ششمین همایش ملی تجارت و اقتصاد الکترونیکی

نشست تخصصی امنیت و اعتماد

تبیین جایگاه امنیت در تجارت الکترونیکی

مجید یوسفی، عضو هئیت علمی و پژوهشگر حوزه فناوری اطلاعات ، معاونت پژوهش دانشگاه علوم دریایی امام خمینی(ره) [1]

سید اسدا... عسگری رانکوه، کارشناس ارشد تجارت الکترونیک دانشگاه تهران ، دانشگاه علوم دریایی امام خمینی(ره) نوشهر

چکیده

تجارت الکترونیک به عنوان انقلابی در عرصه فناوری قرن بیست و یکم تلقی می شود، که با جهانی شدن بازار، به سرعت در عرصه های مختلف رو به گسترش و پیشرفت است. سازمان هایی که به ارائه خدمات تجارت الکترونیک می پردازند، با پذیرش ریسک های امنیتی ناشی از آن، در پی کسب منفعت از فعالیت هایشان هستند. از این رو توجه ویژه به امنیت و تهدیدات و آسیب هایی که می تواند بواسطه عدم توجه به آن، به سازمان های پذیرنده و افراد فعال در حوزه تجارت الکترونیک وارد شود، امری مهم و قابل ملاحظه است. هرچند صحبت از امنیت مطلق، بحثی انتزاعی و خارج از واقعیت های پیرامون ماست، لیکن سازمان ها می باید جهت برخورداری از یک وضعیت غیر شکننده (در زمان بهره گیری از تجارت الکترونیک)، هزینه هایی را متقبل شده و تهدیدات و آسیب هایی که ممکن است به آنها وارد شود را به گونه ای مطلوب مدیریت نمایند. در این مقاله ضمن مروری بر مفاهیم اساسی تجارت الکترونیک، ضرورت امنیت در آن مطرح شده و با بررسی چالش های امنیتی، تقسیم بندی مفیدی جهت ارتقاء سطح امنیت در تجارت الکترونیک ارائه می گردد.

کلمات کلیدی: : فناوری اطلاعات ، تجارت الکترونیک ، چالش های امنیتی ، امنیت اطلاعات کنشی[2] ، امنیت اطلاعات واکنشی[3]

.

---

۱. مقدمه

این روزها با گسترش بحث فن آوری اطلاعات، واژه الکترونیک به صفتی تبدیل شده است که به ده ها کلمه دیگر اضافه شده و عبارات جدید می‌سازد. در بحث تجارت نیز تجارت الکترونیکی انقلابی است که درحال تغییر روش های تجاری وحتی تغییر نحوه تفکر انسان هاست. [۵]

---

[1] مجید یوسفی. تلفن: ۰۹۱۲۳۰۱۵۲۰۲؛ فکس: ۳۲۳۴۳۱۷-۰۱۹۱ .

آدرس پست الکترونیکی: majid55nba@yahoo.com ؛ نوشهر، دانشگاه علوم دریایی امام خمینی(ره)، معاونت پژوهش و فناوری.

[2] Proactive Information Security

[3] Reactive Information Security

هر فناوری پیشرفته، باعث ایجاد تهدیدها و فرصت های جدید برای سازمان ها گشته و تغییر در فناوری، موجب ایجاد تحول در سازمانها و فعالیتهای اجتماعی می گردد. توجه فزاینده سازمان ها به تجارت الکترونیک، ناشی از اهمیت و میزان تاثیر قابل انتظاری است که این فناوری، هم بر محیط اقتصادی و هم بر محیط اجتماعی می گذارد. علی رغم مزایای فراوانی که کاربرد تجارت الکترونیک به همراه داشته است، هر ساله سازمان های بسیاری هدف جرائم مرتبط با امنیت، از حملات ویروسی گرفته تا کلاه برداری های تجاری و سرقت اطلاعات قرار می گیرند. با افزایش کاربران سیستم های اطلاعاتی، دسترسی آسان به اطلاعات و رشد فزاینده کاربران، می توان انتظار داشت که به همین نسبت تعداد سوء استفاده ها از فناوری و تهدیدهای امنیتی افزایش یابد. [۴]

گسترش تجارت الکترونیکی نیازمند بستری ایمن برای مخابره و دریافت اسناد بازرگانی و اطلاعات است. این فناوری در عین حال که دقت و سرعت پردازش را افزایش چشمگیری بخشیده است، باید پاسخگوی مسائل و خطراتی باشد که برای آن پیش می آید. برخلاف سیستمهای سنتی که جهت حفظ اطلاعات غیر الکترونیکی، عمدتاً از حفاظت فیزیکی برای امنیت اطلاعات استفاده می نمایند، اطلاعات الکترونیکی در معرض تهدیدات متنوع تر و پیچیده تری هستند. انتقال اطلاعات در رسانه های بعضاً عمومی، امکان اتصال به انباره های اطلاعاتی، هزینه بسیار کم در انتقال حجم قابل توجهی از اطلاعات، از جمله مواردی هستند که زمینه ساز این تهدیدات بشمار می روند. [۱۲]

