بر فعالیت‌های مرتبط با امنیت اطلاعات را در این کشور نظارت دارند. در حوزه پژوهش در تهدیدهای سایبری، مرکز پاک‌سازی سایبری تأسیس شده است تا ویژگی‌های بات‌ها را تحلیل کرده و یک روش پاسخ‌گویی مؤثر و امن را تدوین کند.

استراتژی امنیت اطلاعات در کشور ژاپن به دو بخش تقسیم می‌شود: ۱) اولین استراتژی ملی در امنیت اطلاعات که به‌طورکلی به‌کار گرفته می‌شود؛ و ۲) ژاپن امن در YYYY . *اولین استراتژی ملی در امنیت اطلاعات*، نیاز به همه موجودیت‌ها در یک جامعه فناوری اطلاعات را "به‌منظور مشارکت در خلق محیطی برای استفاده ایمن از فناوری اطلاعات" به‌رسمیت می‌شناسد. این استراتژی موجودیت‌هایی را "که در واقع، به‌عنوان مؤلفه‌های یک جامعه فناوری اطلاعات، اقداماتی را به‌کار گرفته و اجرا می‌کنند"[۳۰] باز می‌شناسد. این "موجودیت‌های اجراکننده" به چهار دسته تقسیم می‌شوند: دولت‌های مرکزی و محلی، زیرساخت‌های حیاتی، کسب‌وکارها و افراد. هرکدام از این موجودیت‌ها ملزم به تدوین نقش‌ها و طرح‌های خود و عمل کردن به آن‌ها هستند (جدول ۱-۳ را مشاهده کنید).

1- National Information Security Center (Japan)

جدول ۱-۳ نقش‌ها و طرح‌های هر دسته بر اساس اولین استراتژی ملی در امنیت اطلاعات

دسته	نقش‌ها	طرح‌ها
دولت‌های مرکزی و محلی	ارائه بهترین شیوه‌ها برای اقدامات امنیت اطلاعات	استانداردهایی برای اقدامات
زیرساخت‌های حیاتی	تضمین تدارک پایدار خدمات بر اساس زندگی اجتماعی و فعالیت‌های اقتصادی مردم	طرح اقدام زیرساخت‌های حیاتی
کسب‌وکارها	پیاده‌سازی اقدامات امنیت اطلاعات به‌گونه‌ای که از سوی بازار موردتوجه زیاد قرار گیرد.	اقدامات ترویج شده به‌وسیله وزارتخانه‌ها و سازمان‌ها
افراد	بالا بردن آگاهی به‌عنوان بازیگر اصلی در جامعه فناوری اطلاعات	اقدامات ترویج شده به‌وسیله وزارتخانه‌ها و سازمان‌ها

منبع: NISC, Japanese Government's Efforts to Address Information Security Issues(November 2007), http://www.nisc .go.jp/eng/.

سیاست‌های عملی اولین استراتژی ملی در امنیت اطلاعات به شرح زیر هستند:

- ✓ ترویج فناوری امنیت اطلاعات: توسعه فناوری‌هایی که به استفاده دولتی اختصاص داده می‌شود و ترویج توسعه فناوری که "چالش بزرگ" مربوط به نوآوری در فناوری‌های بنیادی را با دورنمای بلند مدت مدنظر قرار می‌دهد؛
- ✓ ترویج همکاری‌ها و مشارکت‌های بین‌المللی: سهیم شدن در تأسیس پایگاه‌های بین‌المللی برای امنیت و اطمینان‌آفرینی اطلاعات و فراهم کردن سهم بین‌المللی ژاپن؛
- ✓ توسعه منابع انسانی: توسعه منابع انسانی با مهارت‌ها و استعدادهای عملی و توانایی گسترده و سازمان‌دهی یک سیستم تعیین صلاحیت برای امنیت اطلاعات؛
- ✓ کنترل جرم و اقدامات حفاظتی و ترمیمی برای حقوق و منافع: تقویت کنترل جرائم سایبری و توسعه پایگاه‌های قانونی مربوطه و نیز توسعه فناوری برای پیشرفت امنیت در فضای سایبری.

ژاپن امن در YYYY طرحی سالانه برای امنیت اطلاعات است. ژاپن امن در سال ۲۰۰۷ شامل ۱۵۹ اقدام اجرایی امنیت اطلاعات و دستورالعمل مستندسازی طرح برای ۲۴ اولویت در سال ۲۰۰۷ بود. این موارد را می‌توان به شرح زیر خلاصه کرد:

- ✓ گسترش اقدامات امنیت اطلاعات برای سازمان‌های دولتی مرکزی

- ✓ انتشار اقدامات برای سازمان‌هایی که از اجرای اقدامات برای تضمین امنیت اطلاعات عقب مانده‌اند و نیز برای عموم.
- ✓ تلاش‌های گسترده برای تقویت پلت فرم‌های امنیت اطلاعات

شورای سیاست‌های امنیت اطلاعات، در ماه فوریه ۲۰۰۹، دومین استراتژی ملی را در امنیت اطلاعات تصویب کرد. این استراتژی به‌عنوان "استراتژی امنیت اطلاعات برای حفاظت از کشور (طرح میان‌مدت: ۲۰۱۰ الی ۲۰۱۳)" در برگیرنده بهنگام‌رسانی‌ها بوده و اقدامات ذکر شده در اولین استراتژی ملی را اولویت‌گذاری کرده است (شکل ۳-۳ نشان‌دهنده خلاصه‌ای از این استراتژی است).

شکل ۳-۳ خلاصه‌ای از استراتژی امنیت اطلاعات برای حفاظت از کشور (طرح میان‌مدت: ۲۰۱۰ الی ۲۰۱۳)

اهداف استراتژی امنیت اطلاعات برای حفاظت از کشور عبارتند از:

- ✓ تضمین زندگی امن و ایمن شهروندان
- ✓ بنیان‌گذاری خط‌مشی‌هایی برای مدیریت امنیت و بحران در مقابل حملات سایبری
- ✓ کمک به رشد اقتصادی از طریق فناوری اطلاعات

دسته‌های اصلی این استراتژی به قرار زیر است:

الف) ایجاد قابلیت‌های پاسخ‌دهی به حملات سایبری در مقیاس بزرگ

۱- بهبود توانایی‌های پاسخ‌دهی

۲- ایجاد و تقویت چارچوب برای جمع‌آوری و به‌اشتراک‌گذاری اطلاعات

ب) تقویت خط‌مشی‌های امنیت اطلاعات برای مواجهه با محیط جدید

۱- تقویت بنیان‌های امنیت اطلاعات برای حفاظت از کشور

- ✓ تقویت بنیان سازمان‌های دولتی، زیرساخت‌های حیاتی و موارد مشابه.

۲- تقویت حفاظت از شهروندان/کاربران فناوری اطلاعات

- ✓ ترویج آگاهی از امنیت
- ✓ فراهم کردن خدمات مشاوره در امنیت اطلاعات
- ✓ ترویج حفاظت از اطلاعات شخصی
- ✓ تقویت دفاع در مقابل جرائم سایبری

۳- ترویج همکاری‌های بین‌الملل

- ✓ تقویت همکاری‌ها با ایالات متحده آمریکا، جامعه کشورهای جنوب شرق آسیا و اتحادیه اروپا
- ✓ ترویج اشتراک اطلاعات در کنفرانس‌های بین‌المللی
- ✓ تقویت عملکردهای NISC به‌عنوان نقطه تماس ملی

۴- ترویج استراتژی تحقیق و توسعه

- ✓ ترویج استراتژیک برنامه‌های تحقیقاتی و توسعه مرتبط با امنیت اطلاعات
- ✓ توسعه منابع انسانی برای امنیت اطلاعات
- ✓ برقراری "حاکمیت امنیت اطلاعات"

۵- ایجاد اصلاحات و بهبود در مؤسسات مربوط به امنیت اطلاعات

- ✓ حمایت از مؤسساتی که به امنیت فضای مجازی کمک می‌کنند.
- ✓ مطالعه و بررسی مؤسسات خارجی مرتبط با امنیت اطلاعات

بر اساس استراتژی اصلاح شده، طرح سالانه ۲۰۱۰ برای امنیت اطلاعات توسعه داده شد. این طرح سیاست‌های مشروحی را که قرار بود از سال مالی ۲۰۱۰ تا ۲۰۱۱ اجرا شوند و شامل ۱۹۶ اقدام هستند بر می‌شمرد.

پرسش‌هایی برای تفکر

۱- فعالیت‌های امنیت اطلاعات در کشور شما تا چه حدی با فعالیت‌هایی که توصیف شد متفاوت است؟

۲- آیا فعالیت‌های امنیت اطلاعاتی در کشورهای ذکر شده در این بخش وجود دارد که در کشور شما قابل اجرا نیست یا به کشور شما مربوط نمی‌شود؟ اگر جواب مثبت است، این فعالیت‌ها کدامند و چرا آن‌ها قابل اجرا نبوده یا نامربوط هستند؟

شکل ۴-۳ خلاصه‌ای از طرح سالانه ۲۰۱۰ برای امنیت اطلاعات

۳-۲ فعالیت‌های بین‌المللی امنیت اطلاعات

فعالیت‌های امنیت اطلاعات در سازمان ملل

در **اجلاس جهانی درباره جامعه اطلاعاتی**[۳۱] **(WSIS)**[1] که با حمایت سازمان ملل برگزار شد، بیانیه‌ای پیرامون اصول و طرح‌های اقدام برای رشد مؤثر جامعه اطلاعاتی و پر کردن "شکاف اطلاعاتی" تصویب شد. طرح اقدام، این موارد را تعریف می‌کند:

- ✓ نقش دولت و همه ذی‌نفعان در ترویج فناوری اطلاعات و ارتباطات برای توسعه
- ✓ زیرساخت‌های اطلاعاتی و ارتباطی به‌عنوان شالوده ضروری برای جامعه اطلاعاتی فراگیر

1- Working Party on Information Security and Privacy (OECD)

- ✓ دسترسی به اطلاعات و دانش
- ✓ ظرفیت‌سازی
- ✓ ایجاد اطمینان و امنیت در استفاده از فناوری اطلاعات و ارتباطات
- ✓ ایجاد و توانمندسازی محیط
- ✓ کاربردهای فناوری اطلاعات و ارتباطات در همه جنبه‌های زندگی
- ✓ تنوع فرهنگی و هویت، تنوع زبانی و محتوای بومی
- ✓ رسانه‌ها
- ✓ ابعاد اخلاقی جامعه اطلاعاتی
- ✓ همکاری بین‌المللی و منطقه‌ای[۳۲]

مجمع نظارت بر اینترنت[۳۳] (IGF)[1] سازمانی حامی برای مشکلات نظارت بر اینترنت در سازمان ملل است. این سازمان به‌دنبال مرحله دوم اجلاس جهانی در مورد جامعه اطلاعاتی در تونس، برای مواجهه با مشکلات مربوط به نظارت در اینترنت تأسیس شد. دومین نشست مجمع نظارت بر اینترنت در ریودوژانیرو از ۱۲ الی ۱۵ نوامبر ۲۰۰۷ برگزار شد که بر مشکلات امنیت اطلاعات، از قبیل تروریسم سایبری، جرائم سایبری و ایمنی فرزندان در اینترنت تمرکز یافته بود.

فعالیت‌های امنیت اطلاعات در سازمان همکاری و توسعه اقتصادی (OECD)[2] [۳۴]

سازمان همکاری و توسعه اقتصادی، محلی یکتا برای تبادل‌نظر دولت‌های ۳۰ دموکراسی فعال است که با یکدیگر و به همراه جامعه کسب‌وکار و مدنی همکاری می‌کنند تا چالش‌های اقتصادی، اجتماعی، محیطی و نظارتی را که پیش‌روی جهانی‌سازی اقتصاد وجود دارد، حل‌وفصل کنند. در سازمان همکاری و توسعه اقتصادی، بخش کاری مربوط به امنیت اطلاعات و حریم خصوصی (WPISP)[3] تحت نظارت کمیته خط‌مشی‌های اطلاعاتی، رایانه‌ای و ارتباطی فعالیت می‌کند تا اثر فناوری اطلاعات و ارتباطات را بر امنیت اطلاعات و حریم خصوصی تحلیل کرده و با اجماع آرا توصیه‌هایی را برای خط‌مشی‌ها فراهم کند و به‌این وسیله اعتماد را در اقتصاد اینترنتی پایدار گرداند.

فعالیت‌های WPISP در امنیت اطلاعات: در سال ۲۰۰۲، سازمان همکاری و توسعه اقتصادی "رهنمودهایی را برای امنیت سیستم‌ها و شبکه‌های اطلاعاتی: به‌سوی فرهنگ توجه به امنیت"[۳۵] صادر کرد تا "امنیت را در توسعه سیستم‌ها و شبکه‌های اطلاعاتی و در به‌کارگیری روش‌های جدید تفکر و رفتار در حین استفاده و تعامل با سیستم‌ها و شبکه‌های اطلاعاتی" ترویج دهد[۳۶].

1- Internet Governance Forum
2- Organisation for Economic Co-operation and Development
3- Working Party on Information Security and Privacy

برای به‌اشتراک‌گذاری تجربیات و بهترین شیوه‌ها در امنیت اطلاعات، نشست جهانی در مورد امنیت سیستم‌های اطلاعاتی و شبکه در سال ۲۰۰۳ و کارگاه آموزشی سازمان همکاری و توسعه اقتصادی- همکاری اقتصادی آسیا و اقیانوسیه پیرامون امنیت سیستم‌های اطلاعاتی و شبکه‌ها در سال ۲۰۰۵ برگزار شدند.

در سال ۲۰۱۰، پروژه‌ای برای روش‌های تحقیق در مورد مواجهه با بات‌نت از دیدگاه حریم خصوصی و امنیت اطلاعات پیشنهاد داده شد. یک گروه داوطلب برای دنبال کردن این پروژه تشکیل شده است. این گروه داوطلب از نمایندگان کشورهای استرالیا، کانادا، آلمان، ژاپن، جمهوری کره، هلند، سوئد، ترکیه، انگلستان، ایالات متحده آمریکا و اتحادیه اروپا و نیز کمیته‌هایی از سازمان همکاری و توسعه اقتصادی (شامل کمیته مشورتی کسب‌وکار و صنعت، کمیته مشورتی جامعه مدنی و جامعه اطلاعاتی و کمیته مشورتی موارد فنی در اینترنت) تشکیل شده بود. جمهوری کره در این پروژه شرکت خواهد کرد و ضمناً حمایت مالی را هم انجام خواهد داد.

فعالیت‌های امنیت اطلاعات و حریم خصوصی پیرامون حریم خصوصی: "دستورالعمل حفاظت از حریم خصوصی و جریان داده‌های شخصی در سیستم‌های مرزی" که در سال ۱۹۸۰ صادر شد، نشان‌دهنده وجود یک وفاق بین‌المللی بر سر اداره اطلاعات شخصی در بخش‌های عمومی و خصوصی است. "حریم خصوصی آنلاین: راهنمای سازمان همکاری و توسعه اقتصادی در خط‌مشی و عمل" که در سال ۲۰۰۲ صادر شد بر فناوری‌های گسترش حریم خصوصی، خط‌مشی‌های لازم در حریم خصوصی آنلاین، اجرا و اصلاح و نیز موارد مشابه در تجارت الکترونیکی تمرکز می‌کند. در حال حاضر، امنیت اطلاعات و حریم خصوصی در حال کار روی همکاری‌های اجرایی در قانون حریم خصوصی است.

در سال ۲۰۱۱، پروژه توسعه شاخص‌های امنیت اطلاعات و حریم خصوصی برای داشتن آمار قابل‌اعتماد و تطبیقی در میان اعضای سازمان همکاری و توسعه اقتصادی پیشنهاد داده شد. جمهوری کره، از طریق شرکت فعال و حمایت مالی، در این پروژه سهیم خواهد بود.

دیگر فعالیت‌ها: در سال ۱۹۹۸، سازمان سازمان همکاری و توسعه اقتصادی "دستورالعمل خط‌مشی رمزنگاری" را صادر کرده و بیانیه مصوب هیئت وزیران دولت اتاوا در مورد احراز هویت و تجارت الکترونیکی را مورد حمایت قرار داد. از سال ۲۰۰۲ تا سال ۲۰۰۳، یک "بررسی در مورد چارچوب‌های حریم خصوصی برای سرویس‌های احراز هویت و امضای الکترونیکی در کشورهای عضو سازمان همکاری و توسعه اقتصادی" انجام شد. در سال ۲۰۰۵، خبر "استفاده از احراز هویت در سراسر مرزهای کشورهای سازمان همکاری و توسعه اقتصادی" اعلام شد.

در سال ۲۰۰۴، "فناوری‌های مبتنی بر بیومتریک" نگاشته شد و در سال ۲۰۰۵ گروه ضربت برای هرزنامه‌ها تشکیل گردید. دیگر فعالیت‌های در حال انجام به مدیریت هویت دیجیتال، بدافزارها،

ردفاشگر فراگیر[1] (RFID)، حس‌گرها و شبکه‌ها و چارچوبی مشترک برای پیاده‌سازی امنیت اطلاعات و حریم خصوصی مربوط می‌شود.

فعالیت‌های امنیت اطلاعات سازمان همکاری‌های اقتصادی آسیا و اقیانوسیه[۳۷]

سازمان همکاری‌های اقتصادی آسیا و اقیانوسیه (APEC)[2] فعالیت‌های امنیت اطلاعات را در کشورهای حوزه اقیانوس آرام از طریق گروه کاری مخابرات و اطلاعات (TEL)[3] دنبال می‌کند این گروه از سه گروه راهبری تشکیل شده است: گروه راهبری لیبرال‌سازی، گروه راهبری توسعه فناوری اطلاعات و ارتباطات و گروه راهبری شکوفایی.

مخصوصاً از نشست ششم سازمان همکاری‌های اقتصادی آسیا و اقیانوسیه در سطح وزرا در صنعت مخابرات و اطلاعات که در ماه ژوئن ۲۰۰۵ در لیما، پایتخت پرو، برگزار شد، گروه راهبری رفاه بحث‌های مربوط به امنیت سایبری و جرائم سایبری را مطرح کرده است. استراتژی امنیت سایبری سازمان همکاری‌های اقتصادی آسیا و اقیانوسیه که شامل تقویت اعتماد مصرف‌کننده در استفاده از تجارت الکترونیکی است، به متحد کردن تلاش‌های متنوع از نظام‌های اقتصادی مختلف کمک می‌کند. این تلاش‌ها در بردارنده تصویب و اجرای قوانین درباره امنیت سایبری است که با قطع‌نامه ۵۵/۶۳[۳۸] مجمع عمومی سازمان ملل و کنوانسیون جرائم سایبری[۳۹] سازگاری دارد. اقدامات قانون‌گذاری گروه کاری مخابرات و اطلاعات پیرامون جرم سایبری و پروژه ظرفیت‌سازی اعمال آن‌ها مؤسسات را در اجرای قوانین جدید حمایت می‌کند.

اعضای سازمان همکاری‌های اقتصادی آسیا و اقیانوسیه همچنین برای پیاده‌سازی تیم‌های پاسخ اضطراری رایانه‌ای به‌عنوان یک سیستم دفاعی هشداردهنده اولیه در مقابل حملات سایبری همکاری می‌کنند. جمهوری کره آموزش‌های لازم را برای کشورهای در حال توسعه مهیا می‌کند و دستورالعمل‌هایی برای ایجاد و به‌کارگیری تیم‌های پاسخ اضطراری تدوین شده‌اند.

حفاظت از شرکت‌های کوچک و متوسط و کاربران خانگی در مقابل حملات سایبری و ویروس‌ها به‌عنوان یک اولویت در نظر گرفته می‌شود و ابزارهایی برای این منظور ساخته شده‌اند. اطلاعاتی در مورد چگونگی استفاده امن از اینترنت، معضلات مربوط به ایمنی فناوری‌های بی‌سیم و نیز تبادل امن ایمیل‌ها فراهم شده است.

کاهش سوءاستفاده مجرمانه از اطلاعات از طریق به‌اشتراک‌گذاری اطلاعات، توسعه روال‌ها و قوانین کمک متقابل و دیگر اقدامات جهت حفاظت از بنگاه‌ها و شهروندان، همچنان برای گروه گروه

1- Pervasive Radio Frequency Identification
2- Asia-Pacific Economic Cooperation
3- Telecommunications and Information Working Group

کاری مخابرات و اطلاعات در سازمان همکاری‌های اقتصادی آسیا و اقیانوسیه یک اولویت خواهد بود. به‌عنوان قسمتی از برنامه کاری در معضلات امنیتی، این گروه در سال ۲۰۰۷ "راهنمای خط‌مشی و رویکرد فنی در مقابل بات‌نت" و کارگاه امنیت سایبری و زیرساخت اطلاعات حیاتی را تصویب کرد.

در سال ۲۰۰۹، "سومین سمینار سازمان همکاری‌های اقتصادی آسیا و اقیانوسیه پیرامون حفاظت از فضای سایبری برای دفاع بهتر از اقتصاد ما از طریق امنیت فناوری اطلاعات"، با تأیید گروه ضربت ضد تروریسم در سازمان همکاری‌های اقتصادی آسیا و اقیانوسیه (CTTF)[1] و گروه گروه کاری مخابرات و اطلاعات، در سئول پایتخت جمهوری کره، ۷ و ۸ سپتامبر ۲۰۱۱، با ۸۶ نماینده و سخنران از ۱۶ اقتصاد دنیا برگزار شد. میزبانی این سمینار با وزارت امور خارجه و بازرگانی، وزارت کشور و کمیسیون ارتباطات کره (KCC)[2] بود و حمایت از آن توسط سازمان اینترنت و امنیت کره (KISA)[3] انجام گرفت.

این سمینار فعالیتی در ادامه دو پروژه مشترک قبلی تأیید گروه ضربت ضد تروریسم- گروه کاری مخابرات و اطلاعات بود، با نام‌های "برنامه آموزشی سازمان همکاری‌های اقتصادی آسیا و اقیانوسیه برای امنیت سایبری تقویت شده در آسیای حوزه اقیانوس آرام" که از ۱۵ تا ۳۰ نوامبر ۲۰۰۷ در سئول برگزار شد و "سمینار سازمان همکاری‌های اقتصادی آسیا و اقیانوسیه درباره حفاظت از فضای سایبری در مقابل حملات و کاربردهای تروریستی" که ۲۷ و ۲۸ ژوئن ۲۰۰۸ در سئول برگزار گردید. سومین سمینار که بر نتایج برنامه آموزشی و اولین سمینار بنا نهاده شد، مقامات دولتی و متخصصان را از کشورهای عضو سازمان همکاری‌های اقتصادی آسیا و اقیانوسیه گرد هم آورد تا معضلات متنوع امنیت سایبری از جمله حفاظت از زیرساخت‌های حیاتی را در مقابل حملات تروریستی مورد بررسی قرار دهد.

فعالیت‌های امنیت اطلاعات اتحادیه بین‌المللی مخابرات[۴۰]

اتحادیه مخابرات بین‌الملل (ITU)[4] نهادی پیشرو در سازمان ملل، در زمینه فناوری اطلاعات و ارتباطات است. اتحادیه بین‌المللی مخابرات که در ژنو سوئیس مستقر شده است، ۱۹۱ دولت عضو و بیش از ۷۰۰ عضو بخش و مؤسسه وابسته دارد.

نقش اتحادیه بین‌المللی مخابرات در کمک به ارتباطات جهانی سه بخش اصلی را پوشش می‌دهد. بخش ارتباطات رادیویی (ITU-R)[5] بر مدیریت طیف فرکانس رادیویی بین‌الملل و منابع

1- APEC Counter-Terrorism Task Force (CTTF)
2- Korea Communications Commission
3- Korea Internet & Security Agency
4- International Telecommunication Union
5- International Telecommunication Union – Radiocommunication Sector

ماهواره‌ای تمرکز دارد. بخش استانداردسازی مخابرات (ITU-T)[1] بر استانداردسازی شبکه‌ها و خدمات اطلاعاتی- ارتباطی متمرکز می‌شود. بخش توسعه (ITU-D)[2] برای کمک به گسترش دسترسی مساوی، پایدار و در حد بضاعت به فناوری اطلاعات و ارتباطات، به‌عنوان وسیله‌ای برای ترغیب توسعه اقتصادی و اجتماعی بیشتر تأسیس شد. اتحادیه بین‌المللی مخابرات همچنین رویدادهای مرتبط با مخابرات را سازمان‌دهی کرده و سازمان قانون‌گذاری پیشرو اجلاس جهانی در مورد جامعه اطلاعاتی است.

یک نقش بنیادی اتحادیه بین‌المللی مخابرات به‌دنبال اجلاس جهانی در مورد جامعه اطلاعاتی ایجاد اطمینان و امنیت در استفاده از فناوری‌های اطلاعاتی و ارتباطی است. در اجلاس جهانی در مورد جامعه اطلاعاتی، رؤسای دولت‌ها و رهبران جهان، اتحادیه بین‌المللی مخابرات را عهده‌دار مسئولیت هماهنگ کردن تلاش‌های بین‌المللی در حوزه امنیت فضای سایبری کردند و این یعنی این اتحادیه تنها تسهیل‌کننده خط اقدام C.5، "ایجاد اطمینان و امنیت در استفاده از فناوری‌های اطلاعاتی و ارتباطی" است. امنیت سایبری یکی از مهم‌ترین حیطه‌های مورد تمرکز در بخش توسعه است.

حیطه‌های مورد تمرکز خط اقدام C.5 عبارتند از:

- ✓ حفاظت از زیرساخت‌های اطلاعاتی حیاتی
- ✓ ترویج فرهنگ جهانی امنیت سایبری
- ✓ مقابله با هرزنامه‌ها
- ✓ ظرفیت‌سازی مراقبت، هشداردهی و پاسخ در هنگام حادثه
- ✓ به اشتراک‌گذاری اطلاعات مربوط به رویکردهای ملی، اقدامات و دستورالعمل‌های مفید
- ✓ حفاظت از حریم خصوصی، داده‌ها و مصرف‌کننده

دستور کار امنیت سایبری سراسری (GCA)[3] چارچوبی در اتحادیه بین‌المللی مخابرات برای همکاری‌های بین‌المللی است که هدف آن ارائه راه‌حل‌هایی برای افزایش اطمینان و امنیت در جامعه اطلاعاتی است. امنیت سایبری سراسری دارای چهار رکن استراتژیک است: چارچوب قانونی، اقدامات فنی، ساختارهای سازمانی، ظرفیت‌سازی و همکاری‌های بین‌المللی. استراتژی‌ها از طریق این اهداف توضیح داده می‌شوند:

- ✓ توسعه مجموعه قوانینی نمونه برای جرائم سایبری که به‌طور جهانی قابل‌کاربرد بوده و با اقدامات قانونی ملی و منطقه‌ای موجود تعامل‌پذیری چندمحیطی داشته باشد.
- ✓ ایجاد ساختارها و خط‌مشی‌های سازمانی منطقه‌ای و ملی برای جرائم سایبری
- ✓ تدوین معیارهای امنیتی حداقلی پذیرفته شده و روش‌های اعتبارسنجی برای برنامه‌های کاربردی و سیستم‌های نرم‌افزاری

1- International Telecommunication Union – Telecommunication Standardization Sector
2- International Telecommunication Union – Development Sector
3- Global Cybersecurity Agenda

- ✓ ایجاد چارچوبی سراسری برای مراقبت، هشداردهی و پاسخ به حوادث برای تضمین هماهنگی اقدامات بین کشورها
- ✓ ایجاد و تأیید یک سیستم هویت دیجیتال سراسری و عام و نیز ساختارهای سازمانی ضروری برای تضمین شناسایی اطلاعات هویتی افراد در سراسر مرزهای جغرافیایی
- ✓ تدوین یک استراتژی سراسری برای تسهیل ظرفیت‌سازی‌های انسانی و سازمانی در جهت افزایش دانش و تخصص در میان بخش‌ها و در تمام حیطه‌های ذکر شده در بالا
- ✓ مشاوره در مورد چارچوب بالقوه برای یک استراتژی سراسری چند ذی‌نفعه جهت همکاری‌های بین‌المللی، گفت‌وگو و هماهنگی در تمام حیطه‌های ذکر شده در بالا

امنیت سایبری سراسری اقداماتی از قبیل حمایت آنلاین از فرزندان را از طریق مشارکت با IMPACT[1] و با پشتیبانی بازیگران پیشروی جهانی ترویج داده است.

ابتکار دیگر اتحادیه بین‌المللی مخابرات دروازه امنیت سایبری است که هدف آن فراهم آوردن یک منبع اطلاعاتی ساده و تعاملی در مورد اقدامات مرتبط با امنیت سایبری ملی و بین‌المللی می‌باشد. این منبع در دسترس شهروندان، دولت‌ها، بنگاه‌ها و سازمان‌های بین‌المللی قرار دارد. خدماتی که به‌وسیله این دروازه مهیا می‌شود شامل اشتراک اطلاعات، مراقبت و هشداردهی، حقوق و قانون‌گذاری، حریم خصوصی و حفاظت، استانداردهای صنعتی و راه‌حل‌ها است.

همچنین، بخش توسعه نظارت بر برنامه عملی امنیت سایبری اتحادیه بین‌المللی مخابرات را بر عهده دارد. این برنامه برای کمک به کشورها در جهت توسعه فناوری‌های لازم برای امنیت سطح بالای فضای سایبری تدوین شد. این برنامه در زمینه‌های زیر کمک ارائه می‌کند:

- ✓ پایه‌گذاری استراتژی‌ها و ظرفیت‌های ملی برای امنیت سایبری و حفاظت از زیرساخت‌های اطلاعاتی حیاتی
- ✓ تدوین قوانین مناسب برای جرائم سایبری و سازوکارهای اعمال آن‌ها
- ✓ ایجاد توانایی‌های مراقبت، هشداردهی و پاسخ به حوادث
- ✓ مقابله با هرزنامه‌ها و تهدیدهای مرتبط
- ✓ پر کردن شکاف استانداردسازی مرتبط با امنیت بین کشورهای توسعه یافته و در حال توسعه
- ✓ تدوین کتاب راهنمای امنیت سایبری اتحادیه بین‌المللی مخابرات و حفاظت از زیرساخت‌های اطلاعاتی حیاتی، پایگاه داده تماس‌ها و انتشار فهرست رجال
- ✓ تعیین شاخص‌های امنیت سایبری
- ✓ ترویج همکاری‌های منطقه‌ای

1- International Multilateral Partnership Against Cyber Threats

- ✓ به‌اشتراک‌گذاری اطلاعات و پشتیبانی از دروازه امنیت سایبری اتحادیه بین‌المللی مخابرات
- ✓ گسترش و ترویج فعالیت‌های مرتبط

دیگر فعالیت‌های بخش توسعه که مربوط به امنیت فضای سایبری هستند عبارتند از: فعالیت‌های مشترک با StopSpamAlliance.org؛ فعالیت‌های منطقه‌ای ظرفیت‌سازی در قانون‌گذاری و اعمال قانون برای فضای سایبری؛ توسعه و توزیع منابع و جعبه ابزارها از قبیل جعبه‌ابزار مقابله با بات‌نت‌ها[۴۱]، جعبه‌ابزاری برای قانون‌گذاری در مورد جرائم سایبری در کشورهای در حال توسعه، جعبه ابزاری برای خودارزیابی امنیت فضای سایبری ملی[۴۲] و انتشار کتاب و مقالات در زمینه امنیت فضای سایبری/جرائم سایبری[۴۳].

بخش استانداردسازی مخابرات نیز از طریق تدوین بیش از ۷۰ استاندارد مرتبط با امنیت[1] به حوزه امنیت سایبری کمک می‌کند. اخیراً در یک سمپوزیوم امنیت فضای سایبری، شرکت‌کنندگان از بخش استانداردسازی مخابرات خواستند به کارش در این حوزه شتاب ببخشد. در پاسخ، بخش استانداردسازی مخابرات اکنون تأکید بیشتری بر تدوین استانداردهای امنیتی قائل است. برای کمک به این فرآیند، بخش استانداردسازی مخابرات "نقشه راه استانداردهای امنیت فناوری اطلاعات و ارتباطات" را تدوین کرد که اطلاعاتی پیرامون استانداردهای موجود، استانداردهای تحت تدوین و حیطه‌های لازم برای استانداردسازی در آینده را در یکجا گرد آورده است[۴۴].

کار استانداردسازی به‌وسیله گروه‌های مطالعات فنی انجام می‌شود که در آن نمایندگان اعضای بخش استانداردسازی مخابرات توصیه‌ها (استانداردها) را برای حوزه‌های مختلف مخابرات بین‌الملل تدوین می‌کنند. این گروه کارش را عمدتاً به شکل پرسش‌های مطالعاتی پیش می‌برد. هر پرسش به مطالعات فنی در یک حیطه خاص از استانداردسازی مخابرات می‌پردازد.

در بخش بخش استانداردسازی مخابرات، گروه مطالعه ۱۷ (SG17)[۴۵] فعالیت‌های مرتبط با امنیت را در سطح همه گروه‌های مطالعاتی هماهنگ می‌کند.

SG17 مسئولیت مطالعات مربوط به امنیت از جمله امنیت سایبری، مقابله با هرزنامه‌ها و مدیریت هویت را به عهده دارد. همچنین، این گروه مسئول کاربرد ارتباطات سیستم‌های باز ار جمله شناسه‌های دایرکتوری و شئ و زبان‌های فنی، روش‌های استفاده از آن‌ها و دیگر معضلات مرتبط با جنبه‌های نرم‌افزاریِ سیستم‌های مخابراتی است.

