فصلنامه علمی تخصصی ایده های نو در علوم، مهندسی و فناوری ، دوره ۶، شماره ۲، تابستان ۱۴۰۱، ص ۲۹-۲۱
ISSN: 2588-3984
http://www.Tajournals.com

عنوان مقاله: بررسی و مطالعه مفهوم امنیت در فناوری اطلاعات
دوره ۶/ شماره ۲ / تابستان ۱۴۰۰/ ص ۲۹- ۲۱

بررسی و مطالعه مفهوم امنیت در فناوری اطلاعات

رودابه حیدری مطلع*[۱]، محمد بایگان[۲]، محمد رئیسی[۳]، زینب نارویی پور[۴]

[۱] کارشناس ارشد مهندسی نرم افزار کامپیوتر ، استاد دانشگاه آزاد واحد ایرانشهر، سیستان و بلوچستان، ایران

[۲] کارشناس فناوری اطلاعات ، دانشگاه اندیشه نو ایرانشهر، سیستان و بلوچستان، ایران

[۳] کارشناسی مهندسی نرم افزار کامپیوتر، دانشگاه آزاد واحد ایرانشهر، سیستان و بلوچستان، ایران

[۴] کارشناسی مهندسی نرم افزار کامپیوتر، دانشگاه آزاد واحد ایرانشهر، سیستان و بلوچستان، ایران

* نویسنده مسئول: رودابه حیدری مطلع

چکیده

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 بقا نظیر امنیت در برابر حمله دیگران یا حیوانات و نیز امنیت تامین غذا. بتدریج نیازهای دیگری چون امنیت در برابر حوادث طبیعی یا بیماری ها 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، محدوده امنیت ابعاد بسیار گسترده تری یافت و با تفکیک حوزه 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.

واژگان کلیدی: فناوری اطلاعات، امنیت، شبکه اینترنت، حفاظت اطلاعات

فصلنامه علمی تخصصی ایده های نو در علوم، مهندسی و فناوری ، دوره ۶، شماره ۲، تابستان ۱۴۰۱، ص ۲۹-۲۱
ISSN: 2588-3984
http://www.Tajournals.com

مقدمه

امنیت اطلاعات یعنی حفاظت اطلاعات و سیستم‌های اطلاعاتی از فعالیت‌های غیرمجاز. این فعالیت‌ها عبارتند از : دسترسی، استفاده، افشاء، خواندن، نسخه برداری یا ضبط، خراب کردن، تغییر، دستکاری. واژه‌های امنیت اطلاعات، امنیت کامپیوتری و اطلاعات مطمئن گاه به اشتباه به جای هم بکار برده می‌شود. اگر چه اینها موضوعات به هم مرتبط هستند و همگی دارای هدف مشترک حفظ محرمانگی اطلاعات، یکپارچه بودن اطلاعات و قابل دسترس بودن را دارند ولی تفاوت‌های ظریفی بین آنها وجود دارد. این تفاوت‌ها در درجه اول در رویکرد به موضوع امنیت اطلاعات، روش‌های استفاده شده برای حل مسئله، و موضوعاتی که تمرکز کرده‌اند دارد. امنیت اطلاعات به محرمانگی، یکپارچگی و در دسترس بودن داده‌ها مربوط است بدون در نظر گرفتن فرم اطلاعات اعم از الکترونیکی، چاپ، و یا اشکال دیگر. امنیت کامپیوتر در حصول اطمینان از در دسترس بودن و عملکرد صحیح سیستم کامپیوتری تمرکز دارد بدون نگرانی از اطلاعاتی که توسط این سیستم کامپیوتری ذخیره یا پردازش می‌شود.امنیت اطلاعات نمی تواند ایمنی را صد در صد سازماندهی اطلاعاتی سیستم کامپیوتری شما ضمانت نماید. به عبارت دیگر امنیت اطلاعات قادر به نگهداری اطلاعات شما نیست. هیچ سحر و جادویی را نمی توان یافت تا امنیت کاملی برای اطلاعات ایجاد نمود. مفاهیم موجود در امنیت اطلاعات، علم نظامی و فنی هم نیست که واضح و آشکار باشد. در واقع امنیت اطلاعات نوعی طرز فکر است. طرز فکری که در آن انواع تهدیدهای ممکن و راههای ضربه زدن به سازماندهی اطلاعاتی بررسی می شود و مدیریت مناسبی برای آن پیشنهاد می گردد. شاید به تعداد زیادی از تولید کنندگان برخورد کرده باشید که هر یک ادعا می کنند محصول تولیدی آنها بهترین راه حل برای رفع مشکلات امنیتی است . لیکن جهان در دهه های اخیر و بویژه در پنج سال گذشته عرصه تحولات چشمیگری بوده که بسیاری ا زمناسبات و معادلات پیشین را بطور اساسی دستخوش تغیر 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 افزایی مشارکتی (COLLABORATION) ، عملاً زندگی فردی و اجتماعی بشر را دگرگون ساخته است. به باور بسیاری از صاحب نظران همانگونه که پیدایش خط و کتابت آنچنان تاثیر شگرفی بر سرنوشت انسان برجای گذاشته که مورخین را بر آن داشته تا داستان زندگی بشر بر این کره خاکی را به دوران ماقبل تاریخ تقسیم نمایند، ورود به فضای مجازی حاصل از فناوری نوین اطلاعات و ارتباطات نیز دوره جدیدی از تمدن بشری را رقم زده، به نحوی که انقلاب عصر اطلاعات شیوه اندیشه، تولید، مصرف، تجارت، مدیریت، ارتباط، جنگ و حتی دینداری و عشق ورزی را دگرگون ساخته است.