۲. تعریف تجارت الکترونیک

در این ارتباط، مقایسهٔ ویژگی‌های تجارت الکترونیک در مقایسه با تجارت سنتی جالب خواهد بود: [۵]

- تجارت الکترونیک ضعفها و مشکلات را در معرض نمایش جهانی قرار می‌دهد.
- در امر تجارت الکترونیک هیچ حد و مرزی وجود ندارد (برای بازاریابی، میزان سفارش، نوع کیفیت و نوع خدمات کالای سفارشی).
- در تجارت الکترونیک نیاز به تفکر مداوم در تدوین استراتژی‌های تجاری احساس می‌شود چراکه عدم برنامه‌ریزی صحیح در این مسیر، جبران‌ناپذیر خواهد بود.
- در تجارت الکترونیک طراحی براساس نقطه‌نظر و دیدگاه مشتری بسیار حیاتی در تجارت الکترونیک نیاز به سرعت بالا در تصمیم‌گیری و اجرای برنامهٔ تدوین شده چشم‌گیر است.

با توجه به موارد فوق تجارت الکترونیکی در برگیرنده مجموعه متنوع و وسیعی از تعاریف و مفاهیم است که در این تعاریف و مفاهیم به موضوعات، کاربردها و مدل‌های گوناگون آن اشاره می شود. به همین لحاظ تعاریف بسیاری از سوی متخصصان این حوزه برای مفهوم تجارت الکترونیک ارائه شده است، که برخی از این تعاریف به شرح زیر می باشند :

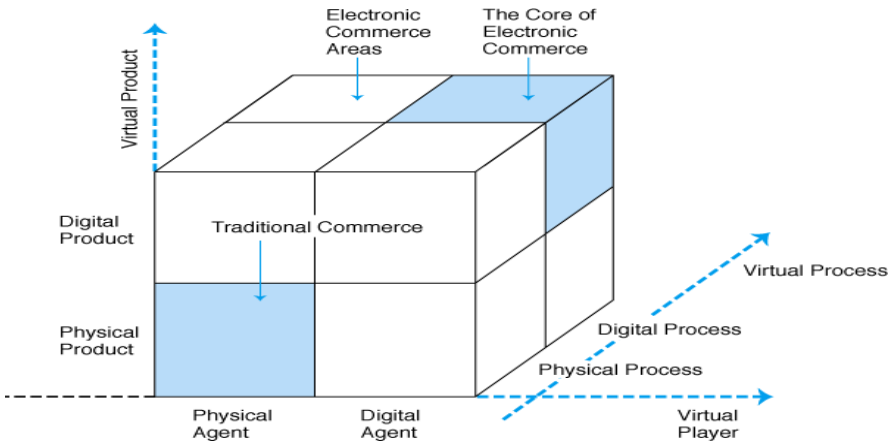
- دسترسی سریع، آسان و بدون واسطه جهت انجام فعالیتهای مختلف تجاری، با حذف دو قید زمان و مکان. [۳]
- تجارت الکترونیکی عبارت است از انجام فرآیند مبادله کالا، خدمات و اطلاعات از طریق شبکه‌های رایانه‌ای از جمله اینترنت.[۴]

- تجارت الکترونیکی شامل تمام فعالیت های بنگاهها و افراد برای انجام مبادلاتی است که تمام یا بخشی از این فعالیت‌ها از طریق شبکه‌های رایانه‌ای صورت می‌گیرد.[۷]
- تجارت الکترونیکی فعالیت‌های گوناگونی از قبیل مبادله الکترونیکی کالا و خدمات، تحویل فوری مطالب دیجیتال و انتقال الکترونیکی را شامل می‌شود.[۴]
- تجارت الکترونیک یعنی استفاده از کامپیوترهای یک یا چند شبکه برای ایجاد و انتقال اطلاعات بازرگانی که بیشتر با خرید و فروش اطلاعات، کالاها و خدمات از طریق اینترنت مرتبط هستند. [۱۳]

