فناوری اطلاعات و ارتباطات و امنیت آن

محمد حسین صنیعی [1]

تاریخ دریافت: 12 / 05 / 1392
تاریخ پذیرش: 23 / 07 / 1392

چکیده

عصر حاضر، عصر اطلاعات است و اکثر اندیشمندان و صاحب‌نظران بر این باورند که در این عصر، عرصه‌ها و مؤلفه‌های نوینی در مقوله امنیت پیش روی جوامع بشری قرار می‌گیرد که ابعاد آن پیچیده و گاه رازآلود می‌نماید. از این رو چالش‌ها و درگیری‌ها در این حوزه فراوان است که یکی از آنها در حوزه فناوری اطلاعات و ارتباطات است.

بدون شک، بقا و ادامه حیات هر جامعه و سازمانی بسته به وجود امنیت است و چنانچه تحت شرایطی این مهم به خطر بیفتد، نابودی آن جامعه یا سازمان حتمی خواهد بود. در دوران کنونی که فناوری اطلاعات و ارتباطات در همه ارکان جامعه رسوخ نموده، یکی از نگرانی‌های جدی برای همگان امنیت اطلاعاتی است که از این طریق مبادله می‌گردد؛ زیرا امروزه بخش عمده‌ای از اطلاعات حتی اطلاعات محرمانه و شخصی سازمان‌ها و افراد در این چرخه قرار دارد. بنابراین، یکی از چالش‌های اساسی در بهره‌برداری از فناوری و ارتباطات، امکان دسترسی دیگران به اطلاعات ذخیره یا مبادله شده سایرین است، لذا برقراری امنیت در این بخش امری ضروری، حتمی و غیرقابل انکار بوده که در این نوشتار تلاش بر آن است تا با استفاده از روش بررسی تاریخی به این مهم پرداخته شود.

کلید واژه‌ها:
امنیت/ اطلاعات/ فناوری/ فناوری اطلاعات.

1- استادیار و عضو هیئت علمی دانشگاه عالی دفاع ملی

مقدمه

امروزه اطلاعات در سازمان‌ها و مؤسسات، به‌منزله شاهرگ حیاتی محسوب می‌گردد. دستیابی به اطلاعات و عرضه مناسب و سریع آن، همواره مورد توجه سازمان‌هایی بوده که اطلاعات در آنها دارای نقشی محوری و سرنوشت‌ساز است.

سازمان‌ها و مؤسسات می‌بایست یک زیرساخت مناسب اطلاعاتی را برای خود ایجاد و در جهت انضباط اطلاعاتی در سازمان خود حرکت نمایند. اگر می‌خواهیم ارائه دهنده اطلاعات در عصر اطلاعات بوده و صرفاً مصرف کننده اطلاعات نباشیم، در مرحله نخست می‌بایست فرآیندهای تولید، عرضه و استفاده از اطلاعات را در سازمان خود قانونمند نموده و در مراحل بعد، امکان استفاده از اطلاعات ذی‌ربط را برای متقاضیان موردنظر در سریع‌ترین زمان ممکن فراهم نماییم. حتی سرعت در تولید و عرضه اطلاعات ارزشمند، یکی از رموز موفقیت سازمان‌ها و مؤسسات در عصر اطلاعات است.

موضوع ایجاد یک سازمان مدرن اطلاعاتی است، فراموش نگردد که سازمان ما در این راستا چگونه حرکت کرده است؟ مختصات نقشه اطلاعاتی یک سازمان مدرن چیست؟ مصرف بهینه و هدفمند اطلاعات در صورتی که به افزایش آگاهی، تولید و ارائه اطلاعات ختم شود، فواید آن برای جامعه چیست؟ میزان توانمندی در جلوگیری از وقایع و حوادث کدام است؟ آیا امکان غلبه بر مخالفان و ناراضیان وجود دارد؟ و...

الف– کلیات:

1/الف - بیان مسئله:

با نگاهی به دوران قرون وسطی، معلوم می‌گردد که دولت‌ها در ارتباط با خیانت از طریق ایجاد وحشت مصلحتی جلوی مفسدان را می‌گرفتند و در اواخر سده هجدهم با این مسئله از دیدگاه‌های مختلف علمی و مذهبی که ایجاد تحول را ممکن می‌دانست، مخالفت شد. شهرنشینی موجب شد به‌طور هم‌زمان در نظام‌های سرمایه‌داری افراد غریبه تجمع نمایند و تنها راه کنترل آنها به‌ویژه اقشار خطرناک، تشدید اقدامات کنترلی بود و در واقع این امر اولین جرقه‌های داشتن یک ترکیب اطلاعاتی برای در امان بودن از شر این آدم‌ها که بعضاً نیز سازمان‌یافته مبادرت به ارتکاب جرم می‌نمودند، شد.

طراحی و پیاده‌سازی یک محیط ایمن در سازمان‌های مدرن اطلاعاتی یکی از چالش‌های اساسی در عصر حاضر محسوب می‌گردد. برای بسیاری از سازمان‌ها و مؤسسات توجه جدی به مقوله امنیت اطلاعات هنوز در هاله‌ای از ابهام قرار دارد و برخی دیگر امنیت را تا سطح یک محصول تنزل داده و فکر می‌کنند که با تهیه یک محصول نرم‌افزاری خاص و نصب آن در سامانه، امنیت را برای سازمان خود به ارمغان می‌آورند. همواره باید به خاطر داشته باشیم که امنیت یک فرآیند است، نه یک محصول (گروه مطالعات امنیت، 1387: 42).

وجود یک حفره و یا مشکل امنیتی، می‌تواند یک سازمان را به روش‌های متفاوتی تحت تأثیر قرار دهد. آشنایی با عواقب خطرناک یک حفره امنیتی در یک سازمان و شناسایی مهم‌ترین تهدیدهای امنیتی که می‌تواند حیات یک سازمان را با مشکل مواجه نماید، از جمله موارد ضروری به‌منظور طراحی و پیاده‌سازی یک مدل امنیتی در یک سازمان است.

وجود حفره‌های امنیتی در یک سازمان، می‌تواند پیامدهای منفی متعددی را برای یک سازمان به دنبال داشته باشد که برخی از آنها به شرح زیر است:

- خدشه به اعتبار و شهرت یک سازمان؛

- از دست دادن داده و اطلاعات مهم؛
- اختلال در فرآیندهای جاری یک سازمان؛
- پیامدهای قانونی به دلیل عدم ایجاد یک سیستم ایمن و تأثیر جانبی منفی بر فعالیت سایر سازمان‌ها؛
- سلب اعتماد مردم؛
- سلب اعتماد مسئولین.

بنابراین، گر چه فناوری اطلاعات و ارتباطات سهولت دسترسی، سرعت در انتقال، حجم بالای انباشتگی، سرعت پردازش و...را باعث شده است، لیکن آنچه که موجب دغدغه و نگرانی در این روند بوده و چالش اساسی محسوب می‌گردد، امنیت اطلاعات در این چرخه است؛ امری که در این مقاله به آن پرداخته می‌شود.

2/الف - هدف تحقیق:

توجه به امنیت در فناوری اطلاعات و ارتباطات.

3/الف - سؤال تحقیق:

چرا توجه به امنیت در فناوری اطلاعات و ارتباطات الزامی است؟

ب– ادبیات نظری:

1/ب - امنیت اطلاعات در سازمان‌ها طی سالیان اخیر:

ماحصل بررسی انجام شده توسط مؤسسات و مراکز تحقیقاتی معتبر در خصوص امنیت اطلاعات، نشان‌دهنده این واقعیت مهم است که حملات مهاجمان بر روی عملکرد و درآمد و هزینه‌های یک سازمان به‌طور مستقیم و یا غیرمستقیم تأثیرگذار خواهد بود؛ یعنی کاهش درآمد و افزایش هزینه (گادسون، 1387: 84).

در سال 2003، ویروس‌ها و حملات از نوع DoS (برگرفته از Denial of Service) بیشترین تبعات منفی را برای سازمان‌ها به دنبال داشته است.

در سال 2004، سرقت اطلاعات بالاترین جایگاه را داشته و حملات از نوع DoS با اندکی کاهش نسبت به سال 2003، در رتبه دوم قرار گرفته است.

با اینکه هزینه پیاده‌سازی یک سیستم حفاظتی اندک نیست، لیکن می‌توان آن را به‌عنوان بخشی از هزینه‌هایی درنظر گرفت که یک سازمان به دلیل عدم ایمن‌سازی، می‌بایست پرداخت نماید (برخورد با تبعات منفی).

