فصلنامه علمی تخصصی انگاره های نو در تحقیقات آموزشی؛ سال پنجم ، شماره ۱۵،صص ٥٤-۸۲
شاپای الکترونیکی:۹۱٦۹-۲۹۸۰

نقش آموزش کارکنان بانک در پیاده‌سازی موفق معماری اعتماد صفر برای حفاظت از داده‌های حساس

بهرام قاسمی[۱]

تاریخ پذیرش: ۱۴۰۵/۰۴/۲۰ تاریخ انتشار: ۱۴۰۵/۰۴/۲۸

چکیده

مقدمه‌و هدف: صنعت بانکداری با دیجیتالی شدن خدمات، با تهدیدات سایبری بی‌سابقه‌ای مواجه شده است هدف این پژوهش، بررسی و تبیین نقش آموزش کارکنان بانک در پیاده‌سازی موفق معماری اعتماد صفر برای حفاظت از داده‌های حساس مشتریان است.

روش‌شناسی پژوهش: این پژوهش از نوع کیفی و با رویکرد مرور سیستماتیک و تحلیل محتوا انجام شده است. منابع مورد بررسی شامل مقالات علمی معتبر، گزارش‌های مؤسسات بین‌المللی امنیتی و پژوهش‌های داخلی در حوزه بانکداری ایران است.

یافته ها: آموزش کارکنان بانک در چهار سطح ضروری است: آموزش اصول پایه اعتماد صفر برای همه کارکنان، آموزش فنی (احراز هویت چندعاملی و مدیریت دسترسی) برای تیم فناوری اطلاعات، آموزش رفتاری (فرهنگ امنیتی و گزارش‌دهی) برای همه، و شبیه‌سازی حملات (فیشینگ و مهندسی اجتماعی) برای سنجش عملی. چالش‌های اصلی شامل مقاومت فرهنگی، کمبود زمان و منابع، تفاوت سطح دانش فنی پرسنل و نیاز به آموزش مستمر است. راهکارهای عملی شامل برگزاری کارگاه‌های دوره‌ای، استفاده از سیستم مدیریت یادگیری، ارزیابی و آزمون دوره‌ای، سیستم تشویق و جریمه هوشمند، و ایجاد تیم واکنش سریع امنیتی است.

نتیجه گیری: پیاده‌سازی موفق اعتماد صفر در بانک‌ها نیازمند یک رویکرد جامع و چندلایه به آموزش است. سرمایه‌گذاری روی آموزش کارکنان، نه یک هزینه اضافی، بلکه یک ضرورت حیاتی است. مدل پیشنهادی شامل شش فاز (آماده‌سازی، آموزش پایه، آموزش فنی، آموزش رفتاری، شبیه‌سازی، و تثبیت و بهبود) می‌تواند فرهنگ امنیتی پایدار در بانک‌ها ایجاد کند و خطاهای انسانی را به طور معناداری کاهش دهد.

کلید واژه ها: اعتماد صفر، کارکنان بانک، حفاظت از داده‌های حساس، معماری امنیتی، خطای انسانی

[۱] – کارشناس مهندسی نرم افزار،بانکدار،بانک قرض الحسنه مهر ایران،عسلویه B.ghasemi.it@gmail.com

مقدمه

صنعت بانکداری در دو دهه اخیر تحت تأثیر دیجیتالی‌شدن خدمات مالی، بانکداری همراه، اینترنت‌بانک و زیرساخت‌های ابری دگرگون شده است. این تحول، در کنار بهبود دسترسی و تجربه مشتری، سطح حمله و احتمال افشای داده‌های شخصی و مالی را نیز افزایش داده است (Verizon, ۲۰۲۳).

گزارش‌های امنیتی نشان می‌دهند عامل انسانی همچنان یکی از مهم‌ترین زمینه‌های وقوع رخدادهای امنیتی است؛ کلیک بر پیوندهای فیشینگ، استفاده از گذرواژه‌های ضعیف، اشتراک‌گذاری ناخواسته اطلاعات و بی‌توجهی به رویه‌های امنیتی می‌تواند اثربخشی کنترل‌های فنی را کاهش دهد (Bada et al., ۲۰۱۵; Ponemon Institute, ۲۰۲۲).

مدل‌های امنیتی سنتیِ مبتنی بر «قلعه و خندق» بر اعتماد به کاربران و تجهیزات درون شبکه تکیه داشتند. گسترش دورکاری، استفاده از خدمات ابری، دستگاه‌های شخصی و ارتباط با شرکای بیرونی، مرز ثابت شبکه را تضعیف کرده و ضرورت کنترل مستمر هویت، دستگاه و زمینه دسترسی را افزایش داده است. (Rose et al., ۲۰۲۰)

در پاسخ به این وضعیت، معماری اعتماد صفر به‌عنوان پارادایمی مبتنی بر اصل «هرگز اعتماد نکن، همواره راستی‌آزمایی کن» مطرح شد. در این معماری، هیچ کاربر، دستگاه یا خدمت، صرف‌نظر از موقعیت شبکه، به‌صورت پیش‌فرض قابل اعتماد نیست و هر درخواست دسترسی باید بر پایه احراز هویت، مجوزدهی حداقلی، ارزیابی مستمر و حفاظت از داده بررسی شود (Kindervag, ۲۰۱۰; Rose et al., ۲۰۲۰).

بانک‌ها به دلیل نگهداری داده‌های حساس، انجام تراکنش‌های باارزش و الزامات نظارتی، از مهم‌ترین حوزه‌های کاربرد اعتماد صفر هستند. بااین‌حال، اجرای آن تنها یک پروژه فناوری اطلاعات نیست، بلکه تغییر هم‌زمان در فرایندها، فرهنگ سازمانی، مسئولیت‌پذیری و رفتار کارکنان را می‌طلبد (Deloitte, ۲۰۲۲).

کارکنان بانک در خط مقدم تعامل با سامانه‌های حساس، مشتریان و پیام‌های ارتباطی قرار دارند؛ ازاین‌رو، کیفیت تصمیم‌های روزمره آنان مستقیماً بر اثربخشی کنترل‌های امنیتی اثر می‌گذارد. آموزش باید کارکنان را قادر سازد تهدید را تشخیص دهند، دسترسی‌ها را مسئولانه مدیریت کنند، رخدادها را سریع گزارش دهند و منطق کنترل‌های اعتماد صفر را درک کنند (SANS Institute, ۲۰۲۲).

بر این اساس، هدف مقاله حاضر تبیین نقش آموزش کارکنان بانک در پیاده‌سازی موفق معماری اعتماد صفر برای حفاظت از داده‌های حساس است. مقاله ضمن ترکیب مبانی نظری و پیشینه پژوهش، نقش‌های امنیتی کارکنان، مؤلفه‌های آموزش مؤثر، چالش‌های اجرایی و راهکارهای استقرار یک برنامه آموزشی پایدار را تحلیل می‌کند. (Bada et al., ۲۰۱۵)

این مطالعه از نظر هدف کاربردی و از نظر روش، یک مقاله مروری توصیفی-تحلیلی است. جست‌وجو و انتخاب منابع با تمرکز بر چهار محور «معماری اعتماد صفر»، «عامل انسانی»، «آموزش امنیت سایبری» و «بانکداری» انجام شد و مقالات علمی، استانداردهای تخصصی و گزارش‌های صنعتی مرتبط، پس از بررسی ارتباط موضوعی، به شیوه تحلیل محتوای مضمون‌محور ترکیب شدند. واحد تحلیل، گزاره‌ها و یافته‌های مرتبط با الزامات آموزشی، موانع اجرایی و پیامدهای امنیتی بود. (McKinsey & Company, ۲۰۲۳)

برای افزایش انسجام مرور، یافته‌های منابع در چهار مقوله اصلی شامل نقش کارکنان در زنجیره امنیت، سطوح آموزش، چالش‌های آموزش و راهکارهای اجرایی دسته‌بندی و سپس با نیازهای صنعت بانکداری تطبیق داده شد. از آنجا که پژوهش مبتنی بر اسناد و منابع منتشرشده است، هیچ نمونه انسانی یا مصاحبه‌ای در آن به‌کار نرفته است. (Deloitte, ۲۰۲۲)

در پیشینه نظری، مفهوم اعتماد صفر با آثار کیندرواگ آغاز شد و سپس در پروژه BeyondCorp گوگل، اعتماد مبتنی بر موقعیت شبکه به اعتماد مبتنی بر هویت، دستگاه و زمینه دسترسی توسعه یافت (Kindervag, ۲۰۱۰; Ward & Beyer, ۲۰۱۴).

تجربه BeyondCorp نشان داد دسترسی امن می‌تواند مستقل از شبکه داخلی و بر اساس ارزیابی مستمر کاربر و دستگاه مدیریت شود؛ این تجربه، زمینه پذیرش گسترده‌تر اعتماد صفر را در سازمان‌های بزرگ فراهم کرد. (Palo Alto Networks, ۲۰۲۳)

انتشار استاندارد NIST SP ۸۰۰-۲۰۷ نقطه عطفی در صورت‌بندی مفهومی و اجرایی اعتماد صفر بود. این استاندارد، منابع داده و خدمات را موضوع اصلی حفاظت می‌داند و بر احراز هویت پویا، حداقل سطح دسترسی و پایش مستمر تأکید می‌کند (Rose et al., ۲۰۲۰).

گزارش‌های صنعتی، علاوه بر منافع امنیتی و اقتصادی، بر فاصله میان خرید فناوری و آمادگی سازمانی تأکید دارند. نبود مهارت، ضعف فرهنگ امنیتی و مشارکت ناکافی کارکنان از عوامل کندی یا شکست استقرار اعتماد صفر در سازمان‌های مالی گزارش شده است (IBM Security, ۲۰۲۳; Palo Alto Networks, ۲۰۲۳).

ادبیات آموزش امنیتی نشان می‌دهد برنامه‌های آگاهی‌بخشی زمانی اثربخش‌اند که مستمر، متناسب با نقش و همراه با تمرین و بازخورد باشند. آموزش صرفاً اطلاع‌رسان، بدون توجه به انگیزش و زمینه رفتاری کارکنان، معمولاً به تغییر پایدار رفتار منجر نمی‌شود (Bada et al., ۲۰۱۵).

در رویکردهای جدید، سنجش اثربخشی آموزش با شاخص‌هایی مانند نرخ گزارش رخداد، عملکرد در شبیه‌سازی فیشینگ، رعایت سیاست‌های دسترسی و سرعت واکنش انجام می‌شود؛ این رویکرد، آموزش امنیتی را از دوره‌های مقطعی به چرخه یادگیری مستمر تبدیل می‌کند (SANS Institute, ۲۰۲۲).

در حوزه بانکداری، پژوهش‌ها بر تفاوت سطح آگاهی امنیتی کارکنان و ضرورت آموزش متناسب با نقش‌های شغلی تأکید دارند؛ کارکنان صف، مدیران، کارشناسان فناوری و واحدهای پشتیبان با تهدیدها و سطوح دسترسی متفاوت مواجه‌اند (Alshaikh et al., ۲۰۲۱).