ساختار SG17 برای دوره مطالعاتی ۲۰۰۹-۲۰۱۲ به قرار زیر است:

- ✓ تیم کاری ۱. امنیت شبکه و اطلاعات
  - پرسش ۱- پروژه امنیت سیستم‌های مخابراتی
  - پرسش ۲- معماری و چارچوب امنیتی
  - پرسش ۳- مدیریت امنیت اطلاعات مخابراتی

1- ITU-T Recommendations

- پرسش ۴- امنیت سایبری
- پرسش ۵- مبارزه با هرزنامه به‌وسیله ابزارهای فنی

✓ تیم کاری ۲. امنیت برنامه کاربردی

- پرسش ۶- جنبه‌های امنیتی خدمات مخابراتی همه جا حاضر
- پرسش ۷- خدمات کاربردی امن
- پرسش ۸- امنیت معماری سرویس‌گرا
- پرسش ۹- بیومتریک‌های راه دور

✓ تیم کاری ۳. مدیریت هویت و زبان‌ها

- پرسش ۱۰- معماری‌ها و سازوکارهای مدیریت هویت
- پرسش ۱۱- سرویس‌های دایرکتوری، سیستم‌های دایرکتوری و گواهی‌های ویژگی یا کلید عمومی
- پرسش ۱۲- نمادگذاری دستوری انتزاعی یک[1] (ANS.1)، شناسه‌های شئ و ثبت‌نام‌های مربوطه
- پرسش ۱۳- زبان‌های رسمی و نرم‌افزارهای مخابراتی
- پرسش ۱۴- آزمون زبان‌ها، روش‌ها و چارچوب
- پرسش ۱۵- اتصال سیستم‌های باز[2]

یک مرجع مهم برای استانداردهای امنیتی که امروزه مورداستفاده قرار می‌گیرند، توصیه‌های X.509 است که در مورد احراز هویت الکترونیکی در شبکه‌های عمومی، توسط بخش بخش استانداردسازی مخابرات تهیه شده است. X.509 برای طراحی کاربردهای مرتبط با زیرساخت کلید عمومی به‌کار می‌رود و در طیف وسیعی از کاربردها، از ایمن‌سازی اتصال بین مرورگرها و سرورها در وب تا تهیه امضای دیجیتال که تراکنش‌های تجارت الکترونیکی را ممکن می‌کنند، مورداستفاده قرار می‌گیرد. دیگر دستاورد SG17 توصیه‌های X.805 است که به اپراتورها و شرکت‌های فعال در زمینه شبکه‌های مخابراتی این قابلیت را می‌دهد که یک توصیف معماری انتها به انتها را با یک دیدگاه امنیتی فراهم کنند[۴۶].

همچنین، SG 17 محلی برای مطالعه زبان‌های فنی و فنون توصیفی است. مثالی از این دسته، زبان رسمی ASN.1 است که مؤلفه‌ای مهم برای تعیین مشخصات پروتکل یا طراحی سیستم است. ASN.1 قسمتی بسیار مهم از شبکه‌های امروزی است. به‌عنوان مثال، ASN.1 در سیستم‌های ارسال سیگنال برای بیشتر تماس‌های تلفنی، رهیگری بسته‌ها، راستی‌آزمایی کارت‌های الکترونیکی، گواهی‌های دیجیتال و در بسیاری از برنامه‌های نرم‌افزاری مورداستفاده به‌کار برده می‌شود. فعالیت‌های

1- Abstract Syntax Notation One (ANS.1)
2- Open Systems Interconnection

کنونی معطوف به پیشرفت به‌سوی توسعه مشخصات زبانِ مدل‌سازی یکپارچه برای زبان‌های بخش استانداردسازی مخابرات است[۴۷].

فعالیت‌های امنیت اطلاعات ISO/IEC

سیستم مدیریت امنیت اطلاعات (ISMS)[1] همان‌طور که از نامش پیداست، سیستمی برای مدیریت امنیت اطلاعات است. این سیستم از فرآیندها و زیرسیستم‌هایی تشکیل شده است که محرمانگی، صحت و دسترسی‌پذیری دارایی‌های امنیتی را در عین کاهش ریسک‌های امنیتی تضمین می‌کند. محبوبیت گواهی‌نامه سیستم مدیریت امنیت اطلاعات در سراسر دنیا به‌سرعت در حال افزایش است. سال ۲۰۰۵، به‌دلیل انتشار دو سند، به نقطه عطفی در تاریخ سیستم مدیریت امنیت اطلاعات استاندارد شده در سطح بین‌الملل تبدیل شد: IS 27001 نیازمندی‌ها ایجاد یک سیستم سیستم مدیریت امنیت اطلاعات را بیان می‌کند، IS 17799:2000 که با عنوان IS 17799:2005 منتشر شد، اقدامات کنترلی اساسی را برای پیاده‌سازی یک سیستم مدیریت امنیت اطلاعات قید می‌کند.

BS 7799 استاندارد عملاً رایج سیستم مدیریت امنیت اطلاعات است که در ابتدا به‌وسیله مؤسسه استانداردهای بریتانیا (BSI)[2] در سال ۱۹۹۵، به‌عنوان آیین‌نامه مدیریت امنیت اطلاعات تدوین شد. در سال ۱۹۹۸، هنگامی که مشخصه نیازمندی‌ها بر اساس این استاندارد تدوین شد، "آیین‌نامه مدیریت امنیت اطلاعات" به *قسمت ۱* تبدیل گردید و مشخصه نیازمندی‌ها به *قسمت ۲* تغییر یافت. قسمت ۱ اقدامات کنترلی را برای مدیریت امنیت اطلاعات تعیین می‌کند، در حالی‌که قسمت ۲ نیازمندی‌ها برقراری یک سیستم را بیان کرده و فرآیندهای امنیت اطلاعات (حلقه برنامه‌ریزی، اجرا، بررسی، اقدام) را برای بهبود مستمر مدیریت ریسک توصیف می‌کند.

قسمت ۱ با نام IS 17799 به‌وسیله ISO/IEC JTC 1/SC27 WG1 در سال ۲۰۰۰ تدوین گردید. از آن موقع تا کنون، IS 17799 مورد بازبینی و اصلاح قرار گرفته است (با بیش از ۲۰۰۰ نظر). نسخه نهایی در نوامبر سال ۲۰۰۵ در مجموعه استانداردهای بین‌المللی ثبت شد. IS 17799:2000 تعداد ۱۲۶ اقدام کنترلی را در ۱۰ حوزه مقرر می‌کند. IS 17799 که در سال ۲۰۰۵ اصلاح شد، ۱۱ حوزه کنترل مدیریتی و ۱۳۳ اقدام کنترلی را در دسترس قرار می‌دهد.

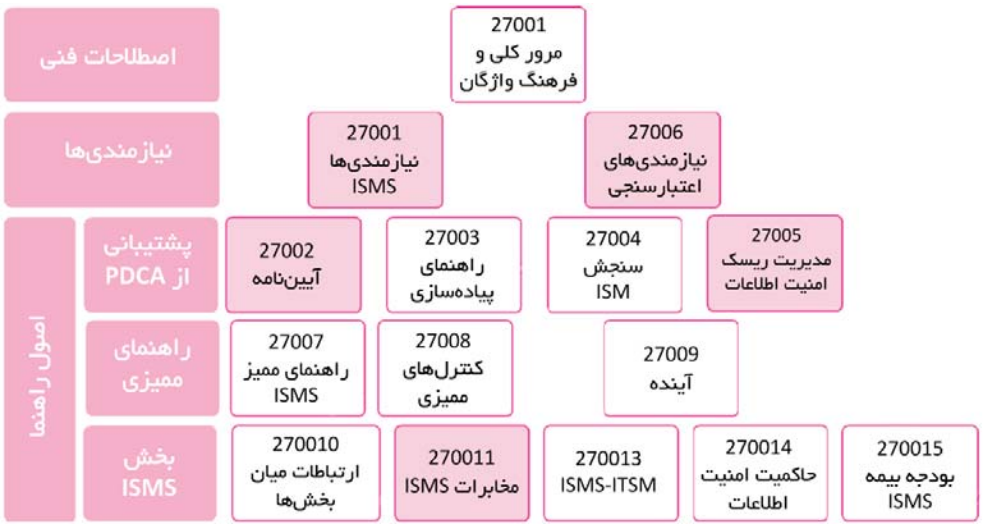
قسمت ۲ از BS 7799 که در سال ۱۹۹۹ تدوین شد، به‌عنوان استانداردی برای گواهی‌نامه سیستم مدیریت امنیت اطلاعات مورداستفاده قرار گرفته است. این استاندارد در سپتامبر ۲۰۰۲ اصلاح شد تا با استانداردهای ISO 9001 و ISO 14001 هم‌راستا باشد. سازمان استانداردسازی بین‌الملل (ISO)، برای مواجهه با تقاضای سیستم مدیریت امنیت اطلاعات استاندارد شده در سطح بین‌المللی، استاندارد BS 7799 Part 2:2002 را از طریق روش پیگیری سریع به‌کار گرفت و با کمی تصحیح در

1- Information Security Management System
2- British Standards Institution

زمانی کوتاه، آن را به‌عنوان استاندارد بین‌المللی ISO 27001 ثبت کرد. تغییرات بارزی که ایجاد شد شامل افزودن محتوایی در مورد اثربخشی و اصلاح ضمیمه بود.

از آنجا که دو سند مهم مربوط به سیستم مدیریت امنیت اطلاعات در سطح بین‌المللی استاندارد شدند، خانواده‌ای از استانداردهای امنیت اطلاعات، تحت الگویی با شماره سریال ۲۷,۰۰۰ پدید آمده است که شبیه به دیگر سیستم‌هالی مدیریتی است (کیفیت کسب‌وکار: سری ۹,۰۰۰، مدیریت محیطی: سری ۱۴,۰۰۰). IS 27001، یعنی نسخه اصلاح شده IS 17799:2005، در بردارنده نیازمندی‌های برقراری یک سیستم مدیریت امنیت اطلاعات است و IS1 7799:2005 که شامل اقدامات کنترلی اساسی برای پیاده‌سازی سیستم مدیریت امنیت اطلاعات است، از سال ۲۰۰۷ به IS 27002 تغییر یافته است. راهنمای پیاده‌سازی یک سیستم مدیریت امنیت اطلاعات، استانداردی برای مدیریت ریسک امنیت اطلاعات و سنجش مدیریت امنیت اطلاعات که به‌وسیله JTC1 SC27 تدوین شدند، در این مجموعه وجود دارند.

شکل ۵-۳ خانواده استانداردهای مربوط به سیستم مدیریت امنیت اطلاعات را نشان می‌دهد. فعالیت‌های مرتبط با گواهی‌نامه سیستم مدیریت امنیت اطلاعات در حال شتاب گرفتن هستند و انتظار می‌رود که استانداردها یا دستورالعمل‌های سیستم مدیریت امنیت اطلاعات که برای صنایع خاص مناسب هستند بر اساس سیستم مدیریت امنیت اطلاعات رایج در سیستم‌های عمومی تدوین گردند. مثالی از این موارد تلاشی در جهت توسعه دستورالعمل‌های سیستم مدیریت امنیت اطلاعات است که منعکس‌کننده مشخصه‌های صنعت ارتباطات باشند.



شکل ۵-۳ خانواده ISO/IEC 27000

پرسش‌هایی برای تفکر

کدام‌یک از فعالیت‌های امنیت اطلاعات که به‌وسیله سازمان‌های بین‌المللی رهبری می‌شود، تاکنون در کشور شما به‌کار گرفته شده یا در حال به‌کارگیری است؟ این فعالیت‌ها چگونه پیاده‌سازی می‌شوند؟

خودآزمایی

۱- شباهت‌های میان فعالیت‌های امنیت اطلاعات که به‌وسیله کشورهای ذکر شده در این بخش انجام می‌شوند چیست؟ این فعالیت‌ها چه تفاوت‌هایی با هم دارند؟

۲- اولویت‌های امنیت اطلاعات در سازمان‌های بین‌المللی ذکر شده در این بخش چیست؟

فصل چهارم

روش‌شناسی امنیت اطلاعات

هدف این فصل توصیف روش‌شناسی اجرایی، فیزیکی و فنی در امنیت اطلاعات است که در سطح بین‌المللی مورداستفاده قرار می‌گیرند.

٤-١ جنبه‌های مختلف امنیت اطلاعات

هدف از روش‌شناسی امنیت اطلاعات به حداقل رسانیدن خسارات و حفظ تداوم کسب‌وکار، با در نظر داشتن تمام آسیب‌پذیری‌ها و ریسک‌های مرتبط با دارایی‌های اطلاعاتی است. برای تضمین تداوم کسب‌وکار، روش‌شناسی امنیت اطلاعات به‌دنبال تأمین محرمانگی، صحت و دسترسی‌پذیری دارایی‌های اطلاعاتی داخلی هستند. این هدف نیازمند کاربرد روش‌های ارزیابی ریسک و اقدامات کنترلی است. اساساً، چیزی که موردنیاز است طرحی خوب است که جنبه‌های اجرایی، فیزیکی و فنی امنیت اطلاعات را پوشش بدهد.

جنبه اجرایی

سیستم‌های مدیریت امنیت اطلاعات بسیاری وجود دارند که بر جنبه اجرایی تمرکز می‌کنند. ISO/IEC27001 یکی از رایج‌ترین استانداردهای مورداستفاده است.

ISO/IEC27001، استاندارد بین‌المللی سیستم مدیریت امنیت اطلاعات، بر اساس BS7799 است که توسط BSI تدوین شده است. BS7799 نیازمندی‌های پیاده‌سازی و مدیریت یک سیستم مدیریت امنیت اطلاعات را مشخص کرده و استانداردهای رایج به کار رفته در استانداردهای امنیتی سازمان‌های مختلف و مدیریت امنیتی اثربخش را تعیین می‌کند. قسمت ۱ از BS7799 فعالیت‌های امنیتی لازم را بر اساس بهترین شیوه‌ها در فعالیت‌های امنیتی سازمان‌ها توصیف می‌کند. قسمت ۲ که تبدیل به ISO/IEC27001 کنونی شد، حداقل شرایط موردنیاز را برای عملکرد سیستم مدیریت امنیت اطلاعات و ارزیابی فعالیت‌های امنیتی توصیه می‌کند. فعالیت‌های امنیتی در ISO/IEC27001 متشکل از ۱۳۳ اقدام کنترلی و ۱۱ حوزه است (جدول ۱-۴ را مشاهده کنید).

جدول ۱-۴ اقدامات کنترلی در ISO/IEC27001

حوزه	اقدامات
A5	خط‌مشی امنیتی
A6	سازمان‌دهی امنیت اطلاعات
A7	مدیریت دارایی‌ها
A8	امنیت منابع انسانی
A9	امنیت فیزیکی و محیطی
A10	مدیریت ارتباطات و عملیات
A11	کنترل دسترسی
A12	تملک سیستم‌های اطلاعاتی، توسعه و نگهداری
A13	مدیریت حوادث امنیت اطلاعات
A14	مدیریت تداوم کسب‌وکار
A15	پیروی و مطابقت

استاندارد ISO/IEC27001 مدل فرآیند PDCA[1] یعنی برنامه‌ریزی، اجرا، بررسی و اقدام را به‌کار می‌گیرد که برای ساختاردهی به همه فرآیندهای سیستم مدیریت امنیت اطلاعات استفاده می‌شود. در ISO/IEC27001، تمام مدارک ارزیابی سیستم مدیریت امنیت اطلاعات باید مستند شوند؛ گواهی‌نامه باید هر شش ماه از خارج مورد ممیزی قرار گیرد؛ و کل فرآیند باید بعد از سه سال مجدداً تکرار شود تا سیستم مدیریت امنیت اطلاعات به‌طور مستمر مدیریت گردد.

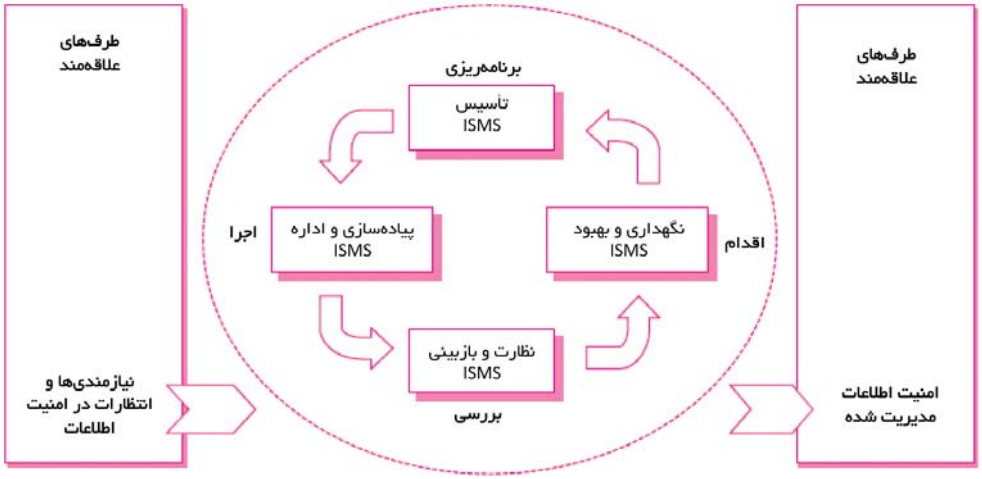
اقدامات کنترلی امنیتی را باید با توجه به نیازمندی‌های امنیتی برنامه‌ریزی کرد. همه منابع انسانی، از جمله تأمین‌کنندگان، پیمان‌کاران، مشتریان و متخصصان خارجی، باید در این فعالیت‌ها شرکت کنند. استقرار نیازمندی‌های امنیتی مبتنی بر این سه عامل است:

- ✓ برآورد ریسک
- ✓ نیازمندی‌های حقوقی و مفاد قرارداد
- ✓ فرآیندهای اطلاعاتی برای عملکرد سازمان

به فرآیند سنجش سطح کنونی امنیت اطلاعات و تعیین جهت آینده در امنیت اطلاعات **تحلیل شکاف**[2] گویند. نتایج تحلیل شکاف از پاسخ‌های مالکان دارایی به ۱۳۳ اقدام کنترلی و ۱۱ حوزه

1- Plan-Do-Check-Act
2- Gap Analysis

استنتاج می‌شود. هنگامی‌که حیطه‌های مختلف از طریق تحلیل شکاف شناسایی شدند، اقدامات کنترلی مناسب برای هر حیطه را می‌توان معین کرد.



شکل ۱-۴ مدل فرآیند برنامه‌ریزی، اجرا، بررسی و اقدام در فرآیندهای سیستم مدیریت امنیت اطلاعات

منبع: ISO/IEC JTC 1/SC 27.

برآورد ریسک[1] به دو بخش برآورد ارزش دارایی و برآورد تهدیدها و آسیب‌پذیری‌ها تقسیم می‌شود. برآورد ارزش دارایی، ارزش‌گذاری کمّی بر دارایی‌های اطلاعاتی است. برآورد تهدید شامل درجه‌بندی تهدیدهای مربوط به محرمانگی، صحت و دسترسی‌پذیری اطلاعات است. مثال زیر محاسبات لازم در برآورد ریسک را نشان می‌دهد:

نام دارایی	ارزش دارایی	تهدید			آسیب‌پذیری			ریسک		
		A	I	C	A	I	C	A	I	C
دارایی شماره ۱	۲	۱	۳	۳	۱	۱	۳	۴	۶	۸

- ✓ ارزش دارایی + تهدید + آسیب‌پذیری = ریسک
- ✓ محرمانگی: ارزش دارایی (۲) + تهدید (۳) + آسیب‌پذیری (۳) = ریسک (۸)
- ✓ صحت: ارزش دارایی (۲) + تهدید (۳) + آسیب‌پذیری (۱) = ریسک (۶)

1- Risk Assessment

- ✓ دسترسی‌پذیری: ارزش دارایی (۲) + تهدید (۱) + آسیب‌پذیری (۱) = ریسک (۴)

کاربرد اقدامات کنترلی[1]: مقدار هر ریسک با توجه به نتیجه برآورد ریسک متفاوت خواهد بود. به‌منظور به‌کارگیری اقدامات کنترلی برای دارایی‌هایی با ارزش متفاوت، تصمیم‌گیری لازم است. ریسک‌ها باید با توجه به معیار درجه اطمینان[2] به دو دسته ریسک‌های قابل‌قبول و ریسک‌های غیرقابل‌قبول تقسیم گردند. برای دارایی‌هایی که ریسک غیرقابل‌قبول دارند اقدامات کنترلی باید به‌کار گرفته شوند. این اقدامات بر اساس اقدامات کنترلی ISO/IEC به‌کار گرفته می‌شوند، اما اثربخش‌تر آن است که اقدامات کنترلی با توجه به حالت واقعی سازمان اجرا گردند.

هر کشور یک نهاد تصدیق و تأیید برای ISO/IEC27001 دارد. جدول ۲-۴ تعداد گواهی‌نامه‌ها را برحسب کشورها فهرست کرده است:

جدول ۲-۴ تعداد گواهی‌نامه‌های سیستم مدیریت امنیت اطلاعات برای هر کشور

کشور	تعداد گواهی‌نامه‌ها	کشور	تعداد گواهی‌نامه‌ها	کشور	تعداد گواهی‌نامه‌ها
ژاپن	۳۸۶۲	بلغارستان	۱۸	ماکائو	۳
هند	۵۲۶	کرواسی	۱۷	قطر	۳
چین	۴۹۲	هلند	۱۶	آلبانی	۲
انگلستان	۴۷۷	فیلیپین	۱۵	آرژانتین	۲
تایوان	۴۳۱	ایران	۱۴	بلژیک	۲
آلمان	۱۷۴	پاکستان	۱۴	بوسنی و هرزگوین	۲
جمهوری کره	۱۰۶	ویتنام	۱۴	قبرس	۲
جمهوری چک	۱۰۳	ایسلند	۱۳	جزیره مَن	۲
ایالات متحده	۱۰۱	اندونزی	۱۳	قزاقستان	۲
اسپانیا	۷۵	عربستان سعودی	۱۳	لوکزامبورگ	۲
مجارستان	۶۸	کلمبیا	۱۱	مقدونیه	۲
ایتالیا	۶۸	کویت	۱۱	مالت	۲
لهستان	۵۸	نروژ	۱۰	اوکراین	۲

1- Application of Control
2- Degree of Assurance

مالزی	۵۵	پرتغال	۱۰	موریس	۲
ایرلند	۴۲	فدراسیون روسیه	۱۰	ارمنستان	۱
تایلند	۴۱	سوئد	۱۰	بنگلادش	۱
اتریش	۳۹	کانادا	۹	بلاروس	۱
رومانی	۳۵	سوئیس	۹	دانمارک	۱
هنگ‌کنگ	۳۲	بحرین	۸	اکوادور	۱
یونان	۳۰	مصر	۵	جرزی	۱
استرالیا	۲۹	عمان	۵	قرقیزستان	۱
سنگاپور	۲۹	پرو	۵	لبنان	۱
مکزیک	۲۷	آفریقای جنوبی	۵	مولداوی	۱
فرانسه	۲۶	سری‌لانکا	۵	نیوزیلند	۱
ترکیه	۲۴	جمهوری دومینیکن	۴	سودان	۱
برزیل	۲۳	لیتوانی	۴	اروگوئه	۱
اسلواکی	۲۳	مراکش	۴	یمن	۱
امارت متحده عربی	۲۰	شیلی	۳		
اسلوونی	۱۹	جبل‌الطارق	۳	**مجموع**	**۷۳۴۶**

*توجه: تعداد گواهی‌نامه‌های نشان داده شده مربوط به ۱۹ سپتامبر ۲۰۱۱ است.

منبع: International Register of ISMS Certificates, "Number of Certificates per Country", ISMS International User Group Ltd., http://www.iso27001certificates.com.

جنبه فیزیکی

در حال حاضر هیچ سیستم مدیریت امنیت اطلاعات فیزیکی بین‌المللی وجود ندارد. در اینجا سند شماره ۴۲۶ سازمان فدرال مدیریت وقایع اضطراری (FEMA)[1] که استانداردی برای سیستم مدیریت امنیت اطلاعات فیزیکی در ایالات متحده است و بسیاری از کشورها از آن به‌عنوان یک روش‌شناسی استفاده می‌کنند توصیف می‌گردد.

FEMA 426[۴۸] رهنمودهایی را برای حفاظت از ساختمان‌ها در مقابل حملات تروریستی ارائه می‌کند. این سند معطوف به "جامعه علمی معماران و مهندسان ساختمان در جهت کاهش

1- Federal Emergency Management Agency

خسارات فیزیکی ناشی از حملات تروریستی به ساختمان‌ها، زیرساخت‌های مرتبط و مردم"[۴۹] است. مجموعه‌ای از رهنمودهای مرتبط با نام FEMA 427 ("کتاب راهنمای پایه برای طراحی ساختمان‌های تجاری در جهت کاهش حملات تروریستی")، FEMA 428 ("کتاب راهنمای پایه برای طراحی پروژه‌های مدرسه امن در هنگام حملات تروریستی")، FEMA 429 ("کتاب راهنمای پایه برای بیمه، منابع مالی و مقررات برای مدیریت ریسک تروریسم در ساختمان‌ها")، FEMA 430 (معمار) و FEMA 438 (مسیر) وجود دارند.

FEMA 426 مستقیماً به امنیت اطلاعات مربوط نمی‌شود، اما می‌تواند از نشت، از دست رفتن یا خرابی اطلاعات به‌خاطر حملات فیزیکی در ساختمان‌ها جلوگیری کند. FEMA 426، به‌ویژه به‌طور تنگاتنگ مرتبط با طرح تداوم کسب‌وکار است که جزئی از امنیت اجرایی است. با ملاحظه FEMA 426 جنبه فیزیکی طرح تداوم کسب‌وکار را می‌توان محافظت کرد.

جنبه فنی

برای جنبه‌های فنی نیز هیچ سیستم مدیریت امنیت اطلاعاتی‌ای وجود ندارد. در عوض، می‌توان از استانداردهای ارزیابی مشترک رایج بین‌المللی از قبیل گواهی معیارهای مشترک (CC)[1] استفاده کرد.

گواهی معیارهای مشترک [۵۰]

گواهی معیارهای مشترک دارای ریشه‌های تجاری است. این گواهی برای برطرف کردن نگرانی‌ها در مورد تفاوت در سطوح امنیتی محصولات فناوری اطلاعات از کشورهای مختلف تهیه شد. استاندارد بین‌المللی برای ارزیابی محصولات فناوری اطلاعات به‌وسیله کانادا، فرانسه، آلمان، انگلستان و ایالات متحده تدوین شد.

معیارهای مشترک مخصوصاً نیازمندی‌های امنیت فناوری اطلاعات را برای یک محصول یا سیستم، تحت دسته‌های مجزای نیازمندی‌های کارکردی و نیازمندی‌های تضمینی ارائه می‌کند. نیازمندی‌های کارکردی معیارهای مشترک رفتارهای امنیتی مطلوب را تعریف می‌کند. نیازمندی‌های تضمینی مبنای حصول اطمینان از اثربخشی اقدامات امنیتی و اجرای صحیح آن‌هاست. کارکردهای امنیتی معیارهای مشترک از ۱۳۴ جزء از ۱۱ کلاسِ درست شده از ۶۵ خانواده تشکیل شده است. نیازمندی‌های تضمینی دارای ۸۱ جزء از ۸ کلاس درست شده از ۳۸ خانواده است.

1- Common Criteria

نیازمندی‌های کارکردی امنیتی (SFR)[1]: این نیازمندی‌ها تمام عملکردهای امنیتی را برای *هدف مورد ارزیابی* مشخص می‌کند. جدول ۳-۴ کلاس عملکردهای امنیتی موجود در نیازمندی‌های کارکردی امنیتی را نشان می‌دهد.

جدول ۳-۴ ترکیب کلاس‌ها در نیازمندی‌های کارکردی امنیتی

کلاس‌ها		جزئیات
FAU	ممیزی امنیتی	به وظایفی اشاره دارد که شامل حفاظت از داده‌های ممیزی، فرمت ثبت و گزینش رویدادها و نیز ابزارهای تحلیلی، هشدار درباره نقض و تحلیلی بلادرنگ است.
FCO	ارتباطات	نیازمندی‌هایی که به‌طور ویژه موردتوجه هدف مورد ارزیابی هستند و برای انتقال اطلاعات استفاده می‌شوند.
FCS	پشتیبانی از رمزنگاری	کاربرد مدیریت کلید رمزنگاری و عملیات رمزنگاری را تعیین می‌کند.
FDP	حفاظت از داده‌های کاربر	نیازمندی‌های مربوط به حفاظت از داده‌های کاربر را مشخص می‌کند.
FIA	شناسایی و احراز هویت	نیازمندی‌ها عملکردی را برای بنا کردن و وارسی هویت مورد ادعای یک کاربر تعیین می‌کند.
FMT	مدیریت امنیتی	مدیریت چندین جنبه از وظایف امنیتی مربوط به هدف مورد ارزیابی را مشخص می‌کند: صفات امنیتی، داده‌ها و وظایف مربوطه
FPR	حریم خصوصی	نیازمندی‌هایی را که می‌توان برای برآوردن نیازهای مربوط به حریم خصوصی کاربران مقرر کرد، توصیف می‌کند، در حالی‌که همچنان اجازه انعطاف‌پذیری را تا حد ممکن به سیستم می‌دهد تا کنترل کافی بر عملیات سیستم داشته باشد.
FPT	حفاظت از کارکردهای امنیتی	حاوی خانواده‌هایی از نیازمندی‌های عملکردی است که مربوط به صحت و مدیریت سازوکارهایی می‌شود که وظایف امنیتی مربوط به هدف مورد ارزیابی و صحت داده‌های آن‌ها را تشکیل می‌دهد.
FRU	بهره‌برداری از منابع	حاوی دسترسی‌پذیری منابع موردنیاز از قبیل قابلیت پردازشی و/یا ظرفیت ذخیره‌سازی است.
FTA	دسترسی به TOE	نیازمندی‌های کارکردی مربوط به کنترل برقراری یک جلسه کاربر را مشخص می‌کند.
FTP	مسیرها/کانال‌های	نیازمندی‌های یک مسیر ارتباطی مورد اعتماد را بین کاربران و کارکردهای

1-Security Functional Requirement

	مورد اعتماد	امنیتی مشخص می‌کند.

منبع: Common Criteria, Common Criteria for Information Technology Security Evaluation, July 2009, CCMB-2009-07-001.

اجزای تضمین امنیت (SACs)[1]: فلسفه معیارهای مشترک نیازمند بیان دقیق تهدیدهای امنیتی و تعهد خط‌مشی‌های امنیتی سازمان‌ها از طریق اقدامات امنیتی مناسب و کافی است. اقداماتی که به‌کار گرفته می‌شوند باید به شناسایی آسیب‌پذیری‌ها کمک کرده، احتمال بهره‌برداری از آن‌ها را کاهش داده و میزان خسارت وارده در صورت بهره‌برداری از یک آسیب‌پذیری را تقلیل دهند[۵۱]. جدول ۴-۴ فهرست کلاس‌های مشمول در اجزای تضمین امنیت را نشان می‌دهد.

جدول ۴-۴ ترکیب کلاس‌ها در اجزای تضمین امنیت

کلاس‌ها		جزئیات
APE	ارزیابی مشخصات حفاظتی	این کلاس لازم است تا نشان دهد که مشخصات حفاظتی صحیح و به‌طور داخلی سازگار هستند و اگر این مشخصات بر مبنای یک یا چند مشخصه حفاظتی یا بر بسته‌ها باشند، مشخصات حفاظتی نمونه‌سازی صحیحی از این مشخصات و بسته‌ها هستند.
ASE	ارزیابی هدف امنیتی	این کلاس موردنیاز است تا نشان دهد که هدف امنیتی صحیح و از لحاظ داخلی سازگار است و اگر هدف امنیتی بر اساس یک یا چند مشخصه حفاظتی یا بسته‌هایی باشد، هدف امنیتی نمونه‌سازی صحیحی از این مشخصات و بسته‌ها است.
ADV	توسعه	این کلاس در مورد هدف مورد ارزیابی اطلاعات فراهم می‌کند. دانشی که به‌دست می‌آید به‌عنوان مبنایی برای اجرای تحلیل آسیب‌پذیری و آزمایش بر اساس هدف مورد ارزیابی استفاده می‌شود، همان‌طور که در کلاس‌های ATE و AVA توصیف می‌شود.
AGD	مستندات راهنما	برای آماده‌سازی و عملیات امن هدف مورد ارزیابی، ضروری است که همه جنبه‌های مرتبط با اداره امن هدف مورد ارزیابی را توصیف کنیم. این کلاس همچنین به‌احتمال پیکربندی یا اداره سهواً اشتباهِ هدف مورد ارزیابی می‌پردازد.
ALC	پشتیبانی از چرخه حیات	در چرخه حیات محصول که در برگیرنده قابلیت‌های مدیریت پیکربندی، دامنه مدیریت پیکربندی، تحویل، امنیت توسعه، ترمیم خطا، تعریف چرخه حیات،

1- Security assurance components

		ابزارها و تکنیک‌ها است، تمیز داده می‌شود که هدف مورد ارزیابی تحت مسئولیت سازنده قرار دارد یا کاربر.
ATE	آزمایش‌ها	تأکید در این کلاس بر تأیید این موضوع است که کارکردهای امنیتی درباره هدف مورد ارزیابی با توجه به مشخصات طراحی عمل می‌کند یا خیر؟ این کلاس به آزمون نفوذ نمی‌پردازد.
AVA	برآورد آسیب‌پذیری	فعالیت برآورد آسیب‌پذیری در توسعه و عملیات مربوط به هدف مورد ارزیابی آسیب‌پذیری‌های مختلفی را پوشش می‌دهد.
ACO	ترکیب	نیازمندی‌های تضمینی را مشخص می‌کند که برای حصول اطمینان از اینکه یک هدف مورد ارزیابی تشکیل شده در هنگامی‌که بر کارکردهای امنیتی مهیا شده به‌وسیله مؤلفه‌های نرم‌افزاری، لخت‌افزاری[1] یا سخت‌افزاریِ ارزیابی شده متکی است، به‌طور امن عمل می‌کند.

