چهارمین
همایش ملی تجارت الکترونیکی
The 4th e-Commerce
CONFERENCE
تهران- ۳ و ۴ آذرماه ۱۳۸۶

راهکارهای کلان امنیت در تجارت الکترونیک

مهدی براتی پور، مدیر دپارتمان امنیت شبکه موسسه تبیان

چکیده:

در این مقاله سعی بر بررسی کلان راهکارهای امنیتی در بحث تجارت الکترونیک از طریق دسته بندی عوامل تجارت الکترونیک در چهار حوزه تولید، ارائه، انتقال و دریافت و همچنین دسته بندی منابع خطرها در سه حوزه ضعف تکنولوژی، ضعف دانش افراد استفاده کننده و اشتباهات انسانی می باشد.

واژه های کلیدی: امنیت، تجارت الکترونیک، تولید، ارائه، انتقال، دریافت

مقدمه

در دنیای رو به رشد و بهم متصل الکترونیکی امروز زندگی انسان در دست بسته[1] هایی می باشد که با سرعتی در حدود نور در حرکت می باشند و حاصل انتقال این بسته ها همان دریافت و ارسال اطلاعات ما از فایلهای صوتی و تصویری تا پیغام و کتاب از کنترل حساب بانکی تا خرید و فروش کالا می باشد.

این انتقال ها که زندگی الکترونیکی ما را شکل می دهند به بخش های مختلفی تقسیم می شوند به طور مثال به انجام کارهای بانکی به صورت الکترونیکی، بانکداری اینترنتی یا الکترونیکی گفته می شود و بهمین شکل به داد و ستد الکترونیکی نیز تجارت الکترونیک می گویند که این داد و ستد می تواند شامل خرید و فروش کالا و یا سرویسی خاص باشد.

از آنجاییکه در سیستم داد و ستد سنتی نیز بدلیل وجود برخی از تهدیدات گاهی افراد و یا دولت متضرر می شدند در سیستم پیشرفته الکترونیکی امروز نیز نوع پیشرفته و الکترونیکی این تهدیدات موجود می باشند.

برای کاهش این تهدیدات در داد و ستد مرسوم راهکارهایی وجود دارند که تقریباً همه کم و بیش با آنها آشنایی دارند از قبیل نصب دوربین های مدار بسته، قرار دادن برچسب های مغناطیسی و ایجاد خروجی های کنترل کننده، بررسی صحت چک های دریافتی و .... این قبیل راهکارهای نجات دهنده که عمدتاً با مسائل فیزیکی مرتبط هستند می توانند سطح خوبی از امنیت را فراهم بیاورند. در سیستم الکترونیکی نیز راهکارهایی به همین شکل اما گسترده تر موجود می باشند بدین صورت که هم امنیت فیزیکی مطرح می باشد و هم امنیت اطلاعات.

تعریف امنیت[2]

بر اساس واژه نامه Webster امنیت به معنای کیفیت یا حالت امن بودن، رهایی از خطر، ترس و احساس نگرانی و تشویش می باشد.[1] این تعبیر در دنیای الکترونیکی نیز صادق می باشد اما افراد متخصص این زمینه امنیت را در حفظ و بقاء 4 اصل می دانند:

1. محرمانگی[3]: اطلاعات فقط و فقط بایستی توسط افراد مجاز قابل دسترس باشد.
2. تمامیت[4]: 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.

---

[۱] Packet

[۲] Security

[۳] Confidentiality

[۴] Integrity

3. دسترس پذیری[5]: اطلاعات بایستی به هنگام نیاز توسط افراد مجاز قابل دسترس باشد.
4. عدم انکار[6]: به هنگام انجام کاری و یا دریافت اطلاعات یا سرویسی، شخص انجام دهنده یا گیرنده نتواند آن را انکار کند.[2]

تجارت الکترونیک

همانطور که ذکر شد، هرگونه داد و ستد الکترونیکی تحت عنوان تجارت الکترونیک بیان می شود که خود می تواند حالت های مختلفی را دربر داشته باشد. در اینجا از تعریف و یا بیان حالت های مختلف آن می گذریم و به بررسی عوامل دخیل در این کار می پردازیم در بحث تجارت الکترونیک عواملی از قبیل برنامه های تحت وب[7]، سرویس دهنده، بستر ارتباطی و دریافت کننده که عمدتاً مشتری می باشد بایستی در کنار هم قرار گیرند تا یک تجارت الکترونیک شکل گیرد و اگر آن را به صورت یک سیستم ترسیم کنیم می توانیم این عوامل را در 4 مفهوم کلی "تولید، ارائه، انتقال و دریافت" سرویس یا کالا داشته باشیم. برای شفاف شدن هرچه بیشتر این موضوع به توضیح هر کدام می پردازیم:

