heise Business Services

Ein eBook von

Powered by KEYIDENTITY WE SECURE IDENTITIES

MFA:

Unkomplizierter Rundumschutz für digitale Identitäten und Transaktionen

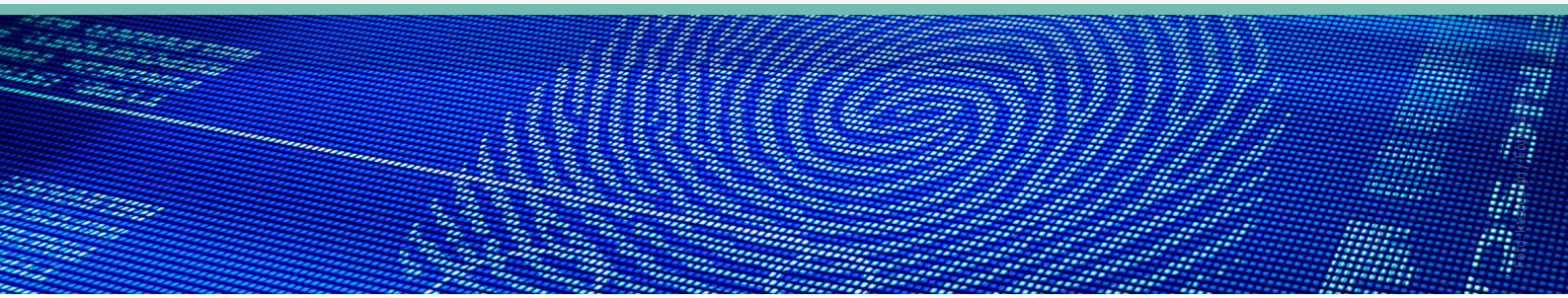
- Multi-Faktor-Authentifizierung – gestern und heute
- Token-Typen und deren Einsatz
- Mit MFA zu sicheren Applikationen

Inklusive

Whitepaper: 10 Schritte zur erfolgreichen Implementierung einer MFA-Lösung

Case Study: Zweiter Authentifizierungsfaktor schützt digitale Logins bei Scania

ktsdesign / Fotolia.de



Katharina Friedmann

Editorial

Komplex, unflexibel, fehleranfällig, schwer zu handhaben und zu implementieren – nach wie vor gibt es Vorbehalte gegen Multi-Faktor-Authentifizierung (MFA). Die Ursache dürfte in den Defiziten der frühen MFA-Systeme liegen. Doch hier hat sich in den vergangenen zwei Jahrzehnten viel getan.

Vor allem der Siegeszug des Cloud Computing und die flächendeckende Verbreitung von Mobilgeräten haben die MFA-Entwicklung vorangetrieben und auch deren Einsatzmöglichkeiten erheblich erweitert. So fungiert das Smartphone mittlerweile als vielseitig einsetzbarer Token-Ersatz – und zusätzliche Hardware-Dongles sind angesichts auf den mobilen Endgeräten befindlicher Authentifizierungs-Apps überflüssig geworden. Auch die gefürchtete MFA-Implementierung in eigene Apps oder auch die firmeneigene Infrastruktur ist heute kein Hindernis mehr und lässt sich längst ohne großen Aufwand umsetzen.

In diesem eBook erfahren Sie...

... wie sich MFA in den vergangenen Jahrzehnten weiterentwickelt hat,
... welche Einsatzszenarien es mittlerweile gibt,
... welche Token-Typen sich dafür jeweils am besten eignen, und...
... wie Multi-Faktor-Authentifizierung Applikationen und Nutzer vor unautorisierten Zugriffen und kritischen Transaktionen bewahrt.

Ich wünsche Ihnen eine interessante Lektüre!

Katharina Friedmann
Manager Solutions & Services, Heise Medien

Heise Medien GmbH & Co.KG
Abt. Heise Business Services
Hans-Pinsel-Straße 10a
85540 Haar bei München

Registergericht:
Amtsgericht Hannover HRA 26709

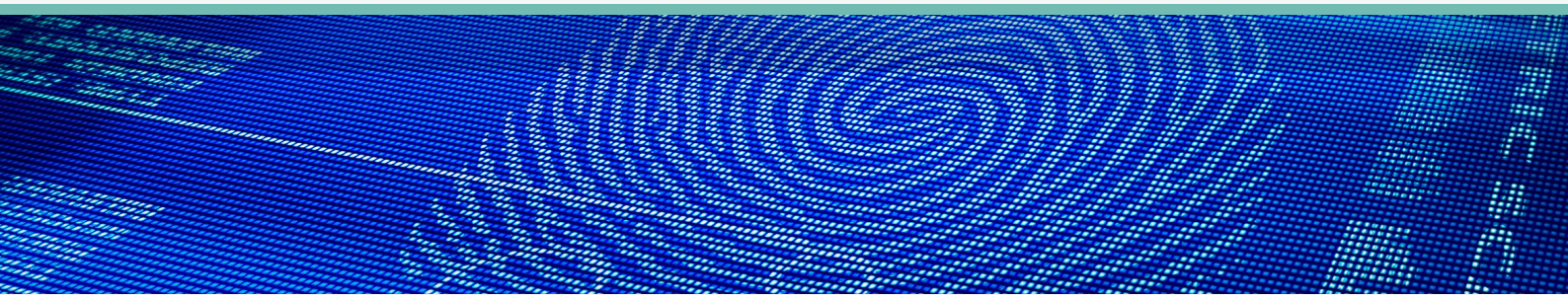
Persönlich haftende Gesellschafterin:
Heise Medien Geschäftsführung GmbH

Registergericht:
Amtsgericht Hannover, HRB 60405

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

Verantwortlich für den Inhalt:
Heise Business Services
Frank Klinkenberg, fkl@heise.de

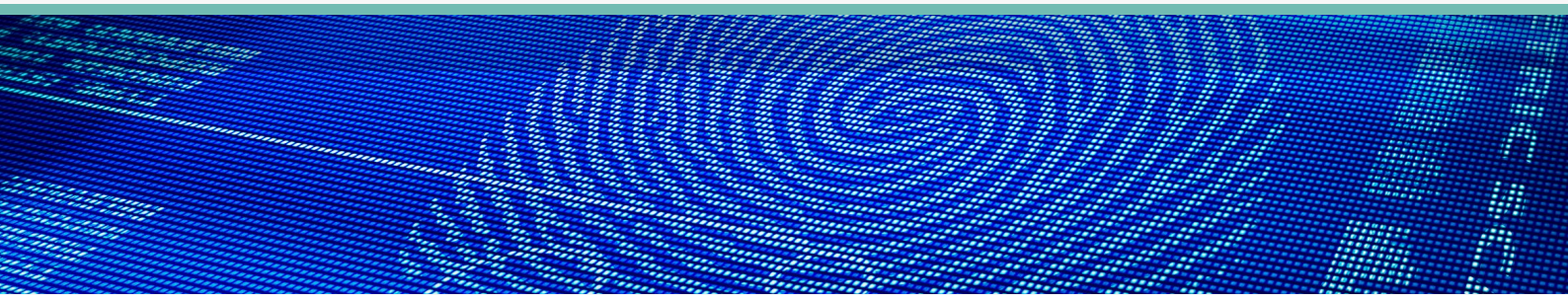
Haben Sie Fragen zu diesem eBook oder haben Sie Interesse an einer eigenen Produktion, dann schicken Sie bitte eine E-Mail mit dem Betreff **„HBS-eBook“** an hbs@heise.de



Inhalt

ÜBER DEN AUTOR

Dr. Thomas Hafen war über 15 Jahre als Redakteur, Moderator und Manager für verschiedene IT-Fachverlage tätig. Seine fachlichen Schwerpunkte liegen in den Bereichen Digitale Transformation, Cloud Computing und Advanced Analytics. Thomas Hafen lebt und arbeitet heute als freier Journalist und Moderator in München.

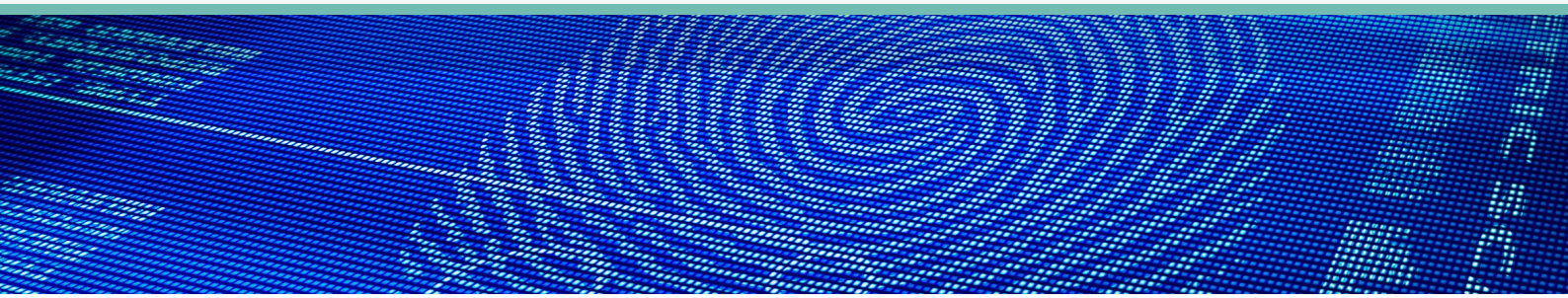


Multi-Faktor-Authentifizierung – gestern und heute

Foto: Yong Hian Lim / Fotolia.de

Multi-Faktor-Authentifizierung (MFA) gilt häufig immer noch als komplex, teuer und nicht gerade nutzerfreundlich. Das mag vor 20 Jahren auch richtig gewesen sein, als MFA mit der Nutzung fehleranfälliger, unflexibler und schlecht zu verwaltender Hardware-Token einherging. Heute jedoch können Anwender aus einer Vielzahl von Authentifizierungsmöglichkeiten wählen, die sich zudem auch noch schnell und unkompliziert implementieren lassen.

Sein, Wissen oder Besitz – das sind die drei Prinzipien, über die Authentifizierung und die damit verbundene Autorisierung funktionieren. Eine Person kann über ihre einzigartigen physischen Merkmale wie Stimme, Fingerabdruck oder Irismuster identifiziert werden, über ein geheimes Wissen, etwa ein Passwort oder eine PIN (Personal Identification Number), verfügen oder etwas besitzen, das sie zum Zugang berechtigt – einen Pass, eine Zugangskarte oder ein Token. Jeder dieser Faktoren für sich allein birgt Schwachstellen: Fingerabdrücke können kompromittiert, Passwörter ausspioniert oder erraten, Pässe und Zugangskarten gefälscht oder gestohlen werden. Es ist daher ein bewährtes und bekanntes Prinzip, mehrere dieser Faktoren zu kombinieren, um die Sicherheit zu erhöhen. Banken machen sich das schon seit vielen Jahrzehnten zunutze, indem sie ihre Kunden nur dann Geld abheben lassen, wenn diese etwas wissen, nämlich ihre PIN, und etwas besitzen: ihre Bankkarte.



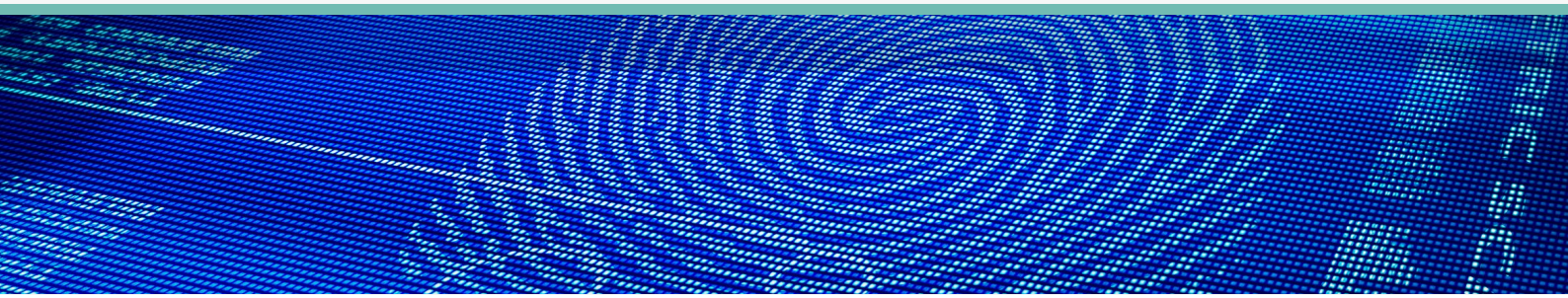
Die Anfänge der Multi-Faktor-Authentifizierung

Im Jahr 1977 entwickelten Ronald L. Rivest, Adi Shamir und Leonard M. Adleman am Massachusetts Institute of Technology (MIT) ein Verschlüsselungsverfahren, das die Kryptografie erheblich vereinfachte. Es beruht auf der Kombination eines öffentlichen mit einem privaten Schlüssel. Im Unterschied zu symmetrischen Verfahren, bei denen die Zahl geheim zu haltender Schlüssel mit steigender Zahl der Benutzer exponentiell zunimmt, muss bei asymmetrischen Verfahren jeder Anwender lediglich seinen eigenen Schlüssel geheim halten. Hinzu kommt, dass die symmetrische Verschlüsselung nur auf einem Passwort beruht, während bei Public-Key-Verfahren sowohl der private Schlüssel als auch das Passwort zum Öffnen des privaten Schlüssels benötigt werden.

