مبانی پدافند غیر عامل در حوزه امنیت فناوری اطلاعات

چکیده

تامین امنیت اطلاعات سازمانها در محیط امروزی که از شبکه های به هم پیوسته تشکیل شده، کاری مشکل است و با ورود هر محصول الکترونیکی و هر ابزار نفوذ و جاسوسی این کار صعب سخت تر نیز می شود. همچنین با توجه به رشد روز افزون حملات در شبکه های کامپیوتری، تلاش برای مقاوم سازی آنها در برابر حملات و در نظر گرفتن مسایل مربوط به پدافند غیر عامل امری حیاتی محسوب می شود.

امروزه عوامل بسیاری وجود دارد که امنیت یک شبکه را تهدید می کند ازجمله حملات گسترده هکرها که ازنقاط آسیب پذیر سیتسم ها ما برای رسیدن به اهدافشان استفاده می کنند با هک کردن یک سرور میزبان صدها یا شاید هزاران سایت هک شوند بنابراین نیازمند حفاظت از سرور و شبکه خود و لحاظ کردن مسایل پدافند غیر عامل با امکانات امنیتی هستیم به همین دلیل شرکت ها و سازمان ها به سمت استفاده از مسایل پدافندی در حوزه غیرعامل هستند. دراین مقاله بعد از بیان مفاهیم امنیت فناوری اطلاعات در محیط

های مجازی و بررسی تهدیدات داخلی و خارجی و حفاظت از سیستم ها و نیاز به تامین امنیت پرداخته و مسایل مربوط به امنیت فناوری اطلاعات در عصر دیجیتال و مباحث مربوط به رایانه های شخصی و اینترنت بحث می شود.

واژه‌های کلیدی: پدافند غیر عامل، امنیت فناوری اطلاعات، حفاظت از سیستم ها، تهدیدات سایبری، امنیت اینترنت

۱-مقدمه

مفهوم امنیت در دنیای واقعی مفهومی حیاتی و کاملاً شناخته شده برای بشر بوده و هست. در دوران ماقبل تاریخ، امنیت مفهومی کاملاً فیزیکی را شامل می شد که عبارت بود از اصول حفظ بقاء نظیر امنیت در برابر حملهٔ دیگران یا حیوانات و نیز امنیت تأمین غذا. بتدریج نیازهای دیگری چون امنیت در برابر حوادث طبیعی یا بیماریها و در اختیار داشتن مکانی برای زندگی و استراحت بدون مواجهه با خطر، به نیازهای پیشین بشر افزوده شد. با پیشرفت تمدن و شکل گیری جوامع، محدودهٔ امنیت ابعاد بسیار گسترده تری یافت و با تفکیک حوزهٔ اموال و حقوق شخصی افراد از یکدیگر و از اموال عمومی، و همچنین تعریف قلمروهای ملی و بین المللی، بتدریج مفاهیم وسیعی مانند حریم خصوصی، امنیت اجتماعی، امنیت مالی، امنیت سیاسی، امنیت ملی و امنیت اقتصادی را نیز شامل گردید. این مفاهیم گرچه دیگر کاملاً محدود به نیازهای فیزیکی بشر نمی شدند، ولی عمدتاً تحقق و دستیابی به آنها مستلزم وجود و یا استفاده از محیط های واقعی و فیزیکی بود.[1]

۲- مفاهیم امنیت فناوی اطلاعات

جهان در دهه های اخیر و بویژه در پنج سال گذشته عرصهٔ تحولات چشمگیری بوده که بسیاری از مناسبات و معادلات پیشین را بطور اساسی دستخوش تغییر نموده است. این تحولات که با محوریت کاربری وسیع از فناوری اطلاعات و ارتباطات امکانپذیر شده، از کاربرد رایانه به عنوان ابزار خودکارسازی (Automation) و افزایش بهره وری آغاز گردیده و اکنون با تکامل کاربری آن در ایجاد فضای هم افزائی مشارکتی (Collaboration)، عملاً زندگی فردی و اجتماعی بشر را دگرگون ساخته است.

به باور بسیاری از صاحبنظران، همانگونه که پیدایش خط و کتابت آنچنان تأثیر شگرفی بر سرنوشت انسان برجای گذاشته که مورخین را برآن داشته تا داستان زندگی بشر بر این کره خاکی را به دوران ما قبل تاریخ و تاریخ تقسیم نمایند، ورود به فضای مجازی حاصل از فن آوری نوین اطلاعات و ارتباطات نیز دورهٔ جدیدی از تمدن بشری را رقم زده، بنحوی که انقلاب عصر اطلاعات شیوهٔ اندیشه، تولید، مصرف، تجارت، مدیریت، ارتباط، جنگ و حتی دینداری و عشق ورزی را دگرگون ساخته است.[1,2]

