جزوه درس معماری امنیت

زهرا میثاقیان
Farahani_mr@yahoo.com

مقدمه

بطور کلی مقولهٔ امنیت فناوری اطلاعات به موضوعات زیر اشاره دارد:

۱-امنیت رایانه : امنیت از نظر فنی در ماشینها، نرم افزار ، داده ها و شبکه ها است که بیشتر بر روی ابعاد فیزیکی، زیرساختی و فنی امنیت فناوری تأکید دارند.

۲- امنیت سایبر [1]: امنیت فناوری اطلاعات وابسته به سیاست دولت ها است . این اصطلاح عموما توسط مؤسسات دولتی و سیاستگذاران ملی در اسناد، قوانین و پروژه های تحقیقاتی استفاده می شود و کما بیش مترادف با" امنیت اینترنت " است. هر دو عبارت به جوانب امنیت شبکه و اصول سیاستگذاری شبکه ها مثل تعریف حریم خصوصی، جرائم سایبر، تجارت و ارتباطات جهانی اشاره دارند . تفاوت این دو اصطلاح چندان زیاد نیست؛ بلکه امنیت رایانه ها، شبکه ها و داده ها تا حد زیادی با مفاهیم روزمرهٔ امنیت در فضای سایبر به هم گره خورده اند.

راهنمای امنیت فناوری اطلاعات:

راهنمای امنیت فناوری اطلاعات ، راهنمایی کاربردی جهت فهم و اجرای گام های دستیابی به امنیت در کاربردهای حوزهٔ فناوری اطلاعات در منزل و محل کار شما است . در این درس بطور خلاصه مطالب زیر ارائه می شود:

۱-سازگارسازی فناوری اطلاعات و ارتباطات در حال افزایش است:

این درس در ابتدا مروری بر رشد بخش فناوری اطلاعات وارتباطات ICT دارد. این رشد و ارتقا کاربران عادی (ICT)را در بر می گیرد و از افزایش تعداد شبکه های خانگی و رشد سازمانهای کوچک و متوسط برای پشتیبانی از بازارهایی که به شدت به توسعه فناوری و بکارگیری آن درسراسر جهان وابسته اند و متکی به منابع رایانه ای می باشند می‌توان به آن پی برد.

۲-اطلاعات موجود از سوابق فعالیتهای تأمین امنیت فناوری اطلاعات:

از آنجا که توسعه بازار محصولات و خدمات فناوری در دو سطح فردی و سازمانی چشم گیر است، اطلاع از مباحث امنیت فناوری اطلاعات بسیار مفید و مهم می باشد . ممکن است کاربران فردی در مورد خطراتی که هنگام استفاد ه از اینترنت متوجه آنها است مطلع نباشند . اگر کاربران خطرات شبکه های حفاظت نشده را تشخیص دهند، باز هم ممکن، است یادگیری در مورد دیواره های آتش ، ویروس یاب ها، رمزگذاری و نگهداری سازمان یافته از اطلاعات را به دلیل هزینه و وقتی که از آنها می گیرد و تغییری که در رفتار رایانه ای آنها ایجاد می کند به تعویق بیاندازند . علاوه بر این سازمانهای کوچک و متوسط ممکن است از یک راه حل فنی نظیر دیوارهٔ آتش

[1] -Cyber-Security

استفاده نمایند و به طبقه بندی سطوح امنیت توجهی نداشته باشند و ندانند که بدون توجه به آن، امنیت سیستم به شدت دچار مخاطره است . همچنین ممکن است به دلایل مختلف ایمن ساختن سیستم های خود را به تأخیر بیاندازند و در تدوین سیاستهای شفاف امنیتی برای کاربران و مدیران نیز کوتاهی کنند . اگر ارتباطات، آگاهی و آموزش مناسب در سازمان وجود نداشته باشد، تبهکاران ممکن است به آسانی حفاظهای فنی را پشت سر بگذارند.

۳-دستگاههای سیار ، نرم افزار های رایج کاربردی، و تهدیداتی که موجب ایجاد پیچیدگی می‌شوند:
در حال حاضر کاربران جدید و غیرمتخصص تنها علت نقض امنیت فناوری اطلاعات نیستند . محیط فناوری اطلاعات و ارتباطات با پیدایش محصولات جدید خصوصا دستگاههای سیار مانند رایانه های کیفی، تلفنهای همراه و PDA[۲] ها چالشهای متفاوتی را در زیرساخت و امنیت داده ها ایجاد می کنند بسرعت رو به تغییر می باشد . پیدایش برنامه های کاربردی رایانهای برای سرمایه گذاری الکترونیکی و تجارت الکترونیک نیز موجب بروز پیچیدگی هایی در محیطهای شبکه‌ای شده اند. از هنگام ظهور دستگاههای خودپرداز گرفته تا زمان رواج بانکداری اینترنتی[۳]، این قابلیتها موجب صرفه جویی مناسب در هزینه ها می شوند، اما تهدیدات و خطرات بالقوهای نیز به همراه دارند. آنچه که اوضاع را بدتر می کند این است که اکنون نفوذگران قادر به توسعه و گسترش تهدیدات خود می باشند : مثل ترکیبی از ویروسها[۴]، کرمها[۵] و تراواهایی[۶] که می تواند آسیبهای شدیدتری را به این سیستم ها و داده ها وارد کند . این صدمات حتی می توانند از بعضی نرم افزارهای مخرب نیز خطرناکتر باشند . از آنجا که تمامی این پیشرفتها کاربران فناوری را در سطح جهانی تحت تأثیر قرار می دهند، بهترین روشهای مقابله با تهدیدات ناشی از آنها تنها از طریق همکاری بین المللی حاصل می شود.

۴- امنیت فناوری اطلاعات درکشورهای درحال توسعه:
امنیت فناوری اطلاعات در کشورهای درحال توسعه از اهمیت شایانی برخوردار است . واضح است که اینترنت فرصتهایی طلایی برای تجارت و ارتباطات فراهم آورده است. اینترنت کاربران را قادر می سازد تا نگاهی به گسترهٔ وسیعی از موضوعات داشته باشند و با استفاده از آن ارتباط مردم از طریق پست الکترونیکی بسیار کارآمدتر از خدمات پستی سنتی شده است. اینترنت بر اصول تجارت بین المللی نیز تأثیر گذاشته است؛ بازارهای کشورهای درحال توسعه اکنون می توانند کالاهای خود را بصورت آنلاین بفروشند . اگرچه هنوز تعداد رقبا در بازار بسیار زیاد است، اما مشتریان می توانند بسادگی توانایی های و محصولات شرکتهای رقیب را ببینند و برای انجام اینکار نیازی به اطلاعات وسیع در این زمینه ندارند . از آنجا که دسترسی به بازارهای آن سوی مرزهای جغرافیایی برای هر سیستم اقتصادی بسیار جذاب است ، همکاری گسترده ای برای جا افتادن مدل یک نظام شبکه ای کارآمد و جهانی لازم است.

---
[2] - Personal Digital Assistants
[3] - Online Banking
[4] -Viruses
[5] - Worms
[6] -Trojans

در این روش مطالب در پنج بخش جداگانه مطرح می شود که این بخش ها عبارتند از : ۱- امنیت فناوری اطلاعات در عصر دیجیتال ۲- امنیت فناوری اطلاعات و کاربران منفرد ۳- امنیت فناوری اطلاعات و سازمانها ۴- امنیت فناوری اطلاعات و سیاستهای دولتی ۵- امنیت فناوری اطلاعات و راهبران فنی

۱-امنیت فناوری اطلاعات در عصر دیجیتال:

بخش اول مقدمه ای بر مباحث کلی امنیت در عصر الکترونیک می باشد و شامل موارد زیر است:

۱. انقلاب دیجیتال
۲. تعریف امنیت
۳. پیدایش و رشد اینترنت
۴. کلیات مسائل امنیتی
۵. مهاجمین به امنیت فناوری اطلاعات

۲- امنیت فناوری اطلاعات و کاربران منفرد:

بخش دوم به کاربرانی می پردازد که از منابع شبکه ای و رایانه ای برای اهداف متعدد در منزل و یا محل کار استفاده می کنند و البته برای سازمانهای کوچکی که قادر به تعیین دقیق سیاستهای امنیت فناوری اطلاعات و راهبری آن سیاستها در سطح سازمانی نیستند نیز مفید خواهد بود .