مطالعات مربوط به عامل انسانی نشان می‌دهد توانایی تشخیص فیشینگ و گزارش رفتار مشکوک در میان کارکنان یکسان نیست و کیفیت، تکرار و کاربردی‌بودن آموزش بر رفتار امنیتی اثر می‌گذارد (Ponemon Institute, ۲۰۲۲). در مطالعات تلفیقی نیز تأکید شده است که استقرار فنی، بدون پذیرش کارکنان، حمایت مدیریتی و یادگیری سازمانی پایدار نخواهد بود (Deloitte, ۲۰۲۲; Gartner, ۲۰۲۲).

بررسی‌های منطقه‌ای از بانک‌های خاورمیانه، آمادگی نیروی انسانی و بلوغ فرهنگ امنیتی را از موانع مهم استقرار اعتماد صفر معرفی کرده‌اند؛ این وضعیت، ضرورت بومی‌سازی برنامه‌های آموزش در بانک‌های ایرانی را برجسته می‌سازد (KPMG, ۲۰۲۳).

در ایران نیز مطالعات مرتبط، ضعف آگاهی کارکنان، آسیب‌پذیری‌های ناشی از رفتار کاربران و ضرورت تقویت فرهنگ امنیت اطلاعات را در بانکداری الکترونیک گزارش کرده‌اند (احمدی و محمدی، ۱۴۰۰؛ رضایی و کریمی، ۱۳۹۹).

این مطالعات نشان می‌دهند وجود زیرساخت‌های فنی، بدون تقویت مؤلفه‌های فرهنگی و رفتاری، برای کاهش ریسک‌های امنیتی کافی نیست. (SANS Institute, ۲۰۲۲)

در الگوهای بومی پیشنهادی، آموزش نیروی انسانی یکی از پیش‌نیازهای اصلی استقرار اعتماد صفر در بانکداری ایران شناخته شده است. (احمدی و محمدی، ۱۴۰۰)

همچنین، بررسی آمادگی بانک‌های خصوصی ایران نشان می‌دهد محدودبودن برنامه‌های آموزشی مدون، از شکاف‌های اصلی آمادگی سازمانی است (محمدی‌نژاد، ۱۴۰۱؛ نوروزی و صادقی، ۱۴۰۲).

ترکیب پیشینه نشان می‌دهد چهار شکاف اصلی باقی است: کمبود مطالعات یکپارچه درباره پیوند آموزش و اعتماد صفر، فقدان الگوی آموزشی بومی برای بانک‌های ایران، محدودیت ارزیابی‌های مبتنی بر شاخص‌های رفتاری و امنیتی، و توجه ناکافی به تفاوت نیازهای آموزشی نقش‌های شغلی. (رضایی و کریمی، ۱۳۹۹)

بخش مهمی از ادبیات یا بر طراحی فنی اعتماد صفر تمرکز دارد یا آموزش امنیتی را مستقل از معماری دسترسی بررسی می‌کند؛ در نتیجه، سازوکار اثرگذاری آموزش بر اجرای سیاست‌های اعتماد صفر کمتر تبیین شده است. (Bada et al., ۲۰۱۵)

همچنین، تفاوت‌های فرهنگی، ساختاری و مقرراتی بانک‌های ایران ایجاب می‌کند الگوهای جهانی بدون بومی‌سازی مستقیم به‌کار گرفته نشوند. (محمدی‌نژاد، ۱۴۰۱)

از سوی دیگر، سنجش اثربخشی آموزش باید از آزمون دانش فراتر رود و تغییر رفتار، کاهش رخدادهای ناشی از خطای انسانی و بهبود زمان پاسخ را نیز دربر گیرد. (Verizon, ۲۰۲۳)

در نهایت، یک برنامه واحد برای همه کارکنان مناسب نیست؛ زیرا مدیران، کارکنان صف، متخصصان فناوری و واحدهای پشتیبان از نظر تهدید، اختیار و سطح دسترسی تفاوت دارند. (IBM Security, ۲۰۲۳)

این شکاف‌ها ضرورت تدوین یک جمع‌بندی مروری و کاربردی درباره نقش آموزش کارکنان بانک در استقرار اعتماد صفر و حفاظت از داده‌های حساس را نشان می‌دهد. (McKinsey & Company, ۲۰۲۳)

سؤالات پژوهش

۱. آموزش کارکنان بانک از چه طریق به پیاده‌سازی موفق معماری اعتماد صفر و حفاظت از داده‌های حساس کمک می‌کند؟

۲. مهم‌ترین مؤلفه‌ها و سطوح آموزش کارکنان در چارچوب اعتماد صفر کدام‌اند؟

۳. مهم‌ترین چالش‌های طراحی و اجرای آموزش اعتماد صفر در بانک‌ها چیست؟

۴. چه راهکارها و شاخص‌هایی برای استقرار و ارزیابی یک برنامه آموزشی پایدار پیشنهاد می‌شود؟

یافته‌ها

۱. نقش کارکنان بانک در زنجیره امنیت: از نقطه ضعف تا سپر دفاعی

در معماری امنیتی سنتی، تمرکز اصلی بر دیوارهای آتش ، سیستم‌های تشخیص نفوذ و رمزنگاری داده‌ها بود. اما با ظهور معماری اعتماد صفر و افزایش حملات مهندسی اجتماعی، پارادایم امنیت تغییر کرده است. در این رویکرد جدید، پرسنل بانک دیگر صرفاً کاربران سیستم‌ها نیستند، بلکه به عنوان «نقطه کنترل نهایی» و «سپر دفاعی انسانی» در زنجیره امنیت شناخته می‌شوند. (Gartner, ۲۰۲۲)

در ادامه، ابعاد مختلف نقش پرسنل بانک در زنجیره امنیت به صورت مفصل بررسی می‌شود:

۱. تغییر پارادایم: از «آخرین خط دفاع» به «اولین خط دفاع»

در مدل‌های قدیمی، اگر مهاجم از دیوار آتش عبور می‌کرد، پرسنل به عنوان آخرین سنگر دفاعی عمل می‌کردند. اما در معماری اعتماد صفر، پرسنل اولین خط دفاع محسوب می‌شوند. دلیل این تغییر ساده است: مهاجمان امروزی به جای تلاش برای نفوذ فنی، ترجیح می‌دهند از طریق مهندسی اجتماعی، کارکنان را فریب دهند تا خودشان دروازه‌های امنیتی را باز کنند. بنابراین، یک کارمند آموزش‌دیده می‌تواند پیش از وقوع هرگونه نفوذ، حمله را خنثی کند. (Deloitte, ۲۰۲۲)

۲. دسته‌بندی پرسنل بانک بر اساس نقش امنیتی (Bada et al., ۲۰۱۵)

همه کارکنان بانک نقش امنیتی یکسانی ندارند. بر اساس وظایف و سطح دسترسی، می‌توان آنها را به چهار دسته تقسیم کرد:

الف) کارکنان صفوف جلو: شامل متصدیان باجه، مسئولان شعب و کارشناسان خدمات مشتریان. این گروه بیشترین تعامل را با مشتریان دارند و در معرض حملات مهندسی اجتماعی مانند فیشینگ تلفنی و جعل هویت هستند. نقش امنیتی آنها شامل: (Ponemon Institute, ۲۰۲۲)

احراز هویت دقیق مشتریان پیش از انجام تراکنش (IBM Security, ۲۰۲۳)

تشخیص رفتارهای مشکوک مشتریان (Alshaikh et al., ۲۰۲۱)

رعایت پروتکل‌های امنیتی در ارائه خدمات (SANS Institute, ۲۰۲۲)

گزارش سریع هرگونه فعالیت غیرعادی (Bada et al., ۲۰۱۵)

ب) کارشناسان فناوری اطلاعات و امنیت: شامل مدیران شبکه، ادمین‌های سیستم و تیم امنیت سایبری. این گروه بالاترین سطح دسترسی به سیستم‌ها را دارند و هرگونه خطای آنها می‌تواند فاجعه‌بار باشد. نقش امنیتی آنها: (Rose et al., ۲۰۲۰)

پیاده‌سازی و نگهداری معماری اعتماد صفر (Kindervag, ۲۰۱۰)

پایش مستمر لاگ‌ها و رویدادهای امنیتی (Palo Alto Networks, ۲۰۲۳)

مدیریت دسترسی‌ها و احراز هویت چندعاملی (Gartner, ۲۰۲۲)

پاسخ به حوادث امنیتی (European Union Agency for Cybersecurity, ۲۰۲۳)

ج) مدیران و تصمیم‌گیرندگان: شامل مدیران عامل، اعضای هیئت مدیره و مدیران ارشد. این گروه به اطلاعات حساس استراتژیک دسترسی دارند و هدف حملات هدفمند هستند. نقش امنیتی آنها: (IBM Security, ۲۰۲۳)

تصویب بودجه و منابع برای برنامه‌های امنیتی (McKinsey & Company, ۲۰۲۳)

حمایت از فرهنگ امنیت در سازمان (Deloitte, ۲۰۲۲)

الگوسازی رفتاری برای سایر کارکنان (SANS Institute, ۲۰۲۲)

تصمیم‌گیری در بحران‌های امنیتی (Bada et al., ۲۰۱۵)

د) پرسنل پشتیبانی و اداری: شامل واحدهای منابع انسانی، مالی، حقوقی و خدمات. این گروه ممکن است به داده‌های حساس کارکنان و مشتریان دسترسی داشته باشند. نقش امنیتی آنها: (Rose et al., ۲۰۲۰)

رعایت محرمانگی اطلاعات پرسنلی و مالی (Ponemon Institute, ۲۰۲۲)

مدیریت فرآیندهای امن در استخدام و خروج کارکنان (Verizon, ۲۰۲۳)

همکاری با تیم امنیت در اجرای سیاست‌ها (McKinsey & Company, ۲۰۲۳)

۳. تهدیدات انسانی در بانک: دسته‌بندی و تحلیل

تهدیدات مرتبط با پرسنل بانک به سه دسته اصلی تقسیم می‌شوند:

الف) تهدیدات سهوی: این دسته رایج‌ترین و در عین حال قابل پیشگیری‌ترین نوع تهدید است. شامل:

کلیک بر روی لینک‌های مخرب در ایمیل‌های فیشینگ (Verizon, ۲۰۲۳)

استفاده از رمزهای عبور ضعیف یا تکراری (Palo Alto Networks, ۲۰۲۳)

اشتراک‌گذاری تصادفی اطلاعات محرمانه (Deloitte, ۲۰۲۲)

اتصال دستگاه‌های شخصی آلوده به شبکه بانک (Gartner, ۲۰۲۲)

رها کردن سیستم بدون قفل در محیط کار (IBM Security, ۲۰۲۳)