روش ارزیابی معیارهای مشترک

۱- **ارزیابی مشخصات حفاظتی (APE):** مشخصات حفاظتی مجموعه‌ای از نیازمندی‌های امنیتی مستقل از اجرا را برای دسته‌هایی از اهداف مورد ارزیابی توصیف می‌کند و شامل بیان یک مسئله امنیتی است که محصول پیرو قصد حل آن را دارد. این مشخصات نیازمندی‌های کارکردی و تضمینی معیارهای مشترک را تعیین می‌کند و توجیهی برای اجزای کارکردی و تضمینی گزینش شده مهیا می‌کند. این مشخصات معمولاً توسط مصرف‌کننده یا جامعه‌ای از مصرف‌کنندگان برای نیازمندی‌های امنیتی فناوری اطلاعات ایجاد می‌شود.

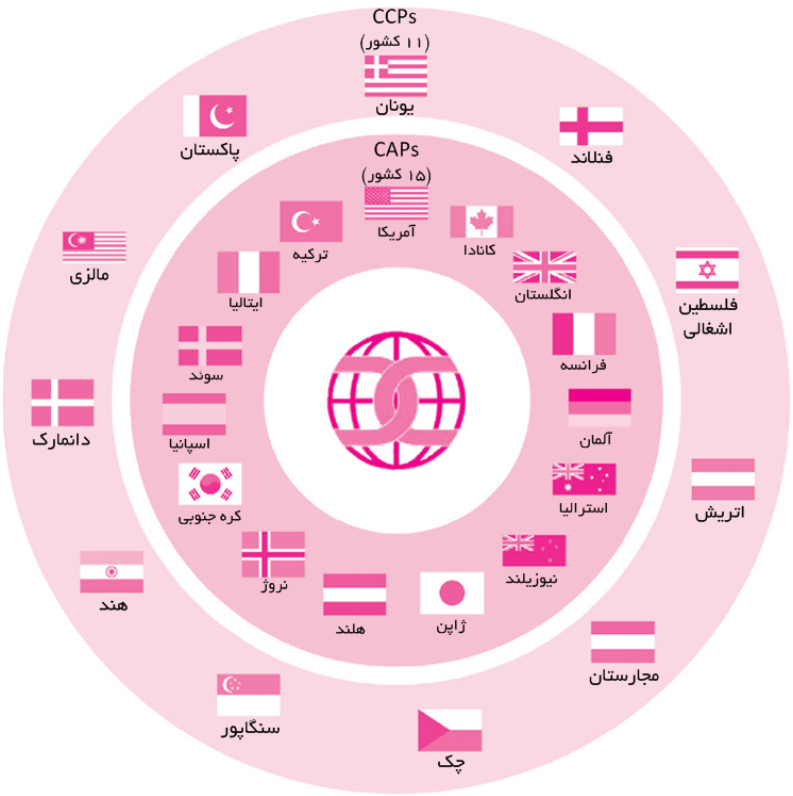
۲- **ارزیابی هدف امنیتی (ASE):** هدف امنیتی مبنای توافق بین سازندگان هدف مورد ارزیابی، مصرف‌کنندگان، ارزیاب‌ها و مراجع ارزیابی بر سر آن است که هدف مورد ارزیابی از چه ویژگی‌های امنیتی برخوردار بوده و دامنه ارزیابی تا کجا باشد. مخاطب هدف امنیتی ممکن است شامل آن‌هایی نیز باشد که هدف مورد ارزیابی را مدیریت، بازاریابی، خرید، نصب، پیکربندی، اجرا و استفاده می‌کنند. یک هدف امنیتی دربردارنده مقداری اطلاعات مختص اجراست که نشان می‌دهد محصول چگونه نیازمندی‌های امنیتی را مورد ملاحظه قرار می‌دهد. این هدف ممکن است به یک یا چند مشخصه حفاظتی اشاره داشته باشد. در این مورد، هدف امنیتی باید نیازمندی‌های امنیتی عمومی ارائه شده در هر یک از این مشخصه‌های حفاظتی را تحقق بخشد و می‌تواند نیازمندی‌های دیگری را تعریف کند.

۳- **دیگر موارد:** ارزیابی ADV، AGD، ALC ، ATE، AVA و ACO.

1- Firmware

تشکیلات بازشناسی معیارهای مشترک

تشکیلات بازشناسی معیارهای مشترک (CCRA)[1] برای تأیید گواهی‌های معیارهای مشترک در در میان کشورها سازمان‌دهی شد. هدف این تشکیلات این است که تضمین کند ارزیابی‌های معیارهای مشترک با توجه به استانداردهای سازگار انجام می‌شوند، ارزیابی‌های مضاعف محصولات فناوری اطلاعات یا مشخصات حفاظتی را حذف کرده یا کاهش دهد و با تأیید گواهی در میان کشورهای عضو، فرصت‌های بازار جهانی را برای صنعت فناوری اطلاعات بهبود بخشد.



شکل ۲-۴ شرکت‌کننده تنفیذکننده گواهی و شرکت‌کنندگان مصرف‌کننده گواهی

تشکیلات بازشناسی معیارهای مشترک از ۲۶ کشور عضو تشکیل شده است که ۱۵ عضو از آن‌ها شرکت‌کننده تنفیذکننده گواهی (CAPs)[2] و ۱۱ عضو شرکت‌کنندگان مصرف‌کننده گواهی

1- Common Criteria Recognition Arrangement
2- Certificate Authorizing Participants

(CCPs)[1] هستند. شرکت‌کننده تنفیذکننده گواهی تولیدکنندگان گواهی‌نامه‌های ارزیابی هستند. آن‌ها حامی یک سازمان صدور گواهی پیرو هستند که در کشور آن‌ها فعالیت می‌کند و گواهی‌نامه‌های صادر شده را تنفیذ می‌کنند. یک کشور باید برای حداقل ۲ سال به‌عنوان یک شرکت‌کننده مصرف‌کننده گواهی عضو تشکیلات بازشناسی معیارهای مشترک باشد تا بتواند برای تبدیل شدن به یک شرکت‌کننده تنفیذکننده گواهی درخواست بدهد. شرکت‌کنندگان مصرف‌کننده گواهی مصرف‌کنندگان این گواهی‌های ارزیابی هستند. اگرچه آن‌ها ممکن است دارای قابلیت ارزیابی امنیت فناوری اطلاعات نباشند، اما علاقه به استفاده از محصولات و مشخصات حفاظتی تصدیق شده یا تأیید اعتبار شده دارند. برای عضویت در تشکیلات بازشناسی معیارهای مشترک، یک کشور باید درخواست کتبی خود را به کمیته مدیریت ارسال کند.

۲-٤ مثال‌هایی از روش‌های امنیت اطلاعات

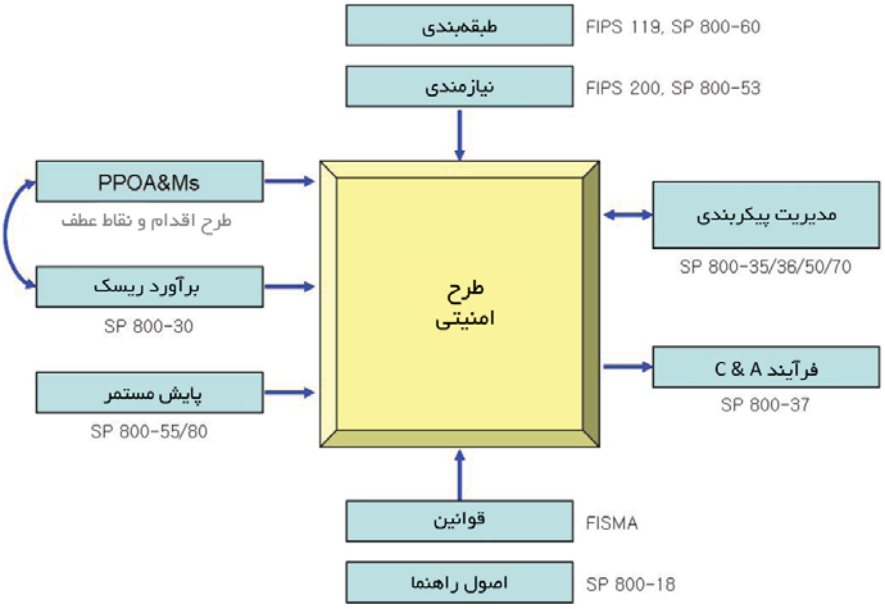
مؤسسه ملی استانداردها و فناوری ایالات متحده آمریکا

مؤسسه ملی استانداردها و فناوری ایالات متحده آمریکا (NIST)[2] رهنمودها و استانداردهایی را بر مبنای FISMA[3]، برای تقویت امنیت اطلاعات و سیستم‌های اطلاعاتی تدوین کرده است که مؤسسات فدرال می‌توانند استفاده کنند. هدف این رهنمودها و استانداردها عبارت است از:

- ✓ فراهم آوردن مجموعه مشخصاتی برای حداقل نیازمندی‌های امنیتی با تدوین استانداردهایی که بتوانند برای دسته‌بندی اطلاعات و سیستم‌های اطلاعاتی فدرال مورداستفاده قرار گیرند؛
- ✓ میسر کردن دسته‌بندی امنیتی برای اطلاعات و سیستم‌های اطلاعاتی؛
- ✓ گزینش و تعیین مشخصات اقدامات کنترلی امنیتی برای سیستم‌های اطلاعاتی که سازمان‌های مجری را در دولت‌های فدرال پشتیبانی می‌کنند؛ و
- ✓ وارسی کارایی و اثربخشی اقدامات کنترلی امنیتی روی آسیب‌پذیری‌ها

رهنمودهای مرتبط با قانون مدیریت امنیت اطلاعات فدرال به‌عنوان نشریات خاص و نشریات استانداردهای پردازش اطلاعات فدرال منتشر می‌شوند: ۵۰۰ مجموعه برای فناوری اطلاعات و ۸۰۰ مجموعه برای امنیت رایانه‌ها. شکل ۳-۴ فرآیندی را نشان می‌دهد که سازمان‌های دولتی آمریکا دنبال می‌کنند تا طرح‌های امنیتی خود را بر اساس این استاندارد تدوین نمایند.

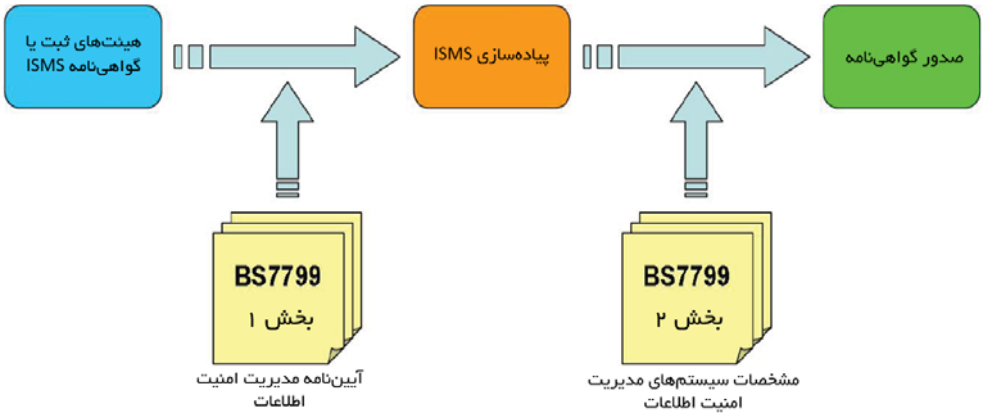
1- Certificate Consuming Participants
2- National Institute of Standards and Technology
3- Federal Information Security Management Act



شکل ۳-۴ ورودی/خروجی فرآیند برنامه‌ریزی امنیت

انگلستان (BS7799)

همان‌طور که قبلاً ذکر گردید، BSI فعالیت‌های امنیتی سازمان‌های موجود در انگلستان را تحلیل کرده و گواهی BS7799 را ارائه می‌کند که هم‌اکنون به (BS7799 part 2) ISO27001 و (BS7799 part 1) ISO27002 تغییر یافته است. شکل ۴-۴ رویه‌ای را که دنبال می‌شود نشان می‌دهد.

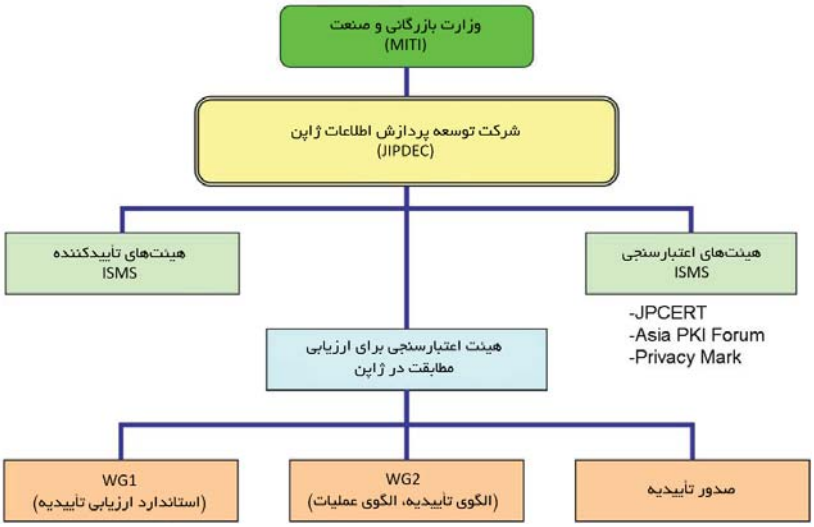


شکل ۴-۴ فرآیند گواهی BS7799

ژاپن (از ISMS Ver2.0 تا BS7799 Part 2: 2002)

گواهی ISMS Ver2.0 که از سوی شرکت توسعه پردازش‌های اطلاعاتی ژاپن تدوین شده است از آوریل سال ۲۰۰۲ تا کنون در این کشور عملیاتی شده است. این گواهی اخیراً به‌وسیله BS7799 Part 2: 2002 جایگزین شده است.

به‌دلیل اینکه دولت مرکزی برنامه‌ریزی امنیت اطلاعات را ترویج داده است، روند درخواست گواهی‌ها شتاب یافته است. دولت‌های محلی برای سازمان‌ها کمک مالی بلاعوض فراهم کرده‌اند تا گواهی ISMS[1] را به‌دست آورند. با این حال، ISMS Ver2.0 صرفاً بر جنبه اجرایی تأکید می‌کند و جنبه‌های فنی امنیت اطلاعات را در بر نمی‌گیرد. به‌علاوه، بیشتر سازمان‌ها تنها علاقه‌مند هستند که گواهی را دریافت کنند و ضرورتاً به دنبال بهبود فعالیت‌های امنیت اطلاعات نیستند. شکل ۵-۴ سیستم صدور گواهی سیستم مدیریت امنیت اطلاعات را در ژاپن نشان می‌دهد.



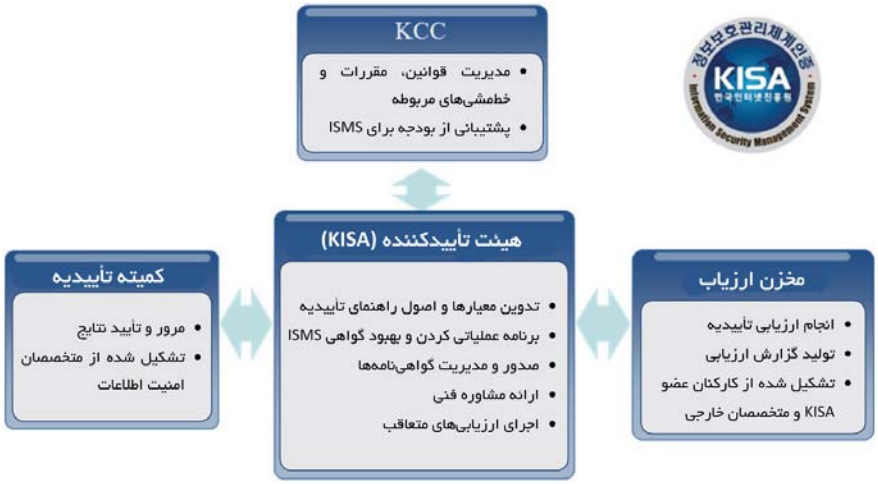
شکل ۵-۴ گواهی سیستم مدیریت امنیت اطلاعات در ژاپن

جمهوری کره (سیستم مدیریت امنیت اطلاعات سازمان اینترنت و امنیت کره)

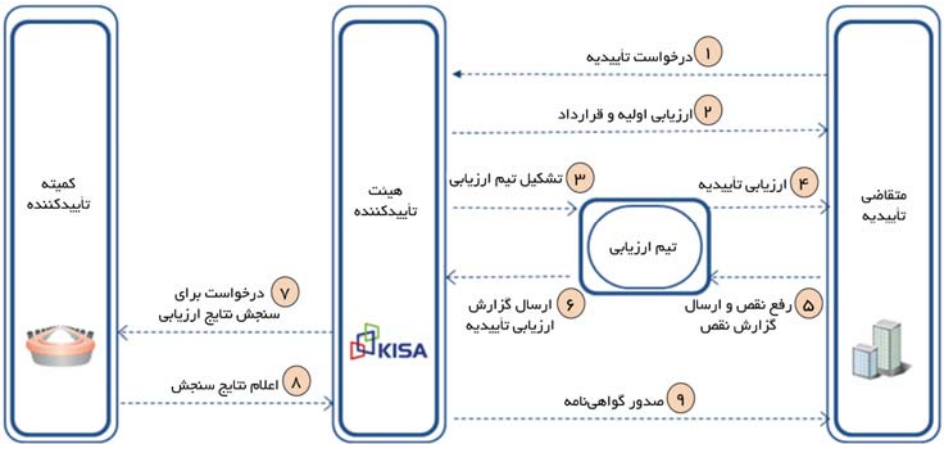
از سال ۲۰۰۲، وزارت کشور و کمیسیون ارتباطات کره و سازمان اینترنت و امنیت کره برنامه اخذ گواهی سیستم مدیریت امنیت اطلاعات را معرفی و عملیاتی کردند. وزارت کشور و کمیسیون ارتباطات کره و سازمان اینترنت و امنیت کره تلاش‌های بسیاری در جهت ترویج گواهی سیستم

1- Information Security Management System

مدیریت امنیت اطلاعات داشته‌اند و امروزه این برنامه بسیار موفق شمرده می‌شود. الگو و رویه‌های اخذ گواهی به ترتیب در شکل‌های ۶-۴ و ۷-۴ نشان داده شده‌اند. در سال ۲۰۱۱ تعداد گواهی‌نامه‌های سیستم مدیریت امنیت اطلاعات به ۱۱۴ رسید. چون این تعداد افزایش یافته است، انتظار می‌رود سطح امنیت اطلاعات هر سازمان تصدیق شده نیز به‌طور قابل‌ملاحظه‌ای بهبود یافته باشد. سازمان‌های تأیید شده شامل شرکت‌های پیشرو در زمینه‌های گوناگون کسب‌وکار از قبیل KT، Korean Air، NHN، Daum و دیگر شرکت‌های مشابه هستند.



شکل ۶-۴ الگوی نظام اخذ گواهی سیستم مدیریت امنیت اطلاعات در جمهوری کره



شکل ۷-۴ رویه‌های اخذ گواهی سیستم مدیریت امنیت اطلاعات در جمهوری کره

آلمان (صلاحیت حفاظت مرجع در فناوری اطلاعات)

سازمان BSI[1] در آلمان سازمانی ملی برای امنیت اطلاعات است. این سازمان خدمات امنیت فناوری اطلاعات را برای دولت آلمان، شهرها، سازمان‌ها و افراد این کشور فراهم می‌کند.

BSI بر اساس استاندارد بین‌المللی ISO Guide 25[GUI25] و استاندارد اروپایی EN45001 که مورد تأیید کمیته اروپایی آزمایش و تصدیق فناوری اطلاعات است، صلاحیت حفاظت مرجع در فناوری اطلاعات[2] را تدوین کرد. انواع تصدیق شامل گواهی حفاظت مرجع فناوری اطلاعات، گواهی خوداظهار حفاظت مرجع فناوری اطلاعات در سطح بالاتر و گواهی خوداظهار حفاظت مرجع فناوری اطلاعات در سطح مقدماتی است.

به‌علاوه، راهنمای حفاظت مرجع (BPM)[3] و راهنمای فرعی در استاندارد BSI مجموعه 100-X تدوین شده‌اند. موارد مهم عبارتند از: BSI Standard 100-1 ISMS، BSI Standard 100-2 BPM Methodology و BSI Standard 100-3 Risk analysis[۵۲].

دیگر موارد

جدول ۵-۴ دیگر نظام‌های تأیید سیستم مدیریت امنیت اطلاعات موجود را نشان می‌دهد.

جدول ۵-۴ گواهی سیستم مدیریت امنیت اطلاعات در دیگر کشورها

	مؤسسات صدور گواهی	استانداردها
کانادا	مؤسسه امنیت ارتباطات	MG-4 A Guide to Certification & Accreditation for Information Technology Systems
تایوان	اداره استانداردها، پیش‌بینی و بازرسی	CNS 17799 & CNS 17800
سنگاپور	کمیته استانداردهای فناوری اطلاعات	SS493: Part1 IT Security Standard Framework & (SS493: Part 2 (Security Services) در دست تدوین

1- Bundesamt für Sicherheit in der Informationstechnik
2- IT Baseline Protection Qualification
3- Baseline Protection Manual

فصل پنجم

حفاظت از حریم خصوصی

این فصل کمک می‌کند تا:
- تغییرات در مفهوم حریم خصوصی دنبال شوند؛
- روندهای بین‌المللی در حفاظت از حریم خصوصی توصیف شوند؛
- مروری کلی بر برآورد تأثیر بر حریم خصوصی داشته و نمونه‌هایی از آن ارائه شوند.

۵-۱ مفهوم حریم خصوصی

اطلاعات شخصی[1] هر نوع اطلاعاتی است که به فردی قابل‌شناسایی[۵۳] یا یک شخصیت حقیقی شناخته شده یا قابل‌شناسایی مربوط می‌شود[۵۴]. اطلاعات شخصی شامل اطلاعاتی از قبیل نام افراد، شماره تلفن، آدرس، آدرس ایمیل، شماره پلاک اتومبیل، ویژگی‌های فیزیکی (ابعاد چهره، اثر انگشتان، دستخط و غیره)، شماره کارت اعتباری و ارتباطات خانوادگی است.

دسترسی، جمع‌آوری، تحلیل و استفاده نابجا از اطلاعات شخصی یک فرد روی رفتار دیگران نسبت به آن فرد اثرگذار است و در نهایت اثری منفی بر جایگاه اجتماعی و امنیت او خواهد داشت. بنابراین، اطلاعات شخصی را باید در مقابل دسترسی، جمع‌آوری، ذخیره‌سازی، تحلیل و استفاده نامناسب محافظت کرد. به این معنی، اطلاعات شخصی موضوع حفاظت است.

هنگامی‌که موضوع حفاظت به‌جای خود اطلاعات، حق داشتن اطلاعات شخصی است، مفهوم حریم خصوصی به‌وجود می‌آید. پنج روش برای توضیح حق برخورداری از حریم خصوصی وجود دارد:
- ✓ حق آزاد بودن از دسترسی ناخواسته (مثلاً دسترسی فیزیکی و دسترسی از طریق سرویس پیام‌های کوتاه)
- ✓ حق ندادن اجازه برای استفاده از اطلاعات شخصی در موارد ناخواسته (مثلاً فروش و افشای اطلاعات)
- ✓ حق ندادن اجازه برای جمع‌آوری اطلاعات شخصی به‌وسیله دیگران بدون اطلاع و اجازه یک شخص (مثلاً از طریق دوربین‌های مدار بسته یا کوکی‌ها)

---

[1]- Personal Information

- ✓ حق بیان و اظهار دقیق و صحیح اطلاعات شخصی (صحت)
- ✓ حق دریافت پاداش به دلیل ارزش اطلاعات مربوط به یک شخص

مفهوم منفعل حریم خصوصی شامل حق رها بودن و حق طبیعی است که مربوط به شأن انسان است. این مفهوم به قانون منع‌کننده تجاوز متصل است.

مفهوم فعال حریم خصوصی شامل کنترل شخصی اطلاعات خصوصی یا حق مدیریت یا کنترل اطلاعات شخصی به‌طور مثبت است، از جمله حق تصحیح مواردی که از اطلاعات شخصی نادرست ناشی می‌شود.

۲-۵ روندهای موجود در حریم خصوصی

رهنمودهای سازمان همکاری و توسعه اقتصادی درباره حفاظت از حریم خصوصی

در سال ۱۹۸۰، سازمان همکاری و توسعه اقتصادی "رهنمودهای حفاظت از حریم خصوصی و جریان اطلاعات شخصی بین مرزها"[1] را تصویب کرد که با عنوان " اقدامات اطلاعاتی سزاوار سازمان همکاری و توسعه اقتصادی"[2] نیز شناخته می‌شود. در سال ۲۰۰۲، "حریم خصوصی آنلاین: رهنمودهای سازمان همکاری و توسعه اقتصادی در حریم خصوصی و طرز عمل"[۵۵] اعلام شد. این رهنمودها به داده‌های شخصی اعمال می‌شد که چه در بخش عمومی و چه در بخش خصوصی، به‌دلیل شیوه پردازش این داده‌ها یا به‌خاطر طبیعت آن‌ها یا مضمونی که در آن استفاده می‌شوند، خطری را متوجه حریم خصوصی یا آزادی‌های فردی می‌کنند. اصولی که سازمان همکاری و توسعه اقتصادی در این رهنمودها شناسایی کرده است حقوق و تعهدات افراد را در زمینه پردازش خودکار داده‌های شخصی و حقوق و تعهدات افرادی که در این پردازش‌ها نقش دارند، ذکر می‌کند. به‌علاوه، اصول مبنای ذکر شده در این رهنمودها در هر دو سطح ملی و بین‌المللی قابلیت کاربرد دارند.

هشت اصلی که رهنمودهای سازمان همکاری و توسعه اقتصادی را در حفاظت از حریم خصوصی تشکیل می‌دهند، عبارتند از:

1- Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
2- OECD Fair Information Practices

۱- اصل محدودیت جمع‌آوری

باید در جمع‌آوری داده‌های شخصی محدودیت وجود داشته باشد و هر داده این‌چنینی باید از طریق روش‌های قانونی و مجاز و در صورت لزوم، با آگاهی و اجازه شخص موردنظر به‌دست آید.

۲- اصل کیفیت داده‌ها

داده‌های شخصی باید با هدفی که برای آن استفاده می‌شوند مرتبط بوده و باید تا حدی که برای آن هدف ضروری است دقیق، کامل و به‌روز باشند.

۳- اصل تشخیص هدف

اهدافی که برای آن‌ها داده‌های شخصی جمع‌آوری می‌شوند باید قبل از شروع به جمع‌آوری داده‌ها تعیین شوند و استفاده متعاقب از داده‌ها محدود به تحقق آن اهداف یا اهدافی دیگری است که با اهداف اولیه ناسازگاری نداشته باشند و به دلایلی از تغییر اهداف اولیه به‌دست آیند.

۴- اصل محدودیت استفاده

داده‌های شخصی نباید فاش شده و در دسترس دیگران قرار گیرند یا برای اهدافی غیر مرتبط با اصل تشخیص هدف مورداستفاده قرار گیرند مگر با اجازه شخص موردنظر یا با مجوز مراجع قانونی.

۵- اصل حراست از امنیت

داده‌های شخصی باید با استفاده از ابزارهای حفاظتی معقول در برابر ریسک‌هایی چون از دست‌رفتگی یا دسترسی غیرمجاز، تخریب، کاربرد، تغییر یا افشاسازی داده‌ها محافظت شوند.

۶- اصل باز بودن

باید یک خط‌مشی کلی باز بودن در توسعه، طرز عمل و خط‌مشی‌های مرتبط با داده‌های شخصی وجود داشته باشد. ابزارها و روش‌ها باید به‌آسانی برای تشخیص هستی و ذات داده‌های شخصی و هدف اصلی استفاده از آن‌ها و نیز هویت و محل اقامت کنترل‌گر داده‌ها در دسترس باشند.

۷- اصل شرکت فردی

یک فرد باید از حقوق زیر برخوردار باشد:

الف) به‌دست آوردن تأیید کنترل‌گر داده‌ها در مورد اینکه آیا داده‌های مربوط به او در اختیار کنترل‌گر هست یا خیر؛

ب) دریافت ابلاغیه در مورد داده‌های مربوط به او در زمانی متعارف، با هزینه‌ای، در صورت وجود که بیش از حد نباشد، به طریقه‌ای معقول و به شکلی که به‌آسانی برای او قابل‌فهم باشد؛

ج) دریافت دلیل در صورتی‌که درخواستی که تحت موارد (الف) و (ب) انجام شده رد گردد و توانایی در مورد پرسش قرار دادن چنین رد کردنی؛

د) مورد پرسش قرار دادن داده‌های مربوط به او و در صورتی‌که حق با او بود، درخواست برای پاک، تصحیح، تکمیل یا ترمیم کردن آن‌ها.

۸- اصل مسئولیت‌پذیری

یک کنترل‌گر داده‌ها باید مسئولیت پیروی از اقداماتی را که به اصول ذکر شده در بالا اثر می‌بخشند، به عهده بگیرد[۵۶].

رهنمودهای سازمان ملل در حفاظت از حریم خصوصی

از اواخر دهه ۱۹۶۰، دنیا متوجه تأثیرات وارده به حریم خصوصی از سوی پردازش خودکار اطلاعات گردید. مخصوصاً نهاد آموزشی، علمی و فرهنگی سازمان ملل (UNESCO) از زمانی که در سال ۱۹۹۰، "رهنمودهای سازمان ملل برای تنظیم مقررات فایل‌های داده‌ای رایانه‌ای شخصی"[1] به‌وسیله مجمع عمومی مورد تصویب قرار گرفت، به مبحث حریم خصوصی و حفاظت از آن علاقه نشان داده است.

رهنمودهای سازمان ملل برای اسناد (کاغذی) و نیز فایل‌های داده رایانه‌ای در بخش‌های عمومی و خصوصی به کار گرفته می‌شود. این رهنمودها مجموعه‌ای از اصول را با در نظر گرفتن حداقل تضمین‌ها ارائه می‌کند که باید برای قانون‌گذاری ملی یا در قوانین داخلی سازمان‌های بین‌المللی فراهم شوند. این اصول عبارتند از:

۱- اصل مشروعیت و منصفانه بودن

اطلاعات پیرامون اشخاص نباید از طرق غیرمنصفانه یا غیرقانونی جمع‌آوری و پردازش شوند و نباید این اطلاعات برای مقاصدی که در تضاد با اهداف و اصول منشور سازمان ملل هستند مورداستفاده قرار گیرند.

۲- اصل صحت

اشخاصی که مسئول گردآوری فایل‌ها هستند یا کسانی که نگهداری آن‌ها را به عهده دارند ملزم هستند که بررسی‌های منظمی را درباره صحت و ربط داده‌های ثبت شده به عمل آورده و تضمین کنند که داده‌ها تا اندازه ممکن به‌طور کامل نگهداری می‌شوند تا از خطاهای ناشی از سهل‌انگاری خودداری شود و اینکه داده‌ها به‌طور منظم به‌روزرسانی می‌شوند.

۳- اصل تشخیص هدف

هدفی که یک فایل باید برآورده کند و نحوه استفاده از آن برای دستیابی به هدف باید مشخص شده، مشروع و هنگامی‌که برقرار شود، میزان خاصی از علنی بودن را به‌دست آورد یا موردتوجه شخص موردنظر قرار گیرد تا متعاقباً امکان تضمین موارد زیر مهیا شود:

1- UN Guidelines for the Regulation of Computerized Personal Data File

الف) همه داده‌های شخصی جمع‌آوری و ثبت شده همچنان برای هدف مشخص شده مربوط و کافی باقی بمانند.

ب) هیچ‌کدام از داده‌های شخصی ذکر شده برای هدفی ناسازگار با اهداف مشخص شده استفاده نشده یا فاش نگردد، مگر با اجازه شخص موردنظر.

ج) دوره زمانی که در آن داده‌های شخصی نگهداری می‌شوند از حدی که باعث دست‌یابی به اهداف مشخص شده می‌شود فراتر نرود.

۴- اصل دسترسی شخص علاقه‌مند

هر فردی که مدارک اثبات هویت خود را ارائه می‌کند دارای این حق است که بداند آیا اطلاعات مربوط به او پردازش می‌شود و این مدارک را به شکل قابل‌فهم، بدون تأخیر یا هزینه بی‌مورد، به‌دست آورد و در صورتی‌که مندرجات غیرمجاز، غیرضروری یا ناصحیح در اطلاعات مربوط به او وجود داشت، درخواست انجام تصحیحات و زدایش‌های مناسب را بکند و هنگامی‌که این داده‌ها در حال تبادل هستند، از گیرنده آن اطلاع حاصل کند.

۵- اصل عدم تبعیض

موارد استثنایی منحصراً دیده شده تحت اصل ۶، داده‌هایی که احتمال بروز تبعیض نامشروع یا مستبدانه را افزایش می‌دهد، از جمله اطلاعات مربوط به اصالت نژادی یا قومی، رنگ پوست، روابط جنسی، عقاید سیاسی، مذهبی، فلسفی و دیگر انواع باورها و نیز عضویت در انجمن‌ها یا اتحادیه‌های بازرگانی، نباید گردآوری شوند.