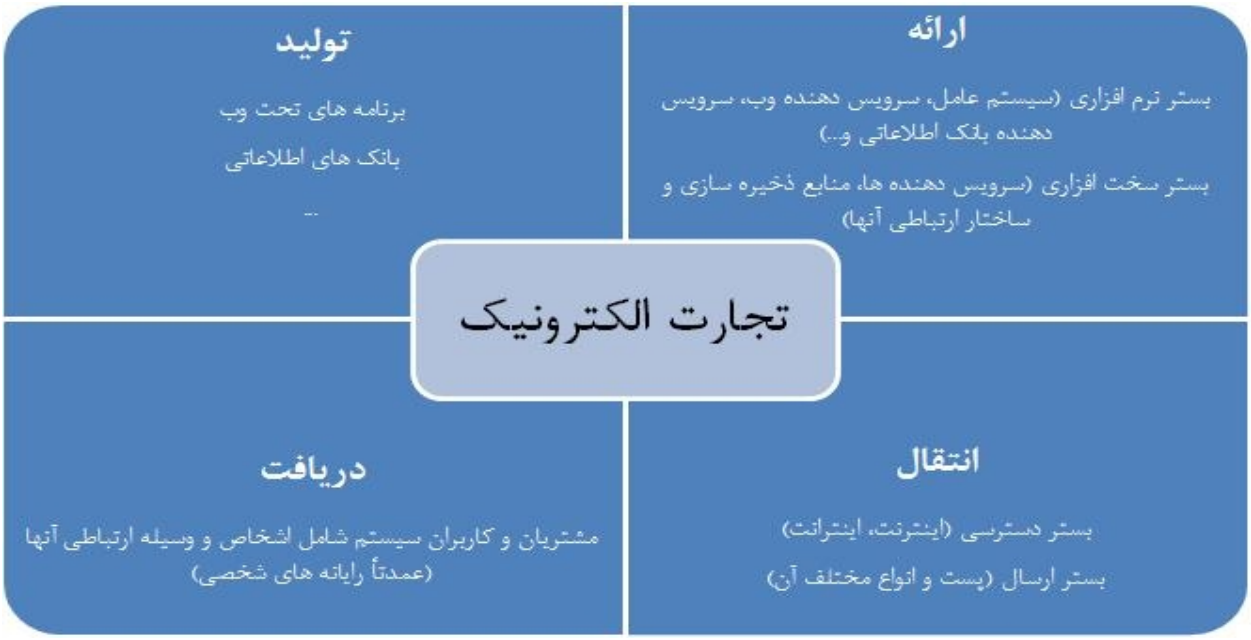
تجارت الکترونیک که در اینجا بیشتر بحث پیرامون بررسی این امر در دنیای اینترنت می باشد به منظور شکل گیری و سرویس دهی، نیازمند محیطی است که از طریق آن افراد مختلف بتوانند داد و ستد خود را انجام دهند این محیط که در اینجا همان برنامه های تحت وب هستند خود نیازمند بستری جهت قرارگیری می باشد، حال نیاز به ارائه سرویس مطرح می گردد که خود در بر گیرنده مباحث نرم افزاری چون سیستم عامل، سرویس دهنده وب و مباحث سخت افزاری چون سرویس دهندگان و ساختار آنها می باشد اما هنوز این سیستم کامل نیست بحث تولید و ارائه مهیا شده اند اما چگونگی ارتباط مشتریان با سیستم مشخص نیست، بستر دسترسی که بنابر مطالب مذکور، اینترنت می باشد در مفهوم انتقال مورد بررسی قرار می گیرد. وجود مشتریان هم که لازمه زنده نگه داشتن این سیستم می باشد در مفهوم دریافت جای داده شده است.

---

[۵] Availability

[۶] Non-Repudiation

[۷] Web Applications



حوزه های در برگیرنده عوامل تجارت الکترونیک

حال که تجارت الکترونیک به صورت یک سیستم در نظر گرفته شده و از مفاهیمی چون تولید، ارائه، انتقال و دریافت به عنوان قالب هایی یاد شد که هرکدام در برگیرنده عوامل این سیستم هستند پس می توانیم نتیجه بگیریم که شکل گیری و پیشرفت این سیستم در گرو همکاری درست و انسجام عوامل این مفاهیم می باشد.

امنیت در تجارت الکترونیک

در بررسی امنیت هر سیستمی بنا بر اصول مشخص شده در استاندارد ISO27001 ابتدا بایستی دارایی های سیستم مشخص و ارزش گذاری شوند پس از آن خطرات متوجه هر دارایی مورد بررسی قرار می گیرد و مطابق با هر خطر راهکاری اندیشیده می شود.[3] بدلیل گستردگی این بحث ما امنیت را در مفاهیم در نظر می گیریم پس بنابراین به منظور ارائه راهکارهای امنیتی بایستی خطراتی که هر کدام از این مفاهیم را تهدید می کند را مورد بررسی قرار دهیم:

- **تولید**

با توجه به دسته بندی انجام شده در مفهوم تولید بیشتر با یکسری از برنامه های تحت وب و بانکهای اطلاعات[8] در ارتباط هستیم. فارغ از این موضوع که این برنامه ها توسط تیمی مشخص به منظور انجام یک داد و ستد اینترنتی به وجود آمده اند و یا به صورت آماده در قالب بسته های نرم افزاری تهیه شده اند تهدیداتی متوجه آنها می باشد. این تهدیدات عمدتاً به منظور به دست آوردن اطلاعاتی محرمانه و یا ایجاد تغییری در سیستم، به منظور جعل هویت، دستکاری مبلغ کل در راستای کاهش آن و یا حتی تغییری در صفحه اصلی به منظور تخریب اعتبار آن مجموعه می باشد. به منظور بررسی اجرایی در ادامه به توضیح چند نمونه از تهدیداتی که می توانند متوجه عوامل مفهوم تولید باشد می پردازیم:

SQL Injection: این روش به وارد کردن دستورها و عباراتی به زبان قابل فهم توسط SQL در قسمتهایی از یک وب سایت که می توانند مقادیری را به صورت ورودی دریافت کنند (مانند فیلدهای نام کاربری و رمز عبور) اطلاق می شود. بنابراین هکر می تواند یک دستور را بر روی سرور بانک اطلاعات اجرا کند. که حاصل اجرای این دستور می تواند به دست آوردن اطلاعات کاربران، اطلاعات کارت های اعتباری، جزییات مبادلات انجام شده و... باشد.