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 شبکه رایانه ای از یک شبکه کوچک کار گروهی به شبکه ای گسترده و جهانی (اینترنت) واقع گردیده، و با توجه به رشد روز افزون 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 ،روشهای، استانداردها و ابزارهایی 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.

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 اندازه کافی و متناسب با نیازها و سرمایه گذاری انجام شده باشد تقریباً در تمامی شرایط محیطی امکانپذیر است. تنها با فراهم بودن چنین سطح مطلوبی است که اشخاص حقیقی، سازمانها، شرکتهای خصوصی و ارگانهای دولتی ضمن اعتماد و اطمنیان به طرفهای گوناگونی که همگی در یک تبادل الکترونیکی دخیل هستند و احتمالاً هیچگاه یکدیگر را ندیده و نمی شناسند، نقش مورد انتظار خود بعنوان گره ای موثر از این شبکه متعامل و هم افزا را ایفا خواهند نمود.

فصلنامه علمی تخصصی ایده های نو در علوم، مهندسی و فناوری ، دوره ۶، شماره ۲، تابستان ۱۴۰۱، ص ۲۹-۲۱
ISSN: 2588-3984
http://www.Tajournals.com

تاریخچه امنیت اطلاعات

برای اینکه نگاهی به تاریخچه امنیت اطلاعات داشته باشیم بد نیست به دوره ظهور یکی از نخستین ماشین های رمز نگاری شرکت Richard Ritter به همراه دوست صمیمی خود Arthur Scherblus توجه کنیم. در سال ۱۹۱۸ میلادی مخترع آلمانی را تأسیس کردند، یک شرکت مهندسی متفاوت با زمینه فعالیت متنوع و نامحدود از توربین تا لوازم خانگی.فعالیت Scherblus & Ritter او منجر به ساخت یکی از نخستین ماشین های رمز نگاری و شناخته شده ترین سیستم رمز الکترو مکانیکی شد.ماشین جدید بر اساس طراحی گردیده بود انیگما نامیده شد و در سال ۱۹۱۸ ثبت گردید. اولین مدل آن Rotor Machine تئوری ماشین های گردان دارای وزنی حدود ۱۲ کیلوگرم و ارزشی معادل ۳۰ هزار دلار در سال ۲۰۰۳ بود. به علت قیمت قابل توجه دستگاه، توجه کمتری در بخش تجاری به آن شد. ارتش آلمان نیز در ابتدا توجه زیادی به ارزش های انیگما نشان نمی داد زیرا هنوز نا امن بودن و ضعف سیستم های مورد استفاده در طول جنگ جهانی اول بر آنها اثبات نشده و همچنان تصور می شد اطلاع متفقین از برخی مکالمات محرمانه در طول جنگ به سبب سرقت اطلاعات مربوط توسط جاسوسان بوده است نه کشف پیام های رمز شده و شکست دستگاه های استفاده شده در طول جنگ اول جهانی.تا یک دهه پس از جنگ جهانی اول این تصور ادامه داشت تا اینکه در سال ۱۹۲۳ با افشای جزئیات چگونگی دستیابی به محتوای پیام های مخابره شده ارتش آلمان توسط ارتش انگلیس دوران بی توجه ای ارتش آلمان به انیگما پایان یافت. در کمتر از دو دهه بعد بیش از ۳۰ هزار انیگما توسط ارتش آلمان خریداری شد. اشتباه جنگ اول جهانی تکرار شد و ارتش آلمان یک بار دیگر تمام ارتباطات خود را با اطمینان و خوش بینی کامل بر انیگما بنا نهاد، اشتباهی که به گواه تاریخ ، یکی از عوامل اصل شکست ارتش نازی و سقوط رایشسوم بود. تا ۱۳ سال پس از ساخت اولین نمونه انیگما، انیگما غیرقابل شکست و رمز آن غیر قابل کشف تصور می شد. تا اینکه در سال روشی کاملاً ریاضی برای شکست انیگما ارائه کرد.

