

آیا بانکداری به سمت بیومتریکی می رود؟

روش های تایید بیولوژیکی - تحقیق صدا، شناسایی چهره ای، اثر انگشت، اسکن شبکه چشم - نه تنها برای استفاده کاربران ساده است، بلکه از سایر روش های امن برای مطابقت بسیار سخت تر است. تایید بیومتریکی یکی از بزرگترین رویه ها در صنعت امنیت است. پس چه چیزی مانع صنعت بانکداری است؟

استفاده از چیزی که برای تایید می شناسید خوب است. چیزی که شما دارید بهتر است، اما چیزی که هستید بهترین است. کاربرد بیومتریکی در بخش مالی، امنیت تراکنش های آنلاین را با ارائه ترکیبی از این عوامل افزایش می دهد؛ برای مثال، استفاده از یک دستگاه موبایل (چیزی که دارید) در ترکیب با اثر انگشت (چیزی که هستید). این روش نیاز دوم مشتری را خطاب قرار می دهد که احراز هویت باید آسان و راحت باشد. علاقه مشتریان به تکنولوژی تایید بیومتریکی بسیار زیاد است. در حقیقت بینش کارمند داخلی تجاری پیش بینی می کند ۹۹ درصد تلفن های هوشمند تا سال ۲۰۲۱ بیومتریکی را پشتیبانی خواهند کرد. با افزایش پذیرش و تقاضای تکنولوژی بیومتریکی از سوی مشتریان، پیش از تاثیر روی بخش مالی و بانکداری، مسئله زمان مطرح است.

با توجه به تلفیق افزایش یافته این تکنولوژی در دستگاه های کاربر، احتمالاً مشتریان در آینده نه چندان دور آن را در کاربری های مالی تقاضا خواهند کرد. این عملکرد امن جدید بدون شک منافع قابل توجهی خواهد داشت که کمترین آن، یک ابزار جدید در مبارزه با فعالیت خبیثانه و کلاه بردارانه است. با این حال، یک ادغام نامعلوم از راه حل های بیومتریکی در تمام کاربری ها در نهایت ثابت می کند برای مشتریان مفید است، اما یک تعییر غلط ممکن است از بسیاری از جوانب رقابتی باشد که مشتریان در تعاملات خود به آن بها می دهند.

خواسته های رقابتی مشتریان

کدام خواسته های رقابتی کاربران در زمان اجرای بیومتریکی باید در فرآیندهای تراکنشی آنها توازن داشته باشد؟ از یک سو، کاربران آشکارا هنگام تراکنش های مالی خود انتظار بالاترین سطح محافظت در دسترس را دارند. البته خواسته هر فرد برای دفع فعالیت های کلاه بردارانه و خبیثانه در این صنعت مطابقت داده می شود. در آن واحد، مشتریان می خواهند این تایید در حدامکان ساده و راحت باشد که مشکل با ورود تکنولوژی بیومتریکی حل می شود.

در حالی که منافع امن تکنولوژی بیومتریکی قابل توجه است، این نیز صحیح است که کاربران به طور سنتی از عملکردهای امن دوری می کنند؛ عملکردهایی که راه آنان را برای تراکنش محدود کرده یا اطلاعات مالی آنان را به کار می گیرد. زمان اجرای فرآیندهای امن جدید، همیشه برترین حالت اجرا این است که مانع راه هایی شود که مشتریان بتوانند از اطلاعاتشان استفاده کنند یا آنها را به اشتراک بگذارند. در حقیقت، اجرای آن نه تنها تمرینات مدیریت ریسک را نادیده می گیرد، بلکه تاثیر قابل توجهی بر قبول مشتری دارد، به علاوه رضایت و وفاداری کلی او. قبول تنها یک شکل از تایید بیومتریکی می تواند اجرای آن را تهدید کند، به این دلیل که مستلزم رویکرد دقیق است. اجرای الزامات بیومتریکی برای تراکنش های داده محور می تواند توانایی مشتریان برای استفاده مجاز از اطلاعات شخصی آنها را از راه هایی که می خواهند تهدید کند، نظیر اشتراک گذاری اطلاعات با مشاور یا استفاده از آن با کاربری های مالی برای کمک به بهبود وضعیت مالی آنان.

