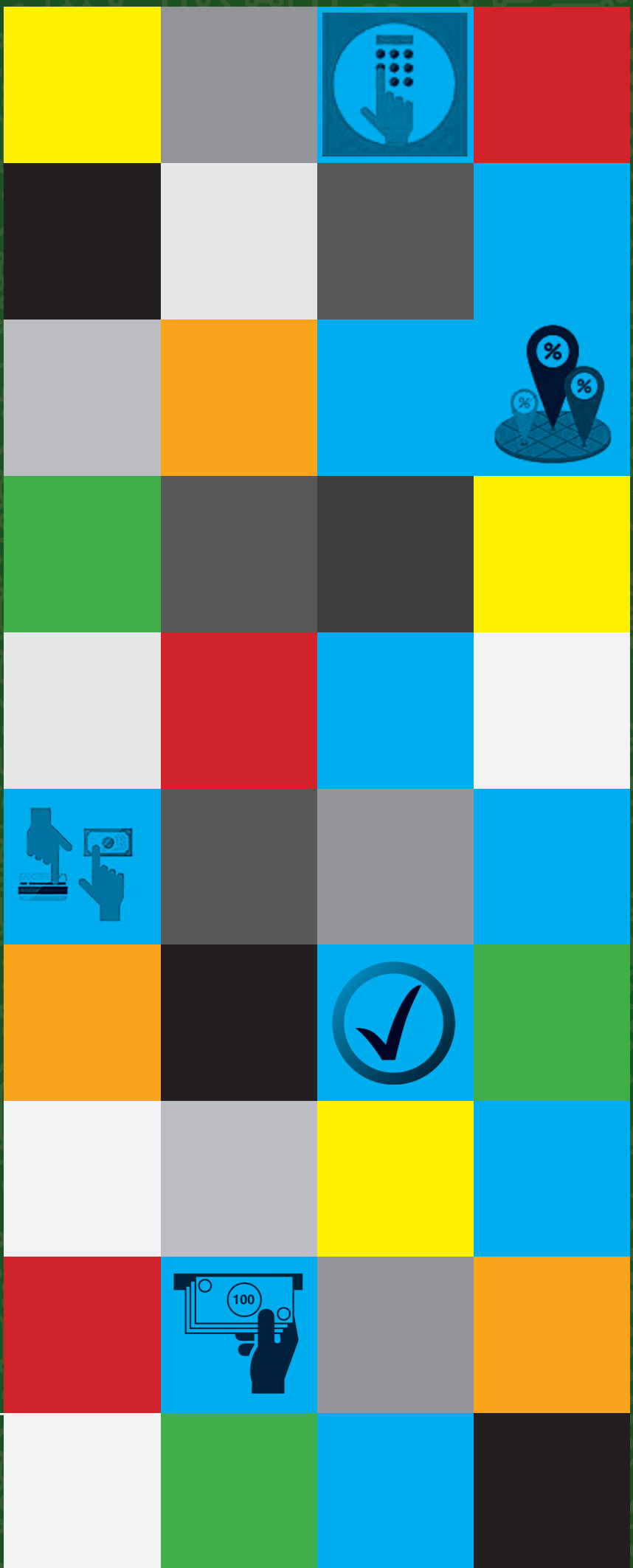
بانک کشاورزی

پیام بر

ویژه‌نامه

بانکداری الکترونیک



۲

آذر ۱۳۹۲

پیام صبر

نشریه داخلی بانک کشاورزی

ویژه بانکداری الکترونیک
بخش دوم

صاحب امتیاز: بانک کشاورزی

مدیر مسئول: خسرو صادقزاده

سردبیر: مرتضی مهدویان

مدیر داخلی: مرضیه امیری

اداره‌کل روابط‌عمومی

سرنوشت

ضرروتی به نام امنیت

همه چیز از اطلاعیه روز شنبه ۲۶فروردین ماه سال گذشته بانک مرکزی، برای افکار عمومی جدی شد. بانک مرکزی در وب‌سایت خود به مردم توصیه کرد که بیایند و رمز کارت اعتباری و بانکی خود را برای موارد ایمنی تغییر دهند. روابط‌عمومی بانک مرکزی اعلام کرد که به اطلاع می‌رساند در پی بروز برخی شایعات در فضای مجازی و به‌منظور ارتقای سطح ایمنی، ایجاد محدودیت در دسترسی غیرمجاز در شبکه کارتی کشور و حفاظت مشتریان در مقابل مخاطرات احتمالی ناشی از آن، به بانک‌های کشور ابلاغ شده ضمن اعلام مراتب به دارندگان کارت‌هایی که طی چند ماه گذشته رمزخود را تغییر نداده‌اند، با مراجعه به خودپردازها یا شعب بانک مربوط نسبت به تغییر رمز کارت اقدام کنند. این اطلاعیه «مهم» بانک مرکزی سبب ایجاد ابهاماتی جدی در میان مردم و دارندگان کارت‌های بانکی کشور شد و بلافاصله شایعات که البته بعدا به شکلی به واقعیت پیوستند آغاز شد. ماجرا از این قرار بود که یکی از مدیران سابق یکی از شرکت‌های ارائه‌کننده خدمات کارت‌های بانکی، پس از خروج از کشور اطلاعات بیش از ۳میلیون کارت متعلق به بانک‌های مختلف کشور را روی وبلاگ خود در اینترنت منتشر کرد.

با اینکه طی این درز اطلاعات امنیتی، به هیچ‌کدام از مشتریان شبکه بانکی و دارندگان انواع کارت‌ها خسران وارد نشد و بانک‌ها با اقدام‌های ضرب‌العجلی، راه را بر سوءاستفاده‌کنندگان احتمالی بستند؛ اما چنان آسیبی به حسن شهرت بانک‌های کشور وارد شد که تا سال‌ها باید برای جبران آن تلاش کنند. ازاین‌رو چنین اتفاقی مقوله امنیت در بانکداری الکترونیک را ضرورتی دوباره بخشید.

بانک کشاورزی در راستای این مهم، ضمن بومی‌سازی نرم‌افزارهای موجود، امنیت را در شبکه خود تا سطح چشمگیری افزوده است. در ویژه‌نامه حاضر که ویژه‌نامه شماره دو با موضوع بانکداری الکترونیک به‌شمار می‌رود، ضمن بررسی ریسک‌ها و تقلب‌های موجود بانکی در فضای مجازی، آخرین دستاوردهای بانک کشاورزی در راستای ارائه خدماتی ایمن به مشتریان به بحث گذاشته شده است.

در گفت‌وگو با یک عضو هیئت‌مدیره بانک کشاورزی مطرح شد؛

توسعه بانکداری الکترونیک در گروی فرهنگ‌سازی و آموزش مستمر

بانکداری الکترونیک در ایران در مسیری قرار گرفته است که هر روز خدمات و سرویس‌های جدید را ارائه می‌کند؛ اما استفاده حداکثری از این سرویس‌ها و خدمات از سوی مشتریان سیستم بانکی نیازمند آموزش و فرهنگ‌سازی مداوم است. حشمت‌اله نظری، عضو هیئت‌مدیره بانک کشاورزی در گفت‌وگویی، توسعه سرویس‌های جدید بانکداری الکترونیک را مستلزم آموزش مستمر و فرهنگ‌سازی در این حوزه می‌داند. مشروح گفت‌وگو با این عضو هیئت‌مدیره بانک کشاورزی را بخوانید:

صحبت را با بانک کشاورزی آغاز کنیم. با توجه به اینکه به اذعان کارشناسان سیستم بانکی، بانک کشاورزی بانکی پیشرو در زمینه استقرار بانکداری الکترونیکی در کشور به‌شمار می‌رود، مهم‌ترین ویژگی بانکداری الکترونیکی بانک کشاورزی را چه می‌دانید؟

بانک کشاورزی درحوزه خدمات بانکداری الکترونیک، قدم در راهی نهاد که خدماتی متمایز به مشتریان سیستم بانکی ارائه دهد و تمام نیازهای آنها را پوشش دهد. برای رسیدن به نقطه‌ای هم که امروز در آن قرار دارد، بانک هزینه داده است. ولی امروز به جایی رسیده‌ایم که نه‌تنها کارشناسان و مسئولان شبکه بانکی که بانک‌های دیگر نیز به این نکته اذعان دارند که بانک کشاورزی تنها موسسه مالی کشور است که نسل چهارم بانکداری الکترونیک را عملیاتی کرده است.

با توجه به اینکه شما از سال‌های دور با بانک کشاورزی همراه بوده‌اید، چه نیازی در بانک احساس شده که به‌سوی توسعه بانکداری الکترونیک برود و درنهایت چه پروسه‌ای پشت سر گذاشته شد تا جامع‌ترین سیستم بانکداری الکترونیک را بانک کشاورزی ارائه کند؟

بانک کشاورزی در سال ۱۳۸۰، چهار چرخش استراتژیک انجام داد که یکی از آن چرخش‌ها، حرکت به سمت بانکداری الکترونیک بود. از آن جا که می‌دانستیم ورود به دنیای مدرن بدون بانکداری نوین امکان‌پذیر نیست، از همان زمان اقدام‌هایی برای پیاده‌سازی این نوع بانکداری در بانک کشاورزی شروع شد. هر چند که این نوع از بانکداری از سالیان گذشته در دنیا مطرح بوده و در ایران به دلایل مختلف یا پیاده‌سازی نشده یا اینکه مطابق الگوهای جهانی پیش نرفته است. در اولین حرکت برای ارائه خدمات نوین بانکی در آن مقطع (سال ۱۳۸۱) به سراغ شرکت‌های داخلی رفتیم و بخش حساب های جاری در Core Banking را شروع کردیم. از آن جا که بانکداری نوین در یک حرکت استراتژیکی باید تمام نیازهای بانک را مرتفع کند، در همان مقطع احساس کردیم که شرکت داخلی طرف قرارداد، توانایی پاسخگویی به تمام نیازهای بانک را ندارد، در نتیجه از سال ۱۳۸۲ به‌طور جدی مطالعه امکانات داخلی کشور و همچنین امکانات بیرون از کشور، برای استقرار کامل Core Banking در دستور کار بانک کشاورزی قرار گرفت. کارشناسان این بانک پس از مطالعات عمیقی که حدود یک سال طول کشید، به این نتیجه رسیدند که شرکت‌های داخلی توان لازم برای برآورده کردن خواسته‌های این بانک از قبیل سپرده‌ها، تسهیلات، وصول مطالبات، انواع کانال‌های ارتباطی مشتریان با بانک و ... را ندارند، ازاین‌رو بانک از طریق برگزاری مناقصه بین‌المللی شرکت FNSرا که برنده مناقصه شده بود، برای پیاده‌سازی کامل سیستم Core Banking انتخاب کرد.

آیا این نرم‌افزار توان ارائه خدمات را در تمام محصولات و خدمات بانکی داشت یا اینکه فقط به ارائه خدمات خاص و محدود می‌پرداخت؟

این نرم‌افزار تمام فعالیت‌های مرتبط با مشتری در بانک را پوشش می‌داد. مزیت برتر این نرم‌افزار هم همین مهم بود که تمام خدمات را به‌صورت یکپارچه ارائه داده و از فعالیت جزیره‌ای سیستم‌ها جلوگیری می‌کرد.

با وجود چنین امکانی که بانک کشاورزی به آن دست یافته است، هنوز خدمات بانکداری الکترونیک در عموم موسسات مالی به‌طور پراکنده و نه در قالب یک سیستم جامع ارائه می‌شود. به‌نظر شما موانع عمده استقرار بانکداری الکترونیکی نسل نوین در بانک‌ها چیست؟

یکی از عمده‌ترین مشکلات در پیاده‌سازی بانکداری نوین، نبود نیروی انسانی متخصص در زمینه پشتیبانی سخت‌افزاری و طراحی نرم‌افزارهای مورد نیاز است که برای رفع این مشکل در حال حاضر اقدام‌هایی برای تربیت نیروی انسانی در دانشگاه‌ها شروع شده و امیدواریم با توجه به رشته‌های مورد نیاز بانک‌ها، در آینده‌ای نزدیک، محدودیت نیروی انسانی برای بانکداری الکترونیکی برطرف شود. مانع دیگر، تهیه سخت‌افزارهای مورد نیاز بانکداری نوین است و همچنین می‌توان به بسترهای ارتباطی اشاره کرد که در حال حاضر با کمک وزارت ارتباطات و فناوری اطلاعات بخشی از این مشکل‌ها برطرف شده است.

نقش آموزش و فرهنگ‌سازی برای استفاده از خدمات بانکداری الکترونیکی را تا چه اندازه موثر می‌دانید، آیا به صرف وجود سخت‌افزارها و امکان خدمات و محصولات نوین بانکی، می‌توان به گسترش و توسعه بانکداری نوین امید داشت؟

خیر، فقط با وجود نرم‌افزارها و سخت‌افزار نمی‌توان بانکداری نوین را توسعه داد، بلکه نکته بسیار مهم توجه به بحث آموزش و فرهنگ‌سازی است. در این مسیر باید به این نکته هم توجه داشت که تنها با تبلیغات نمی‌توان به استفاده از خدمات نوین بانکی امیدوار بود. فرهنگ استفاده از خدمات الکترونیکی بانکی باید در افراد نهادینه شود و فقط از این طریق می‌توان امیدوار بود که افراد به استفاده از خدمات نوین بانکی روی بیاورند، زیرا با نهادینه شدن آن و انتظارات جدید مشتریان، بانک‌ها

را نیز وادار به ارائه خدمات جدید خواهد کرد، به این ترتیب می‌توان انتظار داشت که بانکداری الکترونیک با سرعت خوبی توسعه یابد.

پیشنهاد شما برای آموزش و فرهنگ‌سازی در حوزه بانکداری الکترونیک چیست؟

به اعتقاد من حذف پول فیزیکی و رسیدن به پول الکترونیکی مستلزم نهادینه‌شدن فرهنگ استفاده از خدمات نوین بانکی است که یکی از معتبرترین روش‌های رسیدن به این هدف، آموزش دانش‌آموزان در مقاطع تحصیلی گوناگون است. همان‌گونه که تحقیقات نیز نشان داده است، انتقال مفاهیم نوین از طریق کودکان در خانواده‌ها بسیار راحت‌تر از روش‌های دیگر است و از همین رو باید با کمک آموزش و پرورش واحدهای درسی و محتوا بانکداری الکترونیک به کتاب‌های درسی دانش‌آموزان اضافه شود. از سوی دیگر باید در محتواهای درسی رشته‌های دانشگاهی نیز بازنگری و حتی رشته‌های جدید و مرتبط با بانکداری الکترونیک به رشته‌های دانشگاهی اضافه شود. به نظر من در فرهنگ‌سازی و آموزش خدمات نوین بانکی، رسانه‌ها به‌ویژه رسانه ملی، از اهمیت ویژه‌ای برخوردار است، چراکه مخاطبان این رسانه به‌دلیل گستردگی زیاد به‌راحتی می‌توانند با مفاهیم نوین بانکی آشنا شوند. هرچند که در حال حاضر تبلیغاتی جسته و گریخته در این زمینه انجام می‌شود، اما به‌علت نبود تداوم و آموزش چگونگی استفاده از خدمات نوین بانکی، خیلی از انتظارات برآورده نمی‌شود. از سوی دیگر مهم‌ترین عاملی که می‌تواند سبب گسترش خدمات الکترونیکی بانکی بین مشتریان شود، ارائه سرویس‌ها با کیفیت بالاست و اطمینان دادن به مشتریان که در برخورد با کوچک‌ترین مشکل می‌توانند در کمترین زمان ممکن خدمت مورد نیاز خود را دریافت کنند.

کارکردهای شرکت گسترش فناوری‌های نوین کشاورز در پیشگامی بانکداری الکترونیک بانک کشاورزی؛

فراتر از نیاز مشتری بودن با ارائه سرویس‌های خاص

در فضای به‌شدت رقابتی بانکداری امروز؛ اگر نیاز مشتری را برآورده نکنید، مشتری را از دست خواهید داد. اگر مشتری به اندازه نیازش از شما سرویس و خدمت دریافت کند، از شما راضی خواهد بود. اما اگر فراتر از انتظار مشتری باشید و سرویس‌هایی به او ارائه دهید که مشابهش را هیچ کجا ندیده، چنان به وجد می‌آید که به مشتری ثابت شما تبدیل خواهد شد. این اصل سوم یا همان به وجد آوردن مشتری، اصلی است که مدیرعامل شرکت نوین‌کشاورز بر آن تاکید دارد و معتقد است سیاست‌های شرکت گسترش فناوری‌های نوین کشاورز برای حفظ بازار بانک کشاورزی بر اصل فراتر از انتظار مشتری بودن استوار است.

هنگامی که از نسل‌های بانکداری الکترونیک در دنیا صحبت به میان می‌آید، چهار نسل مطرح است که نسل چهارم، نسل سیستم‌های متمرکز یا کربنکینگ است. نسل یک، دو و سه هر کدام شرایط و اقتضائات خاص خود را داشته و دوره‌های بلوغ خود را پشت سر گذاشته‌اند و فرصت حاضر، جای پرداختن به آنها نیست. اما اینکه چرا عنوان می‌شود بانک کشاورزی، بانک پیشرو در نسل چهارم بانکداری الکترونیک است، موضوعی بود که به بهانه آن به سراغ مسعود آتشی، مدیرعامل شرکت نوین‌کشاورز رفتیم و کارکردهای شرکت گسترش فناوری‌های نوین کشاورز را در این پیشگامی جویا شدیم.

او در اشاره‌ای کوتاه به عقبه استقرار نسل چهارم بانکداری الکترونیک در بانک کشاورزی گفت: بعد از اینکه تصمیم به داشتن چنین سیستمی در بانک کشاورزی نهایی شد، سفری را در سیستم بانکی آغاز کردیم تا برسیم به اینکه چه می‌خواهیم و چطور باید به آن برسیم. اما امروز دیگر از آن دوران گذر کرده و به دوران بهره‌برداری از کاشته‌های‌مان رسیده‌ایم. به این معنا که زمانی بانک کشاورزی برای پیاده‌سازی این سیستم هزینه داد و این هزینه هم به این شکل بود که شاید در برخی سرویس‌ها و خدمات از برخی بانک‌ها کندتر حرکت کرد؛ اما امروز به جایگاهی برتر در سیستم بانکی رسیده که مجموعه‌ای از خدمات را در قالب یک سیستم واحد به مشتریان ارائه می‌کند و از این جهت در سیستم بانکی یک نمونه یگانه به‌شمار می‌رود و به جرات می‌توان ادعا کرد که تنها بانک ایرانی است که نسل چهارم بانکداری الکترونیک را عملیاتی و اجرایی کرده است.