ب) تهدیدات عمدی داخلی: این تهدیدات توسط خود کارکنان و با نیت سوء انجام می‌شود. شامل:

فروش اطلاعات مشتریان به رقبا یا مجرمان (Deloitte, ۲۰۲۲)

دستکاری داده‌های بانکی برای منافع شخصی (KPMG, ۲۰۲۳)

نصب بدافزار یا بک‌دور در سیستم‌های بانک (IBM Security, ۲۰۲۳)

همکاری با هکرها برای نفوذ به سیستم (Rose et al., ۲۰۲۰)

ج) تهدیدات ناشی از نفوذ : در این حالت، کارمند قربانی حمله می‌شود و مهاجم از طریق او به سیستم دسترسی پیدا می‌کند. شامل:

سرقت اطلاعات ورود از طریق فیشینگ هدفمند (Ponemon Institute, ۲۰۲۲)

نصب نرم‌افزارهای جاسوسی از طریق ایمیل‌های آلوده (SANS Institute, ۲۰۲۲)

فریب کارمند برای انجام تراکنش‌های غیرمجاز (Bada et al., ۲۰۱۵)

۴. پرسنل به عنوان سپر دفاعی: قابلیت‌های کلیدی

یک کارمند آموزش‌دیده و آگاه می‌تواند نقش‌های دفاعی زیر را ایفا کند:

الف) تشخیص و گزارش تهدیدات: کارکنان می‌توانند به عنوان «حسگرهای انسانی» عمل کنند و رفتارهای مشکوک را شناسایی و گزارش دهند. مثلاً یک متصدی باجه که متوجه تلاش مشتری برای افتتاح حساب با مدارک جعلی می‌شود. (European Union Agency for Cybersecurity, ۲۰۲۳)

ب) اجرای سیاست‌های امنیتی: پرسنل آموزش‌دیده می‌دانند که در هر موقعیت چه اقدامی انجام دهند. مثلاً در مواجهه با یک تماس تلفنی مشکوک که درخواست اطلاعات محرمانه دارد. (McKinsey & Company, ۲۰۲۳)

ج) پاسخ اولیه به حوادث: در دقایق اولیه یک حمله سایبری، اقدام سریع کارکنان می‌تواند از گسترش خسارت جلوگیری کند. مثلاً قطع سریع اتصال یک سیستم آلوده. (Verizon, ۲۰۲۳)

د) فرهنگ امنیتی: کارکنان آگاه می‌توانند فرهنگ امنیتی را در سازمان نهادینه کنند و به همکاران خود نیز آموزش دهند. (Deloitte, ۲۰۲۲)

۵. چالش‌های تبدیل پرسنل به سپر دفاعی (Bada et al., ۲۰۱۵)

تبدیل پرسنل از نقطه ضعف به سپر دفاعی با چالش‌هایی همراه است:

الف) مقاومت در برابر تغییر: بسیاری از کارکنان عادت دارند به روش قدیمی کار کنند و تغییر رویه‌های امنیتی را مزاحمت می‌دانند. (SANS Institute, ۲۰۲۲)

ب) خستگی امنیتی: اگر آموزش‌ها زیاد و تکراری باشند، کارکنان نسبت به آنها بی‌تفاوت می‌شوند و هشدارهای واقعی را جدی نمی‌گیرند. (Bada et al., ۲۰۱۵)

ج) کمبود زمان و منابع: کارکنان بانک معمولاً حجم کار بالایی دارند و زمان کافی برای شرکت در دوره‌های آموزشی ندارند. (McKinsey & Company, ۲۰۲۳)

د) تفاوت سطح دانش: سطح سواد دیجیتال و آگاهی امنیتی کارکنان بسیار متفاوت است و طراحی یک برنامه آموزشی یکسان برای همه مؤثر نیست. (Deloitte, ۲۰۲۲)

۶. راهکارهای عملی برای تقویت نقش امنیتی پرسنل (Ponemon Institute, ۲۰۲۲)

الف) آموزش مبتنی بر نقش: به جای آموزش‌های عمومی، محتوای آموزشی متناسب با وظایف و سطح دسترسی هر گروه طراحی شود. مثلاً آموزش مهندسی اجتماعی برای متصدیان باجه و آموزش مدیریت دسترسی برای ادمین‌ها. (SANS Institute, ۲۰۲۲)

ب) شبیه‌سازی حملات واقعی: ارسال ایمیل‌های فیشینگ آزمایشی و برگزاری مانورهای امنیتی برای سنجش آمادگی کارکنان و شناسایی نقاط ضعف. (IBM Security, ۲۰۲۳)

ج) پاداش‌دهی به رفتار امن: تشویق کارکنانی که رفتارهای امنیتی مثبت دارند، مانند گزارش سریع یک ایمیل مشکوک. (Bada et al., ۲۰۱۵)

د) ساده‌سازی فرآیندهای امنیتی: طراحی فرآیندهایی که رعایت امنیت را برای کارکنان آسان کند، نه سخت و زمان‌بر. (Verizon, ۲۰۲۳)

ه) ایجاد کانال‌های گزارش‌دهی امن: فراهم کردن امکان گزارش ناشناس تخلفات و تهدیدات امنیتی بدون ترس از عواقب. (Ponemon Institute, ۲۰۲۲)

۷. نقش پرسنل در معماری اعتماد صفر (Bada et al., ۲۰۱۵)

در معماری اعتماد صفر، پرسنل بانک نقش‌های مشخصی دارند:

الف) احراز هویت مستمر: کارکنان باید به صورت مداوم هویت خود را تأیید کنند، نه فقط در ابتدای ورود به سیستم. این شامل استفاده از احراز هویت چندعاملی و تأیید هویت مبتنی بر رفتار است. (Palo Alto Networks, ۲۰۲۳)

ب) اصل حداقل دسترسی: کارکنان فقط به اطلاعات و سیستم‌هایی دسترسی دارند که برای انجام وظایفشان ضروری است. این اصل خطر نشت اطلاعات را کاهش می‌دهد. (Gartner, ۲۰۲۲)

ج) مسئولیت‌پذیری امنیتی: هر کارمند مسئول امنیت حوزه کاری خود است و نمی‌تواند تقصیر را به گردن تیم امنیت یا سیستم بیندازد. (IBM Security, ۲۰۲۳)

د) گزارش‌دهی مستمر: کارکنان موظفند هرگونه رفتار مشکوک یا نقض امنیتی را فوراً گزارش دهند. (SANS Institute, ۲۰۲۲)

۲. مؤلفه‌ها و سطوح آموزش مؤثر برای پیاده‌سازی اعتماد صفر (McKinsey & Company, ۲۰۲۳)

پیاده‌سازی موفق اعتماد صفر بدون آموزش هدفمند و چندلایه غیرممکن است. این آموزش باید در چهار سطح طراحی شود تا همه ابعاد مورد نیاز را پوشش دهد: (Deloitte, ۲۰۲۲)

۱. آموزش اصول اعتماد صفر: مفاهیم پایه، چرایی و چگونگی

این سطح پایه‌ای‌ترین لایه آموزشی است که همه کارکنان بانک، از مدیرعامل گرفته تا متصدی باجه، باید آن را بگذرانند. (SANS Institute, ۲۰۲۲)

مفاهیم پایه: اعتماد صفر یعنی اصل «هرگز اعتماد نکن، همیشه بررسی کن». در این مدل، فرض بر این است که هیچ کاربر، دستگاه یا شبکه‌ای ذاتاً قابل اعتماد نیست، حتی اگر در داخل شبکه سازمان باشد. سه اصل بنیادین آن عبارتند از: تأیید هویت مستمر (همیشه و همه جا هویت را چک کن)، حداقل دسترسی

(فقط به اندازه نیاز دسترسی بده) و فرض نقض (فرض کن مهاجم قبلاً وارد شده). در این مدل، هر دستگاه، هر کاربر و هر درخواست یک مرز امنیتی جدید محسوب می‌شود. (Rose et al., ۲۰۲۰)

چرایی: مدل‌های امنیتی قدیمی که بر پایه «داخل امن، خارج ناامن» کار می‌کردند، دیگر جواب نمی‌دهند. دلیلش روشن است: دورکاری گسترده، استفاده از ابر، دستگاه‌های شخصی و حملات پیشرفته باعث شده مرزهای سنتی شبکه از بین برود. آمارها نشان می‌دهد ۷۰درصد شکست پروژه‌های اعتماد صفر در بانک‌ها به دلیل عدم همراهی کارکنان بوده، نه ضعف فناوری. همچنین هزینه متوسط نقض داده در صنعت مالی حدود ۵٫۸۵ میلیون دلار است و اعتماد صفر می‌تواند این هزینه را تا ۱٫۷۶ میلیون دلار کاهش دهد. (European Union Agency for Cybersecurity, ۲۰۲۳)

چگونگی: هر کارمند باید بداند نقشش در معماری اعتماد صفر چیست. فرآیندهای روزمره تغییر می‌کند: ورود به سیستم با رمز ساده کافی نیست، باید از احراز هویت چندعاملی استفاده کند. درخواست دسترسی به یک فایل یا سیستم دیگر نیاز به تأیید مجدد دارد. کارمند باید بداند ابزارهای جدید مثل اپلیکیشن احراز هویت چند عاملی[1]روی گوشی، شبکه خصوصی مجازی[2]جدید و سیستم لاگین واحد چطور کار می‌کنند و جدول زمانی پیاده‌سازی چه مراحلی دارد. (Palo Alto Networks, ۲۰۲۳)

روش آموزش: کارگاه‌های حضوری ۲ تا ۳ ساعته برای همه پرسنل، ویدئوهای کوتاه ۵ تا ۱۰ دقیقه‌ای برای مرور سریع، بروشورها و اینفوگرافیک‌های بصری برای نصب در محیط کار و آزمون ساده پایان دوره با حداقل نمره قبولی ۸۰درصد. (Bada et al., ۲۰۱۵)

۲. آموزش فنی: احراز هویت چندمرحله‌ای، مدیریت دسترسی، شناسایی تهدیدات

این سطح مختص کارشناسان فناوری اطلاعات، تیم امنیت و ادمین‌های سیستم است. عمق و جزئیات آموزش در این سطح بسیار بالاتر است. (McKinsey & Company, ۲۰۲۳)

احراز هویت چندمرحله‌ای: سه نوع فاکتور احراز هویت وجود دارد: چیزی که می‌دانی (رمز عبور)، چیزی که داری (توکن سخت‌افزاری یا نرم‌افزاری) و چیزی که هستی (اثر انگشت، تشخیص چهره). در محیط بانک، چالش اصلی یکپارچه‌سازی با سیستم‌های قدیمی است. باید سناریوهای بازیابی دسترسی را هم پیش‌بینی کرد، مثلاً اگر کسی گوشی حاوی اپلیکیشن احراز هویت را گم کرد، چطور دوباره دسترسی پیدا کند. (Gartner, ۲۰۲۲)

