DOPPELT gesichert

IT-Systeme und Daten vor unberechtigten Zugriffen und Missbrauch schützen: eine Kernanforderung des sicheren IT-Betriebes. Die Leistung »Starke Authentisierung« unterstützt Sparkassen seit gut einem Jahr hierbei und ergänzt das »Single Sign-On« – Produktangebot.

hält BESSER

Sensible Bereiche schützen, nur berechtigten Personen den Zutritt gewähren und IT-Systeme absichern: Institute müssen ihre Geschäfts- und Kundendaten vor Missbrauch schützen. Aus diesem Grund werden immer mehr Sicherheitskonzepte aufgelegt und deren Umsetzung auch gesetzlich eingefordert. Doch in der Praxis sieht es oft anders aus: Wer kennt sie nicht, die Kennwortzettel unter den Tastaturen? Mitarbeiter müssen sich mitunter an einer Vielzahl von IT-Systemen anmelden. Dafür verwenden sie entweder einfache, aber unsichere Kennwörter, die bekannten Spickzettel kommen zum Einsatz oder Passwörter werden vergessen und müssen dann manuell zurückgesetzt werden.

Abhilfe schafft hier das etablierte, so genannte »Single Sign-On«-Verfahren: Nach erfolgreicher Anmeldung am PC durch den Mitarbeiter übernimmt das Produkt Single Sign-On (SSO) der Finanz Informatik die automatisierte Anmeldung an den zuvor definierten und in SSO integrierten Anwendungen und Diensten. Diese reichen von Windows- über Web- bis hin zu 3270-Anwendungen. SSO steht seit Anfang 2009 den Instituten zur Verfügung. Derzeit nutzen knapp 90 Sparkassen die Leistung mit über 44.000 Usern.

Mit Single Sign-On werden die Anmeldeprozeduren für den Mitarbeiter auf ein Minimum reduziert – das spart viel Zeit und Nerven. Zusätzlich lässt sich auch noch die Sicherheit der Passwörter erhöhen: SSO kann die Kennwörter automatisch generieren und dabei komplexe Passwortvorgaben verwenden. Diese verschlüsselten, persönlichen Anmeldedaten werden zentral gespeichert und sind nur für den Mitarbeiter einsehbar – er selbst merkt sich nur sein »Start-Passwort« für die PC-Anmeldung. Passwort-Rücksetzungen oder Freischaltungen gesperrter User reduzieren sich erheblich und entlasten die Administratoren oder den User-Help-Desk.

Diese Vorteile waren auch ein entscheidender Grund für die Sparkasse Gladbeck, das Single-Sign-On-Verfahren Anfang 2011 einzuführen: Das Institut hatte für das Zurücksetzen von Passwörtern jährliche Kosten von rund 31.000 Euro errechnet. Hierbei waren durchschnittlich fünf Aktionen pro Tag durch die zwei IT-Administratoren als Grundlage herangezogen worden. Ehrgeiziges Ziel der Gladbecker: Eine Kostenreduzierung auf nur 10 Prozent der Summe. Dass das nicht zu hoch gegriffen war, zeigt die Praxis: Nach nur 6-monatigem Einsatz haben die Gladbecker bereits die ursprünglichen Kosten um 80 Prozent gesenkt.

Doch bevor SSO in Gladbeck zum Einsatz kommen konnte, verlangte die Innenrevision, den Domänenzugang und damit das vereinfachte Anmeldeverfahren durch eine »starke Authentisierung« abzusichern. Das bedeutet, dass der Systemzugang für sicherheitskritische Anwendungen wie zum Beispiel OSPlus-Portal durch die Kombination von zwei der nachfolgenden drei Faktoren geschützt wird:

1. Besitz: Der Benutzer muss im Besitz eines eindeutigen Identifikationsmerkmales sein, z. B. einer Smartcard.
2. Wissen: Er verfügt über das Wissen eines nur ihm bekannten Zugangscodes, beispielsweise Kennwort oder PIN.
3. Sein: Er identifiziert sich durch ein biometrisches Merkmal, z. B. Fingerabdruck.