این روش " Marian Reje Wski" 1932 یک افسر ریاضیدان لهستانی به نام علاوه بر ایجاد امید در متفقین برای شکست انیگما یک دستاورد مهم در تاریخ رمزشناسی بود. بی تردید در کنار تمام عوامل مؤثردر تغییر مسیر جنگ جهانی دوم جهانی و سقوط ارتش آلمان، شکست ماشین انیگما و کشف رمز آن تأثیر به سزا داشته است. تلاش های انجام شده در این حوزه در طول جنگ دوم جهانی هم از نقطه نظر ایجاد امنیت و هم از حیث روش ها و تکنیک های شکست ساختارهای امنیتی بسیار قابل توجه هستند. تا اوایل دهه هفتاد، فعالیت های مربوط به دسترسی و محافظت از اطلاعات در سازمان ها و شرکت ها محدود به محل های نگهداری این اطلاعات شامل آرشیو اسناد و شبکه های محلی رایانه ای بود. در چنین محیط های حفاظت فیزیکی امنیت سیستم ها را اطلاعات را تا حد بسیار بالایی تأمین می کرد. در واقع تا اوایل دهه ۸۰ میلادی امنیت فقط با دیدگاه فنی مشاهده می شدو برقراری آن منوط به امنیت رایانه و دستگاههای جانبی می دانستند. اما با گذشت زمان متوجه شدند که بیشتر تجاوزات امنیتی از طریق مسائلی همچون ضعف های مدیریتی (از لحاظ امنیتی) و عوامل انسانی (به دلیل عدم آموزش) می باشد لذا از اواسط دهه ۸۰ میلادی تا اواسط دهه ۹۰ میلادی بحث مدیریت امنیت اطلاعات مطرح شد که آن را منوط به خط مشی امنیت اطلاعات و ساختارهای سازمانی می دانستند. از اواسط دهه ۹۰ میلادی پارامترهای دیگری چون تعریف استراتژیهای امنیتی و خط مشی امنیتی بر اساس نیازهای اصلی سازمان و مدیریت آن می باشد. مؤلفه هایی چون استانداردهای امنیت اطلاعات، گواهی نامه های بین المللی، فرهنگ سازی امنیت اطلاعات در سازمان و پیاده سازی معیارهای ارزیابی دائمی و پویای امنیت اطلاعات را نیز شامل می شود. لازم به ذکر است که این مرحله هنوز ادامه دارد و در حال تکمیل شدن می باشد(نصیری، ۱۳۹۳).

تعریف امنیت اطلاعات

بنا بر فرهنگ Merrian- Webster (که به صورت زنده در آدرس www.m-w.com موجود است) کلمه «اطلاعات» بصورت زیر تعریف شده است: اطلاعات دانشی است که از طریق تحقیق، مطالعه، آموزش، فهم مطلب، اخبار، حقایق، دیتا، سیگنال یا کارکتری که حاوی دیتا باشد (مانند سیستمهای مخابراتی یا کامپیوتری)، چیزی که نحوه ایجاد تغییرات در یک ساختار را بیان

می کند (مانند طرح یا تئوری) و چیزهایی از این قبیل بدست آمده باشد. در همین فرهنگ نامه امنیت بصورت زیر تعریف شده است :

رهایی از خطر، وجود ایمنی، رهایی از ترس یا نگرانی اگر دو کلمه فوق را در کنار هم قرار دهیم ، به تعریفی از «امنیت اطلاعات» بصورت زیر خواهیم رسید: امنیت اطلاعات میزان اجازه و اختیاری است که استفاده از یک سرویس ، عدم استفاده از آن، و مقدار ایجاد اصلاحات توسط آن تعریف می شود و جلوگیری از بکارگیری دانش، حقایق ، دیتا یا قابلیت ها را باعث می شود .این تعریف حوزه وسیعی را شامل می شود که دانش ، حقایق ، دیتا یا قابلیت ها در برابر اتفاقات بد محافظت شود. علاوه بر این در تعریف فوق محدودیتی روی شکل اطلاعات قرار ندادیم بطوریکه می تواند بصورت دانش یا قابلیت های یک سیستم باشد. اما تعریفی که از امنیت شبکه ارائه شد ضمانتی روی حفاظت از اطلاعات ندارد . زیرا اگر بزرگترین قلعه نظامی دنیا بسازیم باز هم یک نفر پیدا خواهد شد که با ابزار جنگی قوی تر و بزرگتری آن قلعه را فتح خواهد کرد. امنیت اطلاعات نامی است که به اقدامات پیشگرانه اطلاق می شود بطوریکه این اقدامات قادر است از اطلاعات و قابلیت هایمان نگهبانی نماید. بدین ترتیب می توانیم اطلاعات را در برابر حملات خارجی و بهره برداری های غیر مجاز محافظت نماییم.