برخی از موضوعات مذکور در بخش دوم عبارتند از:

۱. ضرورت امنیت رایانه و شبکه و تأثیر رخنه های امنیتی
۲. امنیت فیزیکی ، پشتیبانی از تصدیق هویت[۷] از طریق شناسه های کاربری[۸] و رمزهای عبور[۹]
۳. انواع نرم افزارهای مخرب و چگونگی گسترش آنها
۴. مبنای کار پست الکترونیکی و اینترنت و دلیل اینکه ابزاری برای انجام حملات رایانه ای هستند
۵. ابزارهای نرم افزاری شامل ویروس‌یابها، دیواره های آتش و ابزارهای دسترسی از راه دور[۱۰]
۶. مفاهیم پیشرفته تری چون ساختار شبکه های و رمزگذاری

۳- امنیت فناوری اطلاعات و سازمانها:

بخش سوم ابعاد سیاست و راهبری امنیت را از نگاه سازمانی بررسی می کند. اتخاذ سیاستهای امنیتی مناسب و اجرای صحیح آنها خطر از دست دادن ناگهانی اطلاعات را کاهش می دهد، ورود غیرمجاز به سیستم را بسیار مشکل‌تر می کند و ابزار امنیتی برای شناسایی حملات و اصلاح رخنه های امنیتی را فراهم می سازد . برای حفظ داده های محرمانه و کمک به یکپارچگی برنامه ها و داده های ذخیره شده و انتقال این داده ها از طریق شبکه ، باید تلفیقی از سیاستگذاری و پیاده سازی آن انجام شود . این بخش اجزای مختلف سیاستهای امنیتی

[7] - Authentication
[8] - Usernames
[9] -Passwords
[10] - Remote Access Tools

مؤثر برای سازمانهای مختلف مانند شرکتهای تجاری ، دولتها، دانشگاهها و سازمانهای غیرانتفاعی را پوشش می‌دهد. بخش سوم موضوعات زیر را بصورت دقیق مورد بررسی قرار می دهد:

۱. روش هشت رکنی برای تأمین امنیت که خصوصًا در محیطهای خدمات مالی و اعتباری ارزشمند هستند
۲. ارزیابی خطر امنیتی و تحلیل امنیت در یک شرکت نوعی
۳. سیاستها و رویه های پیشنهادی برای تدوین برنامه ها و طرحهای امنیتی
۴. نقش مدیریت در تأمین امنیت رایانه ها، شبکه ها و داده ها
۵. امنیت کارمندان شامل آموزش و آگاهی ، فرآیند استخدام و استفاده از منابع امنیتی خارجی
۶. جرائم رایانه ای، گزارش وقایع و ترمیم سوانح[11]
۷. تهدیدات امنیتی فناوریهای بی سیم برای شرکتها و راهنمایی های ضمیمه و عواملی که به طراحی و پیاده سازی امنیت سازمانی مناسب کمک می کنند.

۴- امنیت فناوری اطلاعات و سیاستهای دولتی:

بخش چهارم عناوین امنیتی را بررسی می کند که فهم آنها در سطوح دولتی لازم است . یک دولت علاوه بر تأمین امنیت منابع اطلاعاتی خود، باید متعهد باشد که مجموعه سیاستهایی را برای ایمن ساختن اطلاعات زیرساختی ملی خود تنظیم کند . این سیاستها نقش مهمی در امنیت فناوری اطلاعات دارد، ولی با اینحال تناقضی نیز وجود خواهد داشت و آن این که چارچوب سیاست ملی باید قادر به افزایش سطح امنیت باشد ، اما قوانین ضعیف دولتی بیش از آنکه سودی در پی داشته باشند، ضرر به بار خواهند آورد. فناوری بسرعت درحال تغییر است و تهدیدات رایانه ای جدید به دلیل همین تغییرات بوجود می آیند. در چنین وضعیتی از قوانین دولتی برای به دام انداختن جنایتکاران استفاده می شود. بخش چهارم حاوی موضوعات زیر است:

۱. شبکهٔ ارتباطی و دیگر زیر ساختهای حیاتی که متعلق به بخش خصوصی بوده اما نظارت بر آنها با دولت است
۲. نقش کلی دولت و وظایف آن در ارتقای امنیت رایانه ای در بخشهای عمومی، خصوصی، و غیرانتفاعی
۳. قوانین جر ائم رایانه ای که برای حفاظت از رایانه ها و شبکه های خصوصی و دولتی تدوین می شوند
۴. مفاهیم سنتی که به نحوی به قالب قوانین رایانه ای منتقل شده اند
۵. قوانین، مقررات و سیاستهای دولتی که بر ارتقای امنیت رایانه ای در عرصهٔ پشتیبانی از مصرف کننده، داده های ارتباطات شخصی ، و چارچوبهای تجارت الکترونیکی تأکید دارند
۶. نمونه هایی از سیاست ها و قوانین تعدادی از کشورها و مراجع در سازمانهای بین المللی معتبر

۵- امنیت فناوری اطلاعات و راهبران فنی:

[11] - Disaster Recovery

بخش پنجم به راهبران شبکه و سیستم کمک می کند تا بتوانند وظایف خود را بصورت کارآمدتری انجام دهند. این بخش مسائلی را پوشش می دهد که باید در سطوح فنی و مدیریتی درک شوند. مثال اینکه ضوابط امنیتی چگونه نقض می شوند و یا روشهای مقابله با تهدیدات کدامند . بخش پنجم حاوی مطالب زیر است:

۱. طراحی سیستمهای امنیتی و روشهای مورد استفاده نفوذگران سیستم
۲. تهدیدات مختلف امنیت فناوری اطلاعات از سوی عوامل محیطی برای خرابکاری و دزدی اطلاعات و راهکارهایی برای مقابله با آنها
۳. مکانیزم های حفاظت از داده ها در مقابله با افشای غیرعمدی اطلاعات که با عناوین محرمانگی داده ها[۱۲] و یکپارچگی داده ها[۱۳] شناخته می شود.
۴. روالهایی برای شناسایی[۱۴] ، تصدیق هویت، و تأیید اعتبار[۱۵] کاربران
۵. مشکلات امنیتی رایج در رایانه هایی که برای ارائه خدمات اطلاعاتی بکار می روند و تنظیمات سرویس دهنده ها[۱۶] برای به حداقل رساندن این مسائل
۶. امنیت شبکه از بعد سخت افزاری (مودمها، مسیریاب ها [۱۷] و دسترسی بی سیم و نرم افزاری پروتکلهای شبکه ای موجود)
۷. فناوریهای مورد استفاده برای حمله به ایستگاههای کاری و سرویس دهنده ها که به آنها تخریب سرویس و تهدیدات برنامه ریزی شده می گویند.
۸. چگونگی استفاده از ابزارهای ممیزی و ورود به سیستم برای کمک به شناسایی سیستمهای آسیب پذیر و یافتن مواردی که روی این سیستمها دچار تغییر شده اند.

۱–امنیت فناوری اطلاعات در عصر دیجیتال:

انقلاب دیجیتال

عصر حاضر را عصر الکترونیک یا دیجیتال می نامند. امروزه استفاده از کامپیوتر و اینترنت بصورت روز افزون افزایش یافته است و اکثر اطلاعات در کامپیوتر ها و رسانه های ذخیره سازی بصورت دیجیتال ذخیره می گردد و از طریق خطوط ارتباطی مبادله می شود ولی با اینحال همواره مخاطراتی جدی مانند از دست دادن سوابق، حملات تخریب سرویس، خراب شدن اطلاعات و سایر انواع حملات خصمانه وجود دارد . از دست رفتن تمام یا

[12] - Data Confidentiality
[13] - Data Integrity
[14] - Identification
[15] -Authorization
[16] - Servers
[17] - Routers

بخشی از سوابق الکترونیکی می تواند یک شرکت را زمین گیر کند. برای کشوری که امنیت فناوری اطلاعات آن ضعیف است این احتمال وجود دارد که منابع حیاتی آن در معرض خطر قرار گیرند و به آنها صدمات جبران ناپذیری وارد شود. عدم توجه کافی به امنیت برای کشورهایی که به روابط خارجی در صنایع خود اهمیت می دهند می تواند موجب خسارتهای جدی و پیش بینی نشده ای گردد . نیل به اهداف به توانایی کشورهای درحال توسعه توسعهٔ هزاره استفادهٔ مؤثر از فناوری اطلاعات و افزایش بودجهٔ آنها با عضویت دائمی در سازمان تجارت جهانی بستگی دارد .

توانایی کسب و تأمین اطلاعات مناسب می تواند در تمامی زمینه های اقتصادی به کشورهای درحال توسعه کمک کند.

امنیت چیست؟

مفهوم امنیت در دنیای واقعی برای بسیاری از ما حیاتی است. در دوران ماقبل تاریخ، امنیت عبارت بود از اصول حفظ بقا نظیر امنیت در برابر حملهٔ دیگران یا حیوانات، و امنیت تأمین غذا. نیازهای دیگر چون امنیت در مقابل حوادث طبیعی یا بیماریها عمومًا برای انسانهای ما قبل تاریخ مطرح نبود . با پیشرفت تمدن، محدودهٔ امنیت فراتر رفته و ابعاد وسیع تری مانند در اختیار داشتن مکانی برای آسایش و زندگی بی خطر را در بر گرفت و امروزه مفهوم اموال شخصی نیز به تعریف امنیت اضافه شده است.

در بعضی زمینه ها دستیابی به سطحی از امنیت که انتظار آنرا داریم ممکن نیست . مثلا همیشه مایلیم عمری طولانی و جسمی سالم داشته باشیم؛ ولی آنچه که در معدل آماری طول عمر وجود دارد نشان می دهد که این مسئله برای بسیاری از افراد صدق نمی کند. عدم توانایی خود درتعیین سرنوشت را با بیمه جبران می کنیم تا ما را در برابر اثرات منفی مالی، حوادث و بیماریها حفاظت کند.

