گزیده‌ای از مقاله:

بانکداری الکترونیکی و چارچوب امنیتی آن

دکترمحمدحسین مشرف جوادی (عضو هیأت علمی گروه مدیریت دانشگاه اصفهان)
فاطمه بهزادفر و حمزه قوچی فرد (دانشجویان کارشناسی ارشد مدیریت مالی دانشگاه اصفهان)

چکیده

گسترش شبکه جهانی اینترنت، مزایای بسیاری را برای تمامی سازمان‌ها، از جمله بانک‌ها به ارمغان آورده است که همراه با آن، مسایل درخور توجهی مطرح می‌شود. امنیت شبکه‌های اینترنتی، یکی از این موضوعات است که اعتماد مشتریان به تجارت از طریق اینترنت و پذیرش بانکداری اینترنتی را تحت تأثیر قرار می‌دهد. از آنجا که مسأله امنیت و حریم خصوصی، از مهمترین موانع توسعه بانکداری الکترونیکی می‌باشند، لذا هدف از ارایه این مقاله، بررسی موضوع امنیت در بانکداری الکترونیکی است. در این راستا ضمن ارایه چارچوبی جامع از بانکداری الکترونیکی و گام‌های لازم، الزامات ضروری در جهت امنیت بانکداری الکترونیکی را بررسی می‌کنیم و در آخر به مدل‌های استراتژیک بانکداری الکترونیکی خواهیم پرداخت.

واژه‌های کلیدی: بانکداری الکترونیکی، تجارت الکترونیکی، امنیت، حریم خصوصی.

حریم خصوصی، به مجموعه‌ای از الزامات قانونی و رویه‌های مناسب در رابطه با بکاربردن داده‌های خصوصی اشاره دارد، در حالیکه مقوله امنیت، به ضمانت‌های فنی مربوط می‌شود.

حریم خصوصی و امنیت

به طور عمومی، حریم خصوصی به حفاظت از اطلاعات شخصی بازمی‌گردد و به طور دقیق، کلارک حریم خصوصی را به عنوان حق افراد برای تنها بودن با در نظر گرفتن ابعاد مختلف مانند حریم خصوصی بدن، رفتار، ارتباطات و داده‌های شخصی افراد تعریف می‌کند[۴]. تا جایی‌که به اینترنت مربوط می‌شود، حریم خصوصی جنبه‌هایی مانند کسب، توزیع یا استفاده غیرمجاز از اطلاعات شخصی را تحت‌تأثیر قرار می‌دهد[۱۵]. ظرفیت رو به رشد تکنولوژی جدید برای پردازش اطلاعات و همچنین پیچیدگی آن، حریم خصوصی را تبدیل به یک موضوع بسیار مهم کرده است. این واقعیت که داده‌های خصوصی چگونه جمع‌آوری می‌شوند و در مبادلات اینترنتی چگونه به جریان در می‌آیند، می‌تواند موجب افزایش بی‌اعتمادی مشتریان باشد و در نتیجه، به صورت یک مانع اصلی بر سر راه گسترش تجارت الکترونیکی قرار گیرد[۵] که به طور اساسی از فقدان کنترل مشاهده شده توسط کاربر در طول استفاده از اطلاعات خصوصی عرضه شده به فروشندگان ناشی می‌شود. علاوه بر مشکلاتی که به علت نبود حریم خصوصی بوجود می‌آیند، فقدان امنیتی که توسط مصرف‌کنندگان اینترنتی مشاهده می‌شود، یکی دیگر از موانع اصلی پیشرفت تجارت الکترونیکی است[۶]. در زمینه اینترنت، امنیت به مشاهداتی در رابطه با امنیتی بازمی‌گردد که به وسایل پرداخت و مکانیزم ذخیره و انتقال اطلاعات مربوط می‌شود[۱۱]. بنابراین، چیزی که ما در اینجا راجع به آن سخن می‌گوییم، جنبه‌های فنی است که انسجام، قابلیت اعتماد، اعتبار و جنبه غیرتشخیصی روابط را اطمینان بخش می‌کند[۵].