Die starke Authentisierung wird deshalb auch Zwei- oder Mehrfaktoren-Authentisierung genannt und ist im Konzept »K102« des Sicheren IT-Betriebes beschrieben. Auch Verbandsprüfungsstellen und IT-Revisionen fordern vermehrt die starke Authentisierung speziell beim Einsatz von Single Sign-On. Die Finanz Informatik bietet im Rahmen ihrer IT-Dienstleistungen hierzu zwei Möglichkeiten: Starke Authentisierung mit Smartcard plus PIN oder durch Fingerabdruck plus Kennwort. >>

Sparkasse Dachau
Sparkassenplatz 1 · 85221 Dachau · Geschäftsvolumen: 2,4 Mrd. Euro
www.sparkasse-dachau.de

Keine Spickzettel mehr

>> Die Sparkasse Gladbeck entschied sich für die kartenbasierte Lösung. André Smeets, Bereichsleiter Organisation und Marktservice, berichtet: »Durch die geplante Modernisierung unserer Hauptstelle letztes Jahr bot sich die Einführung eines neuen Zutritts- und Zeiterfassungssystems an. Dadurch ergab sich die Möglichkeit, mehrere Funktionen auf ein Kartenmedium zu konzentrieren. Dies konnten wir ohne eigene Server in unseren Räumen umsetzen«, so der Bereichsleiter zufrieden. »Der zentrale Betrieb der Single-Sign-On- und Kartenmanagement-Plattform im Hause der Finanz Informatik fügt sich nahtlos in unsere strategische Ausrichtung ein.« Denn 93 Prozent der knapp 200 Arbeitsplätze in Gladbeck basieren bereits auf Thin-Client-Technologie; die Finanz Informatik betreibt und verantwortet die Server. »Mit Unterstützung der FI konnten wir schon in der Vergangenheit die Administrationsaufwände deutlich reduzieren«, bilanziert Carsten Abe, Mitarbeiter Organisation und Marktservice und als Projektleiter für die Einführung tätig. »Diese positiven Effekte sehen wir auch beim Einsatz von SSO und Starker Authentisierung. Die Investitionen haben sich nach knapp einem Jahr bereits amortisiert!«

Zwei aus drei: *Soviel Sicherheit muss sein bei der »Starken Authentisierung«. Deshalb benötigen Mitarbeiter zusätzlich zur Smartcard eine persönliche PIN oder zusätzlich zum Fingerabdruck ein persönliches Kennwort.*

Walter Schmidt,
Mitarbeiter Organisation,
Sparkasse Dachau

An der Pilotierung der Starken Authentisierung hatten die Gladbecker Ende 2010 teilgenommen, ebenso die Sparkasse Dachau. Die bayerische Sparkasse entschied sich bei der Starken Authentisierung für die zweite Variante, der Biometrie-Lösung. Denn »kein Benutzer kann seinen Finger zu Hause vergessen – eine Smartcard oder einen Token aber sehr wohl!«, begründet Walter Schmidt, Organisationsmitarbeiter und Projektleiter, die Entscheidung.

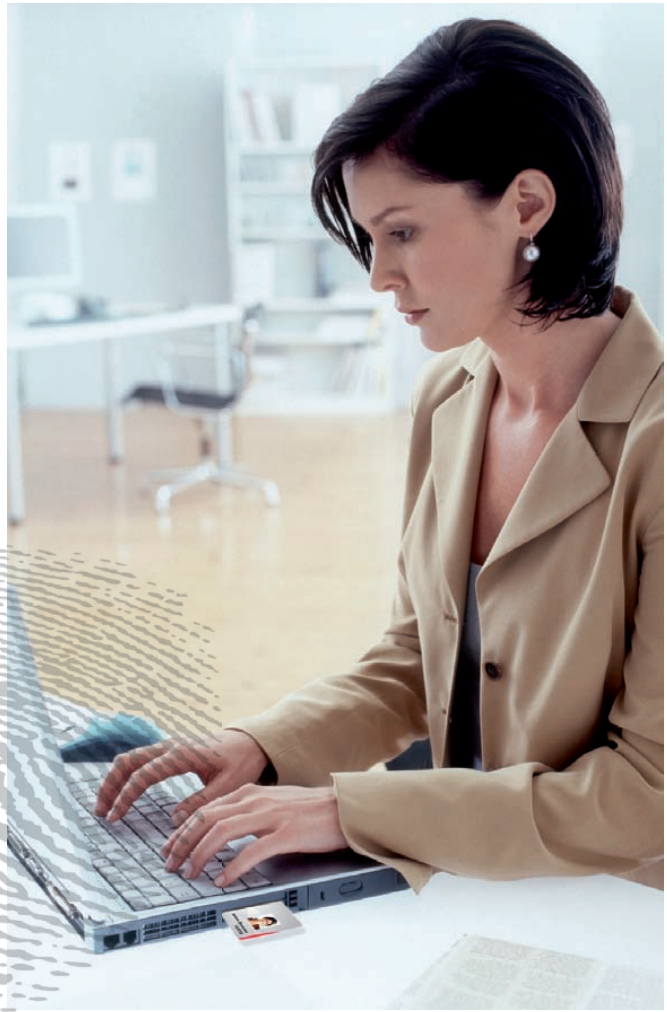
Auszug aus dem Leistungskatalog der »Starken Authentisierung – Smartcard« und der »Starken Authentisierung – Biometrie«

