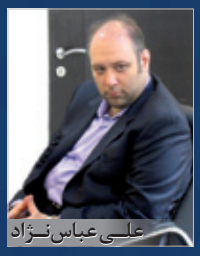
توسعه امنیت بانکداری الکترونیکی نیازمند فرهنگ سازی است

میزگرد بررسی وضعیت امنیت در بانکداری الکترونیکی ایران با حضور کارشناسان


حامد قنادپور


علی جهانی


حمید مختاریان


علی عباس نژاد


علیرضا صالحی

- طرح مباحث امنیتی در شورای راهبردی بانکداری الکترونیک
- نگران امنیت سیستم نباشید
- ۲۳ راهکار امنیتی برای بانکداری الکترونیکی

پس ازمدت‌ها تعطیلی:

طرح مباحث امنیتی در شورای راهبری بانکداری الکترونیک

پس ازمدت‌ها تعطیلی شورای راهبری بانکداری الکترونیک این بار نه در بانک مرکزی که در وزارت اقتصاد تشکیل شد و این شائبه مجددا رنگ گرفت که صنعت بانکداری الکترونیک باز هم دارای دو متولی شد. تجربه قبلی این مسئله به تشکیل کارگروه هشتگانه بانکداری الکترونیک در زمان معاونت پورمحمدی در وزارت اقتصاد برمیگردد. ظاهرا به نظر می رسد زمان تکرار شده با این تفاوت که ابوالحسنی جای پورمحمدی نشسته است.

تشکیل کارگروه‌های بانکداری الکترونیک به زمان معاونت سیدحمید پورمحمدی در معاونت بانک و بیمه و شرکت های دولتی وزارت اقتصاد در سال‌های ۸۶ و ۸۷ برمی‌گردد.

این کارگروه درنهایت با رفتن پورمحمدی به بانک مرکزی به شورای راهبردی بانکداری الکترونیک تغییر نام داد و در عین حال بعد از تشکیل چند جلسه عملا تعطیل شد بخصوص بعد از آنکه قائم مقام سابق بانک مرکزی در بحث تخلف قبزرگ بانکی مورد اتهاماتی واقع شد.

اما پس از حدودا نزدیک دوسال دکتر اصغر ابوالحسنی، معاون فعلی وزیر اقتصاد در معاونت بانک ها و بیمه ها ادامه نقش پور محمدی را مجدد و از همان‌جایی که معاون سابق آغاز کرده بود یعنی وزارت اقتصاد شروع کرده است.

این اتفاق شائبه ایجاد یک متولی دیگر برای بانکداری الکترونیک را به اذهان متبادر می‌کند. همچنین این سوال را که آیا بانک مرکزی طی چند سال اخیر قادر نبوده وظایف خود را در بخش بانکداری نوین به خوبی به انجام برساند و از سوی دیگر آیا وزارت اقتصاد می تواند به عنوان یک متولی در این امر ورود کند.

طبعا اینگونه سوالات تنها از سوی بانک مرکزی و وزارت اقتصاد قابل پاسخگویی است که البته از هم‌اکنون قابل پیش بینی است که هیچ پاسخی به هیچ طرفی داده نخواهد شد و تنها مماشاتی چند ساله بین دو نهاد مورد اشاره از نو به‌وقوع خواهد پیوست و این کشتی یعنی صنعت بانکداری الکترونیک که تازه از ساحل جدا شده دوباره در طوفان سردرگمی گرفتار خواهد شد.

در جلسه چه گذشت

جلسه شورای راهبری بانکداری الکترونیک به ریاست معاون بانک و بیمه وزارت امور اقتصادی و دارایی و با حضور معاون وزارت ارتباطات، مدیر مرکز پدافند سایبری و همچنین مدیران عامل

و فناوری اطلاعات بانک‌ها و بیمه‌ها و اعضای کارگروه‌های شورای راهبری بانکداری الکترونیک، صبح چهارشنبه ۲۱ تیر ماه جاری در وزارت امور اقتصادی و دارایی برگزار شد.

چالش‌ها و راهکارهای توسعه بانکداری الکترونیک با تأکید بر بانکداری متمرکز، امنیت و دفاع سایبری در بخش بانک و بیمه و بانک اطلاعات مشتریان، محورهای عمده مورد بحث در این نشست بود.
در این جلسه دکتر اصغر ابوالحسنی، معاون وزیر اقتصاد، خلاصه‌ای از وضعیت بانکداری الکترونیک در کشور را ارائه داد و با اشاره به توسعه و رشد چشمگیر صورت گرفته در بانکداری الکترونیک گفت: تهدیدات نیز به موازات این رشد در حال افزایش است.

وی نبود استاندارد و تعریف واحد از بانکداری متمرکز (core banking)، کمبود نیروی انسانی متخصص و مشکلات آموزش آنها، تغییر قوانین و مقررات بانکی و اتلاف منابع ملی در بحث پایانه‌های فروشگاهی را از جمله چالش‌های عمده بانکداری الکترونیک در کشور ذکر کرد و خواستار تلاش برای تهیه یک سیستم بانکداری متمرکز استاندارد در کشور شد.

دکتر رحیمی، مدیر مرکز پدافند سایبری کشور، نیز با ذکر این نکته که حوزه عملیات دفاع سایبری متفاوت از تهدیدهای امنیتی معمول است، از بخش بانکی به‌عنوان یکی از زیرساخت‌های مهم و حیاتی کشور یاد کرد که می‌تواند هدف حملات سایبری قرار گیرد و آشنایی با پدافند سایبری در مورد آن اهمیت زیادی دارد.

در بخشی دیگر از جلسه، دکتر علی خورسندیان، مدیرکل بانک و بیمه وزارت اقتصاد گزارشی از وضعیت پیاده‌سازی بانکداری متمرکز در بانک‌های کشور ارائه کرد و گفت بانک‌ها تاکنون به سه شیوه توسعه نرم‌افزار از طریق شرکت‌های وابسته بانک، خرید نرم‌افزار از خارج و خرید نرم‌افزار از شرکت‌های داخلی سعی کرده‌اند سیستم بانکداری متمرکز خود را تهیه نمایند که هر کدام دارای مزای و معایبی بوده است.

مهندس علی حکیم‌جوادی، رئیس سازمان فناوری اطلاعات هم، بحث مقابله با فیشینگ، پیاده‌سازی سیستم مدیریت امنیت‌اطلاعات(ISMS) بانکی، جداسازی اینترنت و اینترانت بانک‌ها، استانداردسازی خدمات فناوری اطلاعات بانکی، داشتن قرارداد سطح خدمات مخابراتی، تهیه سیستم متمرکز داخلی برای بانک‌ها و بیمه‌ها و تدوین معماری کلی بانکداری الکترونیک با توجه به موضوع مهم هوش تجاری را از جمله مباحثی دانست که در حوزه فناوری اطلاعات بانکی حائز اهمیت است و وزارت ارتباطات و فناوری اطلاعات، آمادگی دارد که در این موارد با سیستم بانکی همکاری کند.

مشکلات بانک‌ها در دسترسی به خدمات مخابراتی و نبود تعرفه مشخص و تدوین شده برای این خدمات از جمله مواردی بود که نمایندگان بانک‌ها و بیمه‌های مختلف با معاون وزیر ارتباطات مطرح کردند و حکیم‌جوادی قول مساعد همکاری به آن‌ها داد.