۳. سطوح تجارت الکترونیک

رسالت تجارت الکترونیک تنها ارتباط نیست، بلکه پی ریزی و تقویت روابط بازرگانی است. بطورکلی واژۀ تجارت الکترونیک اشاره به معاملاتی دارد که عمدۀ فرآیند آنها بدون نیاز به حضور فیزیکی طرفین آن و صرفاً از طریق شبکه‌های ارتباطی انجام می‌پذیرد .هریک از ابعاد سه گانه اصلی تجارت، شامل محصول یا خدمات مورد مبادله، فرآیند فروش و خدمات پس از فروش، می توانند از حالت فیزیکی و کاملاً ملموس تا حالت الکترونیکی و نرم افزاری (یا اصطلاحاً مجازی) تغییر نمایند. در حالتی که در تجارت سنتی هر سه عامل، فیزیکی و کاملاً قابل لمس هستند، در بالاترین سطح تجارت الکترونیک، هر سه عامل بصورت کاملا الکترونیکی مطرح می باشند. [۶]

ترکیبات گوناگون از حالت های فیزیکی و الکترونیکی سطوح مختلف تجارت الکترونیکی را شکل می دهند. چرخه تجاری از موارد یافتن کالاها و خدمات متناسب با نیاز ها و یافتن راه های مبادله مورد توافق (جستجو و مذاکره)، سفارش، حمل و پرداخت بها (اجرای توافق و پرداخت) و فعالیت های پس از فروش (مثل گارانتی و خدمات پس از فروش) تشکیل شده است. لذا تجارت الکترونیک می تواند در تمام یا بخشی از مراحل چرخه تجاری[۱] بکار گرفته شود. شکل زیر سطوح مختلف مطرح شده فوق را در فضای سه بعدی نمایش می دهد.[۱]



شکل ۱ : سطوح تجارت الکترونیک

[۱] Business Cycle

۴. تجارت الکترونیک در ایران

در جهانی شدن اقتصاد، حد و مرزهای جغرافیائی کمترین نقش را در فعالیتهای اقتصادی داراست. [۳] ولی آنچه در ایران در حال اتفاق است فقط الکترونیکی کردن تجارت سنتی است و واقعیت امر فراموش شده است. عدم درک مفاهیم کسب و کار وتجارت الکترونیک دلیل اصلی مشکل موجود در این شاخه است. بهمین لحاظ راه اندازی و گسترش تجارت الکترونیکی در کشور با موانع و چالشهایی به شرح زیر روبه رو می‌باشد :[۸]

- فقدان زمینه‌های حقوقی لازم برای استفاده از تجارت الکترونیکی از قبیل عدم مقبولیت اسناد و امضاهای الکترونیکی در قوانین و مقررات جاری کشور.
- نبود سیستم انتقال الکترونیکی وجوه و کارتهای اعتباری.
- محدودیت خطوط ارتباطی و سرعت پایین آنها در انتقال داده‌های الکترونیکی.
- نبود شبکه ارتباطی و سخت افزار و نرم‌افزار مربوط به تجارت الکترونیکی در کشور.
- عدم آگاهی و نیز اطلاع کافی موسسات بزرگ و کوچک داخلی از تجارت الکترونیکی و مزایای آن.
- هزینه اولیه نسبتا بالای استفاده از تجارت الکترونیکی و نبود انگیزه لازم برای استفاده از این روش.
- کمبود دانش و فرهنگ استفاده از تجارت الکترونیکی و شبکه اینترنت.
- عدم تامین امنیت لازم برای انجام مبادلات الکترونیکی و محرمانه ماندن اطلاعات مربوطه.

۵. مزایای تجارت الکترونیک

مطالعات و بررسی های انجام شده موید تاثیر گذاری استفاده از تجارت الکترونیک در سطح خرد و کلان اقتصادی می باشد. در سطح خرد اقتصادی، استفاده از تجارت الکترونیک، صرفه جویی در هزینه، کاهش در هزینه مبادلاتی، افزایش کارایی، تغییر فرآیندهای مدیریت و تاسیس بنگاه های اقتصادی، کاهش هزینه کاوش و جستجوی کالا، دسترسی بیشتر و راحت تر به اطلاعات، کاهش محدودیت ورود به بازار، افزایش رقابت و کاهش سود انحصاری را به دنبال خواهد داشت. در سطح کلان اقتصادی نیز مزیت هایی چون رشد بهره وری، کاهش بیکاری، رشد اقتصادی، کاهش کسری بودجه و تورم پایین در نتیجه بکارگیری تجارت الکترونیک در کشور حاصل خواهد شد. [۲]

با داشتن مزایای فوق، تجارت الکترونیک در کشورهای پیشرفته به عنوان روش قابل قبول در حال اجرا است و سالانه میلیاردها دلار تبادلات تجاری به وسیلهٔ آن انجام می شود. اما بکارگیری آن در کشورهای در حال توسعه با چالش ها و مشکلاتی همراه می باشد که این چالش ها را می توان به صورت زیر طبقه بندی نمود :