2/ب - ضرورت امینت:

1- بروز تهدیدها:

اکثر قریب به اتفاق سازمان‌ها در معرض انواع تهدیدهای داخلی و خارجی خرابکاران هستند؛ تهدیدهایی چون دست‌کاری اطلاعات مرجع و یا سرقت اطلاعات حیاتی و سرمایه‌های اطلاعاتی. در چنین شرایطی، عواملی که می‌توانند از مزایای سیستم‌ها به‌شمار روند (مثل سرعت و قابلیت دسترسی بالا)، اگر تحت کنترل نباشند، ممکن است باعث بروز آسیب‌پذیری شوند و سوءاستفاده افراد بد نیّت از آنها به نفوذ و خرابکاری، کلاهبرداری و یا اخاذی بیانجامد. علاوه بر این، مشکلات طبیعی و خطاهای غیرعمدی که توسط کاربران رایانه‌ای رخ می‌دهد، در صورت فقدان روال صحیح برای حفاظت از اطلاعات، می‌تواند نتایج مخربی به‌بار آورد.

امروزه ما در دنیایی زندگی می‌کنیم که پردازش اطلاعات در آن ارزان و هزینه‌های ارتباطات رو به کاهش است و جهان به‌طور فزاینده‌ای در تبادل و تعامل اطلاعات به‌سر می‌برد. اما فراهم شدن امکانات فنی جدید تنها باعث پیدایش محصولات نوین و راه‌های بهتر و کارآمدتر برای انجام امور نشده، بلکه در کنار آن امکان سوءاستفاده از فناوری را نیز افزایش داده است. فناوری اطلاعات و ارتباطات نیز همانند سایر فناوری‌ها حالت ابزاری داشته و می‌توان آن را به‌گونه‌ای مورد استفاده قرار داد که برای همگان مفید باشد و یا به نحوی از آن استفاده کرد که نتایج خطرناکی به‌بار آورد.

سرعت انتقال در فناوری اطلاعات و ارتباطات چیزی در حدود میکرو ثانیه است که باعث می‌شود اطلاعات غیرقابل مشاهده، تحت کنترل نرم‌افزارهای تهیه شده توسط افراد، جابه‌جا شود. در چنین فضایی اعمال غیرقانونی و مخرب آن‌قدر سریع صورت می‌گیرد که می‌تواند غیرقابل شناسایی باشد؛ هرچند شناسایی آن غیرممکن نیست. به عنوان مثال؛ سیستم‌های تجاریِ رایانه‌ای، نزدیک به پنجاه سال قدمت دارند و سیستم‌های بانکداری نیز انتقال الکترونیکی پول را تقریباً در همان زمان آغاز کرده‌اند. در این سیستم‌های تجاری، برای ارتکاب جرم از طریق نفوذ به شبکه‌های رایانه‌ای و سیستم‌های مالی، انگیزه‌های قوی وجود دارد.

2- فناوری اطلاعات:

انقلاب رایانه‌های شخصی که در اواسط دهه 1970 میلادی شروع شد، موجب شده در حال حاضر رایانه‌های قدرتمند در دسترس صدها میلیون نفر باشند. علاوه بر آن اینترنت و انواع شبکه‌های شخصی، ارتباطات بین رایانه‌ای را میان بسیاری از مردم امکان‌پذیر نمودند.

صدها میلیون رایانه برای پردازش هرگونه اطلاعات قابل تصوری به‌کار می‌روند که با یک شبکه ارتباطی قوی به نام اینترنت به‌هم متصل شده‌اند. این شبکه موجب گسترش ارتباطات مردمی شده و همچنین امکان دسترسی آسان و نسبتاً ارزان به داده‌های دیجیتالی و اسناد تجهیزات فنی و محصولات در حال ساخت را به‌وجود آورده است. عمده کاربران شبکه‌های رایانه‌ای دهه 1970 میلادی را کارشناسان حرفه‌ای رایانه تشکیل می‌دادند؛ حال آنکه امروز بیشتر کاربران از افراد غیرحرفه‌ای هستند و ممکن است عدم اطلاعات کافی آنان باعث شود که از بسته‌های نرم‌افزاری ایمن استفاده مناسب نکنند و در نتیجه نفوذگران و تبهکاران رایانه‌ای صرف‌نظر از محل جغرافیایی خود و یا کاربر، بتوانند به سیستم حمله و از آن سوءاستفاده کنند.

در کنار همه این مسائل، موضوع جرائم سازمان‌یافته دنیای مجازی بر پیچیدگی کار دولت‌ها برای تأمین امنیت زیرساخت‌های حیاتی خدمات عمومی می‌افزاید و تبعات

سنگین سوءاستفاده تبهکاران از منابع دولتی، اهمیت پرداختن صحیح و مؤثر آنها به موضوع امنیت را دو چندان می‌کند (عبدالله‌خانی، 1386: 36).

آمارهای جهانی از رخدادهای پایگاه‌های وب دولتی و تجاری که توسط ویروس، کرم و حملات تخریب سرویس به وقوع پیوسته، آسیب‌پذیری این سیستم‌ها را به‌خوبی به تصویر می‌کشد. به‌عنوان مثال؛ طبق تخمین دستگاه‌های امنیتی ایالات متحده (که به‌عنوان پیشرو در حوزه فناوری‌های اطلاعات و ارتباطات شناخته می‌شود) تنها در سال 2003 ضررهای ناشی از خدشه‌دار شدن امنیت سازمان‌ها بالغ بر 10 میلیارد دلار برآورد شده است.

در دنیای امروز، اعتبارات مالی بیشتر و بیشتر به‌صورت الکترونیکی جابه‌جا می‌شوند، اطلاعات مختلف با حساسیت‌های کم و زیاد از طریق شبکه‌ها منتقل می‌شوند، سامانه‌های رایانه‌ای با سرعت بسیار زیادی پیچیده‌تر و مرتبط‌تر با دنیای بیرونی می‌شوند و ابزارهای ساده نفوذ و بهره‌برداری از آسیب‌پذیری‌ها بیش از هر زمان دیگری در دسترس ماجراجویان دنیای مجازی قرار دارد؛ و هر یک از این عوامل خود به تنهایی دلیل محکمی برای جدی گرفتن موضوع امنیت است که بایستی توسط سازمان‌های ذی‌ربط برقرار گردد.

سیر پیشرفت فناوری اطلاعات و ارتباطات و نوآوری‌های حاصل از آن، موجب افزایش چشمگیر بهره‌وری و پیدایش انواع جدیدی از کالاها و خدمات شده است. با بهبود روزافزون قدرت، ظرفیت و قیمت تجهیزات میکرو الکترونیکی که به رشد سالانه تقریباً 30 درصدی بهره‌وری این تجهیزات نسبت به قیمت منجر شده، امکان استفاده از این فناوری برای همه میسر شده است.

اما کاربران و راهبران فنی در کشورهای در حال توسعه معمولاً فاقد توانایی ارائه این سطح از پشتیبانی هستند. تعداد کاربران اندک است و به هشدارها و راه‌حل‌های ارائه شده نیز توجه نمی‌شود. سازمان‌هایی که از رایانه استفاده می‌کنند، غالباً دارای بخش ستادی کوچکی هستند که توانایی نظارت بر منابع فنی داخلی خود را ندارند. بسیاری از اوقات این عدم توجه و ناتوانی به دلیل عدم وجود اطلاعات و دانش کافی درباره سیستم‌های

رایانه‌ای و امنیت شبکه است و گروه‌هایی هم که اصول اساسی را درک کرده‌اند، معمولاً در فهم چگونگی سازگارسازی راهکارهای فنی با شرایط متغیر و غیرقابل پیش‌بینیِ این محیط، مشکل دارند.

از سوی دیگر فروشگاه‌ها و مراکز خدمات تعمیرات رایانه معمولاً از مشکلاتی که در سایر نقاط دنیا به‌وجود می‌آیند، مطلع نیستند و در نتیجه کاربران و راهبران، به قربانیان توسعه اطلاعات مربوط به امنیت فناوری تبدیل می‌شوند. نقص امنیتی شبکه در همه کشورها اتفاق می‌افتد و حتی ممکن است موجب تحت فشار قرارگرفتن دولت‌ها نیز بشود؛ به غیر از این، بسیاری از این نقص‌ها معمولاً گزارش نمی‌شوند؛ چرا که اطلاع عموم مردم از آنها می‌تواند نتایج نامطلوبی برای سازمان‌ها به‌بار آورد.