این تحول بزرگ الزامات و تبعات فراوانی را به همراه داشته که از مهمترین آنها بوجود آمدن مفاهیم نوین امنیت مجازی یا امنیت در فضای سایبر می باشد. با تغییری که در اطلاق عبارت " شبکهٔ رایانه ای " از یک شبکهٔ کوچک کار گروهی به شبکه ای گسترده و جهانی (اینترنت) واقع گردیده، و با توجه به رشد روزافزون تعاملات و تبادلاتی که روی شبکه های رایانه ای صورت می پذیرد، نیاز به نظام های حفاظت و امنیت الکترونیکی جهت ضمانت مبادلات و ایجاد تعهد قانونی برای طرفهای دخیل در مبادله بسیار حیاتی است. نظام هایی مشتمل بر قوانین، روشها، استانداردها و ابزارها یی که حتی از عقود متداول و روشهای سنتی تعهدآورتر بوده و ضمناً امنیت و خصوصی بودن اطلاعات حساس مبادله شده را بیش از پیش تضمین نمایند. آنچه مسلم است چالش امنیتی رودرروی کشور عدم دسترسی به فناوری و یا عدم وجود محصولات امنیتی نیست، بلکه سیاستگذاری، فرهنگ سازی، بهره وری مناسب از منابع موجود ملاحظه مسایل مربوط به پدافند غیر عامل در فضای سایبری و نیز سازگاری آنها به گونه ای است که نیاز منحصربه فرد شبکه و فضای دیجیتالی کشور را تأمین کند.[2]

۲-۱- امنیت اطلاعات در محیط های مجازی

امنیت اطلاعات در محیط های مجازی همواره بعنوان یکی از زیرساختها و الزامات اساسی در کاربری توسعه ای و فراگیر از ICT مورد تاکید قرار گرفته است. گرچه امنیت مطلق چه در محیط واقعی و چه در فضای مجازی دست نیافتنی است، ولی ایجاد سطحی از امنیت که به اندازهٔ کافی و متناسب با نیاز ها و سرمایه گذاری انجام شده باشد تقریباً در تمامی شرایط محیطی امکان پذیر است. تنها با فراهم بودن چنین سطح مطلوبی است که اشخاص حقیقی، سازمانها، شرکتهای خصوصی و ارگانهای دولتی ضمن اعتماد و اطمینان به طرفهای گوناگونی که همگی در یک تبادل الکترونیکی دخیل هستند و هیچگاه یکدیگر را ندیده و نمی شناسند، نقش مورد انتظار خود بعنوان گره ای مؤثر از این شبکه متعامل و هم افزا را ایفا خواهند نمود.

۲-۲- اهمیت امنیت اطلاعات

توجه به این نکته ضروری است که معماری امنیت اطلاعات فرآیندی از فرآیندهای جاری در معماری فناوری اطلاعات در سطوح مختلف اعم از ملی و سازمانی است که در این فرآیند به تناسب و نیاز از ابزارهای لازم استفاده خواهد شد. نکتهٔ مهم دیگر حاصل از تجارب کشورهای پیشرو حاکی است که امنیت اطلاعات مسأله ای فرابخشی است و نیاز به همکاری های گسترده در این زمینه دارد. این همکاری ها هم در سطح ملی و هم در سطح بین المللی باید مورد توجه قرار گیرد. تعیین نقش ها، وظایف و مسئولیت ها و مسایل امنیتی و پدافندی از نکات مهمی است که در این همکاری ها باید تعریف شوند.

امروزه امنیت فضای دیجیتال وجه تازه ای از امنیت ملی هر کشور را به تصویر می کشد. استفادهٔ درست از اطلاعات صحیح، یکی از نیازهای بسیار مهم برای دستیابی سازمانها به اهداف سازمانی است و قابلیت اطمینان، یکپارچگی و در دسترس بودن این

اطلاعات، از مشخصه های بسیار مهم در کارآیی آنها هستند. مزایای ذخیره سازی اطلاعات بصورت الکترونیکی کاربرد وسیع رایانه ها در اهداف تجاری را ناگزیر کرده و استفاده از شبکه های رایانه ای و بویژه اینترنت، تغییرات اساسی را در روند کسب و کار بوجود آورده و باعث شده که حجم بسیار زیادی از اطلاعات تنها به اندازهٔ یک سر انگشت با ما فاصله داشته باشند؛ و ناگفته پیدا است که در این محیط پیچیده با این ارتباطات وسیع، مخاطرات گسترده ای سیستمهای رایانه ای، سیستمهای اطلاعاتی، و فعالیتها و زیرساختهای حیاتی وابسته به آنها را تهدید می کنند. در دنیای امروز، اعتبارات مالی بیشتر و بیشتر بصورت الکترونیکی جابجا می شوند، اطلاعات مختلف با حساسیتهای کم و زیاد از طریق شبکه ها منتقل می شوند، سامانه های رایانه ای با سرعت بسیار زیادی پیچیده تر و مرتبط تر با دنیای بیرونی می گردند، و ابزارهای سادهٔ نفوذ و بهره برداری از آسیب پذیری ها بیش از هر زمان دیگری در دسترس ماجراجویان و جنایتکاران دنیای مجازی قرار دارد؛ و هریک از این عوامل خود به تنهایی دلیل محکمی برای جدی گرفتن موضوع امنیت و پدافند غیر عامل است.

۲-۳- تهدیدات داخلی و خارجی

اکثر قریب به اتفاق سازمانها در معرض انواع تهدیدات داخلی و خارجی خرابکاران هستند؛ تهدیداتی چون دستکاری اطلاعات مرجع و یا سرقت اطلاعات حیاتی و سرمایه های اطلاعاتی. در چنین شرایطی، عواملی که می توانند از مزایای سیستمها به شمار روند (مثل سرعت و قابلیت دسترسی بالا)، اگر تحت کنترل نباشند ممکن است باعث بروز آسیب پذیری شوند و سوء استفادهٔ افراد بدنیت از آنها به نفوذ و خرابکاری، کلاهبرداری، و یا اخاذی بیانجامد. علاوه بر این، مشکلات طبیعی و خطاهای غیرعمدی که توسط کاربران رایانه ای رخ میدهد، درصورت فقدان روالهای صحیح برای حفاظت