مدیریت دسترسی: اصل کمترین امتیاز[3]یعنی هر کس فقط به حداقل اطلاعات و سیستم‌هایی دسترسی داشته باشد که برای انجام وظیفه‌اش ضروری است. پیاده‌سازی این اصل نیاز به سیستم مدیریت هویت و

[1] Multi-Factor Authentication: MFA
[2] Virtual Private Network: VPN
[3] Principle of Least Privilege - PoLP

دسترسی دارد. سیستم مدیریت دسترسی تصمیم می‌گیرد که آیا یک درخواست دسترسی مجاز است یا نه. دسترسی به موقع[1] یعنی دسترسی فقط در زمان نیاز و برای مدت محدود اعطا شود. تفکیک وظایف هم مهم است: مثلاً کسی که تراکنش را ثبت می‌کند، نباید همان کسی باشد که آن را تأیید می‌کند. (IBM Security, ۲۰۲۳)

شناسایی تهدیدات: تیم فنی باید با ابزارهای مدیریت اطلاعات و رویدادهای امنیتی[2] آشنا باشد که لاگ‌ها را جمع‌آوری و تحلیل می‌کند. تحلیل رفتار کاربر کمک می‌کند الگوهای غیرعادی شناسایی شود، مثلاً اگر یک کارمند نیمه‌شب از یک کشور دیگر به سیستم وارد شد. حرکت جانبی مهاجم در شبکه باید رصد شود. سناریوهای حمله رایج در بانک‌ها شامل فیشینگ هدفمند، حملات مرد میانی[3] و سرقت نشست است. تیم باید بداند در ۱۵ دقیقه اول یک حادثه دقیقاً چه اقداماتی انجام دهد. (Verizon, ۲۰۲۳)

روش آموزش: دوره‌های فشرده ۳ تا ۵ روزه با مربی متخصص، لاب‌های عملی در محیط شبیه‌سازی شده بانک، سناریوهای واقعی از حملات گذشته، گواهینامه داخلی پس از قبولی در آزمون عملی و بازآموزی فصلی با به‌روزرسانی تهدیدات جدید. (IBM Security, ۲۰۲۳)

۳. آموزش رفتاری: فرهنگ امنیتی، گزارش ناهنجاری‌ها، عدم اشتراک رمزها

این سطح به تغییر عادت‌ها و رفتارهای روزمره کارکنان می‌پردازد و معمولاً سخت‌ترین بخش آموزش است چون با عادت‌های قدیمی در تضاد قرار می‌گیرد. (Deloitte, ۲۰۲۲)

فرهنگ امنیتی: باید این باور در سازمان نهادینه شود که امنیت مسئولیت همه است، نه فقط تیم فناوری اطلاعات. امنیت نباید قربانی سرعت و راحتی شود. کارکنان باید تفکر «برای من اتفاق نمی‌افتد» را کنار بگذارند. مدیران ارشد باید در رفتار خود اولویت امنیت را نشان دهند، مثلاً خودشان از احراز هویت چندعاملی استفاده کنند و رمزشان را با کسی به اشتراک نگذارند. سیستم پاداش برای رفتار امن مؤثرتر از تنبیه برای اشتباه است. هدف نهایی این است که امنیت مثل بستن کمربند ایمنی به یک عادت روزمره تبدیل شود. (SANS Institute, ۲۰۲۲)

گزارش ناهنجاری‌ها: کارکنان باید دقیقاً بدانند چه چیزی را باید گزارش دهند: ایمیل مشکوک، تماس عجیب، خطای سیستمی غیرمنتظره، فرد ناشناس در محیط کار. باید یک کانال مشخص برای گزارش وجود داشته باشد: فرم استاندارد، خط تلفن ویژه یا ایمیل مخصوص. اصل مهم این است که گزارش باید بلافاصله انجام شود، نه بعد از اینکه کارمند خودش تحقیق کرد و مطمئن شد. فرهنگ گزارش‌دهی بدون

[1] Just-In-Time:JIT
[2] Security Information and Event Management: SIEM
[3] Man-in-the-Middle

ترس حیاتی است: هیچکس به خاطر گزارش اشتباه تنبیه نمی‌شود. برای موارد حساس، امکان گزارش ناشناس باید فراهم باشد. (Rose et al., ۲۰۲۰)

عدم اشتراک رمزها: اشتراک رمز عبور چند مشکل جدی ایجاد می‌کند: ردپای دیجیتال از بین می‌رود و نمی‌شود فهمید چه کسی چه کاری انجام داده، مسئولیت‌پذیری کاهش می‌یابد و امنیت کلی به خطر می‌افتد. راهکار جایگزین برای مواقع ضروری، استفاده از خزانه رمزعبور[1]است که رمزها را به صورت امن به اشتراک می‌گذارد. کارکنان باید از مدیریت کننده رمزعبور[2]استفاده کنند به جای نوشتن رمز روی کاغذ. رمزهای پیش‌فرض سیستم‌ها باید فوراً تغییر داده شوند و از رمز تکراری بین سیستم‌های مختلف استفاده نشود. (Palo Alto Networks, ۲۰۲۳)

روش آموزش: جلسات گروهی کوچک ۱۰ تا ۱۵ نفره برای بحث و تبادل نظر، نقش‌آفرینی با اجرای سناریوهای واقعی، ارسال ایمیل‌های یادآوری هفتگی با نکات کوتاه، کمپین‌های فصلی با شعارهای جذاب و جوایز، و داستان‌گویی از حوادث واقعی برای تأثیرگذاری بیشتر. (Ponemon Institute, ۲۰۲۲)

۴. شبیه‌سازی حملات: فیشینگ، مهندسی اجتماعی، سناریوهای واقعی

این پیشرفته‌ترین سطح آموزش است که دانش و رفتار کارکنان را در عمل می‌سنجد. شبیه‌سازی‌ها باید بدون اطلاع قبلی کارکنان انجام شوند. (Bada et al., ۲۰۱۵)

شبیه‌سازی فیشینگ: ایمیل‌های فیشینگ آزمایشی برای کارکنان ارسال می‌شود و درصد کلیک روی لینک‌ها اندازه‌گیری می‌شود. سناریوهای مختلفی می‌توان طراحی کرد: ایمیل جعلی از طرف مدیرعامل که درخواست انتقال وجه فوری دارد، ایمیل جعلی از طرف واحد فناوری اطلاعات برای به‌روزرسانی رمز عبور، ایمیل جعلی از طرف بانک مرکزی با لینک مخرب، یا ایمیل جعلی اطلاع‌رسانی جایزه یا تخفیف ویژه. به کسانی که روی لینک کلیک کردند، بلافاصله آموزش داده می‌شود. این شبیه‌سازی باید ماهانه با سناریوهای جدید تکرار شود. هدف این است که نرخ کلیک از میانگین ۳۰درصد به زیر ۵درصد در ۶ ماه برسد. (نوروزی و صادقی، ۱۴۰۲)

شبیه‌سازی مهندسی اجتماعی: تماس تلفنی آزمایشی با کارکنان با هویت جعلی انجام می‌شود. سناریوهای رایج شامل تماس جعلی از پشتیبانی فنی برای دریافت رمز عبور، تماس جعلی از واحد حسابرسی برای دریافت اطلاعات مشتری، مراجعه حضوری فردی با هویت جعلی به شعبه، و پیامک جعلی با لینک مخرب است. ارزیابی می‌شود که چه تعداد اطلاعات را فاش کردند و چه تعداد حادثه را گزارش دادند. با

[1] Password Vault
[2] Password Manager

افرادی که فریب خوردند، جلسه خصوصی آموزشی برگزار می‌شود. (McKinsey & Company, ۲۰۲۳)

سناریوهای واقعی ترکیبی: حملات چندمرحله‌ای شبیه‌سازی می‌شود: ایمیل فیشینگ، کلیک روی لینک، دانلود بدافزار و تلاش برای دسترسی به سیستم. سناریوی دورکاری: کارمند در خانه تماس می‌گیرد که رمز سیستم را فراموش کرده. سناریوی بحران: اعلام خبر جعلی قطعی سیستم و درخواست ورود اضطراری. سناریوی زنجیره تأمین: تماس جعلی از طرف شرکت پشتیبان نرم‌افزاری بانک. سناریوی فیزیکی: فردی با لباس تعمیرات وارد مرکز داده می‌شود. (European Union Agency for Cybersecurity, ۲۰۲۳)

اندازه‌گیری و گزارش: درصد کارکنانی که در هر سناریو فریب خوردند، درصد کارکنانی که حادثه را گزارش کردند، زمان واکنش از لحظه حمله تا گزارش، مقایسه عملکرد بین شعب و واحدهای مختلف و روند بهبود در طول زمان اندازه‌گیری می‌شود. (Ponemon Institute, ۲۰۲۲)

روش اجرا: با هماهنگی تیم امنیت و منابع انسانی انجام می‌شود. کارکنان از قبل مطلع نمی‌شوند. از ابزارهای تخصصی مثل KnowBe4 یا Gophish استفاده می‌شود. ارزیابی ماهانه و گزارش فصلی به مدیریت ارائه می‌شود. افراد فریب‌خورده تنبیه نمی‌شوند، فقط آموزش می‌بینند. (Deloitte, ۲۰۲۲)

۳. چالش‌های آموزش اعتماد صفر در بانک‌ها (SANS Institute, ۲۰۲۲)

پیاده‌سازی برنامه آموزشی اعتماد صفر در بانک‌ها با چالش‌های متعددی روبرو است که اگر به درستی مدیریت نشوند، می‌توانند کل پروژه را با شکست مواجه کنند. در ادامه چهار چالش اصلی بررسی می‌شود: (Bada et al., ۲۰۱۵)

۱. مقاومت فرهنگی در برابر تغییر (McKinsey & Company, ۲۰۲۳)

این چالش شاید بزرگترین مانع در مسیر آموزش اعتماد صفر باشد. ریشه این مقاومت به عوامل مختلفی برمی‌گردد:

علل مقاومت: بسیاری از کارکنان بانک سال‌هاست با یک روش خاص کار می‌کنند و تغییر رویه‌های امنیتی را یک مزاحمت بیهوده می‌دانند. جمله رایجی که بارها شنیده می‌شود این است: «ما ۲۰ ساله اینجوری کار می‌کنیم، چیزی هم نشده!» این طرز فکر خطرناک است چون تهدیدات امروز با ۲۰ سال پیش اصلاً قابل مقایسه نیست. همچنین برخی کارکنان احساس می‌کنند آموزش‌های امنیتی به معنای بی‌اعتمادی سازمان به آنهاست و این حس باعث مقاومت ناخودآگاه می‌شود. (Verizon, ۲۰۲۳)

نشانه‌های مقاومت:

- حضور فیزیکی در جلسات آموزشی اما عدم توجه واقعی (Deloitte, ۲۰۲۲)
- بهانه‌آوری برای شرکت نکردن در دوره‌ها (SANS Institute, ۲۰۲۲)
- مسخره کردن یا دست‌کم گرفتن اهمیت آموزش‌ها (Bada et al., ۲۰۱۵)
- بازگشت سریع به عادت‌های قدیمی پس از آموزش (McKinsey & Company, ۲۰۲۳)
- شکایت از وقت‌گیر بودن فرآیندهای امنیتی جدید (Deloitte, ۲۰۲۲)

راهکارهای مقابله: اولین قدم، جلب حمایت مدیران ارشد است. وقتی مدیرعامل یا اعضای هیئت مدیره شخصاً در جلسات آموزشی شرکت کنند و از اعتماد صفر حمایت کنند، مقاومت بقیه کاهش می‌یابد. دوم، باید دلیل تغییر را به زبان ساده و با مثال‌های ملموس توضیح داد، نه با اصطلاحات فنی. سوم، می‌توان از کارکنان تأثیرگذار و محبوب در هر واحد به عنوان «سفیران امنیت» استفاده کرد تا بقیه را همراه کنند. چهارم، باید به کارکنان نشان داد که آموزش‌های امنیتی به نفع خودشان هم هست، نه فقط به نفع بانک. مثلاً یادگیری تشخیص ایمیل فیشینگ در زندگی شخصی هم به کارشان می‌آید. (IBM Security, ۲۰۲۳)

۲. کمبود زمان و منابع (SANS Institute, ۲۰۲۲)

بانک‌ها محیط‌های پرمشغله‌ای هستند و کارکنان معمولاً حجم کار بالایی دارند. این چالش دو بعد دارد: کمبود زمان کارکنان برای شرکت در آموزش و کمبود بودجه سازمان برای اجرای برنامه آموزشی جامع. (Bada et al., ۲۰۱۵)

کمبود زمان کارکنان: یک متصدی باجه که روزانه با ده‌ها مشتری سروکار دارد، به سختی می‌تواند چند ساعت را صرف یک کارگاه آموزشی کند. فشار کاری باعث می‌شود آموزش در اولویت آخر قرار بگیرد. برخی مدیران میانی هم کارکنان را برای شرکت در آموزش‌ها تشویق نمی‌کنند چون نگران عقب افتادن کارها هستند. راهکار این است که آموزش‌ها به صورت ماژول‌های کوتاه ۱۵ تا ۲۰ دقیقه‌ای طراحی شوند که کارمند بتواند در زمان‌های مرده روز (مثلاً ابتدای شیفت یا زمان استراحت) آنها را ببیند. همچنین می‌توان بخشی از آموزش را به صورت گیمیفیکیشن (بازی‌سازی) درآورد تا جذابیت بیشتری داشته باشد. (McKinsey & Company, ۲۰۲۳)

کمبود بودجه: طراحی و اجرای یک برنامه آموزشی جامع هزینه‌بر است: حقوق مربیان متخصص، خرید ابزارهای شبیه‌سازی، تولید محتوای چندرسانه‌ای، برگزاری کارگاه‌ها و... مدیران مالی معمولاً این هزینه‌ها را غیرضروری می‌بینند و ترجیح می‌دهند بودجه را صرف خرید تجهیزات فنی کنند. برای غلبه بر این

چالش، باید بازگشت سرمایه آموزش را به صورت عددی نشان داد. مثلاً محاسبه کرد که هزینه یک نقض داده چقدر است و آموزش چقدر احتمال وقوع آن را کاهش می‌دهد. همچنین می‌توان از راهکارهای کم‌هزینه مثل محتوای آموزشی داخلی، وبینارهای رایگان و همکاری با دانشگاه‌ها استفاده کرد. (Ponemon Institute, ۲۰۲۲)

۳. تفاوت سطح دانش فنی پرسنل (Verizon, ۲۰۲۳)

یکی از بزرگترین چالش‌های آموزش در بانک، تنوع بالای سطح سواد دیجیتال و دانش فنی کارکنان است. یک بانک کارکنانی با طیف وسیعی از دانش فنی دارد: (Deloitte, ۲۰۲۲)

طیف دانش فنی در بانک:

کارکنان مسن یا کم‌تجربه در فناوری: برخی کارکنان قدیمی بانک ممکن است حتی با مفاهیم پایه‌ای مثل ایمیل و مرورگر وب هم مشکل داشته باشند. آموزش مفاهیمی مثل اعتماد صفر و احراز هویت چندعاملی برای این گروه بسیار چالش‌برانگیز است. (SANS Institute, ۲۰۲۲)

کارکنان با دانش متوسط: اکثر کارکنان بانک در این دسته قرار می‌گیرند. آنها با کارهای روزمره دیجیتال آشنا هستند اما دانش عمیق فنی ندارند. (Bada et al., ۲۰۱۵)

کارشناسان فناوری اطلاعات: این گروه دانش فنی بالایی دارند و آموزش‌های سطح پایه برایشان تکراری و خسته‌کننده است. (McKinsey & Company, ۲۰۲۳)

مدیران ارشد: معمولاً وقت محدودی دارند و نیاز به آموزش‌های فشرده و مختصر دارند. (Deloitte, ۲۰۲۲)

مشکل آموزش یکسان برای همه: اگر همه کارکنان در یک کلاس مشترک آموزش ببینند، گروه کم‌تجربه گیج می‌شود و گروه متخصص حوصله‌اش سر می‌رود. نتیجه این می‌شود که هیچکدام آموزش مؤثری دریافت نمی‌کنند. (SANS Institute, ۲۰۲۲)

راهکار: طراحی آموزش مبتنی بر نقش ضروری است. ابتدا باید سطح دانش فنی هر کارمند سنجیده شود (مثلاً با یک آزمون ساده آنلاین). سپس کارکنان در گروه‌های هم‌سطح دسته‌بندی شوند و محتوای آموزشی متناسب با هر گروه طراحی شود. برای کارکنان کم‌تجربه، آموزش باید بسیار ساده و تصویری باشد و مفاهیم پایه را پوشش دهد. برای کارشناسان فناوری اطلاعات، آموزش باید عمیق و فنی باشد. برای مدیران، آموزش باید مختصر و استراتژیک باشد. همچنین می‌توان از سیستم «آموزش همتا به همتا» استفاده کرد: کارشناسان فناوری اطلاعات به عنوان مربی برای همکاران کم‌تجربه‌تر عمل کنند. (Bada et al., ۲۰۱۵)

۴. نیاز به آموزش مستمر (نه یک‌باره)

بسیاری از بانک‌ها اشتباه رایجی مرتکب می‌شوند: یک دوره آموزشی فشرده برگزار می‌کنند، همه را یک بار آموزش می‌دهند و تصور می‌کنند کار تمام شده است. این رویکرد کاملاً اشتباه است. (McKinsey & Company, ۲۰۲۳)

چرا آموزش یک‌باره جواب نمی‌دهد؟ مغز انسان به طور طبیعی اطلاعاتی را که استفاده نمی‌کند فراموش می‌کند. منحنی فراموشی نشان می‌دهد که افراد پس از ۳۰ روز، حدود ۷۰درصد از محتوای آموزشی را فراموش می‌کنند. تهدیدات سایبری هم مدام در حال تغییر هستند. یک روش حمله که امروز رایج است، ممکن است شش ماه دیگر منسوخ شده باشد و روش‌های جدیدی جای آن را گرفته باشند. همچنین کارکنان جدید به بانک ملحق می‌شوند که آموزش ندیده‌اند. کارکنان قدیمی هم ممکن است به مرور زمان دچار غفلت و سهل‌انگاری شوند. (European Union Agency for Cybersecurity, ۲۰۲۳)

الگوی آموزش مستمر: آموزش امنیتی باید مثل ورزش بدنی باشد: یک جلسه سنگین در ابتدای سال کافی نیست، باید به صورت منظم و مداوم تکرار شود. الگوی پیشنهادی شامل موارد زیر است: (Deloitte, ۲۰۲۲)

آموزش اولیه: همه کارکنان جدید باید پیش از شروع کار، دوره پایه اعتماد صفر را بگذرانند. (SANS Institute, ۲۰۲۲)

یادآوری هفتگی: ارسال نکات کوتاه امنیتی از طریق ایمیل یا پیامک (مثلاً «این هفته مراقب ایمیل‌های جعلی با موضوع عیدی باشید»)

آموزش ماهانه: یک ماژول کوتاه ۱۰ دقیقه‌ای با موضوع جدید هر ماه (Bada et al., ۲۰۱۵)

شبیه‌سازی فصلی: برگزاری سناریوهای شبیه‌سازی شده هر سه ماه یکبار (McKinsey & Company, ۲۰۲۳)

بازآموزی سالانه: یک دوره فشرده سالانه برای مرور مفاهیم و معرفی تهدیدات جدید (Verizon, ۲۰۲۳)

آموزش پس از حادثه: اگر یک حادثه امنیتی واقعی رخ داد، بلافاصله یک جلسه آموزشی ویژه برگزار شود. (Deloitte, ۲۰۲۲)

شاخص‌های سنجش تداوم: برای اطمینان از اثربخشی آموزش مستمر، باید شاخص‌های مشخصی تعریف کرد:

درصد کارکنانی که در هر دوره آموزشی شرکت کرده‌اند (SANS Institute, ۲۰۲۲)
نمرات آزمون‌های دوره‌ای (آیا در حال بهبود است یا کاهش؟)
نرخ کلیک روی ایمیل‌های فیشینگ شبیه‌سازی شده (آیا در حال کاهش است؟)
تعداد گزارش‌های دریافتی از کارکنان (آیا در حال افزایش است؟)
زمان بین وقوع حادثه و گزارش آن (آیا در حال کاهش است؟)

٤. راهکارهای عملی برای آموزش و پیاده‌سازی اعتماد صفر (Bada et al., ۲۰۱۵)

در این بخش، پنج راهکار عملی و اجرایی برای غلبه بر چالش‌های آموزش و پیاده‌سازی مؤثر اعتماد صفر در بانک بررسی می‌شود:

۱. برگزاری کارگاه‌های دوره‌ای (McKinsey & Company, ۲۰۲۳)

کارگاه‌های آموزشی باید به صورت منظم و با ساختاری مشخص برگزار شوند تا اثربخشی لازم را داشته باشند. (Deloitte, ۲۰۲۲)

نوع کارگاه‌ها:

کارگاه‌های عمومی (همه کارکنان): مرور مفاهیم پایه اعتماد صفر، آشنایی با تهدیدات جدید، آموزش رفتارهای امنیتی. هر سه ماه یکبار، هر جلسه ۱ تا ۱٫۵ ساعت. (IBM Security, ۲۰۲۳)

کارگاه‌های تخصصی (تیم فناوری اطلاعات): آموزش عمیق ابزارها، سناریوهای حمله پیشرفته، مدیریت بحران. هر ماه یکبار، هر جلسه ۲ تا ۳ ساعت. (SANS Institute, ۲۰۲۲)

