راه‌های جلوگیری از تهدیدات مربوط به تقلب و کلاهبرداری در بانکداری الکترونیک

◆مجتبی جهانشیری
(کارشناس اداره طرح و برنامه)

مشتریان به واسطه کلاهبرداری، از بانکداری آنلاین دوری و آن را رها می‌کنند. این مقاله درباره راه‌هایی است که بانک‌ها می‌توانند روش‌های امنیتی آنلاین خودشان را بهبود و اصلاح نمایند و همچنین تجارب مشتریانشان را در این خصوص افزایش دهند.

امنیت بهتر برای بانک‌ها نسبت به شرکت‌ها کم‌هزینه‌تر است. این حقیقت ناخوشایند زمانی بیشتر مشخص می‌شود که بحث امنیت در تجارت آنلاین پیش می‌آید.

همچنین این حقیقت که استانداردهای جدید نیز نتوانسته‌اند دو فاکتور تصدیق هویت دو عاملی[1] را بهتر نمایند. زیرا سارقین از راه حل و حیله‌هایی که در گذشته به صورت جسته و گریخته بهره برده‌اند برای تصدیق کاربری خود استفاده می‌نمایند.

بسیاری از بانک‌ها، مخصوصاً آنهایی که بزرگ هستند، گزارش می‌شود از کلاهبرداری‌های کوچک واقعاً رنج می‌برند. اما مشتریان بیشتر متضرر می‌شوند. برای مثال مشتریان در سال ۲۰۰۶ تقریباً دو برابر بیشتر از سال ۲۰۰۴ ایمیل‌های متقلبانه دریافت کرده‌اند.

مطابق بررسی‌های گروه گارتنر، نتایج مرتبط با تجربه ۱۰۹ میلیون مشتری و حمله کلاهبردارانه به آنها در سال ۲۰۰۶ در مقایسه با ۷۹ میلیون در سال ۲۰۰۵ و فقط ۵۷ میلیون در سال ۲۰۰۴ نشان می‌دهد که تعداد افرادی که از کلاهبرداری آنلاین دچار زیان مالی شده‌اند ۲۴ درصد کاهش داشته است ولی متوسط زیان‌های ناشی از کلاهبرداری آنلاین از ۲۵۷ دلار در سال ۲۰۰۵ به ۱۲۴۴ دلار در سال ۲۰۰۶ افزایش یافته است. بدتر اینکه درصد پول‌هایی که برای پوشش زیان و برگشت پول به مصرف‌کنندگان در نظر گرفته شده است، از قلم افتاده است.

به واسطه نتایج شبیه به هم، مشتریان از تهدیدات بانکداری و فروشگاه‌های آنلاین دوری و آن را رها می‌کنند. بنابراین هزینه تمام بانک‌ها در خصوص موارد امنیتی بیشتر از ارایه خدمات آنها به مشتریان است. گروه گارتنر برآورد کرده است که تنها در سال ۲۰۰۶ بیش از ۲ میلیارد دلار زیان بابت تجارت الکترونیک به واسطه مشتریانی که از بانکداری آنلاین و خریدها و پرداخت‌های الکترونیکی دوری و یا آن را رها کرده‌اند، بوده است.

علاوه بر این، بررسی اخیر جاولین نشان می‌دهد که ۴۱ درصد مشتریان در صورتی که موسسات آنها به واسطه اطلاعات متقلبانه به خطر افتاده باشند، بانک‌های خود را تغییر داده و یا استفاده آنلاین خود را کاهش می‌دهند.

مقاومت در برابر بهسازی:

چرا بسیاری از بانک‌ها در برابر بهسازی امنیت آنلاین مقاومت می‌کنند؟ این یک پیشامد است زیرا به نظر می‌رسد بانک‌ها خود را در برابر تخلفات امنیتی متمایز می‌شمارند. آنها زیان ناشی از تغییر سریع بانک توسط مشتریان را به دلیل عدم اطمینانشان به حساب نمی‌آورند. از طرفی هزینه خدمت به مشتریان از طریق شعب و کاهش درآمدی بواسطه ناتوانی در تامین امنیت، ارزش خدمات آنلاین را بالا می‌برد. چرا که بانک‌ها مجموع زیان‌هایشان را به طور نادرست پیش‌بینی کرده‌اند. همچنین بسیاری معتقدند که مخارج بالا برای برقراری امنیت، دارای توجیه اقتصادی نیست.