- *sowohl für IT-konsolidierte Sparkassen als auch für nicht-IT-konsolidierte Institute*
- *Lizenzierung und Software-Wartung*
- *Integration in die FI-Infrastruktur inkl. Fehlerbehebung und Support*
- *Integration in Release- und Update-Prozesse*
- *Hardware-Validierung durch die Finanz Informatik*
- *gesicherte Einkaufskonditionen für Hardware und Smartcards durch FI-Rahmenverträge*
- *Bereitstellung der erforderlichen digitalen Zertifikate über zentrale Anbindung an das Trustcenter des DSV (für Smartcard-Lösung)*
- *zentraler Betrieb der Kartenmanagement-Infrastruktur (für Smartcard-Lösung)*
- *mehr im OSPlus-Produktkatalog unter »IT-Dienstleistungen // Single Sign-On«*

Die »Starke Authentisierung – Biometrie« enthält die Leistung »Biometrie – Basiskomponenten«. Hierbei handelt es sich um die technische Plattform samt Lizenzen für den biometrischen Zugang zur Plus-Lösung in OSPlus-Kasse. Sparkassen, die die Plus-Lösung in OSPlus-Kasse bereits separat nutzen, können mit minimalem Aufwand auf die Starke Authentisierung upgraden und so die Sicherheit um einen weiteren Schritt erhöhen.

Biometrie liegt auf der Hand

Biometrische Merkmale wie Fingerabdrücke stellen ein für jede Person einzigartiges Erkennungszeichen dar, das nicht verlorengehen und auch nicht von anderen Personen benutzt oder an diese weitergegeben werden kann. Das Handling der Biometrie-Lösung ist denkbar einfach: Die Sparkasse Dachau stattete zunächst alle Arbeitsplätze mit einem »Fingerprint-Reader« aus. Gleichzeitig wurden von jedem User vier Fingerabdrücke eingescannt und in Verbindung mit der persönlichen Benutzer-ID zentral bei der Finanz Informatik verschlüsselt hinterlegt. Dabei werden nur biometrische Auffälligkeiten des Fingerabdrucks gespeichert, um zu verhindern, dass daraus wieder ein Fingerabdruck rekonstruiert werden könnte.



Carsten Abe,
Mitarbeiter Organisation
und Marktservice,
Sparkasse Gladbeck

Die Anmeldung am Arbeitsplatz erfolgt durch Eingabe von User-ID und Domänenkennwort sowie durch das Einlesen des Fingerabdrucks über den Fingerprint-Reader. Ein schnelles Aktivieren des Bildschirmschoners geht ebenfalls durch einfaches Auflegen eines Fingers auf den Reader.

Die Einführung der Starken Authentisierung mittels Biometrie wurde in Dachau jüngst im Mai dieses Jahres abgeschlossen, sehr zur Zufriedenheit der Mitarbeiter. »Wir wollten das tägliche Arbeiten so einfach wie möglich machen«, erläutert Walter Schmidt. »Die vereinfachten Anmeldevorgänge mit Single Sign-On, das wir bereits seit Anfang 2009 nutzen, können wir nun mit der starken Authentisierung absichern – Komfort und Sicherheit ergänzen sich hierbei optimal«, freut sich der Projektleiter von der Sparkasse Dachau.

