Foto: Fotolia / Pixsooz

Doppelt hält besser

Sicherer Zugang mit 2-Faktor-Authentifizierung

Nutzername und Passwort reichen als Zugangsschutz allein nicht aus.

Adobe, Ebay, Twitter und viele andere mehr: Die Reihe prominenter Konzerne, die in die Schlagzeilen geraten, weil Datenbanken mit Benutzerinformationen gehackt worden sind, wird länger und länger. Allein bei den bekannt gewordenen Fällen waren überschlägig kalkuliert mehrere Millionen Nutzer betroffen. Und auch wenn sich mit den gehackten Daten allein keine Konten leerräumen ließen, so können die Hacker auch schon mit geklauten Passwörtern und Benutzerdaten schweren Schaden anrichten.

Hier heißt das Hauptproblem Identitätsdiebstahl: Kriminelle können sich mit den Daten Zugang zu einem System verschaffen und gelten dann für die intern aktiven Schutzsysteme als legitime Nutzer. Sie können gefälschte Nachrichten versenden, die von anderen Nutzern als glaubwürdig angesehen werden und die auch Spamfiltern nicht schon wegen der Absenderadresse als verdächtig auffallen. Die Eindringlinge erhalten in einem System die Rechte der wahren Nutzer und Zugriff auf alle Daten, die über das Benutzerkonto ansprechbar sind. Mehr noch: Die unrechtmäßig durchgeführten Aktionen sind nur auf den Nutzer zurückzuführen, dessen Zugangsdaten gehackt wurden.

Eine Lösung, die ohne übermäßig viel Aufwand deutlich mehr Sicherheit bringen würde, heißt 2-Faktor-Authentifizierung, kurz 2FA. Anwender geben dabei in der Regel neben einem Benutzernamen und dem dazugehörigen Kennwort eine Zusatzinformation ein, die eindeutig dem Benutzer zugeordnet ist.

Hardware-Token: Der Codemeter-Dongle von Wibu dient der Authentifizierung.

2-Faktor-Authentifizierung (2FA)

Bei der 2FA kommen zwei Erkennungsmerkmale (Faktoren) zum Einsatz, die unabhängig voneinander verwaltet beziehungsweise generiert werden und schrittweise abgefragt und mit Daten verifiziert werden, die im System hinterlegt sind. Als Authentifizierungsfaktoren, die im Rahmen der 2FA über gesondert abgefragte Benutzerdaten im Rahmen der Authentifizierung verbunden und geprüft werden, sind möglich:

- Informationen, die nur der Benutzer kennt (zum Beispiel Benutzername und Kennwort oder PIN und TAN)
- ein Informationselement, das nur der Anwender besitzt (zum Beispiel ein Smartphone oder Tablet beziehungsweise ein Token wie Plastikkarte, USB-Stick oder Schlüssel)
- ein körperliches Merkmal (Fingerabdruck, Iris, Stimme)

Die bekannteste Variante der 2-Faktor-Authentifizierung findet sich an Geldautomaten. Hier sind die beiden Faktoren eine Bankkarte (als Token) und eine vierstellige PIN (als Information, die nur der Benutzer kennt).

Hardware- und Software-Token

Die 2-Faktor-Authentifizierung kennt Hardware-Tokens wie Smartcard oder USB-Stick oder Software-Tokens. Hardware-Tokens haben den Nachteil, dass der Nutzer sie mitführen muss und dass sie verloren gehen können und dann ersetzt werden müssen. Außerdem braucht man dazu meist Geräte wie Kameras, Audiorekorder, Kartenlesegeräte oder Fingerabdrucksensoren, um die Authentifizierungs-Infos abzurufen. Und es muss darauf geachtet werden, dass die Hardware-Tokens nicht einfach kopierbar sind. Das gilt vor allem für USB-Sticks, die verschlüsselt und kopiergeschützt sein sollten, wenn sie für die Authentifizierung verwendet werden.

Software-Tokens sind Daten, die ohne Zusatzgerät oder Hardware generiert werden und direkt vorliegen, sodass keine Kommunikation zwischen Server und Client erfolgen muss, etwa in der Kommunikation aus Benutzername/Kennwort und fester PIN. Die zeitlich nicht begrenzten Daten werden auf PC oder Laptop gespeichert und sind von Gerät zu Gerät kopierbar, ohne an eine spezielle Hardware gebunden zu sein.