این مقدمه حقیقتی را دربارهٔ امنیت پیش روی ما قرار می دهد که امنیت مطلق چه در زندگی واقعی و چه در فضای سایبر غیرممکن و محال است. ولی با اینحال امنیتی که به اندازهٔ کافی مناسب باشد تقریبًا در تمامی شرایط محیطی دست یافتنی می باشد. راههای گوناگونی برای در اختیار گرفتن مکانیزمهای تقویتی افزایش و حفظ امنیت وجود دارد.

ما معمولا از چندین روش مختلف برای افزایش امنیت خود استفاده می کنیم تا درصورتیکه یکی از تدابیر مفید واقع نشد دیگری خلاء آنرا پر کند. این تدابیر و روشهای حفاظتی در فضای سایبر به شکلی دیگر مطرح می شوند. ما هم در دنیای واقعی و هم در فضای سایبر نیازمند حفاظت و دفاع از سرمایه های خود در برابر حملات دیگران و درصورت موفقیت آمیز بودن حملات، بازپس گیری سرمایه های از دست رفته می باشیم.

تعریف امنیت در فضای سایبر را بصورت زیر بیان می کنیم هنگامی در فضای سایبر ایمن هستید که دسترسی به منابع اطلاعاتی شما تحت کنترل خودتان باشد، یعنی هیچ کس بدون کسب اجازه از جانب شما قادر به دسترسی به این منابع اطلاعاتی نباشد. این منابع شامل داده ها و منابع رایانه ای، شبکه ای، تراکنشی، پردازشی، و اطلاعاتی می باشند. طبیعتًا ممکن است برخی از این منابع از جانب دیگران و برای استفادهٔ شما ارائه شده باشند، مثل حساب کاربری در یک رایانهٔ اشتراکی یا دسترسی به اینترنت از طریق یک ارائه کنندهٔ خدمات اینترنتی (ISP) . از آنجا که این موارد هیچگاه کاملا ایمن نیستند، تنها تا وقتیکه دستورالعملهای فروشندهٔ خدمات برای استفادهٔ صحیح از آنها را دنبال کنید می توانید بر دسترسی مداوم و استفادهٔ مناسب از خدمات اشراف داشته باشید.

در دنیای واقعی می دانیم که چطور باید از منابع اطلاعاتی خود حفاظت نماییم و همچنین می دانیم که بعضی از اطلاعات را باید بصورت محرمانه نگهداری کرد و برخی از آنها را می توان بصورت آزادانه در اختیار دیگران قرار دهیم یا انتقال دهیم . برای این منظور درهای اتاق ها و کمدهای حاوی فایلهای محرمانه را قفل می کنیم و حتی ممکن است نسخه هایی از اطلاعات مهم را خارج از محل نگهداریم تا در مواقعی چون بروز آتش سوزی و یا سایر بلایای طبیعی از آنها حفاظت کرده باشیم . بعضی اطلاعات را تنها می توان به تعداد محدودی از افراد انتقال داد و بسته به درجهٔ اهمیت اطلاعات می توان به افراد سطوح مختلفی داد. از نظر مفهومی میان ماهیت تهدیدات فضای سایبر و تهدیداتی که در دنیای واقعی وجود دارند هیچ تفاو تی نیست ، بلکه تفاوت این دو مقوله برخاسته از خصوصیات فضای الکترونیکی و تهدیدات این حوزه است.

عناوین حریم خصوصی[18] و محرمانگی [19] با مسئله امنیت در ارتباط هستند . اطلاعاتی که" خصوصی "بشمار می روند تنها زمانی می توانند واقعًا خصوصی بمانند که بصورت ایمن ذخیره شده باشند . برای این منظور در دنیای واقعی بگونه ای رفتار می کنیم که گویی چنین اطلاعاتی وجود خارجی ندارند . این سیاست را امنیت گمنامی[20] می نامند . به همین ترتیب اطلاعاتی که باید بصورت محرمانه به اشتراک گذارده شوند باید برای کسانیکه آنها را به اشتراک گذاشته اند بصورت ایمن باقی بمانند و هنگام انتقال این اطلاعات باید سیاستهای امنیتی کافی در مورد آنها اعمال شود. موقعیتهایی نظیر این مسئله در فضای سایبر نیز وجود دارد، ولی با فرض طبیعت خاص فضای سایبر و ارتباط میان رایانه های موجود در آن، امنیت گمنامی یا استفاده از پنهان سازی سیاستی ضعیف می نماید و باید از آن اجتناب کنیم.

مفاهیم رایانه ، شبکه و امنیت داده ها در فضای سایبر همانند دنیای واقعی هستند، ولی مکانیزمهای پیاده سازی روالهای مرتبط با آنها متفاوت است. مثلا برای استفاده از حسابهای کاربری که اجازهٔ دسترسی به اطلاعات یا خدمات را فراهم می آورند، به جای کلیدهای فیزیکی یا الکترونیکی، دارای شناسهٔ کاربری و رمز عبور هستیم

18 - Privacy
19 - Confidentiality
20 -Security By Obscurity

و بجای استفاده از پاکتهای دربسته برای انتقال اطلاعات می توانیم دادهٔ انتقالی را به نحوی رمزگذاری کنیم که توسط افراد ناشناس، غیرقابل خواندن باشد.

در مقایسهٔ دنیا ی واقعی با فضای سایبر می توانیم تخلفات مشابهی را در مورد قابلیت اطمینان و محرمانگی ببینیم . در هر دوی آنها ممکن است آدرسهای نادرست و یا امضاهای جعلی وجود داشته باشد . در هر دو فضا امکان ارائه اطلاعات غلط یا گمراه کننده نیز وجود خواهد داشت . همچنین امکان به اشتباه انداختن اشخاص با اطلاعات - چه بصورت تصادفی و چه از روی عمد - وجود دارد که باعث می شود نتوان تعیین کرد که چه اطلاعاتی مهم و قابل تأیید هستند .دست آخر اینکه در هر دو فضا امکان دسترسی غیرمجاز به اطلاعات محرمانه و استفاده از آنها برای مقاصد غیرقانونی نیز وجود دارد. اما با همهٔ این شباهتها سه تفاوت عمده میان این دو فضا مشاهده میشود:

اول : هر نوع نقض امنیت در فضای سایبر می تواند بسیار سریع اتفاق بیافتد؛ یعنی تا زمانیکه بخواهید آگاه شوید چه اتفاقی برای سرمایه های شما افتاده، ممکن است دیگر برای جلوگیری از وارد آمدن خسارت بسیار دیر شده باشد . البته تمامی حملات سریع اتفاق نمی افتند؛ بلکه بعضی از آنها در هنگام وقوع قابل مشاهده اند و برای به نتیجه رسیدن زمان زیادی می برند. بنابراین باید برای مقابله با تحدیدات فضای سایبر تدابیر امنیتی و بازدارنده باید از توانایی کافی برای تشخیص نقض حریم امنیتی در حین وقوع جرم یا پس از آن برخوردار باشند.

دوم : لازم نیست شما در یک محل بصورت فیزیکی حضور داشته باشید تا بتوانید امنیت فضای سایبر را خدشه دار کنید. این بدان معناست که مثلا یک نفر در اروپا می تواند امنیت رایانه های یک هدف در هند را خدشه دار نماید . تهدید امنیتی در فضای سایبر می تواند از هر جای شبکه شروع شود و به سمت هدفی معلوم و مشخص جهت گیری کند؛ و هدف نیز می تواند بصورت تصادفی انتخاب شده باشد . این تهدیدات خطرناک باعث می شوند که ما نحوهٔ تفکر خود در مورد امنیت را تغییر دهیم. بطور مثال می توان گفت این هیچ ارزشی ندارد که در آیین نامهٔ حق تکثیر Digital Millennium طراحی نرم افزارهای قفل شکن غیرقانونی اعلام شود؛ چراکه درحال حاضر کمیته های ملی و جهانی حق تکثیر در این موضوع و سایر موارد مرتبط به حفاظت از داده ها، هنوز مشغول تدوین راهکارهای اجرایی هستند.

سوم : فضای سایبر محیطی قدرتمند اما پیچیده را بوجود آورده که در آن نقش تأمین امنیت بر عهدهٔ چند گروه از افراد است. مثلا اگر شما یکی از کاربران ISP باشید، راههای مختلفی برای حفاظت از خود و رایانه شخصی تان پیش رو دارید اگرچه نمی توانید سیاستهای امنیتی ISP مورد استفادهٔ خود یا نحوهٔ پیاده سازی آنرا کنترل کنید . همچنین نمی توانید نرم افزارهای مشتریان خود را تحت کنترل داشته باشید؛ حتی اگر در ارتباط نزدیک با سیستم های آنها باشید . پس باید یک استراتژی حفاظتی برای سرمایه هایتان اتخاذ کنید، چراکه می دانید برقراری ارتباط با دنیای بیرون باعث می شود نتوانید تمام آسیب پذیریهای شبکه را خنثی نمایید.

خطرات احتمالی در فضای سایبر

اگر هیچ ملاحظهٔ امنیتی را مد نظر قرار نداده باشید بعضی نتایجی که ممکن است به بار بیایند عبارتند از:

۱- تخریب اطلاعات : داده های ذخیره شده روی رایانهٔ شما ممکن است حذف شوند . البته معمولا امکان بازیابی آنها وجود دارد، اما فرآیندی زمان بر و احتمالا ناقص خواهد بود . اگر یک مؤسسهٔ دولتی باشید ممکن است فعالیتهایتان حین این دوره دچار اختلال شود.