سایتهای Guess.com و PetCo.com که در زمینه ارائه سرویس و محصولات به صورت اینترنتی فعالیت دارند قربانی این تهدید بوده اند که به دنبال آن اطلاعات حساس و مهم بسیاری از کاربرانشان به دست یک هکر 20 ساله ساکن کالیفرنیا افتاد.[4,5]

Cross-Site Scripting (XSS): عبارت است از فرستادن Script در فیلد های ورودی به منظور به دست آوردن اطلاعات مهم و یا ایجاد تغییر در کدهای HTML که عمدتاً این روش به دو صورت ذخیره شده[9] و منعکس[10] تقسیم می شود.

در روش ذخیره شده، Scriptهای هکر به صورت دائمی در سرویس دهنده مورد نظر قرار می گیرند مانند بانک اطلاعاتی، صفحات پیغام و یا نظرات، و هنگامی که کاربری درخواستی را به این قسمت ها ارسال نماید Script هکر بر روی سیستم کاربر اجرا می شود.

در روش منعکس، هکر ابتدا Script مورد نظر خود را به شکلی با قسمت آسیب پذیر سایت مورد نظربرای کاربر می فرستد که کاربر با کلیک بر روی آن URL در واقع Script هکر را اجرا کرده است.

---

[8] Database

[9] Stored

[10] Reflected

در هر دو روش حاصل اجرا شدن Script می تواند منجر به این شود که هکر بتواند اطلاعات نشست[11] احراز هویت شده[12] کاربر با وب سایت مورد نظر را به دست آورد و بتواند خود از آن استفاده کند در واقع هویت خود را جعل و خود را به عنوان کاربر قربانی ابراز نماید.

برای نشان دادن درجه خطر این تهدید می توانیم مثال واقعی زیر را ذکر کنیم:

در روز 16 ماه جون سال 2006 سایت Netcraft اعلام کرد که به علت ضعف امنیتی (XSS Vulnerability) موجود در سایت PayPal هکرها توانستند اطلاعات شخصی و کارت های اعتباری اعضاء این سایت را به دست آورند.[6]

Price Manipulation: همانطور که اسم این روش نشان می دهد عبارت است از دستکاری قیمت، به این صورت که به هنگام محاسبه قیمت کل به علت ذخیره سازی یکسری از اطلاعات خرید بر روی سیستم مشتری، هکر با استفاده از یک برنامه که بتواند ارتباطات خود و سرویس دهنده را پروکسی کند (مانند برنامه Achilles) می تواند اطلاعات مهمی از جمله قیمت را تغییر دهد که اگر کنترل های لازم در سمت برنامه سرویس دهنده وجود نداشته باشد ضرر مالی این کار متوجه شرکت سرویس دهنده می شود.

یک نمونه از این مشکل که باعث متضرر شدن شرکت های سرویس دهنده شده است ضعف موجود در برنامه "3D3 ShopFactory Shopping Cart" بوده است. شرکت هایی که برای انجام محاسبات مالی تجارت اینترنتی خود از این برنامه استفاده می کردند به علت اینکه این برنامه قیمت نهایی را در یک Cookie سمت کاربر ذخیره سازی می کرده و امکان تغییر قیمت نهایی توسط هکرها وجود داشته، متضرر شده اند.[7]

Buffer Overflow: این ضعف هم که مربوط به اشتباه در برنامه نویسی می باشد نیز می تواند به عنوان تهدیدی برای تجارت الکترونیک به حساب آید. اگر بخواهیم این تهدید را مورد بررسی قرار دهیم می توانیم خطر آن را به دو قسمت تقسیم کنیم: یکی افشاء یکسری اطلاعات از طریق پیغام های خطایی است که سیستم به علت سریز شدن بافر بر می گرداند که می تواند اطلاعات بسیار خوبی را در اختیار هکر قرار دهد و از آنجایی که براساس اصول و مراتب هک کسب اطلاعات از نخستین گامها می باشد پس این امر می تواند در این مرحله کمک خوبی برای هکر باشد و دوم اینکه در برخی از شرایط هکر قادر است با استفاده از این ضعف دستوری را بر روی سرویس دهنده اجرا کند.

به عنوان مثالی از این ضعف می توان برنامه "PDGSoft Shopping Cart"، که یکی از برنامه های انجام محاسبات خرید می باشد را نام برد. ضعف موجود در این برنامه امکان اجرای دستورات دلخواه را به هکر می داد.[8]

---

[11] Session

[12] Authenticated

Password guessing: به دست آوردن غیر مجاز رمز عبور افراد اگرچه یک خطر بسیار کلی می باشد اما مصداق های بسیاری از آن در تجارت الکترونیک، آنجا که احتیاج به احراز هویت[13] وجود دارد دیده می شود. این روش خود به دو قسمت حمله های واژه نامه ای[14] و حمله های مبتنی بر آزمایش تمامی عبارات ممکن[15] تقسیم می شود. در روش واژه نامه ای هکر لیستی از رمزعبورهای متداول (مانند "123456"، "admin"، "test"،...) را در فایلی قرار می دهد و سپس با استفاده از یک برنامه به بررسی خودکار آن رمزعبورها به منظور یافتن رمزعبور صحیح می پردازد. در روش ورود به زور هکر با استفاده از برنامه هایی که خاص این کار می باشند شروع به تست رمزعبورهای مختلفی می کند که بر اساس قوانین از پیش تعریف شده ساخته می شوند به عنوان مثال تمامی رمزعبورهایی که از 1 تا 10 حرف می باشند و فقط شامل اعداد هستند.