به گزارش پیام‌مهر؛ باید به یک نکته توجه ویژه‌ای شود، با اینکه بارها و بارها هم به آن اشاره شده است. این نکته آن است که بانک‌ها و موسسات مالی زیادی مدعی هستند که سیستم یکپارچه و متمرکز بانکداری الکترونیکی را دارند و آن را عملیاتی کرده‌اند. اما تنها بانکی که به جرات می‌توان گفت کربنکینگ را به‌معنای واقعی عملیاتی کرده بانک کشاورزی است. چنانکه سال گذشته وزیر محترم اقتصاد و دارایی وقت، طی بازدید و سفری که درون نظام بانکی کشور داشتند به این نکته اشاره کردند که کربنکینگ یا سیستم جامع متمرکز بانکداری الکترونیک تنها در بانک کشاورزی عملیاتی شده است. این اقدامی هم که در بانک کشاورزی به منصه‌ظهور رسیده نه‌تنها خدمتی به بانک کشاورزی که خدمتی به شبکه بانکی کشور و گامی موثر در راستای توسعه سیستم‌های بانکداری در کشور است. مسعود آتشی در این رابطه افزود: سیستم‌های مشابهی که در بانک‌های دیگر به تبعیت از بانک کشاورزی پیاده‌سازی شده است، یک تفاوت عمده دارد و آن عدم جامعیت یا متمرکز نبودن آن است. چنان‌که سیستم‌های عملیاتی شده به‌صورت بخش‌های متفاوت بوده و هر کدام به‌صورت جزیره‌ای واحد کار می‌کنند. این در حالی است که در سیستم جامع و متمرکز مهرگستر که ماژولار می‌باشد تمام نیازهای بانکی الکترونیک دیده شده و هر خدمت جدیدی هم که در بانک تعریف می‌شود در همان سیستم کربنکینگ جای می‌گیرد.

آتشی در ادامه بر هزینه‌های که بانک کشاورزی برای استقرار این سیستم در بانک متحمل شد، تاکید کرده و خاطرنشان کرد: بانک کشاورزی پیش‌تر با راه‌اندازی سیستم مهر در نسل سوم بانکداری الکترونیکی هم پیش‌رو بوده است. اما به‌واسطه تمرکز بر سیستم متمرکز و جامع بانکداری الکترونیک یا همان نسل چهارم، به اذعان برخی از روند حرکتی نظام بانکی در نسل سوم کمی عقب ماند. این روند طبیعی بود، چراکه بانک کشاورزی

آگاهانه قدم در راهی نهاده بود که امری متمایز از آنچه هست را در نظام بانکی کشور عملیاتی کند. در نتیجه امروز می‌بینیم که بانک کشاورزی به حاصلی در این حوزه دست یافته و توان ارائه خدماتی در بانکداری الکترونیک را دارد که در نظام بانکی کشور بی‌مانند است.

شرکت نوین کشاورز: مولود بانک کشاورزی، خدمتی به نظام بانکی

مسعود آتشی در رابطه با تولد شرکت گسترش فناوری‌های نوین کشاورز هم اشاره‌هایی داشت. او گفت: طی سال‌های ۱۳۸۶ و ۱۳۸۷ احساس شد که نیاز به شرکتی داریم که مختص بانک نباشد و در حوزه بانکداری الکترونیکی دست به تولید دانش و فناوری مطابق نیازهای بانکی بزند. از سوی دیگر در بانک کشاورزی به دانشی دست یافته بودیم که در نظام بانکی کشور بی‌مانند بود و ضرورتی نداشت که این دانش تنها در اختیار بانک کشاورزی باشد و باید به‌عنوان خدمتی به نظام بانکی کشور عرضه می‌شد. این دو عامل دست به دست هم داد تا شرکت گسترش فناوری‌های نوین کشاورز شکل بگیرد. علاوه بر آنچه تاکنون به آن رسیده‌ایم، هر روزه بانک کشاورزی به‌واسطه فعالیت شرکت گسترش فناوری‌های نوین کشاورز به نوآوری‌ها و داشته‌های تکنولوژیکی زیادی دست پیدا می‌کند و این داشته فراتر و بزرگ‌تر از آن است که تنها در یک بانک محبوس شود و عرضه این دانش‌ها و خدمات می‌تواند توسعه‌ای در صنعت بانکداری کشور ایجاد کند.

مدیرعامل شرکت گسترش فناوری‌های نوین کشاورز افزود: نظر به موارد مطرح شده، فکر ایجاد یک شرکت مستقل پرورش یافت تا اینکه در نهایت شکل اجرایی به خود گرفت. بخشی از کارکنان شرکت گسترش فناوری‌های نوین کشاورز را همان همکاران بخش فناوری اطلاعات بانک تشکیل می‌دهند. این افراد که هسته تولید دانش و ایده در شرکت گسترش فناوری‌های نوین کشاورز به‌شمار می‌روند، رشدیافته در دامان سیستم جامع و متمرکز مهرگستر هستند، با توانمندی‌های این سیستم هماهنگ شده و افق دید وسیعی پیدا کرده‌اند. بخش دیگر کارکنان شرکت گسترش فناوری‌های نوین کشاورز را افرادی تشکیل می‌دهند که به مرور به سیستم تزریق شده و در این مجموعه به پختگی رسیده‌اند. البته بخش دوم و یا همکارانی که از بیرون به مجموعه تزریق شده‌اند، همگی افراد صاحب فکر و ایده و نخبگانی بوده‌اند که بنا بر احساس نیاز به مجموعه افزوده شدند. به هر حال، مجموعه‌ای که روزی تعداد کارکنانش حدود ۲۰ نفر بود، اکنون به مجموعه‌ای بزرگ با حدود ۴۰۰ نفر نیرو تبدیل شده است.

اینک مجموعه شرکت گسترش فناوری‌های نوین کشاورز به مجموعه‌ای بزرگ و صاحب فکر، ایده و خلاقیت تبدیل شده و این توانایی را دارد که نه‌تنها نیازهای و ضروریات بانک کشاورزی در حوزه بانکداری الکترونیک را پاسخ گوید، که برای خلاءهای موجود در نظام بانکی هم برنامه داشته باشد. بنابراین در هدف‌گذاری‌های شرکت گسترش فناوری‌های نوین کشاورز این مهم وجود دارد که به نظام بانکی کشور خدمت و سرویس ارائه کند. البته ذکر این موضوع هم ضرورت دارد که امروزه شرکت گسترش فناوری‌های نوین کشاورز با وجود راه‌اندازی دفاتر استانی، تبدیل به مجموعه‌ای شده که توان ارائه هر نوع خدمت و سرویسی را به موسسات مالی در هر نقطه از کشور دارد. آتشی در رابطه با محصولاتی که شرکت گسترش فناوری‌های نوین کشاورز توان تولید آنها را دارد، تصریح کرد: محصولات شرکت گسترش فناوری‌های نوین کشاورز مشتمل بر موارد متعددی است که سیستم متمرکز بانکداری الکترونیک یا همان کربنکینگ تنها یکی از این موارد است. او اشاره کرد که بسیاری از نرم‌افزارهای ویژه حوزه بانکی مانند بخش پرداخت، وصول، نظارت و بازرسی، اوراق بهادار، اینترنت‌بانک، نظارت بر طرح‌ها و... توسط شرکت طراحی و تولید شده و در حال استفاده است. علاوه بر این توانایی تولید محصولات سفارشی ویژه مشتریان هم در شرکت وجود داشته و در حوزه سخت‌افزار و شبکه نیز قابلیت ارائه خدمت را دارد.

او همچنین افزود: البته ما همواره در حال پویایی، به‌روز شدن و داد و ستد اطلاعات با مراکز دانش‌بنیان هستیم. همین روند به ما کمک می‌کند همواره به‌روز بوده و در نوآوری در شبکه بانکی پیشگام باشیم. در این مسیر دو رویه جداگانه در نظر گرفته می‌شود. نخست اینکه ضرورت‌ها و نیازهای داخلی را بررسی کرده و برای پاسخ به آنها چاره‌جویی می‌کنیم و سپس نگاهی تیزبینانه به پیشرفت‌ها و نوآوری‌های روز جهان در این زمینه داریم تا روند پویایی خود را به‌صورت مستمر حفظ کنیم.

مدیرعامل شرکت گسترش فناوری‌های نوین کشاورز در بخش دیگری از گفته‌هایش به فروش محصولات جدید در حوزه بانکداری اشاره کرد و عنوان کرد: مقوله تولید نرم‌افزار، سیستم و خدمت یک مقوله جداگانه است و مقوله فروش آن مبحث جداگانه دیگر؛ چنانکه شرکت گسترش فناوری‌های نوین کشاورز این خدمات نوین در حوزه بانکداری الکترونیک را تهیه کرده و برای فروش در اختیار امور مشتریان بانک‌ها قرار می‌دهد و اینکه چگونه این سرویس‌ها به فروش می‌رسند را آنها تعیین می‌کنند. اما شرکت در بازارشناسی و کمک به امور مشتریان برای فروش این محصولات بیکار ننشسته و سیاست‌هایی را طراحی می‌کند.

او در اشاره به طراحی این سیاست‌ها گفت: آنچه برای امور مشتریان بانک‌ها در حوزه بانکداری الکترونیک ارزش ایجاد می‌کند، مزیت‌های اضافی است. شرکت گسترش فناوری‌های نوین کشاورز درصدد است برای کمک به امور مشتریان سرویس‌ها و خدمات جدیدی را طراحی کرده و اجرایی کند تا مشتری بیش از نیاز خود از بانک خدمات دریافت کند و این عاملی باشد برای جذب مشتری بیشتر؛ این رویه را در علم بازاریابی فراتر از انتظار مشتری می‌نامند.

آتشی در پایان از تولید خدمات و برنامه‌های خاص بانک کشاورزی در حوزه بانکداری الکترونیک خبر داد و افزود: در راستای جذب مشتریان جدید و حفظ مشتریان کنونی در مسیر تولید خدمات خاص بانک کشاورزی هستیم. البته با توجه به اینکه دوره و خاص بودن خدمات در حوزه بانکداری الکترونیک کوتاه است و نظر به فضای رقابتی حوزه بانکداری، این سرویس‌ها به‌سرعت در بانک‌ها و موسسات مالی دیگر هم اجرایی می‌شوند، باید همواره پویا بوده و هر از گاهی خدمت جدیدی را ارائه کنیم تا فراتر از انتظار مشتری باشیم.

محصولات شرکت گسترش فناوری‌های نوین کشاورز مشتمل بر موارد متعددی است که سیستم متمرکز بانکداری الکترونیک یا همان کربنکینگ تنها یکی از این موارد است. آتشی اشاره کرد که بسیاری از نرم‌افزارهای ویژه حوزه بانکی مانند بخش پرداخت، وصول، نظارت و بازرسی، اوراق بهادار، اینترنت بانک، نظارت بر طرح‌ها و... توسط شرکت طراحی و تولید شده و در حال استفاده است

امنیت آی‌تی بانک کشاورزی در گفت‌وگو با رئیس اداره امنیت آی‌تی بانک؛

کلاه سفیدها نمی‌خوابند

چنـدان مهـم نیسـت که چـه تعداد هکـر و متقلـب شـبکه بانکـداری الکترونیـک در دنیـا وجـود دارد، که مهـم توانایـی حفـظ امنیت سیسـتم و شناسـایی تقلب‌ها و راه‌هـای نفوذ کلاهبرداران شـبکه مجازی اسـت؛ وظیفـه مهمـی که امـروزه در شـبکه‌های امنیتـی و حفاظتی در فضـای مجازی بـر عهده هکرهـای اخلاقی یا در مثـل متخصصـان حـوزه آی‌تی همان «کلاه‌سـفیدها» نهاده شـده اسـت. به گفتـه رئیـس اداره کل امنیت آی‌تـی بانک کشـاورزی، متخصصـان و هکرهـای اخلاقـی (کلاه سـفید) اداره امنیت آی‌تی بانک کشـاورزی همـگام بـا علم روز دنیـا در زمینه هـک و سوءاسـتفاده از سیسـتم‌های بانکـداری الکترونیـک حرکت کرده تـا امکان بـروز خطـرات امنیتی را بـه حداقل برسـانند. متخصصان ایـن اداره به‌صـورت شـبانه‌روزی از تمام اطلاعـات مربـوط بـه رخدادهای مختلـف در زمینـه سوءاسـتفاده از سیسـتم‌های الکترونیک بانکـی در دنیا آگاه شـده و بـا اطلاعـات به‌دسـت آمـده از بررسـی مشـکلاتی که سـبب به‌وجـود آمـدن ایـن رخدادها در بانک‌هـای دیگر شـده، اقـدام به بررسـی و رفع مشـکلات احتمالـی در سیسـتم‌های امنیتی در سـطح بانک می‌کننـد. گفت‌وگوی پیشـرو با محسـن شـفیعی، رئیـس اداره کل امنیت آی‌تـی بانک کشـاورزی را پیرامون کارکردهـای اداره امنیـت فنـاوری اطلاعات و همچنین بررسـی دسـتاوردها و برنامه‌های آینـده این مجموعه بخوانید.

بـرای شـروع بفرماییـد جایـگاه و کارکـرد سیسـتم‌های امنیتی در بانکـداری الکترونیک کجاسـت و توضیحی هم پیرامـون وظایف اداره امنیـت آی‌تی بانـک ارائـه دهید.

امنیـت کامپیوتـری شـامل همـه فرآیندهـا و مکانیزم‌هایـی اسـت کـه از تجهیـزات کامپیوتـری، اطلاعـات و سـرویس‌ها در برابـر دسـتیابی غیرمجـاز، تغییر و تخریـب محافظت می‌کند. امنیت کامپیوتری شـامل محافظـت در برابـر رویدادهـای برنامه‌ریـزی نشـده و بحران‌هـای طبیعـی نیـز هسـت. به‌منظـور تامیـن امنیـت، امنیـت بایـد در مراحـل و جایگاه‌های مختلـف سیسـتم مانند امنیـت در طراحـی، معماری امنیتی، مکانیزم‌های سـخت‌افزاری بـرای محافظت از کامپیوترهـا و داده‌ها، سیسـتم عامل امن، کدنویسـی امـن، کنترل‌هـای امنیتـی، حفره‌هـای امنیتـی و خط‌مشـی‌های امنیتی تامین شـود. با توجـه به اینکه امنیت در همه جنبه‌های سیسـتم مطرح اسـت، اداره کل امنیـت بانک کشـاورزی در راسـتای وظایف ذاتی خـود در بانـک، طرح‌هـا و پروژه‌های متعـددی دارد تا امنیـت را در همـه ابعـاد سیسـتم‌های بانکـی تامیـن کرده و از اطلاعات حسـاب مشـتریان در سیسـتم‌های الکترونیکی و سـنتی مانند اینترنت‌بانـک، همراه‌بانک، تلفن‌بانک و همچنین در تمام شـعب بانک کشـاورزی محافظـت کند.

بانـک کشـاورزی در زمینـه امنیـت سیسـتم‌های الکترونیکـی، در شـبکه بانکـی کشـور چـه جایگاهـی دارد؟

بانـک کشـاورزی از جملـه بانک‌هـای پیشـرو در سـطح کشـور در زمینه امنیت سیسـتم‌های بانکداری الکترونیـک اسـت. چنان‌کـه می‌تـوان گفـت بانـک کشـاورزی، اولیـن بانـک در سـطح کشـور بوده اسـت کـه اقـدام بـه راه‌انـدازی بخشـی مسـتقل در زمینـه تامیـن امنیـت سیسـتم‌های خود کـرده و بـه موضوع امنیـت نـگاه و توجـه ویژه‌ای داشـته اسـت. همچنین تاکنون گزارشـی مبنی بر سوءاسـتفاده از سـامانه‌های الکترونیکـی ایـن بانـک نداشـته‌ایم، البتـه مـواردی به‌دلیـل سـهل‌انگاری مشـتریان در حفـظ و رعایـت اصـول امنیتـی وجود داشـته اسـت.

الگـوی بانـک کشـاورزی در زمینـه تامیـن امنیـت بانکـداری الکترونیـک، آیـا الگوهـای بومی اسـت یـا از الگوهـای امنیتـی بانک‌های خارجـی هـم اسـتفاده می‌شـود؟

سـعی بر ایـن اسـت کـه بیشـتر از اسـتانداردهای روز دنیـا اسـتفاده شـود، امـا در بخش‌هـای مختلـف و متعـددی اسـتانداردهای روز دنیـا را بومی‌سـازی کرده‌ایـم. امـروزه بخـش زیـادی از سـخت‌افزارها، سیسـتم‌های عامـل و نرم‌افزارهایـی کـه در زمینـه امنیـت تولیـد می‌شـود خارجـی اسـت و بـا توجـه بـه اسـتانداردهای جهانـی تولیـد شـده و در کل دنیـا مـورد اسـتفاده قـرار می‌گیرنـد. ایـن بانک نیـز از این موضـوع مسـتثنا نبـوده و از ابـزار و دانـش روز دنیـا اسـتفاده می‌کنـد. امـا در زمینه‌هـای جلوگیـری از سوءاسـتفاده از اطلاعـات بانکـی، اداره امنیـت آی‌تـی فـارغ از به‌کارگیری اسـتانداردهای روز دنیا، روش‌های سوءاسـتفاده و کلاهبـرداری در داخـل کشـور را هـم رصـد کـرده و به‌نوعـی بخشـی از پروسـه امنیـت بانکـداری الکترونیـک را بومی‌سـازی می‌کنـد.

مهم‌تریـن طرح‌هـا و پروژه‌هـای امنیتـی بانـک شـامل چه مـواردی اسـت؟

اهـم طرح‌هـا و پروژه‌هـای امنیتـی اداره کل امنیـت آی‌تـی بانک کشـاورزی عبارت از طرح تسـت نفوذپذیـری، طـرح مدیریـت امنیـت اطلاعـات، طرح مرکـز عملیـات امنیـت و مانیتورینـگ سیسـتم‌ها، مدیریـت فریـب‌کاری، کنتـرل دسترسـی مدیریـت شـده، طـرح به‌کارگیـری اسـتانداردهای امنیتـی در بانکـداری الکترونیکـی، طـرح پشـتیبانی از حـوادث، طـرح مدیریت بحـران و تداوم خدمـات و طرح تامین امنیـت سیسـتم‌ها بـه کمـک به‌روزرسـانی مدیریـت شـده سیسـتم‌ها و اسـتفاده از آنتی‌ویـروس متمرکـز اسـت.