۲- سرقت اطلاعات و نقض حریم خصوصی : ممکن است از سرقت اطلاعات بلافاصله یا با تأخیر مطلع شوید اما این مسئله از اینکه متوجه شوید چه کسی داده های شما را در اختیار گرفته، چه اطلاعاتی در اختیار اوست، یا با آنها چه کارهایی انجام خواهد داد کاملا مجزاست . اگر حجم وسیعی از اطلاعات شخصی شما به سرقت رفته باشد به احتمال زیاد سارق اطلاعات کلیدی شما را در اختیار دارد و همین امر می تواند نتایجی نامعلوم و تا اندازه ای خطرناک در پی داشته باشد.

۳- نقض یکپارچگی اطلاعات : اطلاعات موجود در رایانه ممکن است بدون اطلاع شما تغییر کنند و دستکاری شوند. بر اساس نوع اطلاعاتی که نگهداری می کنید نتایج این دستکاری می تواند مقطعی یا درازمدت باشد. اگر این داده ها شامل سوابق مالی ، اطلاعات مشتریان ، وضعیت سفارشات یا پرونده های کارمندان باشند، پیامدهای نقض یکپارچگی آنها ممکن است بسیار پرهزینه و زیانبار باشد.

۴- نقض انسجام شبکه از طریق سایر سیستمها و شبکه ها: هرچند در این مورد به طور مستقیم مورد حمله قرار نگرفتهاید، ولی ممکن است رایانه های دیگری که به آنها دسترسی داشته اید مورد حمله قرار گیرند و این مسئله روی شما نیز تأثیرگذار باشد . در اینصورت اگر مثلا عنصر یک مؤسسهٔ مالی و اعتباری باشید حین دورهٔ بازیابی اطلاعات قادر به تکمیل تراکنشهای مالی خود نخواهید بود.

۵- ثبت کلیدها: نرم افزارهای پنهانی می توانند روی رایانهٔ شما نصب شوند که فشرده شدن دکمه های صفحه کلید توسط شما را ثبت کرده و آنها را به رایانه ای دیگر ارسال نمایند . این مسئله می تواند دسترسی به منابع خارجی نظیر دسترسی به یک سرویس دهندهٔ وب[۲۱] محافظت شده، دسترسی به یک سرویس دهندهٔ پست الکترونیکی، نقل و انتقالات مالی، و یا دریافت اطلاعات محرمانه را دچار اشکال کند . در اینحالت سارق می تواند نشانهای تصدیق هویت [۲۲] ، شمارهٔ کارت اعتباری، و رمزهای عبور شما را بدست آورد و در آینده برای منافع شخصی خود مورد استفاده قرار دهد.

۶- منع دسترسی [۲۳] : ممکن است شما از دسترسی به اطلاعات خود محروم شوید، حتی اگر آن اطلاعات پاک نشده باشند . مثلا امکان دارد اطلاعات شما در قالبهای رمزگذاری شدهای ظاهر شوند و تنها مهاجم کلید رمزگشایی آنها را در اختیار داشته باشد.

---

21 - Web Server

22 - Authentication Tokens

23 - Denial of Access

هزینهٔ ترمیم موفقیت آمیز از هر یک از این حملات قابل ملاحظه است و بازیابی در برخی موارد ناممکن بنظر می آید.

انگیزهٔ خرابکاران امنیتی چیست؟

در زندگی واقعی انگیزه های زیادی برای انجام تخلفات جنایی علیه یک شخص یا جناح وجود دارد. یکی از دلایل عمده، انتقام گیری فرد خرابکار از شخصی که فکر می کند به او آسیبی رسانده، و یا بدست آوردن پول است. از دلایل تخلفات نیز در فضای سایبر وجود دارد، اما تخلف در این فضاانگیزه های دیگری نیز وجود دارد. فضای سایبر برای گروهی از افراد – که اصطلاحا "خرابکار "نامیده می شوند یک محیط چالش انگیز است که وارد حسابهای کاربری افراد شوند و یا بعنوان تفریح و سرگرمی به افراد دیگر آسیب برسانند.

بعبارت دیگر، آنها قدرت نفوذ به حسابهای کاربری، پایگاههای داده و تجهیزات شبکه ای را یک افتخار برای خود می دانند. مشابه این رفتار در دنیای واقعی بسیار نادر است. خرابکارها معمولا فعالیتهای خود را " جنایات بدون قربانی " به حساب می آورند. استدلال آنها این است که وقتی یک حساب کاربری یا پایگاه داده مورد نفوذ قرار می گیرد ولی چیزی تغییر نمی یابد و دزدیده نمی شود چه آسیبی به کسی وارد شده است؟ در واقع این افراد به تأثیرات حقوقی و پیامدهای اینکار توجه نمی کنند و به احساس ناامنی قربانیانشان که ناشی از انجام این فعالیتها می شود نیز اهمیتی نمی دهند. مشابه این رفتار در دنیای واقعی مثل این است که فردی وارد خانهٔ شما شود و هر زمان که بخواهد نیز بتواند اینکار را تکرار کند. مسلمًا این مسئله برای شما غیرقابل تحمل خواهد بود. متأسفانه اینترنت به ناقضان امنیت کمک بزرگی است. برخی از خرابکارها از ابزارهای نفوذی استفاده می کنند. که این ابزارها حتی به نفوذگران تازه کار هم امکان می دهد که از آسیب پذیری ها سیستم بهره برداری نمایند. از آنجا که بسیاری از این ابزارها ممکن است بدون خطر باشند، هرگز کسی مطمئن نیست آثار استفاده از هریک از آنها دقیقًا چیست . علاوه بر آن این امکان وجود دارد که با انجام تغییراتی در بعضی از این ابزار به اصطلاح بی خطر بتوان به رایانه ها و حسابهای کاربری که از طریق آنها مورد دسترسی قرار گرفته اند آسیب وارد کرد. اگرچه بیشتر جرائم قابل مشاهده در دنیای سایبر توسط افراد انجام می شود، ولی سازمانها و مؤسسات نیز قادر به سوء استفاده از خصوصیات این فضا برای رسیدن به اهداف سازمانی خود هستند. جرائم سازماندهی شده ممکن است دستکاری در شبکهٔ اینترنت برای رسیدن به نتایج مطلوب آنها باشد، اما می تواند باعث ارتکاب جرم علیه دیگران نیز بشود. ممکن است برخی سازمانها علاقه داشته باشند که نتیجهٔ یک نظرسنجی یا حتی انتخابات را دستکاری کنند تا به نتایج مطلوب خود برسند واضح است که منافع بالقوهٔ موجود در عصر نوین دیجیتال بسیار است . بسیار حائز اهمیت است که با ایمن سازی محیط فیزیکی، زیرساختها، رایانه ها، خطوط ارتباطی و منابع اطلاعاتی

خود از این منافع حفاظت کنیم . اولین گام در انجام این مهم رسیدن به سطح شناخت کافی و صحیح از فناوری است که می تواند در اتخاذ تصمیمات عاقلانه دربارهٔ چگونگی رسیدن به سطح مطلوبی از امنیت به ما کمک کند .

بسیاری از ما در این زمینه چندین نقش را بر عهده داریم : ممکن است بعنوان یک کاربر عادی از این منابع استفاده کنیم، در قبال سیستمهای دیجیتال و خدمات موجود (فناوری اطلاعات) در یک سازمان مسئولیت داشته باشیم، و یا به با دولت در اجرای سیاستهای حمایتی از امنیت همکاری داشته باشیم.

همهٔ ما در هریک از این نقشها در قبال تحقق سطح مطلوبی از امنیت مسئول هستیم. متأسفانه امنیت در یک محیط پیچیده معمولا به اندازهٔ امنیت ضعیفترین جزءِ آن محیط استحکام دارد؛ از اینرو باید مطمئن شویم که اجزای محیطی که روی آن کنترل داریم که ضعیفتری اجزاء آن هم از توانایی دفاع در برابر تهدیدات موجود برخوردار است.

اهمیت امنیت برای سازمانهای کوچک و متوسط در کشورهای درحال توسعه

با اینکه امنیت برای همه حائز اهمیت است، اما برای سازمانهای کوچک و متوسط کشورهای درحال توسعه اهمیت ویژه ای دارد. نتایج حاصل از ورود به بازار جهانی با کمک فناوری اطلاعات و ارتباطات بسیار مطلوب است، ولی مخاطرات ناشی از انجام اینکار بصورت ناامن نیز بسیار زیاد است. در بسیاری از کارهای تجاری عملیات دستی به سیستم های مبتنی بر رایانه ها تغییر یافته است . با معرفی منابع رایانه ای جدید، مدیران به سمت و سوی کسب دانش و اطلاعات دربارهٔ موضوعات کاربردی چون پشتیبان گیری نگهداری شبکه، به روزرسانی نرم افزارها و ممیزی (بازبینی) رایانه ای روی آورده اند. کسب موفقیت در همگی موارد فوق مستلزم آشنایی با رایانه، شبکه، و مفاهیم امنیت اطلاعات است.