Häufig wird das Hardware-Element, auf dem das Hardware-Token erzeugt wird, durch ein mobiles Standardgerät wie Smartphone oder Tablet ersetzt. Das Gerät selbst dient dabei nicht zur Authentifizierung, sondern als Empfänger für eine Authentifizierungsinformation, die dynamisch generiert wird und zeitlich befristet und nur einmal gültig ist. Die 2FA mit Handy oder Tablet wird auch als tokenlose 2-Faktor-Authentifizierung bezeichnet. Oft kommen auf den mobilen Geräten auch spezielle Apps zum Einsatz, die den eingehenden E-Mail-Verkehr überwachen und Alarm geben, wenn eine Mail mit Authentifizierungsinformationen vorliegt. Auch Datenentschlüsselungen nehmen sie mitunter vor.

2FA nachrüsten

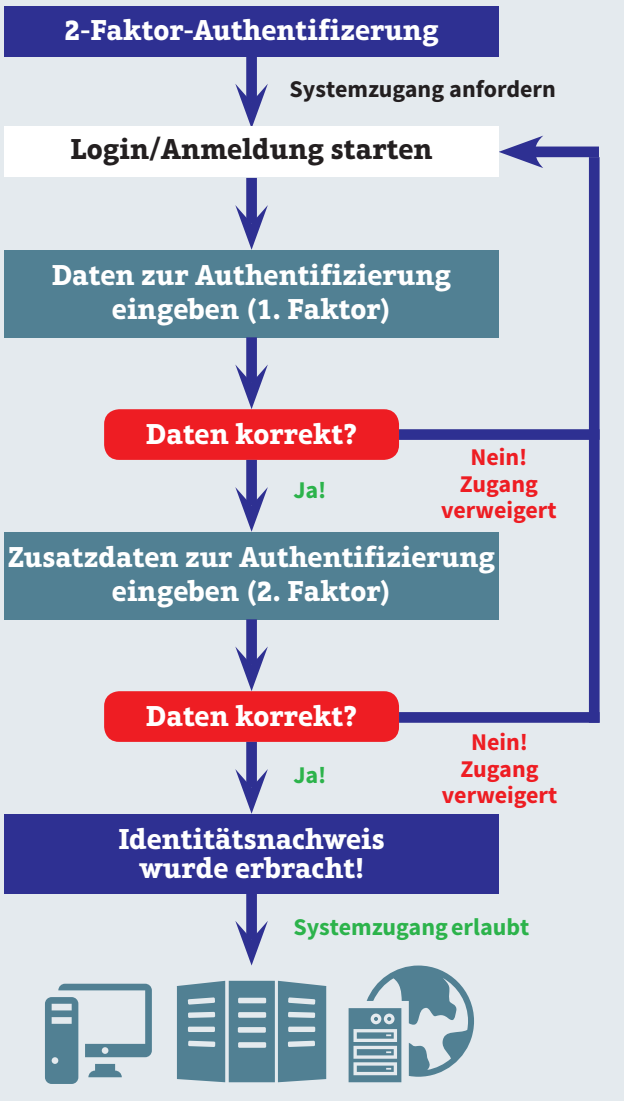
Die gute Nachricht: Jede Software lässt sich durch ihre Entwickler um beliebige, auch mehrstufige Authentifizierungsfunktionen erweitern. Besonders einfach ist das für Unternehmen mit eigenen Entwicklern und eigenen Firmen- beziehungsweise Webanwendungen. Um Authentifizierungsverfahren allerdings unternehmensweit zu vereinheitlichen und mit vorgefertigten Verwaltungswerkzeugen einzusetzen, führt kein Weg an spezieller Unternehmenssoftware vorbei.

Bei einer softwarebasierten 2FA werden kopierbare Software-Tokens per PC, Laptop, PDA oder Smartphone verwaltet und sind nicht an bestimmte Hardware gebunden. Um eine 2FA hardwarebasiert zu realisieren, empfehlen sich kopiergeschützte USB-Sticks, bei denen Daten auf dem Stick verwaltet werden, die nicht kopierbar sind.