- کمبود دانش و فرهنگ جهت استفاده از تجارت الکترونیکی
- نبود زیر ساخت های حقوقی در استفاده از تجارت الکترونیک و لزوم حمایت از حقوق مصرف کنندگان
- سرعت پایین اینترنت و شبکه های ارتباطی و نیز محدودیت های استفاده از آنها
- امنیت

۶. جایگاه امنیت در تجارت الکترونیک

همانطور که ملاحظه گردید بحث امنیت به عنوان یکی از چالش های اساسی تجارت الکترونیکی مطرح است. بر اساس واژه نامه وبستر، امنیت به معنای کیفیت یا حالت امن بودن، رهایی از خطر، ترس و احساس نگرانی و تشویش می باشد، که این تعبیر در دنیای الکترونیکی نیز صادق می باشد.[۱۶]

توجه به رشد سریع و روز افزون تجارت الکترونیک و مزایای رقابتی حاصل از آن باعث گردیده تا روش های تجاری با قابلیت ها و توانایی های مناسب و قابل اطمینان ایجاد گردند. با توجه به نقش اطلاعات به عنوان کالای با ارزش در تجارت امروز، لزوم حفاظت از آن گریز ناپذیر است. با توسعه فناوری اطلاعات و استفاده از اطلاعات به عنوان یک ابزار تجاری و سرمایه سودآور، بحث امنیت اطلاعات بعد جدیدی به خود می گیرد. با توجه به تغییر ماهیت از تجارت سنتی به تجارت الکترونیک، برای حفاظت از اطلاعات، هر سازمان متناسب با سطح اطلاعات موجود در آن، نیازمند به طراحی و بکارگیری سیستم های امنیتی مختص به خود است تا بتواند از سرمایه های اطلاعاتی خود در عصر اطلاعات به نحو مطلوبی حفاظت نماید. [۱۰]

بیشتر جرائم تجاری که در اینترنت رخ می دهند تازگی چندانی ندارند، کلاهبرداری، سرقت، جعل هویت و اخاذی سال هاست که صنایع خدمات مالی را به ستوه آورده اند، اما پیشرفت فناوری، همواره باعث بوجود آمدن ابعاد جدیدی می گردد و این مسئله می تواند عمق و دامنهٔ جرائم را گسترده تر نماید. اقتصاد شبکه ای، برای ایجاد ثروت و همچنین انجام سرقت و تخریب، فرصتهای متفاوتی ایجاد می کند. در بررسی مزایا و معایب این فرآیند، سیاستگذاران و تصمیم گیران باید آگاهی خود را در مورد نقشی که امنیت الکترونیکی در تضمین داد و ستدهای قابل اطمینان تجاری بازی می کند، افزایش دهند. [۱۰]

۷. امنیت الکترونیکی در تجارت الکترونیکی

بطور کلی امنیت الکترونیکی عبارت است از هر ابزار، فن یا فرآیندی که برای حفاظت از سرمایه های اطلاعاتی یک سیستم مورد استفاده قرار می گیرد و ارزش یک شبکه را زیاد می کند. امنیت الکترونیکی از زیرساخت های نرم و سخت تشکیل شده است. زیرساخت های نرم عبارتند از سیاست ها، فرآیندها، پروتکل ها و راهبردهایی که از مورد سوء استفاده قرار گرفتن سیستم و داده ها جلوگیری می کنند. زیرساخت های سخت نیز متشکل از نرم افزار و سخت افزار مورد نیاز برای حفاظت از سیستم و داده ها در مقابل تهدیدات امنیتی داخلی و خارجی سازمان می باشد. [۲]

هدف از امنیت در تجارت الکترونیک ، استفاده از مجموعه سیاست ها، راهکارها، ابزار، سخت افزارها و نرم افزارها، برای فراهم آوردن محیطی عاری از تهدید در تولید، پالایش، انتقال و توزیع اطلاعات است. فراهم آوردن چنین محیطی مستلزم انجام مواردی است که از آن ها به نیازهای امنیت الکترونیکی یاد می شود. [۹]

در تجارت الکترونیکی از سرویس های ارتباطی جهت ارسال و دریافت پیام بین فرستنده و گیرنده استفاده می گردد. اطلاعات طبق قاعده و ضوابط خاصی رد و بدل شده و در عین حال با استفاده از سرویسهای امنیتی از مشکلاتی از قبیل افشای محتوای پیام، ارسال پیام توسط فرد غیرمجاز و غیره جلوگیری می شود. بکارگیری سیستم های امنیتی کارآمد درکنار ابزارهای امنیتی

جهت احراز هویت فرستنده، تمامیت و محرمانگی اطلاعات و عدم انکار فرستنده و گیرنده به عنوان ملزومات سیستم تجارت الکترونیکی مطرح هستند، که برحسب نیاز روی اطلاعات اعمال می گردند تا امنیت فراهم آید.[۹]