در صـورت امـکان و نبـود محدودیت‌هـای امنیتـی تنها بـه ذکـر مـوارد و عناویـن اکتفا نکـرده و توضیحـات بیشـتری را در رابطـه بـا طرح‌هـا بیـان کنیـد؟

از جملـه طرح‌هـای مـورد اشـاره طـرح تسـت نفوذپذیـری بـود. تمـام نرم‌افزارهـای بانکـی، سیسـتم‌های عامل، پایگاه‌های داده‌ای و سیسـتم‌های سـخت‌افزاری ممکن اسـت نواقصی داشـته باشند که وجـود ایـن نواقـص سـبب ایجـاد حفره‌هـای امنیتی در سیسـتم‌های الکترونیـک بانـک شـده و موجبـات سوءاسـتفاده یـا حتـی مخـدوش کـردن و تغییـر اطلاعـات را فراهـم مـی‌آورد. بخـش امنیـت بانـک با اسـتفاده از طـرح تسـت نفوذپذیـری بـه بررسـی این نواقـص پرداخته و با برطرف کردن عیوب و شناسـایی حفره‌هـای امنیتـی موجـود در نرم‌افزارهـای بانـک، از امـکان سوءاسـتفاده از اطلاعـات مشـتریان جلوگیری می‌کنـد. اداره امنیت با این تسـت، به مشـتریان بانک ایـن اطمینـان خاطـر را می‌دهـد کـه در فضایـی امن می‌تواننـد نقل‌وانتقـالات و دیگـر امـور مالـی خـود

را انجام دهند. روش کار در این تست هم به این ترتیب است که تمام سامانه‌ها و ابزارها، مورد حملات مختلف قرار می‌گیرند و چنانچه نقطه ضعف یا نقصی داشته باشند، قبل از عملیاتی شدن اصلاح می‌شوند.

دیگر طرح، مدیریت امنیت اطلاعات است. طرح مدیریت امنیت اطلاعات، مجموعه‌ای از خط‌مشی‌ها هستند که مربوط به مدیریت امنیت اطلاعات و ریسک‌های وابسته به سیستم‌های بانکداری است. این سیستم در بانک با توجه به استاندارد ایزو ۲۷۰۰۱ توسعه یافته است. در سیستم مدیریت امنیت اطلاعات، مجموعه‌ای از خط‌مشی‌ها، فرایندها و سیستم‌ها برای مدیریت ریسک دارایی‌های بانکی طراحی، پیاده‌سازی و نگهداری می‌شوند تا اطمینان حاصل شود که سیستم‌های بانک سطح قابل قبولی در برابر ریسک‌های امنیتی دارد. هم‌اکنون خط‌مشی‌های امنیتی برای شعب و ستاد مرکزی بانک کشاورزی توسعه یافته و در حال اصلاح و تکمیل شدن هستند.

طرح مرکز عملیات امنیت و مانیتورینگ سیستم‌ها، برنامه دیگری است که در اداره امنیت آی‌تی تدارک دیده شده است. مرکز عملیات امنیت محلی برای جمع‌آوری، تحلیل و پاسخگویی به حوادث امنیتی به وقوع پیوسته در شبکه بانکی و شعب هستند

در طرح مدیریت فریب‌کاری نیز با یادگیری رفتار معمول مشتریان در استفاده از خدمات بانکداری الکترونیک و مدل‌سازی رفتار نرمال آنها، مدیریت فریب‌کاری انجام می‌شود. هم‌اکنون سیستم مدیریت فریب‌کاری در بانک کشاورزی در حال توسعه است تا هنگام تغییر الگوی رفتاری نرمال کاربران بانکی هشدارهایی صادر شود.

در طرح کنترل دسترسی مدیریت شده در بانک کشاورزی، با راه‌اندازی Active directory، تمام کارمندان شعب و ستاد مرکزی به دامنه بانک وارد شده و به این ترتیب دسترسی آنها کنترل می‌شود.

همچنین با طرح به‌کارگیری استانداردهای امنیتی در بانکداری الکترونیکی، الگوی بانک مرکزی مبنی بر لزوم استفاده از استاندارد امنیت بانکداری PCI DSS اجرایی می‌شود. این استاندارد اصولی را برای مدیریت داده‌های بانکی وضع می‌کند. مثلا رمز دوم کارت مشتریان در سوئیچ‌ها و واسطهای میانی و درگاه‌های پرداخت، نباید ذخیره‌سازی شوند. این استاندارد به‌طور کامل در بانک کشاورزی پیاده‌سازی شده و در همه سامانه‌ها و سیستم‌های در حال پیاده‌سازی بانک رعایت می‌شود.

طرح پشتیبانی از حوادث هم که در بانک کشاورزی در حال اجراست، فرایندها و ابزارهایی است که اطمینان می‌دهند بانک کشاورزی، برنامه و منابع مناسب برای رسیدگی به رویدادها و تهدیدات امنیتی را دارد.

به توانایی بانک برای بازیابی از بحران یا حادثه غیرمترقبه و بازیابی عملیات نرمال سیستم، مدیریت بحران می‌گویند که هم‌اکنون این طرح به‌طور کامل در بانک کشاورزی پیاده‌سازی شده است.

طرح تداوم خدمات بانکی در شرایط اضطرار هم از دیگر طرح‌های در حال اجراست که عبارت از مجموعه مستنداتی است که روش پاسخگویی با سرعت مناسب برای بانک را در مقابل وقفه‌های غیرقابل قبول برای تداوم ارائه خدمات مهم و حیاتی مشخص می‌کند. در طرح تامین امنیت سیستم‌ها به کمک به‌روزرسانی مدیریت شده سیستم‌ها و استفاده از آنتی‌ویروس متمرکز، هم‌اکنون تمام سیستم‌های بانک کشاورزی به‌روزرسانی مدیریت شده، می‌شود و به آنتی‌ویروس متمرکز مجهز هستند.

با اینکه بخش زیادی از خدمات بانکی، امروزه به‌صورت غیرحضوری و در فضای مجازی انجام می‌شود، اما هنوز برخی مخاطبان سیستم بانکی، حضور در شعبه برای انجام عملیات بانکی را به بانکداری الکترونیک ترجیح می‌دهند و توجیه‌شان نیز ضریب امنیتی بالای انجام امور به‌صورت حضوری است. حال با توجه به اینکه طیف عمده‌ای از مشتریان بانک کشاورزی را جوامع روستایی تشکیل می‌دهند و همچنین اعتقاد به این موضوع که اطمینان انجام عملیات بانکی به‌صورت حضوری بیشتر است، به‌منظور فرهنگ‌سازی در مورد ایمن بودن استفاده از امکانات الکترونیک بانک، تا به امروز چه اقدام‌هایی انجام شده است؟

با توجه به اینکه بانک کشاورزی طیف مختلفی از مشتریان دارد همواره سعی بر این بوده تا با فرهنگ‌سازی و اطلاع‌رسانی درباره طرح‌های امنیتی اجرا شده و در دست اجرا، اطمینان مشتریان به خدمات الکترونیک بانک جلب شود. استفاده از خدمات الکترونیک همچون اینترنت‌بانک، همراه‌بانک و تلفن‌بانک این امکان را برای مشتریان فراهم آورده تا بتوانند با صرف کمترین زمان، در امنیت کامل و به سهولت نسبت به انجام امور بانکی خود اقدام کنند و این خود کمک بزرگی برای ترغیب هر چه بیشتر مشتریان بانک در استفاده از این‌گونه خدمات است. از طرفی دیگر در طرح بازاریابی تهاجمی که توسط اداره کل بانکداری خرد مدیریت می‌شود، سعی شده با استفاده از تبلیغات محیطی مشتریان را به استفاده هر چه بیشتر از این خدمات تشویق کند.

چه تمهیدات امنیتی در مقوله‌هایی مانند اینترنت‌بانک، تلفن‌بانک و همراه‌بانک در بانک کشاورزی لحاظ شده که به‌واسطه آن می‌توان اعتماد مشتریان را جلب کرد؟

اداره امنیت آی‌تی در ابتدا تمام راه‌های موجود که ممکن است سبب سوءاستفاده از اطلاعات مالی مشتریان شود را بررسی کرده و بر اساس اطلاعات به‌دست آمده اقدام به استفاده از راهکارهای امنیتی مختلف از جمله طراحی و تهیه نرم‌افزارها و سخت‌افزارها می‌کند. بعد از طراحی نیز این اداره با انجام آزمون‌های نفوذپذیری و همچنین با به‌کارگیری آخرین متدها و ابزارهای روز دنیا و نیز استفاده از متخصصان مختلف در این زمینه، کارکرد صحیح و امن این سیستم‌ها را تایید کرده و پس از آن اجازه عملیاتی شدن سیستم را در بانک صادر می‌کند. البته لازم به ذکر است که این بررسی‌ها

اداره امنیت فناوری اطلاعات تا از امنیت سیستم‌ها اطمینان حاصل نکند اجازه عملیاتی شدن آن را صادر نمی‌کند. از این‌رو سیستم‌ها باید ابتدا در آزمون‌های امنیتی تایید شده و بعد از آن وارد مرحله عملیاتی شوند

به‌صورت دوره‌ای تکرار و تمام سیستم‌ها به‌طور متناوب از لحاظ ضریب ایمنی با توجه به دانش روز آزمایش شده و حتی در صورت ایجاد تغییرات در این سیستم‌ها تمام مراحل آزمون و بررسی دوباره تکرار می‌شود.

یعنی می‌فرمایید سیستم‌های امنیتی بانکداری الکترونیک در بانک کشاورزی ابتدا به‌صورت پایلوت اجرا می‌شود. ضرورت این اجرای آزمایشی چیست؟

اداره امنیت فناوری اطلاعات تا از امنیت سیستم‌ها اطمینان حاصل نکند اجازه عملیاتی شدن آن را صادر نمی‌کند. از اینرو سیستم‌ها باید ابتدا در آزمون‌های امنیتی تایید شده و بعد از آن وارد مرحله عملیاتی شوند. در مرحله عملیاتی ممکن است بانک با توجه به شرایط و امکانات تصمیم به راه‌اندازی سیستم‌ها به‌صورت مرحله‌ای (فازبندی شده) داشته باشد. در هر حال از لحاظ

امنیتی تفاوتی برای اجرایی شدن این سیستم‌ها در مناطق مختلف کشور وجود نداشته و در تمام موارد آزمایش‌های امنیتی به‌طور کامل لحاظ می‌شود.

با توجه به اینکه بانک به‌عنوان یک موسسه مالی کلان به‌طور مداوم در معرض خطر حمله‌های جدید هکرهاست، این اداره برای مقابله با این معضل چه تدابیری را اندیشیده است؟

سعی شده که این اداره و متخصصان آن از لحاظ علم روز دنیا از هکرها عقب نمانده و با استفاده از هکرهای اخلاقی یا همان هکرهای کلاه سفید که به علم روز دنیا در زمینه هک آشنایی دارند امکان بروز خطرات امنیتی را به حداقل برساند. متخصصان این اداره هم به‌صورت روزانه از تمام اطلاعات مربوط به رخدادهای مختلف در زمینه سوءاستفاده از سیستم‌های الکترونیک بانکی در دنیا آگاه شده

اداره امنیت آی‌تی در ابتدا تمام راه‌های موجود که ممکن است موجب سوءاستفاده از اطلاعات مالی مشتریان شود را بررسی کرده و براساس اطلاعات به‌دست آمده اقدام به استفاده از راهکارهای امنیتی مختلف از جمله طراحی و تهیه نرم‌افزارها و سخت‌افزارها می‌کند

و اقدام به بررسی مشکلاتی که سبب به‌وجود آمدن این رخدادها در بانک‌های دیگر شده است، می‌کنند. همچنین با توجه به اطلاعات به دست آمده اقدام به بررسی و رفع مشکلات احتمالی در سیستم‌های امنیتی در سطح بانک می‌کنند.

جایگاه آموزش در این میان کجاست؟

این اداره با توجه به نگرش و ماموریت خود در حوزه امنیت اطلاعات، برنامه‌های آموزشی را در دو سطح در دستور کار خود قرار داده است. سطح اول شامل کارکنان شعب و ستاد بانک است که آموزش‌های مربوط به امنیت اطلاعات برابر استاندارد ایزو ۲۷۰۰۱ و دوره آموزشی نحوه استفاده امن از رایانه CSCU (Certified Secure Computer User) بوده و علاوه بر دوره‌های اختصاصی یادشده، در همایش‌های بانک نیز این اداره کل نسبت به ارائه مطالب مرتبط با امنیت اطلاعات برای مدیران بانک اقدام می‌کند. سطح دوم هم برای مشتریان بانک است که شامل اطلاع‌رسانی و آگاه‌سازی مشتریان درمورد استفاده امن از خدمات بانکداری الکترونیک است و این اطلاع‌رسانی از طریق درج نکات امنیتی در سایت بانک و همچنین تهیه بروشور و پخش تیزر در شعب انجام می‌شود.

از دیگر موارد و مصادیق قابل طرح در مقوله امنیت بانکداری الکترونیک، اتفاقی بود که سال گذشته در زمینه کارت‌های عابربانک افتاد؛ چنان‌که حضرتعالی مستحضرید و در جریان ریز موضوع هم قرار دارید، سال گذشته شاهد انتشار رمز تعداد زیادی از کارت‌های مشتریان بانک‌های مختلف کشور در اینترنت بودیم. این اتفاق چه تاثیری بر اعتماد مشتریان به سیستم بانکداری الکترونیک بانک کشاورزی داشت و بانک برای بازگرداندن این اعتماد به مشتریان خود چه اقدام‌هایی انجام داد؟

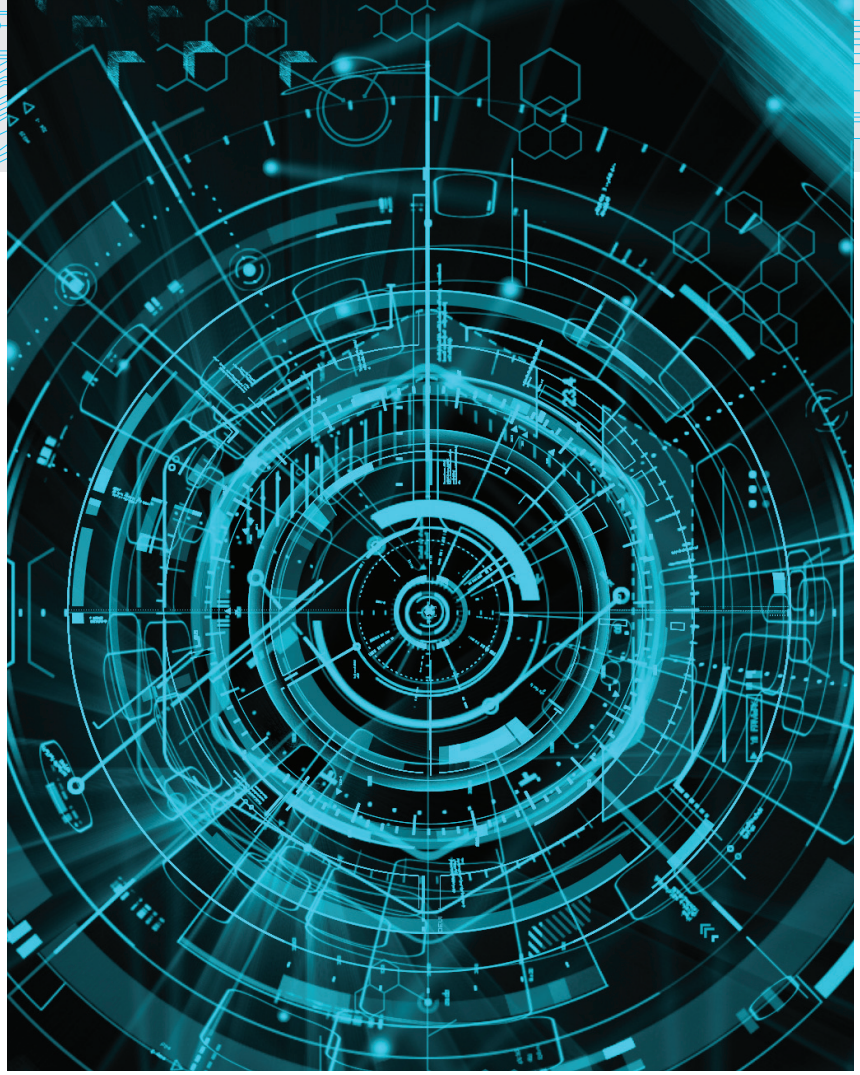
پس از رخ دادن این اتفاق، در بانک کشاورزی کمیته بحران تشکیل شد. در گام نخست تصمیم گرفته شد تا به دور از هیاهو و جنجال ایجاد شده که موجب تشویش و اضطراب مشتریان می‌شد با ایجاد اطمینان به مشتریان، رخداد یادشده را مدیریت کند. موضوع از این قرار بود که یکی از شرکت‌های ارائه کننده خدمات POS به بانک‌ها به‌علت سهل‌انگاری و نارضایتی یکی از کارشناسانش موجب افشای اطلاعات رمز کارت تعدادی از مشتریان بانک‌های مختلف کشور شد. البته در عمل به‌دلیل اینکه در اطلاعات افشا شده رمز چهار رقمی مشتریان در یک رشته ۱۶ رقمی قرار داده شده بود امکان سوءاستفاده وجود نداشت، چراکه برای استفاده از کارت نیاز به رمز و فیزیک کارت است. و این در حالی بود که فیزیک کارت در اختیار سوءاستفاده‌کننده احتمالی قرار نداشته و رمز نیز به‌علت اینکه در یک رشته ۱۶ رقمی قرار داشت، قابل تشخیص برای سوءاستفاده‌کننده نبود. در نهایت از مشتریانی که اطلاعات کارت آنها افشا نشده بود، با اطلاع‌رسانی انجام شده درخواست شد تا اقدام به تغییر رمز خود کنند و کارت‌های آن تعداد از مشتریانی هم که اطلاعات آنان منتشر شده بود، غیرفعال شد تا مشتریان با مراجعه به بانک کارت جدید دریافت کنند. تمام این اقدام‌ها به‌منظور ایجاد اعتماد مشتریان بانک انجام شد.

اما مورد دیگری که طرح آن ضرورت دارد، امکان به اشتراک گذاردن تجربیات حوزه امنیتی بانکداری الکترونیک است. سال‌هاست رسم بر این بوده که اگر بانک یا یک موسسه مالی مورد حمله قرار گرفته و از آن کلاهبرداری شود، به‌واسطه حفظ اعتبار برند بانک، این اتفاق از سوی بانک مورد نظر تا حد ممکن در خفا می‌ماند و چه بسا بانکی دیگر با روشی مشابه مورد حمله قرار می‌گرفت. این در حالی است که به اشتراک گذاردن تجربیات حاصل از این دست رخدادها در شبکه بانکی کشور، می‌تواند نقش بسیار چشمگیری در ممانعت از تکرار مجدد حمله‌ها داشته باشد. جنابعالی بفرمایید وضعیت شبکه بانکی کشور در این زمینه چگونه است؟ آیا این تجربیات در میان بانک‌ها به اشتراک گذارده می‌شود؟

مدتی است که در بانک مرکزی، مرکزی به نام مرکز کاشف (مرکز کنترل امنیت شبکه و فوریت‌های بانکی) به‌منظور لزوم حفظ و ارتقای امنیت نظام پرداخت و بانکداری الکترونیکی و مواجهه درست با تهدیدات درونی و بیرونی نظام بانکی کشور، راه‌اندازی شده است. علاوه بر آن در صورت بروز رخداد امنیتی بانک‌ها موظف به اطلاع‌رسانی به مرکز کاشف هستند.

