NetIQ

Multifaktor-Authentifizierung:

Risiken senken und Abläufe vereinfachen

Passwörter haben einmal mehr ausgedient

Das althergebrachte Verfahren der Benutzerauthentifizierung mithilfe von Benutzernamen und Passwörtern ist nicht mehr praktikabel. Warum? Aus verschiedenen Gründen: Viele Benutzer gehen zu sorglos mit ihren Anmeldeinformationen um. Sie wählen offensichtliche Passwörter, nutzen dieselben Passwörter für verschiedene Anwendungen und notieren diese sogar leicht ersichtlich auf ihrem Schreibtisch. Aber es liegt nicht einzig und allein am Benutzer.

Da Benutzername und Passwort oftmals die einzigen Zugangsschlüssel sind, ist es für Hacker längst zur Routineaufgabe geworden, dieses Authentifizierungsmodell zu knacken. Intelligente Kriminelle schreiben ausgeklügelte Algorithmen und finden den Weg in Ihr System. Hat der Benutzer dann auch noch dasselbe Passwort für verschiedene Anwendungen eingesetzt, ist es für den Hacker ein Leichtes, sich mit dem geknackten Passwort auch zu anderen Bereichen Zugang zu verschaffen. So könnte z. B. ein Hacker, der in den Besitz des Facebook-Passworts eines Ihrer Benutzer gekommen ist, in alle Bereiche Ihrer Unternehmensinfrastruktur eindringen.

Das Fazit? Beim Einsatz von Benutzernamen und Passwörtern beruht der gesamte Authentifizierungsprozess einzig auf Informationen, die der Benutzer kennen muss. Und diese Informationen können abgefangen oder gestohlen werden.

Multifaktor-Authentifizierung (MFA) ist in aller Munde

Wie der Name vermuten lässt, werden bei der Zugangserteilung über MFA mehrere Identitätsquellen kombiniert. Aber nicht nur das. Die besten Methoden kombinieren sogar verschiedene *Typen* von Identitätsquellen. Im Idealfall werden bei der MFA drei Dinge kombiniert: etwas, das Sie *kennen* (z. B. eine PIN), etwas Physisches, das Sie *besitzen* (z. B. eine Schlüsselkarte oder ein Token), und etwas, das Ihre *Identität* nachweist (z. B. ein Fingerabdruck, ein Netzhautscan oder Spracherkennung). Indem Sie zwei dieser drei Identitätsquellen für den Zugang erforderlich machen, senken Sie das Risiko einer Sicherheitsverletzung deutlich.

Prinzipiell handelt es sich auch um MFA, wenn Ihre Bank nach Ihrer PIN und Ihrer Sozialversicherungsnummer fragt, weil dabei zwei Identitätsquellen (eine von der Bank, eine von einer anderen Institution) einbezogen werden. Allerdings ist dieses Szenario nicht besonders ausgereift, denn beide Authentifizierungsschlüssel beruhen auf etwas, das Sie *kennen*.

Das Konzept ist nicht neu

Neu ist nur die Implementierung. Die meisten Menschen machen im alltäglichen Leben bereits Gebrauch von der MFA. Bei der Benutzung eines Geldautomaten besitzen Sie eine Bankkarte und *kennen* Ihre PIN. Bei der Nutzung eines Kiosk-Check-in am Flughafen ziehen Sie Ihre Kreditkarte (etwas, das Sie besitzen) durch den Schlitz und geben den dreistelligen Code Ihres Zielflughafens (etwas, das Sie kennen) ein. Selbst das Vorzeigen Ihres Lichtbildausweises (der Ihre Identität nachweist) bei der Kreditkartenzahlung ist eine Form der Multifaktor-Authentifizierung.

Die Vorteile der MFA liegen auf der Hand. Ein System, das zwei verschiedene Formen der Authentifizierung verlangt, ist grundsätzlich sicherer, da ein Missbrauch ausschließlich vor Ort erfolgen kann. Der Hacker kann nicht mehr einfach aus der räumlichen Distanz Benutzernamen und Passwörter abgreifen: Er muss sich auch Zugriff auf etwas verschaffen, das Sie besitzen oder das Ihre *Identität* nachweist, bzw. er muss vortäuschen, über diese Schlüssel zu verfügen. Das ist nicht ganz so einfach.