۶- قدرت استثنا قائل شدن

می‌توان اجازه عدول از اصول ۱ تا ۴ را داد، تنها اگر برای حفظ امنیت ملی، نظم عمومی، سلامت و اخلاق همگانی و نیز در میان موارد دیگر، حقوق و آزادی‌های دیگران، مخصوصاً افرادی که مورد ستم واقع می‌شوند (شرط بشردوستانه) ضروری باشند، به شرطی که چنین عدول کردن‌هایی به‌صراحت در یک قانون یا مقررات معادلی که رسماً اعلام شده‌اند، در تطابق با سیستم حقوقی داخلی که صریحاً محدودیت‌ها را اعلام کرده و امکانات حفاظتی مناسب را نیز فراهم می‌کند، بیان شده باشند. استثناهای اصل ۵ که مربوط به منع تبعیض است، علاوه بر اینکه در معرض اقدامات حفاظتی ذکر شده برای موارد استثنایی اصول ۱ تا ۴ هستند، صرفاً زمانی مجاز هستند که در محدوده تجویز شده در اعلامیه جهانی حقوق بشر و دیگر اسناد مرتبط در حوزه حفاظت از حقوق بشر و جلوگیری از تبعیض باشند.

۷- اصل امنیت

برای محافظت از فایل‌ها در مقابل خطرات طبیعی، از قبیل از دست‌رفتگی ناخواسته یا تخریب و خطرات انسانی، از قبیل دسترسی غیرمجاز، سوءاستفاده متقلبانه از داده‌ها یا آلوده‌سازی به‌وسیله ویروس‌های رایانه‌ای باید اقدامات مناسب و به‌جا را انجام داد.

۸- نظارت و ضمانت اجرا

قانون هر کشوری باید مرجعی قانونی را که در تطابق با سیستم حقوقی داخلی، مسئولیت نظارت بر مجموعه اصول بالا را دارد مشخص کند. این مرجع باید تضمین‌هایی را در ارتباط با بی‌طرفی، استقلال افراد یا سازمان‌هایی که مسئولیت پردازش و استفاده از داده‌ها را به عهده دارند و نیز کفایت فنی آن‌ها ارائه دهد. در صورت نقض موارد قید شده در قانون ملی که اصول بالا را اجرا می‌کند، باید مجازات‌ها و جریمه‌هایی اعمال شده و جبران‌های مناسب برای فرد قربانی صورت گیرد.

۹- جریان داده‌ها به آن سوی مرزها

وقتی‌که قانون‌گذاری در دو یا بیش از دو کشور که علاقه‌مند به انتقال داده‌ها به آن سوی مرزها هستند، ابزارهای حفاظتی مشابهی برای محافظت از حریم خصوصی ارائه کنند، اطلاعات باید بتوانند به همان آسانی که در داخل قلمرو این کشورها رد و بدل می‌شوند بین مرزهای آن‌ها نیز در گردش باشند. اگر ابزارهای حفاظتی متقابل وجود نداشته باشد، نمی‌توان بی‌جهت محدودیت‌هایی بر چنین گردشی اعمال کرد و این کار تنها تا جایی که حفاظت از حریم خصوصی نیاز دارد انجام می‌گیرد.

۱۰- زمینه کاربرد

اصول حاضر، در اولین نمونه، باید برای همه فایل‌های رایانه‌ای عمومی و خصوصی، به‌وسیله بسط‌های انتخابی و با استفاده از اِعمال تنظیم‌های مناسب به فایل‌های دستی، کاربردی شوند. تبصره‌های مخصوص نیز که اختیاری هستند، می‌توانند برای بسط همه یا بخشی از اصول به فایل‌های اشخاص حقوقی، به‌ویژه زمانی‌که آن‌ها شامل اطلاعات افراد باشند، انجام شوند[۵۷].

دستورالعمل اتحادیه اروپا در حفاظت از داده‌ها[1]

شورای وزرای اتحادیه اروپا دستورالعمل اروپایی را برای حفاظت از افراد با توجه به پردازش داده‌های شخصی و نیز حرکت آزادانه چنین داده‌هایی (دستورالعمل اتحادیه اروپا) در ۲۴ اکتبر ۱۹۹۵ تصویب کرد تا چارچوب مقرراتی را برای تضمین گردش امن و آزاد داده‌های شخصی در میان مرزهای ملی کشورهای عضو اتحادیه اروپا ارائه کند. به‌علاوه، مبنایی را برای امنیت اطلاعات شخصی در هر جایی که ذخیره می‌شوند، انتقال می‌یابند یا پردازش می‌شوند تنظیم کرد.

1- EU Data Protection Directive

دستورالعمل اتحادیه اروپا در حفاظت از داده‌های شخصی تلاشی برای متحد و هماهنگ شدن با قوانین شهری مربوط به حفاظت از حریم خصوصی بود. ماده ۱ از دستورالعمل اتحادیه اروپا تصریح می‌کند که: "دولت‌های عضو باید از حقوق و آزادی‌های اساسی اشخاص حقیقی، به‌ویژه حق داشتن حریم خصوصی، در هنگام پردازش اطلاعات شخصی، محافظت کنند."

این دستورالعمل انتقال داده‌های شخصی را به کشورهایی که از سطح کافی حفاظتی برخوردار نیستند ممنوع می‌کند، چون منجر به بروز خصومت بین اتحادیه اروپا و دولت ایالات متحده آمریکا می‌گردد[۵۸].

هر کشور عضو اتحادیه اروپا قوانین موجود خود را اصلاح کرده یا مجموعه قوانین جدیدی برای حفاظت از حریم خصوصی تدوین نموده است تا در جهت دستورالعمل اتحادیه اروپا حرکت کند.

نمونه‌های دیگری از قوانین اتحادیه اروپا پیرامون حریم خصوصی ماده ۸ کنوانسیون اروپا درباره حقوق بشر، دستورالعمل 95/46/EC (دستورالعمل حفاظت از داده‌ها)، دستورالعمل 2002/8/EC (دستورالعمل حریم خصوصی الکترونیکی) و دستورالعمل 2006/24/EC ماده ۵ (دستورالعمل نگهداری داده‌ها) می‌باشند[۵۹].

حفاظت از حریم خصوصی در جمهوری کُره

در کُره، اطلاعات شخصی تحت قوانین مختلف حفاظت می‌شد. با این حال، برای افزایش سطح حفاظت در حیطه‌هایی که هیچ قانون قابل اجرایی وجود نداشت، قانون حفاظت از حریم خصوصی تدوین گردید.

قانون حفاظت از حریم خصوصی در ۲۸ مارس ۲۰۱۱، در مجلس ملی تصویب شد و در ۳۰ سپتامبر ۲۰۱۱ به مرحله اجرا در آمد. هدف اصلی این قانون عبارت است از: (۱) رفع نقاط کور موجود به‌دلیل غیبت قوانینی که کسب‌وکار آفلاین و سازمان‌های غیرانتفاعی را سامان‌دهی کند؛ (۲) برآوردن نیازها برای به‌کارگیری استانداردهای جهانی مرتبط با قانون حفاظت از حریم خصوصی؛ (۳) محافظت از حقوق افراد با تقویت حق خودمختاری اطلاعاتی و جبران قانونی در مقابل نقض حقوق افراد.

قوانینی از قبیل "قانون حفاظت از اطلاعات شخصی در معرض عموم" و "قانون ترویج استفاده از شبکه‌های اطلاعاتی و ارتباطی و حفاظت از اطلاعات" نیز وجود داشت که مرتبط با حفاظت از حریم خصوصی بود. "قانون حفاظت از اطلاعات شخصی در معرض عموم"، در ۳۰ سپتامبر ۲۰۱۱ ملغی گردید، چون قانون حفاظت از حریم خصوصی به اجرا در آمد. "قانون ترویج استفاده از شبکه‌های اطلاعاتی و ارتباطی و حفاظت از اطلاعات" از زمان تصویبش تا کنون اصلاح شده است. اخیراً، این قانون به‌گونه‌ای تغییر یافت که به افراد اجازه می‌داد که محتوای آن چیزی را که از اطلاعات شخصی آن‌ها منتقل شده و به دیگران سپرده می‌شود تعیین کنند.

قانون حفاظت از اطلاعات شخصی در معرض عموم: این قانون حاوی قیودی برای رسیدگی و مدیریت اطلاعات شخصی پردازش شده در رایانه‌های مؤسسات عمومی، جهت حفاظت از حریم خصوصی است. همچنین مقرراتی را برای عملکرد معقول در کسب‌وکارهای عمومی و حفاظت از حقوق و منافع مردم ارائه می‌کند.

قانون ترویج استفاده از شبکه‌های اطلاعاتی و ارتباطی و حفاظت از اطلاعات: هدف این قانون بهبود سیستم حفاظت از حریم خصوصی در بخش خصوصی، با توجه به گسترش شبکه‌های اطلاعاتی و ارتباطی و فراگیر شدن جمع‌آوری و توزیع اطلاعات شخصی است. این قانون فرآیند حفاظت از حریم خصوصی را بر اساس چرخه حیات اطلاعات شخصی، از قبیل جمع‌آوری، استفاده، مدیریت و حذف، دنبال می‌کند. همچنین، این قانون مقرراتی را در مورد حقوق کاربران اطلاعات شخصی و نیز تأسیس و نحوه عملکرد یک کمیته میانجی در حریم خصوصی در بردارد.

قانون محافظت از اسرار ارتباطات: این قانون دامنه هدف حریم خصوصی و آزادی ارتباطات را محدود می‌کند تا از حریم خصوصی ارتباطات حفاظت نموده و آزادی آن را تضمین کند. این قانون دخول بی‌اجازه به مکالمات مخفی، از قبیل ضبط یا استراق سمع را ممنوع می‌کند و از حریم خصوصی در ارتباطات حفاظت می‌کند.

قانون حفاظت از اطلاعات مربوط به موقعیت: این قانون به دنبال آن است که جمع‌آوری و استفاده از اطلاعات مبتنی بر محل را سامان‌دهی کند، چنین اطلاعاتی را در مقابل نشت و سوءاستفاده محافظت کند و استفاده از اطلاعات را در محیط امن ترویج کند. این قانون ظرفیت فناوری ارتباطات امروزی را برای تعیین محل افراد (به‌عنوان مثال از طریق تلفن همراه) و این واقعیت را که نشت اطلاعات مربوط به محل می‌تواند باعث نقض جدی حریم خصوصی گردد، باز می‌شناسد. از این رو، قانون مقرر می‌دارد که اطلاعات مربوط به محل هرگز فاش نشود، مگر در مواردی که قانون نیازمند آن باشد.

حفاظت از حریم خصوصی در ایالات متحده آمریکا

از آنجایی که محدودیت‌های بیش از حد اعمال شده از سوی دولت باعث ایجاد اختلال در فعالیت‌های تجارت الکترونیکی شده بود، ایالات متحده فعالیت‌های مرتبط با حفاظت از حریم خصوصی را به عهده بازار گذاشته است. در نتیجه، مهرهایی برای تأیید رعایت حریم خصوصی از قبیل Trust-e یا Better Business Bureau Online پدید آمده‌اند و قوانین مربوط به حفاظت حریم خصوصی یکپارچه نشده‌اند. قانون حریم خصوصی سال ۱۹۷۴ محافظت از حریم خصوصی اطلاعات را در بخش عمومی فراهم می‌کند در حالی‌که قوانین مختلفی حریم خصوصی را در بخش خصوصی کنترل می‌کنند. هیچ سازمانی نیست که به همه موضوعات مربوط به حفاظت حریم خصوصی، در بخش خصوصی رسیدگی

کند. در بخش عمومی، اداره مدیریت و بودجه (OMB)[1] نقشی را در تدوین سیاست‌های دولت فدرال در مورد حریم خصوصی با توجه به قانون حریم خصوصی ایفا می‌کند. در بخش خصوصی، کمیسیون بازرگانی فدرال اختیار اجرای قوانینی را دارد که حریم خصوصی آنلاین کودکان، اطلاعات اعتباری مشتریان و شیوه‌های معاملاتی منصفانه را محافظت می‌کند.

قوانین مرتبط با حفاظت از حریم خصوصی در ایالات متحده شامل این موارد است:

- ✓ قانون حریم خصوصی، ۱۹۷۴
- ✓ قانون حفاظت از اعتبار مشتریان، ۱۹۸۴
- ✓ قانون حفاظت از حریم ارتباطات الکترونیکی، ۱۹۸۶
- ✓ قانون گرم-لیچ- بلایلی، ۱۹۹۹[2]
- ✓ قانون قابلیت حمل و مسئولیت‌پذیری بیمه سلامت، ۱۹۹۶
- ✓ قانون ساربِینس- اوکسلی، ۲۰۰۲[3]
- ✓ قانون حفاظت از حریم خصوصی آنلاین کودکان، ۱۹۹۸

اقدامات حفاظت از حریم خصوصی در ژاپن

در سال ۱۹۸۲، ژاپن اقدامات حفاظت از حریم خصوصی را بر مبنای ۸ اصل اساسی سازمان همکاری و توسعه اقتصادی تدوین کرد. در سال ۱۹۸۸، قانون حفاظت از حریم خصوصی در بخش عمومی رسماً اعلام شد و به مرحله اجرا در آمد. در بخش خصوصی، راهنمای حفاظت از حریم خصوصی، به‌وسیله وزارت بازرگانی و صنعت در سال ۱۹۹۷ صادر شد. برای بهبود مطابقت قوانین ملی حفاظت از حریم خصوصی با رهنمودهای بین‌المللی، مرکز پیشبرد انجمن اطلاعات پیشرفته و مخابرات[4] در تلاش بوده است تا قوانین حفاظت از اطلاعات شخصی را تدوین کند.

به‌علاوه، مرجع حفاظت از داده‌ها به‌عنوان سازمانی مستقل در نظر گرفته شده است که رعایت درست حریم خصوصی را تضمین می‌کند و به افراد در صورت بروز تجاوز به حریم خصوصی یاری می‌رساند. مرجع حفاظت از داده‌ها متعهد است تا شفافیت پردازش اطلاعات را بهبود دهد، حقوق و مزایای افراد مرتبط با داده‌ها را تضمین کند و اطمینان حاصل کند که هم سازمان‌های پردازش‌کننده اطلاعات و هم کاربران اطلاعات وظایفشان را انجام می‌دهند. همچنین، از این مرجع انتظار می‌رود که در حفاظت از منافع ملی نقش ایفا کند، مخصوصاً در مواردی که مستلزم انتقال داده‌ها به آن سوی مرزها هستند.

1- Office of Management and Budget (USA)
2- Gramm-Leach-Bliley Act, 1999
3- Sarbanes-Oxley Act, 2002
4-Advanced Information and Telecommunications Society Promotion Headquarters

قوانین ژاپن که مرتبط با حفاظت از حریم خصوصی هستند عبارتند از:

- ✓ قانون حفاظت از داده‌های پردازش شده با رایانه که در اختیار سازمان‌های اجرایی هستند، ۱۹۸۸.
- ✓ مقررات دولت‌های محلی (تصویب شده در سال ۱۹۹۹ برای ۱۵۲۹ دولت محلی)
- ✓ قانون حفاظت از اطلاعات شخصی، ۲۰۰۳
- ✓ قانون حفاظت از اطلاعات شخصی در اختیار سازمان‌های اجرایی هستند، ۲۰۰۳
- ✓ قانون حفاظت از اطلاعات شخصی که توسط مؤسسات اجرایی مستقل حفظ می‌شوند، ۲۰۰۳
- ✓ مجموعه قوانین ممیزی، ۲۰۰۳
- ✓ راهنمای حفاظت از حریم خصوصی با توجه به تگ‌های RFID، ۲۰۰۴

پرسش‌هایی برای تفکر

۱- در کشور شما چه سیاست‌ها و قوانینی برای حفاظت از حریم خصوصی اطلاعات اجرا می‌شوند؟

۲- چه مسائل و ملاحظاتی روی تصویب یا اجرای چنین سیاست‌ها و قوانینی اثرگذار هستند؟

۳- به نظر شما چه اصولی زیربنای سیاست‌ها و قوانین مربوط به حفاظت از حریم خصوصی را تشکیل می‌دهند؟ (رهنمودهای سازمان همکاری و توسعه اقتصادی و رهنمودهای سازمان ملل را مشاهده کنید).

۳-۵ برآورد تأثیر بر حریم خصوصی

برآورد تأثیر بر حریم خصوصی چیست؟

برآورد تأثیر بر حریم خصوصی (PIA)[1] فرآیندی نظام‌مند از بررسی، تحلیل و ارزیابی اثر به‌کارگیری سیستم‌های اطلاعاتی جدید یا اصلاح سیستم‌های اطلاعاتی موجود بر حریم خصوصی مشتریان یا مردم است. برآورد تأثیر بر حریم خصوصی بر مبنای اصل پیش‌گیری اولیه - یعنی پیش‌گیری بهتر از درمان است- عمل می‌کند. این فرآیند فقط یک ارزیابی سیستمی ساده نیست، بلکه در نظر گرفتن آثار جدی بر حریم خصوصی با معرفی یا تغییر سیستم‌های جدید است. از این رو، این فرآیند با ممیزی حفاظت از حریم خصوصی که از رعایت سیاست‌های داخلی و نیازمندی‌های خارجی برای حریم خصوصی اطمینان حاصل می‌کند، متفاوت است.

1- Privacy Impact Assessment

چون برآورد تأثیر بر حریم خصوصی انجام می‌شود تا میزان تجاوز به حریم خصوصی را در هنگام ساخت سیستمی جدید تحلیل کند، باید در مراحل ابتدایی ساخت اجرا شود، هنگامی‌که هنوز امکان اعمال تنظیمات و تطبیق‌ها با مشخصات ساخت وجود دارد. با این حال، وقتی‌که ریسک تجاوز جدی در جمع‌آوری، استفاده و مدیریت داده‌های شخصی، در هنگام اجرای سرویس‌های موجود رخ بدهد، مطلوب است که یک فرآیند برآورد تأثیر بر حریم خصوصی انجام شده و سپس سیستم طبق آن اصلاح گردد.

فرآیند برآورد تأثیر بر حریم خصوصی[۶۰]

به‌طور کلی فرآیند برآورد تأثیر بر حریم خصوصی از سه مرحله تشکیل شده است (جدول ۱-۵ را مشاهده کنید).

جدول ۱-۵ فرآیند برآورد تأثیر بر حریم خصوصی

تحلیل مفهومی	تحلیل جریان داده‌ها	تحلیل تکمیلی
یک توصیف زبان واضح از دامنه و منطق کسب‌وکار ابتکار پیشنهادی آماده کنید.	جریان داده‌ها را از طریق نمودارهای فرآیند کسب‌وکار تحلیل کرده و عناصر داده یا خوشه‌هایی از داده‌های شخصی را شناسایی کنید.	سخت‌افزار و طراحی سیستم ابتکار پیشنهادی را مرور و تحلیل کنید تا از تبعیت سیستم از نیازمندی‌های طراحی در حریم خصوصی اطمینان حاصل نمایید.
به شیوه‌ای مقدماتی، مشکلات بالقوه حریم خصوصی، ریسک‌ها و ذی‌نفعان اصلی را شناسایی کنید.	پیروی پاز طرح پیشنهادی را از آزادی اطلاعات و قوانین مربوط به حریم خصوصی و دیگر قوانین مدون مربوطه برآورد کنید.	یک مرور نهایی از ابتکار پیشنهادی فراهم کنید.
توصیفی مشروح از جنبه‌های ضروری طرح پیشنهادی، از جمله تحلیل سیاست در زمینه مسائل عمده فراهم کنید.	مطابقت وسیع‌تر طرح پیشنهادی را با اصول عمومی حریم خصوصی برآورد کنید.	یک تحلیل حریم خصوصی و ریسک را از هر تغییر جدید در ابتکار پیشنهادی که مربوط به طراحی سخت‌افزاری و نرم‌افزاری باشد اجرا کنید تا از مطابقت با آزادی اطلاعات و قوانین مربوط به حریم خصوصی، قوانین مدون مربوطه و اصول کلی حریم خصوصی اطمینان حاصل نمایید.
جریان‌های اصلی اطلاعات شخصی را مستند کنید.	بر اساس تحلیل حریم خصوصی ابتکار، ریسک را تحلیل کرده و راه‌حل‌های ممکن را شناسایی کنید.	
معضلات محیطی پیرامون را پویش کرده و مرور کنید که چگونه دیگر سیستم‌های قضایی با ابتکاری مشابه برخورد می‌کنند.	گزینه‌های طراحی را مرور کرده و مشکلات / نگرانی‌های برجسته حریم	طرحی را برای ارتباطات آماده کنید.

مشکلات و نگرانی‌های ذی‌نفعان را شناسایی کنید. واکنش عمومی را برآورد کنید.	خصوصی را که مورد رسیدگی قرار نگرفته‌اند شناسایی کنید. پاسخی را برای مسائل حل نشده حریم خصوصی آماده کنید.	

منبع: Information and Privacy Office, Privacy Impact Assessment: A User's Guide (Ontario, Management Board Secretariat, 2001), p. 5.

دامنه ارزیابی برآورد تأثیر بر حریم خصوصی

یک برآورد تأثیر بر حریم خصوصی هنگامی انجام می‌شود که:

۱- سیستم اطلاعاتی جدیدی ساخته می‌شود که مقدار زیادی از اطلاعات شخصی را نگهداری و مدیریت می‌کند؛

۲- فناوری جدیدی مورداستفاده قرار می‌گیرد که در آن حریم خصوصی ممکن است نقض گردد.

۳- یک سیستم اطلاعاتی موجود تغییر می‌کند که اطلاعات شخصی را نگهداری و مدیریت می‌کند؛

۴- جمع‌آوری، استفاده، نگهداری یا نابودسازی اطلاعات شخصی انجام می‌شود که در طی آن خطر تجاوز به حریم خصوصی امکان بروز داشته باشد.

اما اجرای برآورد تأثیر بر حریم خصوصی برای همه سیستم‌های اطلاعاتی ضروری نیست. هنگامی‌که فقط تغییر کوچکی در برنامه‌ها و سیستم‌های موجود داده می‌شود لازم نیست برآورد تأثیر بر حریم خصوصی انجام شود.

مثال‌هایی از برآورد تأثیر بر حریم خصوصی

جدول ۲-۵ سیستم‌های برآورد تأثیر بر حریم خصوصی را در سه کشور نشان می‌دهند.

جدول ۲-۵ نمونه‌هایی از برآورد تأثیر بر حریم خصوصی در کشورها

	ایالات متحده	کانادا	استرالیا/نیوزیلند
زمینه‌های قانونی	بخش ۲۰۸ از قانون دولت الکترونیکی در سال ۲۰۰۲ اداره مدیریت و بودجه نیازمندی‌های برآورد تأثیر	سیاست‌ها و رهنمودهای خود را در مورد برآورد تأثیر بر حریم خصوصی در ماه می ۲۰۰۲ معرفی کرد. اجرای اجباری برآورد تأثیر	اجرای داوطلبانه (هیچ زمینه قانونی وجود ندارد) کتاب راهنمای برآورد تأثیر بر حریم خصوصی برای پشتیبانی

	بر حریم خصوصی را در سند OMB-M-03-22 مشخص می‌کند.	بر حریم خصوصی بر اساس قانون رایج در حریم خصوصی	از آن (۲۰۰۴، نیوزیلند)، راهنمای برآورد تأثیر بر حریم خصوصی (۲۰۰۴، استرالیا)
حوزه	تمام بخش‌ها و سازمان‌های اجرایی و پیمان‌کارانی که از فناوری اطلاعات استفاده می‌کنند یا وب‌گاه‌هایی را برای تعامل با عموم راه‌اندازی می‌کنند؛ اقدامات مرتبط بین سازمانی، از قبیل آن‌هایی که دولت الکترونیکی را به پیش می‌برند.	تمام برنامه‌ها و خدماتی که سازمان‌های دولتی فراهم می‌کنند.	هیچ وظیفه یا محدودیتی وجود ندارد.
اقدام‌گر	سازمان‌هایی که پروژه‌های دولت الکترونیکی را اجرا می‌کنند و با اطلاعات شخصی سروکار دارند.	سازمان‌های دولتی که برنامه‌ها و خدمات را ایجاد و اداره می‌کنند.	سازمان‌های مرتبط یا با درخواست از سازمان‌های مشاور خارجی
نشر	قرار دادن برآورد تأثیر بر حریم خصوصی در دسترس عموم از طریق وب‌گاه سازمان، نشر در اداره ثبت فدرال، یا دیگر روش‌ها که به دلایل امنیتی یا برای حفاظت از اطلاعات طبقه‌بندی شده، حساس یا خصوصی در یک برآورد، می‌توان آن‌ها را تغییر داد یا از آن‌ها چشم‌پوشی کرد. سازمان‌ها باید یک کپی از برآورد تأثیر بر حریم	قرار دادن خلاصه‌ای از برآورد تأثیر بر حریم خصوصی در دسترس عموم فراهم کردن یک کپی از برآورد تأثیر بر حریم خصوصی نهایی و گزارش آن به دفتر کمیساریای حریم خصوصی به‌منظور دریافت مشاوره یا راهنمایی‌های مناسب با توجه به استراتژی حفاظتی به‌جا.	نتایج معمولاً در دسترس عموم قرار نمی‌گیرد (وظیفه‌ای در خصوص گزارش و انتشار آن وجود ندارد)

	خصوصی را برای هر سیستمی که برایش بودجه درخواست شده به رئیس اداره مدیریت و بودجه تحویل دهند.		

خودآزمایی

۱- اطلاعات شخصی چه تفاوت‌هایی با دیگر انواع اطلاعات دارد؟

۲- چرا باید از اطلاعات شخصی محافظت کرد؟

۳- اهمیت اصول سازمان همکاری و توسعه اقتصادی و سازمان ملل درباره حفاظت از حریم خصوصی در چیست؟

۴- چرا برآورد تأثیر بر حریم خصوصی انجام می‌شود؟

فصل ششم

تأسیس و تیم پاسخ به حوادث امنیتی رایانه‌ای

اهداف این فصل عبارتند از:

- تشریح چگونگی تأسیس و تیم پاسخ به حوادث امنیتی رایانه‌ای (CSIRT)[1] در سطح ملی؛
- ارائه مدل‌های تیم پاسخ به حوادث امنیتی رایانه‌ای از کشورهای مختلف

جرائم سایبری و تهدیدهای گوناگون را در مقابل امنیت اطلاعات باید جدی گرفت چون تأثیر اقتصادی عظیمی دارند. Group-IB که یک شرکت امنیتی روسی است، پیش‌بینی کرده است که بازار جهانی جرائم سایبری به اندازه ۲/۵ میلیارد دلار آمریکا ارزش داشته و تا حد ۷ میلیارد دلار رشد خواهد داشت. طبق بررسی اخیر IDC، تقریباً نیمی از شرکت‌ها با هر اندازه‌ای گزارش داده‌اند که کل تأثیر حاصل از خسارت مالی برای هر رویداد بیش از ۱۰۰,۰۰۰ دلار آمریکا بود، در حالی‌که ۸/۵ درصد از شرکت‌ها خسارت مالی بیش از یک میلیون دلار گزارش کرده‌اند.

تأسیس تیم پاسخ به حوادث امنیتی رایانه‌ای راهی مؤثر برای مقابله و کمینه‌سازی خسارات ناشی از حملات به سیستم‌های اطلاعاتی و نقض امنیت اطلاعات است.

۶-۱ توسعه دادن و عملیاتی کردن یک تیم پاسخ به حوادث امنیتی رایانه‌ای

تیم پاسخ به حوادث امنیتی رایانه‌ای سازمانی است رسمیت یافته و مخصوص که مسئولیت دریافت، بازبینی و پاسخ به گزارش‌های مربوط به حوادث و فعالیت‌های مرتبط با امنیت رایانه‌ها را به عهده دارد. هدف اصلی تیم پاسخ به حوادث امنیتی رایانه‌ای فراهم کردن خدمات رسیدگی به حوادث امنیتی رایانه‌ای جهت کمینه کردن خسارت و امکان بازگشت کارآمد از یک حادثه امنیتی رایانه‌ای است[۶۱].

1- Computer Security Incident Response Team

در سال ۱۹۸۸، اولین شیوع یک کرم به نام موریس رخ داد و این کرم به‌سرعت در سراسر دنیا پخش شد. پس از این واقعه، سازمان پروژه‌های تحقیقاتی پیشرفته دفاعی[1] یک مؤسسه مهندسی نرم‌افزار را بنیان نهاد و سپس سازمان CERT/CC[2] را در دانشگاه کارنِگی ملون و تحت یک قرارداد با دولت آمریکا تأسیس کرد. از آن موقع تا کنون، هر کشوری در اروپا سازمانی مشابه را پایه‌گذاری کرده است. از آنجا که هیچ تیم پاسخ به حوادث امنیتی رایانه‌ای به‌تنهایی نمی‌توانست حوادث مربوط به آسیب‌پذیری‌های وسیع را حل کند، مجمع پاسخ به حادثه و تیم‌های امنیتی (FIRST)[3] در سال ۱۹۹۰ تأسیس گردید. از طریق مجمع پاسخ به حادثه و تیم‌های امنیتی، بسیاری از سازمان‌های امنیت اطلاعات و تیم‌های پاسخ به حوادث امنیتی رایانه‌ای قادر به تبادل‌نظر و به‌اشتراک گذاردن اطلاعات هستند.

انتخاب مدل مناسب برای تیم پاسخ به حوادث امنیتی رایانه‌ای[۶۲]

پنج مدل سازمانی عمومی مختلف برای تیم پاسخ به حوادث امنیتی رایانه‌ای وجود دارد. مدلی را باید به کار گرفت که برای یک سازمان مناسب‌ترین است، یعنی شرایط مختلفی از قبیل محیط، وضعیت مالی و منابع انسانی را در نظر می‌گیرد.

۱- مدل تیم امنیتی (با استفاده از کارکنان موجود در بخش فناوری اطلاعات)

مدل تیم امنیتی یک مدل ویژه برای تیم پاسخ به حوادث امنیتی رایانه‌ای نیست. در واقع، این مدل در نقطه مقابل تیم پاسخ به حوادث امنیتی رایانه‌ای مطلوب قرار می‌گیرد. در این مدل، هیچ سازمان متمرکزی که به آن مسئولیت رسیدگی به حوادث امنیت رایانه‌ای محول شده باشد موجود نیست. در عوض، وظایف رسیدگی به حوادث به‌وسیله مدیران سیستم و شبکه یا توسط متخصصان سیستم‌های امنیتی انجام می‌شود.

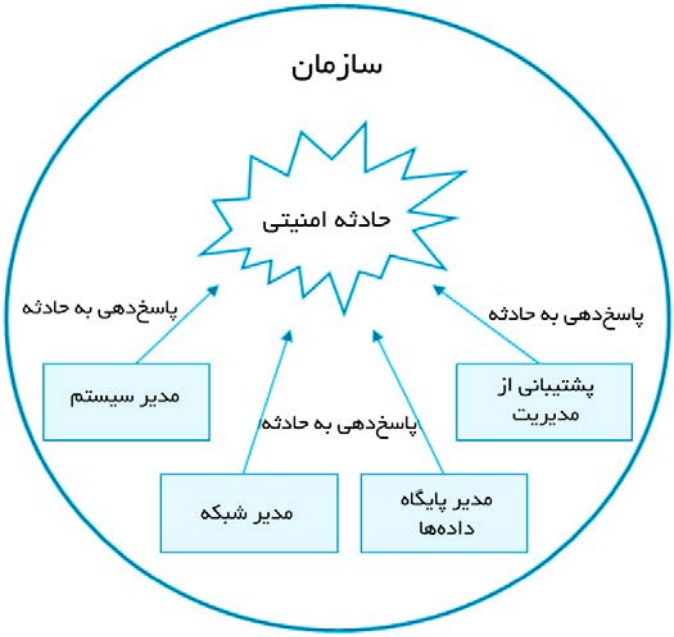
۲- مدل تیم پاسخ به حوادث امنیتی رایانه‌ای توزیع‌شده داخلی

به این مدل "تیم پاسخ به حوادث امنیتی رایانه‌ای توزیع شده" نیز می‌گویند. تیم در این مدل از مدیر تیم پاسخ به حوادث امنیتی رایانه‌ای که مسئول گزارش‌دهی و مدیریت سراسری است و کارکنان بخش‌های دیگر آن سازمان یا شرکت تشکیل می‌شود. تیم پاسخ به حوادث امنیتی رایانه‌ای در این مدل سازمانی رسمیت یافته است که مسئولیت رسیدگی به همه فعالیت‌های پاسخ‌دهی به حوادث را بر عهده دارد. چون این تیم در داخل شرکت یا سازمان تشکیل می‌شود، تیم را به‌عنوان "داخلی" در نظر می‌گیرند.

1- Defence Advanced Research Projects Agency
2- Computer Emergency Response Team/CC
3- Forum of Incident Response and Security Teams

مدل تیم پاسخ به حوادث امنیتی رایانه‌ای توزیع شده داخلی از چند جهت با مدل تیم امنیتی متفاوت است:

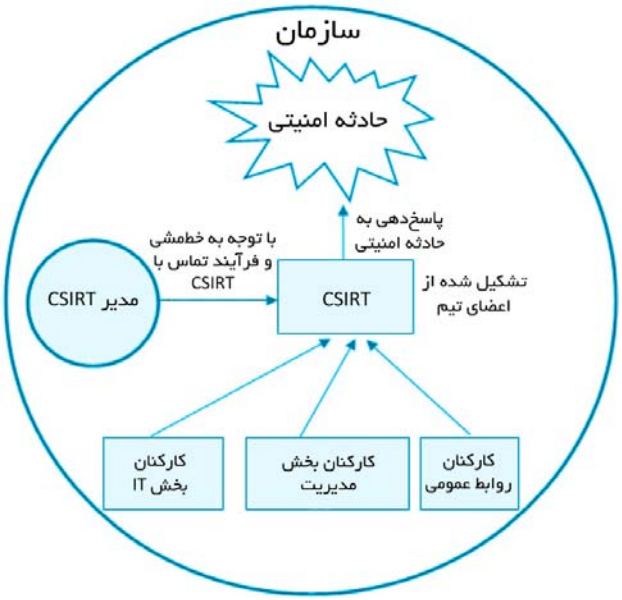
- ✓ وجود خط‌مشی‌ها، رویه‌ها و فرآیندهای رسمی‌تر برای رسیدگی به حوادث
- ✓ روشی تثبیت شده برای ارتباط با کل سازمان با در نظر گرفتن تهدیدهای امنیتی و استراتژی‌های پاسخ‌دهی
- ✓ یک مدیر در تیم پاسخ به حوادث امنیتی رایانه‌ای منصوب شده و به اعضای تیم، وظایف رسیدگی به حوادث محول می‌شود.