در واقع تهدیدهای امنیتی زیر در تجارت از طریق اینترنت وجود دارد : [۴]

۱- تقلید یا کلاهبرداری[۱] : ایجاد سایتهای تقلبی به تقلید از بنگاههای واقعی
۲- آشکارسازی غیرمجاز[۲] : دسترسی به اطلاعات خصوصی مشتریان توسط هکرها (سرقت اینترنتی)
۳- افعال غیر مجاز[۳] : تغییر یا تخریب یک سایت توسط مشتریان یا رقبا به منظور اخلال در سرویس دهی
۴- تغییردادن داده ها[۴] : تغییر در اطلاعات ارسالی (نام کاربر، شماره کارت،. . .) بصورت سهوی یا عمدی

بهمین لحاظ افراد متخصص در زمینه تجارت الکترونیک، امنیت را در حفظ و بقاء چهار اصل زیر می دانند[۱۱]:

۱- محرمانگی[۵] : محرمانگی اطلاعات یعنی حفاظت از اطلاعات در مقابل دسترسی و استفاده غیر مجاز، تا داده های محرمانه تنها توسط افراد مجاز قابل دسترسی باشند.
۲- تمامیت[۶] : یک سیستم از عناصری متشکل است که در کنار هم برای رسیدن به هدفی یکسان همکاری دارند. حفظ تمامیت به معنای پیشگیری از بروز مشکل در این همکاری و پیوسته نگه داشتن عناصر یک سیستم می باشد. یعنی داده ها نمی توانند توسط افراد غیر مجاز ساخته شده، تغییر یافته و یا حذف گردند. تمامیت همچنین یکپارچگی داده ها که در بخش های مختلف پایگاه داده ذخیره شده اند را تحت شعاع قرار می دهد.
۳- دسترسی پذیری[۷] : دسترسی پذیری به این معنا است که داده ها، پایگاه داده و سیستم های حفاظت امنیت، در زمان نیاز به اطلاعات در دسترس باشند. اطلاعات بایستی به هنگام نیاز، توسط افراد مجاز قابل دسترس باشد.
۴- عدم انکار[۸] : به این معنی است که هنگام انجام کاری و یا دریافت اطلاعات یا سرویسی، شخص انجام دهنده یا گیرنده، نتوانند آن را انکار کند.

۸. پیش‌نیازهای استقرار و نهادینه شدن امنیت در تجارت الکترونیک

با توجه به مفهوم تجارت الکترونیک می‌توانیم موارد زیر را بعنوان مهمترین پیش نیازهای استقرار امنیت در تجارت الکترونیک نام ببریم :[۱۰]

- ایجاد نظام حقوقی اطلاع‌رسانی (ضمانت اجرایی) و تعریف حقوق مالکیت معنوی (قانون کپی رایت)

---

[1] Spoofing
[2] Unauthorized Disclosure
[3] Actions Unauthorized
[4] Data Alteration
[۵] Confidentially
[۶] Integrity
[۷] Availability
[۸] Non- Repudiation

- تأمین امنیت اطلاعات و سامانه های مدیریت امنیت اطلاعات
- تعریف حقوق فردی در ارتباط با محرمانه بودن اطلاعات شخصی
- راه‌اندازی خطوط ارتباطی سریع ، مطمئن و امن
- پذیرش اسناد الکترونیکی توسط قوهٔ قضائیه با اعتباری برابر با اسناد کاغذی
- معرفی مراجع صدور گواهی امضاء دیجیتالی در کشور و تأیید احراز هویت خریدار و فروشنده توسط این مراجع.

البته چنانچه مشخص است این موانع کاملاً از یکدیگر تفکیک شده نیستند، بلکه دارای همپوشانی با یکدیگر می‌باشند ولی در جمع‌بندی نتایج این تحقیق می‌توان چنین گفت‌که بطور کلی مشکلات عمدهٔ محدودکنندهٔ رشد تجارت الکترونیک در کشورهای در حال توسعه عبارتند از عدم امنیت اطلاعات، نبود نظام بانکی الکترونیکی قابل اعتماد و دارای قابلیتهای موردنیاز و فقدان پوشش‌های قانونی در ارتباط با معاملات تجاری و مالی که در جهت تسریع رشد آن باید نسبت به رفع این موانع اقدام شود. با وجود افزایش سطح آگاهی از امنیت الکترونیکی، برخی از سازمان ها همچنان در مدیریت این امنیت با مشکل و برخی اشتباهات روبرو هستند. موارد زیر را می توان به عنوان چالش های مهم امنیتی در سازمان ها نام برد[۶]:

- جدی نگرفتن اهمیت برخی اطلاعات : برخی از سازمان ها از اهمیت اطلاعات و فایلهای خود بی خبرند.
- تعریف غیر مشخص از حد و مرزهای امنیتی : بسیاری از سازمانها تنها به ایمن سازی شبکه کامپیوتری داخلی خود پرداخته و فراموش می کنند که کارمندان بخشهای گوناگون نیز باید اقدامات امنیتی را انجام دهند.
- واکنش پذیری در مدیریت امنیت : برخی از سازمانها به جای پیشگیری معمولاً زمانی به کنترل مسائل امنیتی می پردازند که مشکلی روی داده باشد. در نتیجه مسئولین این سازمانها، معمولاً پس از رویداد یک حادثه در پی مدیریت مسائل امنیتی بر می آیند.
- عدم به روز رسانی اقدامات امنیتی : سازمانها به ندرت اقدامات امنیتی خود را طبق تغییرات پیش آمده به روز می کنند. آنها همچنین در بهنگام رسانی اطلاعات کارمندان خود در زمینه اقدامات امنیتی نیز ضعیف عمل می کنند.

بهمین لحاظ راه کارهای امنیتی زیر در تجارت الکترونیک معرفی می گردند: فناوری های امنیت اطلاعات کنشی یا کنش گرایانه و فناوری های امنیت اطلاعات واکنشی.

۸,۱. امنیت اطلاعات کنش گرایانه[۱] یا کنشی

این فناوری شامل انجام عملیات پیشگیرانه قبل از وقوع یک مشکل خاص امنیتی است و فناوری های مربوط آن به شرح زیر می باشد [۴و۱۴]

۱. رمزنگاری[۲] : نوعی نوشتن پنهان، و علم حفاظت، اعتمادپذیری و تأمین تمامیت داده ها است، که شامل سه مرحله رمزگذاری[۳]، رمزگشایی[۱] و تحلیل رمز[۲] است. کدگذاری واژه ها به صورت پنهان را رمزگذاری گویند و بازیابی متن آشکار از متن رمزی را رمز گشایی می نامند.

---

[۱] Proactive
[۲] Cryptography
[۳] Encryption

۲. امضاهای رقومی[۳] : معادل امضای دست نوشت بوده و همان هدف را دارد، در واقع نشانه منحصر به فرد یک نفر بوده و بنابراین نباید براحتی قابل جعل باشد.
۳. شبکه های مجازی خصوصی[۴] : فناوری شبکه های مجازی خصوصی، عبور و مرور شبکه را رمزگذاری میکند. این فناوری برای تضمین صحت و امنیت داده ها، به رمزنگاری وابسته است. این شبکه، برای انتقال داده های حساس از جمله اطلاعات تجاری الکترونیکی از اینترنت به عنوان رسانه انتقال بهره می گیرد.
۴. نرم افزارهای آسیب نما[۵] : برنامه هایی برای بررسی نقاط ضعف یک شبکه یا سیستم یا سایت هستند. به این معنا که میزبان های روی شبکه در فواصل نامنظم پویش می شوند، به محض خاتمه یافتن بررسی یک میزبان ، از داده های آن نمونه برداری می شود و در واقع یک عکس فوری[۶] گرفته می شود.
۵. پویشگرهای ضد ویروس[۷] : برنامه های نرم افزاری هستند که برای بررسی و حذف ویروس های رایانه ای طراحی شده اند.
۶. پروتکل های امنیتی[۸] : شیوه های استاندارد که تبادل اطلاعات را میان سیستم ها، کنترل و هدایت می کنند.
۷. سخت افزارهای امنیتی[۹] : ابزارهای فیزیکی مانند امنیت سرورها، امنیت کابل ها و غیره که کاربرد امنیتی دارند.
۸. جعبه های توسعه نرم افزار امنیتی[۱۰] SDKs : ابزار های برنامه نویسی مانند java security manager و Microsoft. net SDKs که در ایجاد برنامه های امنیتی و ساختن برنامه های کاربردی امنیتی کاربرد دارند.

۸,۲. امنیت اطلاعات واکنشی[۱۱]

این فناوری ها شامل انجام عکس العمل لازم پس از وقوع یک مشکل خاص امنیتی است، که فناوری های مربوط به آن به شرح زیر می باشد : [۴و۱۴]

۱. دیوار آتش[۱۲] : اولین خط دفاعی برای دفع مزاحم می باشد. دیوار آتش یک فیلتر بین سازمان داخلی و اینترنت نصب می شود و هدف آن جلوگیری از ارتباطات غیر مجاز در درون یا بیرون شبکه داخلی میزبان است.
۲. کنترل دسترسی[۱] : مجموعه سیاست های مربوط به دادن اجازه یا عدم اجازه برای دسترسی یک کاربر خاص به قسمت های مختلف اطلاق می شود.