به طور خلاصه، این مطلب قابل بیان است که حریم خصوصی، به مجموعه‌ای از الزامات قانونی و رویه‌های مناسب در رابطه با بکاربردن داده‌های خصوصی اشاره دارد. در حالیکه مقوله امنیت، به ضمانت‌های فنی مربوط می‌شود که برآورده شدن مؤثر این الزامات قانونی و رویه‌های مناسب راجع به حریم خصوصی را

اطمینان بخش می‌سازد[۲]. اما این دو متغیر به یکدیگر مرتبطند و به طور آشکار در سه حوزه متمایز دیده می‌شوند[۵].

۱) باید روی این موضوع تأکید داشت که در ذهن مصرف‌کنندگان، یک رابطه نزدیک میان این دو مفهوم وجود دارد و معمولاً آنها این دو را با هم اشتباه می‌کنند.

۲) سازمان‌ها نیز مایل هستند که هر دو مفهوم را به طور مشترک بکار برند.

۳) مؤسسات عمومی نیز هر دو مفهوم را برای اجرا در کنار هم در نظر می‌گیرند.

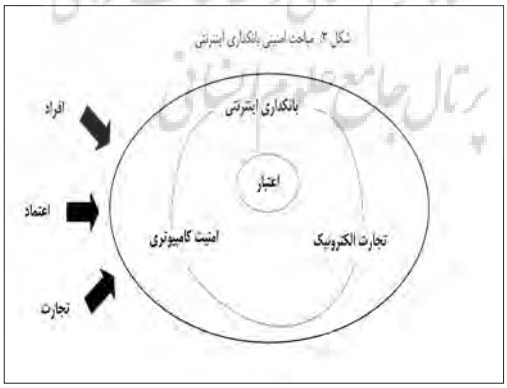
بدین گونه، اقدامات قانونگذاران شامل دسته‌ای اقدامات از نوع فرآیندی (به عنوان مثال، جمع‌آوری و استفاده و انتقال داده‌های خصوصی) و دسته‌ای که به طور کلی از نوع فنی هستند، می‌باشد. بنابراین، منصفانه به نظر می‌رسد که بگوییم از نظر خصوصیات، متغیرهای حریم خصوصی و امنیت باید به عنوان مفاهیم متمایز بکار برده شوند، اما همانگونه که می‌بینیم، نه تنها مصرف کننده، بلکه سازمان و قانونگذار نیز دریافته‌اند که این دو مفهوم رابطه نزدیکی با یکدیگر دارند. این حقیقت، حاکی از آن است که این دو متغیر، باید ابعادی از یک طرح‌ریزی (ساخت) باشند. این طرح‌ریزی امنیت مشاهده شده در کار کردن با داده‌های خصوصی نامیده می‌شود (SHPD) و درک مصرف‌کننده از روش‌هایی را نشان می‌دهد که راجع به حفاظت انجام شده از داده‌های خصوصی توسط خدمات مالی وب‌سایت و امنیت سیستم اطلاعاتی می‌باشند.

امنیت بانکداری الکترونیکی

مشابه با بسیاری از بررسی‌های الکترونیکی که امنیت اطلاعات را در درجه اول اهمیت برای تجارت و مشتریان ذکر می‌کنند[۸]، این موضوع (همانند قابلیت اعتماد در خصوص پردازش اطلاعات خصوصی و شخصی) توسط استفاده کنندگان و کاربران بالقوه و با توجه به امنیت و حریم خصوصی مبادلات بانکی اینترنتی به چالش کشیده می‌شود[۱۰]