و به‌عنوان پرسش پایانی، بپردازیم به برنامه‌های آتی مهم‌ترین رئوس برنامه‌های اداره امنیت آی‌تی مشتمل بر چه مواردی ا ست ؟

یکی از مهم‌ترین برنامه‌های این مجموعه راه‌اندازی مرکز کنترل و عملیات امنیت است که وظیفه بررسی تمام اتفاقاتی که در بانک رخ می‌دهد را بر عهده داشته تا از این طریق بتواند از بروز حوادث و مشکلات امنیتی قبل از وقوع جلوگیری کند. از دیگر برنامه‌های اداره امنیت می‌توان به ایجاد امکان ذخیره اطلاعات مربوط به مشتریان به‌طور همزمان در سایت‌های دیگر و خارج از بانک اشاره کرد. این روش امکان حفظ و نگهداری اطلاعات مربوط به مشتریان به‌منظور بازگشت به حالت عادی و ادامه کار، در صورت بروز رخدادهای امنیتی و حوادثی مانند بلایای طبیعی را فراهم می‌آورد. راه‌اندازی سیستمی هوشمند که بر اساس ثبت رفتار مشتریان و همچنین میزان تراکنش آنان، اقدام به کنترل حساب و نقل‌وانتقالات مالی مشتریان به‌منظور جلوگیری از کلاهبرداری می‌کند، از دیگر برنامه‌های این بخش در آینده است. همچنین توسعه پروژه «ISMS» بر اساس استاندارد بین‌المللی ایزو ۲۷۰۰۱ در زمینه امنیت، به‌صورت سراسری و در تمام شعب سطح کشور برقرار است.



ضرورت‌های استفاده از یک سیستم کارآمد در بانک کشاورزی؛

S.O.C: مرکز کنترل و عملیات امنیت

ظریفی می‌گفت، اگر سایر حوزه‌های اقتصادی کشور هم به موازات سیستم بانکی و خدمات آن رشد یافته بودند، شاید می‌شد ایران را به لحاظ اقتصادی در زمره کشورهای توسعه‌یافته لحاظ کرد. آری؛ بانک‌ها و موسسات مالی برای جذب مشتریان بیشتر در ارائه خدمات هر چه بهتر و به‌روزتر از هیچ اقدامی فروگذار نمی‌کنند و یک گام از سایر موسسات اقتصادی پیش‌تر هستند. در این میان، توسعه بانکداری الکترونیک هم موسسات مالی و بانک‌ها را در رقابتی جدی برای کارآمدی هر چه بیشتر و بهتر قرار داده، به‌نحوی که هر روزه هم‌زمان دست به ارائه فناورهای نوین و پشتیبانی از این فناوری‌ها می‌زنند. بانک کشاورزی هم به‌عنوان بانکی پیشرو در بانکداری الکترونیک، همواره در بکارگیری سیستم‌ها و رویه‌های جدید، پیشگام بوده است. از جمله این رویه‌های نوین و کارآمد هم پیاده‌سازی مرکز کنترل و امنیت عملیات یا S.O.C در بانک کشاورزی است. حال آنکه این سیستم چه بوده، چه کارکردهایی دارد و ضرورت اجرای آن در بانک چیست؛ در مقاله حاضر گردآوری شده است. مقاله‌ای که توسط پاشا رفیعی، کارشناس معاونت مستقل امنیت فناوری اطلاعات بانک کشاورزی تهیه شده است. بخوانید:

ضرورت وجودی

به‌منظور افزایش اثربخشی کنترل‌های امنیتی موجود، حفاظت موثر از عملیات جاری در کسب‌وکار بانک و در واقع ایجاد و نگهداری مستمر از وضعیت امنیتی بانک در سطحی قابل قبول، ناگزیر به ایجاد زیرساختی برای پایش، تحلیل و پاسخگویی متمرکز به وقایع امنیتی گزارش شده از سوی تمام تکنولوژی‌های مورد استفاده در بانک خواهیم بود. اما بخش عمده‌ای از این زیرساخت در مرکز کنترل و عملیات امنیت تحقق پیدا خواهند کرد. مرکز کنترل و عملیات امنیت بانک کشاورزی که طبق صورت‌جلسه هیئت مدیره، به‌زودی در معاونت مستقل امنیت فناوری اطلاعات راه‌اندازی می‌شود، وظیفه پایش، تحلیل و پاسخگویی متمرکز به وقایع امنیتی را برعهده دارد.

چیستی یک طرح نوآورانه

مرکز کنترل و عملیات امنیت، دیدی بلادرنگ و جامع نسبت به وضعیت امنیتی کسب‌وکار بانک ایجاد می‌کند. درواقع این مرکز به‌واسطه اطلاع‌رسانی‌های اتوماتیک حوادث و وقایع، تولید گزارش‌های جزئی و کلی، پاسخ‌دهی اتوماتیک به حوادث و وقایع، رویکردی پیشگیرانه را به‌منظور مدیریت ریسک‌های امنیتی ایجاد خواهد کرد. مرکز کنترل و عملیات امنیت تمام جوانب مرتبط با امنیت بانک را به‌صورت بلادرنگ و آنی و از یک نقطه متمرکز مدیریت و مورد پایش لحظه‌ای خواهد داد. این مرکز با شناسایی آنی حوادث و وقایع، براساس سطح ریسکی که هر یک از آنها ایجاد خواهند کرد، وقایع و حوادث را اولویت‌بندی هم می‌کند. همچنین این مرکز دارایی‌های متاثر شده از وقایع اتفاق افتاده را مشخص کرده، راهکارهای اصلاحی یا پیشگیرانه را پیشنهاد داده یا در مواردی از پیش تعیین شده‌ها را اجرا می‌کند.

این مرکز با ارائه گزارش‌هایی در سطوح مختلف، نیازمندی‌های مربوط به فرآیندهای ممیزی، مانیتورینگ بلادرنگ و همچنین ارزیابی بخشی از ریسک‌های عملیاتی بانک را برآورده می‌کند. این مرکز، اطلاعات امنیتی زیادی را از ابزارهای امنیتی مانند دیواره آتش، آنتی‌ویروس، سیستم‌های تشخیص نفوذ و انواع نرم‌افزارهای کاربردی و زیرساختی در سطح شبکه جمع‌آوری کرده، سپس آن اطلاعات را نرمال‌سازی و مرتبط کرده و گزارش بلادرنگی از آنچه در حال اتفاق است فراهم می‌کند. بنابراین اپراتورها، توانایی مدیریت و پاسخ‌گویی مناسب در مقابل حوادثی که وقوع آنها موجب به خطر افتادن سازمان می‌شود را خواهند داشت. از سوی دیگر در مواردی که جلوگیری کامل در مقابل خطرات امکان‌پذیر نباشد، گزارش‌دهی مرکز عملیات شبکه، به اپراتورها امکان تشخیص حمله و کاهش خسارات آن را

قبل از انتشار در شبکه می‌دهد.

ساختار اجرایی

به‌طور کلی مرکز عملیات امنیت شبکه از پنج ماژول مولدهای وقایع (Event Generator)، جمع‌آوری اطلاعات (Collection)، پایگاه داده رخداد (Incident Database)، موتورهای تحلیل (Analysis Engines)و مدیریت واکنش (Reaction Management)تشکیل شده است. ارتباط بین ماژول‌های SOC هم در شکل شماره یک نشان داده شده است.

روند حرکتی

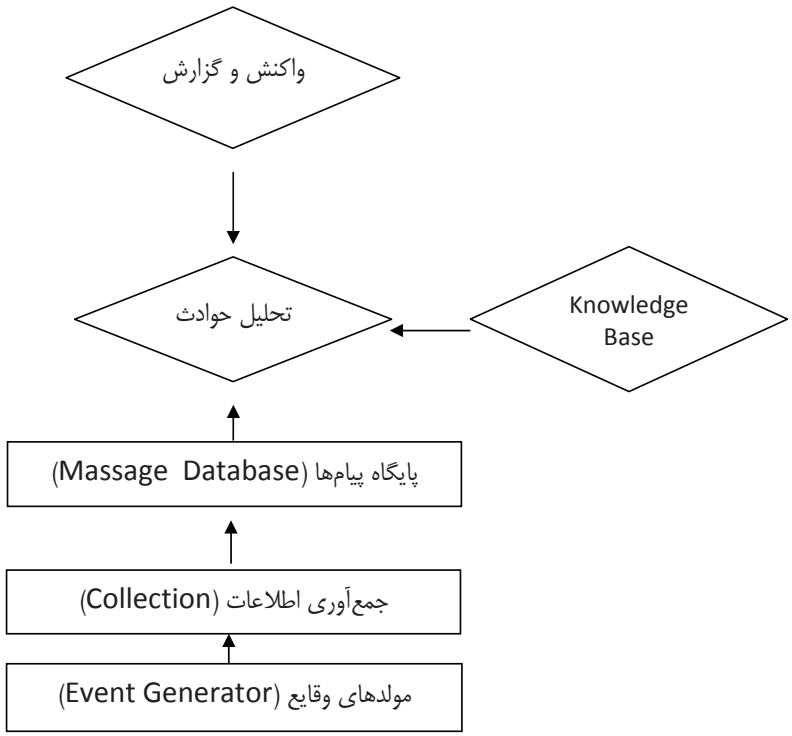
با توجه به تعاریف بالا، ترتیب زیر در روند حرکت مرکز عملیات امنیت شبکه انجام می‌شود.

۱. ثبت وقایع امنیت
۲. جمع‌آوری اطلاعات
۳. ذخیره‌سازی
۴. تحلیل
۵. واکنش

لازم به یادآوری است که قبل از طراحی و تعیین قوانین تحلیل و همبستگی، باید سطوح امنیتی در زیرساخت آی‌تی به‌منظور تشخیص مسیرهای ممکن برای نفوذ به سیستم‌های تحت شبکه، مورد بررسی قرار گرفته و در صورت لزوم سیاست‌های امنیتی مناسبی مانند حقوق دسترسی و عملیات‌های مجاز برای سازمان اتخاذ شود.

طرح مفهومی مرکز عملیات امنیت شبکه (SOC)

این مرکز ارائه‌کننده خدمات متفاوتی است که عمده آنها در بخش طراحی مفهومی آورده شده است. خدمات یادشده از طریق موجودیت‌هایی که در مرحله تحلیل و طراحی مورد شناسایی قرار می‌گیرند، ارائه خواهد شد. سلسله مراتب این موجودیت‌ها عبارت است از زیرسیستم‌ها، ماژول‌ها و در نهایت مجموعه نرم‌افزارها، سخت‌افزارها و فرآیندهایی که برآورده کننده ماژول‌ها هستند. به‌عنوان مثال زیرسیستم مدیریت تهدیدات شامل ماژول‌های مدیریت رخدادها، ماژول پیشگیری از دست دادن داده‌ها و ماژول‌های دیگری خواهد بود و هر یک از ماژول‌ها به‌واسطه نرم‌افزارها و سخت‌افزارهای صنعتی یا گروهی از فرآیندها محقق خواهند شد.



شکل شماره یک

حوزه‌های عملیاتی

ساختار مرکز کنترل و عملیات امنیت به‌صورت پنج حوزه عملیاتی در نظر گرفته شده که این حوزه‌ها عبارت از زیرسیستم مدیریت تهدیدات (Threat Management)، زیرسیستم مدیریت آسیب‌پذیری (Vulnerability management)، زیرسیستم مدیریت پیکربندی (Configuration Management)، زیرسیستم مدیریت تقلب (Transaction Fraud Management) و داشبورد امنیتی (Security Dashboard) هستند. در ادامه این زیرسیستم‌ها به‌صورت مختصر مورد بررسی قرار خواهند گرفت.

مدیریت تهدیدات

جمع‌آوری و مرتبط‌سازی وقایع گزارش شده از سوی سامانه‌های نامتجانس و گاهی ناهمگن، یکی از مهم‌ترین چالش‌هایی است که مراکز کنترل و عملیات امنیت با آن روبه‌رو هستند. بنابراین این مراکز ملزم خواهند بود تا با هدف جمع‌آوری و مرتبط‌سازی اتوماتیک وقایع، سامانه‌ای را با عنوان سامانه مدیریت وقایع و اطلاعات امنیتی پیاده‌سازی کنند. این عنوان که عنوانی معروف در حوزه امنیت اطلاعات است، در طرح مفهومی مرکز کنترل و عملیات امنیت بانک کشاورزی با عنوان زیرسیستم مدیریت تهدیدات مطرح است. زیرسیستم مدیریت تهدیدات در واقع پاسخی است به نیازهای موجود در حوزه‌های مرتبط با مدیریت ریسک سازمان‌هایی که کسب‌وکار آنها در دنیای دیجیتال جاری است؛ نیازهایی همچون مانیتورینگ و مرتبط‌سازی بلادرنگ وقایع، تحلیل بی‌درنگ حوادث، بررسی‌های پس از وقوع حوادث و پاسخ‌دهی اتوماتیک به آنها.

این زیرسیستم به‌عنوان مغز متفکر مرکز کنترل و عملیات امنیت قادر خواهد بود هزاران رخداد را در هر ثانیه از سامانه‌های مختلف جمع‌آوری کرده و با ذخیره طولانی مدت آنها، امکاناتی از قبیل نمایش و تحلیل بلادرنگ رخدادها، تولید گزارش‌های مختلف، آنالیزهای پس از وقوع حوادث و اعلام هشدار را به روش‌های مختلف در زمان وقوع حوادث فراهم آورد. حال پس از اطمینان از اینکه دیتای لازم از تمام تکنولوژی‌های مورد استفاده در

سازمان به‌صورت متمرکز جمع‌آوری شده، زیرسیستم مدیریت تهدیدات اقدام به نرمال‌سازی، دسته‌بندی و مرتبط‌سازی دیتاهای جمع‌آوری شده خواهد کرد. به‌طور خلاصه این زیرسیستم اقدام‌های زیر را پس از جمع‌آوری دیتاهای لازم به انجام خواهد رساند:

ـ نرمال‌سازی (Normalization):
در این مرحله رخدادهای جمع‌آوری شده از انواع تجهیزات، سیستم‌های امنیتی، سرورها، نرم‌افزارهای کاربردی، تجهیزات کنترل دسترسی فیزیکی و کنترل‌های محیطی، نرمال شده و به فرمتی واحد تبدیل خواهند شد.

ـ دسته‌بندی (Categorization):
زیرسیستم مدیریت تهدیدات به روشی قابل توسعه و به‌واسطه ایجاد قوانینی مستقل از تولیدکننده و با هدف فهم آسان‌تر و سریع‌تر انواع رخدادهای جمع‌آوری شده، آنها را گروه‌بندی می‌کنند.

ـ مرتبط‌سازی ساده وقایع (Simple Event Correlation):
زیرسیستم مدیریت تهدیدات قادر خواهد بود تا به‌سادگی با جمع‌آوری رخدادها و مرتبط‌سازی چند رخداد با یکدیگر، تهدیداتی را شناسایی کند که بدون این زیرسیستم، امکان شناسایی آنها وجود نخواهد داشت. به‌طور مثال پنج بار تلاش ناموفق برای ورود به سیستمی با استفاده از یک نام کاربری مشخص و در مدت زمان یک دقیقه می‌تواند نشان‌دهنده حمله شکست کلمه عبور باشد.

ـ مرتبط‌سازی چند مرحله‌ای وقایع (Multi-Stage Event Correlation):
این زیرسیستم قادر است رخدادهای غیرمتجانس گوناگون را تحلیل کرده و مشخص کند که تمام آن رخدادهای متفاوت مربوط به حادثه‌ای یکسان هستند. البته ترکیب این رخدادها به‌صورت بلادرنگ و همزمان با ورود میلیون‌ها رخداد به این زیر سیستم، انجام خواهد شد .

ـ اولویت‌بندی (Prioritization):
اولویت‌بندی تهدیدات شناسایی شده، امکان دیگری است که در زیرسیستم مدیریت تهدیدات برآورده خواهد شد. اولویت‌بندی رخدادها، مبتنی بر ریسک اندازه‌گیری شده برای هر یک و بر اساس پارامترهایی چون میزان اهمیت و حساسیت سامانه تولیدکننده رخداد (مورد هدف) برای کسب‌وکار بانک، نرخ وقوع رخداد در گذشته، سوابق گذشته حمله‌کنندگان و میزان آسیب‌پذیری سامانه مورد هدف انجام می‌شود.

ـ تحلیل آماری (Statistical Analysis): زیرسیستم مدیریت تهدیدات قادر است از طریق انجام محاسبات ریاضی پیشرفته روی دیتاهایی (سوابق رخدادها) که در طول زمان جمع‌آوری کرده، الگوهای رفتاری نرمال را تعیین و موارد نقض این الگوها را گزارش کند.

تحلیل‌های پس از وقوع حادثه (Historical Analysis): زیرسیستم مدیریت تهدیدات با جمع‌آوری و نگهداری طولانی‌مدت سوابق رخدادهای سامانه‌های مختلف، امکان بررسی و پیگیری رخدادها را پس از وقوع حوادث فراهم می‌کند. سوابق نگهداری شده توسط این زیرسیستم می‌تواند در پیگیری‌های قانونی مورد

استفاده قرار گرفته و در دادگاه‌های کشور مطابق قوانین تجارت الکترونیک برای اثبات جرایم رایانه‌ای به‌کار برده شود. همچنین بررسی مجدد سوابق رخدادهای نگهداری شده می‌تواند نشان‌دهنده مواردی باشد که در زمان وقوع از چشم پرسنل و زیرسیستم‌های موجود در مرکز کنترل و عملیات امنیت پنهان مانده است. ازاین‌رو این بررسی‌ها می‌توانند موجب بهبود فرآیندها و پیکربندی سامانه‌های موجود در مرکز شود.