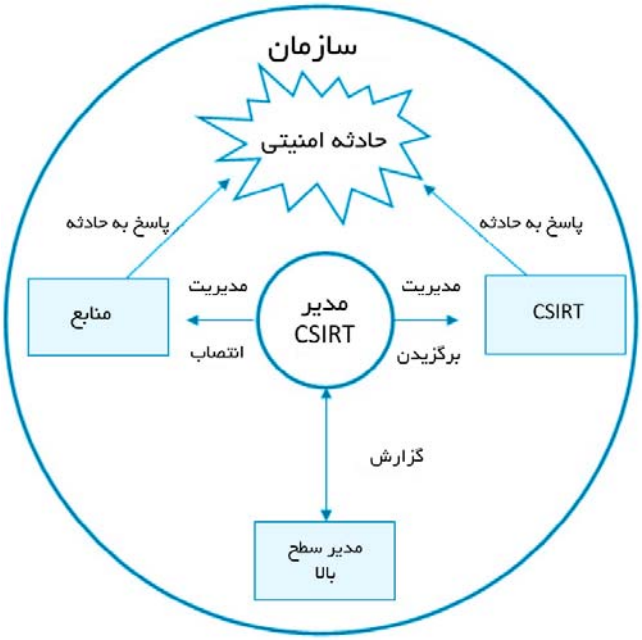
شکل ۱-۶ مدل تیم امنیتی

۳- مدل تیم پاسخ به حوادث امنیتی رایانه‌ای متمرکز داخلی

در مدل تیم پاسخ به حوادث امنیتی رایانه‌ای متمرکز داخلی، یک تیم در موقعیت مرکزی سازمان را کنترل و پشتیبانی می‌کند. تیم پاسخ به حوادث امنیتی رایانه‌ای دارای مسئولیت سراسری برای تمام گزارش‌دهی‌ها، تحلیل‌ها و پاسخ‌های مرتبط با حوادث است. از این رو، اعضای تیم نمی‌توانند به کارهای دیگر بپردازند و تمام وقت خود را صرف کار در تیم و رسیدگی به حوادث می‌کنند. همچنین، مدیر تیم پاسخ به حوادث امنیتی رایانه‌ای به مدیران سطوح بالا در سازمان، از قبیل مدیر اطلاعات، مدیر امنیت یا مدیر ریسک گزارش می‌دهد.



شکل ۲-۶ مدل تیم پاسخ به حوادث امنیتی رایانه‌ای توزیع‌شده داخلی

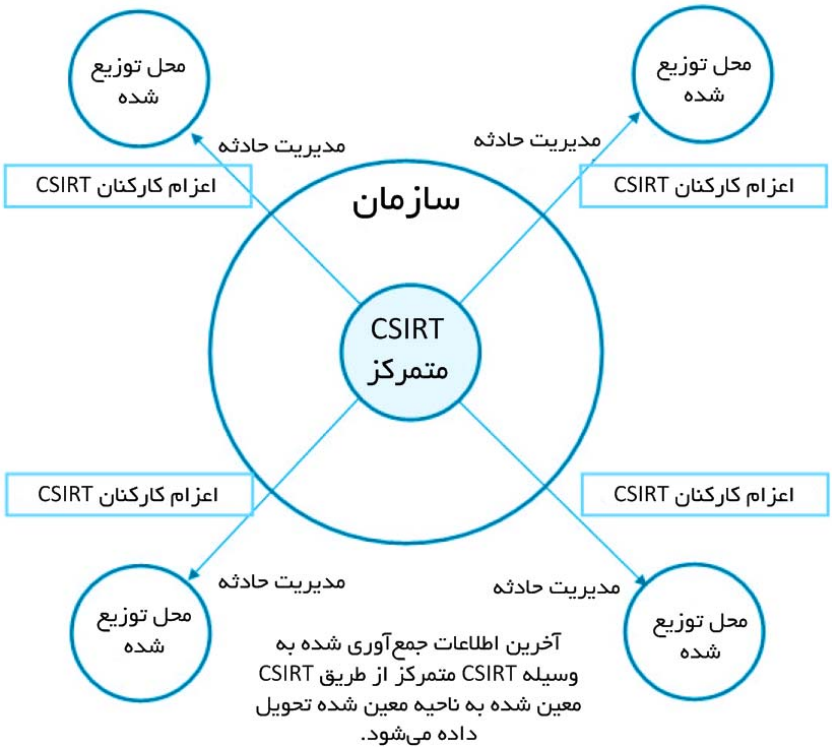


شکل ۳-۶ مدل تیم پاسخ به حوادث امنیتی رایانه‌ای متمرکز داخلی

۴- مدل تیم پاسخ به حوادث امنیتی رایانه‌ای مرکب توزیع شده و متمرکز

این مدل به نام "تیم پاسخ به حوادث امنیتی رایانه‌ای مرکب" نیز شناخته می‌شود. جایی که متمرکز نتواند کل سازمان را کنترل و پشتیبانی کند، بعضی از اعضای تیم در میان سایت‌ها، شعبه‌ها یا بخش‌های سازمان پخش می‌شوند تا در حیطه مسئولیتشان، همان سطح از خدمات را که توسط تیم پاسخ به حوادث امنیتی رایانه‌ای متمرکز ارائه می‌شود ارائه کنند.

تیم متمرکز تحلیل سطح بالای داده‌ها، روش‌های بازیابی و استراتژی‌های مقابله را مهیا می‌کند. این تیم، همچنین اعضای تیم توزیع شده را با پشتیبانی از پاسخ به حوادث، آسیب‌پذیری‌ها و مصنوعات تجهیز می‌کند. اعضای تیم توزیع شده در هر محل استراتژی‌ها را اجرا کرده و تخصصشان را در حیطه کاری خود ارائه می‌کنند.



شکل ۴-۶ تیم پاسخ به حوادث امنیتی رایانه‌ای مرکب

۵- مدل تیم پاسخ به حوادث امنیتی رایانه‌ای هماهنگ‌کننده

تیم پاسخ به حوادث امنیتی رایانه‌ای هماهنگ‌کننده کارکرد تیم‌های توزیع شده را در تیم پاسخ به حوادث امنیتی رایانه‌ای مرکب تقویت می‌کند. در مدل تیم پاسخ به حوادث امنیتی رایانه‌ای هماهنگ‌کننده، اعضای تیم در تیم پاسخ به حوادث امنیتی رایانه‌ای مرکب، بر اساس خصوصیاتی چون اتصالات شبکه، مرزهای جغرافیایی و مانند آن‌ها به تیم پاسخ به حوادث امنیتی رایانه‌های مستقل گروه‌بندی می‌شوند. این گروه‌ها توسط تیم پاسخ به حوادث امنیتی رایانه‌ای متمرکز کنترل می‌شوند.

مدل تیم پاسخ به حوادث امنیتی رایانه‌ای هماهنگ‌کننده برای سیستم ملی تیم پاسخ به حوادث امنیتی رایانه‌ای مناسب است. این مدل می‌تواند برای فعالیت‌های داخلی در یک سازمان و پشتیبانی و هماهنگی دقیق سازمان‌های خارجی به‌کار برود.

فعالیت‌های هماهنگی و تسهیل شامل به‌اشتراک‌گذاری اطلاعات، تهیه استراتژی‌های مقابله، پاسخ به حادثه، روش‌های بازیابی، تحقیق یا تحلیل روندها و الگوهای موجود در حوادث، پایگاه داده‌های آسیب‌پذیری، مراکز دسته‌بندی و توزیع ابزارهای امنیتی و خدمات مشاوره و هشداردهی است.

شکل ۵-۶ تیم پاسخ به حوادث امنیتی رایانه‌ای هماهنگ‌کننده

استقرار تیم پاسخ به حوادث امنیتی رایانه‌ای: گام‌های ایجاد تیم پاسخ به حوادث امنیتی رایانه‌ای ملی[۶۳]

برای استقرار تیم پاسخ به حوادث امنیتی رایانه‌ای پنج مرحله وجود دارد. هدف، دید یا نقش‌های تیم پاسخ به حوادث امنیتی رایانه‌ای باید به‌عنوان یک راهنما در پیمودن این مراحل عمل کنند.

مرحله ۱- آموزش ذی‌نفعان در مورد تشکیل یک تیم ملی

مرحله ۱ مرحله آگاهی است، جایی که ذی‌نفعان به این درک می‌رسند که چه مواردی در تأسیس تیم پاسخ به حوادث امنیتی رایانه‌ای دخیل هستند. از طریق روش‌های آموزشی متنوع، آن‌ها مفاهیم زیر را فرا می‌گیرند:

الف) محرک‌ها و عوامل انگیزاننده در پشت نیاز برای تیم پاسخ به حوادث امنیتی رایانه‌ای ملی

ب) نیازمندی‌های ایجاد توانایی‌های پاسخ‌دهی به حوادث در تیم پاسخ به حوادث امنیتی رایانه‌ای ملی

پ) شناسایی افرادی که باید در بحث‌های مربوط به ساخت تیم ملی درگیر شوند

ت) منابع مهم و زیرساخت‌های حیاتی که در کشور وجود دارند

ث) انواع کانال‌های ارتباطی که باید برای ارتباط با دریافت‌کنندگان خدمات تیم پاسخ به حوادث امنیتی رایانه‌ای تعریف شوند

ج) قوانین، مقررات و دیگر سیاست‌های خاص که تشکیل تیم پاسخ به حوادث امنیتی رایانه‌ای ملی را تحت تأثیر قرار می‌دهند

چ) استراتژی تأمین بودجه که برای توسعه، برنامه‌ریزی، پیاده‌سازی و اداره قابلیت‌های پاسخ‌دهی به‌کار می‌رود

ح) فناوری و زیرساخت‌های اطلاعات شبکه که برای حمایت از عملکرد تیم ملی موردنیاز است

خ) طرح‌های اساسی پاسخ و وابستگی‌های متقابل که در میان بخش‌های مختلف به‌کار گرفته می‌شوند

د) مجموعه بالقوه‌ای از خدماتی که تیم پاسخ به حوادث امنیتی رایانه‌ای می‌تواند برای دریافت‌کنندگان فراهم کند

ذ) بهترین شیوه‌ها و راهنماها

مرحله ۲- برنامه‌ریزی تیم پاسخ به حوادث امنیتی رایانه‌ای: ساخت بر اساس دانش و اطلاعاتی که در حین مرحله ۱ به‌دست آمد

مرحله ۲ شامل برنامه‌ریزی تیم پاسخ به حوادث امنیتی رایانه‌ای بر اساس دانش و اطلاعاتی است که در طی مرحله ۱ به‌دست آمده است. موضوعات بحث شده در مرحله ۱ مرور شده و بیشتر موردبحث قرار می‌گیرند، سپس جزئیات دقیق تعیین شده و در طرح اجرایی به‌کار گرفته می‌شوند. این طرح با در نظر گرفتن موارد زیر تدوین می‌شود:

الف) شناسایی نیازمندی‌ها و نیازهای تیم پاسخ به حوادث امنیتی رایانه‌ای ملی
- ✓ قوانین و مقرراتی که عملکرد تیم ملی را تحت تأثیر قرار می‌دهند
- ✓ منابع حیاتی که باید شناسایی و حفاظت شوند
- ✓ حوادث و روندهای کنونی که گزارش داده می‌شوند یا باید گزارش شوند
- ✓ قابلیت‌های موجود در پاسخ‌دهی به حوادث و تخصص در امنیت رایانه‌ای

ب) تعریف چشم‌انداز تیم پاسخ به حوادث امنیتی رایانه‌ای ملی

پ) تعریف مأموریت تیم ملی

ت) تعیین دریافت‌کننده (دریافت‌کنندگان) خدماتی که خدمات دریافت می‌کنند

ث) شناسایی رابطه‌های ارتباطی بین دریافت‌کنندگان خدمات و تیم ملی

ج) شناسایی انواع تأیید، رهبری یا حمایت ملی (دولتی)

چ) شناسایی انواع مهارت‌ها و دانش کارکنان که برای عملکرد تیم موردنیاز است

ح) تعریف انواع نقش‌ها و مسئولیت‌ها برای تیم پاسخ به حوادث امنیتی رایانه‌ای ملی

خ) مشخص کردن فرآیندهای مدیریت حادثه در تیم پاسخ به حوادث امنیتی رایانه‌ای و نیز تعیین رابطه آن‌ها با فرآیندهای مشابه در هر یک از سازمان‌های تشکیل‌دهنده خارجی

د) توسعه مجموعه‌ای استاندارد از معیارها و اصطلاحات سازگار برای دسته‌بندی و تعریف فعالیت‌ها و رویدادهای مربوط به حادثه

ذ) تعریف چگونگی تعامل تیم پاسخ به حوادث امنیتی رایانه‌ای ملی با دریافت‌کنندگان خدمات یا دیگر تیم پاسخ به حوادث امنیتی رایانه‌های جهانی یا شرکای خارجی

ر) تعیین هر فرآیند موردنیاز برای یکپارچه‌سازی با طرح‌های بازیابی از فاجعه و پاسخ به حادثه، طرح‌های تداوم کسب‌وکار، مدیریت بحران یا دیگر طرح‌های مدیریت اضطراری

ز) تدوین ترتیب زمانی پروژه

ژ) ایجاد طرح تیم پاسخ به حوادث امنیتی رایانه‌ای ملی بر مبنای نتایج خروجی فعالیت‌های برنامه‌ریزی، چشم‌انداز و چارچوب مربوطه

مرحله ۳- پیاده‌سازی تیم پاسخ به حوادث امنیتی رایانه‌ای

در مرحله ۳، تیم پروژه از اطلاعات و طرح حاصل از مراحل ۱ و ۲ برای پیاده‌سازی تیم پاسخ به حوادث امنیتی رایانه‌ای استفاده می‌کند. فرآیند پیاده‌سازی به قرار زیر است:

الف) دریافت بودجه از منابع شناسایی شده در مرحله برنامه‌ریزی

ب) اعلان رسمی به‌طور وسیع در مورد این‌که تیم پاسخ به حوادث امنیتی رایانه‌ای ملی در حال تشکیل است و اطلاعات اضافی را در کجا می‌توان یافت (در مورد پیشرفت توسعه، گزارش نیازها و ...)

پ) رسمی‌سازی سازوکارهای هماهنگی و ارتباط با ذی‌نفعان و دیگر طرف‌های مناسب مرتبط

ت) پیاده‌سازی سیستم‌های اطلاعاتی و زیرساخت شبکه امن برای عملیاتی کردن تیم پاسخ به حوادث امنیتی رایانه‌ای ملی (مثلاً سرورهای امن، برنامه‌های کاربردی، تجهیزات مخابراتی و دیگر منابع پشتیبانی زیرساختی)

ث) تشریح عملیات و فرآیندها برای کارکنان تیم پاسخ به حوادث امنیتی رایانه‌ای، از جمله استاندارد توافق شده در مرحله برنامه‌ریزی و راهنمای گزارش‌دهی

ج) تدوین خط‌مشی‌ها و رویه‌هایی برای دسترسی و کار با تجهیزات تیم پاسخ به حوادث امنیتی رایانه‌ای و تجهیزات شخصی و نیز خط‌مشی‌ها در مورد استفاده قابل‌قبول.

چ) پیاده‌سازی فرآیندها برای تعامل تیم پاسخ به حوادث امنیتی رایانه‌ای ملی با دریافت‌کنندگان خدماتش

ح) شناسایی و استخدام (یا انتصاب مجدد) کارکنان، با به‌دست آوردن آموزش‌های مناسب برای کارکنان تیم پاسخ به حوادث امنیتی رایانه‌ای و نیز تعیین دیگر تلاش‌های کمک‌رسانی برای آموزش و تربیت دریافت‌کنندگان خدمات

مرحله ۴- راه‌اندازی تیم پاسخ به حوادث امنیتی رایانه‌ای

در مرحله عملیاتی، خدمات اساسی که تیم پاسخ به حوادث امنیتی رایانه‌ای ملی باید فراهم کند تعریف شده و کارایی عملیاتی برای استفاده از قابلیت مدیریت حادثه مورد ارزیابی قرار می‌گیرد. بر اساس نتایج، جزئیات عملیاتی تدوین شده و بهبود می‌یابند. فعالیت‌های این مرحله عبارتند از:

الف) اجرای فعالانه خدمات متنوعی که به‌وسیله تیم پاسخ به حوادث امنیتی رایانه‌ای ملی فراهم می‌شوند.

ب) تدوین و پیاده‌سازی سازوکارهایی برای ارزیابی اثربخشی عملکردهای تیم پاسخ به حوادث امنیتی رایانه‌ای ملی

پ) بهبود تیم پاسخ به حوادث امنیتی رایانه‌ای ملی با توجه به نتایج ارزیابی

ت) گسترش رسالت، خدمات و کارکنان تا جایی که مناسب باشد و بتواند برای افزایش خدمت‌رسانی به دریافت‌کنندگان خدمت تقویت شود
ث) ادامه تدوین و گسترش سیاست‌ها و رویه‌های تیم پاسخ به حوادث امنیتی رایانه‌ای

مرحله ۵- همکاری

تیم پاسخ به حوادث امنیتی رایانه‌ای ملی می‌تواند رابطه مورد اعتمادی را با ذی‌نفعان، از طریق عملیات کارآمد (مرحله ۴) ایجاد کند. اما تیم پاسخ به حوادث امنیتی رایانه‌ای ملی همچنین نیاز دارد تا اطلاعات مهم و تجربیات رسیدگی به حادثه را از طریق تبادلات دراز مدت با مؤسسات همکاری‌کننده، تیم پاسخ به حوادث امنیتی رایانه‌های داخلی و تیم پاسخ به حوادث امنیتی رایانه‌های بین‌المللی رد و بدل کند. فعالیت‌های این مرحله عبارتند از:

الف) شرکت در فعالیت‌های به‌اشتراک‌گذاری داده‌ها و اطلاعات و پشتیبانی از تدوین استانداردها برای به اشتراک‌گذاری داده‌ها و اطلاعات بین شرکا، سایر تیم‌های پاسخ به حوادث امنیتی رایانه‌ای، دریافت‌کنندگان خدمات و دیگر متخصصان امنیت رایانه‌ای
ب) شرکت در وظایف سراسری "مراقبت و هشداردهی" برای پشتیبانی از جامعه تیم‌های پاسخ به حوادث امنیتی رایانه‌ای
پ) بهبود کیفیت فعالیت‌های تیم پاسخ به حوادث امنیتی رایانه‌ای با فراهم کردن آموزش، کارگاه‌ها و کنفرانس‌هایی که روند حملات و استراتژی‌های پاسخ را به بحث می‌گذارند
ت) همکاری با دیگران در جامعه برای تدوین مستندات بهترین شیوه‌ها و راهنماها
ث) بازبینی و اصلاح فرآیندهای مدیریت حادثه به‌عنوان قسمتی از فرآیند بهبود مستمر

خدمات تیم پاسخ به حوادث امنیتی رایانه‌ای[۶۴]

خدماتی را که تیم پاسخ به حوادث امنیتی رایانه‌ای ارائه می‌کند، می‌توان به خدمات واکنشی، خدمات کنشگر و خدمات مدیریت کیفیت سرویس دسته‌بندی کرد.

خدمات واکنشی خدمات اصلی تیم پاسخ به حوادث امنیتی رایانه‌ای هستند. این خدمات شامل موارد ذیل هستند:

۱- اعلام خطر و هشدارها: این خدمت شامل فراهم کردن اطلاعات و روش‌های پاسخ برای مواجهه با مشکلاتی از قبیل آسیب‌پذیری‌های امنیتی، اعلام خطر مربوط به نفوذ، ویروس رایانه‌ای یا یک حقه است.

۲- رسیدگی به حوادث: این خدمت شامل دریافت، دسته‌بندی اقدام‌ها و پاسخ به درخواست‌ها و گزارش‌ها و تحلیل و اولویت‌بندی حوادث و رویدادهاست. فعالیت‌های خاص مربوط به پاسخ‌دهی شامل این موارد است:

- ✓ **تحلیل حادثه:** بررسی تمام اطلاعات در دسترس و شواهد و مصنوعات پشتیبانی‌کننده مرتبط با حادثه یا رویداد. هدف این تحلیل، شناسایی دامنه حادثه، وسعت خسارت ایجاد شده به‌وسیله حادثه، ماهیت حادثه و استراتژی‌ها یا ترفندهای پاسخ‌دهی در دسترس است.
- ✓ **جمع‌آوری شواهد قانونی:** جمع‌آوری، حفظ، مستندسازی و تحلیل شواهد مربوط به یک سیستم رایانه‌ای که مورد حمله واقع شده است، به‌منظور تعیین تغییرات لازم در سیستم و کمک در بازسازی رویدادهایی که منجر به حمله شده است.
- ✓ **ردگیری و تعقیب:** شامل ردگیری یا دنبال کردن مسیری است که چگونگی وارد شدن نفوذگر را به سیستم و شبکه‌های مرتبط نشان می‌دهد. این فعالیت شامل ردیابی مبدأ نفوذگر یا شناسایی سیستم‌هایی است که او به آن‌ها دسترسی داشته است.

۳- پاسخ به حادثه در محل: تیم پاسخ به حوادث امنیتی رایانه‌ای کمک مستقیم و در محل را برای متقاضیان فراهم می‌کند تا از یک حادثه بهبودی حاصل کنند.

۴- پشتیبانی از پاسخ به حادثه: تیم پاسخ به حوادث امنیتی رایانه‌ای قربانیان یک حمله را از طریق تلفن، ایمیل، دورنگار یا اسناد کمک و راهنمایی می‌کند تا از حادثه بهبودی حاصل کنند.

۵- هماهنگی برای پاسخ به حادثه: تلاش‌های انجام شده از سوی طرف‌های درگیر در این حادثه هماهنگ می‌شود. این‌ها شامل قربانی حمله، دیگر محل‌های درگیر در حمله و هر محلی که در تحلیل حمله نیازمند کمک باشد، می‌شود. همچنین ممکن است دربرگیرنده طرف‌هایی که قربانی را با فناوری اطلاعات پشتیبانی می‌کنند، از قبیل ارائه‌دهندگان خدمات اینترنت یا سایر تیم‌های پاسخ به حوادث امنیتی رایانه‌ای باشد.

۶- رسیدگی به آسیب‌پذیری‌ها: این شامل دریافت اطلاعات و گزارش‌ها درباره آسیب‌پذیری‌های سخت‌افزاری و نرم‌افزاری، تحلیل اثرات این آسیب‌پذیری‌ها و تدوین استراتژی‌های پاسخ برای تشخیص و ترمیم این آسیب‌پذیری‌ها است.

- ✓ **تحلیل آسیب‌پذیری‌ها:** به تحلیل و بررسی فنی آسیب‌پذیری‌ها در سخت‌افزار یا نرم‌افزار اشاره دارد. این تحلیل ممکن است شامل بازبینی کد منبع، استفاده از یک برنامه اشکال‌یابی برای تعیین محل رخداد آسیب‌پذیری یا سعی در بازتولید مشکل در یک سیستم آزمایشی باشد.
- ✓ **پاسخ به آسیب‌پذیری‌ها:** شامل تعیین پاسخ‌های مناسب به‌منظور رفع یا ترمیم آسیب‌پذیری‌ها است. این خدمت می‌تواند دربرگیرنده اجرای پاسخ با نصب ترمیم‌ها، انجام

تعمیرها یا به‌کاربردن ترفندهایی باشد. همچنین به دیگران در مورد استراتژی‌های مقابله، مشاوره یا اعلام خطرها اطلاع‌رسانی می‌کند.

- ✓ **هماهنگی در پاسخ به آسیب‌پذیری‌ها:** تیم پاسخ به حوادث امنیتی رایانه‌ای قسمت‌های مختلف سازمان یا متقاضیان در مورد آسیب‌پذیری‌ها اطلاع‌رسانی می‌کند و اطلاعات مربوط به چگونگی ترمیم یا رفع آن‌ها را در اختیار این قسمت‌ها می‌گذارد. همچنین تیم پاسخ به حوادث امنیتی رایانه‌ای استراتژی‌های موفقیت‌آمیز در پاسخ به آسیب‌پذیری‌ها را دسته‌بندی می‌کند. فعالیت‌ها شامل تحلیل آسیب‌پذیری یا گزارش‌های مربوط به آسیب‌پذیری و ترکیب تحلیل‌های فنی انجام شده به‌وسیله طرف‌های مختلف است. ضمناً این خدمت می‌تواند شامل نگهداری یک آرشیو خصوصی یا عمومی یا پایگاه دانش از اطلاعات مربوط به آسیب‌پذیری‌ها و استراتژی‌های پاسخ مرتبط باشد.

۷- رسیدگی به مصنوعات: شامل تحلیل، پاسخ، هماهنگی و رسیدگی به مصنوعاتی است که دربرگیرنده ویروس‌های رایانه‌ای، اسب‌های تروایی، کرم‌ها، اسکریپت‌ها و جعبه‌ابزارها است.

- ✓ **تحلیل مصنوعات**: تیم پاسخ به حوادث امنیتی رایانه‌ای یک بررسی و تحلیل فنی را در مورد هر مصنوعی که در یک سیستم یافت شده انجام می‌دهد.
- ✓ **پاسخ به مصنوعات**: شامل تعیین اقدامات مناسب برای تشخیص و حذف مصنوعات از یک سیستم است.
- ✓ **هماهنگی پاسخ به مصنوعات**: شامل تسهیم و ترکیب نتایج تحلیل و استراتژی‌های پاسخ مربوط به مصنوعات با دیگر محققان، تیم‌های پاسخ به حوادث امنیتی رایانه‌ای، فروشندگان و دیگر متخصصان امنیتی است.

خدمات فعالانه[1] برای بهبود زیرساخت‌ها و فرآیندهای امنیتی متقاضیان، قبل از تشخیص هرگونه حادثه یا رویداد انجام می‌گیرد. این خدمات شامل این موارد هستند:

۱- **اعلان‌ها:** این‌ها شامل اعلام خطر نفوذ، هشدارهای مربوط به آسیب‌پذیری‌ها، توصیه‌های امنیتی و مشابه آن است. چنین اعلان‌هایی پیرامون تحولات جدید که در دوره متوسط تا بلند تأثیرگذار هستند، از قبیل آسیب‌پذیری‌های تازه کشف شده یا ابزارهای نفوذگران، به متقاضیان خدمات اطلاع‌رسانی می‌کند. اعلان‌ها به متقاضیان امکان می‌دهد سیستم‌ها و شبکه‌های خود را در مقابل مشکلاتی که تازه کشف شده، قبل از اینکه بتوان از آن‌ها بهره‌برداری کرد، محافظت کنند.

1- Proactive Services

۲- **مراقبت از فناوری:** این خدمت شامل نظارت و مشاهده پیشرفت‌های فنی جدید، فعالیت‌های نفوذگرانه و روندهای مربوطه به‌منظور کمک به شناسایی تهدیدهای آتی است. نتیجه این خدمت می‌تواند نوعی از اصول راهنما یا توصیه‌هایی باشد که بر مسائل امنیتی میان مدت تا دراز مدت متمرکز شده است.

۳- **بازبینی‌ها یا ارزیابی‌های امنیتی:** این خدمت یک بازبینی و تحلیل مشروح از زیرساخت امنیتی یک سازمان، بر اساس نیازمندی‌های تعریف شده به‌وسیله سازمان یا دیگر استانداردهای صنعتی مورد کاربرد فراهم می‌کند.

۴- **پیکربندی و نگهداری از ابزارهای امنیتی، برنامه‌های کاربردی، زیرساخت‌ها و سرویس‌ها:** این خدمت راهنمایی‌های مناسب را درباره چگونگی پیکربندی امن و نگهداری از ابزارها، برنامه‌های کاربردی و زیرساخت‌های رایانشی عمومی مهیا می‌کند.

۵- **ساخت ابزارهای امنیتی:** این خدمت شامل ساخت ابزارهای جدید، نرم‌افزارها، برنامه‌های الحاقی و ترمیم‌هایی است که مخصوص متقاضیان خدمات ساخته شده و توزیع می‌شوند.

۶- **خدمات تشخیص نفوذ:** تیم پاسخ به حوادث امنیتی رایانه‌هایی که این خدمت را ارائه می‌کنند فایل‌های ثبت وقایع سیستم‌های تشخیص نفوذ موجود را مرور کرده، مورد تحلیل قرار داده و برای رویدادهایی که به آستانه تعریف شده آن‌ها رسیده باشند پاسخ مناسب را اجرا می‌کنند.

۷- **انتشار اطلاعات مربوط به امنیت:** این خدمت برای متقاضیان مجموعه جامع و سهل‌الوصولی را فراهم می‌کند که در بهبود امنیت به آن‌ها یاری می‌رساند.

خدمات مدیریت کیفیت امنیت طراحی می‌شوند تا دانش به‌دست آمده از مجموع فعالیت‌های پاسخ به حوادث، آسیب‌پذیری‌ها و حملات را فراهم کنند. این خدمات عبارتند از:

۱- تحلیل ریسک: این خدمت شامل بهبود توانایی تیم پاسخ به حوادث امنیتی رایانه‌ای در برآورد تهدیدهای واقعی، فراهم کردن برآوردهای کمی و کیفی واقع‌بینانه از ریسک‌های مرتبط با دارایی‌های اطلاعاتی و ارزیابی استراتژی‌های حفاظت و پاسخ است.

۲- برنامه‌ریزی تداوم کسب‌وکار و بازگشت از فاجعه: تداوم کسب‌وکار و بازگشتن از فاجعه‌ای که به‌وسیله حملات به رایانه‌ها ایجاد می‌شود از طریق برنامه‌ریزی کافی تضمین می‌گردد.

۳- مشاوره امنیتی: تیم‌های پاسخ به حوادث امنیتی رایانه‌ای ضمناً می‌توانند توصیه‌ها و راهنمایی‌های عملی را برای عملیات کسب‌وکار ارائه کنند.

۴- ایجاد آگاهی: تیم‌های پاسخ به حوادث امنیتی رایانه‌ای می‌توانند آگاهی از امنیت را با شناسایی و فراهم کردن اطلاعات و رهنمودهایی در مورد شیوه‌ها و خط‌مشی‌های امنیتی که متقاضیان نیاز دارند بهبود بخشند.

۵- آموزش و تعلیم: این خدمت شامل فراهم کردن آموزش و تعلیم در موضوعاتی مانند رهنمودهای گزارش‌دهی حوادث، روش‌های پاسخ‌دهی مناسب، ابزارهای پاسخ به حوادث، روش‌های جلوگیری از حادثه و دیگر اطلاعات ضروری برای حفاظت، تشخیص، گزارش و پاسخ به حوادث امنیتی رایانه‌ای است. نوع آموزش می‌تواند شامل سمینارها، کارگاه‌ها، دوره‌های آموزشی و مطالب خودآموز باشد.

۶- ارزیابی یا تأیید محصول: تیم پاسخ به حوادث امنیتی رایانه‌ای می‌تواند ارزیابی‌هایی را بر ابزارها، برنامه‌های کاربردی یا دیگر سرویس‌ها انجام دهد تا از امنیت محصولات و پیروی آن‌ها از شیوه‌های قابل‌قبول تیم پاسخ به حوادث امنیتی رایانه‌ای یا امنیت سازمانی اطمینان حاصل کند.

جدول ۱-۶ سطح هر خدمت تیم پاسخ به حوادث امنیتی رایانه‌ای را در هر مدل تیم پاسخ به حوادث امنیتی رایانه‌ای نشان می‌دهد- یعنی اینکه آیا آن یک خدمت اصلی، افزوده یا نامعمول است.

جدول ۱-۶ خدمات تیم پاسخ به حوادث امنیتی رایانه‌ای

دسته خدمت	خدمات		تیم امنیتی	توزیع شده	متمرکز	مرکب	هماهنگ‌کننده
واکنشی	اعلام خطر و هشدارها		افزوده	اصلی	اصلی	اصلی	اصلی
	رسیدگی به حادثه	تحلیل حادثه	اصلی	اصلی	اصلی	اصلی	اصلی
		پاسخ به حادثه در محل	اصلی	افزوده	افزوده	افزوده	نامعمول
		پشتیبانی از پاسخ به حادثه	نامعمول	اصلی	اصلی	اصلی	اصلی
		هماهنگی پاسخ به حادثه	اصلی	اصلی	اصلی	اصلی	اصلی
	رسیدگی به مصنوعات	تحلیل آسیب‌پذیری	افزوده	افزوده	افزوده	افزوده	افزوده
		پاسخ به آسیب‌پذیری	اصلی	افزوده	نامعمول	افزوده	افزوده
		هماهنگی پاسخ به	افزوده	اصلی	اصلی	اصلی	اصلی

	آسیب‌پذیری						
	تحلیل مصنوعات	افزوده	افزوده	افزوده	افزوده	افزوده	افزوده
	پاسخ به مصنوعات	اصلی	افزوده	افزوده	افزوده	افزوده	افزوده
	هماهنگی پاسخ به مصنوعات	افزوده	افزوده	اصلی	اصلی	اصلی	اصلی
فعال	اعلان‌ها	نامعمول	اصلی	اصلی	اصلی	اصلی	اصلی
	مراقبت از فناوری	نامعمول	افزوده	اصلی	اصلی	اصلی	اصلی
	بازبینی‌ها یا ارزیابی‌های امنیتی	نامعمول	افزوده	افزوده	افزوده	افزوده	افزوده
	پیکربندی و نگهداری ابزارها، برنامه‌های کاربردی، زیرساخت‌ها و سرویس‌های امنیتی	اصلی	افزوده	افزوده	افزوده	افزوده	نامعمول
	ساخت ابزارهای امنیتی	افزوده	افزوده	افزوده	افزوده	افزوده	افزوده
	خدمات تشخیص نفوذ	اصلی	افزوده	افزوده	افزوده	افزوده	افزوده
	انتشار اطلاعات مرتبط با امنیت	نامعمول	افزوده	اصلی	اصلی	اصلی	اصلی
مدیریت کیفیت امنیتی	تحلیل ریسک	نامعمول	افزوده	افزوده	افزوده	افزوده	افزوده
	برنامه‌ریزی تداوم کسب‌وکار و بازیابی از فاجعه	نامعمول	افزوده	افزوده	افزوده	افزوده	افزوده
	مشاوره امنیتی	نامعمول	افزوده	افزوده	افزوده	افزوده	افزوده
	ایجاد آگاهی	نامعمول	افزوده	افزوده	افزوده	افزوده	اصلی
	آموزش و تعلیم	نامعمول	افزوده	افزوده	افزوده	افزوده	اصلی
	ارزیابی یا تأیید محصول	نامعمول	افزوده	افزوده	افزوده	افزوده	افزوده

منبع: Georgia Killcrece, et. al., Organizational Models for Computer Security Incident Response Teams (CSIRTs), http://www.cert.org/archive/pdf/03hb001.pdf, (Pittsburgh, Carnegie Mellon University, 2003).