Rivest, Shamir und Adleman gründeten 1982 die nach ihren Initialen benannte Firma RSA Security, die auf Basis des asymmetrischen Kryptografieverfahrens eine Zwei-Faktoren-Authentifizierung entwickelte. Ein Hardware-Token namens „SecurID" lieferte dazu alle 60 Sekunden ein neues Einmalpasswort, das der Anwender zusätzlich zu seinem Kennwort eingeben musste, um Zugang zu erhalten.

Der Einsatz eines zweiten Faktors bedeutete einen erheblichen Sicherheitsgewinn gegenüber der bloßen Anmeldung mit einem statischen Passwort. Die ersten Systeme hatten jedoch auch gravierende Nachteile: Sie waren komplex, aufwendig zu installieren und verursachten nicht unerhebliche Kosten. Neben der Serverinfrastruktur mussten Unternehmen eine Vielzahl von Hardwareschlüsseln erwerben. Diese funktionierten nur so lange, wie die integrierte Batterie Energie lieferte. Da ein Batteriewechsel nicht möglich war, ohne das Gerät zu zerstören, mussten folglich die Token regelmäßig ersetzt werden. Zudem machte die Synchronisation der Code-Generatoren mit dem zentralen Server häufig Schwierigkeiten: Liefen die Uhren in beiden Systemen nicht im Takt, schlug die Autorisierung fehl. Die kleinen Hardware-Token gingen außerdem leicht (und häufig auch unbemerkt) verloren – ein Sicherheitsrisiko, das die Vorteile der Zwei-Faktoren-Authentifizierung zumindest zum Teil wieder zunichtemachte.

Der von einem RSA-SecurID-Token alle 60 Sekunden neu erzeugte Einmal-Code wird als zweiter Faktor für die Authentifizierung verwendet. (Foto: Alexander Klink, CC BY 3.0)



Möglichkeiten moderner MFA-Systeme

Die großen IT-Trends der vergangenen Jahre wie die flächendeckende Verbreitung mobiler Endgeräte und der Siegeszug des Cloud Computing haben auch die Entwicklung und die Möglichkeiten der MFA massiv beschleunigt und erweitert. Smartphones haben sich als vielfältig einsetzbarer Token-Ersatz bewährt. Statt zusätzlich einen Hardware-Token mit sich zu führen, nutzt der Anwender einfach eine Authentifizierungs-App auf seinem Endgerät, das er ohnehin immer bei sich hat. Viele Smartphones sind heute schon mit Fingerabdruckscannern ausgestattet, was zusätzlich Sicherheit vor unautorisierten Zugriffen auf den Token bietet.

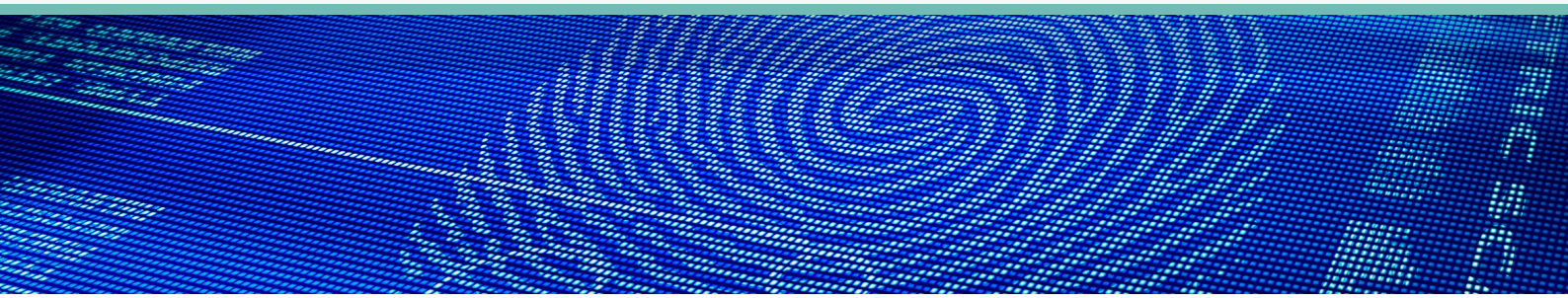
> Die MFA-Integration lässt sich mittlerweile in wenigen Schritten vornehmen.

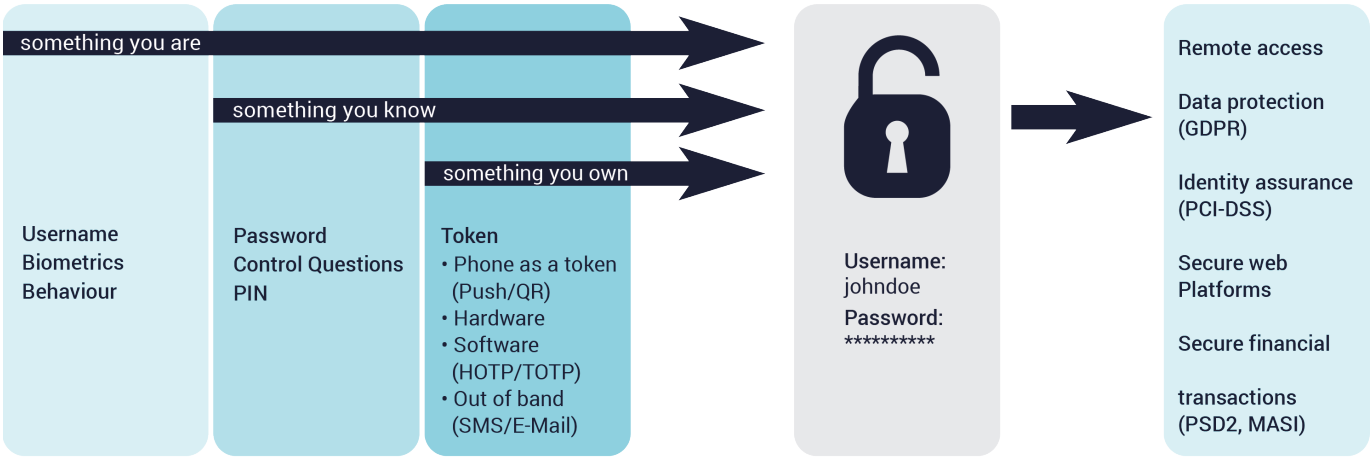
Die Integration von MFA in eigene Apps oder die firmeninterne Infrastruktur lässt sich heute über On-Premise-Lösungen oder Cloud-basierte Services in wenigen Schritten durchführen. Diese Plattformen bieten Schnittstellen in Form von APIs (Application Progamming Interface), über die Entwickler MFA-Funktionalitäten in ihre Applikationen integrieren können. Auch die Anbindung verschiedenster Hard- und Software-Token-Systeme ist möglich. Dank des modularen Aufbaus können Unternehmen nur diejenigen Bestandteile implementieren beziehungsweise mieten, die sie auch wirklich brauchen, während es ein skalierbares Design ermöglicht, schnell und flexibel auf Nachfrageveränderungen zu reagieren.

> Auf Nummer sicher: Um Manipulationen weitgehend auszuschließen, empfiehlt es sich, auf eine Open-Source-basierte MFA-Lösung zu setzen.

Moderne MFA-Systeme sind aber vor allem eines: anwenderfreundlich. Das gilt sowohl für die Integration und Verwaltung, die zum Teil vom Nutzer selbst erledigt werden kann, vor allem aber für die Verwendung der zusätzlichen Sicherheitsfaktoren. Statt beispielsweise umständlich die von einem Hardware-Token angezeigten Werte eintippen zu müssen, kann der Anwender direkt einen Push-Token akzeptieren; mit Voice-Token können auch blinde oder sehbehinderte Menschen MFA barrierefrei nutzen. Hier ist es besonders wichtig, möglichst viele unterschiedliche Authentifizierungsverfahren anbieten und so auf die unterschiedlichen Voraussetzungen, Kenntnisstände und Bedürfnisse der Anwender eingehen zu können.

Allerdings basieren auch heute noch viele Systeme auf proprietärer Software, deren Quellcode nicht öffentlich zugänglich ist, was aus zwei Gründen problematisch ist: Zum einen wird diese Software anders als Open-Source-Lösungen nicht von einer großen Entwickler-Community gepflegt und überprüft, Fehler und Schwachstellen werden so womöglich nicht schnell genug erkannt. Zum anderen geraten Sicherheitsprodukte immer wieder in den Verdacht, über eingebaute Hintertüren Geheimdiensten und anderen Regierungsorganisationen Zugang zu den sensiblen Daten der Kunden zu ermöglichen. Da der Code nicht geprüft werden kann, lassen sich solche Vorwürfe nicht restlos widerlegen. Es empfiehlt sich also, auf eine MFA-Lösung zu setzen, die auf Open-Source-Software basiert.





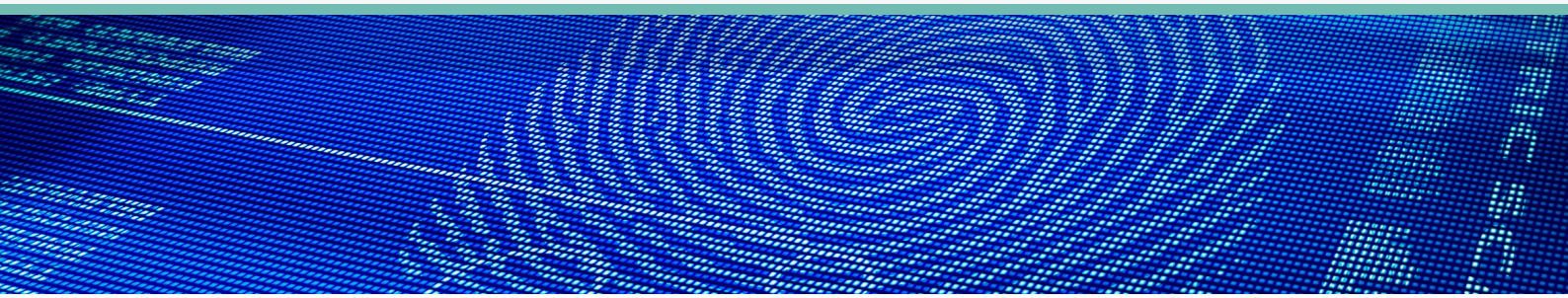
Multi-Faktor Authentifizierung:
Sein, Wissen, Besitz – auf diesen drei Prinzipien basiert MFA.

Einsatzszenarien für MFA

Längst wird MFA nicht mehr nur dazu genutzt, sich an einem Firmennetzwerk anzumelden. Die Einsatzmöglichkeiten sind so vielfältig wie die Faktoren selbst:

Authentifizierung: Die Identifikation eines Nutzers ist das klassische Einsatzgebiet für MFA. Ob es um die Anmeldung am Virtual Private Network (VPN) einer Firma, einem speziell abgesicherten internen Server mit Forschungsdaten, einem Laptop, E-Mail-Konto oder Kunden-Account geht – ein zweiter Faktor reduziert das Risiko, dass durch geknackte, erratene oder gestohlene Passwörter fremde Personen unerlaubten Zugang erhalten, erheblich. Insbesondere Software-Token sowie SMS-Token erlauben heute zudem Szenarien, in denen problemlos Massen-Accounts abgesichert werden können, da keine Hardware-Token versandt, registriert und verwaltet werden müssen.

Risikobasierte Authentifizierung: Um den Anwendern mehr Komfort zu bieten, lässt sich die Anforderung eines zweiten Faktors auf bestimmte Risikoszenarien einschränken. Loggt sich ein Nutzer während der üblichen Arbeitszeiten über seinen Standard-PC am Arbeitsplatz ein, genügt die Eingabe des Passworts.