دولت‌ها و سازمان‌های موجود در کشورهای توسعه‌یافته عموماً توانایی مقابله با چنین نقص‌هایی را دارند، ولی نتایج ناشی از بروز نقص‌ها و اشکالات امنیتی در کشورهای در حال توسعه می‌تواند بسیار وخیم‌تر از کشورهای توسعه یافته باشد (خدابنده، 1386: 18).

در کنار همه این موارد، بازارها، سازمان‌ها و دولت‌های کشورهای در حال توسعه، به دلیل عدم توجه به عواقب ناشی از نفوذهای رایانه‌ای در حجم وسیع، عدم توانایی تحلیل ضررهای مالی ناشی از این حملات و نیز نداشتن تخمین مناسب از زمان لازم برای ترمیم خسارات وارده، معمولاً تمایل چندانی به رفع نقایص امنیتی ندارند.

3- الزام پیشگیری:

یک رویکرد پیشگیرانه می‌تواند به یک سازمان در جهت کاهش تعداد حوادث امنیتی در آینده کمک نماید، ولی این بدین معنی نخواهد بود که چنین مسائلی در آینده اتفاق نخواهند افتاد. بنابراین، سازمان‌ها می‌بایست فرآیند پاسخ به حوادث امنیتی را بهبود داده و به‌طور هم‌زمان ایجاد رویکردهای پیشگیرانه درازمدت را در دستور کار خود قرار دهند.

استفاده «درست و مشروع» از اطلاعات «صحیح»، یکی از الزامات بسیار مهم برای دستیابی سازمان‌ها به اهداف سازمانی است و قابلیت اطمینان، یکپارچگی و در دسترس بودن این اطلاعات، از مؤلفه‌های بسیار مهم در کارایی آنها هستند (آدامز، 1380: 25).

مزایای ذخیره‌سازی ساختارمند اطلاعات به‌صورت الکترونیکی، کاربرد وسیع رایانه‌ها در اهداف تجاری را ناگزیر کرده و استفاده از شبکه‌های رایانه‌ای و به‌ویژه اینترنت، تغییرات اساسی را در فرآیندهای کسب و کار به‌وجود آورده و باعث شده که حجم بسیار زیادی از اطلاعات تنها به اندازه یک سر انگشت با ما فاصله داشته باشند؛ و ناگفته پیداست که در یک محیط پیچیده با این ارتباطات وسیع، مخاطرات گسترده‌ای سیستم‌های رایانه‌ای، سیستم‌های اطلاعاتی، و فعالیت‌ها و زیرساخت‌های حیاتی وابسته به آنها را تهدید کنند. به عنوان مثال؛

- در سال 2004، 70% سازمان‌ها حداقل یک مرتبه مورد تهاجم قرار گرفته‌اند؛
- در سال 2003 بالغ بر 666 میلیون دلار صرف برخورد با مشکلات امنیتی در سازمان‌ها شده است؛
- نیمی از سازمان‌ها به این موضوع اعتراف نموده‌اند که نمی‌دانند چه میزان از اطلاعات سازمان خود را به دلیل حملات از دست داده‌اند؛
- 41% سازمان‌ها اعلام داشته‌اند که دارای هیچ‌گونه طرح و یا برنامه‌ای برای گزارش و یا پاسخ به تهدیدهای امنیتی نمی‌باشند.

3/ب - مزایای سرمایه‌گذاری در امنیت اطلاعات:

- کاهش احتمال غیرفعال شدن سیستم‌ها و برنامه‌ها (از دست دادن فرصت‌ها) ؛
- استفاده مؤثر از منابع انسانی و غیرانسانی در یک سازمان)؛
- کاهش هزینه از دست دادن داده توسط ویروس‌های مخرب و یا حفره‌های امنیتی (حفاظت از داده‌های ارزشمند) ؛
- افزایش حفاظت از مالکیت معنوی.

4/ب - ضرورت توجه به امنیت اطلاعات:

فناوری اطلاعات دارای یک نقش حیاتی و تعیین‌کننده در اکثر سازمان‌های مدرن اطلاعاتی است. امروزه زیرساخت فناوری اطلاعات سازمان‌ها در محیطی قرار گرفته‌اند که

به‌طور فزاینده بر تعداد دشمنان و مهاجمانی که علاقه‌مند به حضور مستمر، مطمئن و سودمند سیستم‌های رایانه‌ای نیست، افزوده می‌گردد. حملات، روند کاملاً صعودی را داشته و متأسفانه اغلب سازمان‌ها قادر به واکنش مناسب در مقابل تهدیدهای امنیتی جدید در زمان مطلوب و قبل از سوءاستفاده از سیستم‌های رایانه‌ای خود نیست.

کاهش مدت زمان لازم به‌منظور برخورد با تهدیدهای امنیتی و افزایش بهره‌وری، از جمله خواسته‌های مشترک سازمان‌ها و کاربران است. به‌منظور برخورد مناسب و سازمان‌یافته با تهدیدهای امنیتی، مدیریت خطرات امنیتی و یا مدیریت ریسک امنیتی به یکی از نیازهای اولیه و اساسی مراکز فناوری اطلاعات تبدیل شده است.

5/ب- مفاهیم مدیریت خطرات امنیتی (مدیریت ریسک):

در بسیاری از سازمان‌ها، ضرورت توجه به «مدیریت خطرات امنیتی» پس از بروز یک حادثه امنیتی کوچک نظیر آلودگی یک رایانه توسط ویروس و یا هدف قرارگرفتن وب‌سایت سازمان، احساس می‌گردد. در ادامه با افزایش حملات و تشدید اوضاع، مشکلات و مسائل امنیتی متعددی برای سازمان‌ها ایجاد می‌گردد. سازمان‌ها یکی پس از دیگری در مواجهه منطقی با مشکلات امنیتی، ناامید شده و به‌منظور برخورد با بحران‌های امنیتی، برخوردهای انفعالی را در دستور کار خود قرار می‌دهند.

افزایش بی رویه حملات موفقیت‌آمیز مبتنی بر شبکه، ضرورت پیاده‌سازی یک رویکرد پیشگیرانه (در مقابل رویکردهای انفعالی) برای مدیریت خطرات امنیتی را برای بسیاری از سازمان‌ها به اثبات رسانده است (برایهول، 1388).

مدیریت خطرات امنیتی، فرآیندی است که در آن تهدیدهای موجود در یک سازمان شناسایی، اولویت‌بندی و نحوه مدیریت آنان در یک سطح قابل‌قبول مشخص می‌گردد.

وجود یک استراتژی مدون به‌منظور مدیریت خطرات امنیتی، سازمان‌ها را قادر می‌سازد که فرآیندهایی را به‌منظور شناسایی و اولویت‌بندی فعالیت‌ها در محیط فناوری اطلاعات پیاده‌سازی و از آنان نگهداری نمایند.

جایگزینی برخوردهای پیشگیرانه با برخوردهای انفعالی، مهم‌ترین دستاورد مدیریت خطرات امنیتی در یک سازمان می‌باشد که قطعاً بهبود وضعیت یک سازمان را به‌دنبال خواهد داشت؛ چرا که احتمال دستیابی مستمر به زیرساخت فناوری اطلاعات، افزایش یافته و در فرآیندهای جاری یک سازمان خللی ایجاد نمی‌گردد.

پیاده‌سازی فرآیند مدیریت خطرات امنیتی برای سازمان‌ها دستاوردهای متعددی را به دنبال خواهد داشت که عبارتند از:

1- زمان پاسخ به تهدیدها:

با ایجاد سازمان امنیتی، کشورها می‌توانند در مقابل تهدیدهای امنیتی جدید در زمان مناسب و به سرعت واکنش لازم را داشته باشند (قبل از سوءاستفاده سرویس‌های حریف).

مدیریت خطرات امنیتی، بستر لازم برای پیشگیری در مقابل تهدیدها و یا آسیب‌پذیری سازمان‌ها را فراهم می‌نماید. بدین ترتیب، نحوه برخورد کشور با مسائل و مشکلات امنیتی از واکنش‌های انفعالی به واکنش‌های پیشگیرانه تغییر خواهد کرد.