با معرفی ارتباطات شبکه ای و امکان ورود به عرصهٔ تجارت الکترونیکی، فرآیندهای سیستم و فرآیندهای مدیریت باید از دو دیدگاه متفاوت نظاره شوند. سیستمهای مستقل عمومًا محصول محور یا فرآیند محور هستند (مثل انبارداری، سفارشات یا فرآیندهایی نظیر تولید، ثبت در دفاتر عمومی، و حسابهای پرداختنی و دریافتنی)، اما سیستمهای موفق تجارت الکترونیکی آنلاین (برخط) به روش دیگری سازماندهی می شوند. در این سیستمها برای کسب موفقیت لازم است که طراحی مشتری مدار باشد و سیستم به تعقیب رفتار مشتری در فرآیندهای جستجو و ارزیابی محصولات، ارائه سفارش، تکمیل تراکنشهای مالی و ردگیری محصول ارسال شده بپردازد. در این سیستمها علاوه بر اینکه نگرانی در مورد محصولات و فرآیندها همچنان اهمیت دارد، اما در مقابل نیاز به تعقیب رفتار مشتری در پایگاه وب و انجام هر معاملهای که مشتری آنرا درخواست می کند نیز می باشد. این طراحی مجدد برای دستیابی به موفقیت ضروری است و به یک راهکار جایگزین برای مدیریت درخواست های

جدید مشتری نیاز دارد. این روش اگر بدون توجه کافی به امنیت پیاده سازی شود ممکن است راه را برای روش های جدید نفوذ های امنیتی باز بگذارد. سازمانهای کوچک و متوسط باید آگاه باشند که اصلاح نگرش سیستمهای تجاری برای بکارگیری اینترنت، خطرات جدیدی برای آنها به همراه دارد . یکی از این خطرات احتمال به سرقت رفتن و در معرض فروش قرار گرفتن سرمایه های موجود در شرکت.

در عصری که اطلاعات یا محصولات اطلاعاتی جزء کالاها و خدمات فروخته شده می باشند ، احتمال توزیع و تهیهٔ غیرقانونی آنها بصورت رایگان و یا در بازار سیاه وجود دارد که در اینحالت منافع اینکار به سارقان می رسد، و نه به شرکتی که اطلاعات را تولید کرده است.

امنیت فناوری اطلاعات و سیاست های دولتی

مقدمه :

همانند سایر زمینه های تأثیرگذار در اینترنت، سیاست های دولت نیز نقش مهمی در مقوله امنیت فناوری اطلاعات ایفا می کند. با اینحال در این مورد باید با احتیاط اظهار نظر کرد، چراکه یک چا رچوب عمومی سیاست می تواند امنیت را تقویت کند ؛ اما اشکالاتی که در اثر مقررات نادرست دولتی بوجود می آید بیش از مزایای چنین مقرراتی است. فناوری اطلاعات بسرعت درحال تغییر است و تهدیدات سایبری جدید نیز با چنان سرعتی انتشار می یابند که برخی از مقررات دولتی براحتی می توانند تبدیل به موانعی برای ارائه سریع پاسخهای مبتکرانه شوند.

بنابراین بهترین راه این است که میان معیارهای قانون گذاری و غیر قانونی یک نقطهٔ تعادل پیدا کنیم. برای دستیابی به چنین تعادلی، سیاستگذاران باید به برخی ویژگیهای ذاتی و منحصر به فرد اینترنت توجه کنند. در مقایسه با فناوریهای اطلاعات و ارتباطات پیشین، فضای سایبر یک فضای غیر متمرکز است. بخشی از قدرت اینترنت ناشی از این حقیقت است که فاقد دربان یا نگهبان می باشد و بیشتر کارایی آن در مرزهای شبکه است تا در مرکز آن سیاستهای امنیت سایبر دولت باید این ویژگیهای اینترنت را مد نظر قرار دهند. در ادامه بحث گام هایی که دولتها می توانند با استفاده از آنها و مستقل از تصمیم گیریهای فنی، امنیت رایانه های خود را ارتقا دهند را مطرح می کنیم.

با اینکه این مسئله از کشوری به کشور دیگر متفاوت است، در بسیاری از کشورها یک جزء یا تمامی اجزای شبکه‌های ارتباطی و بسیاری از زیرساختهای مهم و حساس که مبتنی بر سیستم های رایانه ای هستند نظیر بانکداری، حمل و نقل، انرژی، تولید و..... تحت تملک و عملکرد بخش خصوصی قراردارند . بنابراین قسمت اعظم مسئولیت کسب اطمینان از امنیت این سیستم ها وابسته به بخش خصوصی است . ولی از آنجایکه وجود و کارایی سیستم های این چنینی برای رفاه ملی ضروری است و معمولا کاربرد آنها در مواقعی است که از آن استقبال بیشتری می شود و لذا دولت به آن توجه زیادی نشان می دهد. دولتها معمولا سیستم رایانه ای خاص خود را دارند؛ از جمله رایانه هایی که برای امنیت ملی، خدمات اضطراری، بهداشت و سایر عملکردهای ضروری مورد استفاده قرار می گیرند و غالبًا به شبکه های ارتباطی خصوصی وابسته اند. در مجموع بسیاری از سیستم های رایانه ای شرکتهای خصوصی و سازمانهای دولتی وابسته به همان نرم افزارها و سخت افزارهایی هستند که توسط شرکتهای خصوصی طراحی و ساخته شده اند و بنابراین مسئله امنیت در آنها یکی از مسائل قابل توجه است. با توجه به دلایل گفته شده، مسئولیت امنیت این سیستم ها میان دولت و بخش خصوصی تقسیم شده است . در اولویت اول، دولت مسئولیت" تنظیم امور مربوط به خود " را بر عهده دارد؛ یعنی باید روشهای صحیح امنیتی را برای ارتقای ایمنی در سیستم های خود بکار گیرد. بعلاوه از لحاظ جهانی مشخص شده که دولت باید برای مجازات و پیشگیری از انجام حملات به سیستم های بخش خصوصی، مثل سیستم های دولتی از قدرت قوانین حقوق و جزا کمک بگیرد. فراتر از آن بسیاری از دولتها به این نتیجه رسیده اند که برای ارتقای روالهای تأمین امنیت رایانه ای در بخش خصوصی باید مسئولیتهای بیشتری را متحمل شوند . این تلاش برای این است که سیاستهایی توسط دولت اتخاذ شود که باعث نشوند قوانین و برنامه های فناوری مجال ظهور ابتکارات و نوآوری‌ها را بگیرند، بلکه باعث به حداکثر شدن مزایای دخالت دولت در این موارد گردند . در یک فضای همکاری میان دولت و بخش خصوصی می توان تعادلی بصورت زیردر نظر گرفت:

- فشار بازار کار که شرکتهای خصوصی را بسوی امنیت سیستم های رایانه ای ترغیب می کند تا سود بیشتری کسب کنند؛
- تحقیقات دولتی و آگاه سازی؛
- قوانین جرائم رایانه ای که از رایانه های شبکه های دولتی و خصوصی حمایت می کنند؛
- مفاهیم قوانین سنتی که وارد محیط رایانه ای شده اند؛ و
- قوانین، مقررات و سیاستهای دولتی که خصوصا بر ارتقای امنیت رایانه ای می باشد مطابقت داده می شود؛

مفهوم" سیاست امنیت رایانه ای "را می توان جزئی از موضوع گسترده تری به نام" نقش قانون در گسترش اعتماد اینترنتی" مشاهده نمود . ایجاد یک محیط قابل اطمینان در فضای سایبر نیازمند تطبیق قوانین و سیاستهای دولتی سایر زمینه ها بر حوزهٔ امنیت سایبر است . این زمینه ها شامل حمایت از مصرف کننده[۲۴]،

[24] - Consumer Protection

خصوصی ماندن داده ها و ارتباطات[25] ، حقوق مالکیت معنوی [26] و چارچوب تجارت الکترونیکی [27] می باشد . در دنیای واقعی(بدون اینترنت)، قانون برای معاملات تجاری و مصرف کنندگان حمایتهایی ایجاد می کند. قسمت اعظم این قوانین در حوزهٔ فضای سایبر نیز قابل اعمال هستند، اما کشورهایی که بدنبال گسترش فناوری اطلاعات و ارتباطات هستند باید این مسئله را بررسی کنند که آیا در قوانین آنها خلأیی وجود دارد که مانع ایجاد اعتماد لازم برای افزایش امنیت فضای سایبر شود یا خیر. در حقیقت کشورهایی که علاقه مند به گسترش تجارت الکترونیکی هستند ممکن است دریابند که قوانین آنها در مورد خدمات مالی، مالکیت سایبر و حمایت از مصرف کننده از اعتماد یا پشتیبانی لازم برای تعاملات خارج از دنیای اینترنت برخوردار نیست. اصلاح قوانین دنیای سایبر ممکن است بعنوان بخشی از اصلاحات روی قوانین کلی تر انجام شود.