در این نشست مقرر شد جلسات مشترک بانک‌ها با معاونت وزارت ارتباطات ادامه یابد. اختصاص مکان به دیتاسنتر و سایت‌های پشتیبان بانک‌ها، تفاهم‌نامه همکاری چهارجانبه بین وزارت‌خانه‌های اقتصاد و ارتباطات، بانک مرکزی و شرکت مخابرات ایران، همکاری در مرکز امداد رایانه‌ای، ممیزی و حسابداری IT ،توافق‌نامه سطح خدمات و مباحث آموزشی از جمله محورهای همکاری آینده خواهدبود.

مرجع: مرکز فابا

نگران امنیت سیستم نباشید

۵ سال موبایل بانکینگ ایرانی

موبایل بانکینگ یا بانکداری با استفاده از تلفن همراه که این روزها در کشور ما ۵ ساله شده است، سرویسی است که حالا تقریبا تمامی بانک‌های ایرانی آن را در اختیار مشتریان خود قرار می‌دهند.

در ایران اولین‌بار این سرویس را شرکت خدمات انفورماتیک ارائه داده‌است. این شرکت با تعدادی از بانک‌های کشور قرارداد دارد و خدمات بانکداری با تلفن همراه را به مشتریان این بانک‌ها ارائه می‌دهد.

سابقه این خدمات به خرداد سال ۸۶ برمی‌گردد. البته در آن زمان سیستم SMS Banking راه‌اندازی شد که اساس آن تبادل SMSهای متنی بود و فقط خدمات غیرمالی یعنی اطلاعاتی چون مانده حساب و سه گردش آخر حساب را در اختیار مشتری قرار می‌داد.

« نرم‌افزار همراه بانک را ما برای اولین بار در ایران پیاده کردیم. نسخه یک این نرم‌افزار را تیرماه ۸۷ ارائه کردیم که این نسخه به‌تدریج کامل شد و تا بهمن ۸۸ به مرور نسخه‌های ۱.۱، ۱.۲، ۱.۳ و ۱.۴ را در اختیار بانک‌های طرف قرارداد و مشتریانشان قرار دادیم که هر نسخه نسبت به قبلی از نظر امکانات و یا عملکرد برتری داشت. به‌طور کلی در نسخه یک تا ۱.۴ همراه‌بانک امکاناتی چون مانده حساب، صورتحساب، انتقال وجه بین حساب‌های مشتری، استعلام چک، پرداخت قبض، خرید شارژ سیم‌کارت، دریافت اطلاعات سه شارژ آخر، نرخ ارز، دریافت و تغییر رمز حساب و اعلام کد شبا وجود دارد.»

مهران افسری، رییس گروه تلفن‌بانک و همراه‌بانک شرکت خدمات انفورماتیک با بیان این مطلب از ارائه نسخه دوم این نرم‌افزار از آذرماه سال ۸۹ می‌گوید: این نسخه در سطح یک علاوه بر سرویس‌های نسخه یک، اعلام مفقودی کارت و مانده کارت شتابی به آن اضافه شده و در سطح دو، انتقال وجه به حساب دیگران در همان بانکی

که مشتری حساب دارد، انتقال وجه بین بانکی و پرداخت اقساط تسهیلات را برای مشتریان بانک از طریق تلفن همراهشان مقدور می‌سازد.

نرم‌افـزاری بر پایه پیـامک

سال ۸۶ و زمانی که برای اولین بار نرم‌افزار همراه بانک در ایران ارائه شد، خبری از GPRS در کشور نبود و طبیعی‌ترین انتخاب همان پیامک بود. اما حالا که چند وقتی است سر و کله GPRS در موبایل‌های ایرانی پیدا شده، این نرم‌افزار همچنان از سرویس پیام کوتاه استفاده می‌کند. سرویسی که مسلما نسبت به GPRS مشکلاتی چون آنلاین نبودن و احتمال تاخیر و یا حتی نرسیدن پیام کوتاه دارد. به این معایب این نکته را هم اضافه کنید که برای انجام یک عملیات بانکی با استفاده از نرم‌افزاری که بر پایه پیام کوتاه کار می‌کند، لازم است تا چندین پیامک میان کاربر و بانک رد و بدل شود و هزینه این پیامک‌ها هم بر مبنای پیامک انگلیسی محاسبه می‌شود و این ماجرا یک هزینه اضافی هم به بانک و هم به مشتری بانک تحمیل می‌کند.

با این اوصاف چرا همچنان از این شیوه استفاده می‌شود؟ مهندس افسری در پاسخ به این سوال می‌گوید: «چون سیستم پیام کوتاه گستردگی بیشتری بین کاربران شبکه همراه در ایران داشت ما از ابتدا نرم‌افزارمان را بر مبنای پیام کوتاه نوشتیم. از آن گذشته سال ۸۶ که ما کار را شروع کردیم اصلا GPRS در ایران ارائه نشده بود و بعد از آن هم ترجیح دادیم روی همین سیستم پیش برویم چون الان هم درصد کمی از کاربران شبکه همراه در کشور از خدمات GPRS استفاده می‌کنند.

از همه این‌ها گذشته برای استفاده از GPRS باید تنظیمات حرفه‌ای‌تری روی گوشی انجام شود تا کاربر بتواند بانکداری با موبایل را تجربه کند.»

ساده‌تر بودن شناسایی مشتری با استفاده از SMS نکته دیگری است که افسری به آن اشاره می‌کند: هنگامی که یک کاربر با استفاده از SMS با نرم‌افزار بانک ارتباط برقرار می‌کند، شماره موبایلش مشخص است و شناسایی بسیار ساده می‌شود، درحالی‌که با استفاده از GPRS لازم است هربار شماره موبایل و شماره حساب مشتری فرستاده شود و این کار را سخت می‌کند.

نگـران امنیت سیستـم نبـاشید

اما شاید یکی از شایع‌ترین دلایل استفاده نکردن خیلی از مشتریان بانک‌ها از سرویس‌های بانک‌داری با تلفن همراه، بی‌اعتمادی آن‌ها نسبت به امنیت این سرویس‌ها باشد.

« اگر افراد توصیه‌های ایمنی را جدی بگیرند، امنیت این سیستم هیچ مشکلی نخواهد داشت.»

رییس گروه تلفن‌بانک و همراه‌بانک شرکت خدمات انفورماتیک، روش انتقال وجه در این سیستم را این‌گونه تشریح می‌کند: برای اینکه شخصی بخواهد از حساب خودش به حساب دیگر خودش انتقال وجه انجام دهد، محدودیتی وجود ندارد، اما اگر بخواهد از یک حساب به حساب شخص دیگر در همان بانک و یا بانک دیگر انتقال وجه داشته باشد، باید یک بار به صورت حضوری به بانک مراجعه کند و شماره موبایل و شماره حسابش را در فرمی ثبت کند و برای فعال‌سازی این سرویس درخواست دهد. در این صورت هنگامی که از نرم‌افزار استفاده می‌کند چون شماره موبایلش ثبت شده و شناسایی می‌شود، مشکلی به وجود نمی‌آید.