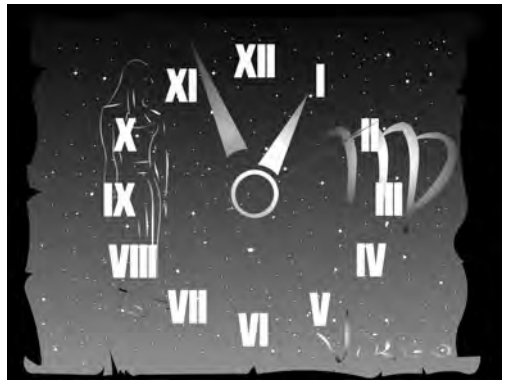
شکل شماره یک

مباحث امنیتی بانکداری الکترونیکی



این بخش از مقاله به خدمات اینترنتی بانکی و مباحثی در رابطه با تأیید کاربران که مکانیزمی در مرکز امنیت تجارت الکترونیکی است، مربوط می‌شود. هنگامی که این چارچوب در جهت سناریوهای بانکداری الکترونیکی مشخصی بکار رود، می‌تواند رهنمودهایی را در خصوص اجرای مکانیزم‌های مناسب

در گذشته، ارزیابی امنیت از طریق اجرای روش‌های تجزیه و تحلیل ریسک متعارف انجام می‌شد، ولی باظهور شبکه‌های توزیعی، این روش ناکافی شده و اتخاذ روش‌هایی جدید برای برآورد ریسک ضروری شده است.



یک چارچوب امنیت تجارت الکترونیکی، بایدضمن نگهداری سوابق عملیات و در دسترس بودن، از حریم خصوصی هم به خوبی حفاظت کند.

برای تأیید کاربران به مشتریان ارایه کند و سطح مطلوبی از اعتماد را میان طرفین مبادله برقرار سازد.

این مطلب نیز قابل ذکر است که تحقیقات قبلی به طور کلی روی ریسک‌های امنیتی اینترنتی متمرکز بودند، امادر این مقاله به الزامات امنیتی بانکداری اینترنتی که برای حفاظت از امنیت سیستم حیاتی است، توجه می‌شود.

چارچوب بانکداری اینترنتی

مدل ارایه شده برای شناسایی الزامات امنیت در یک محیط بانکداری اینترنتی و حمایت از استفاده از آن، هم در مدل تجارت به تجارت و هم تجارت به مصرف کننده (در تجارت الکترونیکی) در نظر گرفته می‌شود.

سازمان‌ها و مؤسسات با اندازه کوچک و متوسط (SMEها) و مصرف کنندگان خانگی قادر خواهند بود تا از این چارچوب به عنوان یک راهنما برای مشخص کردن الزامات امنیت برای محیط بانکی مخصوص به خود استفاده کنند. هدف سناریوی ارایه شده، تقویت یک حس اعتماد در میان طرفین درگیر در مبادلات بانکی اینترنتی است، مانند اینکه از اطلاعات شخصی آنها در برابر نقض امنیت مورد انتظار محافظت می‌شود. بار کلی (Barclay) که ادعا می‌کرد بزرگ‌ترین بانک اینترنتی انگلستان است، مجبور شد وب‌سایت خود را در پایان جولای ۲۰۰۰، یعنی هنگامی که صورت حساب‌های بانکی دیگری توسط مشتریان استفاده می‌شد، راه‌اندازی کند[۸].

بیشتر مبادلات تجارت الکترونیکی از طریق جستجو کننده‌های web که به سایت‌های تجاری متصل می‌شوند، انجام می‌شود. این سایت‌ها نیز به نوبه‌خود به برخی از مؤسسات مالی مرتبط هستند. به طور مثال، در هر سیستم اطلاعاتی بی‌نقص، هنگام انجام مبادله، انتقال اطلاعات باید برای کاربر به صورت یکپارچه و شفاف صورت گیرد و وجود بازخورد به منظور ایجاد کنترل ضروری است. برخی از ضمانت‌های امنیتی در جستجوگرها و وب‌سایت‌ها، به شکل نمادها و علامت‌هایی برای مشتریان در حال انجام مبادلات نمایش داده می‌شوند که تا حدی با این چارچوب‌ها مطابقت دارند. به طور نمونه، از تصویر یک قفل شکسته نشده برای نشان دادن یک مدت زمان امن برای اجرای برنامه استفاده می‌شود که در جهت کمک به انسجام و قابلیت اعتماد از طریق رمزدار کردن، توضیحاتی در رابطه با حفاظت از داده‌ها و سیستم‌های امنیتی ارایه کننده حفاظت، اسامی نواحی آشنا و قابل رسیدگی جهت بررسی و تأییدیه‌های دیجیتال می‌باشد[۳]. بدون وجود راه محسوسی برای یک کاربر روزانه در جهت معتبرسازی امنیت واقعی سیستم‌های بانکداری اینترنتی، مدارک بسیار کمی برای حمایت از اینکه این علامات تقلیدی و جعلی نیستند، وجود دارد. این چارچوب مبنایی برای تعیین احتیاجات امنیتی لازم و ترسیم آنها به صورت معماری امنیتی مناسب برای محیط متناظر را فراهم می‌کند.