مفهوم زیرساختهای حیاتی

در تعدادی از کشورها روالهای واکنشی دولت به مشکلات امنیتی رایانه ها زیرساختهای حیاتی گفته می شود. زیرساخت حیاتی، شبکه ای از سرمایه های فیزیکی و سیستم هایی است که نقش بسزایی در اقتصاد یا رفاه یک کشور دارند. بعنوان مثال شبکهٔ خدمات مالی یک زیرساخت حیاتی است که شامل تمامی بانکهای خصوصی، بانک مرکزی، بازارهای مبادلات کالا، سازمانهای تبادل چک، و دیگر نهادهایی که درگیر خدمات مالی و اعتباری هستند می شود. تقریبًا در تمامی کشورهای جهان این عملیات با استفاده از رایانه ها انجام می گیرد. شبکهٔ حمل و نقل نیز زیرساخت حیاتی دیگری است که از جاده ها، پلها، کانالها، خطوط راه آهن و فرودگاهها تشکیل شده است . زیرساخت حمل و نقل غالبًا فیزیکی و مکانیکی است؛ اما عملکرد صحیح چراغهای راهنمایی، باز و بسته کردن پلها، راه انداختن قطارها و کنترل ترافیک هوایی، سیستم توزیع برق و آب و سوخت همه و همه به عملکرد صحیح رایانه ها بستگی دارند. هیچ تعریف مشخصی برای گروههای زیرساختهای حیاتی وجود ندارد و فهرست زیرساخت حیاتی که توسط سیاستگذاران بکار می رود از کشوری به کشور دیگر و از زمانی تا زمان دیگر متفاوت است . استراتژی امنیت سایبر دولت ایالات متحدهٔ آمریکا که در فوریه سال ۲۰۰۳ به چاپ رسید، ۱۳ گروه زیرساخت حیاتی را مشخص می سازد:

۱- کشاورزی،۲- تغذیه،۳- آب، ۴- بهداشت عمومی، ۵- خدمات اضطراری، ۶- دولت، ۷- صنایع دفاعی، ۸- اطلاعات و ارتباطات راه دور، ۹- انرژی، ۱۰ - حمل و نقل، ۱۱- بانکداری و امور مالی، ۱۲ - مواد شیمیایی و پرخطر، ۱۳ - خدمات پستی و کشتیرانی .

مفهوم زیرساختهای حیاتی به دلایل زیادی حائز اهمیت است.

اول، به روشن شدن این مسئله کمک می کند که چرا امنیت رایانه ای مهم است . اگر سیاستگذاران درک کنند که درصورت خرابی رایانه ها، پول در بانکها غیر قابل پرداخت می شود، قطارها قادر به ترک ایستگاه نمی باشند و حتی آب آشامیدنی و برق قطع می شود، آنگاه بهتر خواهند توانست آثار ناشی از مشکلات امنیتی را درک کنند.

25 - Data & Communications Privacy
26 - Intellectual Property Rights
27 - E-Commerce Framework

دوم، گروههای زیرساختی به این دلیل اهمیت دارند که به تعریف مسئولیتهای جوامع کمک می کنند و جوامعی با علایق مشترک که برای ارتقای امنیت نیاز به همکاری با یکدیگر دارند بوجود می آورند. عنوان مثال صنعتگران صنعت برق و مستشاران دولتی می توانند با مشارکت یکدیگر نقش مثبتی در رفع آسیب پذیریهای سیستم برق داشته باشند. معیارهای امنیت رایانه ای از جمله شناسایی الگوهای بهینه[۲۸] و اشتراک اطلاعات در مورد آسیب پذیریها تا حدودی می تواند در محدوده مؤسسات و خطوط تولید صنعتی موجود بکار رود.

این مؤسسات در بخش خصوصی شامل اتحادیه های تجاری، شرکتهای استاندارد و سایر شرکتهای نظارت بر صنایع مختلف می باشند. اکثر کشورها در بخش دولتی سیاستهای امنیت سایبر را از طریق وزارتخانه ها و سازمانهای نظارتی انجام می دهند.

درحال حاضر تعدادی از شرکتهای بزرگ وجود دارند که در مقیاس بزرگتری در این زمینه همکاری می کنند. بعنوان مثال گروه G۸ در ماه می سال ۲۰۰۳، ۱۱ اصل را مشخص کرد که برای توسعهٔ استراتژی کاهش مخاطرهٔ زیرساخت اطلاعات حساس مد نظر قرار گیرند . این اصول به شرح زیر هستند:

۱- کشورها باید دارای شبکه های هشدار دهندهٔ اضطراری برای تهدیدات و حوادث دنیای سایبر باشند.

۲-کشورها باید سطح آگاهی و دانش خود را ارتقا دهند تا به درک افراد از ماهیت و وسعت زیرساخت اطلاعات حساس خود کمک نمایند و نقش آنها را در راستای حفاظت از این اطلاعات تعریف کنند.

۳- کشورها باید زیرساختهای خود را مورد مطالعه قرار دهند و ارتباطات متقابل میان آنها را مشخص سازند و بدینوسیله حفاظت از این زیرساختها را افزایش دهند.

۴- کشورها باید مشارکت میان بخش عمومی و بخش خصوصی را افزایش داده و اطلاعات زیرساختی مهم خود را مورد تجزیه و تحلیل قرار دهند و آنها را به اشتراک بگذارند تا بتوانند از آسیب دیدن آنها تا حد امکان جلوگیری نمایند و نسبت به آسیبهای وارده واکنش نشان دهند.

۵- کشورها باید شبکه های ارتباطی مخصوصی برای زمان بحران ایجاد و از آن نگهداری کنند، و آنها را موردارزیابی قرار دهند تا اطمینان یابند که در موقعیتهای اضطراری همچنان امن و پایدار باقی می مانند و می توان از آنها استفاده کرد.

۶- کشورها باید اطمینان یابند که سیاستهای در دسترس بودن داده [۲۹]، امنیت زیرساختهای اطلا عات حساس را نیز مد نظر قرار داده اند.

۷- کشورها باید ردیابی حملات به زیرساختهای مهم اطلاعاتی را تسهیل بخشیده و در زمان مناسب، اطلاعات این ردیابی را برای سایر کشورهای متقاضی منتشر سازند.

۸-کشورها باید در خصوص افزایش قابلیت واکنش، آموزشها و تمریناتی داشته باشند و برنامه های خود را برای پیشامدهای احتمالی در زمان وقوع حمله مورد ارزیابی قرار دهند و همگان را نیز تشویق به انجام فعالیتهای مشابه سازند.

---

28 - Best Practices

29 - Data Availability

۹- کشورها باید اطمینان حاصل کنند که برای مقابله با مشکلات امنیتی، قوانین مناسب و روالهای قابل قبول دارند و این تحقیقات را با سایر کشورها به نحو احسن مطابقت دهند مانند قوانینی که در کنوانسیون تخلفات سایبر شورای اروپا [۳۰] در نوامبر سال ۲۰۰۱ تصویب شد و پرسنل آموزش دیده ای را آمادهٔ ارزیابی و ردیابی حملات انجام گرفته به زیرساختهای اطلاعات حساس نمود.

۱۰ - کشورها باید در زمان مناسب در همکاریهای بین المللی مشارکت کنند تا زیرساختهای مهم اطلاعاتی خود را ایمن سازند، که این امر شامل تأسیس سیستم های هشداردهندهٔ اضطراری، اشتراک و تحلیل اطلاعات بر اساس آسیب پذیریها و رخدادها، و نیز همکاری در مورد حملات انجام شده به زیرساختهای اینچنینی و البته با درنظر گرفتن قوانین محلی می باشد.

۱۱- کشورها باید تحقیق و توسعهٔ ملی و بین المللی خود را افزایش دهند و بر اساس استانداردهای بین المللی، مشوق بکارگیری فناوریهای امنیتی باشند. خصوصیت منحصر به فرد امنیت رایانه ای، ارتباطات داخلی شامل سخت افزارها و نرم افزارهای مشابه و وابستگی به یک شبکه ارتباطی مشترک است.

بنابراین دولتها باید بگونه ای سیاستگذاری کنند که ضامن اشتراک اطلاعات مربوط به آسیب پذیریها و راه حلهای مرتبط با گروههای زیرساختی باشند . می توان اینکار را با انتخاب یک مرکز راهبری در دولت برای هماهنگ سازی متمرکز برنامه ها و سیاستهای امنیت سایبر عملی کرد.