از اطلاعات می تواند نتایج مخربی به بار آورد. در کنار همهٔ این مسائل، موضوع جرائم سازمان یافتهٔ دنیای مجازی بر پیچیدگی کار دولتها برای تأمین امنیت زیرساختهای حیاتی خدمات عمومی می افزاید، و اهمیت سوء استفاده از منابع دولتی، اهمیت پرداختن صحیح و مؤثر آنها به موضوع امنیت را دو چندان میکند.[2,3]

به این ترتیب تدوین و اجرای تدابیر امنیتی در قبال این تهدیدات گسترده، ضرورتی اجتناب ناپذیر برای سازمانها محسوب می شود. تدابیر مناسب می توانند احتمال وقوع مخاطرات را به حداقل برسانند، درصورت وقوع آنها میزان خسارتهای وارده را در حد بسیار ناچیزی نگه دارند، و قابلیت واکنش سریع و مؤثر بوجود آورند تا سازمانها برای ترمیم خسارتها از فرآیندهای از پیش تعیین شده استفاده کنند تا بهره وری و ایمنی اطلاعات افزایش یابد و کسب و کار با خیالی آسوده تر تداوم یابد.

۳- پیشرفت فناوری اطلاعات و ارتباطات

امروزه ما در دنیایی زندگی می کنیم که پردازش اطلاعات در آن ارزان و هزینه های ارتباط تلفنی رو به کاهش است و جهان بطور فزاینده ای در تبادل و تعامل می باشد. اما فراهم شدن امکانات فنی جدید تنها باعث پیدایش محصولات نوین و راه های بهتر و کارآمدتر برای انجام امور نشده، بلکه در کنار آن امکان سوء استفاده از فناوری را نیز افزایش داده است.

فناوری اطلاعات و ارتباطات نیز همانند سایر فناوریها حالت ابزاری دارد و می توان آنرا بگونه ای مورد استفاده قرار داد که برای همگان مفید باشد و یا به نحوی از آن استفاده کرد که نتایج خطرناکی به بار آورد.

عامل سرعت در فناوری اطلاعات و ارتباطات چیزی در حدود میکروثانیه است که باعث می شود اطلاعات غیرقابل مشاهده با چشم غیرمسلح، تحت کنترل نرم افزار تهیه شده توسط افراد جابجا گردد. در چنین فضایی اعمال غیرقانونی و مخرب آنقدر سریع صورت می گیرد که می تواند غیرقا بل شناسایی باشد هرچند شناسایی آن غیر ممکن نیست. مشکلات مربوط به امنیت سیستمهای اطلاعاتی، فرآیندهای وابسته به آنها و ذخیره و ارسال اطلاعات به شکل الکترونیکی مسائل تازه ای نیستند. سیستمهای تجاریِ رایانه ای نزدیک به پنجاه سال قدمت دارند. سیستمهای بانکداری نیز انتقال الکترونیکی پول را تقریباً در همان زمان آغاز کرده اند. در این سیستمهای تجاری، برای ارتکاب جرم از طریق نفوذ به شبکه های رایانه ای و سیستمهای مالی انگیزه های قوی وجود دارد. در واکنش به افزایش احتمال انجام فعالیت های تبهکارانه و برای تهیهٔ معیارهای امنیتی قوی تر در عرصهٔ ارتباطات و پردازش، طرحهای تحقیقات و توسعه ای اطلاعات آغاز شده است.[4]

۳-۱- حفاظت از سیستم ها

توجه به اهمیت امنیت باعث می شود اقدامات ضروری و اطمینان بخشی برای حفاظت از سیستمها صورت پذیرد و استفاده از مجموعه ای مؤثر از سیاستهای امنیتی، گام مهمی در جهت اطمینان از این مسئله است. در آنصورت در بیشتر موارد رایانه ها و اطلاعات شما از دسترسی های غیرمجاز ایمن خواهند بود و خواهید توانست اطلاعات خود را بصورت امن در شبکه با سایرین مبادله کنید. زمانی که یک رایانه یا شبکه دچار اشکال می شود، مجموعه ای غنی از کانالهای اطلاعاتی وجود دارد که اخبار و اطلاعات امنیتی از طریق آنها ارسال می گردد. سازمانهایی که از رایانه ها و شبکه ها استفاده می

کنند دارای مراکز کمک رسانی (Help Centers) هستند که توسط متخصصین فنی اداره می شوند و قادر به جلوگیری از کاربرد سوء منابع سازمانی و تأمین حفاظت آنها می باشند.

کاربران و راهبران فنی در کشورهای درحال توسعه معمولاً فاقد توانایی ارائه این سطح از پشتیبانی هستند. تعداد کاربران اندک است و به هشدارها و راه حلهای ارائه شده نیز توجه نمی شود. سازمانهایی که از رایانه استفاده می کنند غالبا دارای بخش ستادی کوچکی هستند و لذا 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 دربارهٔ سیستمهای رایانه ای و امنیت شبکه و پدافند غیر عامل است، و گروه هایی که اصول اساسی را درک کرده اند نیز معمولاً در فهم چگونگی سازگارسازی راهکارهای فنی با شرایط متغیر و غیرقابل پیش بینی این محیط مشکل دارند.[4]