گم شدن یا به سرقت رفتن گوشی، مشکل امنیتی

دیگری است که افسری به آن اشاره می‌کند: در این صورت هم مشکلی پیش نمی‌آید، مگر اینکه شخص تمام اطلاعات حسابش را در دفترچه موبایلش ثبت کرده باشد که البته ما توصیه می‌کنیم افراد مرتکب یک چنین بی‌دقتی نشوند. اگر هم موبایلی گم شود طبیعتا اولین کار صاحبش باید سوزاندن سیم‌کارت و بستن حساب بانکی باشد. در نهایت هم سقف انتقال وجه از طریق موبایل محدود و ۵۰۰هزار تومان در شبانه‌روز است.

میزان استقبال، هر روز بیشتر از دیروز

با همه این اوصاف استقبال از Mobile banking تاکنون خوب بوده است. به‌گونه‌ای که از سال ۸۶ که این سیستم ارائه شده، هرسال مشتریان ۳ برابر و تعداد تراکنش‌ها ۴ برابر شده است.

به گفته افسری، از میان همه سرویس‌های که از طریق موبایل‌بانکینگ ارائه می‌شود، اعلام مانده حساب، صورتحساب، پرداخت قبض، خرید شارژسیم‌کارت و انتقال وجه از پرطرفدارترین سرویس‌هاهستند.

البته اگر ملاک استفاده مشتریان بانک‌ها از این سیستم را به جای رشد سالانه، درصد حساب‌های بانکی که از این سرویس استفاده می‌کنند قرار دهیم، نتیجه زیاد هم رضایت‌بخش نخواهد بود. چراکه کمتر از ۱۰ درصد مشتریان بانک‌های طرف قرارداد شرکت خدمات انفورماتیک از موبایل‌بانکینگ بهره می‌برند. مهندس افسری در این زمینه می‌گوید: «ملاک درصدگیری ما تعداد مشتریانی که از این خدمات استفاده می‌کنند نسبت به کل حساب‌های بانکی موجود در یک بانک است. اما خیلی از حساب‌های بانکی را نمی‌توان در این مورد دخیل کرد. حساب‌هایی مثل حساب یارانه‌ها، حساب‌های دانش‌آموزی و از این قبیل را.»

وی ادامه می‌دهد: به‌طور کلی در بانک‌های جدید فرهنگ استفاده از ebanking بهتر است. کیفیت مشتریانی که در یک بانک حساب دارند هم در این موضوع دخیل است. اما باید قبول کنیم که استفاده از این سیستم‌ها احتیاج به فرهنگ‌سازی دارد تا اعتماد مردم جلب شود. مردم باید بدانند که مثلا کسی که یک گوشی و خط تلفن همراه دارد با استفاده از نرم‌افزاری چون همراه بانک واقعا کمتر دلیلی برای مراجعه حضوری به بانک دارد.
مشکلات مخابراتی مثل دیر رسیدن و یا نرسیدن پیامک‌ها و دانش فنی از دیگر موانع فراگیر شدن بانکداری همراه از نظر افسری است: مثلا نصب نرم‌افزار روی گوشی به حداقلی از دانش فنی نیاز دارد. روی وب‌سایت بانک‌ها نرم‌افزار و دستورالعمل نصب آن روی گوشی قرار دارد و معمولا هم کارشناسانی برای پاسخگویی تلفنی به کسانی که در این زمینه با مشکل مواجه می‌شوند، در دسترس هستند. اما باز هم بعضی افراد با این مساله مشکل دارند.

به هرحال حالا موبایل‌بانکینگ در ایران یک تجربه ۵ ساله را پشت سر گذاشته است. فرهنگ‌سازی در زمینه استفاده بیشتر از این سرویس، رفع کردن مشکلات این سیستم مانند همخوان نبودن نرم‌افزار با بعضی مدل‌های گوشی که از نرم‌افزارهای جدید استفاده می‌کنند و اقداماتی چون درنظر گرفتن سیستم‌های تشویقی برای کسانی که از این شیوه استفاده می‌کنند شاید راهی باشد برای استفاده بیشتر از این سیستم و جلوگیری از مسافرت‌های غیرضروری شهری.

مرجع : روزنامه همشهری

۱۲ راهکار امنیتی برای بانکداری الکترونیکی

فناوری اطلاعات و ارتباطات فرصتی برای حوزه‌های پولی و مالی خلق کرد تا بهره‌وری این حوزه رشد و پیشرفت قابل توجهی در دو دهه اخیر کسب کند اما این فرصت امروز به یک ضرورت تبدیل شده است به‌گونه‌ای که نمی‌توان هیچ راهکار غیرالکترونیکی‌ای برای توسعه صنعت بانکداری متصور شد.

در کنار این پیشرفت به واسطه تراکنش‌هایی که هر یک ارزش مادی فراوان دارند از یک سو چشمان ناپاک سوءاستفاده مترصد یک ضعف ذاتی یا ساختاری و فرآیندی نشسته‌اند و از دیگر سو مشکلات و نقاط ضعف غیرعاملانه نیز منجر به ضرر و زیان این صنعت می‌شوند.

این بدان معنی است که ارزش، اعتبار و صحت کارکرد فرآیندهای بانکداری در گرو تامین امنیت به ویژه در حوزه الکترونیکی است و هر خدشه‌ای به این امنیت وارد شود گاهی به تمامیت بانکداری ضربه می‌زند، نظیر افشای اطلاعات دسترسی به کارت‌های بانکی و یا حتی مسائلی که در پرونده فساد ۳۰ هزار میلیارد ریالی به واسطه ضعف‌های سیستمی و نظارتی دیده می‌شود.

ارکان صنعت بانکداری الکترونیکی سامانه‌های بانکداری اطلاعات و داده‌های بانکی و مالی، تجهیزات سخت‌افزاری و ارتباطی، پرسنل فناوی اطلاعات، پرسنل کاربر سامانه‌ها، تولیدکنندگان سامانه‌ها و تجهیزات، شرکت‌های ارائه‌دهنده خدمات پرداخت عموم کاربران سامانه‌های بانکداری هستند.

همه این ارکان در معرض دو نوع معضل امنیتی هستند، سوءاستفاده از نقاط ضعف این ارکان و رخدادهای غیرعمدی ناشی از ضعف‌های عملکردی آنها برای مثال اکثر سامانه‌های کربنکینگ (core banking) و تجهیزات اصلی شبکه بانکی منبع خارجی دارند لذا در جایی که رخدادهای امنیتی نظیر استاکس‌نت روی می‌دهد نمی‌توان انتظار داشت هیچ تهدید امنیتی در این حوزه وجود نداشته باشد.

از دیگر سو فقدان یک مرکز ریشه جهت تایید صحت امضای الکترونیکی که مورد تاکید ماده ۴۹ قانون برنامه پنجم توسعه نیز هست، چالشی است که باعث شده بسیاری از فرآیندهای تبادل اطلاعاتی را از زیرساخت امن امضای الکترونیکی محروم کند.

اما مهم‌تر از همه اینها عدم پوشش کامل فرآیندهای

بانکی توسط سامانه‌های بانکداری الکترونیکی است. نمود این مشکل در پرونده فساد بانکی مشهود است. فرآیندهای مرتبط با LCها و استعلامات آنها توسط سامانه‌های متمرکز پشتیبانی نشده لذا منجر به سوءاستفاده‌هایی می‌شود که یکی از آنها در این پرونده دیده شده است.