کارگاه‌های مدیریتی (مدیران ارشد): تحلیل ریسک، تصمیم‌گیری در بحران، تخصیص بودجه امنیتی. هر شش ماه یکبار، هر جلسه ۲ ساعت. (Bada et al., ۲۰۱۵)

کارگاه‌های موردی: پس از وقوع هر حادثه امنیتی واقعی یا شبیه‌سازی شده، یک کارگاه فوری برای تحلیل و یادگیری برگزار شود. (McKinsey & Company, ۲۰۲۳)

ساختار هر کارگاه: یک کارگاه مؤثر باید سه بخش داشته باشد: ۱۵ دقیقه اول مرور سریع مطالب جلسه قبل، ۴۰ تا ۶۰ دقیقه محتوای جدید با مثال‌های عملی و سناریوهای واقعی، و ۱۵ دقیقه پایانی پرسش و پاسخ و بحث گروهی. استفاده از ویدئوهای کوتاه، اینفوگرافیک و داستان‌گویی تأثیر کارگاه را چند برابر می‌کند. (Deloitte, ۲۰۲۲)

نکات کلیدی:

کارگاه‌ها را در ساعات کاری برگزار کنید، نه بعد از کار (SANS Institute, ۲۰۲۲)

از مربیان داخلی (کارشناسان فناوری اطلاعات بانک) به همراه مربیان خارجی استفاده کنید (Gartner, ۲۰۲۲)

حتماً حضور و غیاب کنید و به مدیران واحدها گزارش دهید (SANS Institute, ۲۰۲۲)

بازخورد شرکت‌کنندگان را بعد از هر کارگاه جمع‌آوری کنید (Bada et al., ۲۰۱۵)

محتوای کارگاه‌ها را بر اساس بازخوردها و تهدیدات جدید به‌روز کنید. (Ponemon Institute, ۲۰۲۲)

۲. استفاده از سیستم مدیریت یادگیری (McKinsey & Company, ۲۰۲۳)

یک سیستم مدیریت یادگیری خوب ستون فقرات برنامه آموزشی بانک است. بدون آن، مدیریت آموزش‌ها در مقیاس یک بانک با صدها یا هزاران کارمند تقریباً غیرممکن می‌شود. (Deloitte, ۲۰۲۲)

انتخاب سیستم مدیریت یادگیری مناسب: سیستم باید قابلیت‌های زیر را داشته باشد: بارگذاری محتوای چندرسانه‌ای (ویدئو، اسلاید، اینفوگرافیک)، برگزاری آزمون آنلاین، پیگیری پیشرفت هر کارمند، گزارش‌گیری مدیریتی، ارسال نوتیفیکیشن و ایمیل خودکار، قابلیت اجرا روی موبایل، و امکان تعریف نقش‌های مختلف (کارمند، مربی، مدیر).

محتوای بارگذاری شده در سیستم مدیریت یادگیری:

ویدئوهای کوتاه آموزشی (۵ تا ۱۵ دقیقه) برای هر مبحث (SANS Institute, ۲۰۲۲)

اسلایدهای قابل دانلود برای مرور (Bada et al., ۲۰۱۵)

آزمون‌های آنلاین با سوالات چهارگزینه‌ای و تشریحی (McKinsey & Company, ۲۰۲۳)

سناریوهای تعاملی (مثلاً «اگر این ایمیل را دیدی چکار می‌کنی؟»)

اینفوگرافیک و چک‌لیست‌های قابل چاپ (Deloitte, ۲۰۲۲)

کتابخانه مرجع شامل سیاست‌ها و پروتکل‌های امنیتی بانک (Hassan & Al-Muhtadi, ۲۰۲۲)

مدیریت با سیستم مدیریت یادگیری:

هر کارمند یک حساب کاربری دارد و می‌تواند در هر زمان و مکانی به محتوا دسترسی داشته باشد (IBM Security, ۲۰۲۳)

سیستم پیشرفت هر فرد را ثبت می‌کند و یادآوری ارسال می‌کند (Rose et al., ۲۰۲۰)

مدیران می‌توانند گزارش جامع از وضعیت آموزش کل سازمان بگیرند (SANS Institute, ۲۰۲۲)

محتوای آموزشی بر اساس نقش و سطح دانش هر کارمند شخصی‌سازی می‌شود (Bada et al., ۲۰۱۵)

سیستم مدیریت یادگیری به سیستم منابع انسانی بانک متصل است تا آموزش کارکنان جدید و خروجی‌ها مدیریت شود (McKinsey & Company, ۲۰۲۳)

سیستم مدیریت یادگیریهای مناسب برای بانک‌های ایرانی: سیستم‌های خارجی مثل Moodle (رایگان و متن‌باز) یا Talent LMSو سامانه‌های داخلی مثل لرنیکس، سامانه آموزش مجازی فرادرس و پلتفرم‌های بومی دیگر. انتخاب باید بر اساس نیازها، بودجه و زیرساخت فنی بانک انجام شود. (بانک مرکزی جمهوری اسلامی ایران، ۱۴۰۰)

۳. ارزیابی و آزمون دوره‌ای (Deloitte, ۲۰۲۲)

آموزش بدون ارزیابی مثل تیراندازی در تاریکی است: نمی‌دانی به هدف زدی یا نه. ارزیابی باید در سه سطح انجام شود. (SANS Institute, ۲۰۲۲)

سطح اول: سنجش دانش (آزمون‌های تئوری)

- پس از هر دوره آموزشی، یک آزمون آنلاین ۱۰ تا ۱۵ سوالی برگزار شود (Bada et al., ۲۰۱۵)
- سوالات ترکیبی از مفاهیم پایه، سناریوهای عملی و سیاست‌های بانک باشد (Alshaikh et al., ۲۰۲۱)
- حداقل نمره قبولی ۸۰درصد تعیین شود (McKinsey & Company, ۲۰۲۳)
- افراد مردود باید تا قبولی مجدداً آموزش ببینند و آزمون دهند (Deloitte, ۲۰۲۲)
- آزمون‌ها به صورت تصادفی از بانک سوال انتخاب کنند تا تقلب کاهش یابد (SANS Institute, ۲۰۲۲)

سطح دوم: سنجش رفتار (شبیه‌سازی و مانور)

- ارسال ایمیل‌های فیشینگ آزمایشی و اندازه‌گیری نرخ کلیک (European Union Agency for Cybersecurity, ۲۰۲۳)
- تماس‌های تلفنی آزمایشی مهندسی اجتماعی (Bada et al., ۲۰۱۵)
- سناریوهای حضوری (فرد ناشناس در مرکز داده)
- اندازه‌گیری زمان واکنش در مواجهه با حادثه شبیه‌سازی شده (McKinsey & Company, ۲۰۲۳)
- این ارزیابی‌ها بدون اطلاع قبلی و به صورت دوره‌ای انجام شود (Deloitte, ۲۰۲۲)

سطح سوم: سنجش تأثیر (شاخص‌های کلیدی)

- کاهش تعداد حوادث امنیتی واقعی در طول زمان (Verizon, ۲۰۲۳)
- کاهش میانگین زمان تشخیص و پاسخ به حوادث (IBM Security, ۲۰۲۳)
- افزایش تعداد گزارش‌های دریافتی از کارکنان (Ponemon Institute, ۲۰۲۲)
- کاهش هزینه‌های ناشی از خطاهای انسانی (SANS Institute, ۲۰۲۲)
- بهبود نتایج ممیزی‌های امنیتی داخلی و خارجی (Bada et al., ۲۰۱۵)
- نحوه گزارش‌دهی: نتایج ارزیابی‌ها باید به صورت شفاف به ذی‌نفعان گزارش شود:
- گزارش ماهانه به تیم امنیت: جزئیات فنی و آماری (McKinsey & Company, ۲۰۲۳)
- گزارش فصلی به مدیران ارشد: روندها و شاخص‌های کلان (Verizon, ۲۰۲۳)
- گزارش سالانه به هیئت مدیره: ارزیابی کلی و پیشنهادات بودجه‌ای (Deloitte, ۲۰۲۲)
- بازخورد فردی به هر کارمند: نقاط قوت و ضعف شخصی (SANS Institute, ۲۰۲۲)

۴. تشویق و جریمه برای رعایت امنیت (Bada et al., ۲۰۱۵)

ایجاد انگیزه در کارکنان برای رعایت اصول امنیتی نیاز به ترکیبی از تشویق و جریمه دارد. تمرکز اصلی باید بر تشویق باشد، اما جریمه‌های هوشمندانه هم لازم است. (SANS Institute, ۲۰۲۲)

سیستم تشویق:

کارمند امن ماه: به کارکنانی که در شبیه‌سازی‌ها بهترین عملکرد را دارند یا بیشترین گزارش‌های مفید را ثبت کرده‌اند، جایزه نقدی یا کارت هدیه تعلق گیرد (Ponemon Institute, ۲۰۲۲)

امتیاز امنیتی: هر کارمند یک امتیاز امنیتی داشته باشد که با رفتارهای مثبت افزایش یابد (مثلاً گزارش ایمیل مشکوک +۵ امتیاز، قبولی در آزمون +۱۰ امتیاز)

تخفیف در آموزش‌های جانبی: کارمندانی که امتیاز بالایی دارند، از تخفیف دوره‌های آموزشی غیرمرتبط بهره‌مند شوند (McKinsey & Company, ۲۰۲۳)

تقدیر عمومی: در جلسات ماهانه یا خبرنامه داخلی از کارکنان برتر تقدیر شود (Verizon, ۲۰۲۳)

جوایز تیمی: بهترین شعبه یا واحد از نظر شاخص‌های امنیتی، جایزه تیمی دریافت کند (Deloitte, ۲۰۲۲)

سیستم جریمه: جریمه‌ها باید آموزشی باشند، نه تنبیهی صرف. هدف اصلاح رفتار است، نه تنبیه کارمند. (SANS Institute, ۲۰۲۲)

تذکر شفاهی: برای اولین تخلف جزئی (مثلاً رها کردن سیستم بدون قفل)

آموزش اضافه: برای تخلفات تکراری، کارمند باید یک دوره آموزشی اضافی بگذراند (Bada et al., ۲۰۱۵)

کسر امتیاز امنیتی: برای تخلفات جدی‌تر (مثلاً اشتراک رمز عبور)

گزارش به مدیر مستقیم: برای تخلفات جدی و تکراری (McKinsey & Company, ۲۰۲۳)

تأثیر بر ارزیابی سالانه: برای تخلفات بسیار جدی (مثلاً افشای عمدی اطلاعات)، امتیاز ارزیابی عملکرد کاهش یابد (Deloitte, ۲۰۲۲)

نکات مهم:

قوانین تشویق و جریمه باید از قبل به صورت شفاف به همه کارکنان ابلاغ شود (Bada et al., ۲۰۱۵)