مدیریت آسیب‌پذیری

نقاط آسیب‌پذیر در واقع ضعف‌ها و نقص‌هایی هستند که در سامانه‌های مبتنی بر فناوری اطلاعات وجود داشته و می‌توانند برای سوءاستفاده از آن سامانه‌ها مورد استفاده قرار گیرند. نقاط آسیب‌پذیر می‌توانند از طریق مواردی چون پیکربندی ناقص و نادرست، عدم شناسایی و برطرف کردن به‌موقع مشکلات امنیتی و وجود نرم‌افزارهای مخرب ایجاد شوند.

امروزه با وجود پیشرفت تکنولوژی‌های امنیتی، هنوز مدیریت آسیب‌پذیری‌های موجود در نرم‌افزارها و سیستم‌ها، از چالش‌های بزرگ پیش‌روی سازمان‌هایی است که کسب‌وکار آنها مبتنی بر فناوری اطلاعات است. شناسایی نقاط آسیب‌پذیر بالقوه و برطرف کردن آنها قبل از آنکه با سوءاستفاده از آنها ضرری متوجه سازمان شود، نیاز به همکاری و هماهنگی شدیدی بین بخش‌های عملیاتی بانک و بخش امنیت دارد. به‌علاوه ایجاد دیدی جامع و بلادرنگ نسبت به نقاط آسیب‌پذیر موجود در سراسر سازمان، برطرف کردن اتوماتیک آسیب‌پذیری‌ها و تولید گزارش‌های دقیق از فعالیت‌های انجام شده در این حوزه از نیازمندی‌های حیاتی برای کاهش ریسک‌های سیستم‌های مبتنی بر فناوری اطلاعات و برآورده کردن نیازمندی‌های قانونی و مقرراتی است.

زیرسیستم مدیریت نقاط آسیب‌پذیر در مرکز کنترل و عملیات امنیت بانک کشاورزی در حقیقت به‌واسطه ایجاد و ترکیب امکان شناسایی دقیق و بلادرنگ نقاط آسیب‌پذیر، با امکان برطرف کردن اتوماتیک نقاط آسیب‌پذیر شناخته شده و تولید گزارش‌هایی به‌منظور برآورده کردن نیازمندی‌های قانونی و مقرراتی، شکاف بین بخش‌های عملیاتی و امنیت بانک را برطرف می‌کند.

لازم به یادآوری است که خروجی حاصل از این زیرسیستم، ورودی زیرسیستم مدیریت تهدیدات خواهد بود. چراکه یکی از پارامترهای مورد استفاده در زیرسیستم مدیریت تهدیدات، برای محاسبه سطح ریسک رخدادهای به‌وقوع پیوسته، سطح آسیب‌پذیری تولیدکنندگان رخدادهای یادشده است. به این ترتیب، زیرسیستم مدیریت تهدیدات می‌تواند اولویت‌بندی مناسب‌تری روی میلیون‌ها رخدادی که روزانه در سیستم‌ها و تجهیزات مبتنی بر فناوری اطلاعات بانک ایجاد می‌شوند، به انجام رساند.

امروزه با وجود پیشرفت تکنولوژی‌های امنیتی، هنوز مدیریت آسیب‌پذیری‌های موجود در نرم‌افزارها و سیستم‌ها، از چالش‌های بزرگ پیش‌روی سازمان‌هایی است که کسب‌وکار آنها مبتنی بر فناوری اطلاعات است. شناسایی نقاط آسیب‌پذیر بالقوه و برطرف کردن آنها قبل از آنکه با سوءاستفاده از آنها ضرری متوجه سازمان شود، نیاز به همکاری و هماهنگی شدیدی بین بخش‌های عملیاتی بانک و بخش امنیت دارد

مدیریت پیکربندی

امروزه مدیریت پیکربندی زیرساخت‌های حیاتی که کسب‌وکار سازمان بر آنها تکیه کرده، از اهمیت زیادی برخوردار است. چراکه اغلب آسیب‌پذیری‌ها و همچنین اختلالات ایجاد شده در ارائه سرویس مطلوب، حاصل عدم مدیریت مناسب پیکربندی این زیرساخت‌ها است. زیرسیستم مدیریت پیکربندی با دو ماموریت مشخص «کنترل تغییرات پیکربندی» و «ارزیابی پیکربندی» در معماری فنی مرکز کنترل و عملیات امنیت گنجانده شده است.

مدیریت تقلب

در طول چند سال گذشته، حملات مشهوری در سراسر دنیا اتفاق افتاده که بررسی آنها نشان‌دهنده تغییر ماهیت تهدیدات و حتی ماهیت حمله‌کنندگان است. چنان‌که ماهیت مهاجمان از مهاجمان فردی به سمت مهاجمان سازماندهی شده با اهداف مالی قابل توجه‌تری سوق پیدا کرده است. این مهاجمان سازماندهی شده به‌واسطه استفاده از دانش بانکداری، اطلاعات تکنولوژیکی و اطلاعات محرمانه بانک‌ها، تراکنش‌های کلاهبردارانه خود را به انجام می‌رسانند. در این راستا استفاده از کنترل‌های قدیمی همچون فایروال، سیستم‌های تشخیص نفوذ(IDS)، پایش حملات زیرساخت‌ها، فیلترینگ URL و کنترل‌های امنیتی موجود در برنامه‌ها به‌منظور تشخیص و کاهش ریسک‌های جدید (حملات مهاجمان سازماندهی شده) چندان موثر نیست. بنابراین پایش تراکنش‌ها در زمره دستورالعمل‌های اصلی بانک‌ها به‌منظور مدیریت تقلب‌های سازمان‌دهی شده، قرار گرفته است.

زیرسیستم داشبورد امنیتی

این سیستم علاوه بر ایجاد یک Interface به‌منظور ارتباط و مشاهده سریع‌تر مدیران و کاربران بخش‌های گوناگون SOC ، فراهم آورنده امکانات ارتباط با کاربران به‌منظور گزارش مشکلات و مسائل امنیتی و پیگیری آنهاست. این زیرسیستم از بخش‌های سیستم مدیریت Service Desk ، سیستم Trouble Ticket، مشورت‌های امنیتی (Security Advisories)و سیستم Online Security Dashboard تشکیل شده است.

جمع‌بندی

با توجه به ضرورت و اهمیت امنیت در فناوری اطلاعات و حملات سایبری که اخیرا سازمان‌ها و به‌ویژه سازمان‌های مالی را تهدید می‌کند، ضرورت پیاده‌سازی مرکز کنترل و عملیات امنیت به‌منظور پایش، تحلیل و پاسخگویی متمرکز به وقایع امنیتی احساس می‌شود.

راه‌های شناسایی تقلب در بانکداری الکترونیک؛

متقلبان یک قدم جلوتر از قانون‌گذاران!

آنها که دهه سوم زندگی خود یا همان ۳۰سالگی را پشت سر گذاشته‌اند، تلفن‌های سکه‌ای راه دور دهه شصت را به‌خوبی به یاد می‌آورند. تلفن‌هایی که با انداختن سکه‌ای امکان ارتباط برون‌شهری را به فرد می‌داد و ارتباط برقرار می‌شد؛ اما ادامه این مکالمه مشروط به انداختن سکه‌های بیشتر در تلفن بود و هر زمان که روند انداختن سکه در قلک تلفن قطع می‌شد، مکالمه را نیز باید پایان یافته تلقی می‌کرد. کارکرد این تلفن‌ها به‌گونه‌ای بود که سکه ابتدا در قلک کوچک یا بالایی تلفن می‌رفت و به محض برقراری ارتباط به قلک اصلی می‌افتاد که دیگر قابل بازگشت نبود. اما متقلبانی هم بودند که راه خرج نکردن سکه‌ها و برقراری ارتباط را یافته بودند: سکه‌هایی سوراخ که بندی به آنها وصل شده بود. سکه متصل به بند به داخل قلک کوچک‌تر می‌رفت، اما هنگام برقراری تماس، به داخل قلک بزرگ یا اصلی نمی‌افتاد؛ چراکه به‌وسیله همان بند موصوف نگه داشته شده بود و مکالمه بدون خرج کردن سکه‌های بیشتر ادامه می‌یافت.

این تنها نمونه‌ای کوچک از تقلب‌های عصر مدرنیته است. تقلبی که بسیار برایمان ملموس و پیش‌پا افتاده است. اما عمر تقلب و تخلف اگر به اندازه عمر بشر نباشد؛ این را به صراحت می‌توان گفت که عمری بیشتر از قوانین و ضوابط بشری دارد؛ که در هر دوره‌ای و برهه‌ای از تاریخ و هر کجای این کره خاکی اگر ضابطه‌ای تعیین شده، مثل است که می‌گویند تقلب‌ها و تخلف‌های آن زودتر تدارک دیده شده‌اند. امروزه نیز به‌واسطه رشد چشمگیر فناوری اطلاعات و قرار گرفتن عمده امور بر بستر آی‌تی، تقلب‌های اینترنتی بسیار فراگیر شده و همواره موسسات و نهادهایی که فعالیت‌شان بر پایه آی‌تی استوار شده، به فکر گام نهادن پیش از متقلب‌ها هستند. لذا حرکت کردن پیش از متخلفان در یک حوزه خاص، نیازمند این است که تقلب را در آن حوزه شناخت تا بتوان راهکارهای مقابله با آن را ارائه داد. نظر به موضوع ویژه‌نامه حاضر و اهمیت امنیت در بانکداری، گفتار حاضر نگاهی گذرا دارد به تقلب‌های موجود در بانکداری الکترونیک و راه‌های مقابله با آنها.

تقلب چیست؟

تقلب در مفهوم عام، عبارت است از تحریف حقایق بااهمیت توسط کسی که می‌داند مطلبش حقیقت ندارد یا عدم ارائه حقایق به قصد فریب دیگران. در تعریف دیگر، واژه تقلب عبارت است از سوءاستفاده از سود یک سازمان بدون اینکه لزوما به عواقب قانونی آن منجر شود. در تعریفی دیگر، تقلب به فرآیندی اشاره دارد که طی آن یک یا چند نفر، عمدا و مخفیانه دیگران را از هر چیز باارزشی، برای منافع شخصی خود محروم کنند. در کنار این تعاریف، تعریف‌های متعدد دیگری هم از تقلب ارائه شده، ولی آنچه در تمام این تعاریف، مشترک و یکسان بوده، این است که تقلب، نوعی سوءاستفاده از منابع دیگران، به‌منظور منافع شخصی، به عمد و کاملا غیرقانونی است.

ضرورت شناسایی تقلب در بازارهای مالی

امروزه خسارت‌های غیرمستقیمی که متقلبان به صنعت بانکداری وارد می‌سازند، بسیار بالاتر از رقمی است که این سازمان‌ها به‌طور مستقیم متضرر می‌شوند. به‌عنوان نمونه در سال‌های اخیر، بازارهای مالی ایالات متحده با افشای متعدد اعمال متقلبانه برخی شرکت‌ها به‌طور جدی متضرر شده‌اند. ورلدکام، انرون، آدلفیا، گلوبال کروسینگ و تیکو فقط تعداد اندکی از رسوایی‌های صورت‌های مالی هستند که بازار سهام را دچار نوسان کرد و موجب سلب اعتماد عمومی شد. از سوی دیگر، این رسوایی‌ها زیان‌هایی جبران‌ناپذیر بر سرمایه‌گذاران وارد آورده و توان رقابت آنها را از میان برده است. بسیاری از این رسوایی‌ها هم به پس‌انداز افراد، مزایای بازنشستگی، آموزش دانشگاهی و امنیت آینده آنها نیز زیان زده است.

این در حالی است که نتایج جدیدترین تحقیقات بانک جهانی، حکایت از افزایش روزافزون نرخ تقلب در بازارهای مالی دارد. به استناد این تحقیقات بیش از ۸۰ درصد سازمان‌های تحت مطالعه، نمونه‌هایی از تقلب را تجربه کرده‌اند. در نتیجه پرداختن به مقوله شناسایی تقلب‌ها در بازارهای مالی و شبکه بانکی، ضرورتی دو چندان یافته است.

تقلب در بانکداری الکترونیک

تقلب در بانکداری الکترونیک در بستر خدمات الکترونیک و به‌صورت برخط اتفاق می‌افتد و حاصل آن، انتقال پول الکترونیکی از یک حساب به حساب دیگر، به‌صورت نامشروع و غیرقانونی است. امروزه حجم زیادی از معاملات و نقل‌وانتقالات پولی و مالی در سطح اینترنت و در بستر الکترونیکی انجام می‌شود؛ بنابراین رشد روزافزون این خدمات و تراکنش‌ها از یک طرف و همچنین ناشناس ماندن مجرمان در بستر اینترنت از طرف دیگر، سبب تشویق و تحریک متقلبان و شیادان برای ورود به این حوزه می‌شود.

به‌دلیل عدم حضور فیزیکی مشتریان در بستر خدمات الکترونیک، لزوم تشخیص هویت در ارائه این خدمات از دیدگاه موسسات مالی و پولی بسیار حیاتی و بااهمیت است و شاید بتوان ادعا کرد که محدودیت اصلی در ارائه خدمات گسترده‌تر و وسیع‌تر بانکی، لزوم تشخیص هویت افراد است. این مسئله مهم‌ترین عامل جذابیت تقلب در بستر خدمات الکترونیک است که با توجه به گسترش خدمات بانکداری الکترونیک در حال افزایش است.

شناسایی انواع تقلب در بانکداری الکترونیک

به مجموعه عملیات یا اقدام‌هایی که بر اساس روش‌ها یا متدهایی، سعی در کشف و شناسایی تقلب‌های انجام شده یا در حال وقوع دارند، شناسایی تقلب گفته می‌شود. بااین حال مدت‌هاست که روش‌های سنتی تجزیه و تحلیل داده‌ها به‌عنوان یک روش برای تشخیص تقلب استفاده می‌شود. این کار نیاز به تحقیقات پیچیده و وقت‌گیری دارد و نیازمند به‌کارگیری حوزه‌های

مختلف دانش مانند مالی، اقتصادی، روش‌های کسب‌وکار و مباحث قانونی است. بنابراین موسسات مالی و پولی به‌شدت به‌دنبال سرعت عمل در شناخت فعالیت‌های کلاهبرداران و متقلبان هستند. ازاین رو در روش‌شناسی جدید شناخت تقلب، به‌طور گسترده این روش‌ها به دو دسته تشخیص سوءاستفاده و تشخیص ناهنجاری تقسیم می‌شوند.

ـ تشخیص سوءاستفاده

روش تشخیص سوءاستفاده تلاش می‌کند که حملات مشاهده شده قبلی را در قالب یک الگو یا امضا تشخیص دهد. به‌عنوان مثال، می‌توان به تغییر مداوم یک پوشه یا تلاش‌های متعدد به‌منظور خواندن یک فایل حاوی رمزهای عبور اشاره کرد. به‌عبارت دیگر می‌توان گفت که تشخیص سوءاستفاده به‌کارگیری حملات شناخته شده قبلی و علامت‌گذاری الگوی قابل تطبیق به‌منظور شناسایی تقلب‌های آتی است. دقت بالا از مزایای این روش است، اما بدیهی است که حملات جدیدی که قبلا توسط سیستم شناسایی نشده‌اند را شامل نمی‌شود. بنابراین سازوکار بسیار امنی نیست.

ـ تشخیص ناهنجاری

در روش تشخیص ناهنجاری تلاش می‌شود تا یک مشخصه از تاریخچه عملکرد برای هر کاربر ایجاد شده و سپس از استخراج هرگونه انحراف به‌قدر کافی بزرگ در مشخصه کاربر، به بروز یک حمله پی برده شود. به‌عبارت دیگر اگر بخواهیم تشخیص ناهنجاری را تعریف کنیم، شاید بهترین تعریف، تشخیص انحراف از آنچه انتظار داریم یا انحراف از رفتار نرمال باشد. این روش در حقیقت تشخیص تلاش‌های بدون مجوز به‌منظور دسترسی به سیستم است. در این روش رفتار معمولی تعریف شده است و هر رفتار دیگری، غیرطبیعی توصیف می‌شود. به‌دلیل محدود نبودن این روش، توانایی تشخیص حملات جدید از مزایای آن است.

نقطه ضعف این رویکرد هم این است که سنجش آماری مشخصه یک کاربر به‌تدریج می‌تواند آموخته شود؛ ازاین‌رو متقلبان می‌توانند در یک دوره زمانی خاص روی این سیستم‌ها آموزش دیده تا بتوانند حملات نامشروع خود را به‌صورت طبیعی و عادی جلوه دهند. در عین حال، روش تشخیص ناهنجاری به‌دلیل نیاز به نگهداری تاریخچه و اثر تاریخی مشخصه هر کاربر، از دیدگاه محاسباتی، روش گران قیمتی محسوب می‌شود.

تکنیک‌های تشخیص تقلب

با توجه به دو رویکرد تشخیص ناهنجاری و تشخیص سوءاستفاده، تکنیک‌های متعددی به‌منظور شناسایی تقلب در بانکداری الکترونیک طراحی و اجرا شده که در ادامه به برخی از آنها اشاره می‌شود.

ـ سیستم‌های خبره: سیستم‌های خبره به‌گونه‌ای از سیستم‌های محاسباتی اطلاق می‌شود که توانایی ارائه و استدلال در برخی از حوزه‌های غنی دانش با نگاه حل مشکلات و دادن راهکار داشته باشد. آشکارسازی سیستم‌های خبره، دانش را در قالب قانون اگر ـ سپس رمزگذاری می‌کنند. به این معنی که به کمک قانون اگر ـ سپس مشخص می‌کنند در چه حالتی؛ چه اتفاقی باید بیفتد.

ـ سازوکار برون‌هسته‌ای: سازوکار برون‌هسته‌ای به معنی مشاهده و استخراج انحراف‌هایی است که تفاوت‌هایی را با دیگر مشاهدات، تعیین می‌کند. این سازوکار به دو نوع بدون نظارت و با نظارت تقسیم می‌شود. رویکردهای بدون نظارت، نیازی به دانش قبلی و تاریخچه اتفاقات و تراکنش‌های قبلی در پایگاه‌های داده ندارند، اما با همین اوصاف، امکان تشخیص تغییرات را در رفتار تراکنش‌های غیرعادی دارند و می‌توانند هرگونه تغییری که منجر به تقلب می‌شود را شناسایی کنند. در تکنیک‌های با نظارت هم مدل‌هایی طراحی می‌شوند که می‌توانند بین رفتارهای تقلب‌گونه و رفتارهای عادی و واقعی تفاوت قائل شوند. اما در این روش‌ها به‌طور حتم باید تاریخچه‌ای از اطلاعات در بانک اطلاعاتی داشت تا بتوان، با مقایسه این داده‌ها، رفتارهای غیرعادی را شناسایی کرد.