امنیت فیزیکی

از جهت تاریخی می توان گفت اولین شکل اطلاعاتی که بشر آنها را نگهداری می کرد به صورت فیزیکی بودند بطوریکه در ابتدا آنها را روی سنگ و بعداً روی کاغذ ثبت می کرد. (بسیاری از کتابهای راهنمای تاریخی در مکان امن و مناسبی قرار نداشته اند تا اطلاعات حیاتی آنها در امان بماند . به همین دلیل امروزه اطلاعات بسیار کمی درباره علم کیمیا وجود دارد. علاوه بر این کسانی که اطلاعات مهم در اختیار داشتند آنرا فقط در برخی شاگردان خاص خود قرار می دارند چنانکه ضرب المثلی معروف میگوید دانش همان قدرت است . شاید این روش بهترین روش باشد . یک ضرب المثل معروف می گوید: رازی که بیش از یکنفر آنرا بداند دیگر راز نیست). بهر حال برای محافظت از این سرمایه ها امنیت فیزیکی بصورت دیوار ، خندق و نگهبان بکار می رفت. برای ارسال این نوع اطلاعات از یک پیام رسان استفاده می شد که اغلب نگهبانی هم او را همراهی می کرد. خطر موجود در این حالت کاملاً فیزیکی است چون راهی وجود ندارد که بدون بدست آوردن آن شئ اطلاعاتش را بدست آورد. در اکثر موارد سرمایه موجود به سرقت می رفت (این سرمایه پول یا اطلاعات مکتوب بود) و مالک اصلی آنرا از دست می داد.

امنیت مخابراتی

متأسفانه امنیت فیزیکی دارای نقص عمده ا ی است و آن اینکه اگر هنگام جابجایی اطلاعات، پیام به سرقت رود اطلاعات آن قابل استفاده و یادگیری برای دشمن خواهد بود . این نقیصه توسط ژولیس سزار شناسایی شده بود. راه حل این نقص در امنیت مخابراتی است. ژولیس سزار برای رفع این مشکل رمز سزار را ایجاد کرد. این نوع رمز باعث میشد تا اطلاعات در حال انتقال حتی اگر به سرقت برود توسط کسی قابل خواندن و استفاده نباشد. این مسئله در جنگ جهانی دوم ادامه پیدا کرد. آلمانی ها از ماشینی به نام Enigma استفاده کردند که پیام های ارسالی به واحدهای نظامی توسط آن رمز میشد. آلمانی ها ادعا می کردند اگر از ماشین Enigmaبدرستی استفاده شود نمی توان قفل آنرا شکست . اما استفاده درست از آن کار بسیار سختی بود، به همین دلیل برخی اپراتورها هنگام استفاده از این ماشین دچار اشتباه می شدند و در نتیجه طرف مقابل قادر بود برخی پیامها را بخواند (بعد از آنکه مقادیر قابل توجهی از منابع رمز این ماشین بدست آمد مشکل خواندن پیام های آن نیز حل شد).

ارتباطات نظامی برای ارسال پیام به واحدها و مکان های نظامی از کلمات کد استفاده می نمایند. ژاپن در طول جنگ از کلمات کدی استفاده می کرد که درک درست پیام ها را برای آمریکایی ها ، حتی اگر کدها را کشف می کردند بسیار مشکل می ساخت . زمانیکه جنگ به نبرد Midway کشیده شد، کد شکن های آمریکایی سعی می کردند هدف ژاپنی ها پیدا کنند. این هدف در پیام های ژاپنی ها بصورت " AF " دیده می شد. سرانجام آمریکایی کاری می کردند تا Midway عمداً پیامی درباره کمبود آب ارسال نماید. ژاپنی ها مجبور شدند در پاسخ و یک پیام کد ارسال کنند. در پیام کد شده معلوم گردیده که AF مخفف

فصلنامه علمی تخصصی ایده های نو در علوم، مهندسی و فناوری ، دوره ۶، شماره ۲، تابستان ۱۴۰۱، ص ۲۹-۲۱
ISSN: 2588-3984
http://www.Tajournals.com

آب است . از انجام که آمریکایی ها پیام ژاپنی ها را خواندند لذا قادر بودند که بفهمند AF در واقع همان Midway است. پیام ها تنها نوع ترافیکی نبود که کد می شدند . واحدهای ارتش آمریکا از یک زبان محلی استفاده می کردند تا دشمن نتواند به پیام های مخابره شده گوش کند . این افراد محلی برای ارسال پیام ها استفاده می کردند به همین دلیل اگر دشمن به این پیام ها گوش می داد نمی توانست از آن چیزی بفهمد.

بعد از جنگ جهانی دوم جاسوسان اتحاد جماهیر شوروی برای ارسال اطلاعات از یک سیستم خاص استفاده می کرد که one- time pads (الگوی یکبار مصرف) نام داشت. این سیستم در واقع از چند صفحه کاغذ ادبی تشکیل شده بود که هر صفحه از آن دارای یک عدد تصادفی بود. هر صفحه فقط و فقط برای یک پیام بکار می رفت . چنانچه از این روش رمز نگاری بدرستی استفاده می شد، غیر قابل شکست بود اما در اینجا هم اشتباهات انسان باعث شد تا برخی از پیام ها قابل رمز گشایی شود.