»Eine hohe Akzeptanz der Mitarbeiter für die geschaffene Lösung« konnte auch in Gladbeck erzielt werden, wie Carsten Abe berichtet. »Wir haben unsere speziellen Anforderungen für die starke Authentisierung per Smartcard mit dem Kartenlieferanten DSV und der Finanz Informatik abgestimmt. Die auf der Karte enthaltene Funktechnologie sowie der Chip sichern unseren Mitarbeitern den Zutritt, die Zeiterfassung sowie einen besonders gesicherten Systemzugang«, so der Projektleiter über die nutzerfreundliche Lösung. >>

Sparkasse Gladbeck
Friedrich-Ebert-Straße 2 · 45964 Gladbeck · Geschäftsvolumen: 0,8 Mrd. Euro
www.sparkasse-gladbeck.de

Gut vorbereitet

>> Um den Einsatz vorzubereiten, erhielten die IT-Administratoren die entsprechende Hardware zur Kartenerstellung. Für das Zutrittsmodul bespielten sie die Smartcards mit Karten- und Firmennummer zur eindeutigen Identifikation. Ferner statteten sie die Karten mit einem digitalen Zertifikat aus. Dieses enthält einen öffentlichen Schlüssel, der zum Besitzer des Zertifikats gehört sowie einen weiteren, geheimen Schlüssel, der weder ausgelesen noch manipuliert werden kann. Die im Hintergrund ablaufenden automatisierten Prüfvorgänge beim Einstecken der Smartcard in den Reader sind sehr komplex – und sicher.

Für die Mehrfaktoren-Authentisierung kommt zur Smartcard noch die persönliche Geheimzahl hinzu. Um eine Funktionstrennung zwischen PIN- und Kartenerstellung sicherzustellen, erhielt die Personalabteilung die Aufgabe, PIN-Briefe anzufertigen.

Fast alle Arbeitsplätze in der Sparkasse Gladbeck wurden mit Tastaturen mit integriertem Kartenleser ausgerüstet oder mit Standkartenlesern für spezielle Arbeitsbereiche, wie AKT-Steuerplätze. Vorteil der kartenbasierten Lösung: Verlässt der Mitarbeiter seinen Arbeitsplatz, muss er seine Smartcard für den Zutritt z. B. zu den Verwaltungsbüros oder zur Kundenhalle mitnehmen. Dadurch findet eine konsequente Sperrung der Arbeitsplätze statt.

Die Vorbereitungen haben sich ausgezahlt: »Einmal installiert und Abläufe definiert, beschränken sich die Tätigkeiten im laufenden Geschäftsbetrieb auf die PIN- und Kartenerstellung«, fasst Carsten Abe zusammen. Und in der Sparkasse Dachau »haben wir durch den Einsatz von Single Sign-On und der Starken Authentisierung einen entscheidenden Schritt in Richtung Datensicherheit im Unternehmen Sparkasse erreicht«, so Walter Schmidt. »Die Revisoren werden uns damit sicher Recht geben.«

Gut aufgestellt

Single Sign-On und Starke Authentisierung ergänzen sich optimal, können jedoch auch unabhängig voneinander genutzt werden. Entscheidet sich ein Institut für beide Lösungen, empfiehlt sich die zeitversetzte Einführung. Die Infrastrukturberater der Finanz Informatik unterstützen hierbei mit Konzepten und stehen den Sparkassen beratend zur Seite. Dies weiß man auch in Gladbeck zu schätzen: »Neben dem gestiegenen Sicherheitsaspekt und den reduzierten Administrationsaufwänden haben wir mit den Einführungsprojekten von SSO und Starker Authentisierung die Weichen gestellt, um auch zukünftige Anforderungen der IT-Sicherheit zu erfüllen«, resümiert Carsten Abe.

Der »Sichere IT-Betrieb« *ist ein Produkt der Finanz Informatik in Zusammenarbeit mit dem SIZ und bietet mit Beschreibungen, Vorgehensweisen, Dienstleistungen und beispielhaften Ergebnissen eine umfassende Grundlage zum Aufbau eines IT-Sicherheitsmanagements auf strategischer sowie operationaler Ebene. Das Konzept K102 umfasst die Starke Authentisierung.*