نقص امنیتی شبکه در همهٔ کشورها اتفاق می افتد و حتی ممکن است موجب تحت فشار قرار گرفتن دولتها نیز بگردد. معمولاً بسیاری از این نقصها گزارش نمی شوند؛ چراکه اطلاع عموم مردم از آنها می تواند نتایج نامطلوبی به بار آورد. دولتها و سازمانهای موجود در کشورهای توسعه یافته عموماً توانایی مقابله با چنین نقصهایی را دارند، ولی نتایج ناشی از بروز نقصها و اشکالات امنیتی در کشورهای درحال توسعه می تواند بسیار وخیم تر از کشورهای توسعه یافته باشد. در کنار همهٔ این موارد، بازارها، سازمانها و دولتهای کشورهای درحال توسعه به دلیل عدم توجه به عواقب ناشی از نفوذهای رایانه ای در حجم وسیع، عدم توانایی تحلیل ضررهای مالی ناشی از این حملات، و نیز نداشتن تخمین مناسب از زمان لازم برای ترمیم خسارات وارده (البته اگر این خسارات قابل ترمیم باشند) تمایل چندانی به رفع نقایص امنیتی ندارند.

کشورهای درحال توسعه باید تأمین امنیت را بعنوان اولویت اصلی خود در نظر بگیرند، چراکه خطر فعالیتهای تبهکارانه بیشتر متوجه مکانهایی است که از کنترل کافی برخوردار نبوده و ناامن هستند. تجارت الکترونیکی در کشورهایی که امنیت فناوری اطلاعات در آنها کمتر تأمین شده اهداف جذابتری برای حمله هستند. کدام سازمان کوچک یا متوسط است که علیرغم به سرقت رفتن اطلاعات محرمانهٔ مشتریان، فایلهای تجاری و یا دستکاری شدن اطلاعات کلیدی سازمان همچنان بتواند پابرجا بماند؟ کشورهای درحال توسعه باید ظرفیت منابع انسانی آموزش دیده و زیرساختهای فناوری خود را بهبود بخشند تا اهداف آسانی برای حملهٔ تبهکاران فضای رایانه ای نباشند.

۳-۲- نیاز به تأمین امنیت

در مورد نیاز به تأمین امنیت، دیدگاه های متفاوتی وجود دارد. افرادی که در مورد داده ها نگرانی دارند به این مسئله بعنوان یک موضوع در حوزهٔ امنیت اطلاعات می نگرند؛ کسانیکه با مکانیزمهای فنیِ ذخیره و ارسال اطلاعات سر و کار دارند این مبحث را از دید امنیت سیستم و شبکه می بینند؛ حال آنکه دیگرانی که به تجارت مشغول هستند به آن بعنوان یک حوزهٔ جدید در تجارت و عموماً تحت عنوان امنیت الکترونیکی نگاه میکنند.این مسئله حائز اهمیت است که هم اطلاعات و هم مکانیزمهای پردازش آن باید از سوء استفاده مصون باشند.بطور کلی مقولهٔ امنیت و پدافند غیر عامل در حوزه فناوری اطلاعات به موضوعات زیر اشاره دارد:

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

امنیت سایبر(Cyber-Security): امنیت فناوری اطلاعات وابسته به سیاست دولتها. این اصطلاح عموماً 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؛ امنیت رایانه ها، شبکه ها و داده ها تا حد زیادی با مفاهیم روزمرهٔ امنیت در فضای سایبر به هم گره خورده اند.[1,4]

٤- تأمین امنیت فناوری اطلاعات

از آنجا که توسعهٔ 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 استفاده 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 یابها ، رمزگذاری و نگهداری قاعده مند از اطلاعات را به دلیل هزینه و وقتی که از آنها می گیرد و تغییری که در رفتار رایانهای آنها ایجاد می کند به تعویق بیاندازند. علاوه بر این سازمانهای کوچک و متوسط ممکن است از یک راه حل فنی نظیر دیوارهٔ آتش 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 سیستمهای خود را به تأخیر بیاندازند و در تدوین سیاستهای شفاف امنیتی و پدافندی 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.

٤-١- فناوری دریک محیط متغیر

دستگاه های سیار، نرم افزارهای 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 خصوصاً دستگاه های سیار (مانند رایانه های کیفی، تلفنهای همراه و PDA ها) که 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 پیچیدگیهایی در محیطهای شبکه ای شده اند.[2,4]

از هنگام ظهور دستگاه های خودپرداز گرفته تا زمان رواج بانکداری اینترنتی، 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، کرم ها و تراوا هایی که می تواند آسیبهای شدیدتری را به این سیستمها و داده ها وارد کند. این صدمات حتی می توانند از بعضی نرم افزارهای مخرب (بدافزارها) 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.

٤-٢- همکاری بین المللی و امنیت در کشورهای 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 که حدود ده سال قبل حتی تصور آنها مشکل بود. البته دسترسی به اینترنت همیشه هم ارزان نیست. 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 برخط بفروشند. اگرچه هنوز تعداد رقبا در بازار بسیار زیاد است، اما مشتریان می توانند بسادگی تواناییها و محصولات شرکتهای رقیب را ببینند و برای انجام اینکار نیازی به اطلاعات وسیع در این زمینه ندارند. از آنجا که دسترسی به بازارهای آنسوی 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.[3,4]

٥- امنیت فناوری اطلاعات در عصر دیجیتال

ظهور فناوری دیجیتال یکی از بارزترین پیشرفتهای فناوری در نیمقرن اخیر به شمار می آید که در زندگی کنونی بشر بصورت عاملی حیاتی درآمده است. برای بسیاری از ما این نوع فناوری در قالب رایانه های دیجیتالی تجلی کرده و به ابزاری لازم برای انجام کارها و رفع نیازهای شخصی تبدیل شده است. در سال۱۹۵۱ میلادی زمانیکه اولین رایانهٔ دیجیتال تجاری به سازمان آمار و سرشماری ایالات متحده آمریکا تحویل داده شد، بسیاری از مردم در مورد رایانه ها چیزی نمی دانستند و آن رایانه ها