امنیت کامپیوتری

اگر از سیستم تله تایپ برای ارسال پیام استفاده شود، کافی است برای محافظت پیام امنیت مخابراتی و امنیت تشعشع رعایت شود. اما با ورود کامپیوتر به عرصه زندگی انسان چشم اندازهای جدیدی در نحوه ذخیره و ارسال اطلاعات ایجاد گردید و فرمت های جدیدی برای سیگنالهای الکتریکی حاوی پیام ابداع گردید . با گذشت زمان استفاده از کامپیوتر آسانتر شد و مردمان بیشتری امکان استفاده و برقراری ارتباط دو طرفه با آنرا پیدا کردند. بدین ترتیب اطلاعات موجود روی سیستم کامپیوتر ی برای هر کسی ک بتواند از این وسیله استفاده کند قابل استفاده می شود. در سال ۱۹۷۰ دو نفر به نامهای Leonard La Padula و Davd Bel مدلی برای عملکرد ایمن کامپیوتر ابداع کردند. این مدل بر اساس یک مفهوم حکومتی بنا شده است که در آن اطلاعات بصورت طبقه بندی شده وبا سطوح مختلف قرار می گیرد و مجوزهایی با سطوح مختلف برای استفاده از اطلاعات وجود دارد . (در این سیستم اطلاعات به چهار فرم طبقه بندی نشده ، محرمانه ، سری و بسیار سری تقسیم بندی می شود) . بدین ترتیب اگر کسی یا سیستمی دارای مجوزی باشد که سطح آن از سطح طبقه بندی اطلاعات بالاتر باشد می تواند به آن فایل دسترسی پیدا کند. مدل فوق اساس استاندارد ۵۲۰۰/۲۸ در آمریکا گردید که به نام TCSEC شناخته می شود (البته به نام کتاب نارنجی هم شناخته می شود). کتاب نارنجی سیستم های کامپیوتری را بر طبق معیار زیر تعریف می کند :

حداقل محافظت (و یا خارج از محدوده)	D
محافظت امنیتی از روی احتیاط	C1
محافظت بصورت دسترسی کنترل شده	C2
محافظت امنیتی طبقه بندی	B1
محافظت ساختار یافته	B2
حوزه های امنیتی	B3
طراحی بازبینی	A1

برای هر یک از تقسیم بندی های فوق کتاب نارنجی وظایف خاصی را به عنوان پیش نیاز معین کرده است تا اطمینان و ضمانت لازم حاصل شود. بنابراین برای آنکه سیستمی به سطح خاصی از اطمینان برسد و مورد تصدیق قرار گیرد باید این وظایف و خصوصیات را بدرستی رعایت نماید. فراهم کردن ملزومات سیستمی کاملاً امن و مطمئن ، نیاز به دقت بسیار و هزینه بالا دارد. به همین دلیل سیستم های کمی وجود دارند که از تقسیم بندیC2 بالاتر باشند (تاکنون فقط یک سیستم توانسته به A1 برسد و آن سیستم Honeywel Scomp است. معیار های دیگری که وجود دارند سعی کردهاند وظایف یک سیستم را از اطمینان و ضمانت آن جدا نمایند. برای نمونه می توان به German Green Book در سال ۱۹۸۹، Canadian Criterid در سال ۱۹۹۰ ، CISE یا Criteria Information Security Evaluation در سال ۱۹۹۱ و بلاخره Federal Criteria در سال ۱۹۹۲ اشاره کرد. هر یک از این معیارها تلاش کرده اند برای امنیت بخشیدن به سیستم های کامپیوتری روشی را پیشنهاد دهند. در آخر باید گفت سیستم های کامپیوتری به سرعت به طرف برنا مه های تضمین شده و مطمئن در حرکتند . این حرکت

آنقدر سریع است که قبل از آنکه نسخه های قدیمی سیستم عامل و سخت افزار کامپیوتر بتواند مورد تائید واقع شوند، نسخه های جدید به بازار می آید.

امنیت شبکه

از جمله مشکلات موجود در هنگام ارزیابی معیار های امنیت کامپیوتری فقدان درک مفهوم شبکه بود. هنگامی که کامپیوترها به هم شبکه شدند مفاهیم جدیدی از امنیت هم پدیدار شد و مفاهیم قبلی امنیت دیگر مفید نبود. به عنوان مثال هنگام استفاده از مخابرات، شبکه ای محلی وجود دارد و نه یک شبکه گسترده، علاوه بر این در یک شبکه کامپیوتری از سرعت های بالاتری استفاده می شود و تعداد زیادی ارتباط از طریق یک واسطه ایجاد می شود. در این حالت استفاده از یک رمز کننده خاص به هیچ عنوان جوابگوی نیاز امنیتی نمی باشد. علاوه بر این مسئله تشعشع الکتریکی از سیم هایی که در یک اتاق یا ساختمان کامپیوترها را به هم شبکه کرده است نیز وجود دارد و سرانجام این که در یک شبکه کامپیوتری کاربرانی وجود دارند که از سیستم های بسیار متنوع به سیستم ما دسترسی دارند بدون اینکه توسط یک کامپیوتر واحد، کنترل مرکزی روی آنها اعمال گردد.