این روش در سایتهایی چون www.123greetings.com و www.register.com با موفقیت انجام شده است.[9]

- **ارائه**

عواملی که در مفهوم ارائه نقش دارند عمدتاً بسترهایی هستند که عوامل مفهوم تولید به منظور فعالیت بر روی آن سوار می شوند.

سیستم عامل، سرویس دهنده وب، سرویس دهنده بانک اطلاعاتی، سخت افزارهای مورد استفاده و... از جمله عواملی هستند که می توانیم در این مفهوم نام ببریم.

بیشتر تهدید هایی که عوامل ارائه را در معرض خطر قرار می دهد مربوط به ضعف تکنولوژی می باشد و موارد دیگر در جایگاه های بعدی قرار می گیرند. از جمله تهدیدهای این دسته از عوامل می توان چند نمونه زیر را نام برد:

کدهای مخرب[16] (Worm, Virus,...): این دسته از تهدیدها که می توانند باعث از کار افتادن سیستم شوند از این جهت که در روند عادی سرویس دهی ایجاد اختلال کرده اند و در نتیجه دسترس پذیری مختل شده است به عنوان یکی از مهمترین تهدیدهای سیستم عامل به حساب می آیند.

---

[۱۳] Authentication

[۱۴] Dictionary Attack

[۱۵] Brute Force Attack

[۱۶] Malicious Code

DoS (Denial of Service): این دسته از حملات تنها هدفشان از کار انداختن سرویس دهنده می باشد که می تواند هم به علت وجود یک ضعف در سیستم باشد و یا به علت حجم بالایی از تقاضا که می تواند منجر به پر شدن ظرفیت منابع سیستمی از قبیل حافظه، پردازشگر و یا پهنای باند شود.

به عنوان مثالی برای این دسته از حملات اینترنتی در زمینه تجارت الکترونیک می توان به از کار افتادن سرویس دهی دو شرکت Authorize-it و 2CheckOut اشاره کرد.[10]

آسیب پذیری[17] **سرویس دهنده**: از جمله بزرگترین معضلات تکنولوژی وجود ضعف های امنیتی می باشد. آسیب پذیری از طریق این ضعفها از چند جهت قابل بررسی می باشد: یکی از این جهت که معمولاً این ضعفها اول توسط تیم های هکری کشف می شوند و در جهت کارهای خرابکارانه مورد استفاده قرار می گیرند و تا زمانی که بوجود آورنده آن تکنولوژی یا سرویس دهنده بسته ای در جهت رفع آن ضعف ارائه ندهد این خطر همواره تمامی استفاده کنندگان را مورد تهدید قرار می دهد.

دوم اینکه در برخی از موارد علیرغم انتشار بسته های امنیتی ممکن است که یکسری از استفاده کنندگان آنها رایا بعلت سهل انگاری و یا به علت عدم آگاهی در سرویس دهنده و یا سیستم عامل اعمال نکنند و همواره در معرض خطر باقی بمانند.

به عنوان مثالی برای این تهدید می توان به آسیب پذیری امنیتی IBM e-commerce Servers اشاره کرد. تمامی محصولات زیر که در این مجموعه قرار می گیرند دارای آسیب پذیری بوده اند که توسط آن اطلاعات مهم سیستم از جمله رمز عبور مدیر سیستم می توانست در اختیار هکر قرار گیرد.[11]

Net.Commerce: v3.1, v3.1.1, v3.1.2, v3.2--- WebSphere Commerce Suite: v4.1, v4.1.1--- Net.Commerce Hosting Server: v3.1.1, v3.1.2, v3.2--- WebSphere Commerce Suite--- Service Provider Edition: v3.2--- WebSphere Commerce Suite--- Market Place Edition: v4.1

- **انتقال**

در بحث انتقال که تنها با بستر ارتباطی سروکار دارد از جمله مهمترین خطراتی که آن را تهدید می کند شنود[18] اطلاعات مهم توسط یک فرد غیر مجاز می باشد حال این شنود می تواند منجر به افشاء اطلاعات کارت اعتباری و یا شناسه کاربری شود و یا می تواند از طریق شنود شناسه نشست، هکر بتواند کنترل ارتباط را به دست گیرد و با جعل هویت خود شروع به کار کند.

از جمله اصطلاحاتی که در خصوص این تهدیدها وجود دارد می توان به Eavesdropping، Session Hijacking،

---

[۱۷] Vulnerability

[۱۸] Eavesdropping

Man-in-the-middle و Reply Attack اشاره نمود.