نیز تنها در تعداد انگشت شماری از دانشگاه ها و آزمایشگاه های تحقیقاتی مورد استفاده قرار داشتند. این رایانه ها بزرگ، گران و مملو از اشکال بودند. در مقابل، رایانه های امروزی اندازه ای نسبتا کوچک دارند، ارزان و قابل اطمینان هستند و می توان آنها را در هر کشوری یافت. به فاصلهٔ کوتاهی پس از رواج رایانه ها در دانشگاه ها، پروژه های تحقیقاتی برای مرتبط ساختن آنها با یکدیگر به نحوی که امکان مبادلهٔ اطلاعات میان آنها بوجود آید آغاز شدند. از میان این پروژه ها، پروژهٔ توسعهٔ شبکهٔ ARPANET موفقیت بیشتری کسب کرد و به آن چیزی تبدیل شد که امروز آنرا بعنوان " اینترنت " می شناسیم و درحال حاضر بیش از۳۰۰ میلیون رایانه را در سراسر جهان به هم مرتبط کرده است. طی ده سال اخیر اینترنت به یک ابزار مهم ارتباطی میان تمامی اقشار جامعه تبدیل شده و ما برای دسترسی آنی به اطلاعات، ارتباطات اختصاصی، تمامی انواع برنامه های کاربردی، تجاری، روابط کاری و نقل و انتقالات مالی به آن وابسته ایم. قابلیت اطمینان و دسترسی آسان به اینترنت برای موفقیت پایدار و مداوم کشورهای توسعه یافته یک عامل حیاتی بشمار می رود و اهمیت آن برای کشور های درحال توسعه نیز بسرعت رو به افزایش است. آثار استفاده از رایانه ها و نتایج حاصله از انقلاب اینترنت از مرز فواید مستقیم آنها فراتر رفته و پیش بینی می شود که تأثیرات بیشتری نیز در راه باشند.[5]

اول از همه اینکه اینترنت مرزهای جغرافیایی میان کاربران متصل به خود را کمرنگ کرده و روند جهانی سازی را با ارائه قابلیتهای رسانه های ارتباطی تسهیل نموده و لذا هر کسی مستقل از محل فیزیکی خود قادر به برقراری ارتباط با آن میباشد. موتورهای جستجو بر روند این تغییر تأثیری مضاعف داشته اند؛ چراکه نتایج جستجو بر اساس موضوعات ظاهر می شوند و نه بر اساس فاصله ای که کاربر با آ نها دارد؛ بطوریکه

پایگاه وبِ کارخانجات و شرکتهای واقع در کشورهای توسعه یافته و درحال توسعه از موقعیت یکسانی برای نظارهشدن توسط مراجعین برخوردار هستند.

دومین مسئله این است که اینترنت تأثیری شگرف در فرآیند حذف واسطه های تجاری داشته است. بعنوان مثال می توان به کاهش چشمگیر نرخ استخدام منشی در کشورهای توسعه یافته اشاره کرد که دلیل آن این است که نوشتن متن و چاپ و ارسال پیام شخصی برای افراد از طریق تسهیلاتی چون پردازشگر کلمات و پست الکترونیکی آسانتر از دیکته کردن متن برای یک منشی است. به همین ترتیب گردشگری دسته جمعی نیز درحال حاضر رو به انقراض است، چراکه گردشگران می توانند بلیطهای هوایی یا قطار و همچنین اتاقهای هتل مورد نظر خود را بصورت برخط رزرو کنند و این امر موجب صرفه جویی در هزینه و وقت مشتری شده و باعث شده بتوان با کمی دقت روی سفارشات، از یک سفر مفرح لذت بر د. پیدایش شرکتهای فروشندهٔ کتاب، موسیقی و محصولات الکترونیکی بصورت برخط موجب تهدید و ضربه به فروشگاه های عرضه کنندهٔ اینگونه محصولات شده، اما در عین حال در بسیاری از بخشهای این صنف به گسترده تر شدن طیف بازار هدف نیز انجامیده است.

سومین پیامد این است که نرخ بهره وری حداقل در صنایع وابسته به فناوری اطلاعات با شتابی چشمگیر افزایش خواهد یافت. به کمک پست الکترونیکی امکان ارسال و تبادل اطلاعات در سراسر جهان طی تنها چند ثانیه ممکن شده، بطوریکه مباحث و مذاکرات جهانی را می توان بسیار سریعتر از گذشته پیگیری کرد و به نتیجه رساند. امور بازرگانی که تا چندی قبل از طریق پست، تلکس و تلفن انجام می شدند اکنون با بکارگیری مفاهیمی نوین در صنعت مخابرات سیار، سریعتر و کارآمدتر به انجا م می رسند و این مسئله چرخهٔ زمانی انجام فعالیتها را کاهش داده است.