گام‌هایی در فرآیند اجرای چارچوب مورد نظر

درگذشته، ارزیابی امنیت از طریق اجرای روش‌های تجزیه و تحلیل ریسک متعارف انجام می‌شد، ولی با ظهور شبکه‌های توزیعی، این روش ناکافی شد و اتخاذ روش‌هایی جدید برای برآورد ریسک ضرورت یافت. از اینرو، چارچوب زیر قصد تشخیص الزامات امنیتی را برای یک محیط بانکداری اینترنتی دارد، به نحوی که پیشرفته‌تر از یک چارچوب برای امنیت تجارت الکترونیکی باشد[۱۲] و شامل یک فرآیند شش مرحله‌ای است:

۱) به طور کلی، لیستی از تمام احتیاجات امنیتی برای یک محیط بانکداری اینترنتی را تهیه کنید.

۲) همه شرکت کنندگان و افرادی را که در فرآیند بانکداری اینترنتی سهیم هستند، شناسایی کنید.

۳) مبادلات را به صورت اقدامات مستقل و متفاوت طبقه‌بندی کنید

۴) اقدامات مشخص شده را برای شرکت کنندگان رسم کنید تا به صورت مدلی برای محیط بانکداری اینترنتی بکار رود.

۵) از اطلاعات بدست آمده در مرحله قبل برای تعیین الزامات امنیتی در یک محیط بانکداری اینترنتی ایمن استفاده کنید.

۶) از این الزامات برای ایجاد معماری امنیتی شامل روش‌ها، مکانیزم‌ها و سیاست امنیتی مناسب استفاده کنید.

الزامات امنیتی کلی برای یک محیط بانکداری اینترنتی

رابطه نزدیکی که بین تجارت الکترونیکی و بانکداری اینترنتی وجود دارد، به معنای محدود بودن مدت زمان اجرای

موضوع امنیت شبکه‌های اینترنتی، اعتماد مشتریان نسبت به تجارت از طریق اینترنت و پذیرش بانکداری اینترنتی را تحت تأثیر قرار می‌دهد.

بانکداری اینترنتی است که باید احتیاجات امنیتی را که در زیر به صورت لیست آورده شده است، برآورده کند:

۱) شناسایی و تأیید اعتبار (کاربر): توانایی منحصر به فرد تعیین یک شخص یا هویت و اثبات آن.

۲) اختیار دادن: توانایی کنترل اقدامات یک شخص یا هویت بر مبنای خصوصیات او.

۳) قابلیت اعتماد: توانایی جلوگیری از گروه‌های غیرمجاز در زمینه تفسیر یا درک داده‌ها.

۴) یکپارچگی: توانایی اطمینان دادن راجع به اینکه داده‌ها به طور تصادفی یا توسط گروه‌های غیرمجاز تغییر نخواهند کرد.

۵) انکارناپذیری: توانایی جلوگیری از انکار یا تکذیب اقدامات توسط یک شخص یا هویت.

۶) دردسترس بودن: توانایی فراهم آوردن یک خدمت بی‌وقفه.

۷) حریم خصوصی: توانایی جلوگیری از استفاده غیرقانونی یا غیراخلاقی از اطلاعات یا داده‌ها.

۸) قابلیت رسیدگی: توانایی نگهداری یک سابقه دقیق از تمامی مبادلات برای اهداف بعدی.

این هشت دسته از الزامات امنیتی، به عنوان یک مبنا برای چارچوب امنیت تجارت الکترونیکی ارایه شده‌اند[۱۲].