۲-۶ انجمن‌های تیم پاسخ به حوادث امنیتی رایانه‌ای بین‌المللی

در حال حاضر تعدادی از انجمن‌های تیم پاسخ به حوادث امنیتی رایانه‌ای تخصصی و بین‌المللی وجود دارند که برای پاسخ‌دهی به حوادث امنیتی رایانه‌ای در سراسر دنیا تشکیل شده‌اند. درحالی‌که

تیم پاسخ به حوادث امنیتی رایانه‌ای ملی می‌تواند به حملات پاسخ داده و دیگر وظایفش را انجام بدهد، یک حمله بین مرزی که بیش از دو کشور را تحت‌الشعاع قرار می‌دهد نیازمند توجه انجمن‌های تیم پاسخ به حوادث امنیتی رایانه‌ای بین‌المللی است.

مجمع تیم‌های امنیتی پاسخ به حادثه[۶۵]

مجمع پاسخ به حادثه و تیم‌های امنیتی از مرکز هماهنگی تیم پاسخ اضطراری در رایانه، سازمان‌های دولتی و شرکت‌های امنیتی از ۵۲ کشور تشکیل شده است. اعضای آن شامل ۲۴۸ سازمان، از جمله CERT/CC و US-CERT (از سپتامبر ۲۰۱۱) هستند. مجمع پاسخ به حادثه و تیم‌های امنیتی انجمنی برای به‌اشتراک‌گذاری اطلاعات و همکاری در میان تیم‌های پاسخ‌دهی به حادثه است. اهداف آن راه‌اندازی فعالیت‌های پاسخ به حادثه و حفاظت و ایجاد انگیزش برای همکاری در میان اعضا با فراهم کردن فناوری، دانش و ابزارهایی برای پاسخ به حادثه است. فعالیت‌های مجمع پاسخ به حادثه و تیم‌های امنیتی به شرح زیر است:

- ✓ توسعه و تسهیم بهترین شیوه‌ها، رویه‌ها، ابزارها، اطلاعات و روش‌های فنی برای پاسخ به حادثه و حفاظت؛
- ✓ ترغیب توسعه سیاست‌ها، خدمات و محصولات امنیتی با کیفیت بالا؛
- ✓ پشتیبانی و تدوین رهنمودهای امنیتی مناسب؛
- ✓ کمک به دولت‌ها، شرکت‌ها و مؤسسات آموزشی برای تشکیل یک تیم پاسخ به حادثه و گسترش آن؛
- ✓ تسهیل به اشتراک‌گذاری فناوری، تجربیات و دانش در میان اعضا برای ایجاد محیط الکترونیکی امن‌تر.

مرکز هماهنگی تیم پاسخ اضطراری در رایانه‌ها در آسیا و اقیانوسیه[۶۶]

تیم پاسخ اضطراری رایانه‌ای در آسیا و اقیانوسیه (APCERT)[1] در ماه فوریه ۲۰۰۳ تشکیل شد تا به‌عنوان شبکه‌ای از متخصصان امنیتی خدمت کند، پاسخ‌های ارائه شده به حوادث را تقویت کرده و آگاهی از امنیت را در آسیا و اقیانوسیه بهبود بخشد. اولین کنفرانس تیم‌های پاسخ در این حوزه، در سال ۲۰۰۲ و در کشور ژاپن برگزار شد. یک سال بعد، تیم پاسخ اضطراری رایانه‌ای در آسیا و اقیانوسیه در کنفرانسی در شهر تایپه و با شرکت ۱۴ تیم پاسخ اضطراری از آسیا و اقیانوسیه بنیان نهاده شد. از

1- Asia-Pacific Computer Emergency Response Team

ماه سپتامبر ۲۰۱۱، تیم پاسخ اضطراری رایانه‌ای در آسیا و اقیانوسیه دارای ۱۸ عضو کامل و ۹ عضو عمومی از ۱۸ کشور است.

اعضای تیم پاسخ اضطراری رایانه‌ای در آسیا و اقیانوسیه توافق دارند که امروزه حوادث امنیتی رایانه‌ها بسیار متعدد و پیچیده بوده و کنترل آن‌ها برای هر سازمان یا کشوری دشوار است و این‌که می‌توان با همکاری و مشارکت با دیگر اعضای تیم پاسخ اضطراری رایانه‌ای در آسیا و اقیانوسیه پاسخی مؤثرتر را ایجاد کرد. همانند مجمع پاسخ به حادثه و تیم‌های امنیتی، مهم‌ترین نکته در تیم پاسخ اضطراری رایانه‌ای در آسیا و اقیانوسیه رابطه‌ای مبتنی بر اعتماد بین اعضا برای تبادل اطلاعات و همکاری با یکدیگر است. بنابراین فعالیت‌های تیم پاسخ اضطراری رایانه‌ای در آسیا و اقیانوسیه در جهت اهداف زیر طراحی شده‌اند:

- ✓ گسترش همکاری‌های منطقه‌ای و بین‌المللی در آسیا و اقیانوسیه؛
- ✓ توسعه مشترک اقدامات برای مواجهه با حوادث امنیتی شبکه‌ها در مقیاس بزرگ یا منطقه‌ای؛
- ✓ بهبود تسهیم اطلاعات امنیتی و تبادل فناوری، از جمله اطلاعات پیرامون ویروس‌های رایانه‌ای، اسکریپت‌های بهره‌برداری و غیره؛
- ✓ بهبود پژوهش‌های مشارکتی در مسائل مشترک؛
- ✓ کمک‌رسانی به دیگر تیم‌های پاسخ در منطقه برای پاسخ‌دهی مؤثرتر به حوادث امنیتی رایانه‌ای؛
- ✓ ارائه مشاوره و راه‌حل برای مشکلات حقوقی مرتبط با امنیت اطلاعات و پاسخ به حادثه در منطقه.

مرکز هماهنگی تیم پاسخ اضطراری در رایانه‌ها در دولت‌های اروپایی[۶۷]

مرکز هماهنگی تیم پاسخ اضطراری در رایانه‌ها در دولت‌های اروپایی (EGC) کمیته‌ای غیررسمی است که هم‌پیوند با تیم پاسخ به حوادث امنیتی رایانه‌های دولتی در کشورهای اروپایی است. اعضای آن شامل فنلاند، فرانسه، آلمان، مجارستان، هلند، نروژ، سوئد، سوئیس و انگلستان هستند. نقش‌ها و مسئولیت‌های این نهاد عبارتند از:

- ✓ توسعه مشترک اقدامات برای مواجهه با حوادث امنیتی شبکه‌ها در مقیاس بزرگ یا منطقه‌ای؛
- ✓ ترویج تسهیم اطلاعات و تبادل فناوری مرتبط با حوادث امنیتی و تهدید کدهای مخرب و آسیب‌پذیری؛
- ✓ شناسایی حیطه‌های دانش و تخصص که می‌تواند در گروه به اشتراک گذاشته شود؛
- ✓ شناسایی حیطه‌های پژوهش و پیشرفت مشارکتی در موضوعاتی که موردعلاقه اعضا هستند؛
- ✓ ترویج تشکیل تیم پاسخ به حوادث امنیتی رایانه‌های دولتی در کشورهای اروپایی.

سازمان امنیت شبکه و اطلاعات اروپا[۶۸]

هدف سازمان امنیت شبکه و اطلاعات اروپا (ENISA)[1] گسترش امنیت اطلاعات و امنیت در اتحادیه اروپا از طریق ایجاد فرهنگ امنیت شبکه و اطلاعات است. این سازمان در ماه ژانویه ۲۰۰۴ توسط شورای وزرا و پارلمان اروپا تشکیل شد تا به جرم "فناوری پیشرفته" پاسخ دهد. این سازمان دارای نقش‌های زیر است:

- ✓ ارائه پشتیبانی برای تضمین امنیت اطلاعات و شبکه در میان اعضای سازمان امنیت شبکه و اطلاعات اروپا یا اتحادیه اروپا؛
- ✓ ترویج تبادل پایدار اطلاعات بین ذی‌نفعان؛
- ✓ بهبود هماهنگی وظایف مرتبط با امنیت اطلاعات و شبکه.

از سازمان امنیت شبکه و اطلاعات اروپا انتظار می‌رود که در تلاش‌های بین‌المللی برای مقابله با ویروس‌ها و هک و نیز برقراری نظارت آنلاین بر تهدیدها سهیم باشد.

۶-۳ تیم پاسخ به حوادث امنیتی رایانه‌های ملی

کشورهای متعددی دارای تیم پاسخ به حوادث امنیتی رایانه‌های ملی هستند. جدول ۶-۲ فهرست این کشورها و تیم پاسخ به حوادث امنیتی رایانه‌ای مربوط به آن‌ها را به همراه وب‌گاه هرکدام نشان می‌دهد.

جدول ۶-۲ فهرست تیم پاسخ به حوادث امنیتی رایانه‌های ملی

کشور	نام رسمی	آدرس وب‌گاه
آرژانتین	Computer Emergency Response Team of the Argentine Public Administration	http://www.arcert.gov.ar
استرالیا	Australia's National Computer Emergency Response Team	http://www.cert.gov.au
برزیل	Computer Emergency Response Team Brazil	http://www.cert.br
برونئی دارالسلام	Brunei Computer Emergency Response Team	http://www.brucert.org.bn
کانادا	Canadian Cyber Incident Response Centre	http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx
شیلی	Chilean Computer Emergency Response Team	http://www.clcert.cl
چین	National Computer Network Emergency Response Technical Ream – Coordination Center of China	http://www.cert.org.cn
دانمارک	Danish Computer Emergency Response Team	http://www.cert.dk

1- European Network and Information Security Agency

السالوادر	Response Team for Computer Security Incidents	
فنلاند	Finnish Communication Regulatory Authority	http://www.cert.fi
فرانسه	CERT-Administration	http://www.certa.ssi.gouv.fr
آلمان	CERT-Bund	http://www.bsi.bund.de/certbund
هنگ‌کنگ	Hong Kong Computer Response Coordination Centre	http://www.hkcert.org
مجارستان	CERT-Hungary	http://www.cert-hungary.hu
هند	CERT-In	http://www.cert-in.org.in
اندونزی	Indonesia Security Incident Response Team on Internet Infrastructure	http://www.idsirtii.or.id
ژاپن	JP CERT Coordination Center	http://www.jpcert.or.jp
لیتوانی	LITNET CERT	http://cert.litnet.lt
مالزی	Malaysian Computer Emergency Response Team	http://www.mycert.org.my
مکزیک	Universidad Nacional Autonoma de Mexico	http://www.cert.org.mx
هلند	GOVCERT.NL	http://www.govcert.nl
نیوزیلند	Centre for Critical Infrastructure Protection	http://www.ccip.govt.nz
نروژ	Norwegian National Security Authority	http://www.cert.no
فیلیپین	Philippines Computer Emergency Response Team	http://www.phcert.org
لهستان	Computer Emergency Response Team Polska	http://www.cert.pl
قطر	Qatar Computer Emergency Response Team	http://www.qcert.org
عربستان سعودی	– Computer Emergency Response Team Saudi Arabia	http://www.cert.gov.sa
سنگاپور	Singapore Computer Emergency Response Team	http://www.singcert.org.sg
اسلوونی	Slovenia Computer Emergency Response Team	http://www.arnes.si/english/si-cert
کره جنوبی	CERT Coordination Center Korea	http://www.krcert.or.kr
اسپانیا	IRIS-CERT	http://www.rediris.es/cert
سوئد	Swedish IT Incident Centre	http://www.sitic.se
تایلند	Thai Computer Emergency Response Team	http://www.thaicert.nectec.or.th
تونس	Tuncert – Tunisian Computer Emergency Response Team	http://www.ansi.tn/en/about_agency/about_tuncert.html
ترکیه	TP-CERT	http://www.uekae.tubitak.gov.tr
انگلستان	GovCertUK	http://www.govcertuk.gov.uk
آمریکا	United States Computer Emergency Readiness Team	http://www.us-cert.gov
ویتنام	Viet Nam Computer Emergency Response Team	http://www.vncert.gov.vn

منبع: CERT, "National Computer Security Incident Response Teams", Carnegie Mellon University, http://www.cert.org/csirts/national/contact.html.

فعالیت

آیا در کشور شما تیم پاسخ به حوادث امنیتی رایانه‌ای ملی وجود دارد؟

۱- اگر جواب مثبت است، این تیم را از نظر مدلی که از آن سرمشق گرفته و نحوه کار آن توصیف کنید. برآورد کنید که این تیم چقدر در اجرای وظایفش اثربخش است.

۲- اگر جواب منفی است، تعیین کنید که چه مدلی از تیم پاسخ به حوادث امنیتی رایانه‌ای برای کشور شما مناسب است و توصیف کنید چه موارد برای تأسیس یک تیم اسخ به حوادث امنیتی رایانه‌ای ملی در کشورتان لازم است.

خودآزمایی

۱- وظایف اصلی تیم پاسخ به حوادث امنیتی رایانه‌ای کدامند؟

۲- چه تفاوت‌هایی بین تیم پاسخ به حوادث امنیتی رایانه‌ای بین‌المللی و تیم پاسخ به حوادث امنیتی رایانه‌ای ملی وجود دارد؟

۳- چه نیازمندی‌هایی برای استقرار تیم پاسخ به حوادث امنیتی رایانه‌ای وجود دارد؟

فصل هفتم

چرخه حیات خط‌مشی امنیت اطلاعات

اهداف این فصل عبارتند از:

- مروری بر فرآیند سیاست‌گذاری در امنیت اطلاعات
- بحث پیرامون مسائلی که سیاست‌گذاران باید در هنگام تعیین خطوط مشی برای امنیت اطلاعات در نظر داشته باشند

سیاست‌گذاران باید چند مورد را در نظر داشته باشند که از آن میان می‌توان به منطق یک خط‌مشی، منابع در دسترس، جهت خط‌مشی، نیازمندی‌های قانونی و مرتبط با بودجه و نیز نتایج مورد انتظار خط‌مشی اشاره کرد. در این فصل، این ملاحظات در طی مراحل مختلف سیاست‌گذاری امنیت اطلاعات موردبحث قرار می‌گیرند.

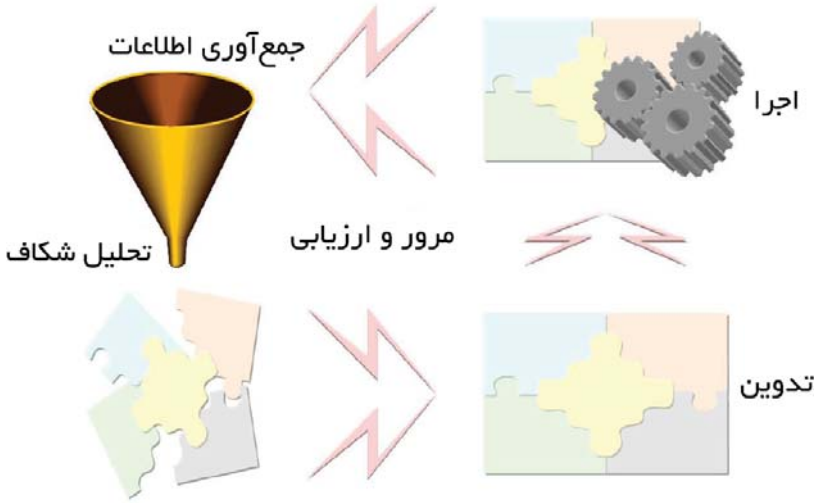
لازم به ذکر است که کشورهای مختلف ملاحظات و زمینه‌های نسبتاً متفاوتی در ارتباط به خطوط مشی دارند. فرآیند سیاست‌گذاری که در این فصل توصیف می‌شود عمومی بوده و بر این فرض استوار است که هیچ خط‌مشی امنیت اطلاعات ملی موجود نیست.

از قبیل دیگر سیاست‌ها، چرخه حیات خط‌مشی امنیت اطلاعات را می‌توان به چهار مرحله تفکیک کرد: (۱) جمع‌آوری اطلاعات و تحلیل شکاف؛ (۲) تدوین خط‌مشی؛ (۳) اجرای خط‌مشی؛ (۴) کنترل و بازخورد (شکل ۱-۷ را مشاهده کنید). به‌علاوه، خط‌مشی ملی امنیت اطلاعات باید شامل استراتژی امنیت اطلاعات، روابط قانونی، سازمان‌دهی امنیت اطلاعات، فناوری امنیت اطلاعات و ارتباط میان آن‌ها باشد.

۱-۷ جمع‌آوری اطلاعات و تحلیل شکاف

اولین مرحله در تنظیم خط‌مشی امنیت اطلاعات جمع‌آوری اطلاعات و تحلیل شکاف است. در جمع‌آوری اطلاعات، مروری بر نمونه‌های امنیت اطلاعات و خط‌مشی‌های مرتبط در دیگر کشورها و نیز خط‌مشی‌های موجود در کشور مفید خواهد بود. در تحلیل شکاف، درک زیرساخت‌های موجود مرتبط با امنیت اطلاعات، از قبیل قوانین و نظام‌های موجود و همچنین حیطه‌ها و شکاف‌هایی که باید پر شوند،

از اهمیت زیادی برخوردار هستند. این مرحله به این دلیل گامی مهم محسوب می‌شود که جهت یا اولویت خط‌مشی امنیت اطلاعات را که باید تدوین شود تعیین می‌کند.



شکل ۱-۷ چرخه حیات خط‌مشی امنیت اطلاعات

جمع‌آوری اطلاعات

جمع‌آوری نمونه‌ها از آن سوی مرزها: در تعیین محل نمونه‌های مربوط در کشورهای دیگر، سیاست‌گذاران باید شباهت‌ها را در موارد زیر در نظر بگیرند:

- ✓ سطح امنیت اطلاعات ملی
- ✓ جهت تدوین خط‌مشی
- ✓ زیرساخت‌های شبکه و سیستم

با ملاحظه این شباهت‌ها، اطلاعات زیر باید گردآوری شوند:

- ✓ اطلاعات مربوط به تأسیس و اداره سازمان‌هایی که درگیر امنیت اطلاعات هستند (فصول ۳ و ۶ را در این کتاب مشاهده کنید).
- ✓ خط‌مشی‌ها، قوانین و مقررات امنیت اطلاعات (فصل ۳ را ببینید)
- ✓ روش‌ها و نمونه‌های امنیت اطلاعات در دیگر کشورها که به‌طور بین‌المللی مورداستفاده قرار می‌گیرند (فصل ۴ را مشاهده کنید)
- ✓ روند تهدیدها و اقدامات متقابل یا کنترلی با توجه به نوع حملات (فصول ۲ و ۶ را ببینید)
- ✓ اقدامات متقابل برای حفاظت از حریم خصوصی (فصل ۵ را مشاهده کنید)

جمع‌آوری اطلاعات از داخل: اگرچه بیشتر سیاست‌گذاران در امنیت اطلاعات متخصص نیستند، اما فعالیت‌هایی را انجام می‌دهند که مربوط یا مرتبط با امنیت اطلاعات است. به‌ویژه، آن‌ها قوانین، مقررات و خط‌مشی‌ها را در حیطه‌های مربوط به امنیت اطلاعات مهارت پیدا می‌کنند. با این حال، چون قوانین، مقررات و خط‌مشی‌ها معمولاً بر زمینه‌های خاص تمرکز دارند، هم‌بستگی میان آن‌ها ممکن است مستقیماً برای سیاست‌گذاران واضح نباشد. بنابراین، نیاز است تا قوانین، مقررات و خط‌مشی‌هایی که مرتبط یا مربوط به امنیت اطلاعات هستند جمع‌آوری و تحلیل گردند.

تحلیل شکاف

سان تزو[1] در کتاب هنر جنگ می‌گوید "دشمنتان را بشناسید". یعنی شما باید از محدودیت‌های خود و دشمنتان آگاه باشید. در مورد سیاست‌گذاری امنیت اطلاعات، این جمله به معنای دانستن مواردی است که باید از طریق خط‌مشی امنیت اطلاعات محافظت شوند و نیز آسیب‌پذیری‌ها و تهدیدهای موجود در امنیت اطلاعات را نیز شامل می‌شود.

تحلیل شکاف را می‌توان به دو مرحله تفکیک کرد:

۱- شناخت توانایی‌ها و ظرفیت‌های کشور- یعنی سازمان و منابع انسانی و نیز زیرساخت‌های اطلاعاتی و ارتباطی- در حیطه عمومی امنیت اطلاعات

۲- شناسایی تهدیدهای خارجی در امنیت اطلاعات

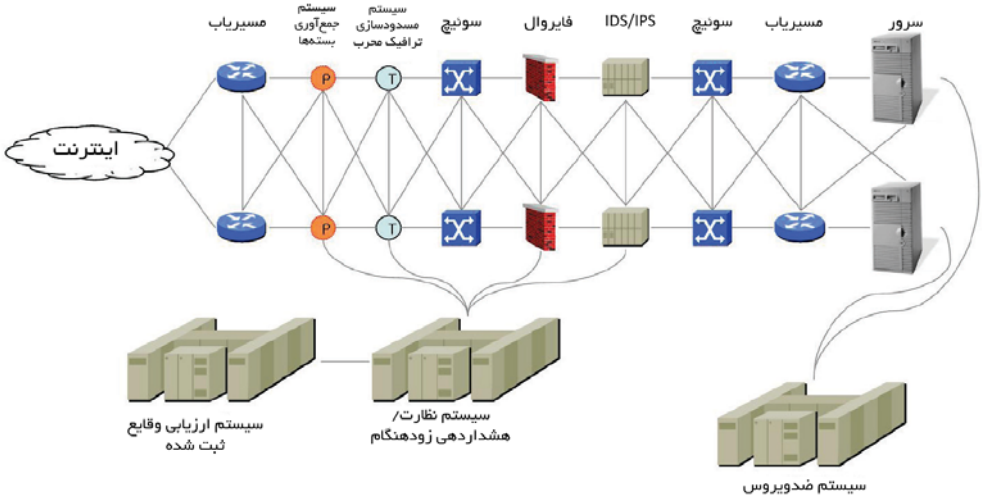
سیاست‌گذاران باید با سازمان امنیت اطلاعات و منابع انسانی آن آشنا باشند که به معنای مؤسسات عمومی و خصوصی در زمینه‌های مرتبط با امنیت اطلاعات است. آن‌ها باید سازمان‌های درگیر در کارهای مرتبط با امنیت اطلاعات را بشناسند و دامنه فعالیت‌ها، نقش‌ها و مسئولیت‌های آن‌ها را درک کنند. این شناخت به‌منظور جلوگیری از ایجاد ساختارهای مضاعف در امنیت اطلاعات حائز اهمیت است.

همچنین در همین زمان است که متخصصان امنیت اطلاعات باید شناسایی شده و برگزیده گردند. این متخصصان معمولاً دارای پیش‌زمینه‌ای در حقوق، سیاست، فناوری، آموزش و زمینه‌های مرتبط هستند.

ساختار فناوری اطلاعاتی که سیستم‌ها و اطلاعات مدیریت کنترل الکترونیکی را جمع‌آوری، پردازش، ذخیره، جست‌وجو، ارسال و دریافت می‌کند، زیرساخت اطلاعاتی-ارتباطی گویند. شناخت وضعیت کنونی زیرساخت اطلاعاتی-ارتباطی مخصوصاً از دیدگاه اقتصادی حائز اهمیت است. چون برای ایجاد اتصال در کل کشور سرمایه‌گذاری بزرگی لازم است، استفاده حداکثری از امکانات اطلاعاتی-ارتباطی سودمند است. شکل ۲-۷ یک زیرساخت نمونه اطلاعاتی-ارتباطی را برای امنیت اطلاعات

[1]- Sun Tzu

نشان می‌دهد. این شکل همه اقلام موردنیاز را شامل نمی‌شود و در اینجا صرفاً با هدف ارائه نمای کلی آورده شده است. به رابطه میان اجزای مختلف شبکه توجه داشته باشید.



شکل ۲-۷ نمونه‌ای از ساختار شبکه و سیستم

سیاست‌گذاران باید درک کنند که شبکه عمومی و سیستم‌های لازم برای امنیت اطلاعات چگونه مستقر می‌شوند.

مرحله دوم در تحلیل شکاف شناسایی تهدیدهای خارجی است که پیش روی امنیت اطلاعات وجود دارد. همان‌گونه که در فصل ۲ ذکر شد، تهدیدهای موجود در امنیت اطلاعات نه تنها در حال افزایش هستند، بلکه مرتباً پیچیده‌تر می‌شوند. سیاست‌گذاران باید این تهدیدها را درک کنند تا بتوانند در مورد اقدامات متقابل ضروری تصمیم‌گیری کنند. به‌ویژه، سیاست‌گذاران باید شناخت صحیحی از موارد زیر داشته باشند:

- ✓ ضریب نفوذ تهدیدها به امنیت اطلاعات
- ✓ رایج‌ترین و جدیدترین انواع حملات
- ✓ انواع تهدیدها و درجه قدرت مورد انتظار آن‌ها در آینده

پس از تحلیل سازمان، منابع انسانی و زیرساخت اطلاعاتی-ارتباطی در کشور و نیز فهم تهدیدها در امنیت اطلاعات، استخراج اجزای آسیب‌پذیر از اهمیت زیادی برخوردار است. این عمل تعیین می‌کند که کشور تا چه حدی توان مقاومت در برابر تهدیدهای خارجی را دارد. تعیین این مهم با بررسی موارد زیر انجام می‌شود:

- ✓ وضعیت فعلی تیم پاسخ اضطراری رایانه‌ای و توانایی آن به انجام واکنش

- ✓ وضعیت فعلی متخصصان امنیت اطلاعات
- ✓ سطح ساخت و نیرومندی نظام امنیت اطلاعات
- ✓ حفاظت قانونی در مقابل تجاوز به دارایی‌های اطلاعاتی
- ✓ محیط فیزیکی برای حفاظت از دارایی‌های اطلاعاتی

هدف تحلیل شکاف این است که اقدامات متقابل عملی که باید انجام شوند شناسایی گردند. لازم به تأکید است که این مرحله اساسی‌ترین گام در سیاست‌گذاری امنیت اطلاعات است.

۷-۲ تدوین خط‌مشی امنیت اطلاعات

تدوین یک خط‌مشی ملی برای امنیت اطلاعات شامل چند مرحله است: (۱) تعیین جهت خط‌مشی؛ (۲) تشکیل سازمان امنیت اطلاعات و تعریف نقش‌ها و مسئولیت‌های آن؛ (۳) تعیین چارچوب خط‌مشی امنیت اطلاعات؛ (۴) بنیان‌گذاری یا اصلاح قوانین برای سازگار کردن آن‌ها با خط‌مشی؛ (۵) تخصیص بودجه برای اجرای خط‌مشی امنیت اطلاعات.

۱- تعیین جهت و مسیر خط‌مشی

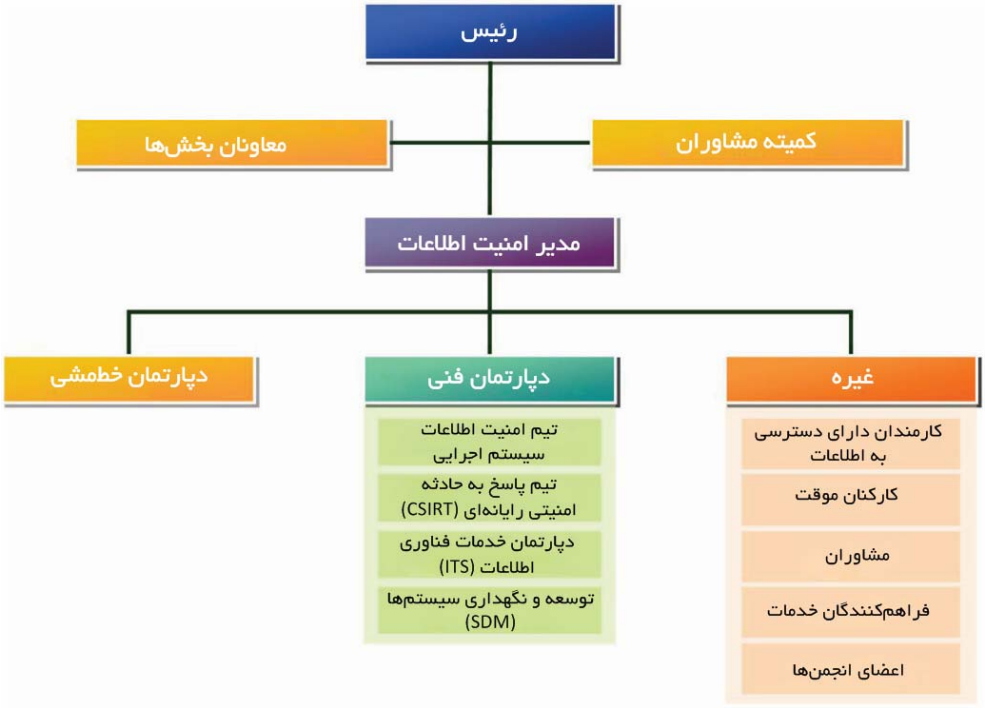
در بیشتر موارد دنبال کردن خط‌مشی باید توسط دولت رهبری شده و به عهده بخش خصوصی گذارده نشود. به‌ویژه، لازم است که دولت خط‌مشی را تنظیم کند، نقش یک رهبر را در ایجاد زیرساخت‌های ضروری ایفا نماید و پشتیبانی دراز مدت را فراهم کند. اساساً، بخش خصوصی برای مشارکت در تحقیق و توسعه و ساخت سیستم، در زمان مقتضی به پروژه ملحق می‌شود.

برنامه‌ریزی برای مشارکت بخش خصوصی شامل فعالیت‌های افزایش آگاهی به‌موازات ساخت و تقویت زیرساخت اطلاعاتی-ارتباطی است. اگر هدف دولت تشویق بخش خصوصی برای پذیرش استراتژی امنیت اطلاعات است، دولت باید نقشی حمایتی را به‌جای نقش کنترلی ایفا کند. این مسأله شامل توزیع رهنمودهای امنیت اطلاعات است.

۲- تشکیل سازمان امنیت اطلاعات و تعریف نقش‌ها و مسئولیت‌های آن[۶۹]

هنگامی‌که جهت حرکت خط‌مشی اطلاعات تعیین شد، سازمان اجراکننده باید تشکیل شود. شکل ۳-۷ نشان‌دهنده ساختار نمونه‌ای از یک سازمان ملی امنیت اطلاعات است.

سازمان‌های ملی امنیت اطلاعات با توجه به ویژگی‌ها و فرهنگ‌های هر کشور تا حدودی متفاوت هستند. با این وجود، یک اصل اساسی این است که اطمینان حاصل شود نقش‌ها و مسئولیت‌ها به‌طور واضح مشخص می‌شوند.



شکل ۳-۷ نمونه یک سازمان ملی امنیت اطلاعات

سازمان اجراکننده

معاونان بخش مسئولیت اولیه را در مورد اطلاعاتی که به‌وسیله بخش آن‌ها جمع‌آوری، نگهداری و استفاده شده یا متعلق به آن بخش است، دارا هستند. این معاونان می‌توانند یک مدیر امنیت اطلاعات یا افرادی دیگر را برای کمک به او برای اجرای خط‌مشی امنیت اطلاعات منصوب کنند. این افراد منصوب شده باید اطمینان حاصل کنند که دارایی‌های اطلاعاتی در محدوده کنترل آن‌ها دارای مالک مشخص باشند، برآورد ریسک انجام شود و فرآیندهای مقابله بر اساس آن ریسک‌ها اجرا گردند.

ناظران (مدیران، راهبران، رؤسا و غیره) کارمندانی را که به اطلاعات و سیستم‌های اطلاعاتی دسترسی دارند مدیریت کرده و اقدامات کنترلی امنیت اطلاعات را برای حیطه تحت نظارتشان تعیین، اجرا و اعمال می‌کنند. آن‌ها باید اطمینان حاصل کنند که همه کارمندان وظایف فردی خود را در ارتباط با امنیت اطلاعات شناخته‌اند و از سطح دسترسی موردنیاز برای انجام کارهایشان برخوردار هستند. ناظران باید به‌طور متناوب سطح دسترسی همه کاربران را بازبینی کنند تا

تضمین گردد که آن‌ها مناسب هستند و اقدامات مقتضی را برای از بین بردن تناقضات و نقایص انجام دهند.