در کنار اینها باید عدم آشنایی کلیه عوامل انسانی درگیر با فرآیندها با مقوله امنیت فضای تبادل اطلاعات (افتا) و حتی در برخی موارد عدم آشنایی کافی با فرآیندهای الکترونیکی را ذکر کرد. سهم هزینه‌های ایجاد افتا در مقابل هزینه‌های توسعه فاوای بانک بسیار ناچیز است.

که این دو دلیل عمده دارد؛ یا دانش امن‌سازی بانکداری الکترونیکی و اهمیت آن نزد پرسنل فنی نهادینه نشده است یا هنوز این مهم به باور مدیران ارشد نظام بانکی نرسیده است.

سایر عوامل انسانی نظیر کاربران نیز به واسطه عدم آگاهی باعث رخ دادن بسیاری از مشکلات امنیتی در این حوزه می‌شوند که نمود آن در سوءاستفاده از حساب اشخاص به واسطه عدم رعایت محرمانگی کارت و رمز عبور و عدم اشراف به مقوله پرداخت‌های اینترنتی دیده می‌شود و در مورد افشای اطلاعات کارت‌ها عدم نظارت کافی نهادهای نظارتی و بانک‌ها بر ماهیت و نحوه تبادل داده‌ها بین شرکت‌های ارائه خدمات پرداخت و بانک قابل بررسی است.

راهکارهای ارتقای امنیت در حوزه بانکداری الکترونیکی را می‌توان در قالب ارکان ذکرشده به شرح زیر ارائه کرد.

عوامل انسانی:

- آموزش مداوم پرسنل فنی توسعه‌دهنده سامانه‌ها برای امن‌سازی سامانه‌ها و تبادل اطلاعات
- آموزش کاربران درون‌بانکی سامانه‌ها جهت رعایت استانداردها و دستورالعمل‌های فنی
- اطلاع‌رسانی و آگاه‌سازی به کاربران و مشتریان خدمات بانکی
- آموزش مدیران ارشد بانک‌ها جهت اهمیت امنیت و شناسایی نقاط ضعف.

سامانه‌های بانکی:

- یکپارچه‌سازی سامانه‌ها به صورت تولید بومی و غیروارداتی به نحوی که هیچ فرآیند بانکی بدون پوشش سیستمی آن انجام نشود.
- تدوین استانداردهای امنیتی و بازبینی‌های ممیزی این سامانه جهت رعایت استانداردهای نظیر sms که مورد تاکید ماده ۲۳۱ قانون برنامه پنجم توسعه نیز هست.
- رمزنگاری کلیه اطلاعات تبادلی و نیز تبادل اطلاعات منوط به امضای الکترونیکی آنها
- ایجاد و توسعه مرکز ریشه و میانی صدور گواهی
- تدوین برنامه عملیاتی آزمون‌های امنیتی درونی و بیرونی از سامانه‌ها.

شرکت‌های پیمانکار:

- انعقاد قراردادهای حقوقی به همراه ضمانت اجراهای سنگین مالی برای پیمانکاران خدمات و محصولات بانکداری الکترونیکی جهت حذف محرمانگی اطلاعات
- تدوین استانداردهای امنیتی برای رعایت آنها نزد پیمانکاران
- بازبینی تبادلات داده‌ای بین پیمانکاران و سامانه‌ها و بانک جهت پرهیز از تبادل داده‌ای که در مسوولیت حقوقی طرفین قرار ندارد یعنی داده‌ها مورد نیاز یا ضروری برای تبادل نیستند.

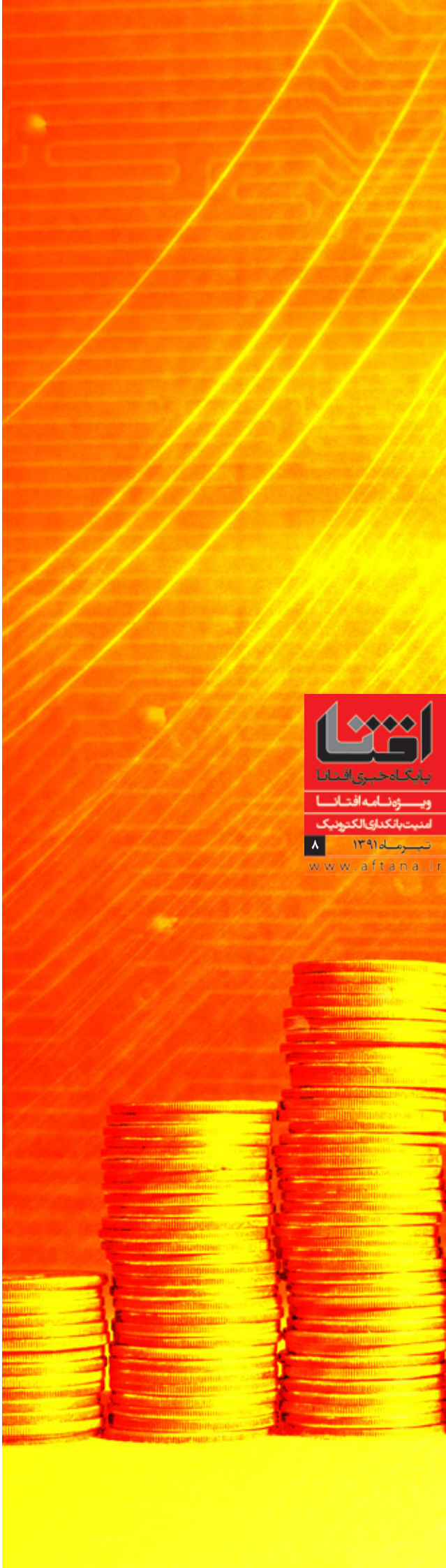
تجهیزات سخت‌افزاری و مخابراتی:

- تدوین مستندات امنیتی شبکه‌بندی و توسعه شبکه‌های ارتباطی و حفظ محرمانگی دسترسی به این تجهیزات و اجرای استقرار و توسعه شبکه‌ها بر مبنای مستندات ذکرشده
- تکیه بر راهکارهای ارتباطی امن و مطمئن ترجیحا غیرماهواره‌ای که به نوعی کل مسیر تبادل داده در اختیار کارفرما باشد.
- رمزنگاری کلیه ارتباطات بر مبنای الگوریتم‌های بومی و پیچیده
- بررسی‌های مستمر استانداردها و نیز ممیزی نقاط ضعف تجهیزات مخابراتی و سخت‌افزاری
- حذف فوری تجهیزات دارای رخنه‌های امنیتی
- ایجاد راهکارهای شبکه‌موازی و تجهیز پشتیبان‌هایی با قابلیت راه‌اندازی بدون درنگ.

اطلاعات و داده‌ها:

- پشتیبان‌گیری مستمر از داده و آزمون راه‌اندازی مجدد با استفاده از این اطلاعات
- رمزنگاری کلیه اطلاعات
- اجرای آزمون‌های امنیت دسترسی درونی و بیرونی
- حذف مکرر مازاد اطلاعات.