Erfolgt der Zugriff jedoch nachts, von einem fremden Rechner oder einer ausländischen IP-Adresse aus, wird der zweite Faktor angefordert.

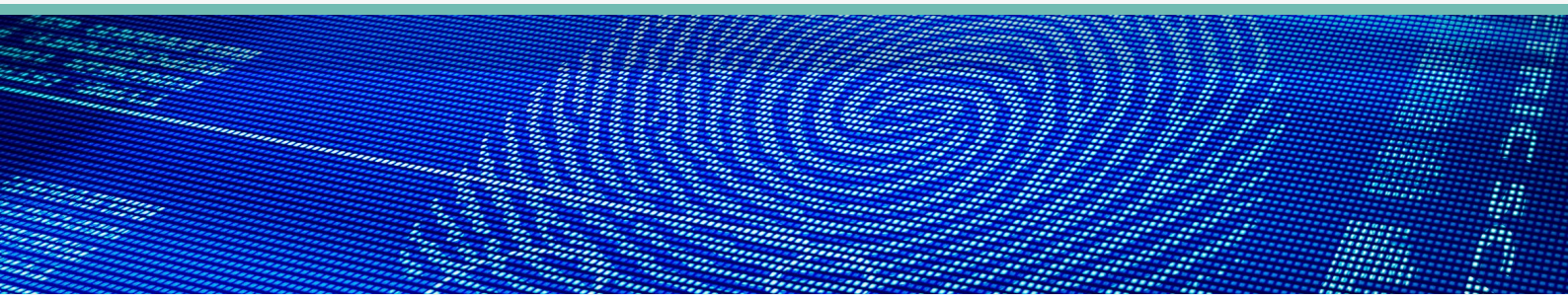
Zeitlich begrenzte Authentifizierung: Häufig müssen Unternehmen Dienstleistern für einen begrenzten Zeitraum Zugang zu ihren Systemen gewähren. Im Falle einer Authentifizierung über Passwörter oder Zugangskarten besteht die Gefahr, dass dieser Account nach Ablauf des Kontrakts nicht gesperrt wird. Bei modernen MFA-Systemen lässt sich die Gültigkeit eines zweiten Faktors dagegen von vornherein zeitlich begrenzen und so dieses Sicherheitsrisiko ausschließen.

Notfall-Logins: In manchen Szenarien sollen Mitarbeiter nur im äußersten Notfall Zugriff auf Systeme erhalten. Dafür lassen sich Einmal-Token konfigurieren. Sie erlauben nur einen einzigen Login und deaktivieren sich danach selbsttätig.

Autorisierung: Diese Art der MFA-Nutzung kennt jeder Bankkunde: Während für den Online-Zugang ein relativ schwaches, sechsstelliges Passwort genügt, wird für jede Überweisung ein eigener zusätzlicher Faktor angefordert. Die früher üblichen TAN-Listen sind dabei praktisch flächendeckend von elektronischen Verfahren wie der Autorisierung per SMS oder App abgelöst worden.

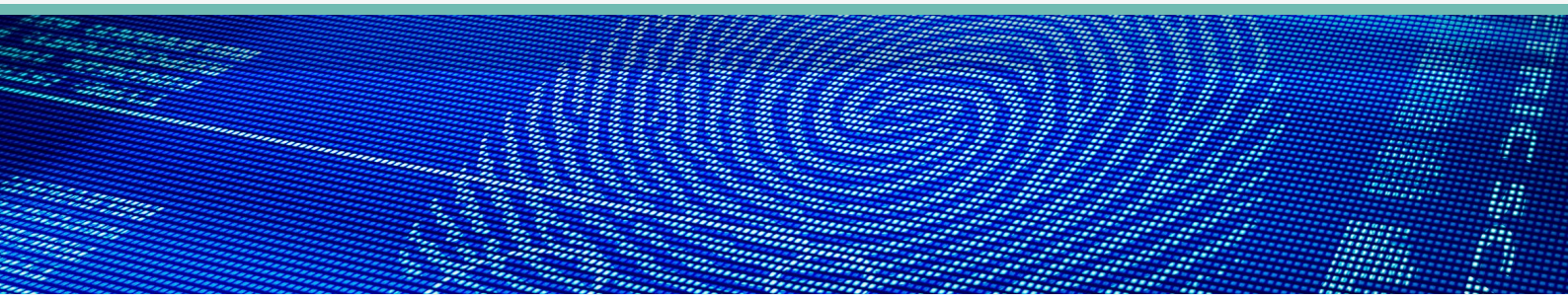
Transaktionssicherheit: Ein System, das Token zur Transaktion benutzt, muss darüber hinaus auch noch die Integrität der Parameter sicherstellen. Wichtig ist außerdem, dass die Übertragung rechtssicher dokumentiert wird, sodass die Autorisierung im Streitfall nachgewiesen werden kann (Nichtabstreitbarkeit).

Mehraugenprinzip: Diese Form der MFA kommt in besonders kritischen oder sensiblen Bereichen zum Einsatz – etwa, wenn Verträge elektronisch unterzeichnet werden sollen, weitreichende Personalentscheidungen zu treffen sind, Daten besonderer Geheimhaltung unterliegen oder sehr große Geldsummen überwiesen werden sollen. Dann genügt es nicht, dass sich ein Mitarbeiter authentifiziert und die Transaktion über einen zweiten Faktor autorisiert; vielmehr müssen zwei, drei oder mehr Verantwortliche gemeinsam mit ihrem jeweiligen Schlüssel die Transaktion genehmigen.



Fazit

Die Multi-Faktor-Authentifizierung ist heute sehr einfach zu implementieren. Die Erzeugung und die Verteilung der Sicherheitsschlüssel lassen sich über wenige Zeilen Code in eine Applikation integrieren, die notwendige Hardwareinfrastruktur ist in Form von Smartphones flächendeckend vorhanden. Angesichts der immer gravierenderen Bedrohungen durch Cyberkriminalität und Spionage und die hohen Risiken, die eine Kompromittierung von Accounts mit sich bringen kann, ist es geradezu fahrlässig, MFA nicht wo immer möglich zu implementieren und zu nutzen. ■



Token-Typen und deren Einsatz

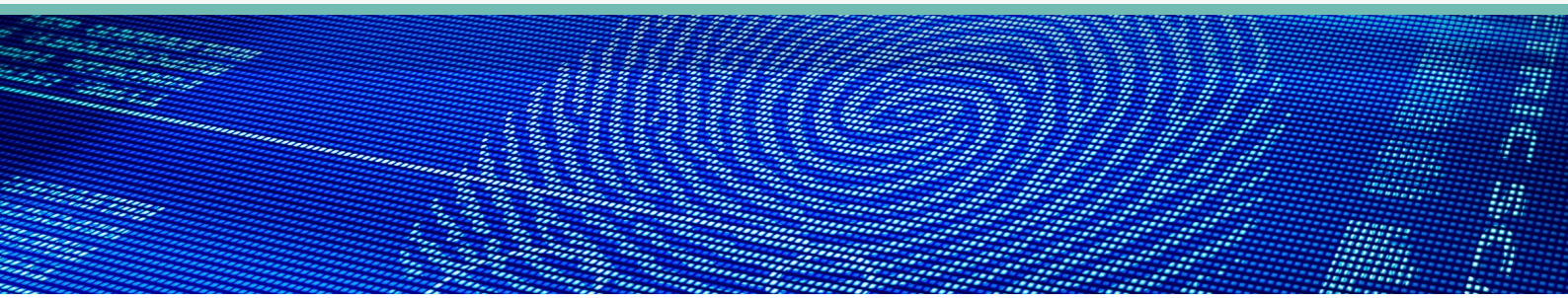
Foto: Stockfotos-MG / Fotolia.de

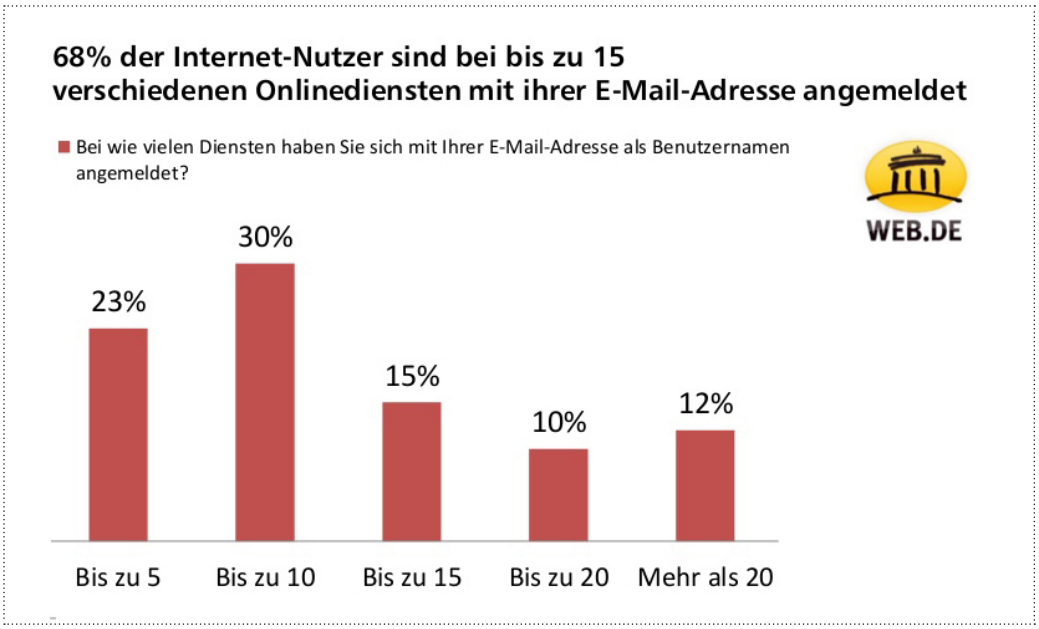
Moderne Multi-Faktor-Authentifizierung (MFA) erhöht nicht nur die Sicherheit beim Zugang zu Online-Konten oder Firmen-Accounts, sondern auch bei der Autorisierung von Transaktionen erheblich. Die dafür benötigten Faktoren, sogenannte Token, stehen in unterschiedlichen Formen zur Verfügung. Dieser Beitrag zeigt, welche Token-Optionen es gibt, welche Vor- und Nachteile sie jeweils haben und für welche Einsatzszenarien sie sich eignen.

Ob Firmenzugang, E-Mail-Konto oder Webshop-Login: Die meisten Accounts, die wir heute privat oder beruflich verwenden, sind in der Regel nur durch einen einfachen Zugang per Nutzername und Passwort gesichert. Die Verwaltung der vielen Passwörter ist jedoch eine echte Herausforderung geworden. Laut einer Studie des E-Mail-Dienstleisters Web.de ist mehr als ein Drittel der deutschen Internetznutzer bei zehn und mehr Online-Diensten mit jeweils eigenem Login angemeldet, zwölf Prozent sogar bei mehr als 20. Über die Hälfte empfindet den Login-Zwang als lästig, und 44 Prozent sind von der hohen Zahl zu verwaltender Passwörter genervt.

Kein Wunder also, dass Anwender versuchen, diesen Aufwand zu minimieren. Rund jeder fünfte Internetnutzer verwendet nach einer Auswertung des Potsdamer Hasso-Plattner-Instituts (HPI) das gleiche Passwort für mehrere Dienste, und die Zahlenfolge „123456“ ist laut HPI nach wie vor das weltweit beliebteste Passwort, dicht gefolgt von „12345678“, „111111“ und „qwerty“.