Der bekannteste Anbieter solcher Sticks ist die deutsche Firma Wibu Systems AG aus Karlsruhe. Die Hardware-Schlüssel von Wibu Systems, die Codemeter-Dongles, können zum Beispiel sowohl zur Lizenzierung von Software ▶

2-Faktor-Authentifizierung der Identität

Um Zugang zu erhalten, muss der Nutzer seine Identität nachweisen. Dazu muss er zwei separate Faktoren eingeben.



com! professional 11/14

Schritt für Schritt: Nur wenn der erste Zugangsfaktor korrekt eingegeben wird, fragt das System den zweiten Faktor ab.

und Dokumenten als auch zum Speichern von Zertifikaten verwendet werden. Codemeter-Dongles werden außerdem eingesetzt, um Service-Technikern einen zeitlich begrenzten Zugang zu Geldautomaten zu gewähren.

Für Wibu-CEO Oliver Winzenried ist das wichtigste Grundprinzip bei der 2-Faktor-Authentifizierung die „Trennung von Wissen und Besitz", also zum Beispiel die Trennung von Kennwort auf der einen Seite und Token auf der anderen Seite.

Trotz des Sicherheitsgewinns durch 2FA verhalten sich viele Firmen bei diesem Thema noch zurückhaltend. So unterstützt etwa die verbreitete Unternehmenssoftware von Combit derzeit 2FA nicht standardmäßg – sie lässt sich aber auf Anforderung nachrüsten, wie Combit-Geschäftsführer Jürgen Bartlau erklärt: „Wir beobachten die Entwicklung auf jeden Fall und rüsten alternative Authentifizierungsvarianten entsprechend den Bedürfnissen in den Unternehmen nach."

„Die 2-Faktor-Authentifizierung trennt Wissen (Kennwort) und Besitz (Token)."

Oliver Winzenried
CEO des Sicherheitstechnik-Spezialisten Wibu Systems AG
www.wibu.com

Demo-Programm

Auf der Heft-DVD finden Sie binär und im Quelltext ein in Visual Basic .NET geschriebenes Beispielprogramm, das die 2-Faktor-Authentifizierung im Verbund mit mobilen Geräten und PIN-Übergabe per E-Mail demonstriert. Die Kennwörter werden über Hash-Werte gesichert, aus denen sich keine Rückschlüsse auf die ursprünglichen Zugangswerte ziehen lasssen. Das Programm starten Sie per Doppelklick auf die Datei „2-Faktor-Authentifizierung.exe". Als Erstes tragen Sie dann den gewünschten Benutzernamen samt Kennwort ein und übernehmen die Zugangsdaten mit einem Klick auf „Daten speichern". Sie werden automatisch in die Felder unter „1. Faktor" eingetragen. Mit „Zugang anfordern" starten Sie den ersten Schritt der Authentifizierung. Sind die Zugangsdaten korrekt, wird zunächst das Feld zur PIN-Anforderung aktiviert. Geben Sie dann im Textfeld „E-Mail-Adresse" die Adresse an, an die die Mail mit der PIN verschickt werden soll, und klicken Sie auf „PIN per Mail verschicken".

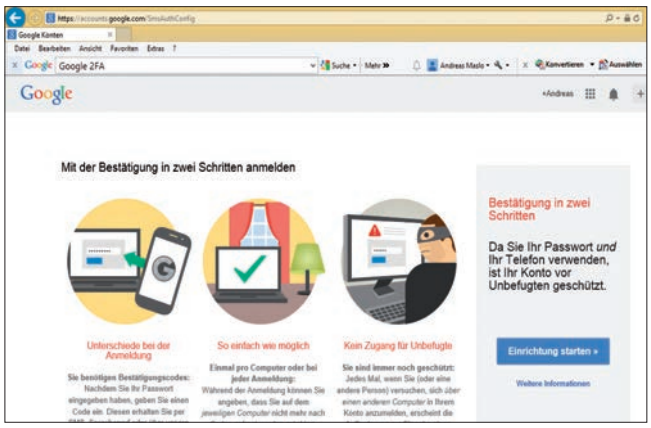
Dadurch wird eine nur für 60 Sekunden gültige fünfstellige PIN generiert und an die angegebene E-Mail-Adresse verschickt. Die Mail kann am PC, Smartphone oder auch auf Tablet-PCs empfangen werden. Um die Authentifizierung vorzunehmen, geben Sie die PIN ins Feld „2. Faktor: PIN-Eingabe" ein und klicken abschließend auf „Authentifizieren".

