مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۴ ، زمستان ۱۳۹۵، ص ۵- ۱

ISSN: 2745-3673
http://www.Rcsj.ir

مجلـه‌ی علمی پژوهش در علوم رایانه (سال دوم)
شماره ۴ / زمستان ۱۳۹۵ / ص ۵-۱

بررسی امنیت اطلاعات در تجارت الکترونیک

آرمان رستمی [۱]

[۱] دانشجوی کارشناسی ارشد،دانشگاه صالحان قائم شهر

نام و نشانی ایمیل نویسنده مسئول:
آرمان رستمی
arman.92779277@gmail.com

چکیده

هرگونه داد و ستد الکترونیکی تحت عنوان تجارت الکترونیک بیان می شود که خود می تواند حالتهای مختلفی را دربر داشته باشد .در بحث تجارت الکترونیک عواملی از قبیل برنامه های تحت وب، 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 .این مقاله سعی بر بررسی 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.

واژگان کلیدی: امنیت، تجارت الکترونیک، انتقال، دریافت

مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۴ ، زمستان ۱۳۹۵، ص ۵- ۱

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه

در دنیای رو به رشد و بهم متصل الکترونیکی امروز زندگی انسان در دست بسته 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 فروشکالا و یا سرویسی خاص باشد. فارغ از ضریب نفوذ اینترنت، تعداد سرویس دهنده و فروشندگان آنلاین، میزان گسترش فرهنگ خرید در اینترنت و مباحث دیگری از این دست ...هستند کسانی که در اینترنت تبادلات مالی دارند.

این دسته از کاربران اینترنت که مخاطب این مقاله اند بی شک به امنیت نیاز خواهند داشت(امنیت در خرید)که از دو طریق مورد مخاطره قرار می گیرید:

۱ -مورد سرقت واقع شدن اطلاعات حساب بانکی۲-پرداخت وجه و عدم دریافت محصول.

تهدیدات الکترونیک

از آنجایی که 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

واژه «امن» یعنی بی گزند و بی آسیب و دارای آرامش. امنیت هم یعنی بی گزندی و بی آسیبی یا حالتی که در آن گزند و خطر و آسیب راه ندارد و آرامش در آن برقرار است . در تعریف امنیت «Security» می توان گفت :

در لغت حالت فراغت از هر گونه تهدید یا حمله و یا آمادگی برای رویارویی با هر تهدید و حمله را گویند. در اصطلاح سیاسی و حقوقی به صورت امنیت فردی، امنیت اجتماعی، امنیت ملی و بین المللی به کار برده می شود

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

اما افراد متخصصاین زمینه امنیت را در حفظ و بقاء 4 اصل می دانند:

محرمانگی [۱] :اطلاعات فقط و فقط بایستی توسط افراد مجاز قابل دسترسباشد

تمامیت :یک سیستم از عناصری متشکل است که در کنار هم برای رسیدن به هدفی یکسان همکاری دارند .حفظ تمامیت [۲]به معنای پیشگیری از بروز مشکل در این همکاری و پیوسته نگه داشتن عناصر یک سیستم می باشد.

دسترس پذیری [۳] :اطلاعات بایستی به هنگام نیاز توسط افراد مجاز قابل دسترس باشد.

عدم انکار [۴] : به هنگام انجام کاری و یا دریافت اطلاعات یا سرویسی، شخص انجام دهنده یا گیرنده نتواند آن را انکارکند.

---

[1] Confidentiality
[2] Integrity
[3] Availability
[4] Non-Repudiation

مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۴ ، زمستان ۱۳۹۵، ص ۵- ۱

ISSN: 2745-3673
http://www.Rcsj.ir

تجارت الکترونیک

هرگونه داد و ستد الکترونیکی تحت عنوان تجارت الکترونیک بیان می شود که خود می تواند حالتهای مختلفی را دربر داشته باشد .در بحث تجارت الکترونیک عواملی از قبیل برنامه های تحت وب، 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 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، سرویسدهنده 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.

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 IS027001 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. تولید با توجه به دسته بندی انجام شده در مفهوم تولید بیشتر با یکسری از برنامه های تحت وب و بانکهای اطلاعاتی در ارتباط هستیم .فارغ از این موضوع که این برنامه ها توسط تیمی مشخصبه منظور انجام یکداد 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

راهکارهای مقابله

بالابردن امنیت آنلاین کارت های بانکی در هنگام خرید اینترنتی

امروزه فاصله بین دنیای مجازی و واقعی هر روز درحال کم شدن است، بسیاری از اموری که در دنیای واقعی درحال انجام شدن است در دنیای مجازی یک معادل پیدا کرده است .یکی از این امور که در دنیای حقیقی انجام می شود تبادلات مالی بین انسانها است که در طول روز انجام می شود و در این چند سال اخیر جای زیادی را در دنیای مجازی باز کرده است.