نکتهٔ آخر اینکه ایمن نگاه داشتن محل ذخیرهٔ اطلاعات و خطوط ارتباطی مخابراتی نیز در این محیط جدید الزامی است. صنعت و فناوری امروز به شدت در تکاپوی یافتن راهی برای تضمین امنیت زیرساختهای خود هستند، چراکه دست اندرکاران آن دریافته اند که بیشتر نقایص امنیتی اینترنت ناشی از وجود سخت افزارها و نرم افزارهای ناامن در آن می باشند. در این محیط ایجاد اطمینان و اعتماد به رایانه، شبکه و داده های ذخیره شده نسبت به محیطی که در آن روابط کاری بر اساس گفتگوهای رو در رو انجام می گیرد کمابیش از اهمیت یکسانی برخوردار است. این مطلب در مورد کشورهای درحال توسعه نیز واضح است:سازمانهایی که به سطح امنیتی مناسبی در زیر ساختهای دیجیتالی خود دست نیافته و از ارسال اطلاعات خویش به نحو مطلوبی محافظت نمی کنند شایستهٔ اعتماد نخوا هند بود و از کاروان اقتصاد نوین جهانی عقب خواهند ماند. [4,5]

۵-۱- انقلاب دیجیتال

امروزه فناوری دیجیتال از حیطهٔ رایانه ها فراتر رفته است. پیشرفتهای فناوری در صنعت میکروالکترونیک امکان ساخت ابزارهای پیچیدهٔ الکترونیکی در مقیاسهای بسیار کوچک را فراهم آورده بطوریکه اکنون شما می توانید تجهیزات ارتباطی و محاسباتی بسیار پیچیده را در جیب خود جای دهید. علاوه بر این بهبود نسبت قیمت به کارآیی برای این نوع فناوری در هر سال چیزی حدود۳۰ ٪ است و احتمال برقراری این نسبت تا ده سال آینده نیز بسیار بالاست. انتظار ما این است که این فنا وری مورد استقبال گسترده قرار گیرد و عرصه های نوینی در تجارت پدید آورد و نقطهٔ شروعی برای آغاز عصر طلایی فناوری دیجیتالی باشد.

۵-۱-۱- تجهیزات تلفنی

تجهیزات تلفنی مدرن امروز کاملاً دیجیتالی هستند و سیستمهای هدفمند رایانه ای جایگزین تجهیزات Switching مبتنی بر رلهٔ مکانیکی شده اند. از زمان پیدایش دیسک فشرده در اواخر دههٔ ۸۰ میلادی، صدا و موسیقی شکل دیجیتالی به خود گرفته و با پیدایش قالب موسیقی MP3 در اواخر دههٔ ۹۰ میلادی ضبط صدا حتی در محیطهای خانگی نیز کاملاً دیجیتالی شده است. در دنیای عکاسی و فیلمبرداری نیز تصاویر دیجیتالی و دوربینهای دیجیتالی ثبت تصاویر فیلمهای عکاسی گشته اند.

استانداردهای تلفنهای بی سیم درحال حرکت به سمت فناوری دیجیتال هستند و با وجود پروتکلهایی چون GSM، TDMA وCDMA گونه های مختلف آنها بتدریج جایگزین نسل قدیمی استانداردهای فناوری آنالوگ خواهند شد. در کشورهای توسعه یافته تلویزیون دیجیتال به صحنه آمده است و دیری نخواهد گذشت که جای استانداردهای پخش برنامه را خواهد گرفت (هرچند که این تغییر کمی کندتر از بقیه خواهد بود؛ چرا که حجم گیرنده های خانگی موجود که به استانداردهای قدیمی تر وابسته اند بسیار وسیع است). سیستمهای امنیت فیزیکی نیز درحال تبدیل به انواع الکترونیکی خود هستند. در هتلها، آپارتمانها و دفاتر اداری، کلیدهای فیزیکی جای خود را به کارتهای الکترونیکی داده اند. دوربینهای تلویزیونی مورد استفاده در سیستمهای نظارتی ساختمانها و تأسیسات نیز اغلب از تجهیزات الکترونیکی استفاده می کنند که بجای ارسال سیگنالهای تلویزیونی به یک مانیتور ویدئویی، تصاویر الکترونیکی را به ایستگاه های نظارت دیجیتالی ارسال می کنند. بسیاری از خدماتی که امروزه از آنها استفاده می کنیم بدون وجود رایانه، شبکه و فناوری دیجیتال قابل ارائه نخواهند بود.[4]

۵-۱-۲- خطوط هوایی

خطوط هوایی نیز بدون سیستمهای رزرو رایانه ای و سیستمهای نگهداری و پشتیبانی پرواز قادر به رقابت با هم نیستند. هواپیماها تا اندازهٔ زیادی به حسگرهای الکترونیکی و کنترلهای دیجیتالی وابسته اند و بدون آنها نمی توانند به خوبی کار کنند. حتی اتومبیلها نیز برای عملکرد مناسب و کمک به عیب یابی و نگهداری خود از ریزپردازنده ها استفاده می کنند.سیستمهای مکانیابی جهانی (GPS) نیز به شما این امکان را می دهند که بدانید در هر لحظه در چه مکانی روی کرهٔ زمین قرار گرفته اید و با داشتن چنین دستگاه نسبتا ارزانی در کنار رایانه ای که حاوی پایگاه د ادهای از نقشه ها باشد قادر به یافتن مسیر حرکت، نقاط مهم، رستورانها، تابلوهای راهنما، خدمات ارائه شده در طول مسیر، و در نهایت مقصد مورد نظر خواهید بود.