بحث شنود ارتباط در تمامی آنها مشترک است و تنها تفاوت در برخورد با این شنود است به عنوان مثال در Man-in-the-middle هکر دقیقاً در بین راه قرار می گیرد و تمامی اطلاعات بین کاربر و سرویس دهنده را همانند یک پراکسی در اختیار می گیرد به طوریکه از دید کاربر سیستم هکر، سرویس دهنده به حساب می آید و از دید سرویس دهنده، هکر یک کاربر مجاز می باشد. اما در حمله Reply هکر ابتدا اطلاعات مربوط به نشست را به دست می آورد و سپس با قطع ارتباط کاربر با سرویس دهنده و فرستادن مجدد اطلاعات نشست (البته با اعمال تغییراتی در آن) ادامه ارتباط را به دست می گیرد.

بجز خطر عمده و مهمی که در خصوص این مفهوم بیان شد تهدید دیگری که وجود دارد خراب شدن کالا در طول راه می باشد. برخی از اجناس بسته به نوع آنها بایستی تحت شرایط خاصی حمل شوند مانند وسائل شکستنی و یا خوراکی که عدم پیروی از راهکارهای ارسال صحیح می تواند منجر به خرابی آنها شود.

- **دریافت**

در مفهوم دریافت به طور کلی با کاربران سیستم در ارتباط هستیم. اما چه معضلات و خطراتی در این ناحیه وجود دارد:

انکار سفارش: این تهدید شاید در دنیای تجارت الکترونیک پیشرفته امروز اندکی بی معنا باشد اما در ایران در برخی از سیستم ها که سفارش به صورت اینترنتی انجام می گیرد و دریافت هزینه همزمان با تحویل کالا در محل مشتری انجام می پذیرد می تواند تهدیدی جدی به حساب آید چرا که هیچ سیستمی به طور پیش فرض به منظور اثبات این موضوع که چه شخصی سفارش دهنده بوده وجود ندارد.

انکار دریافت کالا: این تهدید به طور عمده ای می تواند در نقل و انتقالات اینترنتی وجود داشته باشد به طوریکه دریافت کننده همواره انکار کننده دریافت سرویس و یا کالا می باشد.

کلاه برداری: کلاه برداری های اینترنتی حالتهای بسیار زیادی دارند اما آن دسته که در ارتباط با تجارت الکترونیک می باشد شامل فریب دادن کاربران و دریافت اطلاعات کارت اعتباری آنها و یا دریافت هزینه ای بیشتر از قیمت کالا یا سرویس می باشد.

مهندسی اجتماعی[19]: مهندسی اجتماعی در واقع هک شدن ذات بشر می باشد به این منظور که با استفاده از ترفندهایی خاص در ارتباطات بشری هکر می تواند به اطلاعات مطلوب خود دست یابد و یا به نوعی آنها را متقاعد به انجام کاری بکند.

راهکارهای مقابله

قبل از شروع هر کاری در زمینه مقابله با خطرها بایستی بیان داشت که هیچگاه نمی توان تمامی تهدیدها را به طور کامل مرتفع ساخت چرا که در آن هنگام دیگر خطری باقی نمی ماند و این به معنای امنیت 100% می باشد که چنین چیزی تعریف نشده است پس بایستی بدانیم که در مقابله با تهدیدها و خطرات موجود چه باید کرد.

بر اساس مستندات رسمی امنیت در مدیریت خطر در راستای پاسخگویی به آنها 4 رویکرد وجود دارد:

1. **اجتناب از خطر**[20]: به این معنی می باشد که آن کاری را که می تواند برای سیستم ایجاد خطر نماید را انجام ندهیم و یا با انجام کاری آن خطر را دور نماییم به طور مثال هنگامی که با قرار دادن مستقیم سرویس دهنده بانک اطلاعات در اینترنت خطرهای مربوط به سیستم عامل آن متوجه ما می شود، آن را در پشت سرویس دهنده وب قرار می دهیم تا از سمت اینترنت به آن دسترسی نباشد بنابراین آن خطرات دیگر متوجه سرویس بانک اطلاعاتی ما نیستند.

2. **انتقال خطر**[21]: در برخی از شرایط می توانیم خسارت ناشی از یک خطر را به سازمان و یا شرکت دیگری منتقل کنیم . یکی از متداولترین کارها در این زمینه بیمه می باشد. به طور مثال با انجام بیمه آتش سوزی خسارت خطر آتش گرفتن ساختمان را به بیمه منتقل کرده ایم.

3. **کاهش خطر**[22]: در اکثر موارد کارهایی که انجام می دهیم در جهت کاهش خطر هستند به طور مثال با بروز نگه داشتن سیستم عامل خطر هک شدن از طریق ضعفهای امنیتی سیستم عامل را کاهش می دهیم.

---

[۱۹] Social Engineering

[۲۰] Risk Avoidance

[۲۱] Risk transfer

[۲۲] Risk Mitigation

4. **پذیرش خطر**[23]: در شرایطی که هیچگونه از موارد بالا تحقق نیابند چاره ای جز پذیرش آن خطر نیست یعنی آگاهانه می پذیریم که از یک خطری ممکن است متضرر شویم. به طور عمده این بحث در مواقعی مطرح است که هزینه بر طرف کردن و یا کاهش خطر بسیار بالاست به طور مثال یک سرویس دهنده وب با پهنای باند 10Mbps در برابر یک حمله DDoS که مجموعه ترافیک وارده به آن از سمت هکرها در حدود 20Mbps می باشد تمامی پهنای باند خود را از دست می دهد و هزینه مقابله در برابر این خطر ارتقاء پهنای باند به بیش از 20Mbps می باشد که ممکن است این کار خود برای شرکت ضرر آفرین باشد. بنابراین آن شرکت خطر حملات DoS با پهنای باند بالاتر از 10Mbps را می پذیرد.