Wenn Sie länger als 60 Sekunden brauchen sollten, um diese abschließende Authentifizierung vorzunehmen, ist die PIN bereits wieder ungültig geworden und Sie erhalten eine ▶

Marktübersicht: Software für die 2-Faktor-Authentifizierung

Die wichtigsten Softwarelösungen, mit denen Unternehmen eine 2-Faktor-Authentifizierung bereitstellen können.

Anbieter	Website	Produkt	Beschreibung
Secur Envoy	http://securenvoy.de	Secur Envoy	Tokenfreie 2-Faktor-Authentifizierung, um sichere Systemzugänge mit Hilfe eines Mobiltelefons zu erhalten (Secur Access), Kennwörter über ein Mobiltelefon abgesichert zurückzusetzen (Secur Password) oder um E-Mails sicher zu übertragen (Secur Mail)
Prosoft	www.prosoft.de/produkte/securaccess	Secure Access	Tokenfreie 2-Faktor-Authentifizierung mit Hilfe von Mobiltelefonen und Tablets. Dabei werden alle E-Mails und Kennwörter verschlüsselt
Safenet	www.safenet-inc.com/multi-factor-authentication	Multi-Factor Authentication (MFA)	Multi-Faktor-Authentifizierung mit drei Faktoren: Informationselement (Name/PIN, Kennwort), Element, das nur dem Benutzer zur Verfügung steht (Token/Smartcard), und persönliche Zusatzinformation (biometrische Daten/Fingerabdruck). Die Lösung kann als Webdienst in der Cloud genutzt werden
Computent	www.computent.de/computent-secure/2-factor-authentication-2-faktor-authentifizierung	Computent Secure Box	Der erste Faktor besteht aus Benutzername und Kennwort, der zweite Faktor ist ein USB-Stick. Eine Hardware-Komponente namens Secure Box sorgt für die verschlüsselte Anbindung zum Router
RC Devs Security Solutions	www.rcdevs.com/products/openotp	Open OTP Authentication Server	Serverbasierte Authentifizierungsplattform mit webbasiertem Verwaltungszugang. Sie unterstützt softwarebasierte Tokens, die auf Smartphones übertragen werden. Für bis zu 40 Benutzer ist der Einsatz kostenfrei
Optimal	www.optimal.de/produkte/dualshield	Dual Shield	Unterstützt den Einsatz von Hardware- und Software-Tokens sowie viele Systemplattformen. Über ein ausgeklügeltes Rechtesystem lassen sich Zugriffsfunktionen detailliert festlegen



Google-Dienste: Anwender, die ihr Google-Konto besser schützen wollen, können eine 2-Faktor-Authentifizierung aktivieren.

Fehlermeldung über eine gescheiterte Authentifizierung. Fordern Sie dann eine neue PIN an. Erst wenn beide Zugangsinformationen als gültig erkannt sind, ist der benötigte Identitätsnachweis für den Zugang zum Demo-System erbracht.

Beachten Sie, dass im Beispielprogramm übertragene Mails der Einfachheit halber nicht verschlüsselt werden. Inhalte der verschickten Mails können also ausgespäht werden. Falls Sie eine Verschlüsselung einbauen wollen, bietet .NET aber bereits alle wichtigen Grundfunktionen dafür an, und zwar über den Namespace „System.Security.Cryptography“.

Fazit

Die 2-Faktor-Absicherung ist, das zeigt bereits das Beispielprogramm, einfach durch Entwickler in eigenen Lösungen, Webdiensten oder Servern nachzurüsten. Und Unternehmen, die sich nicht selbst darum kümmern wollen, finden mittlerweile leistungsfähige Lösungen unterschiedlicher Anbieter.

Erfreulich ist, dass immer mehr der großen Webfirmen wie Google, Microsoft, LinkedIn, Evernote, Twitter, Dropbox und Last Pass ihren Nutzern eine 2-Faktor-Authentifizierung anbieten. Weniger schön ist, dass die 2FA im Regelfall nicht standardmäßig aktiv ist, sich also der Nutzer selbst darum kümmern muss, dass sie eingeschaltet wird.