مرجع : هفته نامه عصر ارتباط



تخفیف ویژه
+
دوره رایگان
Security+

کهکشان مجری بزرگترین پروژه‌های آموزش امنیت اطلاعات در کشور

در راستای آماده‌سازی هر چه بیشتر کشور در مقابل تهدیدات امنیتی
کهکشان دوره‌های آموزش امنیت اطلاعات ویژه‌ای را طراحی نموده است

اولین دوره ویژه تلفیقی CEH+CISSP

Security+ CEH CISSP

خیابان سیدجمال‌الدین اسدآبادی، خیابان ابن‌سینا، نبش خیابان سی و یکم، پلاک ۱۱۱
info@kahkeshan.com تلفن: ۸۸۷۱۹۲۹۴ www.kahkeshan.com
کهکشان نور

توسعه امنیت بانکداری الکترونیکی نیازمند فرهنگ سازی است

امروزه تهدیدات سایبری در حوزه خدمات بانکی به یکی از چالش‌های اصلی تبدیل شده است. برای بررسی ابعاد این مشکلات در میزگرد تخصصی صاحبنظران به طرح دیدگاه‌ها و بیان نظرات خود پرداختند.

در این میزگرد دکتر علی جهانی (مدیر روابط عمومی بانک پارسیان)، دکتر علی عباس نژاد (مدیرعامل موسسه کهکشان نور)، مهندس مختاریان (دبیر کمیته امنیت اطلاعات شرکت توسن) و مهندس حامد قنادپور (کارشناس بانکداری الکترونیک) و علیرضا صالحی (دبیر کمیسیون افتای سازمان نظام صنفی تهران) حضور داشتند.

صاحبنظران در این میزگرد همگی بر این باور تاکید کردند که بانک مرکزی به عنوان بزرگترین و قوی‌ترین متولی در امر بانکداری الکترونیک باید بیشتر از گذشته در بحث فرهنگ سازی و آموزش کاربران نسبت به حساس سازی آن‌ها به مباحث امنیت اطلاعات بانکی وارد عمل شده و تحرک بیشتری به خرج دهد.

برای آشنایی بیشتر با دیدگاه‌های صاحبنظران حاضر در این میزگرد، مشروح این گفتگو را بخوانید.

صالحی: به عنوان سوال اول بحث را اینگونه آغاز می‌کنم که آیا در حال حاضر از دید مشتریان بانک، سامانه‌های بانکداری الکترونیک کشورمان سامانه‌های ایمنی هستند؟ با توجه به اینکه بعد از افشای اطلاعات کارت‌های بانکی، شاید سابقه خوبی در اذهان عمومی در خصوص امنیت سامانه‌های مبتنی بر بانکداری الکترونیک وجود نداشته باشد.

عباس‌نژاد: من در صحبت‌هایی که با کاربران نهایی انجام داده‌ام و تماس‌هایی که با آن‌ها داشته‌ام، به این نتیجه رسیدم که از نظر این کاربران، سامانه بانکی کشور، سامانه امنی محسوب می‌شود. چراکه اغلب آن‌ها با این سامانه فعالیت‌هایی انجام می‌دهند که شاید من خودم انجام ندهم. به طور مثال در یکی از بانک‌های کشور، بین ساعت ۹ شب تا ۹ صبح حدود ۶۰ هزار حواله اینترنتی انجام می‌شود.

عباس‌نژاد: به طور مثال در یکی از بانک‌های کشور، بین ساعت ۹شب تا ۹صبح حدود ۶۰هزار حواله اینترنتی انجام می‌شود که رقم قابل توجهی است.

انجام این تعداد تراکنش در ساعاتی که عمدتا ساعات تجاری و کاری محسوب نمی‌شود، رقم قابل توجهی است و نشان از مشارکت سطوح مختلف کاربران دارد. حتی در مورد پرداخت قبوض هم می‌بینیم که آمار تراکنش‌ها بسیار بالا است؛ اما باید گفت متاسفانه کاربران به صورت ناآگاهانه اعتماد زیادی به بسترهای الکترونیک دارند و البته در این بین بانک‌ها نیز تلاش زیادی کرده‌اند تا این اعتمادها پابرجا بماند. واقعیت هم این است که در این حوزه تا به حال اتفاق چندان جدی‌ای در کشور نیفتاده و سوءاستفاده خاصی نشده است.

صالحی: شما این حد از اعتماد را ناشی از ایمن بودن زیر ساخت‌های بانکی می‌دانید یا عدم مهارت کافی هکرها و نفوذگرها؟

عباس‌نژاد: ببینید این یک مسئله کاملا نسبی است. آگاهی هکرها و کارآمد بودن زیرساخت‌های بانکی، دو مسئله کاملا مرتبط به یکدیگر است. در کشور ما مهمترین مسئله‌ای که باعث شده است تا حدی زیادی از گزند هکرهای بین‌المللی در امان باشیم، عدم اتصال سامانه‌های ما به سامانه‌های بین‌المللی است. اگر در ایران سوئیچ‌های دیگری به جز سوئیچ شتاب وجود داشت که به ما اجازه انجام تراکنش بین‌المللی را می‌داد، قطعا وضعیت به گونه دیگری بود. اما نمی‌توان گفت که زیر ساخت‌های بانکی کشور امن نیستند؛ بلکه باید گفت امنیت لازم را ندارند و بسیاری از مباحث امنیتی هنوز در آنها رعایت نشده است. علاوه بر این کاربران هم نسبت به اینکه چه مشکلاتی می تواند برای آن‌ها اتفاق بیفتد، آگاه نیستند.

قنادپور: نظر شما در مورد اینکه مردم نسبت به اینکه چه اتفاقاتی می تواند برای آن‌ها رخ دهد، ناآگاه هستند را می‌پذیرم اما اینکه نادانسته به سامانه‌ها اعتماد دارند را به دو دلیل قبول نمی‌کنم. یکی اینکه میزان کلاهبرداری خیلی کم است. بطوریکه گرچه روزانه حدود یک میلیون تراکنش اینترنتی انجام می‌شود، اما میزان کلاهبرداری در این بخش، عددی بین ۳۶ تا ۴۰ مورد است. بخش عمده ای از این کلاهبرداری‌ها، هک نیست بلکه ممکن است به دلیل ناآگاهی کاربران که شما می فرمائید، در قالب فیشینگ انجام شود. نکته دوم روش برخورد با کلاهبرداری است. چرا که در اغلب موارد با توجه به مکانیزم‌هایی که در حال حاضر در کشور وجود دارد، کلاهبرداری‌های مختلفی پیگیری شده و البته به نتیجه هم رسیده است.

صالحی: یعنی پیگیری قضایی، به خوبی انجام می‌شود؟

قنادپور: هم پیگیری بانکی به خوبی انجام می‌شود، هم پیگیری قضایی خوبی در این زمینه وجود دارد. خوشبختانه در حال حاضر بانک‌ها همکاری خوبی با مشتریان دارند تا در صورت وقوع مشکل بتوان آن را خیلی زود بررسی و حل کرد. در نتیجه می‌خواهم به این جمع‌بندی برسم که این سطح از اعتماد مشتریان به سامانه‌های بانکداری الکترونیک، به دلیل وجود همین همکاری‌ها است.

مختاریان: حالا واقعا بانک‌ها خسارت‌های

متاسفانه کاربران به صورت ناآگاهانه اعتماد زیادی به بسترهای الکترونیک دارند.