با توجه به موارد ذکر شده ابتدا به طور مختصر به بیان راهکارهایی در خصوص هر یک از موارد می پردازیم و سپس با دسته بندی کلی تهدیدها و مخاطرات راهکارهایی را به صورت جامع و کلی بیان می کنیم:

- **تولید**

در این قسمت که بیشتر با برنامه ای تحت وب و یا مرتبط با اینترنت در ارتباط هستیم یکی از مهمترین راهکارها، طراحی ایمن و سپس برنامه نویسی ایمن آنهاست که باز اگر بخواهیم به عمل نزدیک تر شویم می توانیم بگوییم که درصد بسیار بالایی از تهدیدهای این عوامل با کنترل و بررسی صحت داده ها و مقادیر ورودی برطرف می شوند در مراتب بعدی می توانیم به دقت در انتخاب روشهای مناسب اشاره نمود به طور مثال استفاده از روش ذخیره سازی اطلاعات خرید در سیستم کاربر و سپس استفاده از آنها بدون هیچگونه اعتبار سنجی به منظور محاسبه قیمت نهایی روشی کاملاً نا مطمئن می باشد.

بنابراین بایستی در این خصوص دقت داشته باشیم که تمامی اطلاعاتی را که در سمت کاربر قرار داده ایم به هنگام دریافت، آنها را بررسی کنیم و یا اطلاعات را به طوری در سیستم کاربر قرار دهیم که کاربر قادر به فهم و تغییر در آنها نباشد. برای مثال می توان از روشهای رمزنگاری به منظور مخفی نگه داشتن اطلاعات مهم و از توابع Hash به منظور بررسی صحت اطلاعات دریافتی استفاده کرد.

بنابراین به طورکلی می توان بیان داشت که هیچگاه نبایستی به اطلاعات رسیده از سمت کاربر اطمینان داشت مگر اینکه روشی برای اثبات صحت آنها موجود باشد.

راهکار دیگر آنکه در قسمتهایی از سایت که می توانند مقادیر ورودی را از کاربر دریافت کنند و به سمت سرویس دهنده انتقال دهند بایستی از نظر حجم نیز بررسی شوند.

---

[۲۳] Risk Acceptance

نکته مهم اینکه در انجام این کنترل ها بایستی دقت شود که یک کاربر نتواند از آن کنترل ها و محدودیت ها به نوعی غیر مجاز عبور کند به طور مثال هنگامی که تمامی کنترل ها و اعمال محدودیت ها در سمت کاربر انجام پذیرد هکر می تواند با استفاده از روشهای مختلفی در آنها تغییر ایجاد کند و یا حتی آن محدودیت ها را به طور کامل حذف کند. راهکاری که برای مقابله با چنین کاری موجود می باشد این است که تمامی کنترل ها و محدودیت ها در سمت سرویس دهنده نیز بررسی شوند و تنها متکی به سمت کاربر نباشند.

از دیگر راه های عبور از محدودیت ها به صورت غیر مجاز استفاده از اشکال دیگر دستورات می باشد به این صورت که اگر برنامه نویس، در یک صفحه اینترنتی به منظور پیشگیری از SQL Injection کاما (') را محدود کرده است و آن را در فیلدهای ورودی برنامه نمی پذیرد هکر می تواند برای عبور از چنین محدودیتی از عبارت متناظر Unicode آن یعنی (%27) استفاده کند. راهکاری که برای اینکار می توان در نظر گرفت شامل محدود کردن تمامی عبارات و کاراکترها جز موارد مورد نیاز می باشد اما در شرایطی که چنین کاری امکان پذیر نمی باشد می توان علاوه بر کاراکتر های مشکل ساز اشکال متناظر دیگر آنها را هم نیز محدود کرد. به طور مثال می توان به مشکل حملات Unicode در نسخه های قدیمی سرویس دهنده وب مایکروسافت (IIS) اشاره کرد.

در مورد رمزعبور در وحله اول کاربران سیستم در خصوص اهمیت رمزعبورشان و این که چگونه آن را انتخاب و به صورت ایمن از آن نگهداری کنند بایستی آگاه شوند. اما از آنجایی که همواره بشر به سمت راحت انجام دادن کارها تمایل دارد ممکن است طیف وسیعی از کاربران سیستم در این امر سهل انگاری و رمزعبور ساده و قابل حدسی را انتخاب کنند پس به منظور پیشگیری از انجام چنین کاری در کنار آموزش بایستی سیستم های کنترل و محدود کننده ای موجود باشد تا کاربر را در مسیر ایمنی در خصوص انتخاب رمزعبور قرار دهد. در همین راستا علاوه بر رعایت موارد فوق همچنان امکان کشف رمزعبور از طریق ورود به زور امکان پذیر می باشد. در مورد کاهش خطر این حمله راهکار مرسومی به نام Captcha موجود می باشد. این راهکار شامل تولید یک عکس تصادفی است که در بر گیرنده متنی می باشد که کاربر بایستی به هنگام ورود و یا در مواقعی که تعداد دفعات ورودهای ناموفق از حد معمول بیشتر می باشد برای تمییز خود از برنامه های خودکار رمزعبور وارد کند.