2- هزینه‌های مدیریت زیرساخت:

فرآیند مدیریت خطرات امنیتی، سازمان‌ها را قادر می‌سازد که با یک وضعیت مطلوب، مقرون به صرفه و در یک سطح قابل‌قبول امنیتی، فعالیت‌های جاری خود را انجام دهند. فرآیند فوق همچنین یک مسیر مشخص و پایدار برای سازماندهی و اولویت‌بندی منابع محدود را به‌منظور مدیریت خطرات، ارائه می‌نماید. مزایای داشتن یک سازمان امنیتی، زمانی هویدا می‌گردد که سازمان‌ها بتوانند کنترل‌هایی مقرون به صرفه، به‌منظور کاهش تهدیدهای امنیتی را پیاده‌سازی نمایند.

3- مدیریت و اولویت‌بندی خطرات:

مدیریت خطرات امنیتی، می‌تواند به یک سازمان کمک نماید که اصول امنیتی را به‌منظور کاهش بیشترین خطرات در محیط مربوطه به‌کار گیرد (نه اینکه از یک رویکرد غیرمنسجم برای ایمن‌سازی عناصر مجزا در سازمان استفاده گردد).

4- جلوگیری از رویکردهای انفعالی:

فرآیندی است که بر اساس آن صرفاً پس از بروز یک حادثه امنیتی به آن پاسخ داده می‌شود. تعداد زیادی از کارشناسان حرفه‌ای فناوری اطلاعات همواره با این محدودیت مواجه می‌باشند که فعالیت‌ها را به‌گونه‌ای انجام و به اتمام برسانند که کمترین مشکل را برای کارکنان ایجاد نماید.

پس از بروز یک مشکل امنیتی، کارشناسان فناوری اطلاعات صرفاً می‌توانند از پیشرفت مشکل جلوگیری نموده و پس از ایزوله نمودن آن، مشکل سیستم‌های آلوده را برطرف نمایند. شاید در این رابطه برخی علاقه‌مند باشند که عامل اصلی بروز مشکل را پیدا نمایند، ولی با توجه به محدودیت زمان و منابع موجود در سازمان، عملاً امکان انجام آن وجود نخواهد داشت. متأسفانه برای بسیاری از سازمان‌ها همچنان رویکردهای انفعالی یک نگرش مؤثر به‌منظور برخورد با تهدیدهای امنیتی است (پس از بروز مشکل در رابطه با نحوه برخورد با آن تصمیم گرفته می‌شود و برای پیشگیری از بروز حوادث، از رویکرد خاصی تبعیت نمی‌گردد).

این فرآیند باعث کاهش خطر آسیب‌پذیری در یک سازمان می‌گردد. مدیریت پیشگیری از خطرات امنیتی دارای مزایای متعددی نسبت به یک رویکرد انفعالی است. در مقابل اینکه منتظر بمانیم تا یک حادثه اتفاق افتد و به آن پاسخ دهیم، احتمال بروز مشکل در اولین مکان را کاهش خواهیم داد. بدین منظور از رویه‌هایی خاصی به‌منظور حفاظت از سرمایه‌های مهم سازمان استفاده می‌گردد.

با پیاده‌سازی کنترل‌هایی که کاهش آسیب‌پذیری سیستم و سوءاستفاده از آنان توسط نرم‌افزارهای مخرب را به‌دنبال خواهد داشت، امکان سوءاستفاده مهاجمان از فرصت‌های ایجاد شده کاهش یافته و پیشگیری لازم در این خصوص انجام خواهد شد.

- برنامه‌های اسب تروا (دشمنانی در لباس دوست):

برنامه‌های اسب تروا و یا Trojans، به منزله ابزارهایی برای توزیع کدهای مخرب می‌باشند. تروجان‌ها، می‌توانند بی‌آزار بوده و یا حتی نرم‌افزاری مفیدی نظیر بازی‌های رایانه‌ای باشند که با تغییر قیافه و با لباسی مبدل و ظاهری مفید خود را عرضه می‌نمایند. تروجان‌ها، قادر به انجام عملیات متفاوتی نظیر حذف فایل‌ها، ارسال یک نسخه از خود به لیست آدرس‌های پست الکترونیکی، می‌باشند. این نوع از برنامه‌ها صرفاً می‌توانند از طریق تکثیر برنامه‌های اسب تروا به یک رایانه، دریافت فایل از طریق اینترنت و یا باز نمودن یک فایل ضمیمه همراه یک نامه الکترونیکی، اقدام به آلودگی یک سیستم نمایند (بوریس‌دی، 1382).

- ویرانگرها:

در وب‌سایت‌های متعددی از نرم‌افزارهایی نظیر اکتیو ایکس‌ها و یا اپلت‌های جاوا استفاده می‌گردد. این نوع برنامه‌ها به‌منظور ایجاد انیمیشن و سایر افکت‌های خاص مورد استفاده قرار گرفته و جذابیت و میزان تعامل با کاربر را افزایش می‌دهند. با توجه به دریافت و نصب آسان این نوع از برنامه‌ها توسط کاربران، برنامه‌های فوق به ابزاری مطمئن و آسان به‌منظور آسیب‌رسانی به سایر سیستم‌ها تبدیل شده‌اند. این نوع برنامه‌ها که به «ویرانگران» شهرت یافته‌اند، به شکل یک برنامه نرم‌افزاری و یا اپلت ارائه و در دسترس استفاده‌کنندگان قرار می‌گیرند. برنامه‌های فوق، قادر به ایجاد مشکلات متعددی برای کاربران می‌باشند (از بروز اشکال در یک فایل تا ایجاد اشکال در بخش اصلی یک سیستم رایانه‌ای).

- حمله‌ها:

تاکنون حمله‌های متعددی متوجه شبکه‌های رایانه‌ای بوده که می‌توان تمامی آنان را به سه گروه عمده تقسیم نمود:

1- حملات شناسایی: در این نوع حملات، مهاجمان اقدام به جمع‌آوری و شناسایی اطلاعات با هدف تخریب و آسیب‌رساندن به آنان می‌نمایند. مهاجمان در این رابطه، از

نرم‌افزارهای خاصی نظیر Sniffer و یا Scanner به‌منظور شناسایی نقاط ضعف و آسیب‌پذیر رایانه‌ها، سرویس دهندگان وب و برنامه‌ها، استفاده می‌نمایند. در این رابطه برخی تولیدکنندگان، نرم‌افزارهایی را با اهداف خیرخواهانه طراحی و پیاده‌سازی نموده‌اند که متأسفانه از آنان در جهت اهداف مخرب نیز استفاده می‌شود. مثلاً به‌منظور تشخیص و شناسایی رمزهای عبور، نرم‌افزارهای متعددی تاکنون طراحی و پیاده‌سازی شده است. نرم‌افزارهای فوق با هدف کمک به مدیران شبکه، افراد و کاربرانی که رمز عبور خود را فراموش کرده و یا آگاهی از رمز عبور افرادی که سازمان خود را بدون اعلام رمز عبور به مدیر شبکه، ترک نموده‌اند، استفاده می‌گردند. به هر حال وجود این نوع نرم‌افزارها واقعیتی انکارناپذیر بوده که می‌تواند به منزله یک سلاح مخرب در اختیار مهاجمان قرار گیرد.

2- حملات دستیابی: در این نوع حملات، هدف اصلی مهاجمان، نفوذ در شبکه و دستیابی به آدرس‌های پست الکترونیکی، اطلاعات ذخیره شده در بانک‌های اطلاعاتی و سایر اطلاعات حساس، می‌باشد.

3- حملات از کار انداختن سرویس‌ها: در این نوع حملات، مهاجمان سعی در ایجاد مزاحمت به‌منظور دستیابی به تمام و یا بخشی از امکانات موجود در شبکه برای کاربران مجاز می‌نمایند. حملات فوق به اشکال متفاوت و با بهره‌گیری از فناوری‌های متعددی صورت می‌پذیرد. ارسال حجم بالایی از داده‌های غیرواقعی برای یک ماشین متصل به اینترنت و ایجاد ترافیک کاذب در شبکه، نمونه‌هایی از این نوع حملات هستند (دستورالعمل اجرایی مدیریت امنیت اطلاعات، 1388).

- رهگیری داده (استراق سمع):

بر روی هر شبکه رایانه‌ای روزانه اطلاعات متفاوتی جابه‌جا می‌گردد و همین امر می‌تواند موضوعی مورد علاقه برای مهاجمان باشد. در این نوع حملات، مهاجمان اقدام به استراق‌سمع و یا حتی تغییر بسته‌های اطلاعاتی در شبکه می‌نمایند. مهاجمان به‌منظور نیل به اهداف مخرب خود، از روش‌های متعددی به‌منظور شنود اطلاعات، استفاده می‌نمایند.