Doch selbst sichere Passwörter, die nur einmal verwendet werden, mehr als zehn Zeichen umfassen, Sonderzeichen sowie Groß- und Kleinschreibung integrieren und weder Wörter aus dem Duden noch persönliche Informationen wie Geburts-



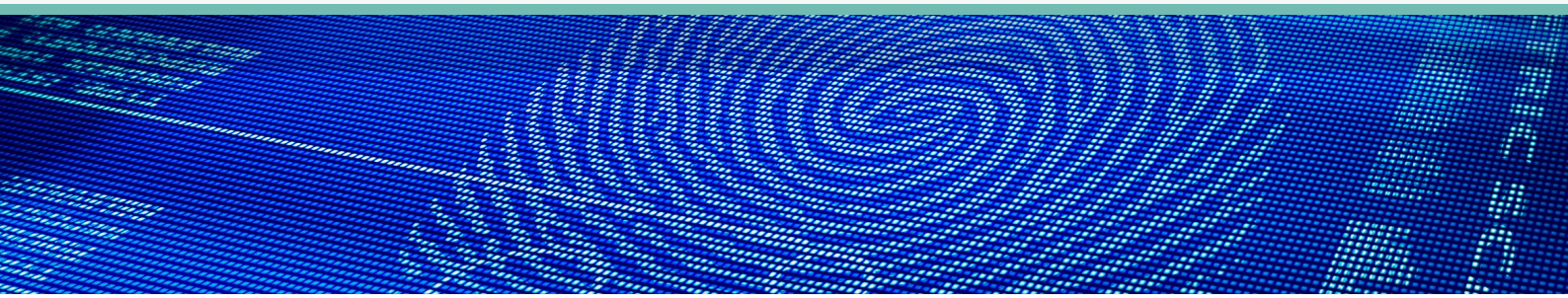


Über ein Drittel der deutschen Internetnutzer ist bei zehn und mehr Online-Diensten angemeldet, zwölf Prozent sogar bei mehr als 20. (Quelle: Bilendi GmbH, im Auftrag von Web.de)

oder Jahrestage enthalten, schützen nur so lange vor nicht autorisierten Zugriffen, wie sie nicht in fremde Hände gelangen. Leider kommt es jedoch häufig zu Einbrüchen und Datendiebstählen bei großen Portalen und Dienstleistern. Dem Karrierenetzwerk LinkedIn kamen laut dem Sicherheitsportal Pwned beispielsweise mehr als 160 Millionen User-Accounts abhanden, beim Softwarehersteller Adobe waren es über 150 Millionen, und der Anbieter von Online-Speicher Dropbox musste den Verlust von mehr als 60 Millionen Login-Daten melden. Laut dem Verizon Data Breach Report waren 2017 bei 81 Prozent aller Hacks schwache oder geknackte Passwörter die Ursache, 2016 waren es noch 63 Prozent.

Der Einsatz von Token: Authentifizierung, Autorisierung, risikobasierte Nutzung

Wesentlich besser geschützt sind Accounts, die über einen zweiten Faktor abgesichert sind. Um sich zu authentifizieren und Zugang zu erhalten, benötigt der Anwender neben seinem Passwort ein sogenanntes Token. Mit einem erratenen, gestohlenen oder geknackten Passwort allein kann ein Dieb daher nichts anfangen, solange er nicht auch in den Besitz des Token gelangt. Multi-Faktor-Systeme können aber nicht nur für die Authentifizierung eines Anwenders, sondern auch zur gezielten Autorisierung einzelner Transaktionen verwendet werden. Das bekannteste Beispiel ist die Online-Überweisung von einem Bankkonto, die durch eine Transaktionsnummer (TAN) autorisiert werden muss. Beide Anwendungs-



szenarien lassen sich natürlich auch kombinieren, was den Schutz sowohl des Zugangs als auch der einzelnen Transaktion verbessert, insbesondere dann, wenn man für Authentifizierung und Autorisierung unterschiedliche Systeme einsetzt. So kann beispielsweise der Zugang zum Online-Banking per PC erfolgen, die Details einer Überweisung können dann per Klick auf OK auf dem Smartphone-Display autorisiert werden.

Um die Nutzer nicht zu überfordern und den Zugang nicht unnötig zu verkomplizieren, können zusätzliche Faktoren risikobasiert eingesetzt werden. Loggt sich ein Anwender beispielsweise zu den üblichen Bürozeiten über ein bekanntes Endgerät und die Firmen-IP-Adresse ein, genügt die Eingabe des Passworts. Erfolgt der Zugriff dagegen nachts von einem fremden PC und einer unbekannten IP aus, wird ein zweiter Faktor angefordert.

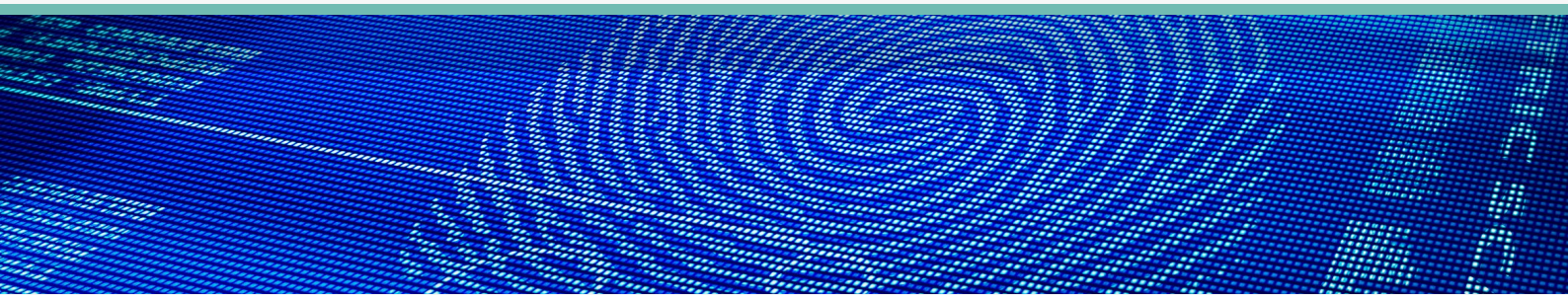
> Multi-Faktor-Systeme lassen sich nicht nur für die Nutzerauthentifizierung, sondern auch zur Autorisierung von Transaktionen verwenden.

Unterschiedliche Token-Typen

Token können auf ganz verschiedene Weise zur Verfügung gestellt werden. Im Wesentlichen lassen sich die folgenden Token-Typen unterscheiden:

Hardware-Token: Mit diesen kleinen, batteriebetriebenen Geräten begann der Siegeszug der Multi-Faktor-Authentifizierung. Hardware-Token erzeugen einen Zufallscode und zeigen diesen auf einem Display an. Sie sind äußerst robust und lassen sich in der Regel aber nicht öffnen, ohne dass sie dabei zerstört werden. Hardware-Token bieten daher ein hohes Sicherheitsniveau. Sie sind zudem unabhängig von anderen Endgeräten wie Smartphones oder der Verfügbarkeit von Mobilfunk- oder WLAN-Netzen und daher universell einsetzbar. Die meisten heute erhältlichen Modelle basieren auf dem Industriestandard OATH (Open Authentication), sodass sie sich in jede OATH-konforme Infrastruktur einbinden lassen. Die Erzeugung des Einmalpassworts kann ereignisbasiert (HMAC-based One-time Password, HOTP) erfolgen. Bei jedem Drücken eines Knopfes wird ein neuer Code generiert. Der Server prüft dann, ob der eingegebene Code mit einem vorgegebenen Werteraum übereinstimmt. Alternativ kommt eine zeitbasierte Methode, (Time-based One-time Password, TOTP) zum Einsatz, bei der in regelmäßigen Intervallen – meist alle 30 oder 60 Sekunden – ein neuer Code erzeugt wird.

Eine Sonderstellung nehmen Hardware-Token ein, die auf dem Standard „Universal Second Factor“ (U2F) der FIDO-Allianz (Fast Identity Online) basieren. Sie können für mehrere Dienste verwendet werden, ohne dass diese voneinander erfahren. Somit sind Datenschutz und Privatsphäre besonders gut gewährleistet. Werden einem Diensteanbieter Login-Daten gestohlen, hat dies zudem keine



Folgen für die Nutzung des Gerätes bei anderen Diensten. Das U2F-Gerät erzeugt dazu bei der Registrierung an einem Dienst ein individuelles Paar aus privatem und öffentlichem Schlüssel. Bei der Anmeldung wird der öffentliche Schlüssel zusammen mit einer Kennung an den Dienstanbieter übermittelt, die den U2F-Token eindeutig identifiziert.

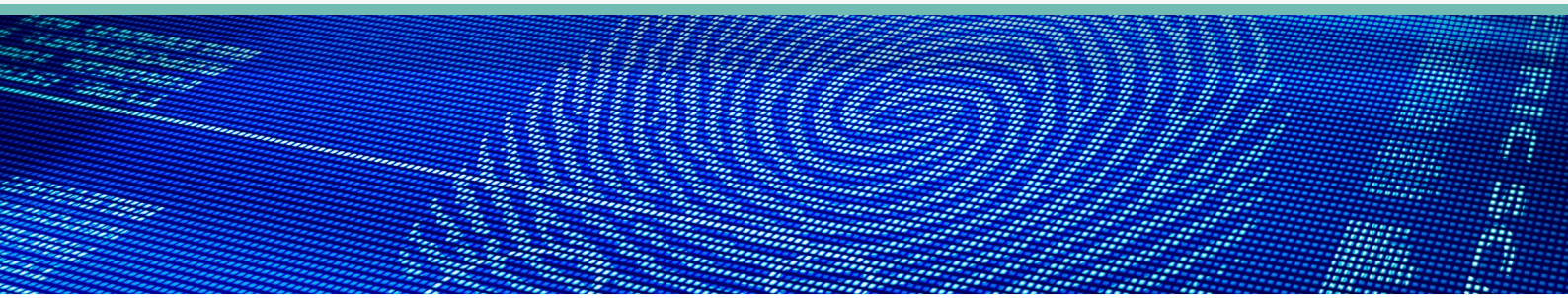
Meldet sich der Nutzer nun an dem Dienst an, sendet der Server die zum Anwender gehörende Schlüsselkennung plus zusätzlicher Informationen wie der Serveradresse an das U2F-Gerät, das aus der Kennung den passenden privaten Schlüssel identifizieren und so die Rückantwort richtig signieren kann. U2F-Token benötigen weder ein Display noch eine interne Stromversorgung und sind daher sehr preiswert herzustellen.

Software-Token: Statt die Einmalpasswörter von einem eigenen Gerät generieren zu lassen, können die Algorithmen auch in Form einer Anwendung oder App zur Verfügung gestellt werden. Diese lässt sich beispielsweise über ein Mobile Device Management (MDM) auf Firmen-Smartphones ausrollen oder über die App Stores von iOS, Android, Blackberry & Co. anbieten. Die Verbreitung und Verwaltung ist daher wesentlich schneller, einfacher und kostengünstiger als bei Hardware-Token. Die Integration in offene Mobilfunkplattformen macht sie allerdings für mobile Malware angreifbar. Daher ist das Sicherheitsniveau nicht so hoch wie bei den Hardwarevarianten.

> Token lassen sich auf ganz unterschiedliche Weise zur Verfügung stellen.

SMS-Token: Der Token-Versand per Kurznachricht ist die einfachste, kostengünstigste und universellste Art, einen zweiten Authentifizierungsfaktor zur Verfügung zu stellen. Man benötigt kein Smartphone, er ist weder von der Installation einer Software noch von den Eigenheiten und Vorgaben der einzelnen Mobilfunkplattformen abhängig. Daher sind SMS-Token vor allem in Massen-Roll-out-Szenarien von Vorteil. Die Absicherung per SMS-Token ist allerdings vergleichsweise leicht zu umgehen: Infektionen mit Malware wie dem Trojaner ZEUS und seiner mobilen Version ZitMo, aber auch Sicherheitslücken im Übertragungsweg SS7 der Netzbetreiber haben in der Vergangenheit mehrfach zur Kompromittierung des auf SMS-Token basierenden mTAN-Verfahrens der Banken geführt.

QR-Token: Der zweidimensionale Quick-Response-Code (QR-Code) kann in einer rechteckigen Matrix aus schwarzen und weißen Quadraten mehr als 4.000 alphanumerische Zeichen speichern. Er lässt sich zur Codierung von Webadressen, Visitenkarten, Zugangsdaten und anderen Informationen verwenden. Als Token



> Push-Token – nicht nur benutzerfreundlich, einfach zu implementieren und zu verteilen, sondern auch sehr sicher.

bietet QR viele Vorteile: Das Verfahren ist weitgehend vor Manipulationen geschützt, sofern der QR-Code verschlüsselt ist und nur mit dem Geheimnis auf dem Smartphone entschlüsselt werden kann. Der größte Vorteil ist aber die erzwungene Gerätetrennung. Ein Angreifer müsste somit zwei Geräte infizieren beziehungsweise kontrollieren.