- **ارائه**

در این قسمت راهکارهای مقابله را در سه قسمت بیان می کنیم:

1. یکی از مهمترین کارها بروز نگه داشتن همیشگی و به موقع محصولات می باشد. زیرا بسیاری از مشکلات در این قسمت مربوط به آسیب پذیری های محصولات مورد استفاده می باشد که شرکتهای ایجاد کننده آن همواره به منظور بر طرف کردن ضعف های موجود، محصولات خود را با بسته های امنیتی بروز رسانی می کنند.
2. تنظیم صحیح و ایمن برنامه ها، سیستم عامل و سرویس دهندگان، زیرا که به طور پیش فرض تنظیمات اولیه یا به دلایل سازگاری با نسخه های قبلی و یا استفاده آسان تر از امنیت کافی برخوردار نیستند.

3. حذف تمامی موارد غیر نیاز و غیر ضروری، هر سرویس اضافه ای که در سیستم ما وجود داشته باشد خود می تواند دارای ضعف های امنیتی باشد و مشکلاتی را برای ما بهمراه بیاورد بنابراین هرگونه سرویس، قابلیت، پروتکل و... که مورد نیاز نمی باشند بایستی از سیستم حذف شوند.

- **انتقال**

در این بخش در خصوص خطرات مربوط به شنود ارتباط می توان از راهکارهای رمزنگاری و بررسی صحت اطلاعات ارتباط استفاده نمود امروزه شرکت های بسیاری در این خصوص مشغول به فعالیت می باشند. زیر ساخت کلید عمومی[24] و تمامی مباحث مربوط به امضای دیجیتال[25] از جمله راهکارهای مناسبی هستند که از پایه های امنیت در تمامی سیستم های تجارت الکترونیکی ایمن می باشند.

در خصوص خطر آسیب دیدگی کالا به هنگام ارسال می توان عواقب ناشی از این خطر را به بیمه انتقال داد. این همان امری است که اشخاص عادی نیز در هنگام استفاده از سرویس های پست با آن روبه رو شده اند.

- **دریافت**

در این قسمت به منظور پوشش خطرات مربوط به انکار می توان از شخص سوم مورد تاییدی در جهت اثبات انجام کاری کمک گرفت به طور مثال تلفیقی از زیر ساخت کلید عمومی و امضای دیجیتال این امر را محقق می سازد.

آنجایی که دریافت و پرداخت در دنیای واقعی انجام می پذیرد یعنی هزینه به هنگام دریافت کالا پرداخت می شود می توان با استفاده از روشهای عضو گیری و شناسایی کامل افراد به این مشکل پاسخ داد.

همچنین به منظور پیشگیری از کلاهبرداری اینترنتی نیز می توان از شخص سوم مورد تاییدی در جهت احراز هویت دوگانه استفاده نمود به این صورت که هم سرویس گیرنده هویتش برای سرویس دهنده احراز شود و هم سرویس دهنده هویتش را برای سرویس گیرنده احراز کند.

در خصوص خطر مهندسی اجتماعی نیز تنها راه ممکن آموزش و آگاهی رسانی می باشد.

---

[۲۴] PKI (Public Key Infrastructure)

[۲۵] Digital Signature

راهکارهای کلان

با بررسی مطلالب بیان شده در قسمت خطرها و تهدیدها می توانیم منبع تمامی این خطرات را در سه حوزه مورد بررسی قرار دهیم:

1. **ضعف تکنولوژی**
2. **ضعف دانش افراد استفاده کننده**
3. **اشتباهات انسانی**

حال براین اساس می توانیم راهکارهایی را به صورت کلی بیان کنیم:

در خصوص ضعف تکنولوژی ابتدا بایستی نیروی انسانی با دانش و همچنین هزینه مناسبی جهت انجام کارهای تحقیقاتی و مطالعاتی قرار بگیرد تا بتوانیم با توجه به تحلیل های صحیح مجموعه به طرحی مناسب دست یابیم و سپس توسط تیمی مجرب و نظارتی مناسب آنها را پیاده سازی کنیم و در نهایت با انجام تستهای مختلف بتوانیم مشکلات سیستم را پیدا و در جهت رفع آنها اقدام کنیم. اگرچه این مواردی که بیان شده همگی از مطالب روشن و واضح می باشند اما به کارگیری صحیح آنها می تواند تا حد بسیار زیادی مفید واقع شود نکته ای که در اینجا مهم است استفاده از تجارب قبلی و تفکر Proactive می باشد به این منظور که با دیدن یک خطر علاوه بر فکر کردن به مرتفع نمودن و یا کاهش آن، به موارد مشابه دیگری هم که ممکن است در سیستم رخ دهند بایستی فکر شود.

در خصوص ضعف دانش افراد نیز تنها راه ممکن آموزش می باشد. بحث کسب دانش مورد نیاز به سه قسمت تحصیل، آموزش و آگاهی رسانی تقسیم می شود و هرکدام در حوزه ای خاص مطرح می گردند به طور مثال در یک سیستم کامل تجارت الکترونیک افرادی که بر روی امنیت آن سیستم کار می کنند بایستی تحصیلات کاملی در زمینه امنیت داشته باشند به این منظور که با گذراندن دوره های مختلف آموزشی به مهارتی ویژه در زمینه تخصصی خودشان (امنیت) دست یابند، افراد دخیل در حوزه تولید، ارائه و انتقال بایستی آموزش های امنیتی لازم را دیده باشند و مفاهیم کلی آن را بدانند و تمامی افراد حوزه دریافت یعنی استفاده کنندگان سیستم بایستی در خصوص موارد پایه امنیت آگاهی داشته باشند.