در این میان روشهای زیادی برای خرید از اینترنت وجود دارد یکی از این روش ها خرید از طریق کارت های عابربانک است .خرید از طریق عابربانک مزایای زیادی دارد ولی در کنار این مزایا خطراتی را نیز برای کاربرانی که آگاهی کافی از موارد امنیتی در رابطه با این موضوع ندارند ایجاد می کند.یکی از خطرات جدی در خرید و فروش آنلاین، لو رفتن شماره کارت های اعتباری و رمز عبور آنها است که سالانه میلیونها دلار خسارت به بانکها و دارندگان کارت ها وارد می آورد.

تشخیص سایت های جعلی

یکی از روش های متداول سرقت اطلاعات تقلید از وب سایت های معتبر و فریب خریداران است .درحقیقت کلاهبرداران اینترنتی اطلاعات حساب کاربران را از طریق ایجاد وب سایت هایی به ظاهر حرفه ای که از شرکت های قانونی تقلید کرده اند، به سرقت می برند . واضح است که هوشیاری کاربران می تواند از بروز این مشکل جلوگیری کند. خریداران باید از طریق تایپ آدرس وب سایتی که می خواهند از آن خرید کنند به سایت وارد شوند و از وارد کردن اطلاعات کارت اعتباری خود در صفحاتی که از طریق لینک های مشکوک به آنها وارد شده اند، خودداری کنند.

ISSN: 2745-3673
http://www.Rcsj.ir

قابلیت اعتماد طرفین

در معاملات آنلاین، فروشندگان باید به مشتریان خود انتخاب های مطمئن و راحتی را برای نحوه پرداخت ارایه دهند، به طوری که بهترین نتیجه را برای مشتری و واحد تجاری در بر داشته باشد .از جمله روشهای متداول پرداخت می توان به پرداخت وجه به صورت آنلاین اشاره کرد.

یکی دیگر از مواردی که منجر به سرقت اطلاعات کارت های اعتباری می شود، مربوط به عدم رعایت نکات ایمنی توسط فروشندگان است. زمانی که تراکنش معامله به صورت باز و بدون امنیت و رمزگذاری مناسب به اینترنت ارسال می شود، هکر ها می توانند با استراق سمع این تراکنش به اطلاعات حساسی همچون شماره کارت های اعتباری و رمز عبور آنها دسترسی پیدا کنند. به همین دلیل فروشندگان در دنیای مجازی باید اصول امنیتی را کاملاً رعایت کنند که یکی از آنها رمزنگاری اطلاعات حساس مشتریان است. رمزنگاری فرآیند تبدیل اطلاعات برای تغییر شکل آن به صورت غیر قابل فهم برای همه بجز برای گیرنده اطلاعات می باشد که زمینه سلامت و پوشش مورد نیاز تجارت الکترونیک را برای اطلاعات رد و بدل شده فراهم می آورد.

استفاده ازچندین کارت بانکی

اگر شما از چندین کارت بانکی استفاده می کنید هیچوقت تمامی کارت های اعتباری خود را به یک رمز خاص تخصیص ندهید می توانید برای هر کارت یک رمزجداگانه استفاده کنید .اگر قادر به خاطرسپردن اطلاعات هر یک از کارت ها نیستید اطلاعات آنها را در یک فایل متنی قراردهید اما توجه کنید که اطلاعات را بصورتی که فقط خود از آن مطلع هستید ذخیره کنید. مثلا رمزهای عبور را بصورت مورب یا عمودی تایپ کنید .اگراطلاعات کارت بانکی خود را در گوشی هوشمند خود ثبت می کنید توجه کنید که فایل متنی خود از امنیت بالایی برخودار باشد می توانید از نرم افزارهای رمزگذاری بر روی فایل متنی استفاده کنید.

فقط در سایت های امن اطلاعات کارت اعتباری خود را وارد کنید. در آدرس بار مرورگر زمانی که می خواهید اطلاعات بانکی کارت خود از جمله رمز عبور را وارد کنید توجه کنید که از در آدرس بار مرورگر زمانی که می خواهید اطلاعات بانکی کارت خود از جمله رمز عبور را وارد کنید توجه کنید که از ویژگیHTTPS استفاده گردد . این گواهی امنیت دیجیتال برای ردوبدل کردن اطلاعات بین بانکی است.پس توجه داشته باشید که حرف S در انتهایHTTP وجود داشته باشد.

نتیجه گیری

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.

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[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