ایجـادشـده بـرای مشتـریـان در ایـن خصـوص را جبـران می‌کننـد؟

قنـادپور: به طور مثال در بحث مغایرت‌ها، بانک‌ها صد در صد مشکلات به‌وجود آمده را کنترل و رفع می‌کنند. اما از نظر کاربر نهایی فرقی ندارد مشکل به‌وجود آمده از طریق کلاهبرداری است یا مغایرت. تنها رفع مشکل است که اهمیت دارد.

مختـاریان: البته نظر من این نیست. حتی در افشای اطلاعات سه میلیون کارت بانکی که اتفاق افتاد، بانک‌هـا متضرر نشدند.

قنـادپور: هیچ کسی متضرر نشد.

مختـاریان: در مورد ماجرای افشای اطلاعات بانکی، ابتدا همه، مسئولیت را متوجه مشتریان

قنـادپور: به نظـر من اصلا نحوه اعلام این ماجـرا به شکلی که منجـر بـه ایجـاد اضطـراب در جـامعه شد، قـابل قبول نبـود.

کردند. اینکه مشتریان می بایست رمزهای خود را عوض می کردند و باید بیشتر مراقب می‌بودند. این عکس العمل‌ها چندان مناسب نیست. در همه دنیا برای مواجهه با چنین مشکلاتی دستورالعمل‌هایی وجود دارد که نشان می‌دهد، ریسک متوجه کدام طرف است.

در یک تراکنش الکترونیک، سه بازیگر اصلی وجود دارد. بانک، فروشنده و مشتری. از این تعامل به صورت عادی فروشنده سود می‌برد و به همین دلیل هم ریسک تراکنش متوجه فروشنده است. اما در دوره‌های زمانی که خطری متوجه فروشنده نیست، چند اتفاق می‌افتد. اول اینکه بنده به عنوان صاحب کار، دائما نگران این موضوع هستم اگر کسی کارت من را داشته باشد، می‌تواند با مراجعه به یک فروشگاه، کل اعتبار کارت من را خرید کند. در واقع می‌خواهم به این نکته اشاره کنم، اینکه سامانه چقدر امن است، شاید چندان مهم نباشد اما اینکه مشتری چقدر احساس امنیت می‌کند، بسیار مهم است. در واقع اگر ما مدل ارجاع ریسک به سمت فروشنده را داشته باشیم، باعث خواهد شد فروشنده هم حساسیت‌های بیشتری در پذیرش هر نوع کارتی از خود نشان دهد. تصور نمی‌کنم در حال حاضر هیچ فروشنده‌ای هنگام پذیرش کارت از خریدار بپرسد آیا این کارت متعلق به شمـا است یا خیـر.

باید بحران را مدیریت می‌کردیم

صالحـی: به نظر می‌رسـد هم اکنون تراکنش نسبتا بالایی در بستر اینترنت در حال انجام است. شاید به دلیل اینکه یا کاربران ما چاره دیگری جز استفاده از آن ندارند و یا اینکه به شبکه بانکی اعتمـاد دارند. شاید هم کاربران ما اصلاً نمی‌داننـد باید چه انتظارات امنیتی‌ای از بانک‌ها داشته باشنـد.

عبـاس‌نژاد: متاسفانه مشکل این است که معمولا ما منتظر می‌مانیم تا اتفاق بیفتد و بعد با مشتری تماس می‌گیریم. اما اصولاً باید در لحظه انجام تراکنش مشکوک با صاحب کارت تماس گرفته شود و در خصوص تایید یا عدم تایید تراکنش از او سوال شود. حتی در برخی از بانک‌ها روی کارت‌های دبیت، صاحب کارت می‌تواند تا ۲۴ ساعت بعد، تراکنشی که مورد تائیدش نیست را به بانک اعلام کند. پس ما هم باید به نوعی عمل کنیم که به تدریج این احساس انتظار امنیتی از بانک، برای مشتری به‌وجود آید.

مختـاریان: مسئله دقیقا همین است. متاسفانه به دلیل عدم اطلاع کافی کاربران، زمانی که یک مشکل فیشینگ بوجود می‌آید، همه توجهات به سمت مشتری معطوف می‌شود.

عبـاس‌نژاد: به نظر من بانک مرکزی باید در زمینه آگاهی دادن به مردم و اطلاع رسانی به آن‌ها تحرک بیشتری داشته باشد. بانک مرکزی بخش بزرگی به نام فاوا دارد و به هر صورت بحث فرهنگ‌سازی و آموزش، وظیفه خاص این بخش است اما متاسفانه من تا به حال خروجی مشخصی در این مورد ندیده‌ام. اطلاع‌رسانی در این حوزه یک رسالت فرابانکی و تا حد زیادی متوجه بانک مرکزی است.

قنـادپور: به نظر می‌رسد متاسفانه نه تنها بانک مرکزی در این حوزه چندان موفق عمل نکرده است بلکه عملکرد انفعالی آن نیز تاثیراتی به مراتب بدتر و مخرب‌تر هم ایجاد خواهد کرد. مثال مشخص و بسیار روشن آن بحث افشای اطلاعات کارت‌های بانکی است که در همه مراحل آن بی‌تدبیری

ناآگـاهی کاربـران و عـدم توجـه بـه فرهنگ پرداخت با کارت بانکی بسیار حائـز اهمیـت است.

صورت گرفت.

مختاریان: من مثالی می‌زنم. زمانی که پلیس ایران برای اتومبیل‌های خود از بنز استفاده کرد، خیلی‌ها اعتراض کردند که خلافکاران ما ماشینی در حد بنز ندارند پس پلیس هم نیازی به خرید ماشین مدل بالا ندارد. اما در واقع این حرکت یک حرکت فعال برای نمایش اقتدار پلیس و البته القای حس امنیت بود. در حوزه بانکداری الکترونیک هم نیاز به چنین حرکتی داریم. نه اینکه زمانی به فکر خرید اتومبیل های مدل بالا بیفتیم که اتومبیل خلافکاران آنقدر پیشرفته شده که دیگر کار از کار گذشته است.

قنادپور: اگر بخواهیم به ماجرای افشای سه میلیون کارت بانکی بازگردیم، باید بگویم افشا و اطلاع‌رسانی آن به کاربران و مدیریت این بحران با بی‌تدبیری همراه بود. به نظر من اصلا نحوه اعلام این ماجرا به شکلی که منجر به ایجاد اضطراب در جامعه شد، قابل قبول نبود. حتی به نظر من این میزان التهاب اصلا ارزش این ماجرا را نداشت. چراکه بعد از این ماجرا حتی یک مورد کلاهبرداری هم گزارش نشد.

عباس‌نژاد: من هم معتقدم که نه تنها شیوه برخورد بانک‌مرکزی با این ماجرا مناسب نبود بلکه حتی بدترین روش ممکن را انتخاب کردند. متاسفانه نداشتن نقشه راه و یک مسیر روشن در مدیریت این بحران، کاملا روشن و محرز بود. با اینکه بانک مرکزی خیلی قبل از این ماجرا از این وضعیت مطلع بود ولی در این زمینه بسیار اشتباه عمل کرد.