حفاظت از سیستمهای دولتی

تمامی موضوعاتی که در مورد امنیت سیستم های سازمانهای کوچک و بزرگ مطرح می باشد در سیستمهای دولتی نیز قابل استفاده هستند . همانطور که شرکتها نیازمند محافظت از خود، تهیه کنندگان و مصرف کنندگان هستند، دولت نیز باید از سیستمها و شهروندان در برابر تهدیدهای فیزیکی و تهدیدات امنیت سایبر محافظت نماید . دولتهای محلی و ملی نمی توانند جلوی بحرانهای شدید مثل وقوع وقفه در عملیات رایانه ای، از بین رفتن داده های محرمانه و یا سرقت منابع رایانه ای را بگیرند. انتشار اخبار رخدادهای امنیتی برای عموم باعث کاهش اعتماد مردم می شود و تبدیل به مانعی برای پیشرفت اقدامات دولت الکترونیکی[۳۱] می گردد. معمولا اولین مسئولیت دولت در امنیت رایانه همان " تنظیم امور مربوط به خود " آن است؛ بدین معنا که سازمانهای دولتی در تمامی سطوح (ملی، منطقه ای و محلی) باید از سیستمهای رایانه ای که مورد استفادهٔ آنان قرار دارد حفاظت بعمل آورند . اینکار شامل سیستمهای رایانه ای مورد استفادهٔ سازمانهای دولتی و یا وزارتخانه ها از جمله نیروهای نظامی و انتظامی، سازمانهای بهداشت و سلامت عمومی، مراکز واکنشهای اضطراری، و همچنین بانکهای مرکزی می شود. زیرساختهای مربوط به دولت که وابسته به رایانه است بسته به اینکه چه چیزی دولتی و چه چیزی خصوصی محسوب شود می توانند شامل سیستمهای آبی، سدهای برقی آبی (هیدروالکتریکی)، سیستمهای کنترل ترافیک هوایی و سایر امکانات و تسهیلات باشند.

30 - Council of Europe Cybercrime Convention

31 -E-Government

فرماندهی و سازمان

یکی از چالش های دولت برای مسئله امنیت رایانه ای دولت چگونگی رهبری ساختار ملی برای این منظور است. برای تعیین مسئولیتها در دولت باید ابتدا به این پرسش پاسخ داد که : آیا از نظر اقتصادی، امنیت ملی و یا مقررات حاکم، امنیت رایانه ای یک مسئله قابل اهمیت محسوب می شود؟

انتخاب محل فرماندهی امنیت الکترونیکی در دولت اهمیت زیادی دارد . بعنوان مثال تصمیم گیری در مورد زمان انتشار اطلاعات در مورد آسیب پذیریهای امنیت سایبر برای عموم، نیازمند بررسیهای چندجانبه است . قرار دادن این مسئولیت در وزارت دفاع که معمولا مسئول حفظ اسرار امنیت ملی است ممکن است انتشار اطلاعات را دچار اختلال کند و باعث شود مطالب کافی برای بالا بردن سطح آگاهی های عمومی منتشر نشود. از آنجا که همکاری بخش دولتی و بخش خصوصی جزء مهمی از آنچه که معتقدیم مؤثرین استراتژی امنیت رایانه ای است می باشد، شاید بهتر باشد رهبری امنیت سایبر در یک سازمان اقتصادی یا شرکت وابسته به دولت و تحت نظارت بالاترین مقام اجرایی کشور قرار گیرد. اما مهمتر از اینکه کدام سازمان یا سازمانها باید مسئولیت امنیت رایانه ای را بر عهده گیرند این است که باید نوعی "فرماندهی ملی " ایجاد شود تا بتوان کسب اطمینان کرد که امنیت رایانه ای از سوی اجزای دولت به اندازهٔ کافی مورد توجه قرار خواهد گرفت. هنگامیکه به وارد کردن مقولهٔ امنیت رایانه ای به وزارتخانه های موجود می اندیشیم، سؤالات سازمانی مهمی پیش می آیند که باید برای آنها پاسخ مناسب پیدا کرد . اگر فقط اختیار سازمان هدایت کنندهٔ امنیت سایبر ، ترغیب مردم و انتشار اطلاعات برای عموم باشد، اختیار عملی آن در حوزهٔ امنیت سایر وزارتخانه ها محدود خواهد بود . بنابراین باید روشهایی بوجود آیند که به رهبران امنیت سایبر اجازه دهند امنیت را در سیستمهای موجود سازمانها و وزارتخانه ها برقرار سازند .

۱- یک روش برای الزام وزارتخانه ها به تبعیت و موافقت با استانداردهای امنیت رایانه ای می تواند این باشد که یک مقام مسئول در ادارهٔ مرکزی امنیت در دولت بتواند سفارشات خرید سازمانهای دولتی که از استانداردهای امنیتی تبعیت نکرده اند را رد کند.

۲- یک اقدام دیگر می تواند الزام وزارتخانه ها و سازمانهای دولتی به اجرای ممیزی سالانهٔ امنیت سایبر و گزارش نتایج آن به ادارهٔ امنیت سایبر باشد . هر ساختاری که انتخاب شود، مدیر ارشد آن باید از طرف دفتر ریاست جمهوری یا نخست وزیری تعیین گردد تا تمامی ادارات و سازمانها آنرا جدی بگیرند.

۳- یک چالش سازمانی دیگر برای دولت، مشکل منابع انسانی است . دولتها برای جذب و نگهداری پرسنل متخصص در زمینهٔ امنیت رایانه ای مشکل دارند . یکی از راه حلها می تواند ارائه بورس تحصیلی برای مطالعات امنیت رایانه ای باشد که با استفاده از این بورسها، افراد برای سالهای مشخصی تعهد خدمت به دولت پیدا خواهند کرد . یک راه حل کوتاه مدت نیز می تواند اجرای برنامه ای دو مرحله ای با کمک بخش خصوصی باشد که در آن متخصصان امنیت سایبر برای دولت کار کنند، اما تمام یا بخشی از حقوقشان توسط کارفرمای بخش خصوصی آنها پرداخت گردد . مشکل منابع انسانی در امنیت سایبر هم در کشورهای توسعه یافته و هم در کشورهای درحال توسعه ممکن است منجر به مواجههٔ دولت با مشکل اساسی دیگری شود، چراکه دولت در مقایسه با بخش خصوصی نمی‌تواند به متخصصین این رشته دستمزد قابل توجهی بپردازد.

تهیهٔ استراتژی ملی امنیت سایبر

روند تهیهٔ استراتژی ملی امنیت سایبر می تواند ابزار مؤثری باشد برای:

۱- تصمیم گیری در مورد اینکه آسیب پذیریهای مالی امنیت سایبر ملی چیست؟

۲- مسئولیتهای دولت باید چه چیزهایی باشد،

۳- و چه سیاستها و اصلاحاتی در قانونگذاری باید دنبال شود .

این استراتژیها همچنین می توانند ارتباط میان دولت و بخش خصوصی را مشخص سازند . در اینجا عمدتا روی آن دسته از عناصر استراتژیهای امنیت ملی سایبر متمرکز می شویم که پشتیبانی از رایانه های دولتی را بر عهده دارند که در بخش بعدی نقش دولت را در ارتقای امنیت سیستم های بخش خصوصی مورد بحث و بررسی قرار خواهیم داد .

بطور کلی بخش خصوصی برای واکنش به تهدیدهای رو به رشد فضای سایبر آمادگی لازم را دارد . با این وجود در بعضی موارد خاص، پاسخ دولت مرکزی مناسبتر و قابل قبول تر می باشد. از نظر داخلی، تداوم اینکار در دولت نیازمند کسب اطمینان از امنیت زیرساختهای سایبر خود دولت و سرمایه های مورد نیاز برای پشتیبانی از مأموریتها و خدمات ضروری آن است . از نظر خارجی، در مواردی که هزینه های بالای تبادلات و موانع قانونی منجر به وقوع مشکلات بزرگ در همکاریها می شوند؛ در مواردی که دولت در غیاب نیروهای بخش خصوصی کار می کند و هنگامیکه تجزیه و تحلیل مشکلات به غیرقابل انتشار شدن منابع حیاتی به اشتراک گذاشته شده می انجامد، نقش دولت در امنیت سایبر تضمین کننده رفع مشکلات خواهد بود. تا کنون ایالات متحده وسیعترین و بیشترین فرآیندهای تهیهٔ استراتژیهای ملی امنیت سایبر را داشته و در عملکرد سایر کشورها و گروههای بین المللی نیز مطا لب و موضوعات مشابهی به چشم می خورد. با اینکه جزئیات این فرآیندها و پیامدهای قوانین و ساختارهای سازمانی از کشوری به کشور دیگر متفاوت هستند، ولی فرآیند تهیهٔ استراتژی امنیت سایبر که بسیاری از کشورها برای تهیه استراتژیهای ملی فناوری اطلاعات و ارتباط ات از آن استفاده کرده اند مشابه یکدیگر هستند. در حقیقت امنیت یک جزء استراتژیهای ملی فناوری اطلاعات و ارتباطات است و استراتژی امنیت سایبر می تواند از طریق اصول حقوقی و روشهای مشابه مورد استفاده در تهیه پیش نویس برنامهٔ ملی توسعه فناوری اطلاعات و ارتباطات بکار گرفته شود .

بر اساس تجربیات کشورهایی که برای خود استراتژیهای ملی امنیت سایبر تهیه کرده اند، در انجام اینکار برخی عناصر و بخشهای مشترک وجود دارد:

۱- ارزیابی آسیب پذیریهای ملی و انتشار گزارشهای عمومی که کلیت موضوع را به تصویر می کشند و برای سیاستگذاران و مردم آگاهی بوجود می آورند؛

۲- ایجاد ساختار فرماندهی در بخش اجرایی دولت برای نظارت بر تهیه و اجرای سیاستها؛

۳- تهیهٔ یک طرح تفصیلی ملی با تبادل نظر با بخش خصوصی؛

۴- تطبیق مقررات و راهبردهای مرتبط با مسائلی نظیر اشتراک و دسترسی به اطلاعات برای بوجود آوردن پاسخگویی.