این دستگاه های دیجیتال با سرعتی باورنکردنی در شبکه قرار می گیرند. تلفنهای بی سیم قادر به برقراری ارتباط با اینترنت هستند و ابتدا قادر به ارسال صوت و اکنون قادر به مبادلهٔ تصاویر از طریق اینترنت می باشند و بزودی دارای قابلیت GPS نیز خواهند شد و به این ترتیب افرادی که در معرض خطر و حادثه قرار گرفته باشند را می توان با دقتی زیاد و تنها با یک تلفن مکانیابی کرد. بسیاری از خدماتی که اکنون مورد استفادهٔ ما قرار می گیرند – مثل دستگاه های خودپرداز که برای تبادل و نقل و انتقال پول بکار می روند بر اساس اصل " در دسترس بودن شبکه " کار می کنند. نقل و انتقالات مالی و اعتباری میان بانکی و بین المللی وابستگی زیادی به شبکه های اعتباری و مالی دارند. امروزه نقل و انتقالات بانکهای الکترونیکی از طریق اینترنت برای افراد میسر است.[5,6]

۵-۲- فناوریهای نوظهور

مسئله اصلی برای دولتها این است که منافع حاصل از فناوریهای نوظهور را تشخیص دهند و در عین حال ارزشها و آزادیهایی که بدون آن فناوریها می توان از آنها برخوردار بود را همچنان حفظ کنند. موضوع این است که دولتها باید فناوریهای جدید را درک کرده و تأثیر قابلیتها و امکانات نوین بر آزادیها را ارزیابی نمایند. همچنین دولتها باید گامهای مؤثری بردارند تا مطمئن شوند اگر قوانین و سیاستهای عمومی در این زمینه آزادیهای فعلی را تقویت نمی کنند، حداقل یک وفاق جمعی در مورد آنها وجود داشته باشد.

دنیای دیجیتالی معمولاً با عنوان فضای سایبر(Cyberspace) شناخته می شود و تعریف آن تمامی رایانه ها و ابزار های دیجیتالی که با شبکه های داخلی و خارجی به هم متصل می شوند و می توانند با یکدیگر ارتباط داشته باشند را در بر می گیرد. در فضای سایبر هم مثل فضای فیزیکی می توان دربارهٔ ملاقاتها و انجام کارها صحبت کرد، اما باید میان رفتار در فضای سایبر و دنیای حقیقی که در آن زندگی، کار و بازی می کنیم تفاوت قائل شد.[6]

٦- رایانه های شخصی و اینترنت

گسترش و رواج سریع رایانه های شخصی و اینترنت در بخشهای مختلف کشورهای درحال توسعه منافع بسیاری داشته است. با اینحال اینترنت بخودی خود رسانه ای نیست که نسبت به رفتار تبهکارانه ایمنی داشته باشد. هزینهٔ عدم توجه کافی به امنیت می تواند از دست دادن داده های مورد نیاز برای انجام کار یک سازمان بزرگ یا مؤسسهٔ دولتی باشد. اینترنت ماهیتا از ایمنی لازم برخوردار نیست اما هزینهٔ امن کردن

آن نیز در مقایسه با هزینهٔ از دست رفتن داده های ارزشمند سازمانها و مؤسسات چندان قابل توجه نمی باشد. از دیگر مواردی که می تواند بسیار مهم باشد آنست که تأثیر سرقت و وقوع تخلف مالی در یک شرکت تنها محصور به آن شرکت نیست و در کل صنعت کشور تأثیر میگذارد. با گسترش اینترنت و افزایش چشمگیر نگرانیهای ناشی از حملات سایبر ، تعداد چنین حوادثی نیز رو به افزایش است.

با وجود اینکه رایانه ها نقطهٔ مناسبی برای انجام حملات تروریستی هستند، اما این نکته را نیز باید درنظر داشت که برخی اقدامات خرابکارانه توسط افرادی صورت می گیرند که از این راه بدنبال کسب درآمد هستند. مرکز فوریتهای امنیت رایانه ای (CERT) در سال ۲۰۰۱ میلادی رقمی برابر با ۵۲۶۵۸ رخداد امنیتی اینترنتی را شناسایی کرده که دو برابر تعداد یکسال قبل تر است و نسبت به دو سال پیش از آن چهار برابر می باشد." بحث امنیت رایانه ها و شبکه ها برای کشورهای درحال توسعه از اهمیت خاصی برخوردار است. اینترنت می تواند فواصل را از میان بردارد و دسترسی به مطالب بی شماری را فراهم کند. 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 توسعهٔ هزاره به توانایی کشورهای درحال توسعه در استفادهٔ مؤثر از فناوری اطلاعات و افز ایش 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.[5,8]

متأسفانه همهٔ ظواهر خوب و بد انسانی را می توان در فضای سایبر نیز مشاهده نمود. به دلیل آنکه اینترنت از یک محیط پژوهشی و تعاونی شروع به کار کرد و هدف آن اشتراک آسان اطلاعات بود، ساختار آن باعث تسهیل حمله به رایانه ها و سرقت