همچنین بانک‌ها نگران این موضوع هستند اقدامات امنیتی با کیفیت بالا، استفاده از سیستم‌های آنلاین را برای مشتریانشان مشکل‌تر کند. مطابق یافته‌های جاولین،

◆ هزینه خدمت به مشتریان از طریق شعب و کاهش درآمدی بواسطه ناتوانی در تامین امنیت، ارزش خدمات آنلاین را بالا می‌برد

مصرف‌کنندگان اقدامات اضافی را تنها در صورتی که امنیت به صورت رایگان تامین شود، استقبال می‌نمایند.

بنابراین دلایل، بانک‌ها در تامین امنیت واقعی کند حرکت می‌کنند. مقاومت بانک‌ها در این خصوص باعث شده است که انجمن اتحادیه بازرسی موسسات مالی، بانک‌ها را متعهد نماید "تصدیق هویت دو عاملی" را تامین کنند. حتی حالا، نزدیک شدن به یک امنیت پایین‌تر نیز برای اینکه بسیاری از بانک‌ها احتیاجات و نیازهای فنی را تامین نمایند، ضروری می‌نماید.

چرا مشتریان آسیب‌پذیری بیشتری دارند

همان‌طور که بانک‌های بزرگ اقدامات امنیتی بهتری انجام می‌دهند تا اطمینان پیدا نمایند که مشتری همان کسی است که او می‌گوید خود او هست، با اجرای قانون، مدت زمانی که طول می‌کشد تا آنها مجرمین را پیدا نمایند کاهش می‌یابد. مجرمینی که در موارد زیر خبره شده‌اند:

- همان‌طوری که تراکنش‌های خراب و فاسد پس از انجام اقدامات امنیتی برای تصدیق کامل کاربر اتفاق می‌افتند. (جاسوسان MITM[۲] و ویروس‌های کامپیوتری)
- حمله‌های کوچکتر به موسسات مالی که انجام اصلاحات اقدامات امنیتی را کند می‌کند.
- به خطر افتادن مشتریان به واسطه سایت‌هایی که در مقابل ضرر و زیان‌ها ضمانتی ندارند، و به واسطه روش‌های پرداخت یا سایت‌های خرده فروشی.
- فهرست نویسی کارمندان در سرقت اطلاعات، بررسی و مطالعات نشان می‌دهد که سرقت اطلاعات توسط کارمندانی که با مراقبت و نظارت کار می‌کنند ۴۰۰ درصد افزایش پیدا کرده است.
- با فعالیت دور از فضای قانون نمی‌توان به آنها رسید. آنها در چین و کشورهای اتحاد جماهیر شوروی سابق هستند، و آنها پراکنده بوده و با تحرک کافی که دارند نمی‌توان آنها را گرفتار کرد.

اجازه بدهید یک قدم به عقب برگشته و به اقدامات امنیتی نگاه کنیم که بیشتر به صورت عادی و سریع به کار برده می‌شوند. خواه برای تجارت اینترنتی، برای معاملات تلفنی، یا حتی برای صندوق‌دار در شعب.

کارت‌های مربوط به دستگاه‌های ATM شاید برای تصدیق هویت دو عاملی موفقیت بیشتری داشته‌اند که مورد توجه قرار گرفته‌اند. برای اینکه ماشین‌های ATM و اتصال آنها به بانک توسط خود بانک کنترل شده و برای کاربر نیز معتبر است، همانند مواردی که نمی‌خواهیم با تراکنش‌های آنلاین کار کنیم. هرچند برای اینکه کامپیوتر و نداشتن ارتباط ما توسط بانک کنترل شده است - بنابراین آنها امنیت کمتری دارند و کاربران نسبت به این موضوع آگاه هستند.

بیشتر سایت‌های تجارت الکترونیکی نام کاربر و رمز عبور مشخص و ثابتی را به کار می‌برند و یک شماره شناسایی شخصی که برای معاملات و تراکنش‌های تلفنی کار می‌کند. تصاویر هویتی که به آسانی دزدیده می‌شود ممکن است (یا شاید ممکن نباشد)، نیازمند تراکنش خاصی در باجه‌های صندوقداری باشد. در صورتی که، کارمندانی بیشتر دزد می‌شوند که خیلی معمولی و متعارف هستند. بانک‌ها محیط شعبه و معاملات و یا تراکنش‌هایی را که بیشتر در خطوط خصوصی و محرمانه است کنترل می‌کنند. بنابراین کاهش ریسک با کانال‌های ارتباطی مرتبط است. بالاترین آسیب‌پذیری با ارتباطات عمومی است - اینترنت و تراکنش‌های تلفنی - و جایی که برای مشتری واقعاً معلوم نیست که بانک است یا جایی که تامین کننده وجهی است.