در ادامه، مکانیزم‌های تأیید کاربر نیز باید جهت فراهم کردن سنگ بنای تأیید اعتبار برای چارچوب بانکداری اینترنتی در نظر گرفته شوند و این مطلب شامل استفاده از کارت‌های هوشمند و شاید علم بیومتریک (علمی از مهندسی پزشکی برای شناسایی انسان‌ها ...) می‌باشد.

مدل استراتژیک بانکداری اینترنتی

اجراوتوسعه‌بانکداری‌اینترنتی‌بایددربافتی‌ازدگرگونی‌های‌اخیر استراتژی‌های‌توزیع‌خدمات‌بانکداری‌درنظرگرفته‌شود.کانال‌های توزیع متعدد خدمات بانکداری به صورت یک استراتژی بانکداری چند کاناله مرکب و پیچیده تغییر شکل می‌دهند. این استراتژی چند کاناله تبدیل به مدل رایج تجارت در اروپا شده است[۷].

ظهور و گسترش سه مدل استراتژیک اصلی برای بانکداری اینترنتی

۱) متمرکز شدن بر مدیریت و مشتری به منظور توسعه و تأمین روابط سودآور بلندمدت: هدف اصلی در بخش مشتری، داشتن یک قدرت مالی برجسته است و هدف بانک هم کوشش برای تبدیل شدن به عرضه کننده منحصر به فرد خدمات برای این مشتریان می‌باشد. این رویکرد، توسعه و ارایه یک پرتفوی وسیع از خدمات بانکی و مالی را که توسط دامنه بزرگی از خدمات مشورتی و پشتیبانی تقویت می‌شود، ایجاب می‌کند. این خدمات بیشتر از طریق اینترنت و یا تلفن، به طور شبانه‌روزی و در هر روز هفته ارایه می‌شوند.

کانال‌های توزیع متعدد خدمات بانکداری به صورت یک استراتژی بانکداری چند کاناله مرکب و پیچیده تغییر شکل می‌دهند.

۲) تمرکز بر روی رفع نیازهای خاص مشتریان: بانک‌ها به علت خدمات بسیار حرفه‌ای و اختصاصی قادر هستند تا کارمزدهای بیشتری را از مشتریان خود دریافت کنند. مطابق با این مدل ویژه، سه ناحیه اصلی تخصصی در این زمینه وجود دارد: ۱) سرمایه‌گذاری، ۲) مدیریت وجوه، ۳) وام‌های بانک. بدیهی است که سرمایه‌گذاری، نویدبخش‌ترین حوزه برای آینده خواهد بود، زیرا رابطه نزدیک‌تری را میان بانک و مشتریان برقرار می‌کند و از اینرو، شخصی کردن خدمت برای احتیاجات خاص مشتریان ضرورت می‌یابد.

۳) فراهم کردن قیمت مناسب و هزینه‌های پایین و خدمات استاندارد شده برای تعداد زیادی از مشتریان: اینترنت و تلفن، راه‌های ایده‌آلی برای انتقال این خدمات می‌باشند، زیرا خصوصیات ویژه‌ای مانند هزینه کم، سرعت و انعطاف‌پذیری دارند. یک ارزیابی کامل از نیازهای مشتریان، به خصوص برحسب کمک‌های شخصی و مشورتی، برای موفقیت بانکداری اینترنتی از هر چیز دیگر مهمتر است. چنانچه روش‌های اینترنتی در حد زیاد استاندارد شوند، بانکداری مستقیم نمی‌تواند احتیاجات سطح بالاتر مشتریان را برآورده کند. پس یک بانک باید استراتژی سوم را با استفاده منحصر به فرد از اینترنت و یا تلفن برای رابطه با مشتریان خود انتخاب کند و یا شبکه‌ای از شعب داخلی و ترکیب شده با بانکداری اینترنتی را ایجاد کند که روش پیچیده و تطبیق داده‌شده‌تری را مبتنی بر نیازهای خاص مشتری ارایه می‌دهد[۷].

مسأله امنیت و حریم خصوصی، از مهمترین موانع توسعه بانکداری الکترونیکی می‌باشند.