اطلاعات محرمانه می گردد. انگیزۀ افرادی که در فضای سایبر چنین رفتاری از خود بروز می دهند شبیه انگیزه هایی است که در دنیای واقعی آنها را به کارهای مشابه وادار می کند، اما با یک تفاوت عمده: محیطی که توسط رایانه ها و اینترنت بوجود آمده باعث شده در افراد این تمایل بوجود بیاید که بخواهند ثابت کنند که می توانند به سیستمها وارد شوند و مشکلاتی بوجود بیاورند. بیشتر مشکلات موجود در فضای سایبر از جانب خرابکارها ناشی می شود. خرابکارها افرادی هستند که می خواهند ثابت کنند می توانند از هر سد امنیتی که سر راهشان قرار داشته باشد عبور کنند. اگر بخواهیم چنین رفتاری را در دنیای واقعی مدل کنیم باید فردی مورد اشاره قرار دهیم که می خواهد ثابت کند می تواند به خانه شما وارد شود و سپس بدون دست زدن به چیزی خارج شود ! چنین پدیده ای نه تنها موجب بروز نوعی احساس عدم اطمینان می شود، بلکه این سؤال را نیز پدید می آورد که چه چیزی درحال تغییر یافتن یا کم شدن است یا اینکه چه اقداماتی می توان برای جلوگیری از نفوذهای بعدی انجام داد. همانطور که چنین رفتاری در دنیای واقعی قابل تحمل نیست، در فضای سایبر هم نمی توان این رفتار را تحمل کرد. امروزه اینترنت دروازۀ ورود به دنیای شگفت انگیز اطلاعات و دانسته ها است و میتواند این اطلاعات را با قیمت بسیار نازل در اختیار عموم قرار دهد. بدین ترتیب می توان اطلاعات را بصورت کارآمد و مؤثری به اشتراک گذارد. با اینحال برای دستیابی به این هدف لازم است امکانات و رفتارهایی که ممکن است در مقابل آن قرار داشته باشند را بشناسیم. با مفهوم هوشیاری در دنیای واقعی آشنا هستیم. اکنون باید بیاموزیم که چگونه می توان در فضای سایبر به هوشیاری (هوشیاری سایبر) رسید. [7,9]

۷- نتیجه گیری

در عصر کنونی که عصر اطلاعات نام گرفته است و با وجود تمامی امکانات و تسهیلاتی که فناوری اطلاعات برای بشر امروز به ارمغان آورده است عرصه ای برای سوء استفاده از فناوری و حتی اعمال مجرمانه نیز فراهم گردیده است هرساله سازمان های بسیاری در سطح دنیا هدف جرائم مرتبط با امنیت از حملات ویروسی گرفته تا کلاهبرداری های تجاری قرار می گیرند برای در امان ماندن از کلیه تهدیدات فضای سایبری اعم از تهدیدات داخلی و خارجی بایستی یک برنامه جامع امنیت سایبری و پدافندی تدوین نمود که برای دستیابی به چنین هدفی بایستی ابتدا انواع تهدیدات سایبری را شناخته و راه کارهای مناسب پدافندی را برای مقابله با آنها اتخاذ نمود. همچنین روند ارزیابی تهدیدات قابل اعمال بر سیستم‌های مبتنی بر IT، به عنوان یکی از عناصر کلیدی تمامی روش‌های تحلیل ریسک سیستم‌های IT در نظر گرفته می‌شود. بدون در نظر گرفتن نتایج حاصل از اجرای این روند، می‌توان به جرأت گفت که اکثر روش‌های تحلیل ریسک موجود نتایج قابل قبول و منطقی‌ای را بوجود نخواهند آورد.

همچنین باید توجه داشت که امنیت اطلاعات امنیت کامپیوتر نیست. این مطلب در چندین مقاله مرجع تکرار شده و بیانگر آن است که در حال حاضر متخصصان امنیتی به تبع رشته و سابقه فنی خود عمدتا بر جنبه های فنی امنیت یک سیستم توجه دارند و از حملات مهندسی اجتماعی که روی انسانها پیاده می شود و غالبا انجام آن برای نفوذگران ساده تر هم هست و شرایط را برای حملات تکنیکی هموار می کنند، غافلند. شاید وقت آن باشد که مسئولین امنیتی به خود آمده و این حملات را نیز هم سنگ سایر انواع حملات جدی بگیرند و راهکارهای پدافندی و دفاعی مناسبی را اتخاذ نمایند.

۱۰- مراجع

[1] Xiao Haidong. ANALISYS OF SECURITY SITUATI ONAL AWARENESS OF CYBERSPACE. Shanghai :Shanghai Jiaotong University, Oct,2007 .

[2] WEI Yong , LIAN Yi Feng. A Network Security Situational Aware ness Model Based on Log Audit and Performance Correction. CHINESE JOURNAL OF COM PUTERS, 2009,32(4): 763-772 .

[3] WANG Longhai, ZHONG Qiuxi, DING Hao. Quantitative Algorithm of Network Security Situation Awareness Based on Performance Parameters Correction.Communication & Information Technology, 2010,(17):113- 116, 120 .

[4] CHEN Xiuzhen,ZHENG Qinghua, GUAN Xiaohong,et. Quantitative Hierarchical Threat Evaluation Model for Network Security. Journal of Software, 2006,17(4):885-897 .

[5] ZHAO Pengyu , LIU Feng, ZHANG Hongli,et. Security situation evaluation system for large scale network, Computer Engineering and Applications, 2008 , 44(33) , 122-124

[6] TanXiaobin,ZhangYong , ZhongLi. An approach to network security situation awareness based on multi-perspective analysis. NETINFO SECURITY,2008(11):47-50 .

[7] LI Lingjuan,KONG Fanlong. A Hierarchical Network Security Situation Evaluation Method Based on Grey Theory COMPUTER TECHNOLOGY AND DEVELOPMENT, 2010, 20(8):163-166 .

[8] Shu Nanfei , Niu Shaozhang. The New Development on Evaluation and Prediction of Network Security Situation, ۲۰۰۹.Workshop on the Information Technology and Its Application.

[9] Ren Wei. THE INTELLIGENT STUDY OF NETWORKS SECURITY SITUATION ASSESSMENT. Shanghai:Shanghai Jiaotong University, Jan,2007.