در این دنیای سراسر ناشناخته، متخصصین امنیت پنج اقدام امنیتی اضافی را که مانع کلاهبرداری شوند بررسی و آزمایش می‌کنند. که شامل موارد ذیل هستند.

۱- فراتر از تحقیق و رسیدگی، شناسایی از راه جداسازی کانال‌های ارتباطی، شبیه بازبینی پست الکترونیکی که جداسازی شده‌اند و شما در سرویس‌های آنها واقعاً ثبت نام می‌کنید.

۲- تجزیه و تحلیل ریسک خصوصیات رفتاری نابهنجار که می‌تواند علامت کلاهبرداری در فرآیند باشد، کنترل بسیار زیاد مانند تراکنش‌های کارت‌های اعتباری با اقتدار کامل مدل نرم افزاری.

۳- کلمات کلیدی تک زمانی که در هر تماس یا در هر دفعه تغییر می‌کند عامل دومی برای تصدیق هویت دو عاملی است.

۴- تلفن‌های همراه، کلید زیر بنایی (PKI)[۳] است که ارتباطات تلفن همراه را تکمیل می‌کند.

۵- زیست‌سنجی همانند روش‌های شناسایی صورت در آزمایشات که دریچه‌های امنیتی را بهبود می‌بخشد.

در بیشتر موارد تنها یکی از این روش‌ها استفاده می‌شود. در هر حال شما یک در یا دو در را ببندید برای دزدان فرقی نمی‌کند مگر اینکه تمام درها را ببندید.

بزرگترین آسیب‌پذیری در سال ۲۰۰۷

- به خطر افتادن کامپیوتر کاربران - ویروس‌های کامپیوتری که روی کامپیوتر کاربران نصب می‌شوند و از این طریق جاسوسان MITM قادرند حمله‌های متقلبانه یا کلاهبردارانه را جاسوسی و هدایت کنند.
- جلوگیری از ایجاد ارتباط بین وب سایت و کاربر توسط افرادی که به صورت مخفی مداخله نموده تا تراکنش را به صورت ناشناخته تغییر دهند. یک نوعی از حمله جاسوسانه است.
- وب سایت‌های ساختگی که کاربر را به دیگر وب سایت‌ها منحرف می‌کنند. که از طریق آن نام کاربر و رمز عبور و دیگر داده‌های بحرانی را جمع‌آوری کنند که برای کلاهبرداری توسط سارقین استفاده می‌شود - این یک حمله متقلبانه است.

اما مشتریان نیز به همان اندازه ریسک‌های بزرگی را در بر دارند. اغلب مشتریان در قبال مسوولیت مقاومت

◆ به خطر افتادن کامپیوتر کاربران - ویروس‌های کامپیوتری که روی کامپیوتر کاربران نصب می‌شوند و از این طریق جاسوسان MITM قادرند حمله‌های متقلبانه یا کلاهبردارانه را جاسوسی و هدایت کنند

می کنند و آن ها برای افزایش امنیت انتظار دارند بانک ها یا شرکت هایی که ابزارهای مسوولیتی را مهیا می کنند خود آنها در قبال شکست ها و قصورات مسوول باشند. مشتریان نمی خواهند وسیله یا دستگاهی را با خود حمل نمایند مگر اینکه به اندازه کیف پولشان باشد. مشتریان نمی خواهند بابت افزایش هزینه های امنیتی خودشان چیزی متحمل شوند (یا آنها تا به حال نداشته اند، آنها انتظار دارند که بانک ها خود هزینه‌های امنیتی را پرداخت نمایند.)، مشتریان نمی خواهند راه حل های مختلف و متمایز امنیتی داشته باشند یا رمزهای دست و پا گیر یا ازدیاد کارت‌ها در هر قسمت و یا در سایت های مختلف.

مطالعات اخیر که توسط دانشگاه (انیستیتو تکنولوژی) ماساچوست هدایت شده است نشان می دهد با وجود اخطارها، ۹۷ درصدکاربران تراکنش هایشان را ادامه داده و از اقدامات امنیتی در جایی که سیستم های امنیتی تجارت الکترونیکی وجود دارند چشم پوشی می کنند. این ها سیستم هایی هستند که در پایان به کاربر تصویر رمزهای انتخاب شده ارایه می کنند که در همان زمان نیز نیازمند رمز عبور می باشند. مطالعات اخیر نشان می دهد با ۹۷ درصد میزان خرابی و نارسایی که به عملکرد کاربر بستگی دارد نشان می دهد کاربران عملکرد مورد قبولی نداشته اند.