- کلاهبرداری (ابتدا جلب اعتماد و سپس تهاجم):

کلاهبرداران از روش‌های متعددی به‌منظور اعمال شیادی خود استفاده می‌نمایند. با گسترش اینترنت، این نوع افراد فضای مناسبی برای اعمال مخرب خود یافته‌اند (چرا که می‌توان به هزاران نفر در زمانی کوتاه و از طریق اینترنت دستیابی داشت). در برخی موارد شیادان با ارسال نامه‌های الکترونیکی وسوسه‌انگیز، از خوانندگان می‌خواهند که اطلاعاتی خاص را برای آنان ارسال نموده و یا از یک سایت به‌عنوان طعمه در این رابطه استفاده می‌نمایند (گادسون، 1384)

به‌منظور پیشگیری از این‌گونه اعمال، می‌بایست کاربران دقت لازم در خصوص درج نام، رمز عبور و سایر اطلاعات شخصی در سایت‌هایی که نسبت به هویت آنان شک و تردید وجود دارد را داشته باشند. با توجه به سهولت جعل آدرس‌های پست الکترونیکی، می‌بایست به این نکته توجه گردد که قبل از ارسال اطلاعات شخصی برای هر فرد، هویت وی شناسایی گردد. هرگز بر روی لینک‌ها و یا ضمائمی که از طریق یک نامه الکترونیکی برای شما ارسال شده است، کلیک نکرده و همواره می‌بایست به شرکت‌ها و مؤسساتی که به‌طور شفاف آدرس فیزیکی و شماره تلفن‌های خود را ذکر نمی‌نمایند، شک و تردید داشت.

- نامه‌های الکترونیکی ناخواسته:

از واژه Spam در ارتباط با نامه‌های الکترونیکی ناخواسته و یا پیام‌های تبلیغاتی ناخواسته، استفاده می‌گردد. این قبیل نامه‌های الکترونیکی، عموماً بی‌ضرر بوده و صرفاً ممکن است مزاحمت و یا دردسر ما را بیشتر نمایند. دامنه این نوع مزاحمت‌ها می‌تواند از به هدر رفتن زمان کاربر تا هرز رفتن فضای ذخیره‌سازی بر روی رایانه‌های کاربران را شامل می‌شود.

- ابزارهای امنیتی:

پس از آشنایی با تهدیدها، می‌توان تمهیدات امنیتی لازم در خصوص پیشگیری و مقابله با آنان را انجام داد. بدین منظور می‌توان از فناوری‌های متعددی نظیر آنتی‌ویروس‌ها و یا فایروال‌ها، استفاده به‌عمل آورد.

- نرم افزارهای آنتی‌ویروس:

نرم‌افزارهای آنتی‌ویروس، قادر به شناسایی و برخورد مناسب با اکثر تهدیدهای مربوط به ویروس‌ها می‌باشند (مشروط به اینکه این نوع نرم‌افزارها به‌صورت منظم به‌هنگام شده و به درستی پشتیبانی گردند). نرم‌افزارهای آنتی‌ویروس در تعامل اطلاعاتی با شبکه‌ای گسترده از کاربران بوده و در صورت ضرورت پیام‌ها و هشدارهای لازم در خصوص ویروس‌های جدید را اعلام می‌نمایند. بدین ترتیب، پس از شناسایی یک ویروس جدید، ابزار مقابله با آن سریعاً پیاده‌سازی و در اختیار عموم کاربران قرار می‌گیرد. با توجه به طراحی و پیاده‌سازی ویروس‌های متعدد در سراسر جهان و گسترش سریع آنان از طریق اینترنت، می‌بایست بانک اطلاعاتی ویروس‌ها بر اساس فرآیندی مشخص و مستمر، به‌هنگام گردد.

- سیاست‌های امنیتی:

سازمان‌های بزرگ و کوچک نیازمند ایجاد سیاست‌های امنیتی لازم در خصوص استفاده از رایانه و ایمن‌سازی اطلاعات و شبکه‌های رایانه‌ای می‌باشند. سیاست‌های امنیتی، مجموعه قوانین لازم به‌منظور استفاده از رایانه و شبکه‌های رایانه‌ای بوده که در آن وظایف تمامی کاربران دقیقاً مشخص و در صورت ضرورت، هشدارهای لازم به کاربران در خصوص استفاده از منابع موجود در شبکه داده می‌شود. دانش تمامی کاربرانی که به تمام و یا بخشی از شبکه دستیابی دارند، می‌بایست به‌صورت منظم و با توجه به سیاست‌های تدوین یافته، به‌هنگام گردد؛ یعنی آموزش مستمر و هدفمند با توجه به سیاست‌های تدوین شده، اجرایی گردد (سند راهبردی، 1388).

- رمزهای عبور:

هر سیستم رایانه‌ای می‌بایست دارای ایمنی مناسبی در خصوص رمزهای عبور باشد. استحکام رمزهای عبور، ساده‌ترین و در عین حال متداول‌ترین روش به‌منظور اطمینان از این موضوع است که صرفاً افراد تأیید شده و مجاز قادر به استفاده از رایانه و یا بخش‌های خاصی از شبکه می‌باشند. فراموش نکنیم که زیرساخت‌های امنیتی ایجاد شده، در صورتی

که کاربران دقت لازم در خصوص مراقبت از رمزهای عبور خود را نداشته باشند، مؤثر نخواهد بود (خط بطلانی بر تمامی تلاش‌های انجام شده). اکثر کاربران در زمان انتخاب رمز عبور، از اعداد و یا کلماتی استفاده نمایند که به‌خاطر آوردن آنان ساده باشد (نظیر تاریخ تولد، شماره تلفن). برخی دیگر از کاربران علاقه‌ای به تغییر منظم رمزهای عبور خود در مقاطع زمانی خاصی نداشته و همین امر می‌تواند زمینه تشخیص رمزهای عبور توسط مهاجمان را فراهم نماید. در زمان تعریف رمز عبور، می‌بایست تمهیداتی به شرح زیر، در خصوص استحکام و نگهداری مطلوب آنان اندیشیده گردد:

- حتی‌المقدور سعی گردد از رمزهای عبور فاقد معنی خاصی استفاده گردد؛
- به صورت منظم و در مقاطع زمانی مشخص شده، اقدام به تغییر رمزهای عبور گردد؛
- عدم افشای رمزهای عبور برای سایرین.

- فایروال‌ها:

فایروال، راه‌حلی سخت‌افزاری و یا نرم‌افزاری به‌منظور تأکید (اصرار) بر سیاست‌های امنیتی می‌باشد. یک فایروال نظیر قفل موجود بر روی یک درب منزل و یا بر روی درب یک اطاق درون منزل می‌باشد. بدین ترتیب صرفاً کاربران تأیید شده (آنانی که دارای کلید دستیابی می‌باشند) امکان ورود به سیستم را خواهند داشت. فایروال‌ها دارای فیلترهای از قبل تعبیه شده‌ای بوده که امکان دستیابی افراد غیرمجاز به منابع سیستم را سلب می‌نمایند.

- رمزنگاری:

فناوری رمزنگاری، امکان مشاهده، مطالعه و تفسیر پیام‌های ارسالی توسط افراد غیرمجاز را سلب می‌نماید. از رمزنگاری به‌منظور حفاظت داده‌ها در شبکه‌های عمومی نظیر اینترنت استفاده می‌گردد. در این رابطه از الگوریتم‌های پیشرفته ریاضی به‌منظور رمزنمودن پیام‌ها و ضمائم مربوطه، استفاده می‌شود.