ـ شبکه‌های عصبی: شبکه‌های عصبی مصنوعی امکان تشخیص رفتارهای آتی مشاهده نشده کاربران را در هر دو رویکرد تشخیص ناهنجاری و تشخیص سوءاستفاده فراهم می‌کنند. این روش‌ها بر اساس شبکه‌های عصبی پس‌پراکنی پیاده‌سازی می‌شوند.

ـ استدلال بر پایه مدل: استدلال بر پایه مدل یک تکنیک تشخیص سوءاستفاده است که حملات را از طریق فعالیت‌های قابل مشاهده‌ای که از طریق یک امضای حمله استنتاج می‌شود، تشخیص می‌دهند. برای این منظور، به یک بانک اطلاعاتی از سناریوی حملات و شامل امضا یا دنباله‌ای از رفتار حملات نیاز است. دقیقا مشابه روال کار نرم‌افزارهای ویروس‌یاب است که از روی امضای هر ویروس روی فایل‌ها، پی به‌وجود ویروس می‌برند، این تکنیک نیز از طریق امضا و بانک اطلاعاتی که در اختیار دارد، حمله را شناسایی می‌کند.

ـ رویکرد مبتنی بر قواعد: این روش ترکیبی است از کاربردهای تجزیه و تحلیل مطلق و تفاضلی. در تجزیه و تحلیل تفاضلی، یک‌سری معیارهای قابل انعطافی می‌توانند پیاده‌سازی شوند تا هر گونه تغییر در جزئیات تاریخچه رفتار یک کاربر را شناسایی کنند. رویکردهای مبتنی بر قواعد عموما با شناسه کاربرانی که شامل اطلاعات شفافی هستند و در آنها معیارهای تقلب به قواعد اشاره می‌کنند، بهترین عملکرد را دارند. مدیریت کردن این روش کاری بسیار دشوار بوده و این مسئله به‌دلیل این است که پیکربندی مناسب قواعد، نیازمند برنامه‌نویسی بهترین راه‌حل در سیستم‌های شناسایی تقلب، تجمیع و ترکیب رویکردهای تشخیص سوءاستفاده و تشخیص ناهنجاری است.

ـ داده کاوی: از روش‌های داده‌کاوی نیز می‌توان برای تشخیص حملات استفاده کرد. یکی از مزایای فوق‌العاده روش‌های داده‌کاوی در تشخیص حملات، امکان پیاده‌سازی کلاسی از مدل‌هاست که می‌تواند حملات جدید را قبل از آنکه هوش انسانی آنها را تشخیص دهد یا توسط متخصصان مشاهده شود، شناسایی و ارائه کند.

ـ تجزیه و تحلیل حالت گذار: این روش یک تکنیک تشخیص سوءاستفاده است که در آن، حملات به‌عنوان دنباله‌ای از حالت گذار سیستم مونیتور شده و نمایش داده می‌شود. فعالیت‌هایی که در یک حمله اتفاق می‌افتند، به‌عنوان یک گذار بین حالت‌ها تعریف می‌شوند.

ـ الگوریتم ژنتیک: یکی دیگر از روش‌های تشخیص تقلب، الگوریتم ژنتیک است که به‌منظور تشخیص حملات مخرب و جداسازی آنها از استفاده‌های عادی و طبیعی به‌کار می‌رود. الگوریتم ژنتیک روشی از هوش مصنوعی است. این الگوریتم به گونه‌ای است که در آن، هر فردی به‌عنوان یک مدل رفتاری ممکن عمل می‌کند. بنابراین این رویکرد یک نرخ تشخیص بالا و همچنین یک نرخ هشدار اشتباه پایین را فراهم می‌کند.

پیشنهاد

با توجه به مطالب ارائه شده، بهترین راه‌حل در سیستم‌های شناسایی تقلب، تجمیع و ترکیب رویکردهای تشخیص سوءاستفاده و تشخیص ناهنجاری است. استفاده ترکیبی از رویکرد تشخیص سوءاستفاده و تشخیص ناهنجاری، موجب تجمیع مزایای دو روش شده و نقاط ضعف هر یک از روش‌ها را نیز پوشش می‌دهد. همچنین فارغ از بحث فنی، ذکر این نکته نیز در پایان بسیار ضروری به‌نظر می‌رسد که با توجه به رشد روزافزون خدمات مالی بانک‌ها و موسسات مالی‌واعتباری به‌صورت الکترونیکی در سطح کشور و افزایش ضریب نفوذ استفاده کاربران از خدمات بانکداری الکترونیک؛ رویکرد کلاهبرداران و متقلبان به‌سمت بانکداری الکترونیک نیز رو به افزایش است. به این ترتیب در صورت عدم به‌کارگیری سازوکارهای تشخیص و جلوگیری از تقلب، باید شاهد افزایش آمار تقلب‌ها در فضای بانکداری الکترونیک باشیم.

امضای دیجیتال، گذر ناگزیر الکترونیکی شدن امور؛

امضای کدگذاری شده

امضای دیجیتال نوعی رمزنگاری نامتقارن است. هنگامی که پیغامی از کانالی ناامن ارسال می‌شود، یک امضای دیجیتال که به شکل صحیح به انجام رسیده باشد، می‌تواند برای شخص گیرنده پیام دلیلی باشد تا ادعای شخص فرستنده را باور کند یا به‌عبارت بهتر شخص گیرنده از طریق امضای دیجیتال می‌تواند این اطمینان را حاصل کند که همان شخص فرستنده، نامه را امضا کرده است و نامه جعلی نیست. امضاهای دیجیتال شاید در بسیاری از جنبه‌ها مشابه امضاهای سنتی دستی هستند؛ اما انجام امضاهای دیجیتال به شکل صحیح بسیار متفاوت از یک امضای دستی است. از این‌رو در گزارش حاضر تلاش شده تا ضمن معرفی امضای نوین دیجیتال، به تشریح زوایای آن بپردازد.

از امضای سنتی تا امضای دیجیتال

امضا، نشانه هویت یک فرد است. کسی که یک نامه، رسید بانکی یا سندی را امضا می‌کند در حقیقت نشانه‌ای از خود باقی می‌گذارد که نماد هویت اوست. این نماد به‌گونه‌ای است که اگرچه همگان می‌توانند آن را بشناسند، اما کسی توان تولید آن را ندارد و منحصر به یک فرد است. در دنیای الکترونیک و فناوری نیز موضوع تصدیق هویت، یکی از موضوعات مهم امنیتی است، از این رو ایده امضای دیجیتالی در جهان فناوری اطلاعات، همانند امضای واقعی، ابزاری مهم برای نیل به هدف تصدیق هویت و امنیت است. این مفهوم برای اولین‌بار به شکلی خام و در سال ۱۹۷۶ وارد ادبیات دیجیتال شد، اما به‌تدریج به تکامل و بلوغ رسید.

امضای دیجیتال چیست؟

با شنیدن واژه «امضای دیجیتال» افراد ممکن است دچار سوءتفاهم شوند و تصورهای متفاوتی از امضای دیجیتال داشته باشند. از این‌رو ابتدا باید به تعریف درستی از امضای دیجیتال پرداخت.

اولین مورد استفاده از اصطلاح امضای دیجیتال را شاید بتوان اسکن کردن امضای یک شخص و کپی کردن آن پای مدارک عمومی و نه‌چندان مهم شرکت‌ها و سازمان‌ها دانست. برای مثال از طرف یک سازمانی می‌خواهند به هزار نفر لوح تقدیر اهدا کنند و امضای مدیر یا رئیس هم باید پای آن باشد. در این مورد مدیر یا رئیس سازمان به احتمال زیاد وقت آزاد برای هزار امضا را ندارد. بنابراین او یک بار یک برگه سفید را امضا می‌کند و آن را اسکن می‌کنند و سپس روی تک تک برگه‌هایی که لازم است، آن را کپی می‌کنند. این مورد در سازمان‌ها، وزارتخانه‌ها، اتحادیه‌ها و شرکت‌های بزرگ کاربرد زیادی دارد.

مورد دومی که از اصطلاح امضای دیجیتال برای آن استفاده می‌شود امضا با مدادی نوری بر روی سیگنچر پد (Signature Pad) است. در این مورد فرد با یک مداد الکترونیکی روی یک صفحه نمایش لمسی امضا می‌کند. از مزایای این نوع امضا این است که سیستم می‌تواند سرعت حرکت مداد امضا، مقدار فشار دست و مواردی این چنینی را هنگام امضا کردن اندازه‌گیری کند و آنها را با نمونه امضای ثبت شده در سیستم مقایسه کند تا از جعل امضا و جعل هویت جلوگیری کند. یعنی حتی اگر یک شخص از لحاظ ظاهری کاملا شبیه شما بوده و امضای شما را هم بلد باشد باز هم نمی‌تواند خودش را جای شما زده و سوءاستفاده کند. این مورد امضا بیشتر در بانک‌ها و دفاتر اسناد رسمی و محضرها استفاده می‌شود.

اما مورد سوم که در واقع امضای دیجیتال به‌معنای واقعی کلمه است، در واقع هیچ شباهتی با تصور ما از یک امضا ندارد. به زبان ساده این

امضای دیجیتال یک نام کاربری و یک رمز است که در سیستم اسنادی به نام شما ثبت می‌شود و در دنیای مجازی و الکترونیکی کارت هویت شماست. در واقع به کمک این نام کاربری و رمز آن، شما در دنیای مجازی نه‌تنها می‌توانید ثابت کنید که دقیقا چه کسی هستید بلکه می‌توانید ثابت کنید اطلاعاتی که برای طرف دیگر می‌فرستید بدون هیچ دخل و تصرفی از سوی شما فرستاده شده است.

امضای دیجیتال چگونه امنیت را تامین می‌کند؟

به زبان ساده، تبادل اطلاعات در دنیا به روش‌های مختلف می‌تواند انجام شود. ساده‌ترین روش، انتقال اطلاعات به‌صورت text Plain یا همان متن ساده است. یعنی نفر اول اطلاعاتی را از کانالی به نفر دوم منتقل می‌کند و اطلاعات به همان شکلی که فرد اول فرستاده بود به دست نفر دوم می‌رسد. اما به مرور و با ارزشمند شدن اطلاعات و بالا رفتن حجم اطلاعات قابل انتقال از طریق بسترهای الکترونیک، دیگر تبادل اطلاعات به شکل ساده، شیوه‌ای امن نیست. زیرا ممکن است در میان کانال ارتباط، اطلاعات توسط نفر سومی مشاهده شده، دست‌کاری یا به کلی عوض شود و سپس به دست نفر دوم برسد. برای جلوگیری از این لو رفتن اطلاعات، کاربرهای اول و دوم یک‌سری رمز بین خود تعریف می‌کنند تا انتقال اطلاعات به‌صورت رمز شده انجام شود. این رمزها همان امضای دیجیتال است.

امضای دیجیتال امنیت چه چیزی را تامین می کند؟

تصدیق هویت، محرمانه بودن، امانت‌داری و غیرقابل انکار بودن مواردی هستند که امضای دیجیتال امنیت آنها را تامین می‌کند.

تصدیق هویت: اطمینان از اینکه شخص یا طرفی که با آن در حال ارتباط هستیم همان کسی است که ما انتظار داریم و خودش می‌گوید.

محرمانه بودن: اطلاعات درون پیغام‌ها یا تبادلات، محرمانه شده و تنها برای اشخاص دریافت‌کننده و ارسال‌کننده قابل فهم و خواندن است.

امانت‌داری: اطلاعاتی که درون پیغام یا تبادلات وجود دارد در طول مسیر به‌طور اتفاقی یا عمدی مورد دستبرد قرار نمی‌گیرند.

غیر قابل انکار بودن: ارسال‌کننده نمی‌تواند منکر ارسال پیام یا تبادل مالی شده و دریافت‌کننده هم نمی‌تواند منکر دریافت آن شود.

ایجاد امضای دیجیتال

قبل از آشنایی با نحوه عملکرد یک امضای دیجیتال، لازم است در ابتدا با برخی اصطلاحات مرتبط با این موضوع مانند کلیدها، حلقه کلید، اثر انگشت و گواهینامه‌های کلید آشنا شویم.

کلیدها (Keys): از کلیدها به‌منظور ایجاد امضاهای دیجیتال استفاده می‌شود. برای هر امضای دیجیتال، یک کلید عمومی و یک کلید خصوصی وجود دارد. کلید خصوصی، بخشی از کلید است که شما از آن به‌منظور امضای یک پیام استفاده می‌کنید. کلید خصوصی یک رمز عبور حفاظت شده است و نباید آن را در اختیار دیگران قرار داد. کلید عمومی هم بخشی از کلید است که امکان استفاده از آن برای سایر افراد وجود دارد. زمانی که کلید یادشده برای یک حلقه کلید عمومی یا یک شخص خاص ارسال می‌شود، آنان با استفاده از آن قادر به بررسی امضای شما خواهند بود.

حلقه کلید (Key Ring): شامل کلیدهای عمومی است. یک حلقه کلید از کلیدهای عمومی افرادی که برای شما کلید مربوط به خود را ارسال کرده یا کلیدهایی که از طریق یک سرویس‌دهنده کلید عمومی دریافت کرده‌اید، تشکیل می‌شود. یک سرویس‌دهنده کلید عمومی شامل کلید افرادی است که امکان ارسال کلید عمومی در اختیار آنان گذاشته شده است.

اثر انگشت: زمانی که یک کلید تایید می‌شود در حقیقت منحصربه‌فرد بودن مجموعه‌ای از حروف و اعداد که اثر انگشت یک کلید را شامل شده، تایید می‌شود.

گواهینامه‌های کلید: در زمان انتخاب یک کلید از روی یک حلقه کلید، امکان مشاهده گواهینامه (مجوز) کلید وجود خواهد داشت. در این رابطه می‌توان به اطلاعات متفاوتی مانند صاحب کلید، تاریخ ایجاد و اعتبار کلید دست یافت.

اما به‌طور خلاصه برای ایجاد یک امضای دیجیتال، ابتدا امضاءکننده باید از طریق کلید عمومی امضای خود را رمزسازی کرده و سپس آن را ضمیمه پیام داده‌ای کند و برای مخاطب خویش ارسال کند. مخاطب که اکنون پیام داده‌ای را به همراه امضای دیجیتال آن دریافت کرده، باید امضای رمزنگاری شده را که قابل فهم نیست از داده پیام‌ها جداکرده و از طریق کلید عمومی ارسال‌کننده، پیام را برای او ارسال کند تا خود ارسال‌کننده با کلید خصوصی‌اش آن را رمزگشایی کند. چنانچه نتایج یکسانی حاصل شد، یعنی همان چیزی که امضاکننده به‌عنوان امضای دیجیتال برای خود تعریف کرده بود و هویدا شد، معلوم می‌شود که نخست امضای یادشده به‌نحو صحیحی از سوی امضاءکننده ارسال شده و سپس او نمی‌تواند ادعا کند که پیام را امضا نکرده یا اینکه پیام تغییر یافته است. بنابراین، به‌کارگیری امضای دیجیتال شامل دو فرآیند است:

- مرحله اول ایجاد امضاء توسط ارسال‌کننده پیام و به‌وسیله کلید خصوصی‌اش است.
- مرحله بعد هم شامل فرآیند چک کردن امضای دیجیتال از طریق مراجعه به پیام اصلی و استفاده از کلید عمومی ارسال‌کننده است.

روش‌های تهیه و تولید امضای دیجیتالی

در طول سال‌ها تحقیق در زمینه امنیت کامپیوتر، روش‌ها و متدهای مختلفی برای امضاهای دیجیتالی ابداع شده ولی چیزی که در همه آنها عمومیت دارد این است که همه روش‌های تولید امضای دیجیتالی به ماهیت پیام وابسته‌اند. با این حال، روش‌های زیر از مهم‌ترین روش‌های تولید امضای دیجیتالی هستند.

امضاهای دیجیتالی مبتنی بر چکیده پیام؛ در این روش متن پیام دست نخورده باقی مانده و تنها یک امضای چند بایتی به آن اضافه می‌شود.

امضاهای دیجیتالی کلید متقارن؛ این امضاها مبتنی بر یک مرکز گواهی امضا هستند.

امضاهای مبتنی بر روش‌های رمزنگاری کلید عمومی

امضاهای مبتنی بر تبدیل‌های مستقل از سیستم‌های رمزنگاری

ویژگی‌های امضاهای دیجیتال

مهم‌ترین ویژگی‌های امضاهای دیجیتال را می‌توان به‌شرح زیر دسته‌بندی کرد.

۱. در تولید آنها از اطلاعاتی که به‌طور منحصر به‌فرد در اختیار امضاکننده است، استفاده می‌شود.

۲. به‌طور خودکار و توسط رایانه تولید می‌شوند.

۳. امضای هر پیام وابسته به کلیه بیت‌های پیام است و هر گونه دست‌کاری و تغییر در متن سند، موجب مخدوش شدن امضای پیام می‌شود.

۴. امضای هر سندی متفاوت با امضای اسناد دیگر است.

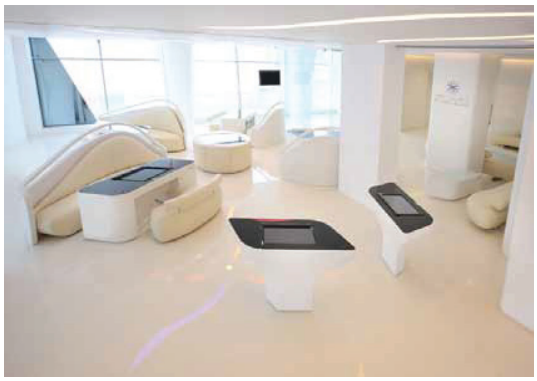
۵. امضای دیجیتال باید به‌راحتی قابل بررسی و تایید باشد تا از جعل و انکار احتمالی آن جلوگیری شود.

۱۰ تاثیر توسعه بانکداری الکترونیک بر طراحی شعب بانک‌ها

از شعبه تا شبکه

شعبه، پیشانی بانکداری است؛ محل تلاقی بانکدار با مشتری، محلی که مشتری آخرین نیازهای خود را در آن مطرح کرده و بانکدار هم آخرین سرویس‌ها و خدمات خود را به مشتری عرضه می‌کند. از این‌رو شعبه را پیشانی بانک می‌دانند. حال شکل و شمایل این پیشانی سیستم بانکی، طی ده‌ها سال بانکداری سنتی، الگوی خاص و واحد خود را پیدا کرده و تمام بانک‌ها هم با درصدی تغییر از آن پیروی می‌کنند: باجه‌هایی متحدالشکل برای ارائه سرویس‌هایی یکسان به مشتریانی که نیازهای متفاوتی دارند.