---

۱ Decryption
۲ Cryptanalysis
۳ Digital signatures
۴ Virtual private networks
۵ Scanners Vulnerability
۶ Snapshot
۷ Anti- virus Scanner
۸ Security protocols
۹ Security hardware
۱۰ Security software development kits
۱۱ Reactive
۱۲ Firewall

۳. کلمات عبور[۲] : کلمه یا عبارتی است که فرد برای دریافت مجوز دسترسی به اطلاعات باید وارد نماید.

۴. بیومتریک[۳] : علم سنجش و تحلیل داده های زیستی است. در امنیت اطلاعات از تحلیل ویژگی های بدن انسان (مانند اثر انگشت، قرنیه و شبکیه چشم، الگوهای صدا، الگوهای چهره و اندازه دست) به منظور تعیین اعتبار استفاده می شود.

۵. نظام های آشکار ساز نفوذی[۴] : یک سیستم دفاعی است که فعالیت های مخاطره آمیز را در یک شبکه تشخیص می دهد. از ویژگی های مهم آن توانایی در تامین نمایی از فعالیت های غیر عادی و اعلام هشدار به مدیران و مسدود نمودن ارتباطات مشکوک است.

۶. واقعه نگاری[۵] : به ثبت ضابطه مند رویدادهای مشخص به ترتیب وقوع آن ها برای فراهم کردن امکان تعقیب و پیگیری داده ها در تحلیل های آتی اطلاق می شود.

۷. دسترسی از را دور[۶] : دسترسی به یک سیستم یا برنامه بدون نیاز به حضور فیزیکی در محل می باشد که خطر جعل هویت در آن ها بیشتر است، به همین دلیل معمولاً کنترل شده نیستند.

۹. نتیجه‌گیری

فناوری های نوین، در همان حال که دقت و سرعت پردازش را افزایش چشمگیری بخشیده اند، باید پاسخگوی مسائل و خطراتی باشند که در صورت پذیرش آنها متوجه سازمان ها و افراد است. گسترش روز افزون تجارت الکترونیکی، نیازمند بستری ایمن جهت مخابره و دریافت اسناد بازرگانی و اطلاعات است. جرایم الکترونیکی و عدم وجود امنیت کامل در تجارت الکترونیکی، هم چنان به عنوان یکی از مشکلات و چالش های عمده به حساب می آید. با توجه به اهمیت امنیت و حفظ اطلاعات در سازمان ها، بکارگیری سیستم های امنیتی موثر و کارامد، بسیار ضروری و حیاتی بوده و اعمال چنین سیستم هایی برای هر سازمان بسته به سطح و ارزش اطلاعات سازمان مذکور، گستردگی متنوعی خواهد داشت.

همواره با مساله امنیتی، به عنوان یک مشکل فناوری اطلاعات و نه یک مساله همه جانبه سازمانی برخورد می شود. شرکتها باید مرتباً نواحی آسیب پذیر و خطرات احتمالی وب سایتهای خود را مورد بررسی قرار دهند. کارمندان و سایر کاربران نهایی نیز باید به یکسان بودن اهمیت اطلاعات و امنیت فیزیکی پی برده و عکس العمل مناسب از خود نشان دهند. همچنین مدیران ارشد و مسئولین اجرایی سازمانها در تبیین جایگاه امنیت نقش مهمی اشته و باید در ایجاد سیاست گذاری های امنیتی و حمایت از قوانین وضع شده درون سازمان، بسیار تلاش کنند. مسلماً ساختار مستحکم و امنیت برخی از سازمانها که در درون، از امنیت محکم و جدی برخوردارند، حاصل همین تلاشهای همه جانبه و شناسایی خطرات احتمالی بوده است.

۱۰. پیشنهادات و راهکارها :

---

[۱] Access control

[۲] Passwords

[۳] Biometrics

[۴] Intrusion detection systems

[۵] logging

[۶] Remote accessing

با عنایت به موارد فوق زیرساختهای لازم برای گسترش تجارت الکترونیکی در ایران را می‌توان به شرح زیر بیان نمود :

۱- زیر ساختهای فنی، ارتباطی و مخابراتی از الزامات گسترش تجارت الکترونیک در ایران است. چون برای تحقق این امر دسترسی به رایانه، اینترنت، تلفن همراه و تلفن ثابت باید بسیار وسیع باشد. یکی از موانع گسترش تجارت الکترونیکی در ایران ضعف زیرساختهای فنی، ارتباطی و مخابراتی است. البته ظرف سالهای اخیر فعالیتهای بسیار خوبی در وزارت I CT صورت گرفته که اگر به این اهداف دسترسی پیدا کنیم می‌توانیم بگوییم موانع در این زیر ساختها برداشته خواهد شد.