صالحی: آقای مختاری شما در شرکت توسن به عنوان تولیدکننده نرم‌افزارهای بانکی تا چه حد می‌توانید به ایمن‌تر شدن شبکه بانکی کشور کمک کنید. در واقع تا چه حد این امکانات و اختیارات به شما داده می‌شود؟

مختاریان: اجازه دهید از نقطه نظر استانداردها توضیح دهم. به طور مثال دقیقا در حوزه سخت‌افزار، استانداردهای مشخصی در این زمینه تدوین شده است. در مرحله بعدی نیز مشخص شده است، نرم افزاری که این سخت‌افزارها را مدیریت می‌کند باید از چه ساختاری پیروی کند. در نهایت در مرحله سوم تراکنش‌ها توسط PSPها انجام می‌شود. بخشی که به ما مربوط می‌شود بخش دوم و تولید نرم‌افزار است. اگر ما در حوزه مربوط به خودمان به برخی مسائل ابتدایی و اصلی توجه نکنیم، اصلا سامانه نرم‌افزاری فعال نخواهد شد؛ البته در بخش‌هایی هم نیاز به انجام فرایندهای تحقیق و توسعه، برای تدوین متدولوژی‌های مناسب طراحی و تولید نرم افزار به خصوص با در نظر گرفتن موارد مربوط به امنیت اطلاعات داریم که طبعاً رویکرد کلی شرکت به سمت انجام موفق این موارد است.

صالحی: اجازه دهید دوباره به مسئله آگاهی‌رسانی و فرهنگ‌سازی برگردیم. در حال حاضر در اغلب موارد خریداری که برای پرداخت وجه خرید خود از کارت بانکی استفاده می‌کند معمولا باید کارت خود را به

مختاریان: در مورد ماجرای افشای اطلاعات بانکی، ابتدا همه، مسئولیت را متوجه مشتریان کردند.

فروشنده بدهد و فروشنده هم معمولا دستگاه POS خود را در محلی غیر قابل دسترس گذاشته است. پس خریدار باید رمز کارت بانکی خود را با صدای بلند به فروشنده بگوید. متاسفانه این روند در حال حاضر به یک فرهنگ تبدیل شده است.

قنادپور: نکته دقیقا همین است. یعنی همانطور که گفتم ناآگاهی کاربران و عدم توجه به فرهنگ پرداخت با کارت بانکی بسیار حائز اهمیت است. بانک مرکزی باید به امر فرهنگ‌سازی در این زمینه توجه‌کرده و وارد عمل شود. چراکه اگر بانک‌ها خودشان به تنهایی و به صورت جزیره ای اقدام به فرهنگ سازی در این زمینه بکنند، نمی‌توان امیدی به ایجاد فرهنگ صحیح در استفاده از سامانه‌های بانکداری الکترونیک داشت. پس به نظر می رسد اگر بانک مرکزی بخواهد موضع انفعالی خود را در خصوص ماجرای افشای اطلاعات سه میلیون کارت بانکی به یک موضع فعال تغییر دهد، بهترین بخش همین ورود به بحث فرهنگ‌سازی است.

حتی در افشای اطلاعات سه میلیون کارت بانکی که اتفاق افتاد، بانک‌ها متضرر نشدند.

عبـاس‌نژاد: متاسفانه بانک مرکزی در بسیاری از اعلانات امنیتی ساده هم آنطور که باید عمل‌نکرده است. به طور مثال کافیست به صفحه پرداخت الکترونیک چند بانک سر بزنید. خواهید دید که دستورالعمل‌های امنیتی هر بانک تفاوت‌های چشمگیری با یکدیگر دارند. به نظرم حداقل کار ممکن، یکپارچه‌سازی این دستورالعمل‌ها است و قطعا ساماندهی این موارد باید توسط یک نهاد حاکمیتی صورت گیرد.

قنـادپور: البته بانک مرکزی فعالیت‌هایی را در این خصوص صورت داده است. به طور مثال در بهمن ماه گذشته، بخش‌نامه‌ای را به بانک‌ها ابلاغ کرد که طی آن بانک‌ها ملزم به استفاده از token شدند. اما در حوزه‌های دیگر کماکان آنچنان که باید اقدام خاصی انجام نداده است.

به‌مشتریان‌حق‌آگاهی‌دهید

صالحـی: جناب جهانی زمانی که ماجرای افشای اطلاعات سه میلیون کارت بانکی اتفاق افتاد باید یک اطلاع رسانی کامل از جانب بانک مرکزی و یک اطلاع‌رسانی از سمت بانک‌ها انجام می‌گرفت؛ اما متاسفانه انگشت اتهام به سمت مشتری گرفته‌شد که اگر شما رمز خود را به صورت دوره‌ای تغییر بدهد طبعا تهدید جدی‌ای متوجه وی نخواهد شد. در واقع ریسک به سمت مشتری برگشت.

جهـانی: در ابتدا تشکر می‌کنم از اینکه این میزگرد را ساماندهی کرده‌اید. به خصوص موضوعی را انتخاب کرده‌اید که دیگران چندان علاقه‌ای به پرداختن به آن ندارند. چنین میزگردی می‌تواند حداقل موجبات فکر کردن روی چنین مسائلی را فراهم آورد. اما مسئله با یک سوال آغاز می‌شود و آن هم حق آگاهی مردم نسبت به یک محصول یا خدمتی است که در جامعه ارائه می‌شود. به خصوص در حوزه فناوری اطلاعات می‌بایست کلیه افراد و سازمان‌هایی که به نحوی در این حوزه فعال هستند و شبکه بزرگی را تشکیل می‌دهند نسبت به این سوال پاسخگو باشند.

برای مثال به دفترچه راهنمای استفاده از کالاهای الکترونیکی اشاره می‌کنم. همه ما این دفترچه‌ها را دیده ایم و می‌دانیم که در تشریح چگونگی کار با یک وسیله برقی ساده مثل آبمیوه گیری به حدی توضیحات داده شده است که مطالعه همه جزئیات آن خسته کننده به نظر می‌رسد. اما در روی دیگر، باید به این مسئله توجه کرد که کارخانه سازنده با این تفکر دفترچه راهنما را منتشر کرده است که مشتری هیچ تصور قبلی از این دستگاه ندارد.

بدیهی است که این نحوه برخورد، به معنی احترام گذاشتن به شعور مصرف کننده کالا یا خدمات است. متاسفانه در کشور ما نه تنها به این نکته توجه نمی‌کنیم بلکه به طور کامل آن را فراموش کرده‌ایم و اطلاع‌رسانی به مشتری چندان اهمیتی برای ما ندارد. از طرفی دیگر مسئله ورود فرهنگ استفاده از یک تکنولوژی، همزمان با ورود خود تکنولوژی به کشور مطرح می شود. متاسفانه ما در این بخش بسیار ضعیف عمل کرده‌ایم.

در مورد بانکداری‌الکترونیک هم سنگ بنای مناسبی در کشور گذاشته نشده‌است. یعنی تشویق و ترویج استفاده از دستگاه‌های خودپرداز را معادل

جهـانی: متـاسفـانه در کشـور اطلاع‌رسانـی به مشتری چنـدان اهمیتـی بـرای مـا نـدارد.

توسعه بانکداری الکترونیک در نظر گرفتیم و تبلیغات فراوانی هم در این بخش انجام‌دادیم؛ اما اطلاع رسانی و تبلیغات در خصوص فرهنگ استفاده از آن‌ها را فراموش کردیم. در حالیکه باید با ایجاد الزامات قانونی این روند را تسریع کرد.