در کتاب نارنجی به مفهوم کامپیوتر های شبکه شده اشاره ای نشده است . به عبارت دیگر دسترسی از طریق شبکه قادر است اعتبار کتاب نارنجی را زیر سؤال ببرد. جواب این مشکل در کتاب آورده شده است که به شرح شبکه امن در TCSEC می پردازد و به TNI یا کتاب قرمز معروف است. مفاد کتاب قرمز در سال ۱۹۸۷ تنظیم شده است . کتاب قرمز تمام نیازهایی که کتاب نارنجی به آن اشاره کرده است را در خود دارد و علاوه برآن سعی کرده است به محیط شبکه ای کامپیوترها هم بپردازد . متأسفانه کتاب قرمز بیشتر به مسائل وظیفه ای پرداخته است به همین دلیل سیستم های کمی توانسته اند تحت TNI یا کتاب قرمز ارزیابی گردند که البته هیچکدام از آنها به موفقیت تجاری نرسیدند.

امنیت اطلاعات

به نظر شما تاریخچه ای که تا اینجا از امنیت ارائه شد ما را به چه چیز راهنمایی می کند ؟ از این تاریخچه معلوم می شود هیچ یک از انواع امنیتی که به آن اشاره شد به تنهایی قادر نیستند مشکلات امنیتی ما را حل نماید. امنیت فیزیکی خوب زمانی نیاز است که بخواهیم سرمایه ای مانند کاغذ یا یک سیستم ثبت اطلاعات را محافظت کنیم. امنیت مخابراتی برای محافظت اطلاعات به هنگام ارسال آنها مفید است . امنیت تشعشع زمانی مفید است که دشمن بتواند با استفاده از منابع کافی که در اختیار دارد تشعشعات الکتریکی حاصل از سیستم کامپیوتری را بخواند . امنیت کامپیوتری برای کنترل دسترسی دیگران به سیستم های کامپیوتری نیاز است و بلاخره امنیت شبکه برای امنیت شبکه محلی نیاز است. جمع بندی تمام مفاهیم فوق و استفاده از تمام آنها در کنار هم، امنیت اطلاعات را تحقق می بخشد.

هر آنچه ما انجام می دهیم نمی تواند نوعی پروسه اعتبار بخشی به سیستم های کامپیوتری باشد. تکنولوژی به سرعت در حال پیشرفت است و بسیاری ا ز این پروسه ها را پشت سر می گذارند. اخیراً آزمایشگاه بیمه گر امنیتی پیشنهاد شده است . در این آزمایشگاه میزان امنیت انواع محصولات موجود مورد ارزیابی قرار گرفته و تصدیق می‌شود . اگر محصولی نتواند گواهی لازم را کسب کند در آن صورت کاربر، تولید کننده آن محصول را بی دقت خواهد دید چون ممکن است سایت یا اطلاعات کاربر در معرض تهاجم قرار گیرد . متأسفانه این ایده دو مشکل دارد:

•تکنولوژی با سرعت رو به جلو در حرکت است و در نتیجه دلیل چندانی وجود ندارد چنین آزمایشگاهی شانس بهتری برای گواهی کردن محصولات داشته باشد. چون ممکن است قبل از تصدیق یک محصول نسخه جدیدتر آن وارد بازار گردد.

•ثابت کردن این مسئله که برخی چیزها امن و مطمئن هستند، اگر غیر ممکن نباشد بسیار سخت است . شما به سادگی تحت تاثیر گواهی چنین آزمایشگاهی به یک حصول اعتماد می کنید و آنرا غیر قابل نفوذ خواهید پنداشت در حالیکه یک پیشرفت جدید و یک توسعه جدیدتر می تواند تمامی گواهی های امروز را بی اعتبار کند.

در حالیکه صنایع در حال جستجو برای یک جواب نهایی هستند ، ما سعی می کنیم تا امنیت را به بهترین حالتی که بتوانیم پیاده کنیم . این کار از طریق ممارست و پشتکار دائم حاصل می شود.

اهمیت و جایگاه امنیت در فناوری اطلاعات و ارتباطات

با ایجاد شبکه های کامپیوتری، مفاهیم جدیدی از امنیت شبکه مطرح گردید که تا قبل از آن هرگز پیش بینی نشده بود. در شبکه های امروزی، چند و یا چندین هزار کامپیوتر به هم متصل شده اند که با سرعت زیادی در حال تبادل اطلاعات با یکدیگری می باشند. در معرض آسیب قرار گرفتن داده ها و اطلاعات حساس، تجاوز به حریم خصوصی کاربران، استفاده از کامپیوتر کاربران برای تهاجم علیه سایر کامپیوترها، از جمله اهداف مهاجمانی است که با بهره گیری از آخرین فنآوری های موجود، حملات خود را سازماندهی و بالفعل می نمایند. بنابراین، می بایست به موضوع امنیت فناوری اطلاعات که شامل مواردی همچون امنیت اطلاعات، ایمن سازی کامپیوترها و شبکه های کامپیوتری می شود، توجه جدی شده و از فرآیندهای متفاوتی در جهت مقاوم سازی آنان، استفاده گردد. پیاده سازی امنیت در این بستر نیاز به طرح های کامل و پیچیده ای دارد. بررسی و ارائه ی روش های امنیتی برای شبکه های کامپیوتری یکی از دغدغه های مهم مربوط به دنیای فناوری اطلاعات است. امنیت فناوری، در کاربردهای اقتصادی و تجاری بیشترین اهمیت را دارد، بطوریکه گسترش فناوری اطلاعات در این زمینه مشروط به حفظ امنیت آن است. البته لازم به ذکر است که به دلایل هزینه، رشد دائم فضاهای نا امن و غیره نمیتوان امنیت را بطور کامل و جامع اعمال نمود. اما می توان حد متوسط و قابل قبولی را برای امنیت تصور نمود و براساس اهمیت موضوع و امکانات موجود، برنامه ریزی نمود و هزینه آن را محاسبه کرد