اجرای قوانین باید برای همه یکسان باشد، از مدیرعامل تا کارمند تازه‌وارد (SANS Institute, ۲۰۲۲)

جریمه‌ها نباید به گونه‌ای باشد که کارکنان تخلفات را پنهان کنند (Ponemon Institute, ۲۰۲۲)

فرهنگ تشویق باید بر فرهنگ جریمه غلبه داشته باشد (نسبت ۷۰ به ۳۰)

۵. ایجاد تیم واکنش سریع امنیتی در بانک (Palo Alto Networks, ۲۰۲۳)

تیم واکنش سریع یک تیم تخصصی است که در زمان وقوع حوادث امنیتی وارد عمل می‌شود. وجود این تیم نه تنها برای پاسخ به حوادث ضروری است، بلکه نقش آموزشی مهمی هم دارد. (Ponemon Institute, ۲۰۲۲)

ساختار تیم: یک تیم واکنش سریع امنیتی در بانک باید حداقل شامل این نقش‌ها باشد:

- مدیر تیم: مسئول هماهنگی کلی و تصمیم‌گیری نهایی (Bada et al., ۲۰۱۵)
- تحلیلگر امنیتی: مسئول تحلیل لاگ‌ها و شناسایی ماهیت حمله (Gartner, ۲۰۲۲)
- کارشناس فناوری اطلاعات: مسئول اقدامات فنی مثل قطع دسترسی یا ایزوله کردن سیستم (IBM Security, ۲۰۲۳)

- کارشناس حقوقی: مسئول مسائل قانونی و مستندسازی برای پیگرد قانونی (McKinsey & Company, ۲۰۲۳)
- مسئول ارتباطات: مسئول اطلاع‌رسانی داخلی و خارجی (به مشتریان، رسانه‌ها، بانک مرکزی)
- نماینده منابع انسانی: مسئول هماهنگی با کارکنان درگیر در حادثه (Verizon, ۲۰۲۳)

وظایف تیم:

- پاسخ به حوادث: شناسایی، مهار، ریشه‌یابی و بازیابی پس از هر حادثه امنیتی (European Union Agency for Cybersecurity, ۲۰۲۳)
- تحلیل پس از حادثه: بررسی علل ریشه‌ای و ارائه توصیه‌های پیشگیرانه (Deloitte, ۲۰۲۲)
- آموزش: برگزاری کارگاه‌های آموزشی بر اساس درس‌های گرفته شده از حوادث واقعی (Verizon, ۲۰۲۳)
- به‌روزرسانی پروتکل‌ها: اصلاح و بهبود مستمر رویه‌های امنیتی (SANS Institute, ۲۰۲۲)
- هماهنگی با نهادهای خارجی: بانک مرکزی، پلیس فتا، مرکز ماهر (احمدی و محمدی، ۱۴۰۰)

آموزش تیم واکنش سریع: اعضای این تیم نیاز به آموزش‌های تخصصی و مداوم دارند:

- شرکت در دوره‌های تخصصی امنیت سایبری (CEH، CISSP، OSCP)
- شرکت در مانورهای ملی امنیت سایبری (Bada et al., ۲۰۱۵)
- شبیه‌سازی سناریوهای حمله در محیط آزمایشگاهی (McKinsey & Company, ۲۰۲۳)
- بازآموزی فصلی با توجه به تهدیدات جدید (IBM Security, ۲۰۲۳)
- شرکت در کنفرانس‌ها و کارگاه‌های بین‌المللی (Deloitte, ۲۰۲۲)

ارتباط تیم با سایر کارکنان: تیم واکنش سریع باید یک خط ارتباطی مستقیم و ساده با همه کارکنان داشته باشد:

- یک شماره تلفن داخلی مخصوص (مثلاً ۱۹۹) برای گزارش حوادث (Ponemon Institute, ۲۰۲۲)

- یک ایمیل اختصاصی (security@bank.ir)
- یک کانال در پیام‌رسان داخلی بانک (Deloitte, ۲۰۲۲)
- امکان گزارش ناشناس برای موارد حساس (SANS Institute, ۲۰۲۲)
- پاسخگویی سریع (حداکثر ۱۵ دقیقه) به هر گزارش (Bada et al., ۲۰۱۵)

مانورهای دوره‌ای تیم: تیم باید حداقل هر سه ماه یکبار یک مانور برگزار کند:

- مانور فیشینگ گسترده (European Union Agency for Cybersecurity, ۲۰۲۳)
- مانور حمله باج‌افزاری (McKinsey & Company, ۲۰۲۳)
- مانور نشت اطلاعات (Deloitte, ۲۰۲۲)
- مانور قطعی سیستم (Rose et al., ۲۰۲۰)
- مانور حمله فیزیکی به مرکز داده (SANS Institute, ۲۰۲۲)

این پنج راهکار عملی مکمل یکدیگر هستند. کارگاه‌ها دانش اولیه را منتقل می‌کنند، سیستم مدیریت یادگیری این دانش را در دسترس و ماندگار می‌کند، ارزیابی‌ها اثربخشی را می‌سنجند، تشویق و جریمه انگیزه ایجاد می‌کند و تیم واکنش سریع ضمانت اجرایی نهایی است. بانکی که این پنج راهکار را به صورت یکپارچه پیاده کند، نه تنها اعتماد صفر را موفق‌تر اجرا می‌کند، بلکه فرهنگ امنیتی پایداری ایجاد می‌کند که در بلندمدت از سازمان و مشتریان محافظت خواهد کرد. (Bada et al., ۲۰۱۵)

نتیجه‌گیری

آموزش مؤثر برای پیاده‌سازی اعتماد صفر در بانک‌ها یک موضوع چندبعدی است که نمی‌توان آن را صرفاً به برگزاری چند کارگاه آموزشی تقلیل داد. آنچه از بررسی جامع این موضوع به دست می‌آید، چند نکته کلیدی است:

اول، آموزش بدون استراتژی شکست می‌خورد. بسیاری از بانک‌ها منابع قابل توجهی صرف خرید ابزارهای امنیتی می‌کنند اما برای آموزش کارکنان بودجه کافی اختصاص نمی‌دهند. این یک اشتباه استراتژیک است. ابزارهای اعتماد صفر بدون همراهی کاربران، مثل قفل‌های فوق‌پیشرفته‌ای هستند که کلیدشان را به همه داده‌اید. تحقیقات نشان می‌دهد بیش از ۷۰درصد شکست پروژه‌های اعتماد صفر ریشه در عوامل انسانی دارد، نه فنی. پس سرمایه‌گذاری روی آموزش، نه یک هزینه اضافی، بلکه یک ضرورت حیاتی است.

دوم، تفاوت سطح دانش فنی کارکنان بانک یک واقعیت انکارناپذیر است. از متصدی باجه ۵۵ ساله که تازه با موبایل هوشمند آشنا شده تا کارشناس ارشد امنیت که چندین گواهینامه بین‌المللی دارد، همه در یک سازمان کار می‌کنند. طراحی یک برنامه آموزشی یکسان برای همه این افراد نه تنها بی‌اثر است، بلکه می‌تواند نتیجه معکوس داشته باشد: گروه کم‌تجربه را سردرگم و گروه متخصص را خسته می‌کند. راهکار، طراحی آموزش مبتنی بر نقش و سطح دانش است.

سوم، مقاومت فرهنگی بزرگترین مانع است. تغییر عادت‌های دیرینه کارکنان بانک کار ساده‌ای نیست. جمله «ما ۲۰ ساله اینجوری کار می‌کنیم» را باید جدی گرفت. این مقاومت ریشه در ترس از تغییر، احساس بی‌اعتمادی و ندیدن دلیل تغییر دارد. غلبه بر این مقاومت نیاز به صبر، ارتباط مؤثر و همراهی مدیران ارشد دارد. جالب اینجاست که وقتی مدیرعامل شخصاً در کارگاه آموزشی شرکت می‌کند و از MFA استفاده می‌کند، تأثیرش از صدها بخشنامه بیشتر است.

چهارم، آموزش یک‌باره کافی نیست. منحنی فراموشی نشان می‌دهد افراد پس از ۳۰ روز حدود ۷۰درصد از محتوای آموزشی را فراموش می‌کنند. تهدیدات سایبری هم مدام در حال تغییرند. پس آموزش باید مستمر، تدریجی و به‌روز باشد. الگوی «آموزش در لحظه» که در آن کارمند درست در زمان مواجهه با یک تهدید، آموزش مرتبط را دریافت می‌کند، اثربخشی بسیار بالاتری نسبت به آموزش‌های فشرده سالانه دارد.

پنجم، ارزیابی و اندازه‌گیری ضروری است. بدون سنجش، نمی‌توان فهمید آموزش مؤثر بوده یا نه. ارزیابی باید در سه سطح انجام شود: سنجش دانش (آزمون)، سنجش رفتار (شبیه‌سازی) و سنجش تأثیر (شاخص‌های کلیدی). بانکی که فقط آزمون برگزار می‌کند اما رفتار واقعی کارکنان را در مواجهه با ایمیل فیشینگ نمی‌سنجد، تصویر ناقصی از وضعیت امنیتی خود دارد.

ششم، تشویق مؤثرتر از جریمه است. تجربه نشان داده سیستم‌های تنبیهی صرف، کارکنان را به پنهان‌کاری تشویق می‌کند. اگر کسی بداند به خاطر کلیک روی یک لینک مشکوک جریمه می‌شود، احتمالاً آن را گزارش نمی‌کند. در مقابل، سیستمی که برای گزارش تهدیدات پاداش می‌دهد، فرهنگ شفافیت و همکاری ایجاد می‌کند. نسبت طلایی ۷۰ به ۳۰ (تشویق به جریمه) در بسیاری از سازمان‌های موفق جواب داده است.

هفتم، تیم واکنش سریع امنیتی ضمانت اجرایی نهایی است. وجود یک تیم تخصصی که ۲۴ ساعته آماده پاسخ به حوادث است، نه تنها خسارت حملات را کاهش می‌دهد، بلکه نقش آموزشی مهمی هم دارد. درس‌های گرفته شده از هر حادثه واقعی، بهترین محتوای آموزشی برای کارکنان است. همچنین

ارتباط ساده و مستقیم کارکنان با این تیم (مثلاً از طریق یک شماره تلفن داخلی ساده) باعث می‌شود گزارش‌دهی افزایش یابد.

پیاده‌سازی موفق اعتماد صفر در بانک‌ها نیازمند یک رویکرد جامع و چندلایه به آموزش است که در آن چهار سطح آموزشی (اصول، فنی، رفتاری و شبیه‌سازی) با پنج راهکار عملی (کارگاه، سیستم مدیریت یادگیری، ارزیابی، تشویق و جریمه، تیم واکنش سریع) ترکیب می‌شوند. این رویکرد باید با در نظر گرفتن چالش‌های خاص بانک‌ها (مقاومت فرهنگی، کمبود زمان، تفاوت سطح دانش و نیاز به آموزش مستمر) طراحی و اجرا شود.