اما به‌واسطه توسعه بانکداری الکترونیک، معماری شعب بانک‌ها دچار تغییر و تحولاتی شده‌اند و در حال فاصله گرفتن از شکل سنتی هستند؛ تغییراتی که هنوز آنچنان که باید به شعب بانک‌های ایرانی راه نیافته است. از این رو در گزارش پیشرو که توسط احسان باقری، کارشناس ارشد بازاریابی خدمات بانکی تهیه شده است، ۱۰ تاثیر بانکداری الکترونیک بر معماری شعب را با تصاویر مرتبط مرور خواهیم کرد.



طراحی دکوراسیون داخلی و خارجی

یکی از تاثیرات مهم بانکداری الکترونیک، بر طراحی دکوراسیون داخلی و خارجی شعب است. معماری در عصر جدید آنگاه معنا و مفهوم خود را می‌یابد که علاوه بر بهره‌گیری از عناصر هویت‌ساز بانک، با پارادایم عصر جدید مانوس و همنشین شود و تردیدی نیست که یکی از مهم‌ترین شاخص‌ها و مولفه‌های عصر حاضر «فناوری اطلاعات و ارتباطات» است. تجربه طراحی مدرن شعب Burgan bank بانک برگن (عکس شماره یک) یکی از الگوهای نوین و موفق در این خصوص به‌شمار می‌رود.

بانکداری مجازی

یکی از پارادیم‌های جدید بانکی مبتنی بر بانکداری الکترونیک، بانکداری مجازی است. بانکداری مجازی یک راهکار نو، خلاق و چابک در عرصه بانکداری محسوب می‌شود که محصولات و خدمات بیشتر، اختصاصی‌تر و متنوع‌تری را با سهولت بیشتر و قیمت کمتر به مشتریان عرضه می‌کند. اما بانک‌های برتر دنیا به تجربه آموخته‌اند که باید هرچه بیشتر درصدد نمایش واقعی بانکداری مجازی برای مشتریان خود باشند. تجربه بانک ING در این‌باره یکی از موارد بسیار خلاق و کاربردی است. این بانک در تلاش است تا با ایجاد شعبی موسوم به «کافی بانک» (عکس شماره ۲) هرچه بیشتر و بهتر خدمات بانکداری مجازی را واقعی کرده و نمایش دهد. در این فروشگاه‌ها علاوه بر ارائه خدمات و فروش محصولات متنوع، زمینه‌های استفاده از خدمات بانکداری مجازی نیز پیگیری می‌شود. از سوی دیگر بانک در تلاش است تا برند بانکداری مجازی خود را در ذهن مشتریان تثبیت و واقعی کند.

شعب هوشمند

آمارها نشان می‌دهد، بیش از ۸۰ درصد فروش محصولات بانکی، در داخل شعبه انجام می‌شود؛ در نتیجه بانک‌ها شعب خود را باید به‌نحوی آرایش دهند که به‌عنوان یک مرکز راهبردی برای ارائه خدمات بانکداری فعالیت کنند. در عصر فناوری‌های نوظهور یکی از ایده‌های مورد استفاده، بهره‌گیری از الگوهای برتر در طراحی مکان‌های هوشمند مانند فروشگاه‌های شرکت‌های تولیدکننده تجهیزات فناوری اطلاعات است. تجربه CITI BANK نمونه موفقی از این ایده است (عکس شماره ۳). طراحی این شعب موید یک مکان دریافت خدمات به‌صورت کاملا دیجیتالی است.

شعب چند منظوره

در طراحی شعب جدید، ارائه برخی از خدمات نوین که در نظام بانکی کمتر به آن پرداخته شده، مورد توجه قرار گرفته است. شعب بانکی امروزه کانال ارائه محصولات و خدمات صنایع مالی چون بیمه، لیزینگ و ... است. در نتیجه ظهور شعبی با عنوان شعب چند منظوره برای پشتیبانی از چنین ایده‌ای به واقعیت پیوسته است. بانکداری الکترونیک یکی از مهم‌ترین ابعاد طراحی این شعب به‌شمار می‌آید زیرا این شعب برای ارائه خدمت به تعداد زیادی از مشتریان طراحی شده‌اند. نمونه این شکل از شعب در بانک BARCLAYS به تصویر کشیده شده است (عکس شماره ۴).

خودخدمتی

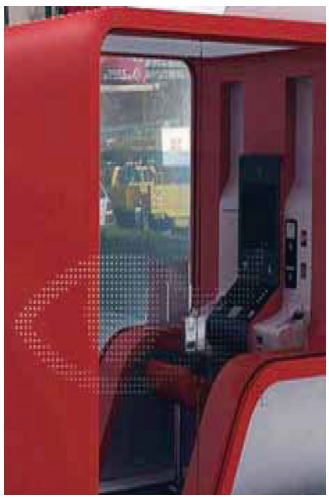
بر اساس پیشرفت‌های تکنولوژیک در حوزه بانکداری الکترونیک، نوع جدیدی از فرهنگ خدمات‌دهی بانکی تعریف شده که بر اساس آن بسیاری از خدمات به‌صورت خودخدمتی یا سلف‌سرویس ارائه می‌شود. همان‌گونه که در تصویر مربوط (عکس شماره ۵) به شعب رویال‌بانک RBSمشخص شده، طراحی و معماری شعب بر مبنای حمایت از این فرایند انجام شده است.

استفاده بهتر از فضای شعب

یکی از مهم‌ترین هزینه‌های بانکی هزینه‌های مرتبط با ایجاد و نگهداری شعب است. بی‌جهت نیست که بسیاری از بانک‌ها برای مدیریت این هزینه‌ها، سودآوری هر شعبه را به‌صورت مجزا بررسی و سنجش می‌کنند. با این حال بانکداری الکترونیک با ویژگی ماهوی خود در کاهش هزینه‌ها از راه‌های گوناگون، این‌بار نیز به کمک مدیریت شعب آمده تا آنها را به حداکثر بهره‌وری نزدیک کند. یکی از ده‌ها مورد این شکل از پشتیبانی می‌تواند بهره‌برداری از تمام فضای شعب به‌ویژه دیوارهای آن از طریق نمایشگرهای هوشمند برای ارائه خدمات اطلاعاتی و خدمات بانکداری الکترونیک باشد.

شکل‌های جدید شعب

یکی از بارزترین ویژگی‌های ورود بانکداری الکترونیک به عرصه بانکداری آن است که شکل‌های سنتی و متعارف و یکسان شعب را به شکل‌های جدید، منعطف و بسیار متنوع تغییر داده است. بانکداری الکترونیک مدعی است بعد زمان و مکان را در نوردیده است. ادعای دیگر می‌تواند تنوع‌بخشی به شکل‌های مختلف شعبه باشد. ادعایی که نمونه آن در عکس نمایان است.



مواجهه با مشتری

شاید برخی ادعا کنند که بانکداری الکترونیک، مواجهه از طریق ابزارهای الکترونیک را جایگزین مواجهه مستقیم با مشتری کرده است. اگرچه تحقیقات در کشورها و بانک‌های مختلف نتایج متفاوتی را نشان می‌دهد؛ با این حال و با پذیرش این فرض، باید توجه داشت که بانکداری الکترونیک، مواجهه مستقیم مربوط به دریافت و پرداخت را بیشتر تحت تاثیر قرار داده است. اما دیگر مواجهه‌ها مانند دریافت مشاوره یا دریافت وام هنوز در شعب انجام می‌شود. از سوی دیگر شکل‌های جدید مواجهه غیرحضوری با مشتری مانند ویدئوکنفرانس جایگزین مواجهه‌های مستقیم در شعبه شده است. این امر سبب شده تا در معماری شعب فضایی برای این تبادلات در نظر گرفته شود. نقطه قابل توجه دیگر در مواجهه با مشتری همانگونه که در عکس شماره ۷ مشخص است، مشارکت بیشتر در دریافت خدمات است، به‌طوری که می‌توان چرخش مانیتورها به‌سوی مشتری و استفاده از نرم‌افزارهای کاربرپسند را یکی دیگر از تغییرات بنیادین در شعب توصیف کرد که بر معماری و طراحی آن تاثیر می‌گذارد.

باجه‌های جدید

یکی دیگر از تغییرات بنیادین حاصل از تاثیر بانکداری الکترونیک بر معماری و طراحی شعب، ایجاد باجه‌های جدید است. این باجه‌های جدید علاوه بر تغییر در فرآیندهای ارائه خدمات، در معماری و طراحی شعب نیز موثرند. چیدمان، طراحی و جانمایی آنها مباحثی است که باید به‌دقت مد نظر قرار گیرند. نمونه‌ای از باجه‌های جدید در عکس شماره ۸ نمایش داده شده است.

ابزارهای نوین بانکداری الکترونیک

ابزارهای متداول بانکداری الکترونیک نقش به‌سزایی در طراحی، چیدمان و شکل شعب دارند. ورود ابزارهای بانکداری الکترونیک به شعب علاوه بر اینکه کارکردهای شعب را تغییر داده و آن را بازآفرینی کرده، طراحی آن را به کلی متفاوت و متمایز کرده است. از سوی دیگر خود این تجهیزات نیز در طول زمان بهبود یافته و کارآمدتر شده‌اند. بنابراین تغییرات آنها در فرآیند طراحی یکپارچه شعب تاثیر متقابل داشته است. به‌عنوان نمونه دستگاه‌های خودپرداز جدید بانک BBVA یکی از نمونه‌های رایج است (عکس شماره ۱۰) که در کنار توسعه کارکردها، بر طراحی شعب نیز تاثیر گذاشته است.

مشتری‌مداری در محیط الکترونیکی، چالش امروز بانک‌ها

کلیک‌هایی که ارتباط با مشتری را مدیریت می‌کنند

اینکه یک مشتری از خدمات شما راضی باشد بسته به خدماتی است که یک موسسه ارائه می‌کند یا اینکه نحوه ارائه خدمات مهم است؟ سرویس‌هایی که به مشتری ارائه می‌شود باید تمام سلایق یک مشتری را تامین کند یا اینکه منافع عمومی مشتریان را در نظر گیرد؟ تامین خواست و نیاز مشتری حول عنوان مشتری مداری شکل می‌گیرد یا اینکه مشتری‌محوری مطرح است؟ تمام این سوالات و سوالات بسیار دیگر، چالشی است که امروزه موسسات بزرگ جهان و در راس آن بانک‌ها با آن مواجهند که چطور با مشتریان خود برخورد کنند تا هم مشتریان قدیمی را از دست ندهند و هم بر میزان مشتریان خود بیفزایند. امروزه تأمین نیازهای مشتریان، مخاطبان و کسب رضایت و اعتماد آنها در واقع نشان از موفقیت سازمان‌ها در پیشبرد اهدافشان دارد. چراکه در بازار فعلی که تولید انبوه کالا و خدمات زمینه افزایش عرضه نسبت به تقاضا را فراهم آورده برای سازمان‌ها و تولیدکنندگان راهی جز جلب رضایت مشتری باقی نمانده است. تجربه نشان داده است، سازمان‌هایی که از منظر سنتی به مفاهیم مشتری، کالا، بازار، فروش، خرید، رقابت، تبلیغات کیفیت نگاه می‌کنند علاوه بر عدم کسب موفقیت، نه‌تنها سرمایه‌های خود را از دست می دهند بلکه با ظهور اقتصاد رقابتی با بی اهمیت شمردن مفاهیمی چون مشتری‌مداری و کسب رضایت مشتری، به‌سرعت از صحنه بازار حذف خواهند شد. اما؛ پرداختن به اهمیت مقوله‌ای به نام مشتری‌مداری، تکرار مکررات است؛ که امروزه تمام سازمان‌ها و نهادها این شعار را که «همیشه حق با مشتری است» نصب‌العین خود کرده و البته برخی در قاب نهاده و کاربردی تزئینی به آن بخشیده‌اند. با این حال، آنچه گردآوری مقال پیشرو را ضرورت می‌بخشید، ترویج کسب‌وکار در محیط الکترونیکی، گذر سازمان‌ها از مرحله سنتی به دوران الکترونیک و توسعه چشمگیر بانکداری الکترونیک است. بانک‌هایی که طی سال‌ها آموخته‌اند در برخورد حضوری با مشتری خود چگونه نیازهای او را پاسخ گویند و به‌عبارتی مشتری خود را مدیریت کنند، اینک با چالشی جدید مواجه شده‌اند: «مدیریت مشتری در فضای مجازی». یعنی باید مشتریانی را مدیریت کنند که ارتباطشان با آنها در حد چند کلیک است. از این‌رو در نظر داریم تا در گفتار پیشرو نگاهی گذرا داشته باشیم به تفاوت‌های مشتری‌مداری در فضای سنتی و محیط الکترونیکی و طرح راهکارهایی برای مدیریت مشتریانی که تنها ارتباطشان با سازمان به فضای مجازی محدود می‌شود.

ضرورت وجودی

با توجه به اینکه هر روز کسب‌وکار و خرید مشتریان در اینترنت در حال افزایش است، تمام سازمان‌های امروزی و در راس آن بانک‌ها برای ادامه حیات باید خود را در برابر پدیده جدیدی با عنوان مدیریت ارتباط با مشتری الکترونیکی سازگار کنند. مدیریت ارتباط با مشتری الکترونیکی به گسترش در زمینه سیستم‌های اطلاعاتی و رشته‌های مربوط به آن مثل علم کامپیوتر، بازاریابی و روان‌شناسی می‌پردازد. ضرورت وجودی مشتری‌مداری در فضای مجازی، این است که خریدارانی که برای اولین بار به سایتی مراجعه می‌کنند، لزوما مشتریان دائمی آنان نیستند و مشتریان دائمی هم می‌توانند به سهولت خدمات خود را از سایت دیگری دریافت کنند، بدون اینکه به قیود زمان و مکان توجه داشته باشند. ازاین‌رو با توجه به اینکه هزینه بازاریابی برای ایجاد مشتری جدید، بالغ بر پنج برابر حفظ مشتریان قبلی برآورد می‌شود، سازمان‌ها باید در حفظ مشتریان خود در فضای مجازی برنامه مدون داشته باشند.

اداره مشتری در فضای سنتی

مدیریت ارتباط با مشتری یک استراتژی برای انتخاب، نگهداری و اداره کردن مشتریان، به‌منظور ایجاد ارزش در درازمدت است. سیستم مدیریت ارتباط با مشتری، یک راهکار تجاری از طریق نرم‌افزار و فنونی که برای کمک بیشتر به مدیریت موثر ارتباطات مشتری در کانال‌های مستقیم یا غیرمستقیم مرتبط شده‌اند، است. مدیریت ارتباط با مشتری از بازاریابی یک به یک به‌منظور سفارشی کردن محصولات خدمات برای مشتری استفاده می‌کند که شامل یک فرآیند جمع‌آوری داده پیوسته در تمام‌مدت، تماس با مشتری و سپس تبدیل این داده‌ها به دانش برای ایجاد ارتباط موثرتر با مشتری به‌منظور سودآوری بیشتر است.

ترکیبی از سخت افزار، نرم‌افزار و تعهدات مدیریتی

مدیریت ارتباط با مشتری الکترونیکی یک استراتژی بازاریابی، فروش و خدمات برخط یکپارچه است که در شناسایی، به دست آوردن و نگهداری مشتریان که

بزرگترین سرمایه سازمان‌ها هستند، ایفای نقش می‌کند. مدیریت ارتباط با مشتری الکترونیکی، ارتباط بین شرکت با مشتریانش را به‌وسیله ایجاد و افزایش ارتباط با مشتری از طریق تکنولوژی جدید، بهبود و افزایش می‌بخشد. نرم‌افزار مدیریت ارتباط با مشتری الکترونیکی، پروفایل‌ها و تاریخچه‌ای از هر تماس سازمان با مشتریانش به‌وجود می‌آورد. در مجموع می‌توان گفت مدیریت ارتباط با مشتری در بانکداری الکترونیکی، ترکیبی از سخت‌افزار، نرم‌افزار، کاربردها و تعهدات مدیریتی است.

کسب‌وکار مبتنی بر استراتژی مشتری‌محور

دو نوع مدیریت ارتباط با مشتری الکترونیکی می‌توان متصور بود که اولی مدیریت ارتباط با مشتری الکترونیکی عملیاتی است و دیگری مدیریت ارتباط با مشتری الکترونیکی تحلیلی. مدیریت ارتباط با مشتری الکترونیکی عملیاتی شامل مراکز تماس با مشتری مانند تلفن، نمابر و پست الکترونیکی که مشتریان از طریق آنها با سازمان در تماسند، می‌شود. اما مدیریت ارتباط با مشتری الکترونیکی تحلیلی، نیازمند تکنولوژی است تا داده‌های زیادی از مشتری را فراهم کند. هدف این بخش، تجزیه و تحلیل داده‌های مشتری، الگوهای خدمات مورد نیاز و فاکتورهای مهم دیگری است که سبب ایجاد فرصت‌هایی در کسب‌وکار جدید می‌شود. در مجموع، مدیریت ارتباط با مشتری الکترونیکی، فقط شامل نرم‌افزار و تکنولوژی نمی‌شود، بلکه شامل فرآیندهای کسب‌وکار مبتنی بر استراتژی مشتری محور است که به‌وسیله نرم‌افزار و تکنولوژی‌های مختلف پشتیبانی می‌شود.

مشتری احساس آرامش می‌کند

در جهان امروزی، ارتباط مشتریان با بانک از طریق کانال‌های ارتباطی مختلفی چون شبکه وب، مراکز تلفن، شعب، باجه‌ها، ای‌تی ام و... انجام می‌شود. سیستم مدیریت ارتباط با مشتری الکترونیکی، مشتریان را به انجام کسب‌وکارها با سازمان تشویق خواهد کرد و راهی را به‌وجود می‌آورد که در آن مشتری هر نوع خدماتی را در هر زمانی و از طریق هر کانالی و در هر زبانی که می‌خواهد، دریافت کند. در نتیجه مشتریان از اینکه با آنان به‌عنوان یک شخص منحصربه‌فرد رفتار می‌شود، احساس آرامش و راحتی می کنند.

مدیریت ارتباط

به‌طور کلی پنج اصل برای بانک‌ها در مدیریت ارتباط با مشتری الکترونیکی وجود دارد که عبارتند از:

۱. تکنولوژی
۲. فاکتورهای انسانی
۳. مدل‌های کسب و کار
۴. بازار
۵. مدیریت دانش.

مهم‌ترین بخش این موارد، تکنولوژی مدیریت ارتباط با مشتری الکترونیکی است. تکنولوژی‌های جدید، ارتباط بین مشتریان و بانک‌ها را تغییر می‌دهند. عمده این تکنولوژی‌ها به سه نوع تکنولوژی تاثیرپذیر مانند اتاق‌های گفت‌وگو و تابلوی اعلانات، تکنولوژی تاثیرگذار مانند نرم‌افزار سفارش‌دهنده و فهرست دهنده خدمات و تکنولوژی تعاملی مانند پست الکترونیکی و عامل‌های خرید تقسیم می‌شوند.