- امنیت اطلاعات در شبکه‌های رایانه‌ای:

به موازات حرکت به‌سمت یک سازمان مدرن و مبتنی بر تکنولوژی اطلاعات، می‌بایست تدابیر لازم در رابطه با حفاظت از اطلاعات نیز اندیشیده گردد. مهم‌ترین مزیت و رسالت شبکه‌های رایانه‌ای، اشتراک منابع سخت‌افزاری و نرم‌افزاری است. کنترل دستیابی و نحوه استفاده از منابع به‌اشتراک گذاشته شده، از مهم‌ترین اهداف یک سیستم امنیتی در شبکه است. با گسترش شبکه‌های رایانه‌ای خصوصاً اینترنت، نگرش نسبت به امنیت اطلاعات و سایر منابع به‌اشتراک گذاشته شده، وارد مرحله جدیدی شده است. در این راستا، لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند، پایبند به یک استراتژی خاص بوده و بر اساس آن سیستم امنیتی را اجرا و پیاده‌سازی نماید. عدم ایجاد سیستم مناسب امنیتی، می‌تواند پیامدهای منفی و دور از انتظاری را به دنبال داشته باشد. استراتژی سازمان ما برای حفاظت و دفاع از اطلاعات چیست؟ در صورت بروز مشکل امنیتی در رابطه با اطلاعات در سازمان، به دنبال کدامین مقصر می‌گردیم؟ شاید اگر در چنین مواردی، همه مسائل امنیتی و مشکلات به‌وجود آمده را به خود رایانه نسبت دهیم، بهترین امکان برون‌رفت از مشکلِ به‌وجود آمده است؛ چرا که رایانه توان دفاع کردن از خود را ندارد. آیا واقعاً روش و نحوه برخورد با مشکل به‌وجود آمده، چنین است؟ در حالی که یک سازمان برای خرید سخت‌افزار نگرانی‌های خاص خود را داشته و سعی در برطرف نمودن معقول آنها دارد، آیا برای امنیت و حفاظت از اطلاعات، نباید نگرانی به‌مراتب بیشتری در سازمان وجود داشته باشد؟ (بسته آموزشی امنیت تجارت الکترونیک، 1386).

- استراتژی (راهبرد):

دفاع در عمق، عنوان یک راهبرد عملی به‌منظور نیل به تضمین و ایمن‌سازی اطلاعات در محیط‌های شبکه امروزی است. استراتژی فوق، یکی از مناسب‌ترین و عملی‌ترین گزینه‌های موجود است که متأثر از برنامه‌های هوشمند برخاسته از تکنیک‌ها و تکنولوژی‌های متفاوت تدوین می‌گردد. استراتژی پیشنهادی، بر سه مؤلفه متفاوت ظرفیت‌های حفاظتی، هزینه‌ها و رویکردهای عملیاتی تأکید داشته و توازنی معقول بین آنان

را برقرار می‌نماید. در این مقاله به بررسی عناصر اصلی و نقش هر یک از آنان در استراتژی پیشنهادی، پرداخته خواهد شد.

6/ب - دشمنان، انگیزه‌ها، انواع حملات اطلاعاتی:

به منظور دفاع مؤثر و مطلوب در مقابل حملات به اطلاعات و سیستم‌های اطلاعاتی، یک سازمان می‌بایست دشمنان، پتانسیل و انگیزه‌های آنان و انواع حملات را به درستی برای خود آنالیز تا از این طریق دیدگاهی منطقی نسبت به موارد فوق ایجاد و در ادامه امکان برخورد مناسب با آنان فراهم گردد. اگر قصد تجویز دارو برای بیماری وجود داشته باشد، قطعاً قبل از معاینه و آنالیز وضعیت بیمار، اقدام به تجویز دارو برای وی نخواهد شد. در چنین مواردی نمی‌توان برای برخورد با مسائل پویا از راه حل‌های مشابه و ایستا استفاده کرد. به‌منظور ارائه راهکارهای پویا و متناسب با مسائل متغیر، لازم است در ابتدا نسبت به کالبد شکافی دشمنان، انگیزه‌ها و انواع حملات، شناخت مناسبی ایجاد گردد.

- دشمنان شامل سارقین اطلاعاتی، مجرمان، دزدان رایانه‌ای، شرکت‌های رقیب و... می‌باشند؛
- انگیزه‌های موجود شامل: جمع‌آوری هوشمندانه، دستبرد فکری (عقلانی)، عدم پذیرش سرویس‌ها، احساس غرور و مورد توجه واقع شدن، می‌باشد؛
- انواع حملات شامل: مشاهده غیرفعال ارتباطات، حملات به شبکه‌های فعال، حملات از نزدیک (مجاورت سیستم‌ها)، سوءاستفاده و بهره‌برداری خودیان (محرمان) و حملات مربوط به ارائه‌دهندگان صنعتی یکی از منابع تکنولوژی اطلاعات است؛
- در عصر انفجار اطلاعات، شبکه‌های رایانه‌ای اهداف مناسب و جذابی برای مهاجمان اطلاعاتی هستند (واحدی، 1388: 89).

بنابراین، لازم است تدابیر لازم در خصوص حفاظت سیستم‌ها و شبکه‌ها در مقابل انواع متفاوت حملات اطلاعاتی اندیشیده گردد. به‌منظور آنالیز حملات اطلاعاتی و اتخاذ راهکار مناسب برای برخورد با آنان، لازم است با انواع حملات اطلاعاتی آشنا شده تا از این طریق امکان برخورد مناسب و سیستماتیک با هر یک از آنان فراهم گردد. قطعاً وقتی ما شناخت مناسبی را نسبت به نوع و علل حمله داشته باشیم، قادر به برخورد منطقی با آن، به‌گونه‌ای خواهیم بود که پس از برخورد، زمینه تکرار موارد مشابه، حذف گردد.

انواع حملات اطلاعاتی به شرح زیر می‌باشند:

- غیرفعال؛
- فعال؛
- نزدیک (مجاور)؛
- خودی‌ها (محرمان)؛
- عرضه (توزیع).

ویژگی هر یک از انواع حملات فوق، به شرح زیر می‌باشد:

- غیرفعال (Passive): این نوع حملات شامل: آنالیز ترافیک شبکه، شنود ارتباطات حفاظت نشده، رمزگشایی ترافیک‌های رمزشده ضعیف و به‌دست آوردن اطلاعات معتبری مانند رمز عبور می‌باشد. ره‌گیری غیرفعال عملیات شبکه، می‌تواند به مهاجمان، هشدارها و اطلاعات لازم را در خصوص عملیات قریب‌الوقوعی که قرار است در شبکه اتفاق افتند، بدهد (قرار است از مسیر فوق در آینده محموله‌ای ارزشمند عبور داده شود!). پیامدهای این نوع حملات، آشکارشدن اطلاعات و یا فایل‌های اطلاعاتی برای یک مهاجم، بدون رضایت و آگاهی کاربر خواهد بود.
- فعال (Active): این نوع حملات شامل: تلاش در جهت خنثی نمودن و یا حذف ویژگی‌های امنیتی، معرفی کدهای مخرب، سرقت و یا تغییردادن اطلاعات

می‌باشد. حملات فوق، می‌تواند از طریق ستون فقرات یک شبکه، سوءاستفاده موقت اطلاعاتی، نفوذ الکترونیکی در یک قلمرو بسته و حفاظت شده و یا حمله به یک کاربر تأیید شده در زمان اتصال به یک ناحیه بسته و حفاظت شده، بروز نماید. پیامد حملات فوق، افشای اطلاعات، اشاعه فایل‌های اطلاعاتی، عدم پذیرش سرویس و یا تغییر در داده‌ها، خواهد بود.

- مجاور (Close-in): این نوع حملات توسط افرادی که در مجاورت (نزدیکی) سیستم‌ها قرار دارند با استفاده از تسهیلات موجود، با یک ترفندی خاص به‌منظور نیل به اهدافی نظیر: اصلاح، جمع‌آوری و انکار دستیابی به اطلاعات باشد، صورت می‌پذیرد. حملات مبتنی بر مجاورت فیزیکی، از طریق ورود مخفیانه، دستیابی باز و یا هردو انجام می‌شود.
- خودی (Insider): حملات خودی‌ها، می‌تواند به‌صورت مخرب و یا غیرمخرب جلوه نماید. حملات مخرب از این نوع شامل استراق‌سمع تعمدی، سرقت و یا آسیب‌رسانی به اطلاعات، استفاده از اطلاعات به طرزی کاملاً شیادانه و فریب‌آمیز و یا رد دستیابی سایر کاربران تأیید شده باشد. حملات غیرمخرب از این نوع، عموماً به دلیل سهل‌انگاری (حواس‌پرتی)، فقدان دانش لازم و یا سرپیچی عمدی از سیاست‌های امنیتی صورت پذیرد.
- توزیع (Distribution): این نوع حملات شامل کدهای مخربی است که در زمان تغییر سخت‌افزار و یا نرم‌افزار در محل مربوطه (کارخانه، شرکت) و یا در زمان توزیع آنها (سخت‌افزار، نرم‌افزار) جلوه می‌نماید. این نوع حملات می‌تواند، کدهای مخربی را در بطن یک محصول جاسازی نماید. نظیر یک درب از عقب که امکان دستیابی غیرمجاز به اطلاعات و یا عملیات سیستم در زمان آتی را به‌منظور سوءاستفاده اطلاعاتی، فراهم می‌نماید.