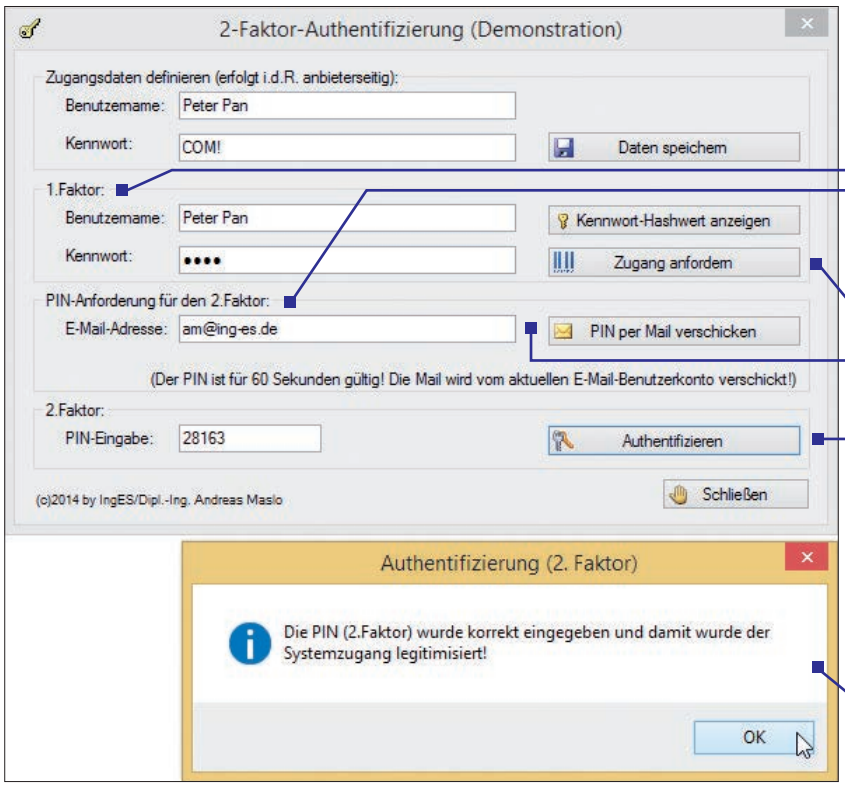
Aber auch wenn 2FA den Zugangsschutz erhöht, sollte sich kein Nutzer in Sicherheit wiegen: Nicht einmal mehrstufige Authentifizierungen sind hundertprozentig sicher – auch wenn das Umgehen von Retina-Scans und Fingerabdrucksensoren viel komplizierter ist als in Hollywoodfilmen.

Realistischer ist die Gefahr, die von einem Diebstahl oder dem Verlust der Hardware-Tokens ausgeht. Bei der tokenlosen 2FA wiederum gilt zu beachten, PINs/TANs nicht nur dynamisch und befristet zu generieren, sondern auch nur über verschlüsselte Datenverbindungen zu übertragen. Nur so wird das Abfangen und schnelle Entschlüsseln der Zugangsdaten unterbunden. ■

Andreas Maslo/js
js@com-professional.de

Demo-Programm: 2FA zum Ausprobieren

Das Beispielprogramm von der Heft-DVD versendet Zugangs-Tokens per E-Mail an stationäre und mobile Geräte.



1 1. Faktor
Der erste Authentifizierungsfaktor besteht aus Benutzername und Kennwort.

2 2. Faktor
Der zweite Authentifizierungsfaktor ist eine fünfstellige Zahlenfolge (PIN).

3 Zugang anfordern
Hier starten Sie die erste Stufe der Authentifizierung mit Benutzername und Kennwort.

4 PIN-Anforderung
An die hier eingetragene E-Mail-Adresse wird die temporär gültige PIN gesendet.

5 Authentifizieren
Nachdem Sie die PIN erhalten und eingetragen haben, lösen Sie hier die Authentifizierung mit dem 2. Faktor aus.

6 System-Meldung
Wenn die 60 Sekunden lang gültige PIN korrekt eingegeben wurde, gibt das System eine Erfolgsmeldung aus.