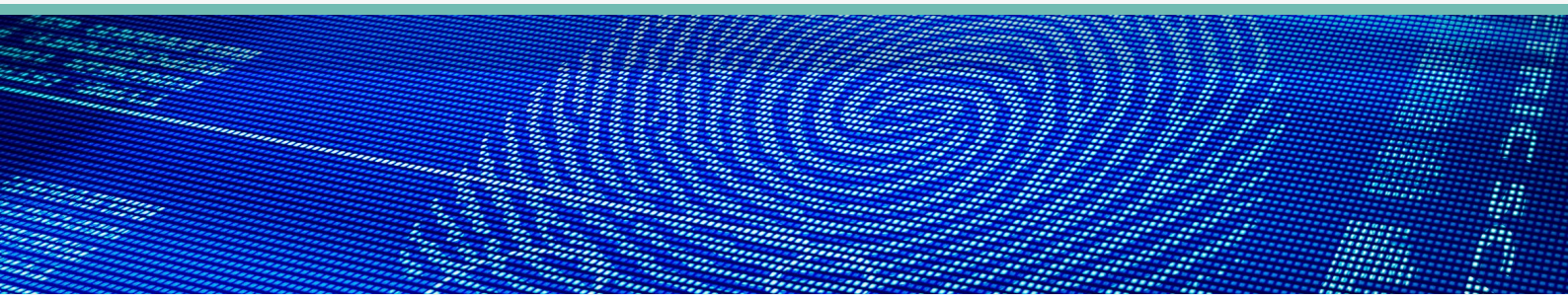
Push-Token: Beim Push-Verfahren erhält der Anwender eine Benachrichtigung auf sein registriertes mobiles Endgerät, wenn er auf geschützte Daten zugreifen oder eine zu autorisierende Transaktion durchführen möchte. Er kann die Aktion dann direkt auf dem Touch-Display bestätigen oder ablehnen. Push-Token sind nicht nur sehr benutzerfreundlich, einfach zu implementieren und zu verteilen, sie sind – wenn korrekt implementiert – auch sehr sicher.

Voice-Token: Blinde und sehbehinderte Menschen haben mit der üblichen, auf der visuellen Übermittlung von Codes basierenden Token-Bereitstellung große Schwierigkeiten. Hilfsmittel wie Screen-Reader können die aus Sicherheitsgründen verschlüsselten Informationen häufig nicht wiedergeben. Dieses Problem lösen Voice-Token: Das System sendet in diesem Fall eine Sprachnachricht mit dem entsprechenden Code an eine hinterlegte Telefonnummer. Der Anwender muss diesen dann eingeben, um sich zu authentifizieren.

Token-Typen

Stärken und Schwächen

Token	Sicherheit	Usability	Verwaltungsaufwand	Kosten
Klassische HW-Token	hoch	gering	mittel	hoch
FIDO U2F-Token	hoch	gering	mittel	mittel
Software-Token	mittel	mittel	mittel	gering
SMS-Token	gering	mittel	gering	gering
QR-Token	hoch	mittel	mittel	gering
Push-Token	mittel	hoch	gering	gering
Voice-Token	mittel	hoch	mittel	gering



Den richtigen Token-Typ für jeden Einsatz finden

Alle vorgestellten Token-Typen haben Vor- und Nachteile. Die Entscheidung für oder gegen den Einsatz hängt deshalb im Wesentlichen von den jeweiligen Anforderungen ab.

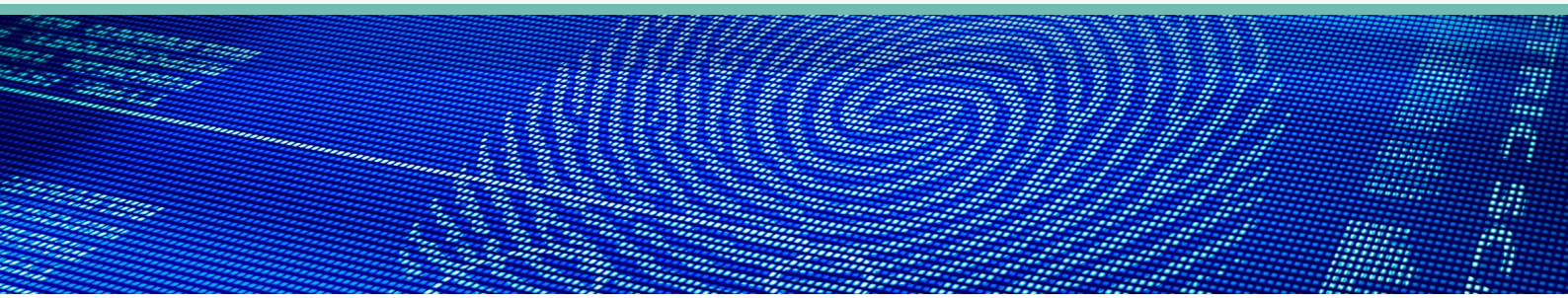
Hardware-Token, die auf dem HOTP- oder TOTP-Verfahren basieren, sind robust, sicher und unabhängig von Betriebssystemen oder mobilen Plattformen einsetzbar. Die Implementierung, Verteilung und Verwaltung ist allerdings komplex, aufwendig und kostenintensiv. Hardware-Token eignen sich deshalb vor allem für große Unternehmen in sicherheitssensiblen Branchen und Bereichen, etwa Banken und Versicherungen oder Regierungsorganisationen. Wesentlich geringer ist der Aufwand dagegen beim Einsatz von FIDO-U2F-Token wie dem Yubikey. Hier kann die Beschaffung eines Tokens dem Anwender selbst überlassen werden (Bring Your Own Token, BIOT). Daher sind sie sogar für den Endkundenbereich geeignet.

Software-Token lassen sich einfach integrieren und verteilen. Sie eignen sich daher sowohl für den Einsatz in Unternehmen als auch in der Kommunikation mit Privatkunden. Aufgrund des geringeren Sicherheitsniveaus sollten sie allerdings nicht ohne Weiteres in sensiblen Bereichen, etwa zur Absicherung von Patenten oder Patientenakten, verwendet werden.

QR-Token bieten hohe Sicherheit bei gleichzeitig hohem Komfort und sind daher bei sicherheitssensiblen Anwendungen dem Software- oder SMS-Verfahren vorzuziehen. Zum Einsatz kommt eine Kombination aus privatem und öffentlichem Schlüssel. Der Server stellt eine Challenge als QR-Code dar, deren Inhalt mit dem öffentlichen Schlüssel eines Smartphones chiffriert wird. Eine App liest den QR-Code ein, decodiert den Wert mit dem privaten Schlüssel und stellt den einzugebenden Wert dann dar. Auf diese Weise lässt sich beispielsweise die Offline-Authentifizierung auf einem Laptop absichern, ohne dass dort ein Geheimnis abgelegt werden muss.

SMS-Token funktionieren mit jedem mobilen Endgerät. Der Anwender muss weder eine Software installieren noch eine App herunterladen. Der Einsatz ist daher immer dann zu empfehlen, wenn die adressierte Nutzergruppe sehr groß und heterogen ist, keine Informationen über die verwendeten Mobiltelefone vorliegen und die Autorisierung schnell und unkompliziert erfolgen soll. SMS-Token sind allerdings von allen Token-Varianten am leichtesten zu kompromittieren und sollten daher in sicherheitssensiblen Bereichen nicht mehr eingesetzt werden.

> Die Entscheidung für oder gegen den Einsatz bestimmter Token-Typen sollte sich nach den jeweiligen Anforderungen richten.



Push-Token sind die moderne und empfehlenswerte Alternative zum SMS-Token. Sie sind deutlich sicherer als der Versand über den Kurznachrichtendienst. Komfort und die damit verbundene Akzeptanz sind hoch, da der Anwender die Transaktion nur bestätigen oder ablehnen muss und keine weiteren Eingaben zu tätigen sind. Push-Token eignen sich außerdem sehr gut für Anwendungen, in denen mehrere Verantwortliche nach dem Vier- oder Mehraugenprinzip gemeinsam einer Aktion zustimmen müssen – etwa, wenn kritische Entscheidungen wie die Abschaltung eines Kraftwerks oder die Überweisung mehrstelliger Millionenbeträge zu treffen sind.

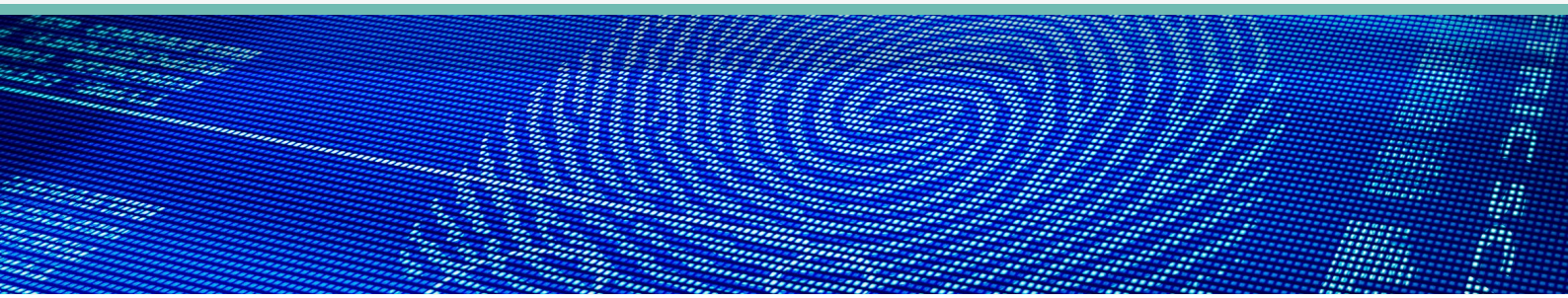
Mit Push-Token lässt sich ein solches Szenario sehr flexibel umsetzen. Damit kann man beispielsweise nicht nur festlegen, dass ganz bestimmte Personen zustimmen müssen, sondern auch, dass aus einer definierten Gruppe eine bestimmte Zahl von Zustimmungen vorliegen muss (sogenanntes N-von-M-Szenario). Die Tokens werden dann einfach an alle Beteiligten der Gruppe (M) gesendet, aus denen dann mindestens N Personen die Transaktion bestätigen müssen.

Voice-Token sind schließlich das Mittel der Wahl, wenn es um den barrierefreien Zugang zu Systemen geht. Ihre Einführung ist für öffentliche Einrichtungen unabdingbar, aber auch Unternehmen sollten sie verwenden, sofern sie sehbehinderte Mitarbeiter beschäftigen oder Kunden mit visuellen Beeinträchtigungen adressieren.

> Mit einer Kombination verschiedener Token lassen sich die Anforderungen an Sicherheit, Nutzerfreundlichkeit und Wirtschaftlichkeit meist am besten erfüllen.

Fazit

Eine Vielzahl von Token-Varianten erleichtert es Unternehmen und Institutionen heute, MFA anzubieten und so das Sicherheitsniveau für Zugänge und Transaktionen erheblich zu steigern. Häufig ist eine Kombination verschiedener Token die beste Lösung, um Sicherheit, Nutzerfreundlichkeit und Wirtschaftlichkeit optimal zu adressieren. Eine MFA-Plattform sollte daher die Möglichkeit bieten, einfach und schnell verschiedene Token-Varianten verwenden zu können. ■

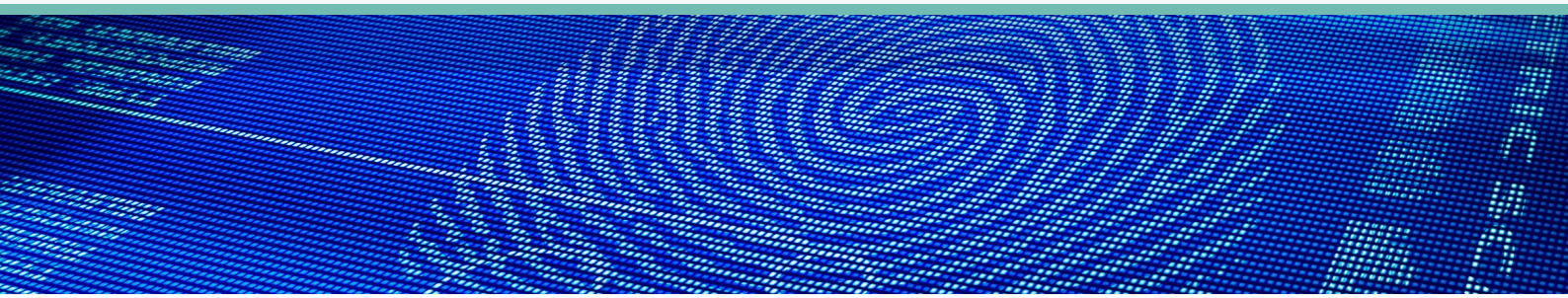


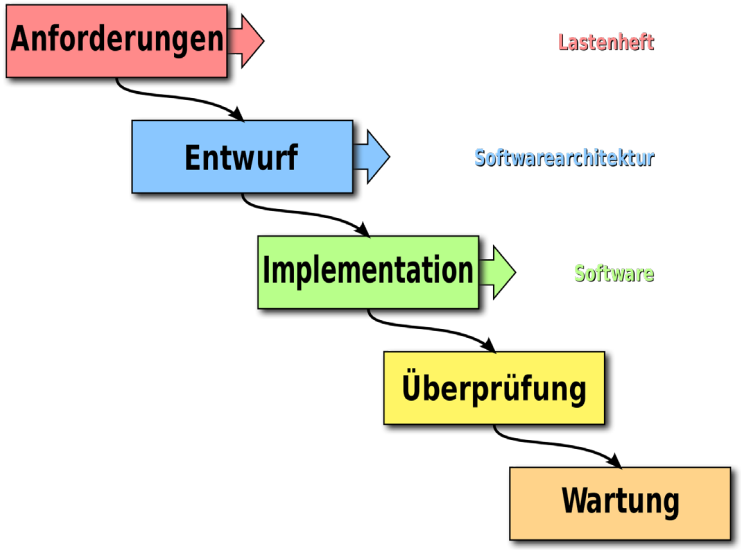
Mit MFA zu sicheren Applikationen

Die Zeiten, in denen es genügte, Firmennetzwerke mit Firewalls gegen unberechtigte Zugriffe von außen abzusichern, sind längst vorbei. Mit Cloud Computing, Portalen und Software as a Service verschwimmen die Unternehmensgrenzen immer mehr. Applikationen vor Missbrauch zu bewahren ist daher eine Herausforderung. Die Integration einer MFA-Lösung bereits bei der Entwicklung kann viel dazu beitragen, Applikationen und Nutzer vor nichtautorisierten Zugriffen und gefährlichen Transaktionen zu schützen.