مدیر امنیت اطلاعات[1] (CISO) مسئولیت هماهنگی و نظارت بر خط‌مشی امنیت اطلاعات را بر عهده دارد. این مقام که به‌طور نزدیک با بخش‌های متنوع در ارتباط است، ممکن است توصیه کند که ناظران بخش‌های خاص نمایندگان دیگری را برای نظارت و هماهنگی عناصر خاصی از خط‌مشی برگزینند. مدیر امنیت اطلاعات، همچنین با بهترین شیوه‌های امنیت اطلاعات، به مالکان اطلاعات در زمینه‌های زیر یاری می‌رساند:

- ✓ تدوین و انتشار مقررات قابل‌اعمال درباره دسترسی و استفاده قابل‌قبول از منابع اطلاعاتی
- ✓ اجرا یا هماهنگی برآورد و تحلیل ریسک امنیت اطلاعات
- ✓ تدوین رهنمودها و اقدامات امنیتی منطقی برای حفاظت از داده‌ها و سیستم‌ها
- ✓ کمک در نظارت و مدیریت آسیب‌پذیری‌های امنیتی سیستم‌ها
- ✓ اجرا یا هماهنگی بازبینی امنیت اطلاعات
- ✓ کمک در تحقیقات و برطرف‌سازی مشکلات یا موارد نقض خط‌مشی‌های امنیت اطلاعات

سازمان فنی

تیم اجرایی امنیت اطلاعات سیستم اقداماتی را تدوین و اجرا می‌کنند تا اطمینان حاصل گردد که ذی‌نفعان می‌توانند به اطلاعات دسترسی مناسب داشته باشند در حالی‌که تعهدات ملی قانونی و اخلاقی برای حفاظت از اطلاعات خصوصی، حساس و حیاتی رعایت می‌شوند. این تیم فرآیندها و استانداردهایی را برای فراهم کردن دسترسی‌پذیری بهینه، صحت و محرمانگی اطلاعات اجرایی سیستم تدوین می‌کند که از آن جمله می‌توان به فرآیندهایی برای کاربران جهت درخواست دسترسی اولیه و تغییر دسترسی؛ مستندسازی دسترسی کاربران مجاز و نیز حقوق و مسئولیت‌های کاربر/ناظر؛ و رفع تعارضات و مشکلات مرتبط با امنیت اشاره کرد.

این تیم شامل مدیران امنیت اطلاعات بخش‌ها و مدیر ارشد امنیت اطلاعات است و از سوی مدیران امنیت اطلاعات دپارتمان‌ها و مدیران اجرایی سیستم‌ها مشاوره می‌گیرد.

تیم پاسخ حادثه امنیتی رایانه‌ای برای ذی‌نفعان اطلاعاتی را فراهم کرده و به آن‌ها در اجرای اقدامات کنش‌گرانه کمک می‌کند تا ریسک‌های حوادث امنیت رایانه‌ای را کاهش دهند و در بررسی، پاسخ و کمینه‌سازی خسارت ناشی از حوادث در هنگام رخداد آن‌ها یاری می‌رساند. تیم پاسخ حادثه امنیتی رایانه‌ای همچنین اعمال متعاقب را تعیین و توصیه می‌کند. تیم پاسخ حادثه امنیتی رایانه‌ای دولایه از یک تیم عملیاتی که مسئولیت آن شناسایی اولیه، پاسخ، رده‌بندی و تعیین شرایط

1- Chief Information Security Officer

تشدید است و نیز یک تیم مدیریتی که عهده‌دار راهبری پاسخ ملی به حوادث عمده یا چشمگیر است، تشکیل شده است. مدیر ارشد امنیت اطلاعات و کارکنان عضو بخش فناوری اطلاعات که از سوی خدمات فناوری اطلاعات و توسعه و نگهداری سیستم‌ها عهده‌دار وظیفه شده‌اند قسمتی از تیم عملیاتی هستند. تیم مدیریت تیم پاسخ حادثه امنیتی رایانه‌ای از مدیر ارشد اطلاعات، رئیس پلیس، مدیر اطلاعات عمومی، مدیر خدمات فناوری اطلاعات، مدیر توسعه و نگهداری سیستم‌ها، مدیر ارشد امنیت اطلاعات، مدیر سیستم‌ها و شبکه، یک مشاور حقوقی، یک مشاور منابع انسانی و نمایندگانی با تخصص فنی که به‌طور ویژه از سوی معاونان بخش‌ها منصوب می‌شوند.

کارکنان عضو **دپارتمان خدمات فناوری اطلاعات** شامل مدیران و مهندسان سیستم‌ها و شبکه، ارائه‌دهندگان خدمات فنی مانند مسئول کمک و پشتیبانی در امور فناوری اطلاعات، تکنیسین‌های پشتیبانی از کاربران و مدیران ارتباطات مبتنی بر صدا هستند. آن‌ها مسئول یکپارچه‌سازی ابزارهای امنیتی، اقدامات کنترلی و شیوه‌های اجرایی در محیط شبکه هستند. این کارکنان، گزارش‌های مبنی بر عیوب یا حوادث مشکوک در امنیت اطلاعات را از کاربران دریافت می‌کنند.

کارکنان عضو **بخش توسعه و نگهداری سیستم‌ها** شامل برنامه‌سازان و مدیران پایگاه‌داده هستند. آن‌ها بهترین شیوه‌های امنیتی را برای برنامه‌های کاربردی ملی تدوین، اجرا و یکپارچه‌سازی می‌کنند و سازندگان برنامه‌های مبتنی بر وب را برای به‌کار بستن اصول امنیتی کاربردها آموزش می‌دهند.

دیگران

کارمندان دارای دسترسی به اطلاعات و سیستم‌های اطلاعاتی باید از خط‌مشی‌ها و رویه‌های ملی قابل اجرا و نیز هر شیوه اضافی یا رویه‌های تدوین شده به‌وسیله رئیس واحد یا مدیران آن‌ها تبعیت کنند. این شامل محافظت از رمز عبور حسابشان و گزارش سوءاستفاده مشکوک از اطلاعات یا حوادث امنیت اطلاعات به مراجع ذی‌ربط (معمولاً به ناظرشان) است.

کارکنان موقت به‌عنوان کارمند تلقی می‌شوند و در ارتباط با دسترسی به اطلاعات و سیستم‌های اطلاعاتی دارای مسئولیت‌های یکسانی با کارمندان تمام وقت یا نیمه وقت هستند.

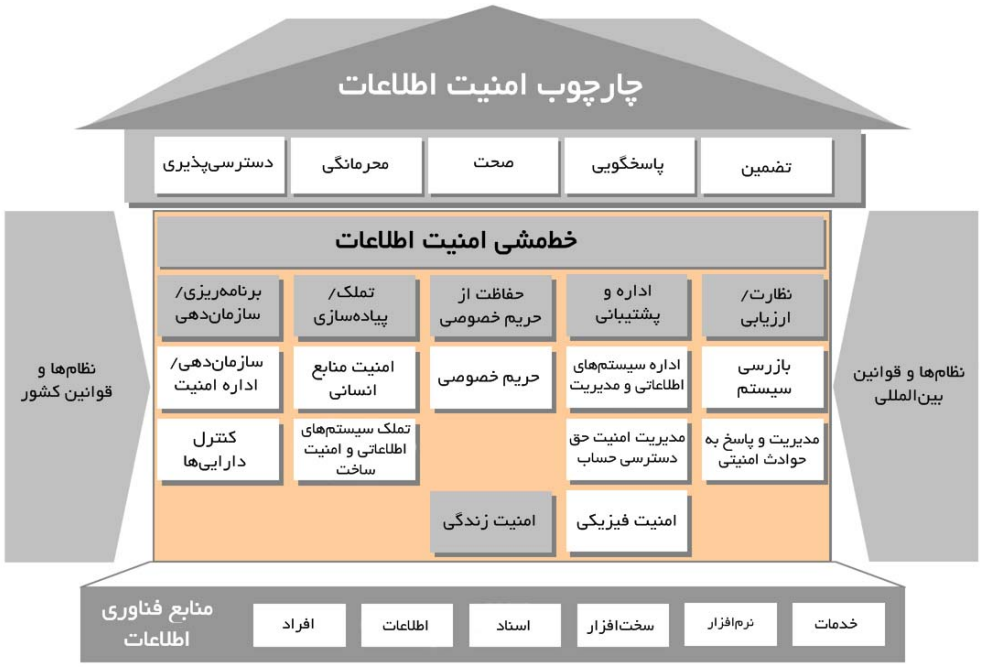
مشاوران، ارائه‌دهندگان خدمت و دیگر طرف‌های دارای قرارداد بر اساس آنچه "نیاز دارند بدانند" به اطلاعات دسترسی خواهند داشت. یک حساب کاربری شبکه که موردنیاز شخص ثالث است باید توسط یک "حامی" در داخل سازمان درخواست شود که تضمین می‌کند آن کاربر شخص ثالث مسئولیت‌های فردی مرتبط با حساب شبکه را درک می‌کند و سپس این درخواست توسط مدیر

یا معاون مربوطه تأیید گردد. آن کاربر باید رمزهای عبورش را امن نگه دارد و مسئولیت هر فعالیتی را که از کاربرد شناسه کاربری او در دامنه معقول کنترل او نشأت می‌گیرد بپذیرد.

۳- تعیین چارچوب برای خط‌مشی امنیت اطلاعات

چارچوب امنیت اطلاعات

چارچوب امنیت اطلاعات پارامترهای لازم در خط‌مشی امنیت اطلاعات را تنظیم می‌کند. این چارچوب تضمین می‌کند که خط‌مشی منابع فناوری اطلاعات (افراد، اسناد اطلاعاتی، سخت‌افزار، نرم‌افزار، خدمات) را در نظر می‌گیرد؛ قوانین و مقررات بین‌المللی را بازتاب می‌دهد و اصول دسترسی‌پذیری اطلاعات، محرمانگی، صحت، پاسخ‌گویی و تضمین اطلاعات را رعایت می‌کند. شکل ۴-۷ یک چارچوب امنیت اطلاعات را نشان می‌دهد.



شکل ۴-۷ چارچوب امنیت اطلاعات

خط‌مشی امنیت اطلاعات مهم‌ترین قسمت چارچوب امنیت اطلاعات است. این خط‌مشی شامل پنج حوزه است که در زیر تشریح می‌شوند:

الف) نقشه و سازمان: این حوزه در برگیرنده سازمان‌دهی و اداره امنیت و نیز طبقه‌بندی و کنترل دارایی‌ها است.

سازمان و عملیات امنیتی این موارد را پوشش می‌دهد:

- ✓ سازمان و سیستم موجود در سازمان امنیت اطلاعات ملی
- ✓ رویه‌های موجود در هر سازمان امنیت اطلاعات
- ✓ تشکیل و مدیریت امنیت اطلاعات کشور
- ✓ همکاری با سازمان‌های بین‌المللی مرتبط
- ✓ همکاری با یک گروه متخصص

طبقه‌بندی و کنترل دارایی‌ها مشتمل بر این موارد است:

- ✓ اعطای مالکیت و استاندارد دسته‌بندی برای دارایی‌های اطلاعاتی با اهمیت
- ✓ دستورالعمل ثبت‌نام و برآورد ریسک دارایی‌های اطلاعاتی با اهمیت
- ✓ مدیریت حقوق دسترسی به دارایی‌های اطلاعاتی مهم
- ✓ نشر و صدور دارایی‌های اطلاعاتی مهم
- ✓ ارزیابی مجدد و بررسی همه‌جانبه دارایی‌های اطلاعاتی مهم
- ✓ مدیریت امنیت اسناد

ب) تملک و پیاده‌سازی: این حوزه در برگیرنده امنیت منابع انسانی و امنیت تملک و توسعه سیستم‌های اطلاعاتی است.

امنیت منابع انسانی شامل تعریف یک روش مدیریتی برای استخدام کارمندان جدید است که موارد ذیل را در بردارد:

- ✓ اقدامات متقابل برای امنیت منابع انسانی و آموزش در زمینه امنیت
- ✓ پردازش مقررات و قوانین مربوط به نقض امنیت
- ✓ مدیریت امنیتی دسترسی شخص ثالث
- ✓ مدیریت امنیتی دسترسی کارکنان برون‌سپاری
- ✓ مدیریت شخص‌های ثالث و کارمندان برون‌سپاری
- ✓ مدیریت امنیتی اتاق و تجهیزات رایانه
- ✓ دسترسی به تأسیسات و ساختمان‌های اصلی
- ✓ پردازش حوادث امنیتی

امنیت تملک و توسعه سیستم‌های اطلاعاتی مستلزم این موارد است:

- ✓ بررسی‌های امنیتی در هنگامی‌که یک سیستم اطلاعاتی تحت تملک در می‌آید
- ✓ مدیریت امنیتی برای برنامه‌های کاربردی داخل و برون‌سپاری شده

- ✓ یک سیستم رمزنگاری ملی (برنامه رمزنگاری، کلید و غیره)
- ✓ آزمایش پس از توسعه نرم‌افزار
- ✓ نیازمندی‌های امنیتی پیشنهادی در هنگام برون‌سپاری ساخت سیستم
- ✓ وارسی امنیتی همراه با توسعه و تملک

ج) حفاظت از حریم خصوصی: شمول حفاظت از حریم خصوصی در خط‌مشی امنیت اطلاعات اجباری نیست. با این وجود، قرار دادن آن یک مزیت است، چون حفاظت از حریم خصوصی موضوعی بین‌المللی است. مقررات حفاظت از حریم خصوصی باید این موارد را پوشش دهد:

- ✓ جمع‌آوری و استفاده از اطلاعات شخصی
- ✓ اجازه اولیه در هنگام استفاده از حریم خصوصی افراد
- ✓ برآورد تأثیر بر حریم خصوصی

د) عملیات و پشتیبانی: این حوزه به امنیت فیزیکی و فنی مرتبط است. استفاده از شبکه و سیستم در جزئیات سامان‌دهی می‌شود و امنیت فیزیکی زیرساخت اطلاعاتی و ارتباطی تعریف می‌گردد.

مدیریت امنیت و عملیات سیستم‌های اطلاعاتی مستلزم این تعریف موارد است:

- ✓ مدیریت امنیت و عملیات سِرور، شبکه، برنامه کاربردی و پایگاه داده
- ✓ توسعه سیستم امنیت اطلاعات
- ✓ ثبت وقایع و پشتیبان‌گیری برای اعمال قانونی
- ✓ مدیریت ذخیره‌سازی اطلاعات
- ✓ رایانش همراه[1]
- ✓ استانداردی برای حفظ و امنیت داده‌های رایانه‌ای
- ✓ خدمات تجارت الکترونیکی

مدیریت امنیت حق دسترسی حساب‌ها: کنترل دسترسی و مدیریت حساب‌ها باید تعریف شوند تا محرمانگی در استفاده از مخزن اطلاعات کشور تضمین شود. این عمل مشتمل بر این موارد است:

- ✓ ثبت، حذف و مدیریت حق دسترسی کاربران به سیستم‌های اطلاعاتی ملی
- ✓ مدیریت حساب و حق دسترسی در شبکه‌های رمزنگاری شده

امنیت فیزیکی: امنیت فیزیکی یعنی حفاظت تأسیسات و تجهیزات اطلاعاتی و ارتباطی که اطلاعات مهم را نگهداری می‌کنند. این موارد عبارتند از:

- ✓ روش‌های پیکربندی و مدیریت امنیت نواحی
- ✓ کنترل دسترسی و انتقال برای مرکز رایانه
- ✓ پیش‌گیری از خسارت‌های طبیعی و دیگر بلایا

[1]- Mobile computing

د) نظارت و ارزیابی: این حوزه از خط‌مشی امنیت اطلاعات نیازمند تنظیم استانداردها و فرآیندهایی برای جلوگیری از حوادث امنیتی و مدیریت و پاسخ‌دهی به حوادث امنیتی است.

بازرسی امنیتی مشتمل بر این موارد است:

- ✓ تدوین طرح بازرسی امنیتی
- ✓ اجرای بازرسی‌های امنیتی دوره‌ای
- ✓ تنظیم و سازمان‌دهی فرم‌های گزارش
- ✓ شناسایی سوژه بازرسی‌های امنیتی و اهداف گزارش

مدیریت و پاسخ به حوادث امنیتی نیازمند تعریف این موارد است:

- ✓ وظیفه و نقش هر سازمان در پردازش حوادث امنیتی
- ✓ رویه‌هایی برای مشاهده و تشخیص علائم حوادث امنیتی
- ✓ رویه‌های پردازش حوادث امنیتی و روش‌های پاسخ‌دهی
- ✓ اقدامات لازم‌الاجرا پس از پردازش حوادث امنیتی

۴- بنیان‌گذاری و اصلاح قوانین برای سازگاری آن‌ها با خط‌مشی امنیت اطلاعات

قوانین باید با خط‌مشی امنیت اطلاعات سازگاری داشته باشند. قوانینی باید وجود داشته باشند که سازمان‌های دولتی و شرکت‌های خصوصی را کنترل کنند. جداول ۱۴ تا ۱۶ قوانین مرتبط با امنیت اطلاعات را در ژاپن، اتحادیه اروپا و ایالات متحده نشان می‌دهند. در ژاپن، قانون فناوری اطلاعات نمونه قانون اساسی در تشکیل جامعه با شبکه‌های پیشرفته اطلاعاتی و مخابراتی است. این قانون استاندارد بنیادی برای امنیت اطلاعات در این کشور است و همه قوانین مرتبط باید از این قانون پیروی کنند.

جدول ۱-۷ قوانین مرتبط با امنیت اطلاعات در ژاپن

قوانین	صنعت هدف	هدف مقررات	مجازات
قانون دسترسی غیرمجاز به رایانه	همه صنایع	عملی که دسترسی غیرمجاز را ترویج کرده و هویت شخص دیگری را بدون اطلاع او در اختیار می‌گذارد	
قانون حفاظت از اطلاعات شخصی	شرکت‌های خصوصی که از اطلاعات شخصی برای اهداف کسب‌وکار استفاده	مدیریت اطلاعات حریم خصوصی (آدرس، شماره تلفن، ایمیل و ...)	مسئولیت جزایی، جریمه نقدی

	می‌کنند.		
قانون امضاها و گواهی‌های الکترونیکی		تسهیل تجارت الکترونیکی که از اینترنت و فعالیت‌های اقتصادی از طریق شبکه‌ها سود می‌برد.	

جدول ۲-۷ قوانین مرتبط با امنیت اطلاعات در اتحادیه اروپا

قوانین	جزئیات
چارچوب قانون‌گذاری مشترک (دستورالعمل 2002/21/EC)	▪ چارچوب ساماندهی شبکه‌ها و خدمات مخابراتی را ارائه می‌کند ▪ قصد حفاظت از حریم خصوصی از طریق شبکه‌های ارتباطی امن دارد
دستورالعمل اتحادیه اروپا درباره حفاظت از داده‌ها (دستورالعمل 1995/46/EC)	▪ رهنمودهایی در مورد پردازش و جابجایی آزادانه اطلاعات شخصی ▪ قانون بنیادی که مسئولیت کشورهای عضو را تعریف کرده و اختیار غایی افراد را بر اطلاعات شخصی به رسمیت می‌شناسد. ▪ سختگیرانه‌تر از استاندارد آمریکا
دستورالعمل اتحادیه اروپا درباره امضای الکترونیکی (دستورالعمل 1999/93/EC) دستورالعمل اتحادیه اروپا درباره تجارت الکترونیکی (دستورالعمل 2000/31/EC)	▪ استفاده از امضاهای الکترونیکی را کنترل می‌کند ▪ انجام تجارت الکترونیکی را سامان‌دهی می‌کند
معاهده جرائم سایبری	▪ جامع‌ترین معاهده بین‌المللی درباره جرم سایبری ▪ تمام اعمال مجرمانه‌ای که از اینترنت استفاده می‌کنند به‌تفصیل تعریف کرده و مجازات‌های مرتبط را مشخص می‌کند

رهنمودهای حفظ داده‌ها در ارتباطات و شبکه‌ها	▪ تأمین‌کنندگان خدمات ارتباطی را ملزم می‌کند که اطلاعات تماس را تا ۶ الی ۲۴ ماه حفظ کنند (بعد از حملات تروریستی در مادرید و لندن به ترتیب در سال ۲۰۰۴ و ۲۰۰۵، رسماً ابلاغ شد)

جدول ۳-۷ قوانین مرتبط با امنیت اطلاعات در آمریکا

قوانین	صنعت هدف	هدف مقررات	مجازات
قانون مدیریت امنیت اطلاعات فدرال ۲۰۰۲	سازمان‌های دولتی فدرال	اطلاعات سازمان‌های دولتی، نظام فناوری اطلاعات، برنامه امنیت اطلاعات	-
قانون حریم خصوصی و مسئولیت‌پذیری در بیمه سلامت ۱۹۹۶	مؤسسات پزشکی و تأمین‌کنندگان خدمات پزشکی	داده‌های الکترونیکی مربوط به اطلاعات پزشکی شخصی	مسئولیت جزایی، جریمه نقدی
قانون گرَم-لیچ-بلایلی ۱۹۹۹	مؤسسات مالی	اطلاعات حریم خصوصی مشتریان	مسئولیت جزایی، جریمه نقدی
قانون ساوبینس-اوکسلی ۲۰۰۲	شرکت‌های فهرست شده در بازار سهام آمریکا	اطلاعات کنترل داخلی و مالی عمومی	مسئولیت جزایی، جریمه نقدی
قانون اطلاعات نقض امنیت پایگاه داده‌های کالیفرنیا ۲۰۰۳	سازمان‌های دولتی و شرکت‌های خصوصی در کالیفرنیا	اطلاعات رمزنگاری شده حریم خصوصی	جریمه نقدی و اطلاع‌رسانی به قربانی

۵- تخصیص بودجه برای اجرای خط‌مشی امنیت اطلاعات

اجرای یک خط‌مشی نیازمند بودجه است. جدول ۴-۷ بودجه امنیت اطلاعات را در ژاپن و ایالات متحده در سال‌های اخیر نشان می‌دهد.

جدول ۴-۷ بودجه امنیت اطلاعات در ژاپن و آمریکا

(واحدها: ژاپن- صد میلیون ین؛ آمریکا- میلیون دلار)

ژاپن	۲۰۰۵	۲۰۰۶	۲۰۰۷	۲۰۰۸	۲۰۰۹
کل بودجه سالانه فناوری اطلاعات	۱۳۰۱۶	۱۳۱۱۵	۱۲۴۸۴	۱۳۵۸۰	-
بودجه امنیت اطلاعات	۲۸۸	۳۱۹	۳۰۰	۳۳۸	-
درصد از کل بودجه فناوری اطلاعات	۲/۲۱	۲/۴۳	۲/۴۰	۲/۴۹	-
آمریکا	**۲۰۰۵**	**۲۰۰۶**	**۲۰۰۷**	**۲۰۰۸**	**۲۰۰۹**
کل بودجه سالانه فناوری اطلاعات	۶۶۲۱۵	۶۶۲۱۵	۶۴۹۱۱	۶۸۳۱۴	۷۰۹۱۴
بودجه امنیت اطلاعات	۳۴۱۱	۵۵۱۲	۵۹۰۵	۶۶۳۱	۷۲۷۸
درصد از کل بودجه فناوری اطلاعات	۵/۱۵	۸/۳۲	۹/۱۰	۹/۷۱	۱۰/۲۶

منبع:. OMB for US figures; and the Japanese Ministry of Internal Affairs and Communications for Japan figures.

فعالیت

اگر کشور شما امنیت اطلاعات دارای خطمشی است، توسعه آن را از نظر پنج جنبه تدوین خطمشی امنیت اطلاعات که در این بخش توصیف شد، دنبال کنید. یعنی این موارد را شرح دهید:

۱- جهت خطمشی

۲- سازمان امنیت اطلاعات

۳- چارچوب خطمشی

۴- قوانین پشتیبانی‌کننده از خطمشی امنیت اطلاعات

۵- تخصیص بودجه برای امنیت اطلاعات

اگر کشور شما هنوز خطمشی‌ای برای امنیت اطلاعات ندارد، به‌طور خلاصه چند امکان را برای هر یک از پنج جنبه بالا جهت تشکیل خطمشی برشمارید. از پرسش‌های زیر به‌عنوان راهنما استفاده کنید:

۱- جهت خطمشی امنیت اطلاعات در کشور شما به کدام سو باید باشد؟

۲- چه ترتیب سازمانی باید استقرار یابد؟ چه سازمان‌هایی باید در تدوین و اجرای خطمشی امنیت اطلاعات در کشور شما درگیر باشند؟

۳- چارچوب خطمشی چه موضوعات خاصی را باید مورد ملاحظه قرار دهد؟

۴- چه قوانینی باید در پشتیبانی از خط‌مشی امنیت اطلاعات، تصویب یا لغو شوند؟
۵- چه ملاحظاتی در ارتباط با بودجه باید موردتوجه قرار گیرد؟ بودجه از کجا باید دریافت شود؟
شرکت‌کنندگان دوره از یک کشور می‌توانند این فعالیت را با همدیگر انجام دهند.

۷-۳ اجرا و پیاده‌سازی خط‌مشی

پیاده‌سازی روان خط‌مشی امنیت اطلاعات به همکاری میان دولت، سازمان‌های خصوصی و بین‌المللی نیازمند است. شکل ۵-۷ حوزه‌های خاصی از پیاده‌سازی خط‌مشی امنیت اطلاعات را نشان می‌دهد که همکاری در آن‌ها حیاتی است.

شکل ۵-۷ حوزه‌های همکاری در پیاده‌سازی خط‌مشی امنیت اطلاعات

تدوین خط‌مشی امنیت اطلاعات

جدول ۵-۷ نشان می‌دهد که چگونه دولت، بخش خصوصی و سازمان‌های بین‌المللی می‌توانند به تدوین خط‌مشی امنیت اطلاعات کمک کنند.

جدول ۵-۷ همکاری در تدوین خط‌مشی امنیت اطلاعات (مثال)

بخش	سهم در تدوین خط‌مشی
دولت	▪ سازمان ملی استراتژی و برنامه‌ریزی؛ تضمین تطابق خط‌مشی با طرح ملی ▪ سازمان فناوری اطلاعات و ارتباطات؛ تضمین همکاری با تدوین استانداردهای فناوری امنیت اطلاعات در کشور ▪ سازمان تحلیل روند امنیت اطلاعات؛ بازتاب روندهای داخلی و بین‌المللی در امنیت و تحلیل آن در خط‌مشی ▪ سازمان تحلیل حقوقی: بررسی تطابق بین خط‌مشی امنیت اطلاعات و قوانین موجود ▪ سازمان ملی اطلاعات: همکاری در تعیین جهت و تدوین استراتژی ▪ سازمان‌های بازرسی: همکاری در پردازش حوادث امنیتی
بخش خصوصی	▪ شرکت‌های مشاوره در امنیت اطلاعات: استفاده از کارشناسان حرفه‌ای در سیاست‌گذاری امنیت اطلاعات ▪ آزمایشگاه فناوری امنیت اطلاعات خصوصی: تدوین استانداردهای فناوری مرتبط با امنیت اطلاعات ▪ گروه امنیت اطلاعات دانشگاه‌ها یا دانشکده‌های تحصیلات تکمیلی: فراهم‌سازی تخصص در تدوین خط‌مشی
سازمان‌های بین‌المللی	▪ تضمین پیروی از استانداردهای بین‌المللی در خط‌مشی ▪ هماهنگی پاسخ به تهدیدها و حوادث بین‌المللی

مدیریت و حفاظت زیرساخت اطلاعات و ارتباطات

استفاده مؤثر (جمع‌آوری، حراست و ...) از اطلاعات نیازمند اداره و حفاظت مناسب از زیرساخت فناوری اطلاعات است. یک خط‌مشی امنیت اطلاعات خوب بدون زیرساخت فناوری اطلاعات سالم، فایده‌ای به همراه نخواهد داشت.

مدیریت و حفاظت اثربخش زیرساخت اطلاعاتی و ارتباطی به همکاری میان مدیران حوزه‌های شبکه، سیستم و فناوری اطلاعات نیاز دارد. همچنین همکاری بین مؤسسات عمومی و خصوصی سودمند است (جدول ۶-۷ را مشاهده کنید).

جدول ۶-۷ همکاری در مدیریت و حفاظت زیرساخت اطلاعات و ارتباطات (مثال)

بخش	سهم در مدیریت و حفاظت زیرساخت اطلاعات و ارتباطات
بخش دولتی	▪ سازمان مرتبط با شبکه‌های اطلاعاتی و ارتباطی: تعریف ترکیب و سطح امنیت شبکه ملی اطلاعات و ارتباطات

	▪ آزمایشگاه فناوری اطلاعات و ارتباطات: توزیع استانداردهای عمومی و به‌کارگیری فناوری قابل‌استفاده
بخش خصوصی	▪ ارائه‌دهنده خدمات اینترنت: همکاری در ساخت شبکه ملی اطلاعات و ارتباطات ▪ آزمایشگاه فناوری اطلاعات و ارتباطات: فراهم‌سازی خدمات توسعه فنی و همکاری در اداره یک زیرساخت پایدار اطلاعات و ارتباطات و فناوری امنیتی
سازمان‌های بین‌المللی	▪ همکاری با سازمان‌های بین‌المللی دارای استاندارد فناوری، برای اطلاعات و ارتباطات بین‌المللی و نیز برای ایمن‌سازی فناوری اطلاعات جدید

پیش‌گیری و پاسخ به تهدیدها و حوادث

پاسخ‌دهی مؤثر به تهدیدها و تخلفات در امنیت اطلاعات نیازمند همکاری در میان سازمان ملی اطلاعات، سازمان‌های بازرسی و مؤسسات حقوقی و نیز سازمان‌هایی که وارسی حوادث امنیتی و برآورد خسارت را انجام می‌دهند، است. همچنین همکاری با سازمانی که بتواند آسیب‌پذیری‌های فنی را تحلیل کرده و اقدامات فنی متقابل را تجویز کند، اهمیت است.

جدول ۷-۷ همکاری در پاسخ به حوادث امنیت اطلاعات (مثال)

بخش	سهم در پاسخ به حوادث امنیت اطلاعات
سازمان‌های دولتی	▪ سازمان پاسخ به حوادث امنیتی: انجام تحلیل‌های موردی، پاسخ به حوادث مربوط به هک کردن، فراهم کردن فناوری برای پاسخ به تخطی‌ها و حوادث ▪ سازمان ملی اطلاعات: تحلیل و تفتیش تخلفات و حوادث مرتبط با امنیت اطلاعات ▪ سازمان‌های بازرسی: همکاری با سازمان‌های درگیر در تعقیب و توقیف متخلفان ▪ سازمان‌های فراهم‌کننده ارزیابی امنیتی: وارسی ایمنی و قابلیت اعتماد شبکه اطلاعات و محصولات مبتنی بر امنیت اطلاعات ▪ سازمان‌های آموزش امنیت اطلاعات: تحلیل عوامل بروز حوادث امنیت اطلاعات و آموزش افراد برای جلوگیری از رخداد مجدد حوادث
بخش خصوصی	▪ سازمان‌های خصوصی پاسخ به حوادث: ارائه پاسخ و پشتیبانی فنی ▪ سازمان‌های بازرسی خصوصی: همکاری با سازمان‌های بازرسی ملی
سازمان‌های بین‌المللی	▪ در صورت بروز تهدیدها و حوادث بین‌المللی، گزارش و همکاری با پلیس بین‌الملل، تیم پاسخ اضطراری رایانه‌ای/معیار مشترک

پیش‌گیری از حوادث امنیت اطلاعات

پیش‌گیری از تخلفات و حوادث در امنیت اطلاعات شامل نظارت، آموزش و مدیریت تغییر است. تیم پاسخ حادثه امنیتی رایانه‌ای ملی مهم‌ترین سازمان ناظر است. مسئله حیاتی تطابقِ خط‌مشی امنیت اطلاعات با داده‌های حقیقی تحت نظارت است. از این رو، بحث در مورد دامنه نظارت بر خط‌مشی امنیت اطلاعات ضروری است. به‌علاوه، آموزش کارمندان دولتی و بخش خصوصی و نیز عامه مردم، در مورد خط‌مشی امنیت اطلاعات از اهمیت زیادی برخوردار است. ممکن است لازم باشد که بعضی از نگرش‌ها به اطلاعات و رفتارهایی که بر امنیت اطلاعات اثرگذارند تغییر یابند. آموزش امنیت اطلاعات و مدیریت تغییر در سند US SP 800-16 (نیازمندی‌های آموزش امنیت فناوری اطلاعات) تعریف شده است.

جدول ۸-۷ همکاری در پیش‌گیری از تخلفات و حوادث امنیت اطلاعات (مثال)

بخش	همکاری و هماهنگی
سازمان‌های دولتی	▪ مأمور نظارت: نظارت پیوسته شبکه و تشخیص پیشرفته تهدیدهای امنیتی ▪ مأمور جمع‌آوری: به‌اشتراک‌گذاری اطلاعات با سازمان‌های بین‌المللی و محل‌های امنیتی ▪ مؤسسات آموزشی: آموزش‌های دوره‌ای به شکل شبیه‌سازی، برای ایجاد توانایی و ظرفیت پاسخ‌دهی سریع به تخلفات و حوادث امنیتی
سازمان‌های خصوصی	▪ ارائه‌دهنده خدمات اینترنت، شرکت‌های کنترل‌کننده امنیت و ارائه‌کننده ضدویروس: ارائه آمار ترافیک، اطلاعات پیرامون نوع حملات و مشخصات کرم‌ها / ویروس‌ها
سازمان‌های بین‌المللی	▪ ارائه اطلاعات در مورد نوع حمله، مشخصات کرم‌ها / ویروس‌ها و موارد مشابه

امنیت حریم خصوصی

برای تدوین اقدامات حفاظتی حریم خصوصی در اینترنت، پیش‌گیری از حوادث مربوط به اطلاعات موقعیت شخصی، حفاظت از اطلاعات بیولوژیکی خصوصی و گزارش نقض حریم خصوصی به همکاری نیاز است.