جدول ۱. مدل پیشنهادی نهایی آموزش اعتماد صفر در بانک

فاز	مدت(ماه)	فعالیت‌های اصلی	خروجی مورد انتظار
فاز ۱: آماده‌سازی (Bada et al., ۲۰۱۵)	۱-۲	ارزیابی وضعیت موجود، سطح‌بندی کارکنان، انتخاب سیستم مدیریت یادگیری، تشکیل تیم واکنش سریع (McKinsey & Company, ۲۰۲۳)	نقشه راه آموزشی، تیم واکنش سریع مستقر (Deloitte, ۲۰۲۲)
فاز ۲: آموزش پایه (SANS Institute, ۲۰۲۲)	۳-۴	کارگاه‌های اصول اعتماد صفر برای همه، بارگذاری محتوای پایه در سیستم مدیریت یادگیری (Bada et al., ۲۰۱۵)	۹۰درصد کارکنان با مفاهیم پایه آشنا شوند (Ponemon Institute, ۲۰۲۲)
فاز ۳: آموزش فنی (McKinsey & Company, ۲۰۲۳)	۵-۶	دوره‌های تخصصی برای تیم فناوری اطلاعات، پیاده‌سازی MFA آزمایشی (Palo Alto Networks, ۲۰۲۳)	تیم فناوری اطلاعات آماده پیاده‌سازی فنی (Gartner, ۲۰۲۲)
فاز ۴: آموزش رفتاری (Deloitte, ۲۰۲۲)	۷-۸	کمپین‌های فرهنگی، سیستم تشویق و جریمه، گزارش‌دهی ناهنجاری‌ها (IBM Security, ۲۰۲۳)	کاهش ۳۰درصد تخلفات امنیتی (SANS Institute, ۲۰۲۲)
فاز ۵: شبیه‌سازی (Bada et al., ۲۰۱۵)	۹-۱۲	شبیه‌سازی فیشینگ، مهندسی اجتماعی، مانورهای تیم واکنش سریع (Ponemon Institute, ۲۰۲۲)	کاهش نرخ کلیک به زیر ۱۰درصد (McKinsey & Company, ۲۰۲۳)

فرهنگ امنیتی پایدار (McKinsey & Company, ۲۰۲۳)	آموزش مستمر، به‌روزرسانی محتوا، ارزیابی دوره‌ای (Bada et al., ۲۰۱۵)	۱۳ به بعد (SANS Institute, ۲۰۲۲)	فاز ۶: تثبیت و بهبود (Deloitte, ۲۰۲۲)

کاهش ۵۰درصد در تعداد حوادث امنیتی ناشی از خطای انسانی در سال اول
افزایش ۸۰درصد در تعداد گزارش‌های دریافتی از کارکنان
کاهش نرخ کلیک روی ایمیل‌های فیشینگ آزمایشی از میانگین ۳۰درصد به زیر ۵درصد
افزایش میانگین نمره آزمون‌های دوره‌ای از ۶۰درصد به بالای ۸۵درصد
کاهش میانگین زمان پاسخ به حوادث از ۴ ساعت به ۳۰ دقیقه

امنیت سایبری در بانک‌ها یک مقصد نیست، یک سفر است. هیچ بانکی به نقطه‌ای نمی‌رسد که بگوید «کاملاً امن هستم». تهدیدات مدام در حال تغییرند و کارکنان جدید همیشه به سازمان ملحق می‌شوند. بنابراین آموزش امنیتی باید به یک فرآیند همیشگی و بخشی از فرهنگ سازمان تبدیل شود، نه یک پروژه موقت.

بانکی که بتواند فرهنگ امنیتی را در همه سطوح نهادینه کند، نه تنها در برابر تهدیدات امروز مقاوم‌تر است، بلکه برای مقابله با تهدیدات فردا نیز آماده‌تر خواهد بود. سرمایه‌گذاری روی آموزش کارکنان، بهترین سرمایه‌گذاری امنیتی است که یک بانک می‌تواند انجام دهد. چون در نهایت، امن‌ترین فناوری‌ها هم توسط انسان‌ها استفاده می‌شوند و ضعیف‌ترین حلقه زنجیره امنیت، همیشه انسان است. اما با آموزش درست، همین انسان می‌تواند قوی‌ترین حلقه باشد.

پرسنل بانک دیگر صرفاً مصرف‌کننده سیستم‌های امنیتی نیستند، بلکه بخش جدایی‌ناپذیر از زنجیره امنیت محسوب می‌شوند. یک کارمند آموزش‌دیده و آگاه می‌تواند از پیچیده‌ترین حملات سایبری جلوگیری کند، در حالی که یک کارمند ناآگاه می‌تواند قوی‌ترین دیوار آتش را بی‌اثر کند. بنابراین، سرمایه‌گذاری بر روی آموزش و توانمندسازی پرسنل بانک، نه یک هزینه، بلکه یک سرمایه‌گذاری ضروری برای امنیت سازمان است.

آموزش مؤثر برای اعتماد صفر یک رویداد یکباره نیست، بلکه یک فرآیند مستمر است. ترکیب آموزش نظری (اصول)، فنی (ابزارها)، رفتاری (فرهنگ) و عملی (شبیه‌سازی) تضمین می‌کند که کارکنان بانک نه تنها مفاهیم را درک کنند، بلکه در عمل نیز رفتار امنیتی صحیح داشته باشند. سرمایه‌گذاری در این آموزش‌ها، بازگشت سرمایه قابل توجهی در کاهش حوادث امنیتی و هزینه‌های ناشی از نقض داده خواهد داشت.

چالش‌های آموزش در بانک‌ها واقعی و جدی هستند، اما غیرقابل حل نیستند. کلید موفقیت در سه چیز است:

واقع‌بینی: پذیرش اینکه همه کارکنان یکسان نیستند و یک راهکار برای همه جواب نمی‌دهد

انعطاف‌پذیری: طراحی آموزش متناسب با محدودیت‌های زمانی و بودجه‌ای

تداوم: تبدیل آموزش به یک فرآیند همیشگی، نه یک رویداد یکباره.

بانکی که بتواند این چالش‌ها را مدیریت کند، نه تنها اعتماد صفر را موفق‌تر پیاده می‌کند، بلکه فرهنگ امنیتی پایداری ایجاد می‌کند که در بلندمدت از سازمان محافظت خواهد کرد.

منابع فارسی

احمدی، ح.، و محمدی، ن. (۱۴۰۰). ارزیابی فرهنگ امنیت اطلاعات در بانک‌های دولتی جمهوری اسلامی ایران. مجله مهندسی و مدیریت کیفیت، ۳۳(۱)، ۸۹–۱۱۰.

بانک مرکزی جمهوری ا سلامی ایران. (۱۴۰۰). د ستورالعمل جامع حفاظت از اطلاعات و امنیت سایبری در مؤسسات اعتباری.

رضایی، م.، و کریمی، س. ا. (۱۳۹۹). بررسی آسیب‌پذیری‌های امنیتی در بانکداری الکترونیک ایران و راهکارهای مقابله با آن. فصلنامه امنیت اطلاعات و فناوری، ۱۴(۲)، ۶۷–۸۸.

محمدی‌نژاد، ع. ا. (۱۴۰۱). ارائه مدل بومی سازی شده اعتماد صفر برای صنعت بانکداری ایران با تأکید بر نقش نیروی انسانی [پایان‌نامه کارشناسی ارشد، دانشگاه تهران].

نوروزی، ف.، و صادقی، ر. (۱۴۰۲). تحلیل آمادگی بانک‌های خصوصی ایران برای پیاده‌سازی معماری اعتماد صفر. مجموعه مقالات کنفرانس ملی امنیت سایبری و فناوری اطلاعات.

منابع انگلیسی

Alshaikh, M., Alshamrani, A., & Alghamdi, A. (2021). Information security awareness in the banking sector: A comparative study. Journal of Cybersecurity and Privacy, 1(2), 45–60.

Bada, M., Sasse, A. K., & Belchior, G. (2015). An updated security awareness framework: A holistic approach to people-centric security. In Proceedings of the 10th International Conference on Cyber Warfare and Security.

Chokshi, N. (2019). Zero trust: The new security paradigm for financial institutions. Journal of Financial Crime, 26(3), 789–802.

Hassan, R., & Al-Muhtadi, J. (2022). Challenges of implementing zero trust in legacy banking systems. IEEE Transactions on Dependable and Secure Computing.

Kindervag, J. (2010). Build a security network you can trust. Forrester Research.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Deloitte. (2022). Zero trust in banking: Beyond technology. Deloitte Insights.

European Union Agency for Cybersecurity. (2023). Cybersecurity skills shortage in the EU financial sector.

Gartner. (2022). Market guide for zero trust technologies.

IBM Security. (2023). Cost of a data breach report 2023.

KPMG. (2023). Zero trust readiness in Middle East banks.

McKinsey & Company. (2023). The human side of zero trust: Why culture matters.

Palo Alto Networks. (2023). State of zero trust report 2023.

Ponemon Institute. (2022). The human factor in data breaches: A study of financial services.

SANS Institute. (2022). Security awareness training: What works, what does not.

Verizon. (2023). 2023 data breach investigations report.

Ward, R., & Beyer, B. (2014). BeyondCorp: A new approach to enterprise security. ;login:, 39(6), 6–11.

The Role of Bank Employee Training in the Successful Implementation of Zero Trust Architecture for Protecting Sensitive Data

[1]Bahram Ghasemi

Abstract

Introduction and Objective: With the digitalization of banking services, the banking industry has faced unprecedented cybersecurity threats. This study aims to examine and explain the role of bank employee training in the successful implementation of Zero Trust Architecture for protecting customers' sensitive data.

Research Methodology: This qualitative study was conducted using a systematic review and content analysis approach. The reviewed sources included credible scientific articles, reports published by international cybersecurity institutions, and domestic studies related to the Iranian banking sector.

Findings: Bank employee training is essential at four levels: basic training on Zero Trust principles for all employees; technical training, including multi-factor authentication and access management, for information technology teams; behavioral training, including security culture development and incident reporting, for all personnel; and attack simulation exercises, such as phishing and social engineering simulations, for practical assessment. The main challenges include cultural resistance, limited time and resources, differences in employees' levels of technical knowledge, and the need for continuous training. Practical solutions include organizing periodic workshops, using learning management systems, conducting regular evaluations and examinations, implementing an intelligent reward and penalty system, and establishing a rapid cybersecurity response team.

Conclusion: Successful Zero Trust implementation in banks requires continuous, multilayered employee training. The proposed six-phase model can strengthen security culture and reduce human error.

Keywords: Zero Trust, Bank Employees, Sensitive Data Protection, Security Architecture, Human Error

[1] - Software Engineering Expert, Banker, Qarz Al-Hosaneh Mehr Bank of Iran, Asaluyeh
B.ghasemi.it@gmail.com