Die Art und Weise, wie neue Applikationen entstehen, hat sich in den vergangenen Jahren grundlegend gewandelt. Früher folgten Softwareingenieure und Programmierer dem klassischen linearen Wasserfallmodell: Wie Wasser über die Kaskaden eines Falles bergab fließt, so „floss" die Entwicklung einer Anwendung von der Definition der Anforderungen im Pflichten- und Lastenheft über Entwurf, Umsetzung, Test und schließlich Implementierung hin zum fertigen Produkt. Und so wie Wasser nicht bergauf fließt, gab es auch in diesem Prozess kein Zurück. Erst wenn eine Planungsphase abgearbeitet, ein Meilenstein erreicht wurde, konnte die nächste Stufe beginnen.

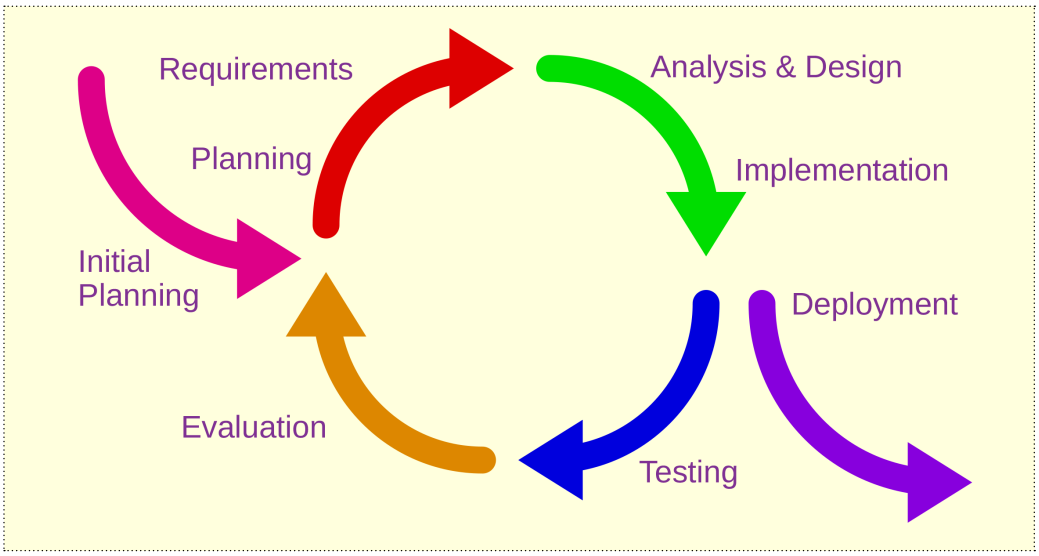
Heute folgt die Entstehung neuer Software völlig anderen Prinzipien: Sie ist agil und iterativ, Entwickler versuchen möglichst schnell, eine funktional zwar eingeschränkte, aber lauffähige Version, das „Minimum Viable Product" (MVP), zu erstellen und dieses so rasch wie möglich vom Kunden testen zu lassen. Dessen Feedback fließt direkt in die Weiterentwicklung der nächsten Version ein, die wiederum getestet und verbessert wird. Eine solche Software ist nie fertig, es gibt keine Versionssprünge im klassischen Sinne mehr, stattdessen verschmelzen Entwicklung (Development) und Betrieb (Operations) zu einem



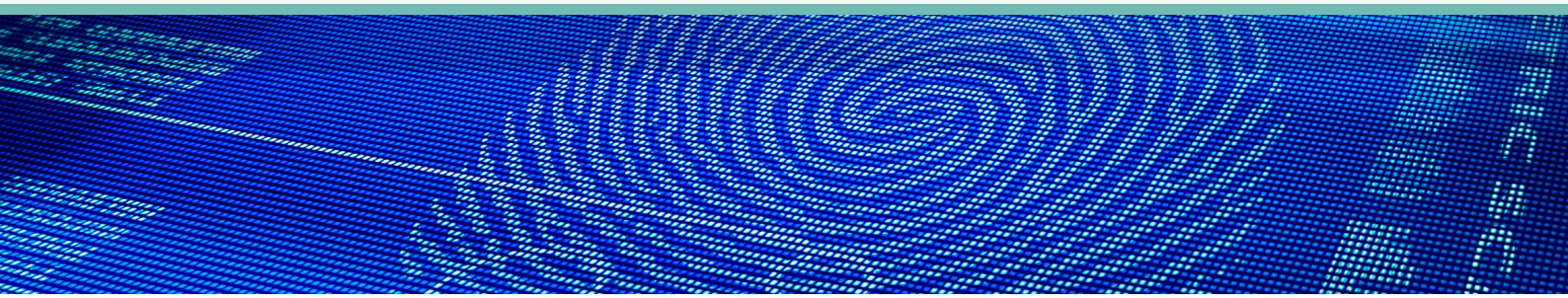


Im Wasserfallmodell der Softwareentwicklung werden die einzelnen Phasen linear nacheinander abgearbeitet. (Quelle: Paul Hoadley, Paul Smith, Shmuel Csaba und Otto Traian, CC BY-SA 3.0)

kontinuierlichen „DevOps"-Prozess. Das ist jedoch nicht der einzige Paradigmenwechsel. Auch die Art und Weise, wie moderne Software aufgebaut ist, hat nur noch wenig mit den monolithischen Architekturen klassischer Anwendungen zu tun. Heute komponieren Entwickler ihr Produkt eher aus einer Vielzahl von Services verschiedenster Quellen, statt jede Zeile Code selbst zu schreiben.



Moderne Entwicklung folgt einem iterativen Modell, in dem Software beständig verbessert und weiterentwickelt wird. (Quelle: Aflafla1, User: Westerhoff, CC0)



Auch angesichts immer komplexerer Bedrohungsszenarien reichen Benutzername und Passwort als Zugangssicherung nicht mehr aus.

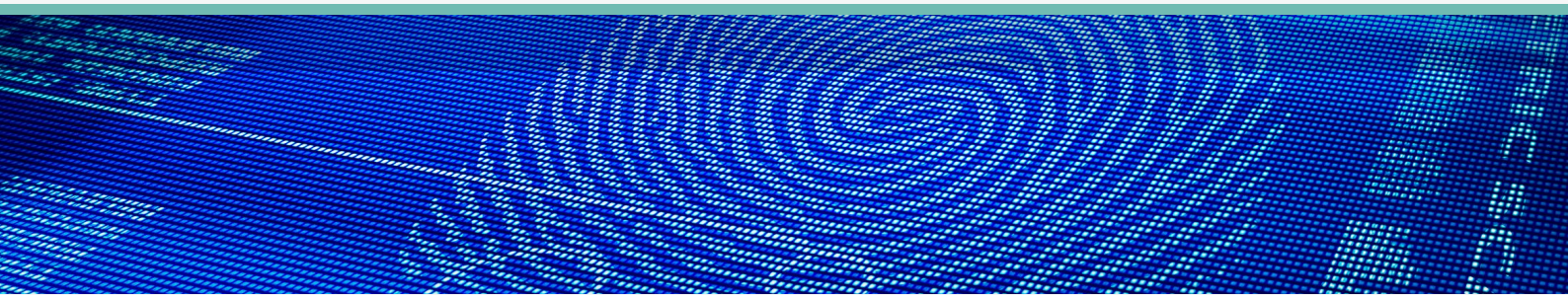
Häufig bestehen solche Dienste sogar aus lediglich einer oder nur wenigen Funktionen und werden daher als Microservices bezeichnet. Diese Microservice-Architektur ist das grundlegende Muster moderner Software. Sie erhöht insbesondere die Skalierbarkeit und reduziert die Komplexität. Anders als bei traditionellen Produkten, in denen ein Logik- oder Implementierungsfehler das gesamte Programm zum Absturz brachte, sind die Services heute so voneinander isoliert, dass die Applikation auch dann weiter funktioniert, wenn eine Komponente abstürzt oder aus anderen Gründen nicht verfügbar ist.

Schwachstelle Passwort

Die fortschreitende Implementierung von Sicherheitsmaßnahmen sowie die Reduktion technischer Implementierungsfehler dank statischer Code-Analyse und anderer Maßnahmen hat für Angreifer den Aufwand, Sicherheitslücken wie Buffer Overflows oder SQL-Injection aufzuspüren, drastisch erhöht. Viel einfacher ist es, die Passwörter aus der Top-10-Liste gegen alle Nutzer eines Unternehmens beziehungsweise einer Anwendung zu testen. Auf diese Weise erhält der Cyber-Kriminelle in der Regel bereits Zugang zu einem Prozent aller Accounts.

Der Schutz der Identitäten wird daher immer wichtiger. Ein Programm kann noch so sicher sein – in dem Moment, in dem ein Angreifer die Identität eines berechtigten Nutzers übernommen hat, kann er tun und lassen, was er möchte. Vor allem auch angesichts immer ausgefeilterer Malware oder Angriffsszenarien wie Spear-Phishing sind Benutzername und Passwort als Zugangssicherung daher nicht mehr ausreichend.

Besondere Bedeutung kommt zudem der Authentifizierung und -autorisierung von sogenannten privilegierten Nutzern wie Administratoren und anderen Verantwortlichen, die weitreichende Rechte besitzen, zu. Diese können beispielsweise Accounts anlegen oder löschen, Passwörter zurücksetzen oder auf die persönlichen Informationen anderer Anwender zugreifen. Diese privilegierten Konten waren früher nur aus dem Firmennetzwerk heraus aufrufbar. Ein potenzieller Angreifer musste sich also zunächst Zugang zum internen Netz beschaffen, um Schaden anrichten und Daten entwenden zu können. In einer Cloud-Umgebung greifen jedoch auch privilegierte Nutzer über das öffentliche Internet auf ihre mit weitreichenden Privilegien ausgestatteten Accounts zu. Und auch Dritte haben im Rahmen von Support- oder Wartungsverträgen immer häufiger privilegierten Zugriff auf Accounts.



Welche Folgen es haben kann, wenn solche Zugänge nur per Nutzername und Passwort abgesichert sind, musste die Wirtschaftsprüfungsgesellschaft Deloitte im vergangenen Jahr erfahren. Ein Hacker hatte sich über einen Administratoren-Account Zugang zum E-Mail-System verschafft, das in der Microsoft-Cloud Azure gehostet wird. So konnte er die Kommunikation von über 240.000 Mitarbeitern mitlesen und Nutzernamen, Passwörter sowie geheime und sensible Informationen abgreifen. Dieser Einbruch, so spektakulär er auch war, ist beileibe kein Einzelfall. Laut dem Verizon Data Breach Report sind rund 81 Prozent aller Datendiebstähle auf gestohlene oder schwache Passwörter zurückzuführen. Solche Vorfälle lassen sich durch die Verwendung einer Multi-Faktor-Authentifizierung (MFA) wesentlich reduzieren. So könnte der Dieb mit Nutzernamen und Passwort allein nichts anfangen, da er einen weiteren Faktor, einen Token, benötigen würde, um Zugriff auf den Account zu erhalten. Diesen erweiterten Zugriffsschutz zu umgehen ist um Vielfaches aufwendiger als das Knacken eines – womöglich auch noch schwachen – Passworts.