فاز اول، ارزیابی مفصل آسیب پذیریها و افزایش سطح آگاهی عمومی است.
فاز دوم، ایجاد ساختارهای ثابت در بخش اجرایی برای همکاری در تهیه و اجرای سیاستها است .
فاز سوم شامل تهیهٔ استراتژیها است . همانطور که در بالا اشاره شد، یک استراتژی ملی امنیت سایبر می تواند یک سند مجزا و یا قسمتی از استراتژیهای ملی ICT باشد . نکتهٔ کلیدی در این فرآیند، تبادل نظر دولت و بخش خصوصی است. درآمریکا قطعنامه ای برای تهیهٔ استراتژی داخلی آمریکا در مقابل تهدیدات د ستیابی به اطلاعات رایانه ای و شبکه ها تدوین نمود سپس سازمان همکاری و توسعهٔ اقتصادی (OECD)[۳۲] نیز خط مشی هایی دولتها و شرکتهای خصوصی در خصوص تهیهٔ استراتژی امنیت سایبر منتشر ساخت. بعد از همهٔ این تلاشها، یک مجموعهٔ موضوعی هماهنگ و یکپارچه از استراتژیهای امنی ت سایبر در سطوح ملی، منطقه ای و بین المللی بدست آمده است که شامل موارد زیر است:

۱- مشارکت بخشهای عمومی و خصوصی

امنیت سایبر نیازمند همکاری بخشهای عمومی و خصوصی است . بخش خصوصی مسئولیت اصلی اطمینان از امنیت سیستمها و شبکه های خود را بر عهده دارد.

۲- آگاهی عمومی

استفاده کنندگان از شبکه از جمله تولیدکنندگان، راهبران، اپراتورها و یا کاربران شخصی باید نسبت به تهدیدات وارده و آسیب پذیریهای شبکه آگاه باشند و مسئولیت حفاظت از شبکه را بر اساس موقعیتها و نقش خود بر عهده گیرند.

۳- تجربیات، راهبردها و استاندار دهای بین المللی

امنیت سایبر باید بر ا ساس تعداد رو به رشد استانداردها و الگوهای سرآمدی، بصورت داوطلبانه و مبتنی بر توافق جمعی تهیه شود و تجربیات از طریق مؤسسات مشاور و سازمانهای استاندارد بین المللی توسعه یابد. این استانداردها راهنمای مهمی برای سیاستهای داخلی دولت هستند. دولت نیازی ندارد و نبای د استانداردهای فنی برای بخش خصوصی تعیین کند.

۴- اشتراک اطلاعات

کاملا مشخص شده که تلا ش برای ایجاد امنیت سایبر با بی توجهی کاربران نسبت به آسیب پذیریها و حملات مواجه شده است . سازمانهای بخش خصوصی باید تشویق شوند که اطلاعات رخدادهای امنیتی را با سایر سازمانهای این بخش، با دولت، و نیز با سایر کشورها به اشتراک بگذارند.

۵- آموزش و پرورش

استراتژیهای سازمان همکاری اقتصادی آسیا (APEC) میگوید: توسعهٔ منابع انسانی برای به ثمر رسیدن تلاشها در جهت ارتقای سطح امنیت امری ضروری است. بمنظور تأمین امنیت فضای سایبر، دولتها و شرکتهای همکار

[32] - Organization for Eonomic Cooperation and Development

آنها باید کارکنان خود را در مورد موضوعات پیچیدهٔ فنی و قانونی با پشتیبانی از زیرساختهای حیاتی و جرائم فضای سایبر آموزش دهند.

۶- اهمیت حریم خصوصی

شبکه های ICT داده های بسیار حساس شخصی را انتقال می دهند و ذخیره می سازند. حریم خصوصی جزء ضروری اعتماد در فضای سایبر است و استراتژیهای امنیت فضای سایبر باید به روشهای سازگار با ارزشهای مهم جامعه پیاده سازی شود.

۷- ارزیابی آسی بپذیری، هشدار و عکس العمل

همانطور که استراتژیهای سازمان همکاری اقتصادی آسیا نیز ابراز داشت : مبارزهٔ مؤثر با تخلفات فضای سایبر و حفاظت از اطلاعات زیرساختی، وابسته به اقتصادهایی است که سیستم هایی برای ارزیابی تهدیدها و آسیب پذیریها دارند و هشدارهای لازم را صادر می کنند. با شناسایی و اشتراک اطلاعات در مورد یک تهدید قبل از آنکه موجب آسیب گسترده ای شود، شبکه ها بهتر محافظت می شوند.

۸- همکاری بین المللی

برای ساده تر کردن تبادل نظر و همکاری در مورد گسترش یک "فرهنگ امنیتی " میان دولت و بخش خصوصی در سطح بین المللی، دولتها باید با یکدیگر همکاری کنند تا برای جرائم دنیای سایبر قوانین سازگاری به تصویب برسانند و نیروهای انتظامی کشورهای مختلف باید از طریق سازمانهای بین المللی به یکدیگر کمک نمایند.

روند توسعه و اجرای استراتژیهای امنیت سایبر برای دولت با توسعه و اجرای برنامه امنیت سایبر در سایر سازمانها و افراد حقوقی عناصر مشترک دارد. که این عناصر عبارتند از:

- ارزیابی آسیب پذیریها؛
- افزایش سطح آگاهی؛
- گماردن یکنفر بعنوان فرمانده برای ایجاد هماهنگی در سیاستها؛
- توسعهٔ برنامهٔ مدیریت مخاطره
- تطبیق خط مشی های امنیتی مناسب؛
- توجیه ساختاری
- ارزیابی مجدد دورهای و ارتقای مداوم

فاز چهارم اعلام خط مشی های و تصویب قوانین مورد نیاز امنیت سایبر با تمرکز بر سیستم های امنیت دولتی است.

پیاده سازی استراتژی امنیت سایبر در سیستمهای دولتی

در ایالات متحده سیاست امنیتی سیستمهای اطلاعاتی دولت با جزئیات بیشتری مشخص شده و از طریق مصوبهٔ مدیریت امنیت اطلاعات (مصوب سال ۲۰۰۲) پیاده سازی شده است . این قانون برخی روشهای اجرایی سیاست امنیت سایبر را به تصویر می کشد که باعث می شوند در سازمانهای مختلف "پاسخگویی" بوجود بیاید.

هدف مشخص مدیریت امنیت رایانه ای فدرال فیسما FISMA ، مدیریت امنیت رایانه ای در گسترهٔ دولت است، و باعث می شود همهٔ تلاشهای انجام شده برای ایمن سازی اطلاعات با یکدیگر هماهنگ شوند و نیز راهکاری برای تهیه و پشتیبانی حداقل کنترلهای لازم جهت حفاظت از سیستم های اطلاعاتی دولت ارائه گردد . قانون تصدیق می کند که محصولات تجاری راه حلهای مؤثر و پویایی برای دولت فراهم می سازند و انتخاب راه حلهای امنیتی سخت افزاری و نرم افزاری خاص به سازمانهای تخصصی واگذار می گردد.

ضمیما می گویند که رئیس هر سازمان باید یک برنامه امنیت اطلاعات در حیطهٔ سازمان خود تهیه، مستندسازی و اجرا کند و این برنامه بگونه ای باشد که کلیه کارهای سازمان از جمله کارهایی که توسط پیمانکاران مدیریت می شود را در بر بگیرد . این برنامه باید شامل موارد زیر باشد:

۱- ارزیابی متناوب مخاطرات و میزان آسیبی که ممکن است به دلایلی چون دسترسی غیرمجاز به اطلاعات واقع شود.

۲- تدوین سیاستها و روال هایی که: بر اساس فرآیند ارزیابی مخاطره هستند؛ منجر به کاهش هزینه های مخاطرات امنیتی می شوند؛ اطمینان می دهند که امنیت اطلاعات در چرخهٔ حیات سیستم اطلاعاتی هر سازمان بصورت کامل درنظر گرفته شده است؛ و اطمینان می دهند که الزامات و استانداردهای امنیتی ادارهٔ مدیریت و برنامه ریزی براورده می شود.

۳- تهیهٔ طرحهای فرعی برای فراهم کردن امنیت اطلاعات در سطح کافی برای شبکه ها، امکانات، و سیستمها یا گروههای سیستمهای اطلاعاتی؛

۴- برگزاری دوره های آموزشی برای افزایش آگاهی امنیتی کارکنان سازمان، پیمانکاران و سایر کاربران سیستمهای اطلاعاتی که در سازمان کار می کنند؛

۵- سنجش و ارزیابی متناوب اثربخشی سیاستهای امنیت اطلاعات، روالها و تجربیات، که شامل آزمودن کنترلهای مدیریتی، عملکردی و فنی می باشد؛

۶- یک فرآیند برای طراحی، اجرا، ارزیابی و مستندسازی عملیات برای جبران نقائص در سیاستها، روالها، و عملکردهای امنیت اطلاعاتی سازمان؛

۷- روالهایی برای شناسایی، گزارش و پاسخ به وقایع امنیتی؛ و

۸- طرحها و روالهایی برای اطمینان از تداوم فعالیت سیستم های اطلاعاتی سازمان.