بخش دوم فاکتورهای انسانی هستند. این بخش شامل تعاملات مجازی بین مشتریان و نیز بین مشتریان و شرکت است. تجربه احساسات مشتری روی مولفه‌های انسانی مدیریت ارتباط با مشتری الکترونیکی که شامل رضایت، تعهد، رضایت از دریافت خدمات و محصولات و عوامل دیگر بوده، موثر است.

بخش بعدی مدل‌های کسب‌وکار در مدیریت ارتباط با مشتری الکترونیکی است. پنج فاکتور اساسی در این رابطه می‌توان ارائه کرد که شامل داشتن ارتباط درازمدت با مشتری، هماهنگ کردن کانال‌های ارتباطی، ساختن یک برند قوی، تغییر دادن ساختار سرمایه‌گذاری و هزینه‌ها و ایجاد ارزش‌افزوده برای مشتریان می‌شود.

بحث بعدی، بازارهای الکترونیکی است. معاملات تجاری در سه عبارت خلاصه می‌شوند: اطلاعات، قرارداد و پرداخت. این تعاملات در توسعه ارتباط مشتریان با یکدیگر و ارتباط آنها با شرکت مفید هستند. حال با توجه به اینکه اینترنت فقط یک رسانه نیست بلکه یک فضای بسیار گسترده و نامحدود است، بانک‌ها باید از فضا بهره جسته و هر روز استراتژی‌های جدیدی برای افزایش تاثیر برند خود در میان مشتریان به‌کار گیرند. مورد آخر هم مدیریت دانش است که این مورد داشته‌های چهار مورد قبل را هدایت و راهبری می‌کند تا بالاترین سطح بازدهی را داشته باشند.

مزایای مدیریت ارتباط با مشتری‌الکترونیکی

راضی نگه‌داشتن مشتریان فعلی سودآورتر از جذب مشتریان جدید است و بهترین راه برای راضی نگه داشتن مشتریان فعلی، ارزش گذاشتن به شرایط آنهاست. علاوه بر این مدیریت ارتباط با مشتری الکترونیکی مزایای متعدد دیگری هم دارد که از جمله آنها می‌توان به افزایش وفاداری مشتری، بازاریابی موثر، بهبود بخشیدن به خدمات و پشتیبانی مشتری و کارایی بیشتر و کاهش هزینه‌ها اشاره کرد.

جمع‌بندی

امروزه شرایط اقتصادی سبب شده که بودجه‌های فناوری اطلاعات به‌صورت دقیق و موشکافانه بررسی شوند، با این حال مدیریت ارتباط با مشتری همچنان به‌عنوان یک اولویت برای سازمان‌ها مطرح است. چراکه یک بانک برای ماندگاری و سودآوری چاره‌ای جز اجرای یک استراتژی مشتری‌محور ندارد. در نتیجه سازمان‌ها به‌منظور شکل‌دهی به یک استراتژی الکترونیکی موثر، باید یک تیم متخصص مجهز به مهارت‌های فنی و کسب‌وکاری که به ایجاد استانداردهای بالای خدمت‌رسانی به مشتری می‌انجامد را سامان‌دهی کند تا در بلندمدت تبدیل به استاندارد و برندی در مشتری‌مداری در فضای مجازی شود.

بانکداری موبایلی، پدیده‌ای که از شتابش برای گسترش کم نمی‌کند

این بانک، تعطیلی ندارد

عـدد متوسـط کاربران سـرویس موبایل در سراسـر دنیـا، در سـال ۲۰۱۰ کمتـر از ۱۰درصد کل مخاطبـان شـبکه بانکی بـود. عـددی که پایـان سـال ۲۰۱۲ بـه بیـش از ۲۰درصد بالغ شـد؛ این در حالـی اسـت که موسسـات پولـی و مالـی، پیش‌بینی می‌کننـد که کاربـران سـرویس موبایل بانـک تـا پایان سـال ۲۱۰۷ به بیـش از ۷۰ درصد کل مشـتریان شـبکه بانکی بالغ شـوند. از این‌رو ضـرورت دارد تـا مروری دوباره داشـته باشـیم بـر بنیان‌های این سـرویس جدید شـبکه بانکی، راهکارهای توسـعه آن و موانع پیشـرویش در کشـور.

امـروزه یکـی از شـیوه‌های نویـن مـورد توجه در عرضـه خدمـات بانکـی، ارائـه خدمـات بـا اسـتفاده از تلفـن همـراه اسـت. بـا اینکـه از عمـر اسـتفاده از تلفن‌هـای همـراه بـرای انجـام عملیـات بانکـی و مالـی بیـش از هفـت یـا هشـت سـال نمی‌گـذرد، پیشـرفت‌های مهمـی در ایـن زمینـه حاصـل شـده و نویددهنده گسـترش چشـمگیر این شـیوه جدید بانکـداری الکترونیکـی در آینـده اسـت؛ به‌گونـه‌ای کـه بیشـتر کشـورهای جهـان در عرصـه بانکـداری و ارائـه خدمـات مالـی خـود در ایـن بخـش، سـرمایه‌گذاری‌های کلانـی انجـام داده‌انـد.

تعریف

آنچـه بـه‌طـور عمومـی بـه‌عنـوان تعریـف موبایل‌بانـک در متـون بانکـداری و مالـی ارائه‌شـده، به‌کارگیـری تلفن‌هـای همـراه در دریافـت خدمـات بانکـی و مالـی اسـت. بـه ایـن معنـا که موسسـه یا بانـک عامـل می‌توانـد خدمـات خـود را از طریـق اینترنـت در اختیـار مشـتریان قرار دهد و مشـتریان بـرای دریافـت خدمـات مـورد نیـاز خـود می‌توانند، بـا اتصـال بـه اینترنـت از طریـق تلفن‌هـای همـراه خـود، خدمـات عرضه‌شـده بانـک یا موسسـه عامل را مسـتقل از زمـان و مـکان دریافت کننـد. اما آنچه در تعریـف موبایل‌بانـک مـورد توجـه قـرار می‌گیرد، انـواع خدمـات ارائه‌شـده و نیز انـواع شـیوه‌های ارائه خدمـات در قالـب بانکـداری از طریـق تلفن‌همراه یا به‌عبارتـی موبایل‌بانـک اسـت. در ایـن زمینـه آنچـه بیشـتر در تعریف بانکـداری از طریـق تلفن‌همراه در انـواع خدمـات ارائه‌شـده و شـیوه‌های آن مورد توجه قـرار می‌گیـرد، در شـکل سـاده آن، امکان مشـاهده تـراز حسـاب توسـط مشـتری از طریـق دریافـت پیامـک توسـط بانـک عامـل اسـت کـه روی صفحه تلفن‌همراه مشتری قابل مشـاهده است و مشتری با دریافـت آن می‌توانـد بدون نیاز به مراجعه مسـتقیم یـا بدون متوصل‌شـدن به شـیوه‌های دیگـر خدمات بانکـی از قبیل اینترنت، رایانه و ...، از آخرین وضعیت حسـاب‌های خود مطلع شـود. این روش، سـاده‌ترین شـیوه عرضـه خدمـات موبایل‌بانک، شـناخته شـده اسـت. ایـن قبیـل عرضـه خدمـات موبایل‌بانک تنها بـه امـکان ارتبـاط بیـن بانـک و تلفن‌هـای همـراه مشـتریان بانـک بسـتگی دارد. درواقع چنین شـیوه عرضـه خدمـات موبایل‌بانـک هماننـد ارتباطـات تلفنـی یـا پیامـک، بین خود مشـتریان اسـت با این تفـاوت کـه در یـک طـرف به‌جـای مشـتری دوم، بانـک عامـل قـرار می‌گیـرد. در ایـن شـیوه خدمات موبایل‌بانـک، مشـتریان فقـط می‌تواننـد آخریـن وضعیـت صورت‌حسـاب شـان را دریافـت کننـد، درحالی‌کـه مشـتریان نیـاز بـه دیگـر خدمـات مالی و بانکـی ازجمله نقل‌وانتقـال وجـوه، پرداخت وجوه، معاملات سـهام، پرداخت قبوض و... دارند. در مسـیر رفع این مشـکل، با پیشـرفت فنـاوری و به‌کارگیری نظام‌هـای ارتباطـی جهـان بی‌سـیم چـون wap و نظـام ارتبـاط بی‌سـیم جهـان (جـاوا) در قالـب پشـتیبانی خدمات‌دهـی جهانـی بسـته رادیویـی و همچنیـن تولیـد تلفن‌های همـراه با قابلیـت اتصال بـه شـبکه جهانـی و سیسـتم‌های ارتباطی بی‌سـیم و اینترنـت، این امکان فراهم شـد کـه انواع مختلفی از خدمـات بانکـی و مالـی همچـون نقل‌وانتقال بین حسـاب‌ها، معامـلات و دادوسـتدهای بـازار سـهام، آگاهـی از موجودی حسـاب‌ها و همچنیـن پرداخت وجـه برای شـهروندان با اسـتفاده از تلفن‌های همراه عملی شـود.

کاهش هزینه‌های خدمات بانکی

در واقـع می‌تـوان گفـت کـه خدمـات بانکـداری موبایلـی همـان خدمـات معمـول بانکـی اسـت که از طریـق شـبکه موبایلـی ارائـه می‌شـود. عاملی که توجـه بانک‌هـا را به‌شـدت بـه این موضـوع معطوف کـرده اسـت؛ امـکان بی‌نظیـر خدمـات موبایلـی در کاهـش هزینه‌هـای ارائـه خدمـات بانکی اسـت.

برتـری بانکـداری موبایلـی بـر بانکـداری الکترونیکـی

بـا توجـه بـه عـدم دسترسـی بـه اینترنـت در شـرایط و موقعیت‌هـای گوناگـون و از سـویی دیگـر مجهـز بـودن اکثـر افراد بـه موبایل و گوشـی همراه، اسـتفاده از موبایـل توانسـت در مدت زمـان کوتاهی از اینترنـت پیشـی گرفتـه و بـا توجـه بـه اینکـه درحال‌حاضر بسـیاری از مشـتریان بانک با بانکداری اینترنتـی آشـنا نشـده‌اند، به‌علت سـادگی اسـتفاده

و در دسترس‌بودن موبایل، به استفاده از خدمات بانکداری موبایلی روی آورده‌اند. متخصصان بانکی کشور اذعان دارند که تا سال ۱۳۹۵ تعداد کاربران بانکداری موبایلی از کاربران شعبه‌ای، ATM و اینترنتی در ایران، پیشی خواهد گرفت، البته به شرط آنکه بانک‌ها با همین آهنگ رشد به سمت بانکداری موبایلی حرکت کنند. مهم‌ترین عوامل برتری بانکداری موبایلی به بانکداری اینترنتی هم مشتمل بر مواردی چون عدم محدودیت مکانی، ضریب نفوذ بالا، شخصی بودن این نوع بانکداری و همراه همیشگی بودن است.

موانع توسعه

برای ارتقای خدمات موجود بانکداری موبایلی در کشور و نیز پیاده‌سازی خدمات جدید، موانعی وجود دارد که موجب شده تاکنون بانکداری موبایلی در ایران به جایگاه واقعی خود، متناسب با جایگاه آن در کشورهای پیشرفته نرسد. بی‌تردید شناخت این مشکلات و کوشش برای رفع آنها می‌تواند آینده روشنی را برای خدمات بانکداری موبایلی نمایان کند. مهم‌ترین موانع را می‌توان در چهار بخش سازمانی، عملیاتی، مالی، تکنولوژیکی و قانونی طبقه‌بندی کرد. موانع یادشده به تفکیک این بخش‌ها چنین است.

موانع فنی؛ تامین امنیت شبکه، موضوعی است که به‌شدت وابسته به سطح فنی شبکه است و علاوه بر این، سرعت انتقال اطلاعات و محرمانه‌بودن اطلاعات شخصی نیز در ارتباط با سطح فناوری هستند و عدم تامین کافی امنیت و سرعت در شبکه، منجر به عدم تمایل کاربران به استفاده از این خدمات می‌شود. از سوی دیگر مدیریت شبکه نیز به‌علت در اختیار نداشتن دانش فنی کافی، فاقد کارایی لازم بوده و مانع توسعه شبکه خواهد شد.

موانع سازمانی؛ پیاده‌سازی شبکه بانکداری موبایلی نیازمند طراحی و پیاده‌سازی یک ساختار سازمانی جدید است. به این منظور لازم است که اصول عملیاتی و فرآیندهای اجرایی، سازماندهی و مسئولیت‌ها و وظایف ابعاد سازمان مشخص شود. نبود یک هدف اصلی و چارچوب سازمانی مشخص، سبب تداخل امور و ایجاد واکنش‌های منفی در بخش‌های داخلی و خارجی شبکه می‌شود. الگوبرداری صرف از مدل‌های مربوط به کشورهای دیگر نیز خود یک اشتباه مضاعف است که می‌تواند منجر به ناسازگاری کل شبکه بانکداری موبایلی با نظام اجتماعی شود.

موانع عملیاتی؛ مسئله تامین امنیت همواره یک دغدغه اصلی در فرآیند عملیاتی شدن خدمات بانکداری موبایلی، یک مانع اصلی برای اجرای این شبکه تلقی می‌شود. از سوی دیگر عواملی وجود دارند که خارج از حیطه اثرگذاری یک بانک قرار دارند، مانند ضعف پوشش شبکه تلفن‌های همراه که مانع از گسترش خدمات بانکداری موبایلی می‌شود. محدودیت‌های فیزیکی و فنی گوشی‌های تلفن‌همراه نیز یک عامل درونی برای عدم رشد سریع شبکه است. علاوه بر موارد یادشده، سطح پایین دانش فنی کارکنان نیز می‌تواند به‌صورت یک عامل محدودکننده به‌حساب آید.

موانع مالی؛ هرچند ارائه خدمات از طریق شبکه موبایلی هزینه تبادلات بانکی را به‌شدت کاهش می‌دهد، اما یک هزینه اولیه که شامل خرید تجهیزات، آموزش فنی و بازاریابی است، بر بانک تحمیل می‌شود. از سوی دیگر هزینه ارتباط تلفن همراه، طی دریافت خدمات بانکداری موبایلی به‌عنوان یک هزینه اضافی برای مشتری به‌وجود می‌آید که در تحلیل‌های هزینه- فایده، این موضوع به مثابه یک عامل محدودکننده عمل خواهد کرد. از سوی دیگر نظام‌های پرداخت موبایلی که وظیفه تبادلات مالی را برعهده دارند، پیچیدگی‌ها و نکات فنی خاص خود را دارند که اگر به‌خوبی مورد توجه قرار نگیرند یا سازماندهی نشوند، در عمل مانعی بزرگ در پیاده‌سازی بسترهای خدمات بانکداری و تجارت موبایلی ایجاد می‌کنند.

راهکارهای توسعه

موانع و مشکلات یادشده مهم‌ترین موانعی هستند که در برابر گسترش و ارتقای شبکه بانکداری موبایلی در کشور وجود دارند و برطرف‌کردن آنها پیش‌نیاز اصلی و اساسی برای پیاده‌سازی یک نظام کارآمد بانکداری موبایلی است. به این منظور، پیشنهادهایی به شرح زیر ارائه می‌شوند که می‌توانند در توسعه شبکه بانکداری موبایلی تاثیرگذار باشند.

ـ توسعه و ارتقای شبکه مخابراتی: پوشش گسترده و سرعت بالای انتقال اطلاعات دو عامل اساسی است که باید در شبکه مخابراتی کشور در نظر گرفته شود.

ـ جی‌پی‌آر اس: پیاده‌سازی سیستم GPRS در مورد شبکه دیتای کشور یک ضرورت اساسی برای توسعه بانکداری موبایلی است.

ـ پرداخت موبایلی ملی: به‌منظور مدیریت صحیح تجارت و بانکداری موبایلی، ضروری است یک نظام پرداخت موبایلی ملی طراحی شود که تمام پرداخت‌های موبایلی کشور از آن طریق هدایت و نظارت شود.

ـ اجرایی‌شدن قوانین: برای ایجاد بسترهای نظام‌مند و کارا باید قوانین مربوط به‌صورت دقیق و جامع وضع و هرچه سریع‌تر اجرایی شوند.

ـ اتصال به شبکه‌های بین‌المللی: پس از اتصال شبکه موبایلی به شبکه‌های بین‌المللی، امکان ارائه و دریافت خدمات بانکداری بین‌المللی در سطح بین‌المللی وجود خواهد داشت.

ـ آموزش: آموزش‌های فنی و کاربردی باید هم برای پرسنل شبکه‌های تجارت و بانکداری موبایلی و هم برای کاربران این خدمات در نظر گرفته شود.

ـ دانش فنی: روزآمدکردن دانش فنی شبکه‌های بانکداری موبایلی، چه از طریق واردات فناوری و چه با تکیه بر توان فنی داخلی، باید مورد توجه جدی قرار گیرد.

برای ارتقای خدمات موجود بانکداری موبایلی در کشور و نیز پیاده‌سازی خدمات جدید، موانعی وجود دارد که موجب شده تاکنون بانکداری موبایلی در ایران به جایگاه واقعی خود، متناسب با جایگاه آن در کشورهای پیشرفته نرسد. بی‌تردید شناخت این مشکلات و کوشش برای رفع آنها می‌تواند آینده روشنی را برای خدمات بانکداری موبایلی نمایان کند

ـ بازاریابی: تجزیه و تحلیل بازار و سنجش امکانات توسعه در بازار خدمات بانکداری موبایلی باید توسط سازمان‌های دولتی در سطح کلان و ارائه‌دهندگان این خدمات در سطح خرد انجام شود.

ـ استانداردهای ملی و جهانی: استانداردسازی خدمات و فعالیت‌های حوزه بانکداری الکترونیکی، چه در سطح ملی و چه در سطح بین‌المللی باید انجام شود.

ـ حمایت: باید به نگهداری، حمایت و ارتقای سیستم‌ها پس از راه‌اندازی توجه کافی شود.

یادآور می‌شود که اجرای این پیشنهادها تنها از طریق تعامل و همکاری سازمان‌ها و نهادهای دولتی از یک سو و شرکت‌ها و موسسات بخش خصوصی از سوی دیگر امکان‌پذیر است. شرکت‌ها و موسسات ارائه‌دهنده خدمات و به‌ویژه بانک‌ها به‌عنوان ارائه‌دهندگان بانکداری موبایلی نقشی اساسی در هماهنگ‌سازی فعالیت‌ها، استانداردسازی فرآیندها و تامین امنیت شبکه بانکداری موبایلی به عهده خواهند داشت.

اداره‌کل روابط‌عمومی