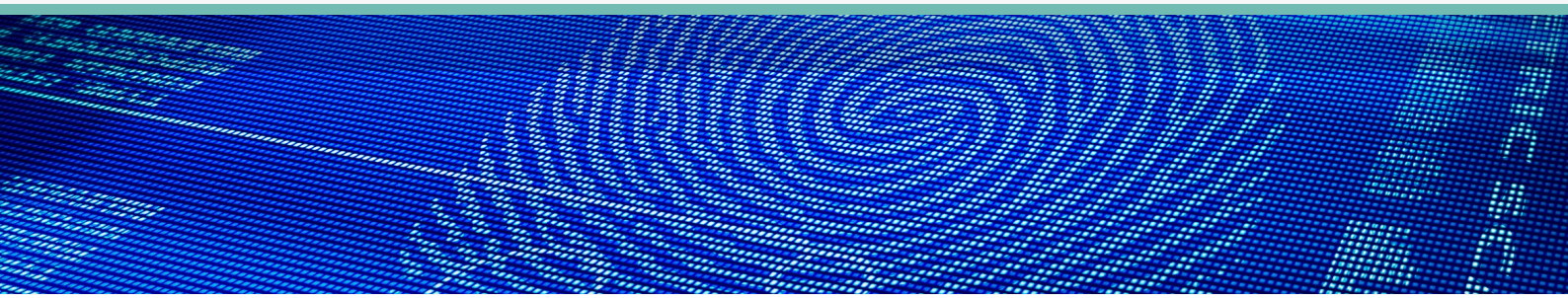
> Rund 81 Prozent aller Datendiebstähle sind laut dem Verizon Data Breach Report auf gestohlene oder schwache Passwörter zurückzuführen.

Wenn Mitarbeiter Millionenschäden verursachen

Nicht nur unzureichend gesicherte Zugänge zu privilegierten Accounts können zu Sicherheitsproblemen führen, auch die legitimen Nutzer dieser Accounts selbst haben schon in vielen Fällen unbeabsichtigt oder auch böswillig Schäden in Millionen- oder gar Milliardenhöhe verursacht. So machte im Februar 2017 der Ausfall des Amazon-Speichersystems S3 Schlagzeilen. Der Tippfehler eines Mitarbeiters hatte zahlreiche Server des Cloud-Anbieters lahmgelegt, der Schaden bei den Kunden belief sich nach Schätzungen des Analystenhauses Cyence auf mehrere Hundert Millionen Dollar.

> Auch legitime Account-Nutzer können - unbeabsichtigt oder auch böswillig – Schäden in Millionenhöhe verursachen.

Mit voller Absicht manipulierte dagegen Jérôme Kerviel die Computersysteme bei seinem Arbeitgeber, der französischen Großbank Société Générale, um Spekulationen im großen Ausmaß tätigen zu können. Die Folge: ein Verlust von nahezu fünf Milliarden Euro. Mit MFA lassen sich solche Vorkommnisse vermeiden, indem sie Transaktionen mit weitreichenden Folgen von der Autorisierung durch mehrere Personen abhängig macht. Diese Zustimmung lässt sich über Token-Systeme einfach implementieren und einsetzen. Im Zuge der Transaktionssicherheit kann sie außerdem gerichtsfest und nichtabstreitbar dokumentiert werden. Aber nicht nur privilegierte Accounts bergen Risiken. Gerade im Massenkundengeschäft mit vielen Hunderttausend oder gar Millionen Privatkunden ist adäquate Sicherheit eine Herausforderung. Betroffene, deren E-Mail-Zugang oder Shopping-Account missbraucht wurde, machen dafür häufig nicht die eigene Nachlässigkeit, sondern den Anbieter verantwortlich. Auch Kunden



einer Versicherung sehen zunächst einmal den Versicherer in der Pflicht, wenn Fremde über ein geknacktes Passwort Zugriff auf Arztrechnungen oder andere sensible Daten erhalten haben.

Eine benutzerfreundliche Multi-Faktor-Authentifizierung, die hochskalierbar ist, kann das Risiko erheblich reduzieren und gleichzeitig die Anwenderzufriedenheit steigern. Damit der Aufwand für die Verwaltung und den Support durch die massenhafte Token-Nutzung nicht ins Unermessliche steigt, sollte die zugrunde liegende MFA-Plattform nicht nur die Token-Ausgabe und -Verwaltung selbstständig und automatisiert durchführen können, sondern auch typische Fehlerszenarien wie verlorene oder vergessene Token abfangen.

> MFA-Funktionen lassen sich wie viele andere Bausteine als Service beziehen und über Standardschnittstellen integrieren.

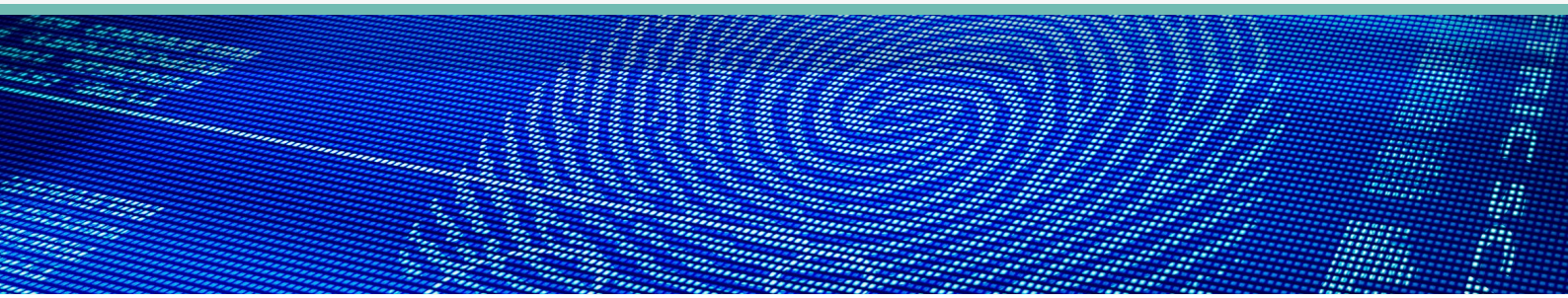
Eingebaute Sicherheit

Um die vielen Gefahren, die von schwachen Passwörtern ausgehen, von vornherein auszuschließen oder zu reduzieren, sollten Unternehmen bereits beim Design neuer Software die Integration einer Multi-Faktor-Authentifizierung vorsehen. MFA-Funktionen lassen sich wie viele andere Bausteine als Service beziehen und über Standardschnittstellen integrieren. Während die Implementierung früher häufig ein halbes Jahr und länger in Anspruch nahm, lassen sich moderne MFA-Plattformen innerhalb weniger Tage integrieren.

```
auth =
requests.post('https://KeyIdentity.com/validate/
check', data={'user': 'MyUserName', 'pass':
'MyOneTimePasswordValue'})

auth_response = json.loads(auth.text)
if (auth_response['result']['status'] == True and
auth_response['result']['value'] == True):
  print('Token is valid')
else:
   print('Token is invalid')
```

Mit wenigen Zeilen Code lässt sich eine MFA-Plattform in eine Anwendung einbinden.



Möglich machen das Schnittstellen beziehungsweise APIs (Application Programming Interfaces), die über das Protokoll HTTPS und das Datenaustauschformat JSON (JavaScript Object Notation) beliebige Web- oder Mobil-Applikationen anbinden können. Standardszenarien wie ein VPN- oder Remote-Access lassen sich direkt über RADIUS integrieren. Für die Anbindung von Cloud-Applikationen empfiehlt sich das XML-Framework SAML (Security Assertion Markup Language) oder auch OpenID Connect. Entscheidend ist, dass die Plattform der Wahl eine nicht-inversive Integration ermöglicht und beliebige Token unterstützt und so einen Vendor-Lock-in verhindert. Dabei sollten sich Nutzerzugänge ebenso per MFA absichern lassen wie einzelne Transaktionen. Wichtig ist auch, darauf zu achten, dass die Autorisierung rechtssicher dokumentiert wird, damit sich im Streitfall nachweisen lässt, dass der Nutzer die Transaktion auch wirklich autorisiert hat (Nichtabstreitbarkeit).

> Unternehmen sollten Sicherheitsmaßnahmen wie MFA schon bei der Softwareentwicklung direkt in die Applikation integrieren.

Fazit

Moderne Web- oder Mobil-Applikationen abzusichern, ist eine große Herausforderung. Die Vollvernetzung, die Wiederverwendung von Passwörtern über mehrere Dienste hinweg sowie die – im Vergleich zum aufwendigeren Aufspüren von Sicherheitslücken oder zum Umgehen von Intrusion-Prevention-Systemen – einfach zu realisierenden Brute-Force-Attacken auf Passwörter macht Account-Zugänge mittlerweile zur am meisten ausgenutzten Schwachstelle. Unternehmen sollten daher bereits bei der Softwareentwicklung Sicherheitsmaßnahmen wie die Multi-Faktor-Authentifizierung direkt in die Applikation integrieren. Das fällt am leichtesten, wenn die MFA-Plattform der Wahl sämtliche Funktionen als leichtgewichtige Programmierschnittstelle (API) zur Verfügung stellt und weder eine Anpassung der Datenbankschemata noch eine Beschränkung auf vom Anbieter zur Verfügung gestellte Token fordert. Mit einer solchen Basis lässt sich MFA mit wenigen Zeilen Code integrieren und so die Sicherheit für Unternehmen und Anwender erheblich steigern. ■

10 SCHRITTE

ZUR ERFOLGREICHEN IMPLEMENTIERUNG EINER MFA-LÖSUNG

KEYIDENTITY

WE SECURE IDENTITIES

LinOTP

KeyIdentity hat bereits an hunderten Sicherheitsprojekten auf der ganzen Welt mitgewirkt.

Basierend auf dieser Erfahrung hat KeyIdentity die Wichtigkeit des richtigen Implementierungskonzepts für MFA-Lösungen erkannt und 10 Tipps zusammengestellt, wie Sie erfolgreich eine MFA-Lösung in Ihre Umgebung integrieren.

☐ **1. Definieren Sie die DIENSTE UND ANWENDUNGEN, für die eine zusätzliche Authentifizierungssicherheit notwendig ist.**

Dies sollte zumindest jeden Dienst einschließen, der öffentlich im Internet zugänglich ist sowie alles, was für Ihr Unternehmen wesentlich oder kritisch ist (einschließlich Admin-Zugang!). Prüfen Sie auch die regulatorischen Anforderungen und denken Sie auch an eine zukünftige Expansion!

☐ **2. Definieren Sie IHRE USER und bestimmen Sie sie genauer.**

Welche User benötigen Zugang zu Ihrem System? Wo befinden sie sich und mit welchen Geräten greifen sie auf Ihre Dienste zu?

☐ **3. Wählen Sie den TOKEN (DIE TOKENARTEN), den/die Sie verwenden wollen.**

Es gibt für jede Art von Token ebenso gute Gründe, sie zu nutzen, wie sie nicht zu nutzen. Versuchen Sie, das beste Gleichgewicht zwischen Sicherheit und Komfort für User und Administrator zu finden. Nicht jeder Token ist für jede Situation geeignet. Manchmal ist es nötig, selbst bei einem einzigen User mehr als nur eine Tokenart zu verwenden.

☐ **4. DEFINIEREN SIE Ihre Prozesse.**

Wie kann innerhalb der Authentifizierung am besten ein zusätzlicher Faktor hinzugefügt werden? Versuchen Sie, den besten Kompromiss zwischen Sicherheit und Komfort für jeden User/jede Gruppe von Usern zu finden.

☐ **5. KOMMUNIZIEREN SIE mit Ihren Usern.**
Jede Sicherheitsstrategie ist nur so gut, wie sie vom User akzeptiert wird! Erklären Sie Ihrem Team, warum Sie es damit „belästigen" und welche Vorteile es für das Unternehmen bringt.

☐ **6. ENTSCHEIDEN SIE, welche Bedingungen durch die Installation erfüllt sein sollen:**
Bevorzugen Sie einen On-Premise - oder einen cloudbasierten Dienst? Wie wollen Sie eine schnelle Verfügbarkeit gewährleisten? Wollen oder müssen Sie einige 2FA-Dienste von anderen trennen?

☐ **7. ENTSCHEIDEN SIE auf Grundlage Ihrer Erkenntnisse, welche Lösung am besten für Sie passt:** Suchen Sie auf dem Markt nach einer Lösung mit einer höchstmöglichen Flexibilität, die einerseits die heutigen Anforderungen erfüllt, der Sie aber ebenso zutrauen, auch für die Fragen von morgen gewappnet zu sein.