توفیق در ایمن‌سازی اطلاعات منوط به حفاظت از اطلاعات و سیستم‌های اطلاعاتی در مقابل حملات است. بدین‌منظور باید از سرویس‌های امنیتی متعددی استفاده گردد.

سرویس‌های انتخابی، می‌بایست پتانسیل لازم در خصوص ایجاد یک سیستم حفاظتی مناسب، تشخیص به‌موقع حملات و واکنش سریع را داشته باشند. بنابراین، می‌توان محور استراتژی انتخابی را بر سه مؤلفه حفاظت، تشخیص و واکنش استوار نمود. حفاظت مطمئن، تشخیص به‌موقع و واکنش مناسب از جمله مواردی است که می‌بایست همواره در ایجاد یک سیستم امنیتی رعایت گردد (واحدی، 1389: 36). سازمان‌ها و مؤسسات، علاوه بر یکپارچگی بین مکانیزم‌های حفاظتی، می‌بایست همواره انتظار حملات اطلاعاتی را داشته و لازم است خود را به ابزارهای تشخیص و روتین‌های واکنش سریع، مجهز نمایند تا زمینه برخورد مناسب با مهاجمان و بازیافت اطلاعات در زمان مناسب فراهم گردد. یکی از اصول مهم استراتژیِ «دفاع در عمق»، برقراری توازن بین سه عنصر اساسی «انسان، تکنولوژی و عملیات» است. حرکت به سمت تکنولوژی اطلاعات، بدون افراد آموزش دیده و روتین‌های عملیاتی که راهنمای آنان در نحوه استفاده و ایمن‌سازی اطلاعات باشد، محقق نخواهد شد.

موفقیت در ایمن‌سازی اطلاعات با پذیرش مسئولیت و حمایت مدیریت عالی یک سازمان (معمولاً در سطح مدیریت ارشد اطلاعات) و بر اساس شناخت مناسب از تهاجمات، حاصل می‌گردد. نیل به موفقیت با پیگیری سیاست‌ها و روتین‌های مربوطه، تعیین وظایف و مسئولیت‌ها، آموزش منابع انسانی حساس (کاربران، مدیران سیستم) و توجیه مسئولیت‌های شخصی کارکنان، حاصل می‌گردد. در این راستا لازم است یک سیستم امنیتی فیزیکی و شخصی به‌منظور کنترل و هماهنگی در دستیابی به هر یک از عناصر حیاتی در محیط‌های مبتنی بر تکنولوژی اطلاعات، نیز ایجاد گردد. ایمن‌سازی اطلاعات از جمله مواردی است که می‌بایست موفقیت خود را در عمل و نه در حرف، نشان دهد. بنابراین، لازم است که پس از تدوین سیاست‌ها و دستورالعمل‌های مربوطه، پیگیری مستمر و هدفمند جهت اجرای سیاست‌ها و دستورالعمل‌ها، دنبال گردد. بهترین استراتژی تدوین شده در صورتی که امکان تحقق عملی آن فراهم نگردد (سهواً و یا عمداً)، هرگز امتیاز مثبتی را در کارنامه خود ثبت نخواهد کرد.

با توجه به جایگاه خاص منابع انسانی در ایجاد یک محیط ایمن مبتنی بر تکنولوژی اطلاعات، لازم است به موارد زیر توجه گردد:

- تدوین سیاست‌ها و رویه‌ها؛
- ارائه آموزش‌های لازم جهت افزایش دانش؛
- مدیریت سیستم امنیتی؛
- امنیت فیزیکی؛
- امنیت شخصی؛
- اتخاذ تدابیر لازم در خصوص پیشگیری.

امروزه از تکنولوژی‌های متعددی به‌منظور ارائه سرویس‌های لازم در رابطه با ایمن‌سازی اطلاعات و تشخیص مزاحمین اطلاعاتی، استفاده می‌گردد. سازمان‌ها و مؤسسات می‌بایست سیاست‌ها و فرآیندهای لازم به‌منظور استفاده از یک تکنولوژی را مشخص تا زمینه انتخاب و به‌کارگیری درست تکنولوژی در سازمان مربوطه فراهم گردد. در این رابطه می‌بایست به مواردی مانند سیاست امنیتی، اصول ایمن‌سازی اطلاعات، استانداردها و معماری ایمن‌سازی اطلاعات، استفاده از محصولات مربوط به ارائه دهندگان شناخته شده و خوش‌نام، راهنمای پیکربندی، پردازش‌های لازم برای ارزیابی ریسک سیستم‌های مجتمع و به‌هم مرتبط، توجه گردد (جنگ سایبری، 1387: 27). در این رابطه موارد زیر، پیشنهاد می‌گردد:

- دفاع در چندین محل:

مهاجمان اطلاعاتی (داخلی و یا خارجی) ممکن است یک هدف را از چندین نقطه مورد تهاجم قرار دهند. در این راستا لازم است سازمان‌ها و مؤسسات از روش‌های حفاظتی متفاوت در چندین محل (سطح) استفاده، تا زمینه عکس‌العمل لازم در مقابل انواع متفاوت حملات، فراهم گردد. لذا می‌بایست به موارد زیر توجه گردد:

- دفاع از شبکه‌ها و زیرساخت: لازم است شبکه‌های محلی و یا سراسری حفاظت گردند (حفاظت در مقابل حملات اطلاعاتی از نوع عدم پذیرش خدمات) ؛
- حفاظت یکپارچه و محرمانه برای ارسال اطلاعات در شبکه (استفاده از رمزنگاری و کنترل ترافیک به‌منظور واکنش در مقابل مشاهده غیرفعال) ؛
- دفاع در محدوده‌های مرزی (به‌کارگیری فایروال‌ها و سیستم‌های تشخیص مزاحمین به‌منظور واکنش در مقابل حملات اطلاعاتی از نوع فعال) ؛
- دفاع در محیط‌های محاسباتی (کنترل‌های لازم به‌منظور دستیابی به میزبان‌ها و سرویس‌دهنده، به‌منظور واکنش لازم در مقابل حملات از نوع خودی، توزیع و مجاور).

- دفاع لایه‌ای:

بهترین محصولات مربوط به ایمن‌سازی اطلاعات، دارای نقاط ضعف ذاتی مربوط به خود می‌باشند. بنابراین، همواره زمان لازم در اختیار مهاجمان اطلاعاتی برای نفوذ در سیستم‌های اطلاعاتی وجود خواهد داشت. بدین ترتیب، لازم است قبل از سوءاستفاده اطلاعاتی متجاوزان، اقدامات مناسبی صورت پذیرد. یکی از روش‌های مؤثر پیشگیری در این خصوص، استفاده از دفاع لایه‌ای در مکان‌های بین مهاجمان و اهداف مورد نظر آنان، می‌باشد. هر یک از مکانیزم‌های انتخابی، می‌بایست قادر به ایجاد موانع لازم در ارتباط با مهاجمان اطلاعاتی (حفاظت) و تشخیص به‌موقع حملات باشد. بدین ترتیب، امکان تشخیص مهاجمان اطلاعاتی افزایش و از طرف دیگر شانس آنها به‌منظور نفوذ در سیستم و کسب موفقیت، کاهش خواهد یافت. استفاده از فایروال‌های تودرتو (هر فایروال در کنار خود از یک سیستم تشخیص مزاحمین، نیز استفاده می‌نماید) در محدوده‌های داخلی و خارجی شبکه، نمونه‌ای از رویکرد دفاع لایه‌ای است. فایروال‌های داخلی ممکن است امکانات بیشتری را در رابطه با فیلترسازی داده‌ها و کنترل دستیابی به منابع موجود ارائه نمایند.

- تعیین میزان اقتدار امنیتی هر یک از عناصر موجود در ایمن‌سازی اطلاعات (چه چیزی حفاظت شده و نحوه برخورد با تهاجم اطلاعاتی در محلی که از عنصر مربوطه استفاده شده، به چه صورت است؟):

پس از سنجش میزان اقتدار امنیتی هر یک از عناصر مربوطه، می‌توان از آنان در جایگاهی که دارای حداکثر کارایی باشند، استفاده کرد. مثلاً می‌بایست از مکانیزم‌های امنیتی مقتدر در محدوده‌های مرزی شبکه استفاده گردد.