در بانک پارسیان مفتخریم اعلام کنیم، نسبت به سال اول تاسیس بانک، یعنی حدود ۱۰ سال پیش تاکنون، نسبت درصد صدور سندهای مالی در شعب، نسبت به تراکنش‌های غیرحضوری ۲۰ به ۸۰ است. یعنی حداقل ۸۰ درصد تراکنش‌ها غیرحضوری انجام شده است. اما اینکه چرا هنوز هم در شعب شلوغی و ازدحام وجود دارد، به دلیل کمبود شعب است که قصد داریم با اعمال برنامه‌های توسعه‌ای، آن را نیز مرتفع کنیم. با ذکر این مقدمه می‌خواهم بگویم تنها نمی‌توان از یک مجموعه حتی بانک مرکزی انتظارداشت یک‌تنه وارد بحث فرهنگ‌سازی شود. به نظر می‌آید باید یک اجماع، یک همفکری عمومی و یک دغدغه مشترک بین همه PSPها، بانک‌های خصوصی، بانک‌های دولتی و... ایجاد شود تا مسئلـه فرهنگ‌سازی به نتیجه مطلوب برسد.

بعد از افشای اطلاعات بانکی، بنده مقاله‌ای نوشتم

باید اتفـاقات کوچکتـر امنیتـی که در حـوزه بانکـداری الکترونیـک رخ می‌دهـد، به نوعی هشدار تلقی شود.

افتا
پایگاه خبری افتا
ویـژه‌نامه افتـا
امنیت بانکداری الکترونیک
نیـرمـاه ۱۳۹۱
۱۴
www.aftana.ir

و در آن ذکر کـردم که این اتفاق یک هشـدار برای جامعـه بانکی و مردم ما بود. در واقـع این اتفـاق مسئـولیت همـه را بـرای جلوگیـری از پیشـامد مجدد آن بیشتـر می‌کند.

به عقیده من بانک مرکزی با انتشـار اطلاعیـه خود پس از افشـای اطلاعات، مشکلات زیـادی در هجوم مردم به سمت عابر بانک‌ها ایجاد کرد. برای جلوگیری از بروز مجدد چنین مشکلات و بحران هایی باید قبل از بروز بحران یک برنامه معینی توسط سازمان‌های دست اندرکار تدوین شود.

اولین واکنش؛ انکار مشکل

صالحـی: نکته‌ای که در این بین باید به‌آن اشاره کرد این است که سیستم حال‌حاضر بانکی کشور، کلیه ریسک‌هـا را به گـردن مشتـری انداخته است و مشتری هم چاره

صالحـی: متاسفانه اولین واکنش بانک‌هـا در خصـوص مخـاطرات بـانکـی، انکـار موضـوع اسـت.

دیگری جز پذیرش این مسئله ندارد. بانک‌ها و بانک مرکزی هم در این خصـوص فعـالیت خاصی انجام نداده است. پس عملا مشتـری است که باید همه خسـارت‌ها را تقبـل کند.

جهـانی: نظر من هم این است که باید به این مسئله قبل از بروز بحران پرداخته شود نه در هنگام وقوع آن. باید اتفاقات کوچکتر امنیتی که در حوزه بانکداری الکترونیک رخ می‌دهد، به نوعی هشدار تلقی شده و توجه جدی به آن کرد. چراکه مدیریت تراکنش‌ها و همچنین حفظ اطلاعات حساب‌های کاربران بسیار مهم و جدی است و هرگونه خلل در آن‌ها بحران محسوب می‌شود.

قنـادپور: اگر بخواهیم از منظر کلان‌تری به مسئله نگاه کنیم، متاسفانه فرهنگ جامعه ما به نحوی شکل گرفته است که معمولاً سازمان‌ها و نهادها در برخورد با هر نوع بحرانی، در اولین واکنش آن را انکار می‌کنند و تاکنون متولی مشخصی در خصوص اصلاح این روند نیز وجود نداشته است.

بانک مرکزی قدرت بالایی دارد که با ورود به هـر حوزه‌ای می‌تواند خودش را نشان دهد و اثر مثبت فراوانی در این حوزه داشته‌باشد. نمونه این قدرت نمایی را می‌توان در اغام بانک‌ها، تاسیس شاپرک و ... دید. حال سوال اینجاست که این بانک با این حد از قدرت، آیا نمی‌تواند اقدام جدی در خصوص ارتقا سطح امنیت سامانه‌های بانکی انجام دهد؟

عبـاس‌نژاد: البتـه بانک مرکـزی در مـرداد مـاه سـال ۸۸ آیین نامه‌ای را با عنـوان الزامـات مدیریت امنیت اطلاعات در حـوزه بانک‌هـا و موسسـات مالی و اعتبـاری تدوین کـرد که روند نگارش آن از سال ۸۶ آغاز شده بود. در همـان متن ذکر شده بـود ظرف شش ماه آینده آئین‌نامه اجرایی آن نیز ابلاغ می‌شود اما متاسفـانه هیچ وقت این اتفـاق نیـافتاد.

جهـانی: به نظر من مشکل اینجاست که دقیقاً همزمان با بروز یک بحران مباحث مختلفی برای مواجه با آن مطرح و در نهایت منجر به ایجاد حرکتی بین افراد و سازمان‌های مرتبط می شود ولی متاسفانه پیگیری‌های بعدی در خصوص به نتیجه رساندن آن انجام نمی‌شود. به اعتقاد من مسئله امنیت سامانه های بانکی اگر مسئله مهمی است نباید رها شود؛ قبل از هر کسی بانک‌ها، باید از بانک مرکزی بخواهند که این ماجرا را پیگیری کرده و تکاپوی مناسبی را در نهادهای حاکمیتی ایجاد کند.

مختـاریان: اگر ما چیزی را از پایه به درستی نسازیم بعدا نیز اصلاح آن بسیار سخت خواهد شد. به طور مثـال هم اکنـون بسیـاری از کاربران سایت‌هـای اینترنتی، زمانی که در مراجعه به سایت با خطای گواهینامه امنیتی مواجه می‌شوند، به راحتی از آن عبور می‌کنند. چرا؟ چون از ابتدا این بی‌توجهی در بین آن‌ها شکل گرفته و جا انداختن این فرهنگ که اگر به درستی با این خطا روبرو نشویم، احتمالا در کلاهبرداری فیشینگ گرفتار خواهیم شد، بسیار سخت است.

قنـادپور: به هر ترتیب ما با یک موج و جریانی روبرو شده‌ایم که چگونگی برخورد با آن بسیار مهم است. از آنجائیکه در نقطه خاصی از شروع رشد استفاده از سامانه‌هـای بانکداری الکترونیک و یا پول‌های الکترونیک قرار گرفته‌ایم، باید به نحوی اطلاع‌رسانی کنیم که اعتماد مردم نسبت به سیستم بانکی کشور سلب نشود.

در این راستا همچنین رسانه‌ها و مسئولان باید خیلی سریع به فکر ایجاد ساز وکاری برای جبران خسارت‌های احتمالی ناشی از کلاهبرداری‌های الکترونیک‌باشند.

متاسفـانه اولیـن واکنـش بانک‌هـا درخصوص مخاطرات بـانکی، انکار موضـوع است.