راهکارهای امنیتی شبکه

۱: کنترل دولتی: علاوه بر بهر هگیری از امکانات فنی، روشهای کنترل دیگری نیز برای مهار اینترنت پیشنهاد شده است. در این روش، سیاست کلی حاکم بر کشور اجازه دسترسی به پایگاه های مخرب و ضد اخلاقی را نمی دهد و دولت شبکه های جهانی را از دروازه اتصال و ورود به کشور با فیلترهای مخصوص کنترل می کند.

۲: کنترل سازمانی: روش دیگر کنترل سازمانی است که معمو ً لا سازمان، اداره یا تشکیلاتی که مسئولیت سروی سده ی و اتصال شهروندان را به اینترنت به عهده می گیرند، خود موظف به کنترل شبکه و نظارت بر استفاده صحیح از آن می شود تا با الزامات قانونی و اخلاقی توامًا انجام این وظیفه را تضمین کند.

۳: کنترل فردی: کنترل فردی روش دیگری است که قابل انجام است. در این نوع کنترل تمام تضمینهای اجرایی، درون فردی است و شخص با بهرهگیری از وجدان فردی و مبانی اخلاقی و تعهد دینی، مراقبتهای لازم را در ارتباط با شبکه های جهانی به عمل آورد. این اعتقاد و فرهنگ در محدودهٔ خانواده نیز اعمال می شود و چه بسا اطرافیان را نیز تحت تأثیر قرار دهد. البته شیوهٔ اخیر در صورتی ممکن پس از شناسایی IP خواه بود که واگذاری خط اشتراک کامل افراد و با ملاحظه خصوصیات اخلاقی آنان انجام پذیرد. در غیر این صورت تصور اعمال چنین کنترلی از سوی تک تک افراد جامعه صرفًا در حد آرزو باقی خواهد ماند. آرزویی که نمی تواند بسیاری از تأثیرات سوء این شبکه را از بین ببرد و آن را بسوی شبکه سالم سوق دهد.

۴: تقویت اینترانت ها: از سوی دیگر تقویت شبکه های داخلی که به اینترانت معرو ف است می تواند نقش بسزایی در کاهش آلودگی های فرهنگی و اطلاعاتی اینترنت یاری کند. قرار دادن اطلاعات مفید اینترنت به صورت ناپیوسته و روی شبکه های داخلی یا اینترانت ها، علاوه بر ارائهٔ خدمات و اطلاع رسانی سالم، پس از چندی، بایگانی غنی و پرباری از انواع اطلاعات فراهم آمده از چهار گوشه جهان را در اختیار کاربران قرار م یدهد که با افزایش اطلاعات داخلی و یا روزآمد کردن آن، به عنوان زیربنای اطلاعاتی کشور قابل طرح می باشد. به هر حال سرعت بالا و هزینه کم در استفاده از اینترانتها، دو عامل مورد توجه کاربران به شبکه های داخلی است که به نظر نم یرسد محمل مناسبی برای اطلاعات گزینش شده اینترنت باشد.

۵: وجود یک نظام قانونمند اینترنتی: مورد دیگر که کارشناسان از آن به عنوان پادزهر آسیب های اینترنتی از قبیل تهاجم فرهنگی، اطلاعات

نادرست و یا پیامدهای ضد اخلاقی نام م یبرند، وجود یک نظام قانونمند اینترنتی در جامعه است که ادارهٔ آن از سوی یک متولی قدرتمند و کاردان می تواند اینترنت سرکش وافسار گسیخته را مهار کند و از آن به نحو شایسته بهره برداری نماید. این نظام اگر با یک نظام حقوقی و دادرسی جامع و عمیق توأم باشد، موارد تخلف و سوءاستفاده از این ابزار به راحتی قابل تشخیص و پیگیری قضایی خواهد بود. در این صورت امکان سوءاستفاده و تأثیرپذیری از فرهنگهای بیگانه که عمومًا مغایر با اصول اخلاقی ماست، به طرز چشمگیری کاهش می یابد.