پاسخ چیست؟

هنگامی که برای کاربری های مالی به بیومتریکی می رسیم، پاسخ نهایی با اجرا متوازن خواهد بود؛ موردی که از احراز هویت بیومتریکی در راه حل های با ریسک بالا استفاده می کند، اما اجازه اشتراک اطلاعات مالی را نمی دهد که در نهایت به نفع کاربر است. در این معنا، معرفی تایید بیومتریکی به عنوان بخشی از مکانیزم احراز هویت برای راه حل های با ریسک بالا نظیر اضافه کردن یک گیرنده جدید، تغییر اطلاعات شخصی یا جابجایی پول در حساب است. به کارگیری فعالیت هایی که تمام قواعد احراز هویت را بررسی می کند، به طور قطع یک جابجایی معقولانه است و به عنوان یک صنعت باید اجرای آن را در زیرساخت خود در نظر داشته باشیم. این امر به این دلیل است که در

موقعیت های با ریسک بالا، مکانیزم احراز هویت مفرد کافی نیست. در چنین شرایطی ادغام تکنولوژی بیومتریک برای مشتریان، دومین روش احراز هویتی را ایجاد می کند که نه تنها بسیار ایمن است بلکه تجربه کاربری یکپارچه ای را فراهم می کند. با این همه تمام تراکنش ها در طبقه ریسک بالا قرار می گیرند و موسسات مالی در جست وجوی ادغام تکنولوژی بیومتریکی هستند که باید بین آنها تمایز ایجاد کنند. موسسات مالی که می خواهند به بهترین نحو خواسته های مشتریان را فراهم کنند باید در جست وجوی تکمیل تکنولوژی های احراز هویت بیومتریک قوی برای تراکنش های با ریسک بالا و همراه یک مکانیزم احراز هویت قابل خواندن در موقعیت هایی با ریسک پایین باشند. این رویکرد به کاربران امنیت دقیقی را که نیاز دارند می دهد، در حالی که قادر به کاربرد اطلاعات مالی با روش هایی هستند که انتظار دارند.

این امر با دو روش قابل دستیابی است. برای نمونه، در چنین موقعیت هایی بانک ها می توانند برای یک نام کاربری ثانویه و غیرتراکنشی تماس بگیرند و یا احراز هویت مبتنی بر نشانه معرفی کنند. همچنین می توانند یک چارچوب ایمن چند لایه ای را اجرا کنند به طوری که نام کاربری و رمز اجازه دستیابی به تراکنش های «قابل خواندن» را بدهد و احراز هویت بیومتریک مستلزم فعالیت های ریسک بالاست.

همزمان با این نوآوری موفقیت آمیز، مشتریان انتظار خواهند داشت تکنولوژی بیومتریک به عنوان بخشی از تجربه بانکداری آنان در آینده نزدیک باشد، هرچند موافق استفاده از تجربه شان نخواهند بود. در این معنا برای تمام موسسات مالی قطعی شده است که باید روش هایی که می توانند بهترین موارد بیومتریک را با کاربری هایی با حضور کاربر ترکیب کنند، امتحان کنند؛ روش هایی که منحصر کاربری های گسترده را درگیر نمی کند. در حالی که این تکنولوژی تعهدی عظیم برای کل این صنعت ایجاد می کند، موسسات رویکرد «یکی برای تمام اندازه ها» را برای اجرای آن به کار می برند که می تواند واکنش شدید مشتری را در پی داشته باشد.

ترجمه : نگار احمدی – مدیریت شمال غرب – منبع: Financialbrand