نیازمندی‌های ضروری برای نسل بعدی امنیت

راه‌حل‌های امنیتی که مطابق اصول به کار می رود تا زمانی که به صورت ترکیبی استفاده می شوند بیش از همه روش ها موثر هستند در نتیجه راه حل های زیر بیش از هر چیزی نیاز ضروری برای نسل بعدی امنیت هستند.

● تایید و تصدیق دو جانبه در جایی که مشتری بانک را بررسی می کند و بانک مشتری را مورد تجزیه و تحلیل قرار می دهد.

● فراتر از تحقیق و رسیدگی به واسطه کانال اولیه و مرکزی، جاسوسانی را که نمی خواهند کاری انجام دهند کشف کند.

● دو سایت اعتباریابی که در هر محل فقط قسمتی از رمز را شناسایی کند.

● تصدیق هویت دو عاملی، تجهیزات فیزیکی که به کار می برید مانند کارت هوشمند به علاوه چیزهایی که شما به عنوان امنیت تجارت الکترونیکی دارید، چیزهای زیادی که شما می دانید شبیه یک رمز عبور.

● نقطه پایانی و کانالی که به امنیت تجارت الکترونیکی وابسته است.

● جلساتی که به امنیت تجارت الکترونیکی بستگی دارد.

● نظارت فعال که ویروس های کامپیوتری را کشف می کند.

آن سوی ابزارهایی که بهترین تکنولوژی امنیتی را دارا هستند، هر یک از بانک ها به عنوان، پردازشگر پرداخت، سایت تجارت الکترونیکی و بنگاه سرمایه گذاری می بایست وظایف خودشان را با دقت انجام دهند تا

مشتریان را برای مغلوب کردن مجرمین قبل از اینکه آنها حمله کنند کمک و سازماندهی نمایند. در جلسه و نشست با چندین تامین کننده جهانی ما از موارد ضروری و لازم به شرح ذیل باخبر شدیم.

● کاهش زیرساخت‌ها یا تنظیم هزینه‌ها برای سازماندهی بهتر.

● تصمیم گیری برای به کارگیری سخت افزارهایی که می بایست انتخابی باشد.

● به کارگیری روش های طبقه بندیی که تحول در سطوح مختلف امنیتی را آسان می کند.

● اجازه دادن به کاربران برای اینکه خودشان تعیین کنند، تنظیم دلخواه داشته باشند بین سطوح مختلف امنیتی و استفاده آسان از آن.

● به کارگیری راه حل های امنیتی که مبنای استاندارد داشته باشند در کنار کاربردهای گوناگون و کانال‌های متعدد.

نتیجه گیری:

امنیت صنعت بانکداری آنلاین برای تمام انواع ریسک های مربوط به این حرفه در حال بهبود است. به خاطر هزینه‌های بالا، بانک‌های بزرگ ابزارهایی امنیتی را برای جاهایی به کار می برند که ریسک خسارات بالا است. از همین رو مشتریان و مصرف کنندگان کوچک زیان می بینند چرا که اندازه و تعداد تراکنش های آنها کوچکتر و شدت زیان‌هایشان نیز کمتر است.

به هر حال، اجازه بدهید که به عقب برگشته و یک بار دیگر اصل ساده و اولیه را تکرار کنیم که هر چه برای امنیت تجارت الکترونیکی کمتر خرج کنیم، هزینه‌ها (به دلیل اشکالات امنیتی) بالاتر خواهد رفت. ما می دانیم که هزینه ارایه خدمات به مصرف کنندگان بنگاه‌های کوچک و متوسط در مقایسه با بانکداری خصوصی و شرکت‌های بزرگ که مشتری ما هستند بسیار بیشتر است و هر زمان که هر یک از آن مشتریان تصمیم می گیرند از بانکداری آنلاین و تراکنش‌های الکترونیکی صرف‌نظر نمایند، هزینه ارایه خدمات به آنها (از طریق باجه‌های غیرالکترونیکی) به صورت تصاعدی افزایش می یابد.

◆ ◆ ◆

◆ مطالعات اخیر نشان می دهد با ۹۷ درصد میزان خرابی و نارسایی که به عملکرد کاربر بستگی دارد نشان می دهد کاربران عملکرد مورد قبولی نداشته اند