۶: کار گسترده فرهنگی برای آگاهی کاربران: اما بهترین روش، کار گستردهٔ فرهنگی، برای آگاهی کاربران است. کافی است که آنها آگاه شوند که گرایش و ارتباط با پایگاه های غیرمتعارف جز ضلالت و تباهی ثمره های ندارد. باید تقوای درونی و اعتقادات دینی کاربران را رشد داد و آنها را تقویت کرد. بنابراین بهترین بارو (فایروال) برای ممانعت از خطرات اینترنت و جلوگیری از تأثیر ابعاد منفی آن، وجدان درونی و ایمان هر نسل است که بخشی از این ایمان را علمای دین باید در وجود نسل جوان و انسانهای این عصر بارور سازند

۷: فایروالها: در حقیقت فایروال یا بارو شبکه های کوچک خانگی و شبکه های بزرگ شرکتی را از حملات احتمالی رخنه گرها (هکرها) و وب سایتهای نامناسب و خطرناک حفظ می کند و مانع و سدی است که متعلقات و دارایهای شما را از دسترس نیروهای متخاصم دور نگاه می دارد. بارو یک برنامه یا وسیله سخ تافزاری است که اطلاعات ورودی به سیستم رایانه و شبک ههای اختصاصی را تصفیه می کند. اگر یک بسته اطلاعاتی ورودی به وسیلهٔ فیلترها نشا ندار شود، اجازه ورود به شبکه و رایانه کاربر را نخواهد داشت.

نتیجه گیری

تمام افراد و کشورها از فناوری اطلاعات بهره می جویند، اما این فناوری برای کشورهای در حال توسعه جاذبه خاصی دارد و می تواند جا افتادن آنها در جامعه اقتصاد جهانی را تسریع کند. این فناوری هنوز در آغاز راه خود است ولی بسرعت در حال پیشرفت می باشد. متأسفانه همانند سایر پیشرفتهای فناوری، اینترنت نیز می تواند هم برای اهداف مشروع و هم برای اهداف نامشروع مورد استفاده قرار گیرد. همانطور که مشاهده کردیم در دنیای سایبر مجرمان و خرابکارانی وجود دارند که از اینترنت برای حمله به کاربران منفرد و سازمانی استفاده می کنند. این پژوهش حاوی مجموعه ای از الگوها سرآمدی در زمینه امنیت است که در اجرای سیاستها و روشهایی که به موقعیت خاص شما مربوط هستند کمک می کنند. علاوه بر آن مراجع چاپی و الکترونیکی فراوانی که در بر دارنده ابعاد خاص امنیت فناوری اطلاعات هستند و همچنین سازمانهایی که به شکل تخصصی بر روی موضوعات امنیت فناوری اطلاعات تمرکز دارند را معرفی می کند. تمامی این منابع برای افراد و سازمان هایی که در پی گسترش آگاهی خود از امنیت در جهان شبکه ای می باشند مفید خواهند بود. این شرایط در کشورهای در حال توسعه از اهمیت خاصی برخوردار است. سرمایه گذاری مستقیم خارجی و اعتماد و قابلیت اطمینان در این کشورها بستگی به سطح امنیت و پیاده سازی موفقیت آمیز فناوری و زیر ساختهای آن دارد. دولتها ، سازمانها و کاربران منفرد همگی نقش بسزای در تأمین امنیت سرمایه های اطلاعاتی و الکترونیکی کشورها ایفا می کنند. شناخت تهدیدات بسیار سودمند است، و عملکرد مناسب براساس چنین شناختی می تواند یک محیط قابل اطمینان ایجاد کند و باعث شود ساکنان کره زمین تا سرحد امکان فواید عصر نوین دیجیتال را حس کنند.

مراجع

- رنجبر، مقصود. (۱۳۷۹). ملاحظات امنیتی در سیاست خارجی جمهوری اسلامی ایرا . ن تهران: پژوهشکده مطالعات راهبرد.ی
- رابرت، ماندل. (۱۳۷۷). چهره متغیر امنیت مل . ی تهران: پژوهشکده مطالعات راهبردی.
- محسنیان راد، مهدی. (۱۳۷۷) ارتباط جمعی در کشورهای اسلام . ی دانشگاه امام صادق، انتشار محدود.

- محسنیان راد، مهدی. (۱۳۷۶). انتقاد در مطبوعات ایرا . ن مرکز مطالعات و تحقیقات رسان هها، انتشار محدود.
- محمدی، مجید. (۱۳۷۹) سیمای اقتدارگرایی تلویزیون دولتی ایرا . ن تهران: جامعه ایرانیان.
- مولانا، حمید. (۱۳۷۹). جریان بین المللی اطلاعات ترجمهٔ یونس شکرخواه. تهران: مرکز مطالعات و تحقیقات رسانه ها.
- سید احسان اعتباریان.(امنیت شبکه)، انتشارات: دانش پرور ، سال انتشار: ۱۳۸۳

- Mohammadi Annabelle Sreberny, Ali. Small media, Big Revolution: Communication, Culture, and
- the Iranian Revolution. Univ of Minnesota Press. Sick, Gary. Middle East Studies Association Bulletin, December, 1999.
- Us Dept of State 2000. A National security Strategy for a new centry, 2000.
- Tehranian, Majid. Global Communication and World Politics: Domination, Development and