☐ **8. ÜBERPRÜFEN SIE nicht nur das technische Konzept, sondern auch die von Ihnen gewählten Prozesse:**
Oft läuft die technische Implementierung glatt, das Projekt scheitert aber dennoch, da die Prozesse scheitern (und/oder vom User nicht angenommen werden). Überprüfen Sie dies auch mithilfe eines technischen POC an einem Querschnitt der User.

☐ **9. STELLEN SIE Ihre User wenn möglich gruppenweise auf das neue System UM:**
Dies gibt Ihnen die Möglichkeit festzustellen, wo mögliche Fallstricke lauern und die Chance, die Installation und die Prozesse anzupassen, bevor die Probleme die gesamte Nutzerbasis beeinträchtigen.

☐ **10. Zu guter Letzt – BEHALTEN SIE Ihre Implementierung stets IM AUGE:**
Überprüfen Sie Ihre Installation in regelmäßigen Abständen und beobachten Sie gleichzeitig den Markt. Halten Sie auch Kontakt zu Ihren Usern. Es kann immer passieren, dass etwas Neues entwickelt wird, was Ihnen das Leben leichter, Ihre Umgebung sicherer oder das Nutzererlebnis komfortabler macht.

KeyIdentity ist ein globaler Anbieter von hoch skalierbaren, einfach einsetzbaren Multi-Faktor-Authentifizierungslösungen (MFA) auf Open-Source-Basis. Die Lösungen von KeyIdentity zeichnen sich durch ihre hohe Usability und Skalierbarkeit aus und lassen sich mit jedem am Markt verfügbaren Authentifizierungstoken (OTP-Token) nutzen – von Software-Token wie Push-, QR- und SMS-Token über Hardware-Token bis hin zu Biometrie-Token.

Kontaktieren Sie uns bei Fragen:
sales@keyidentity.com

KeyIdentity GmbH
Robert-Koch-Straße 9
64331 Weiterstadt
+49 6151 860 86-0
info@keyidentity.com
www.keyidentity.com

KEYIDENTITY

WE SECURE IDENTITIES

SUCCESS STORY:

ZWEITER AUTHENTIFIZIERUNGSFAKTOR SCHÜTZT DIGITALE LOGINS BEI SCANIA

Sicherheit auf dem neuesten Stand der Technik – Scania erweitert Identity- und Access-Management für Mitarbeiter

Scania gehört zu den weltweit führenden Anbietern von Transportlösungen. Das über 125 Jahre alte Traditionsunternehmen mit Sitz im schwedischen Södertälje produziert Lkw und Busse, die für unterschiedliche Transportaufgaben genutzt werden. Des Weiteren umfasst das Angebot von Scania Industrie- und Schiffsmotoren, die in zahlreichen Transport- und Industrieanwendungen im Einsatz sind, von Radladern über Patrouillenbooten bis hin zu Notstromaggregaten. Zusätzlich zu seinen hochentwickelten Transport- und Motorenlösungen bietet Scania seine Kunden ein umfangreiches Serviceangebot, das unter anderem Werkstattleistungen, Finanzierungs- und Versicherungslösungen sowie Fahrtrainings und Support-Dienstleistungen umfasst. Im Rahmen seines weltweiten Vertriebs- und Servicenetzes ist Scania mit rund 46.000 Mitarbeitern in 100 Ländern präsent.

Ergänzend zu seinem Kerngeschäft engagiert sich Scania für die Entwicklung nachhaltiger Transportsysteme und zukunftsweisender Mobilitätslösungen. So arbeitet der Fahrzeugspezialist eng mit strategischen Partnern zusammen, um das Transportwesen durch innovative Technologien wie Fahrzeugvernetzung oder die Optimierung der Energieeffizienz smarter und umweltfreundlicher zu machen.

SCANIA

- **Einsatzbereich:** Authentifizierung von Mitarbeitern im Außendienst und im Homeoffice
- **Lösung:** KeyIdentity MFA-Plattform
- **Token:** SMS- und Software-Token
- **Implementierung:** Erstimplementierung im Mai 2015, Erweiterung in 2017
- **Vorteile:** höhere Sicherheit, Bedienungsfreundlichkeit, Skalierbarkeit, reibungslose Erweiterung, Kosteneffizienz; Erfüllung von Compliance-Standards

KEYIDENTITY

Einhaltung strenger Compliance-Vorgaben

Für Scania stehen stets die Kunden und ihre Sicherheit im Vordergrund: Dies bedeutet zum einen, dass alle Scania Fahrzeuge und Transportlösungen höchste Standards in Sachen Verkehrssicherheit und Zuverlässigkeit erfüllen müssen. Zum anderen hat es sich das Unternehmen zum Ziel gesetzt, alle Compliance-Vorgaben und insbesondere Datenschutz-Regularien wie die EU-Datenschutz-Grundverordnung (EU-DSGVO) einzuhalten. Um dies zu gewährleisten, überprüft und aktualisiert Scania regelmäßig all seine IT-Sicherheitsmechanismen inklusive seines Identity- und Access-Managements (IAM). Die Identitäts- und Zugriffsverwaltung sorgt dafür, dass nur die berechtigten User durch eine strenge Authentifizierungs- und Autorisierungskontrolle auf die Applikationen und Systeme im Unternehmen zugreifen können. Im Zuge ihres Security-Updates hat die Scania Deutschland GmbH am Standort Koblenz unter anderem auch ihre Multi-Faktor-Authentifizierung (MFA) ausgeweitet, mit der das Unternehmen den Zugriff auf seine Virtual Private Networks (VPNs) schützt.

Sicherer Zugriff auf VPN-Verbindungen

Die VPN-Verbindungen ermöglichen es den Scania Mitarbeitern im vertrieblichen oder technischen Außendienst sowie im Homeoffice, jederzeit sicher über webbasierte Anwendungen auf Kunden- und Unternehmensdaten zuzugreifen. Damit die VPN-Nutzung stets unter Einhaltung der strengen Compliance-Vorgaben geschieht, hat sich Scania entschieden, den Einsatz seiner MFA-Lösung von KeyIdentity auszubauen.

Zweiter Authentifizierungsfaktor schützt digitale Logins

Die SMS- und App-basierten Token fungieren im Rahmen der MFA-Lösung als jeweils zweite Faktoren. Damit muss der Nutzer einen zusätzlichen Berechtigungsnachweis unabhängig vom ersten Faktor – dem Passwort oder dem Login-Code – erbringen, bevor eine VPN-Verbindung aufgebaut werden kann. Denn Passwörter allein schützen digitale Identitäten heute nicht mehr ausreichend. Dem „Data Breach Investigations Report“ von Verizon zufolge waren gestohlene oder verlorene Passwörter im Jahre 2017 sogar in 80 Prozent aller Fälle die Ursache für Datendiebstähle oder Hacks. Durch die Multi-Faktor-Authentifizierung wird dieses Risiko ausgeschlossen. Denn selbst wenn potenzielle Angreifer ein Passwort erbeutet haben, befindet sich der zweite Faktor ausschließlich im Besitz des berechtigten Nutzers.

> *„Wir setzen bereits seit 2015 die Multi-Faktor-Authentifizierungslösung von KeyIdentity erfolgreich ein. Aufgrund von Compliance-Vorgaben haben wir uns dazu entschlossen, die Anzahl unserer User deutlich zu erweitern – von etwa 50 auf über 1.000. Wir setzen dabei zu etwa 98 Prozent auf eine Authentifizierung per SMS und zu zwei Prozent auf eine App-basierte Ausgabe des Einmal-Passworts“*
>
> **Michael Zimmer**
> **Teamleiter IT Operations**
> **Scania Deutschland GmbH**

KeyIdentity GmbH
Robert-Koch-Straße 9 | 64331 Weiterstadt
+49 6151 860 86-0 | info@keyidentity.com
www.keyidentity.com

Unternehmenssitz: Weiterstadt
Amtsgericht Darmstadt: HRB8649
Geschäftsführer: Nils Manegold,
Dr. Amir Alsbih
MAX 21-Unternehmensgruppe

KEYIDENTITY

Aufgrund des hohen Sicherheitsniveaus empfehlen sowohl das Bundesamt für Sicherheit in der Informationstechnik (BSI) als auch der Bundesverband IT-Sicherheit e.V. (TeleTrusT) die Technologie. Wenn sie sich für den Aufbau der VPN-Verbindung einloggen, erhalten die Scania Mitarbeiter automatisch ein sogenanntes Einmal-Passwort – oder auch One-Time-Password (OTP) – per SMS oder App-Benachrichtigung auf ihr Smartphone. Sie müssen dieses nur noch als zusätzliche Komponente innerhalb des Authentifizierungsvorgangs eingeben und erhalten dadurch Zugang zur VPN-Verbindung.

Einfach zu nutzen und flexibel erweiterbar

„Unsere Mitarbeiter konnten die Multi-Faktor-Authentifizierung reibungslos in ihre Arbeitsabläufe integrieren. Sie agieren damit bei jedem Login deutlich sicherer als zuvor und ermöglichen uns, die strengen Compliance-Vorgaben auch wirklich einzuhalten. Dafür müssen sie sich kein zusätzliches Passwort merken und können sich somit voll und ganz auf ihre Aufgaben konzentrieren. Dies war uns besonders wichtig, denn für höchstmöglichen Datenschutz und IT-Sicherheit müssen wir mit unseren Kolleginnen und Kollegen an einem Strang ziehen. Daher wollten wir ihnen den Einsatz der MFA-Lösung auch so einfach wie möglich machen“, so Michael Zimmer von Scania weiter. „Die MFA-Lösung ließ sich dank des API-first-Ansatzes von KeyIdentity schnell und einfach erweitern. Durch die Smart-Features der Lösung wie ein Auto-Assignment der Token oder eine Auto-Synchronisierung wird der Aufwand in unserem User-Helpdesk erheblich reduziert. Gleichzeitig steigt damit einmal mehr die Gesamtakzeptanz und die Zufriedenheit der Nutzer.“

Die MFA-Technologie von KeyIdentity erfüllt nicht nur alle aktuell geltenden Sicherheitsstandards und ist einfach einsetzbar. Sie lässt sich darüber hinaus flexibel skalieren und problemlos erweitern. Auch das Rollout weiterer Token-Typen wie Push-, OR- oder Hardware-Token ist damit ohne großen Zusatzaufwand denkbar. Ein weiterer Vorteil: KeyIdentity entwickelt und aktualisiert seine Security-Technologie von Anfang bis Ende in Deutschland. Damit ist gewährleistet, dass der gesamte Einsatz und Support nach strengem deutschen Datenschutz geschieht und selbst neueste Regularien wie die EU- DSGVO eingehalten werden. Scania ist damit in der Lage, die hohen Sicherheitsanforderungen für seine Kunden optimal und auf dem neuesten Stand der Technik umzusetzen.

> *„Die MFA-Lösung ließ sich dank des API-first-Ansatzes von KeyIdentity schnell und einfach erweitern. Gleichzeitig haben wir durch die Smart-Features des IAM-Systems kaum Support-Aufwand für die Verwaltung der sicheren Login-Lösung auf MFA- Basis.“*
>
> **Michael Zimmer**
> **Teamleiter IT Operations**
> **Scania Deutschland GmbH**

Über KeyIdentity

KeyIdentity ist ein führender Anbieter von hoch skalierbaren, einfach einsetzbaren Identity- und Access-Management-Lösungen (IAM) auf Open-Source-Basis für die Absicherung und Verwaltung digitaler Identitäten über Netzwerk- und Cloud-Umgebungen. Der Fokus von KeyIdentity liegt auf den Bereichen Transaktionssicherheit, Identitätsmanagement und der starken Authentifizierung mittels Multi-Faktor-Authentifizierung (MFA).

Die IAM-Lösungen von KeyIdentity werden von Anfang bis Ende in Deutschland entwickelt und bereitgestellt und erfüllen höchste Sicherheitsstandards nach deutschem Recht. Durch den Open-Source-Ansatz lassen sich zudem kryptografische Backdoors ausschließen. KeyIdentity bietet seit 2002 „Security made in Germany“ und hat seinen Sitz in Weiterstadt bei Darmstadt.

.

www.keyidentity.com

KeyIdentity GmbH
Robert-Koch-Straße 9 | 64331 Weiterstadt
+49 6151 860 86-0 | info@keyidentity.com
www.keyidentity.com

Unternehmenssitz: Weiterstadt
Amtsgericht Darmstadt: HRB8649
Geschäftsführer: Nils Manegold,
Dr. Amir Alsbih
MAX 21-Unternehmensgruppe