جدول ۹-۷ همکاری در حفاظت از حریم خصوصی (مثال)

بخش	همکاری و هماهنگی
سازمان‌های دولتی	▪ سازمان‌های تحلیل سیستم: اداره کسب‌وکار مرتبط با اطلاعات خصوصی مبتنی بر محل، تحلیل روندها در حفاظت داخلی و خارجی اطلاعات شخصی

	▪ سازمان برنامه‌ریزی: بهبود قوانین/نظام‌ها، اقدامات فنی و اجرایی و مدیریت استانداردها ▪ پشتیبانی فنی: هماهنگی تأیید کاربر سایبری برای کسب‌وکار ▪ سازمان‌های خدماتی: هماهنگی پشتیبانی برای رفع مشکلات نقض حریم خصوصی و هرزنامه‌ها
سازمان‌های خصوصی	▪ سازمان‌های خصوصی امنیت اطلاعات: ثبت نیازها و سازمان‌دهی مؤسسات همکار برای امنیت اطلاعات شخصی ▪ مشاوره در امنیت اطلاعات شخصی
سازمان‌های بین‌المللی	▪ همکاری برای به‌کارگیری استانداردهای بین‌المللی امنیت اطلاعات شخصی

هماهنگی‌های بین‌المللی

امنیت اطلاعات را نمی‌توان از طریق تلاش‌های یک کشور به‌تنهایی به‌دست آورد، چون تخلفات در امنیت اطلاعات معمولاً دامنه‌ای بین‌المللی دارند. از این رو، هماهنگی بین‌المللی در حفاظت از امنیت اطلاعات، هم در دولت و هم در بخش خصوصی، باید به‌صورت عرف درآید.

برای بخش خصوصی، سازمان بین‌المللی مربوطه برای ترویج و حفاظت از امنیت اطلاعات تیم پاسخ اضطراری رایانه‌ای/معیار مشترک است. در میان دولت‌ها، آژانس امنیت اطلاعات و شبکه اروپا (برای اتحادیه اروپا) و اتحادیه بین‌المللی مخابرات قصد دارند همکاری در امنیت اطلاعات را در میان کشورها ترویج دهند.

در هر کشوری باید یک مؤسسه دولتی وجود داشته باشد که نقش آن تسهیل همکاری سازمان‌های دولتی و خصوصی با سازمان‌ها و مؤسسات بین‌المللی است.

فعالیت

۱- سازمان‌های دولتی و مؤسسات خصوصی را در کشور خود شناسایی کنید که نیازمند همکاری و مشارکت در اجرای خط‌مشی امنیت اطلاعات هستند. همچنین سازمان‌های بین‌المللی را که باید با آن‌ها همکاری کنند مشخص کنید.

۲- در هر کدام از حوزه‌های همکاری در اجرای خط‌مشی امنیت اطلاعات که در شکل ۵-۷ نشان داده شده، اقدامات و فعالیت‌های خاصی را که این سازمان‌ها و مؤسسات می‌توانند انجام دهند مشخص کنید.

شرکت‌کنندگان دوره از کشورهای یکسان می‌توانند این فعالیت را با همدیگر انجام دهند.

۷-٤ بازبینی و ارزیابی خط‌مشی امنیت اطلاعات

گام نهایی در سیاست‌گذاری امنیت اطلاعات ارزیابی خط‌مشی و تکمیل حوزه‌های توسعه‌نیافته است. پس از این‌که میزان اثربخشی خط‌مشی امنیت اطلاعات مشخص شد، بازبینی خط‌مشی ضرورت دارد.

می‌توان یک روش ارزیابی داخلی را برای تعیین اثربخشی خط‌مشی ملی امنیت اطلاعات اجرا کرد. جنبه‌هایی از این روش در ذیل شرح داده می‌شوند:

استفاده از سازمان‌های ممیزی

سازمان‌هایی وجود دارند که نقش آن‌ها اجرای سنجش و ارزیابی خط‌مشی است. چنین سازمانی باید بازرسی‌های منظمی از خط‌مشی ملی امنیت اطلاعات اجرا کند. به‌علاوه، این سازمان باید از سازمان سیاست‌گذار در امنیت اطلاعات و سازمان اجراکننده خط‌مشی مستقل باشد.

بازبینی خط‌مشی امنیت اطلاعات

در طی مرحله ممیزی و بازرسی، حیطه‌های دارای اشکال شناسایی می‌شوند. باید یک فرآیند بازبینی و اصلاح برای رسیدگی به این حیطه‌ها وجود داشته باشد.

تغییرات در محیط

انجام واکنش به تغییرات در محیط خط‌مشی از اهمیت زیادی برخوردار است. تغییراتی که از تهدیدها (حملات) و آسیب‌پذیری‌های بین‌المللی ناشی می‌شوند، تغییرات در زیرساخت فناوری اطلاعات، تغییرات درجه حیاتی بودن اطلاعات و دیگر تغییرات مهم باید بلافاصله در خط‌مشی ملی امنیت اطلاعات بازتاب یابند.

منابع برای مطالعه بیشتر

Butt, Danny, ed. 2005. Internet Governance: Asia-Pacific Perspectives.Bangkok: UNDP-APDIP. http://www.apdip.net/publications/ict4d/igovperspectives.pdf.

CERT. CSIRT FAQ. Carnegie Mellon University.http://www.cert.org/csirts/csirt_faq.html.

_____Security of the Internet. Carnegie Mellon University. http://www.cert.org/encyc_article/tocencyc.html.

Dorey, Paul, and Simon Perry, eds. The PSG Vision for ENISA. Permanent Stakeholders Group, 2006. http://www.enisa.europa.eu/about-enisa/structure-organization/psg/files/psg-vision.

ESCAP. 2007. Module 3: Cyber Crime and Security. In An Introductory Set of Training Modules for Policymakers. Bangkok: United Nations. http://www.unescap.org/idd/pubs/internet-use-for-business-development.pdf.

Europa. Strategy for a secure information society (2006 communication). European Commission.http://europa.eu/legislation_summaries/information_society/internet/l24153a_en.htm.

Information and Privacy Office. Privacy Impact Assessment: A User's Guide. Ontario: Management Board Secretariat, 2001.

Information Security Policy Council. The First National Strategy on Information Security. 2 February 2006. http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.

ISO. ISO/IEC27001:2005. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103.

ITU, and UNCTAD. Challenges to building a safe and secure Information Society. In World Information Society Report 2007, 82-101. Geneva: ITU, 2007. http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/report.html.

ITU-D Applications and Cybersecurity Division. ITU National Cybersecurity / CIIP Self-Assessment Tool. ITU. http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

Killcrece, Georgia. Steps for Creating National CSIRTs. Pittsburgh: Carnegie Mellon University, 2004. http://www.cert.org/archive/pdf/NationalCSIRTs.pdf.

Killcrece, Georgia, Klaus-Peter Kossakowski, Robin Ruefle, and Mark Zajicek. Organizational Models for Computer Security Incident Response Teams (CSIRTs).Pittsburgh: Carnegie Mellon University, 2003. http://www.cert.org/archive/pdf/03hb001.pdf.

OECD. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Paris: OECD, 2002. http://www.oecd.org/dataoecd/16/22/15582260.pdf.

_____OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

Shimeall, Tim and Phil Williams. Models of Information Security Trend Analysis. Pittsburgh: CERT Analysis Center, 2002.http://citeseerx.ist.psu.edu/viewdoc/summary?doi =10.1.1.11.8034.

The White House. The National Strategy to Secure Cyberspace. Washington, D.C.: The White House, 2003. http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.

پیوست‌ها

نکاتی برای مربیان

همانطور که بخشی با عنوان "درباره مجموعه سرفصل‌ها" گفته شد، این سرفصل و دیگر سرفصل‌های این مجموعه به این منظور طراحی شده‌اند که برای مجموعه‌های مختلفی از مخاطبان و در شرایط گوناگون و متغیر دارای ارزش باشند. همچنین، این سرفصل‌ها برای ارائه شدن، به‌طور کلی یا جزئی، در شیوه‌های مختلف، به روش آنلاین یا آفلاین طراحی شده‌اند. سرفصل‌ها می‌توانند به شکل فردی مطالعه شده یا به‌طور گروهی در مؤسسات آموزشی و نیز ادارات دولتی آموزش داده شوند. پیش‌زمینه شرکت‌کنندگان و طول مدت جلسات آموزشی، میزان جزئیات ارائه شده در محتوای آموزشی را تعیین می‌کند.

این یادداشت ایده‌ها و پیشنهادهایی را برای مربیان، در جهت ارائه مؤثرتر محتویات سرفصل فراهم می‌کند. راهنمایی بیشتر در مورد رویکردها و استراتژی‌های آموزشی در کتاب راهنمای طراحی آموزشی که به عنوان ضمیمه برای مجموعه سرفصل‌های *آکادمی مبانی فناوری اطلاعات و ارتباطات برای رهبران دولتی* تدوین شده است، یافت می‌شود. این کتاب راهنما در آدرس http://www.unapcict.org/academy در دسترس است.

ساختار جلسات

برای یک جلسه ۹۰ دقیقه‌ای

مروری بر مفاهیم اساسی و استانداردهای بین‌المللی یا اصول امنیت اطلاعات و حفاظت از حریم خصوصی (فصل‌های ۱ و ۵ از سرفصل) ارائه کنید. نیاز به خط‌مشی مناسب و اثربخش در امنیت اطلاعات و حفاظت از حریم خصوصی را مورد تأکید قرار دهید.

برای یک جلسه سه ساعته

جلسه را به دو بخش تقسیم کنید. در بخش اول، بر مفاهیم اساسی و روندهای امنیت اطلاعات، از جمله شرحی بر تحلیل روند تهدیدها در امنیت اطلاعات (فصل ۲) تمرکز کنید. در بخش دوم، مفاهیم اساسی و اصول حفاظت از حریم خصوصی را مورد توجه قرار دهید، بحثی را پیرامون موضوعاتی

که حفاظت از حریم خصوصی را تحت تأثیر قرار می‌دهند بگویید و به‌طور خلاصه برآورد تأثیر بر حریم خصوصی را توصیف کنید.

برای یک جلسه یک روزه (۶ ساعت)

پس از مرور مفاهیم کلیدی و اصول امنیت اطلاعات و حفاظت از حریم خصوصی، بر تدوین و اجرای خط‌مشی امنیت اطلاعات (فصل ۷) تمرکز کنید. شما می‌توانید با طرح پرسشی از شرکت‌کنندگان در مورد پیامدهای اصول امنیت اطلاعات و حفاظت از حریم خصوصی در خط‌مشی شروع کنید. سپس به‌طور خلاصه چرخه حیات خط‌مشی امنیت اطلاعات را پیش از تمرکز بر فرآیند تدوین خط‌مشی بیان کنید. می‌توانید از شرکت‌کنندگان حاضر از کشورهایی که دارای خط‌مشی امنیت اطلاعات هستند بخواهید تا این خط‌مشی را از حیث اصول و فرآیندهای بحث شده ارزیابی کنند، در حالی‌که از آن‌هایی که از کشورهای بدون خط‌مشی امنیت اطلاعات حضور دارند درخواست کنید تا جنبه‌های چنین خط‌مشیی را به اختصار بیان کنند (فعالیت یادگیری در انتهای بخش ۷-۲ را مشاهده کنید).

برای یک جلسه دو روزه

در روز اول می‌توان آن‌طور که در بالا شرح داده شد عمل کرد، اما در روز دوم می‌توانید بر فعالیت‌ها و روش‌های امنیت اطلاعات (فصل‌های ۳ و ۴)، بویژه تشکیل تیم‌های CSIRT (فصل ۶) تمرکز کنید. مثال‌هایی از دیگر کشورها را می‌توان تشریح کرد و شرکت‌کنندگان باید ترغیب شوند که مناسب‌ترین مدل CSIRT را تعیین کنند و سازوکارهای امنیتی خاص را برای شرایط ملی خود طراحی کنند.

تعامل‌پذیری

داشتن تعامل با مخاطبین و انجام تمرینات عملی اهمیت دارند. این سرفصل اطلاعات مفید فراوانی را مهیا می‌کند، اما شرکت‌کنندگان دوره باید قادر باشند که به‌طور نقادانه این اطلاعات را تحلیل کرده و در جایی که سودمند است به‌کار گیرند. بعضی از مطالعات موردی در این سرفصل ارائه شده‌اند. هر زمان که امکان داشته باشد، می‌توان این موارد را از نظر مفاهیم و اصول امنیت اطلاعات مورد بحث قرار داد. اما شرکت‌کنندگان باید ترغیب شوند که مسائل و مشکلات حقیقی را در امنیت اطلاعات و حفاظت از حریم خصوصی، در شرایط کشور خودشان کاوش کنند.

درباره مؤلف

سازمان اینترنت و امنیت کره[1] (KISA) در سال ۲۰۰۹، با یکپارچه‌سازی سه سازمان مرتبط با فناوری اطلاعات و ارتباطات- سازمان امنیت اطلاعات کره[2] (KISA)، سازمان توسعه اینترنت ملی[3] (NIDA) و سازمان همکاری‌های بین‌المللی در فناوری اطلاعات کره[4] (KIICA)- تأسیس شد. این سازمان وظیفه ترویج، همکاری و تأمین امنیت در اینترنت را به عهده دارد.

در حوزه امنیت اطلاعات، سازمان اینترنت و امنیت کره بر این موارد تمرکز دارد: (۱) ایجاد یک محیط اینترنتی امن؛ (۲) حفاظت از اطلاعات شخصی شهروندان؛ (۳) ارائه راهنمایی در مورد اینترنت و امنیت اطلاعات؛ (۴) حفاظت از زیرساخت اطلاعاتی حیاتی؛ (۵) تقویت امنیت خدمات دولت الکترونیکی؛ (۶) حفاظت از اطلاعات عمومی.

در ترویج اینترنت، تلاش‌های سازمان اینترنت و امنیت کره شامل تدارک یک محیط اینترنتی پایدار، فعال‌سازی عرصه‌های ملی و خلق یک دنیای اینترنتی زیبا است.

برای همکاری در اینترنت، سازمان اینترنت و امنیت کره بر موارد زیر متمرکز می‌شود: (۱) ایجاد ارزشی جدید از طریق همگرایی پخش همگانی و ارتباطات؛ (۲) پشتیبانی از همکاری بین‌المللی در بالا بردن شخصیت پخش همگانی و ارتباطات کره؛ (۳) پشتیبانی از گسترش خدمات و محتوای پخش همگانی و ارتباطات به آن سوی مرزها؛ (۴) فراهم‌سازی اطلاعات بازار جهانی و تقویت ترویج خدمات و محتوای پخش همگانی و ارتباطات به آن سوی مرزها.

http://www.kisa.or.kr

UN- APCICT/ESCAP

مرکز فناوری اطلاعات و ارتباطات توسعه آسیا و اقیانوسیه سازمان ملل (APCICT/ESCAP) بدنه اصلی کمیسیون اجتماعی و اقتصادی سازمان ملل در آسیا و اقیانوس آرام به شمار می‌رود (UN-APCICT/ESCAP) ESCAP کمک می‌کند تا تلاش کشورهای عضو ESCAP در استفاده از فناوری اطلاعات و ارتباطات در توسعه اقتصادی – اجتماعی از طریق ظرفیت‌سازی‌های انسانی و سازمانی تقویت شوند و بر سه محور متمرکز است:

۱- آموزش: افزایش دانش و مهارت‌های فناوری اطلاعات و ارتباطات سیاست‌گذاران و کارشناسان فناوری اطلاعات و ارتباطات و تقویت ظرفیت مربیان و مؤسسات آموزشی فناوری اطلاعات و ارتباطات.

1- Korea Internet & Security Agency
2- Korea Information Security Agency
3- National Internet Development Agency
4- Korean IT International Cooperation Agency

۲- تحقیق: انجام مطالعات تحلیلی مربوط به توسعه منابع انسانی در فناوری اطلاعات و ارتباطات.
۳- مشاوره: ارائه خدمات مشاوره‌ای در زمینه برنامه‌های توسعه منابع انسانی به اعضای ESCAP.

UN.APCICT/ESCAP در اینچئون جمهوری کره واقع شده است.
http://www.unapcict.org

ESCAP

ESCAP بازوی توسعه منطقه‌ای سازمان ملل است و به عنوان مرکز اصلی توسعه اقتصادی و اجتماعی سازمان ملل در منطقه آسیا و اقیانوسیه خدمت می‌کند. دستور کارش ترویج همکاری بین ۵۳ عضو خود و نه عضو همراه است. ESCAP ارتباط استراتژیک بین برنامه‌ها و موضوعات کشوری و جهانی را ارائه می‌دهد و از دولت کشورهای منطقه و رویکردهای منطقه‌ای برای حل چالش‌های اقتصادی-اجتماعی منطقه‌ای در جهان حمایت می‌کنند. اداره ESCAP در بانکوک تایلند واقع شده است.
http://www.unescap.org

آکادمی نیازمندی‌ها فناوری اطلاعات و ارتباطات برای رهبران دولتی

این آکادمی یک فناوری اطلاعات و ارتباطات فراگیر برای دوره آموزشی کامل با ده سرفصل است که کمک می‌کند تا سیاست‌گذاری با دانش و مهارت‌های ضروری تجهیز شوند و بتوانند فرصت‌های ارائه شده از سوی فناوری‌های اطلاعاتی و ارتباطی دست‌یابی به اهداف توسعه و نفوذ و شکاف دیجیتالی را با ایجاد پل می‌کنند. در زیر توضیح کوتاهی از ده سرفصل این آکادمی آورده شده است:

سرفصل ۱- ارتباط بین کاربردهای فناوری اطلاعات و ارتباطات و توسعه هدف‌مند

مسائل کلیدی و نقاط تصمیم‌گیری، از خط‌مشی تا پیاده‌سازی در کاربرد فناوری‌های اطلاعاتی و ارتباطی در دسترسی به MDGها را متمایز می‌کند.

سرفصل ۲- فناوری اطلاعات و ارتباطات برای توسعه سیاست، فرآیند و حاکمیت فناوری اطلاعات و ارتباطات

بر سیاست‌گذاری و حاکمیت ICTD تمرکز دارد و اطلاعات مهمی درباره جنبه‌های سیاست‌ها، استراتژی‌ها و چارچوب‌های ملی ارتقای ICTD ارائه می‌دهد.

سرفصل ۳- کاربردهای دولت الکترونیکی

اصول و مفاهیم دولت الکترونیکی و نمونه‌هایی از برنامه‌های کاربردی را بررسی می‌کند. هم‌چنین به بحث پیرامون تهیه سیستم‌های دولت الکترونیکی و شناسایی ملاحظات طراحی می‌پردازد.

سرفصل ۴- گرایشات فناوری اطلاعات و ارتباطات برای سران دولتی

نگرش‌هایی درباره گرایشات جاری فناوری اطلاعات و ارتباطات و جهت‌گیری‌های آتی آن ارائه می‌دهد. هم‌چنین به ملاحظات کلیدی تکنیکی و سیاسی در هنگام تصمیم‌گیری برای ICTD می‌نگرد.

سرفصل ۵- نظارت بر اینترنت

به بحث پیرامون توسعه سیاست‌ها و روال‌های بین‌الملل ناظر بر استفاده از اینترنت می‌پردازد.

سرفصل ۶- امنیت و محرمانگی اطلاعات

اطلاعاتی پیرامون مسائل و گرایشات امنیتی و فرآیند تدوین استراتژی امنیت اطلاعات ارائه می‌دهد.

سرفصل ۷- مدیریت پروژه فناوری اطلاعات و ارتباطات در عمل و نظر

مفاهیم مدیریت پروژه‌های ICTD شامل روش‌ها، فرآیندها و رشته‌های دانشگاهی مدیریت پروژه را معرفی می‌کند.

سرفصل ۸- گزینه‌های بودجه‌بندی به منظور توسعه فناوری اطلاعات و ارتباطات

گزینه‌های بودجه‌بندی برای پروژه‌های ICTD و دولت الکترونیکی را بررسی می‌کند. به مشارکت بخش‌های خصوصی و دولتی به عنوان گزینه بودجه‌بندی مفید در کشورهای در حال توسعه تأکید می‌شود.

سرفصل ۹- فناوری اطلاعات و ارتباطات برای مدیریت ریسک بلایا

مروری بر مدیریت ریسک بلایا و اطلاعات مورد نیازش دارد و در عین حال به شناسایی فناوری قابل دسترسی جهت کاهش ریسک بلایا و پاسخ به آن‌ها می‌پردازد.

سرفصل ۱۰- فناوری اطلاعات و ارتباطات، تغییرات اقلیمی و رشد سبز

نقش فناوری‌های اطلاعاتی و ارتباطی در مشاهده و پایش محیط، به اشتراک‌گذاری اطلاعات، اقدام به تجهیز، ترویج پایداری محیط زیست و کاهش تغییرات اقلیمی را نشان می‌دهد.

این سرفصل‌ها با مطالعات موردی محلی توسط شرکای آکادمی ملی سفارشی‌سازی می‌شوند. شرکای آکادمی تضمین می‌کنند که این سرفصل‌ها مرتبط هستند و نیاز سیاست‌گذاران در کشورهای مختلف را برآورده می‌سازند. این سرفصل‌ها به زبان‌های مختلف ترجمه شده‌اند تا تضمین کنند که این برنامه مرتبط باقی می‌ماند و گرایشات را ICTD بررسی می‌کند. APCICT به طور منظم این سرفصل‌ها را بازبینی و سرفصل‌های جدید را توسعه می‌دهد.

سرفصل ۱۱- توسعه به‌کمک رسانه اجتماعی

این سرفصل به معرفی مفهوم رسانه اجتماعی و کاربردهای متنوع آن در پیشرفت‌های اجتماعی و اقتصادی می‌پردازد. این سرفصل همچنین به هدایت خط‌مشی رسانه اجتماعی می‌پردازد.

این سرفصل‌ها با مطالعات موردی محلی توسط شرکای آکادمی ملی سفارشی‌سازی می‌شوند. شرکای آکادمی تضمین می‌کنند که این سرفصل‌ها مرتبط هستند و نیاز سیاست‌گذاران در کشورهای مختلف را برآورده می‌سازند. این سرفصل‌ها به زبان‌های مختلف ترجمه شده‌اند تا تضمین کنند که این برنامه مرتبط باقی می‌ماند و روندها را توسعه به‌کمک فناوری اطلاعات و ارتباطات بررسی می‌کند. APCICT به‌طور منظم این سرفصل‌ها را بازبینی و سرفصل‌های جدید را توسعه می‌دهد.

آکادمی مجازی APCICT

آکادمی مجازی APCICT بخشی از سازوکار ارائه چندکاناله است که APCICT در پیاده‌سازی برنامه ظرفیت‌سازی ICTD آکادمی نیازمندی‌ها فناوری اطلاعات و ارتباطات برای سران دولتی به کار می‌رود.

این آکادمی به فراگیران امکان می‌دهد تا به دروس آنلاین دسترسی داشته باشند و دانش خود را در تعدادی از زمینه‌های مهم فناوری اطلاعات و ارتباطات از جمله بهره‌برداری از پتانسیل فناوری‌های اطلاعاتی و ارتباطی برای رسیدن به اجتماعات دورافتاده، افزایش دسترسی به اطلاعات، بهبود ارائه خدمات، ارتقای یادگیری در طول عمر و بالاخره ایجاد پل بین شکاف دیجیتالی و دسترسی به MDGها افزایش دهند.

تمام دروس آکادمی به‌صورت تدریس و تست مجازی هستند که به سادگی قابل پیگیری هستند و به کاربران گواهینامه APCICT مشارکت در تکمیل موفق دروس اعطا می‌شود. تمام

سرفصل‌ها به زبان انگلیسی هستند و نسخه‌های محلی شده به زبان روسی و Bahasa روی اینترنت قابل دسترسند. به‌علاوه، طرح‌های توسعه بیشتر محتوا و محلی‌سازی بیشتر در دست اقدام هستند.

مرکز تشریک مساعی الکترونیکی

مرکز تشریک مساعی الکترونیکی پلت‌فرم آنلاین مختص APCICT برای به اشتراک گذاشتن روی ICTD است. و از طریق دسترسی آسان به منابع مرتبط و فضای اینترنت جهت به اشتراک گذاشتن بهترین درس‌ها و تمرین‌های ICTD به افزایش تجربه یادگیری و آموزش کمک می‌کند. این مرکز موارد زیر را ارائه می‌دهد:

- ✓ یک شبکه به اشتراک‌گذاری دانش و پورتال منابع برای ICTD
- ✓ دسترسی آسان به منابع از طریق سرفصل
- ✓ فرصت بحث‌های آنلاین و تبدیل شدن به بخشی از جامعه تمرین آنلاین مرکز تشریک مساعی الکترونیکی که به اشتراک‌گذاری و توسعه دانش مبتنی بر ICTD کمک می‌کند.

منابع

1- ISO, “ISO/IEC27001:2005”, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103.
2- See (ISC)², “CISSP® - Certified Information Systems Security Professional”, http://www.isc2.org/cissp.
3- Suresh Ramasubramanian, Salman Ansari and Fuatai Purcell, “Governing Internet Use: Spam, Cybercrime and e-Commerce”, in Internet Governance: Asia-Pacific Perspectives, Danny Butt, ed. (Bangkok, UNDP-APDIP, 2005), p. 95, http://www.apdip.net/projects/igov/ICT4DSeries-iGov-Ch5.pdf.
4- Gunter Ollmann, “Understanding the Modern DDoS Threat”, White Paper, Damballa, p. 2, http://www.damballa.com/downloads/r_pubs/WP_Understanding_the_Modern_DDoS_attack.pdf.
5- SearchSecurity.com, “advanced persistent threat (APT)”, http://searchsecurity.techtarget.com/definition/advanced-persistentthreat-APT.
6- This section is drawn from Tim Shimeall and Phil Williams, Models of Information Security Trend Analysis (Pittsburgh, CERT Analysis Center, 2002), http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.11.8034.
7- This sub-section is drawn from CERT, “Security of the Internet”, Carnegie Mellon University, http://www.cert.org/encyc_article/tocencyc.html.
8- Suresh Ramasubramanian, Salman Ansari and Fuatai Purcel, “Governing Internet Use”, p. 94 (see footnote 3).
9- Munir Kotadia, “Email worm graduates to IM”, ZDNet.co.uk, 4 April 2005, http://www.zdnet.co.uk/news/securitymanagement/2005/04/04/email-worm-graduates-to-im-39193674/.
10- Suresh Ramasubramanian, Salman Ansari and Fuatai Purcel, “Governing Internet Use”.
11- Wikipedia, “Zero day attack”, http://en.wikipedia.org/wiki/Zero_day_attack.
12- Nicolas Falliere and Eric Chien, Zeus: King of the Bots, Security Response (Cupertino, CA, Symantec, 2009), p. 1, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf.
13- Wikipedia, “Antivirus software”, http://en.wikipedia.org/wiki/Antivirus_software.
14- SearchSecurity.com, “Intrusion prevention”, TechTarget, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1032147,00.html.

15- The White House, The National Strategy to Secure Cyberspace (Washington, D.C., 2003), http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.
16- Computer Crime and Intellectual Property Section, SEC. 225, Cyber Security Enhancement Act of 2002 (Washington D.C., Department of Justice, 2002), http://www.justice.gov/criminal/cybercrime/homeland_CSEA.htm.
17- OMB, Federal Information Security Management Act: 2004 Report to Congress (Washington, D.C., Executive Office of the President of the United States, 2005), http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/2004_fisma_report.pdf.
18- Europa, "Strategy for a secure information society (2006 communication)", European Commission, http://europa.eu/legislation_summaries/information_society/internet/l24153a_en.htm.
19- Commission of the European Communities, "Critical Information Infrastructure Protection - Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", Communication COM(2009) 149 final, 30 March 2009, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF.
20- Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security (2009/C321/01).
21- European Commission, "A Digital Agenda for Europe", Communication COM (2010) 245, 19 May 2010, http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf.
22- Council Conclusions of 31 May 2010 on Digital Agenda for Europe (10130/10).
23- COM(2010) 2020 and Conclusions of the European Council of 25/26 March 2010 (EUCO 7/10).
24- European Commission, "Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision", Brussels, 30 September 2010, http://www.statewatch.org/news/2010/sep/ceu-com-atacks-on-info-systems-com-517-10.pdf.
25- European Commission, "Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)", Brussels, 30 September 2010, http://www.coe.int/t/dghl/standardsetting/tcy/Proposal%20new%20regulation%20ENISA.pdf.
26- Council of Europe, "Cybercrime: a threat to democracy, human rights and the rule of law", http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp.
27- Paul Dorey and Simon Perry, eds., The PSG Vision for ENISA (Permanent Stakeholders Group, 2006), http://www.enisa.europa.eu/about-enisa/structure-organization/psg/files/psg-vision.

28- This section is drawn from NISC, “Japanese Government’s Efforts to Address Information Security Issues: Focusing on the Cabinet Secretariat’s Efforts”, presentation, November 2007, http://www.nisc.go.jp/eng/.
29- Information Security Policy Council, “The First National Strategy on Information Security: Toward realization of a trustworthy society”, 2 February 2006, p. 5. http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.
30- Ibid., p. 11.
31- World Summit on the Information Society, “Basic Information: About WSIS”, http://www.itu.int/wsis/basic/about.html.
32- World Summit on the Information Society, “Plan of Action”, 12 December 2003, http://www.itu.int/wsis/docs/geneva/official/poa.html.
33- Internet Governance Forum, http://www.intgovforum.org.
34- This section is drawn from WPISP, “Working Party on Information Security and Privacy” (May 2007).
35- OECD, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (Paris, 2002), http://www.oecd.org/dataoecd/16/22/15582260.pdf.
36- Ibid., p. 8.
37- This section is drawn from APEC, “Telecommunications and Information Working Group”, http://www.apec.org/Home/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.
38- “Combating the criminal misuse of information”, which recognizes that one of the implications of technological advances is increased criminal activity in the virtual world.
39- An Agreement undertaken in Budapest that aims to uphold the integrity of computer systems by considering as criminal acts any action that violates said integrity. See http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.
40- This section is drawn from ITU’s website, http://www.itu.int.
41- Suresh Ramasubramanian and Robert Shaw, “ITU Botnet Mitigation Project: Background and Approach”, ITU presentation, September 2007, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit.pdf.
42- ITU-D Applications and Cybersecurity Division, “ITU National Cybersecurity / CIIP Self-Assessment Tool”, ITU, http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.
43- ITU-D Applications and Cybersecurity Division, “Toolkits, Papers and Publications”, ITU, http://www.itu.int/ITU-D/cyb/cybersecurity/.
44- ITU, “ICT Security Standards Roadmap”, http://www.itu.int/ITU-T/studygroups/com17/ict/index.html.
45- ITU-T Study Group 17 (Study period 2009-2012), http://www.itu.int/ITU-T/studygroups/com17/index.asp.
46- ITU, “Study Group 17 at a Glance”, http://www.itu.int/net/ITU-T/info/sg17.aspx.

47- Ibid.
48- FEMA, “FEMA 426 - Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings”, http://www.fema.gov/plan/prevent/rms/rmsp426.
49- Ibid.
50- Common Criteria, http://www.commoncriteriaportal.org.
51- Common Criteria, Common Criteria for Information Technology Security Evaluation, July 2009, CCMB-2009-07-001.
52- Antonius Sommer, “Trends of Security Strategy in Germany as well as Europe”, presentation made at the 2006 Cyber Security Summit, Seoul, Republic of Korea, 10 April 2006, http://www.unapcict.org/ecohub/resources/trends-of-security-strategy-2.
53- Cabinet Office, Privacy and Data-sharing: The way forward for public services (April 2002), http://ctpr.org/wp-content/uploads/2011/03/Privacy-and-data-sharing-the-way-forward-for-public-services-2002.pdf.
54- EurLex, “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data”, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=1995&nu_doc=46.
55- OECD, “Privacy Online: OECD Guidance on Policy and Practice,” http://www.oecd.org/document/49/0,3343,en_2649_34255_19216241_1_1_1_1,00.html.
56- To read the entire document where these principles are listed, see the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.
57- The principles are quoted from the Office of the High Commissioner for Human Rights, “Guidelines for the Regulation of Computerized Personal Data Files”, http://www.unhcr.org/refworld/publisher,UNGA,THEMGUIDE,,3ddcafaac,0.html.
58- Domingo R. Tan, Comment, Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union, 21 LOY. L.A. INT’L & COMP. L.J. 661, 666 (1999).
59- Justice and Home Affairs, “Data Protection”, European Commission, http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.
60- This section is drawn from Information and Privacy Office, Privacy Impact Assessment: A User’s Guide (Ontario, Management Board Secretariat, 2001).
61- CERT, “CSIRT FAQ”, Carnegie Mellon University, http://www.cert.org/csirts/csirt_faq.html.
62- This section is drawn from Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle and Mark Zajicek, Organizational Models for Computer Security Incident Response Teams (CSIRTs) (Pittsburgh, Carnegie Mellon University, 2003), http://www.cert.org/archive/pdf/03hb001.pdf.

63- This section is drawn from Georgia Killcrece, Steps for Creating National CSIRTs (Pittsburgh, Carnegie Mellon University, 2004), http://www.cert.org/archive/pdf/NationalCSIRTs.pdf.
64- This section is drawn from Carnegie Mellon University, CSIRT Services (2002), http://www.cert.org/archive/pdf/CSIRT-serviceslist.pdf.
65- FIRST, “About FIRST”, FIRST.org, Inc., http://www.first.org/about/.
66- APCERT, “Background”, http://www.apcert.org/about/background/index.html.
67- EGC, http://www.egc-group.org.
68- ENISA, “About ENISA”, http://www.enisa.europa.eu/about-enisa.
69- This section is drawn from Sinclair Community College, “Information Security Organization – Roles and Responsibilities”, http://www.sinclair.edu/about/information/usepolicy/pub/infscply/Information_Security_Organization_-_Roles_and_Responsibilities.htm.

UNITED NATIONS
ESCAP /APCICT

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

سازمان فناوری اطلاعات ایران
تهران -خیابان شریعتی - نرسیده به پل سید خندان - ورودی ۲۲
ساختمان مرکزی - کد پستی:۱۶۳۱۷۱۳۹۳۱
تلفنخانه: ۸۴۸۰۲۰۰۲
www.itc.ir

۹۷۸-۶۰۰-۷۶۳۱-۰۷-۲