در خصوص اشتباهات انسانی دو راهکار موجود می باشد یکی نظارت بر اجرا و دیگری بررسی کار اجرا شده که اگر نظارت مناسبی بر کار باشد و پس از انجام آن نیز به دقت مورد بررسی قرار گیرد تا حد بسیار زیادی خطراتی که از این حوزه ناشی می شوند کاهش می یابند.

شروع کار امنیت مطابق جمله معروف "امنیت یک هدف نیست بلکه یک سفر است" به منزله آغاز سفری به اندازه عمر تجارتی است که خواهیم داشت پس همواره تمامی کارهای انجام شده بایستی مورد بررسی قرار گیرند و هر روز در جهت بهبود آن باید تلاش شود. در همین راستا شرکت هایی شروع به کار کرده اند که وظیفه آنها بررسی منسجم و دوره ای امنیت سایت ها می باشد

و سایتهای اینترنتی که از این سرویس ها استفاده می کنند نشان مربوط به آن را در سایت خودشان قرار می دهند به عنوان مثال HackerSafe یکی از همان بررسی کنندگان امنیت می باشد.

نمونه اجرایی

به عنوان یک نمونه که بر این اساس در حال شکل گیری می باشد می توانیم به قسمت تجارت الکترونیک سایت تبیان اشاره نمود.

در این قسمت به منظور کاهش خطرهای حوزه دریافت در تبیان اعضاء در سطوح مختلفی وجود دارند و هر سطح دارای مراتبی از تایید می باشد به طور مثال یکی از سطوح، اعضای تایید شده نهایی می باشد تبیان از افراد موجود در این سطح اطلاعات کاملی از جمله کپی شناسنامه آنها می باشد.

در خصوص حوزه تولید از حدود دو سال پیش برنامه ای به منظور طراحی مجدد سایت برای کاهش معضلات موجود شروع شد و در آن سعی بر آن بود که تمامی موارد امنیت مرتبط با کار تبیان در آن دیده شود.

در حوزه ارائه، تبیان در حال راه اندازی مرکز داده ای می باشد که بتواند سرویسی مناسب را به منظور بستری ایمن و قابل اطمینان برای عوامل تولید به وجود بیاورد.

در انتقال نیز طرحی در خصوص استفاده مناسب از روشهای رمزنگاری و بررسی صحت در حال آماده شدن می باشد.

امنیت موارد پیاده سازی شده نیز به صورت دوره ای بررسی و به هنگام کشف مشکل امنیتی اقدامات لازم در جهت رفع آن انجام می گیرد.

نتیجه

با توجه به مطالب گفته شده می توانیم تمامی عوامل دخیل در تجارت الکترونیک را در چهار حوزه تولید، ارائه، انتقال و دریافت مورد بررسی قرار دهیم و به منظور بررسی کردن امنیت در این حوزه ها می توانیم به طور کلی به بررسی و انطباق منابع خطرها با چهار حوزه یاد شده بپردازیم.

تمامی خطرات عمدتاً از سه حوزه ضعف تکنولوژی، ضعف دانش افراد استفاده کننده و اشتباهات انسانی ناشی می شوند که اگر مراتب تحلیل سیستم، توجه به امنیت در هنگام طراحی و پیاده سازی، بررسی دقیق و کنترل نهایی کار به هنگام پایان پیاده سازی و همچین آموزش صحیح و آگاهی رسانی مناسب امنیتی را در نظر داشته باشیم می توانیم تا حد بسیار خوبی خطرهای امنیتی را کاهش دهیم.

منابع

1. Webster Dictionary, www.merriam-webster.com
2. Stewart James Michael, CISSP, Neil Edde, 2004
3. ISMS/ISO27001 Documents
4. Poulsen Kevin, Guesswork Plagues Web Hole Reporting, SecurityFocus.com, 06-03-2003
5. Poulsen Kevin, FTC investigates PetCo.com security hole, SecurityFocus.com, 05-12-2003
6. Mutton Paul, PayPal security Flaw Allows Identity Theft, News.Netcraft.com, 06.16.2006
7. Van Den Berg Richard, 3D3.com ShopFactory Shopping Cart Cookie Price Manipulation Vulnerability, Securityfocus.com, 12.02.2002
8. PDGSoft Shopping Cart Multiple Buffer overflow Vulnerabilities, Securityfocus.com, 05.25.2000
9. K. K. Mookhey, Common Security Vulnerabilities in e-commerce Systems, 2004
10. Miller Rich, DDoS Attacks Hobble e-commerce Sites, News.Netcraft.com, 05-10-2004
11. Shah Agam, IBM e-commerce Servers Vulnerable to Hack, CNN.com, 03-09-2001
12. Russel Ryan, Hack Proofing Your e-commerce Site, Syngress Publishing, 2001
13. Kesh, framework for analyzing e-commerce security, Information Management & Computer Security. Vol.10, Iss.4, 2002
14. Peeples, Instilling consumer confidence in e-commerce, Advanced Management Journal. Vol.67, Iss.4, 2002