St.Galler Kantonalbank AG und Swisscom realisieren mit Mobile ID Sicherheit und Benutzerfreundlichkeit auf neuem Niveau

Die St.Galler Kantonalbank AG (SGKB) suchte nach einer neuen Lösung, um den Zugriff auf die bankeigenen Anwendungen von unterwegs und aus dem Ausland besser absichern und kontrollieren zu können. Mit Swisscom etablierte die SGKB ein „Bring-Your-Own-Device"-Konzept für Mitarbeiter und Externe und vereinigte Benutzerfreundlichkeit mit einem hohen Sicherheitsniveau, das die strengen Anforderungen im Bankwesen erfüllt – und das bei geringeren Kosten und weniger Administrationsaufwand.

Als führendes Ostschweizer Finanzinstitut bietet die St.Galler Kantonalbank (SGKB) seit über 150 Jahren umfassende Finanzdienstleistungen für Privat- und Geschäftskunden. Insgesamt beschäftigt sie 1.200 Mitarbeiter am Hauptsitz St. Gallen und in den 38 Niederlassungen. Von diesen müssen etwa 300 Bankmitarbeiter sowie etwa 100 externe Mitarbeiter regelmässig ausserhalb des Büros auf die Anwendungen der Bank zugreifen. Dazu gehören Grenzgänger in Österreich und Deutschland sowie Systemadministratoren, die teilweise aus dem Ausland Zugriff auf Anwendungen benötigen.

Sicherheit auf Kosten der Benutzerfreundlichkeit

Guido Kölliker ist seit 1. Juli 2017 Chief Information Security Officer (CISO) bei der SGKB und in dieser Rolle für die Informationssicherheit der Bank verantwortlich. Eine der ersten Herausforderungen als CISO war die Verbesserung der Sicherheit bei der 2-Faktor-Authentifizierung des Remote-Zugriffs sowie eine stärkere Kontrolle der regionalen Zugriffe aus dem Ausland. Mitarbeiter, die sich von unterwegs einloggen wollten, taten dies bis dahin mit einem RSA-Token oder SMS als zweiten Faktor neben dem Passwort. Der physikalische Token generierte einen sechsstelligen Sicherheitscode, den der Nutzer eingeben musste, um sich anzumelden. Gleiches galt für die SMS, die einen vierstelligen Code generierte.

Der RSA-Token war allerdings aus mehreren Gründen sowohl bei den Verantwortlichen als auch den Mitarbeitern unbeliebt. Zum einen bedeutete er ein zusätzliches Device, das Mitarbeiter zu jeder Zeit mit sich führen mussten, um Zugriff auf Anwendungen zu haben. Zum anderen war die IP-basierte Geo-Fencing-Funktion durch VPNs einfach zu umgehen und bot so alleine nicht den nötigen Grad an Sicherheit für den Zugriff aus dem Ausland. Daher wurde als Alternative die Authentifizierung per SMS als zweiten Faktor eingesetzt, um den Token abzulösen und die Privatgeräte (Smartphones) der Mitarbeiter stärker mit einzubeziehen.

„Sobald ein Mitarbeiter seinen RSA-Token zuhause vergass, konnte er nicht arbeiten", erinnert sich Kölliker. „Deshalb war ich auf der Suche nach einer Lösung, die das Smartphone der Mitarbeiter mit einbezog. Das private Smartphone packt man schliesslich immer mit ein. Durch die SMS etablierten wir zwar die Smartphones der Mitarbeiter als zweiten Faktor, allerdings bot diese Methode nicht den gewünschten Sicherheitsgrad, da sie erwiesenermassen in der Vergangenheit bereits ausgehebelt werden konnte."

Gesucht: Sicherheit, Usability und Kontrolle

Die neue Lösung musste also gleichermassen einen hohen Sicherheitsgrad, Nutzerfreundlichkeit und eine stärkere Kontrolle über die Auslandszugriffe bieten. Die Suche nach entsprechender Technologie gestaltete sich zunächst schwierig. Eine App-basierte Lösung, die Hintergrundgeräusche zur Verifizierung nutzte, schied aus, da die benötigten Mikrofone am privaten Computer des Nutzers zusätzliche Kosten verursacht hätten. Device-basierte Lösungen, die beispielsweise eine Smartcard als zweiten Faktor nutzten, waren ebenfalls

swisscom

ungeeignet, da sie die gleichen Probleme wie der RSA-Token mit sich brachten und einen hohen Administrationsaufwand bedeuteten.

Bei der Suche kam Kölliker auch ins Gespräch mit Swisscom, mit der die SGKB bereits seit Jahren erfolgreich zusammenarbeitet. Zum einen betreibt Swisscom die ICT-Infrastruktur und die Arbeitsplätze der SGKB, zum anderen wurden die Workplaces der Mitarbeiter zu diesem Zeitpunkt auf Windows 10 migriert und erneuert derzeit die Infrastruktur durch Desktops, Laptops und Thin Clients. Bereits seit längerem gab es Gespräche über Möglichkeiten, eine starke 2-Faktor-Authentifizierung zusammen mit der Erneuerung der Workplaces zu realisieren. Aufgrund von terminlichen Abhängigkeiten wurde dies jedoch auf einen späteren Zeitpunkt verschoben.