۲- زیرساختهای حقوقی و قانونی که شامل قانون تجارت الکترونیکی، قانون امضای دیجیتال، جرایم الکترونیکی، قانون مالکیت معنوی و قانون نقل و انتقال الکترونیکی وجوه است که ما فقط دارای قانون تجارت الکترونیکی هستیم که در دی ماه ۱۳۸۲ به تصویب رسید.

۳- زیرساختهای سرمایه انسانی که همان نیروی انسانی متخصص است. البته ما در زمینه سرمایه انسانی مشکل آنچنانی نداریم منتهی باید در بحث تحقیق و توسعه دقت کنیم، چون بنگاههایی می‌توانند در دنیای تجارت الکترونیکی فعالیت کنند که به صورت مرتب نوآوری داشته باشند.

۴- چهارمین بستر برای تجارت الکترونیکی بسترهای نهادی و سازمانی هستند. نهادهایی که با این موضوع سر و کار دارند باید در خیلی از زمینه ها تحول ایجاد کنند از جمله تحول در فعالیتهای غیر شفاف و ایجاد یک مهندسی مجدد در فرآیندها.

کشور ما در زیرساختهای اول و دوم دارای مشکل است ولی فعالیتهای ما به گونه ای است که مشکلات در این زیرساختها برطرف خواهد شد که یکی از موارد مهم در هر دو ساختار مباحث مربوط به بانکداری‌الکترونیک (سیستمهای پرداخت الکترونیک، انتقال وجوه الکترونیک و کارتهای بانکی) می‌باشد، در زمینه زیر ساخت سوم مشکل خاصی نداریم ولی مشکل اصلی ایران در زیر ساخت چهارم می‌باشد که باید در این زمینه کار فرهنگی با همکاری تمام دستگاهها و نهادهای ذیربط صورت بگیرد.

مراجع

[۱] بختیاری، شهرام، **" امنیت در تجارت الکترونیکی"**،مجموعه مقالات همایش ملی تجارت الکترونیکی ، صفحه ۲۲۳-۲۳۶.

[۲] سادوسکای ، جورج . دمپزی ، جیمز . گرین برگ ، آلن . مک ، باربارا . شوراتز ، آلن ، **"راهنمای امنیت فناوری اطلاعات"** ، ترجمه ، میردامادی ، مهدی ، شجاعی ، زهرا ، صمدی ، محمد جواد ، دبیر خانه شورای عالی اطلاع رسانی ، تیر ماه ۱۳۸۴.

[۳] قاسم زاده، فریدون،**" تجارت الکترونیک ابزاری برای کاهش شکاف دیجیتالی "**، نشریه عصر ارتباط، شماره۲۰ ، ۱۳۸۲ .

[۴] قاسمی، کبری. مختاری ، وحید . امینی ، منصور ، **"امنیت و تجارت الکترونیکی"**، چهارمین همایش ملی تجارت الکترونیکی ، تهران ۳ و ۴ آذر ماه ۱۳۸۶.

[۵] گرامی، محسن ، **" تجارت الکترونیک "** ، انتشارات سیمای دانش ، چاپ اول ، ۱۳۸۲.

[۶] محمدیانی ،حسین ، **" لایه های مدیریتی پاشنه آشیل تجارت الکترونیکی "**. نشریه عصر ارتباط، شماره۲۰ ، ۱۳۸۲.

[۷] مورل جی،شیلدز، **"تجارت الکترونیک و برنامه ریزی منابع سازمان"**، مترجم پارسائیان، علی، حنفی زاده ،پیام، انتشارات ترمه.

[۸] ویسی ، همت و موحدی ، مسعود ،**" موانع و مشکلات فرهنگی استقرار تجارت الکترونیکی در ایران "**. انتشارات جهاد دانشگاهی،۱۳۸۰.

[9] C.lves, "E-Business and E-Commerce", Managing Information Journal, Vol5, 2001.

[10] D.Chaffcy,"e-Business and e-Commerce Management", Prentice-Hall, 2002.

[11] Kesh , framework for analyzing e-commerce security, Information Management & Computer Security. Vol.10, Iss.4, 2002.

[12] M. Greenstein and M. Vasarhelyi, Electronic Commerce: Security, Risk Management, and Control with Power Web passcode card (E-Commerce), 2nd Edition, McGraw-Hill , 2001.

[13] OECD, "The Economic and Social Impact of Electronic Commerce: Preliminary Findings and Research Agenda", Paris, Oct ۲۰۰۷.

[14] S. Bosworth and M. E. Kabay, Computer Security Handbook, John Wiley & Sons, 2002.

[15] UNCTAD "Electronic Commerce and Development", Internet version, ۲۰۱۰

[16] Webster Dictionary, www.merriam-webster.com