- استفاده از مدیریت کلید مقتدر و زیرساخت کلید عمومی، که قادر به حمایت از تمام تکنولوژی‌های مرتبط با ایمن‌سازی اطلاعات بوده و دارای مقاومت مطلوب در مقابل یک تهاجم اطلاعاتی باشد.
- به‌کارگیری زیرساخت لازم به‌منظور تشخیص مزاحمین، آنالیز و یکپارچگی نتایج به‌منظور انجام واکنش‌های مناسب در رابطه با نوع تهاجم:

زیرساخت مربوطه می‌بایست به کارکنان عملیاتی، راهنمایی لازم در مواجهه با سؤال‌هایی نظیر: آیا من تحت تهاجم اطلاعاتی قرار گرفته‌ام؟ منبع تهاجم چه کسی می‌باشد؟ به چه فرد دیگری تهاجم شده است؟ راه حل‌ها و راهکارهای من در این رابطه چیست؟، را ارائه نماید.

- عملیات:

منظور از عملیات، مجموعه فعالیت‌های لازم به‌منظور نگهداری وضعیت امنیتی یک سازمان است. در این رابطه لازم است، به موارد زیر توجه گردد:

- پشتیبانی ملموس و به‌هنگام‌سازی سیاست‌های امنیتی؛
- اعمال تغییرات لازم با توجه به روند تحولات مرتبط با تکنولوژی اطلاعات: در این رابطه می‌بایست داده‌های موردنظر جمع‌آوری تا زمینه تصمیم‌سازی مناسب برای مدیریت فراهم گردد (تأمین اطلاعات ضروری برای مدیریت ریسک)؛

- مدیریت وضعیت امنیتی با توجه به تکنولوژی‌های استفاده شده در رابطه ایمن‌سازی اطلاعات (نصب Patch امنیتی، به‌هنگام‌سازی ویروس‌ها، پشتیبانی لیست‌های کنترل دستیابی)؛
- ارائه سرویس‌های مدیریتی اساسی و حفاظت از زیرساخت‌های مهم (خصوصاً زیرساخت‌هایی که برای یک سازمان ختم به درآمد می‌گردد)؛
- ارزیابی سیستم امنیتی؛
- هماهنگی و واکنش در مقابل حملات جاری؛
- تشخیص حملات و ارائه هشدار و پاسخ مناسب به‌منظور ایزوله نمودن حملات و پیشگیری از موارد مشابه؛
- بازیافت و برگرداندن امور به حالت اولیه (بازسازی).

نتیجه‌گیری:

کشورهای در حال توسعه باید تأمین امنیت را به‌عنوان اولویت اصلی خود در نظر بگیرند؛ چرا که خطر فعالیت‌های تبهکارانه بیشتر متوجه مکان‌هایی است که از کنترل کافی برخوردار نبوده و ناامن هستند.

در عصر حاضر، تجارت الکترونیکی در کشورهایی که امنیت فناوری اطلاعات در آنها کمتر تأمین شده، اهداف جذاب‌تری برای حمله هستند. توجه به اهمیت امنیت، باعث می‌شود اقدامات ضروری و اطمینان‌بخشی برای حفاظت از سیستم‌ها صورت پذیرد و به‌کارگیری مجموعه‌ای مؤثر از سیاست‌های امنیتی، گام مهمی در جهت اطمینان از این مسئله است. در آن صورت، در بیشتر موارد رایانه‌ها و اطلاعات از دسترسی‌های غیرمجاز ایمن خواهد بود و این امکان وجود دارد که اطلاعات با امنیت مناسب در شبکه مبادله گردد.

در مورد نیاز به تأمین امنیت، دیدگاه‌های متفاوتی وجود دارد. گروهی که در مورد داده‌ها نگرانی دارند، به این مسئله به‌عنوان یک موضوع در حوزه امنیت اطلاعات می‌نگرند؛

کسانی که با مکانیزم‌های فنیِ ذخیره و ارسال اطلاعات سر و کار دارند، این مبحث را از دید امنیت سیستم و شبکه می‌بینند؛ حال آنکه دیگرانی که به تجارت مشغول هستند، به آن به‌عنوان یک حوزه جدید در تجارت و عموماً تحت عنوان امنیت الکترونیکی نگاه می‌کنند.

با این اوصاف، تدوین و اجرای تدابیر امنیتی در قبال این تهدیدهای گسترده، ضرورتی اجتناب‌ناپذیر برای افراد، گروه‌ها و سازمان‌ها محسوب می‌شود. بنابراین، تدابیر مناسب می‌توانند احتمال وقوع مخاطرات را به حداقل برسانند و در صورت وقوع آنها، میزان خسارت‌های وارده را در حد بسیار ناچیزی نگه دارند؛ و قابلیت واکنش سریع و مؤثر به‌وجود آورند تا سازمان‌ها برای ترمیم خسارت‌ها، از فرآیندهای از پیش تعیین‌شده استفاده کنند، بهره‌وری و ایمنی اطلاعات افزایش یافته تا بهره‌برداری و استفاده از آن با خیالی آسوده‌تر تداوم یابد.

پیشنهادها:

- پیش‌بینی اقدامات ضروری و اطمینان‌بخشی برای حفاظت از سیستم‌ها، رایانه‌ها و اطلاعات از دسترسی‌های غیرمجاز به گونه‌ای که بهره‌برداری و استفاده از آنها با خیالی آسوده تداوم یابد؛
- تأمین امنیت مکانیزم‌های فنیِ ذخیره و ارسال اطلاعات به‌عنوان یک حوزه جدید تحت عنوان امنیت الکترونیکی سامانه تبادل اطلاعات، به گونه‌ای که اطلاعات با امنیت در شبکه مبادله گردد؛
- تدوین و اجرای تدابیر امنیتی در قبال حملات گسترده، برای افراد، گروه‌ها و سازمان‌ها، به گونه‌ای که احتمال وقوع مخاطرات را به حداقل برساند.

منابع:

- آدامز، جیمز (1380)، «**دفاع مجازی**»، ترجمه حسین سلیمی.
- بوریس‌دی، برکوویتز (1382)، «**بهترین حقایق اطلاعات در عصر اطلاع‌رسانی**»، معاونت پژوهشی دانشکده امام باقر(ع).
- پرایهول، چندرا (1388)، «**امنیت در شبکه‌های کامپیوتری و مخابراتی بی‌سیم**»، ترجمه عباس ریاضی، انستیتو ایزایران.
- خدابنده، حبیب (1386)، «**مدیریت شبکه‌های کامپیوتری**»، پایان‌نامه رشته کامپیوتر دانشگاه آزاد.
- عبدالله‌خانی، علی (1386)، «**تهدیدات امنیت ملی (شناخت و روش)**»، تهران: انتشارات مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر.
- گادسون، روی (1387)، «**اطلاعات امریکا بر سر دو راهی**»، ترجمه معاونت پژوهش دانشکده امام باقر(ع)، تهران: انتشارات دانشکده امام باقر(ع).
- گروه مطالعات امنیت (1388)، «**نظریه امنیت در جمهوری اسلامی ایران**»، تهران: انتشارات دانشگاه عالی دفاع ملی.
- مؤسسه آموزشی و تحقیقاتی صنایع دفاع (1386)، «**فرهنگ تشریحی واژگان امنیت فناوری اطلاعات**».
- مرکز پدافند غیرعامل ایزایران (1387)، «**جنگ سایبری**».
- موسسه مطالعات و پژوهش‌های بازرگانی (1386)، «**بسته آموزشی امنیت تجارت الکترونیکی**»، تابستان.
- واحدی، مرتضی (1388)، «**امنیت، اطلاعات در عصر جهانی شدن**»، دانشگاه عالی دفاع ملی.
- واحدی، مرتضی (1389)، «**کلیات جنگ الکترونیک**»، دانشکده علوم و فنون فارابی.
- وزارت ارتباطات و فناوری اطلاعات (1388)، «**دستورالعمل‌های اجرایی مدیریت امنیت اطلاعات**».
- United Kingdom Cornish Paul, Hughes Rex and Livingstone David, Cyberspace and the National Security of the: Threats and Responses,۲۰۰۹

Chatham House Report www.chathamhouse.org.uk ›... › Reports and Papers

§ National Security Threats in Cyberspace, Rosenzweig Paul, National Strategy Forum , ۱ Aug ۲۰۰۹.

§ www.abanet.org/natsecurity/threats_%۲۰in_cyberspace.pdf.

§ .intellit.muskingum.edu/cia_folder/ciarequirements.html.