Mit Mobile ID hatte die Swisscom eine Lösung im Angebot, die sämtliche Anforderungen der SGKB erfüllte. Diese ermöglicht die In-house-Kontrolle des Remote-Zugriffs, indem Zugriffsberechtigungen aus verschiedenen Ländern per White-/Blacklisting von den eigenen Mitarbeitern auch temporär erteilt und entzogen werden können. Ein wesentlicher Fortschritt ist zudem, dass die Verifizierung nicht IP-basiert, sondern über das Mobilfunknetz erfolgt. „Hier einen anderen Standort vortäuschen zu wollen, würde ein hohes Mass an krimineller Energie voraussetzen, da die Lokation anhand des Funkturms und dem Provider des jeweiligen Landes bestimmt wird. Das ist wesentlich schwerer zu umgehen," äussert sich Guido Kölliker zufrieden.

Des Weiteren funktioniert Mobile ID unabhängig vom Endgerät und ist ohne zusätzliche App auf den Smartphones der Mitarbeiter nutzbar, was den Kosten- und Administrationsaufwand stark verringert. Beim Login gibt der Nutzer seine Daten ein, erhält anschliessend eine Benachrichtigung auf das Smartphone (egal, ob ein- oder ausgeschaltet) und bestätigt die Anmeldung mit der Eingabe eines sechsstelligem PINs, der vorab individuell festgelegt und jederzeit geändert werden kann.

Adaption auf die individuellen Anforderungen

Die Umstellung auf Mobile ID begann im September 2018 und verlief ohne Probleme, obwohl sich im Rahmen der Implementierung noch einige Hindernisse ergaben.

„Die Anforderungen an die Lösung waren insofern einzigartig, da die SGKB die Administration des Geofencing selbst betreiben wollte, die Infrastruktur aber auf der Citrix-Plattform von Swisscom lief. So eine Situation hatten wir in der Vergangenheit noch nicht," kommentiert Mario Gurschler, Product Manager Mobile ID] bei Swisscom. „Wir mussten sicherstellen, dass Mobile ID kompatibel mit der Citrix-Umgebung war und die Änderungen aus dem Active Directory im Backend von Mobile ID reibungslos übernommen werden. Diese Änderungen haben wir spontan einarbeiten müssen, was uns aber im Rahmen des Zeitplans sehr gut gelang. Am Ende konnte das Projekt wie geplant abgeschlossen werden.

Im Rahmen der Umstellung erhielten die 300 Mitarbeiter und 100 Externe, die von unterwegs auf die Banking-Applikation zugreifen müssen, neue und Mobile-ID-fähige SIM-Karten für ihre privaten Geräte, die mit ihrem Nutzerkonto bei der Bank verknüpft wurden. Diejenigen, die nicht bereits Kunden von Swisscom oder Partner-Providern der Mobile ID waren, erhielten eine Extra-SIM-Karte für die Anmeldung.

Seit April 2019 nutzen die Mitarbeiter für den Login von unterwegs nun exklusiv Mobile ID als zweiten Faktor. Guido Kölliker äussert sich sehr zufrieden über die Umstellung: „Mir war es besonders wichtig, dass die Kontrolle der Auslandszugriffe in unserer Hand liegt und auch die Mitarbeiter den Weg mitgehen, ansonsten hätte es nicht funktioniert. Deshalb bin ich sehr froh, dass wir eine Lösung gefunden haben, die von den Mitarbeitern sehr positiv aufgenommen wurde und gleichzeitig die im Bankumfeld nötige Sicherheit bietet."

Nur der erste Schritt

Nach der erfolgreichen Einführung von Mobile ID für die Remote-Mitarbeiter möchte Guido Kölliker diese Form der 2-Faktor-Authentifizierung bis zum Ende des Jahres 2019 flächendeckend für alle Mitarbeiter auch im Büro einführen, um die allgemeine Sicherheit in der Bank zu verstärken. Unterstützung erhält er dabei auch intern von der HR-Abteilung, die private Smartphones ebenfalls stärker in den Arbeitsalltag integrieren möchte, um so beispielsweise die Arbeitszeit erfassen zu können. Er zieht daher ein durchweg positives Zwischenfazit:

„Mit Mobile ID haben wir bewiesen, dass „Bring-Your-Own-Device"-Konzepte auch im Banken-Umfeld sehr gut funktionieren können, ohne zulasten der Sicherheit oder von Komforteinbussen zu gehen. Ausserdem haben wir einen wichtigen Grundstein für den weiteren digitalen Fortschritt gelegt und können perspektivisch beispielsweise qualifizierte E-Signaturen oder Willensbekundungen bequem über das Smartphone abwickeln, was wiederum angenehmer für die Kunden wird."

Guido Kölliker
CISO SGKB