Flash Point-Paper

Gründe für die Einführung der Multifaktor-Authentifizierung:

- *Einhaltung von Vorschriften*
- *Missbrauch*
- *Technologie-/Infrastruktur-Update*

Die MFA beruht im Idealfall auf mindestens zwei dieser drei Faktoren:

- **Etwas, das Sie kennen**
- **Etwas, das Sie besitzen**
- **Etwas, das Ihre Identität nachweist**

Was macht die MFA zum Trend?

Unternehmen werden sich zunehmend der Risiken und Kosten bewusst, die mit der Ein-Faktor-Authentifizierung beim Zugriff auf Online-Girokonten verbunden sind. Die MFA hingegen macht den elektronischen Zahlungsverkehr so einfach und verlässlich wie eine Barzahlung und könnte somit einen neuen, kostengünstigeren Trend setzen.

„Laut dem Verizon-Datenmissbrauchsbericht 2013, der die Ein-Faktor-Authentifizierung als Hauptursache für Sicherheitslücken ausmacht, waren 76 Prozent der unbefugten Netzwerkzugriffe im Jahr 2012 auf schwache oder gestohlene Passwörter zurückzuführen.“

Ein weiteres Argument für die MFA ist die Zunahme von gesetzlichen Vorschriften wie dem US-amerikanischen Gesetz über die Übertragbarkeit und Nachweispflicht von Krankenversicherungen (HIPAA). Am 26. März 2013 traten neue Vorschriften des US-amerikanischen Gesundheitsministeriums (Department of Health and Human Services) in Kraft, die die HIPAA-Anforderungen an Sicherheit und Datenschutz ausweiteten – und zwar auf Geschäftspartner (darunter Auftragnehmer, Lieferanten und Dienstleister wie z. B. Abrechnungsunternehmen), die Leistungen im Namen eines Gesundheitsdienstleisters oder Lösungen anbieten, bei denen medizinische oder patientenbezogene Daten verarbeitet werden. Da die Nichteinhaltung mit hohen Geldstrafen sanktioniert wird, erwägen zahlreiche Unternehmen nun die Einführung der MFA, um den Zugang zu medizinischen und patientenbezogenen Daten zu schützen.

Nicht zuletzt spricht auch für die MFA, dass biometrische Authentifizierungsmethoden bereits seit einiger Zeit Bestandteil vieler Geräte sind. Unternehmen, die mit Fingerabdruck-Scannern auf Smartphones und PCs arbeiten, verfügen somit längst über die Möglichkeit, die MFA zu implementieren. Dies ist ihnen jedoch oftmals nicht bewusst.

Warum wird die MFA angesichts dieser Vorteile nicht längst allseits eingesetzt?

Wie bei den meisten neuen Entwicklungen sträubt man sich auch hier aus verschiedenen Gründen gegen Veränderung. Viele Unternehmen sind sich nicht darüber im Klaren, dass sie bereits über die für die MFA erforderlichen Komponenten (z. B. Fingerabdruck-Scanner) verfügen. Eine weitere Sorge ist, dass im Rahmen der Neuimplementierung an Benutzerfreundlichkeit eingebüßt werden muss. Oftmals wird Benutzerfreundlichkeit mit Effizienz gleichgesetzt, weshalb Unternehmen sich weigern, bestimmte Workflows komplexer zu gestalten – selbst, wenn dadurch die Sicherheit auf der Strecke bleibt. Nicht zuletzt ist es für eine optimale Nutzung der MFA erforderlich, das Zugriffssystem im Backend einzurichten und zu optimieren. Wenn die eingehenden Informationen nicht angemessen verarbeitet und in das gesamte System eingebunden werden, wird Ihr Unternehmen die Vorteile der neuen Methode auch nicht voll ausschöpfen können.

Es ist an der Zeit, das Blickfeld zu erweitern

Bei der Einführung neuer Technologien kommt es dann zu Misserfolgen, wenn sich niemand Gedanken über die möglichen Auswirkungen gemacht hat. Bei der Einführung der MFA sollten Sie daher im Vorfeld Folgendes tun:

- Betrachten Sie die Benutzerauthentifizierung nicht als isolierte Anschaffung oder eingebetteten Teil eines Elements in Ihrem Sicherheitssystem. Entwickeln Sie Ihre eigene fundierte Authentifizierungsrichtlinie.
- Identifizieren Sie alle Orte, an denen die MFA zum Einsatz kommen wird (denken Sie daran, dass die MFA Ihre Zugangspolitik widerspiegelt und daher auch eingehend genutzt werden sollte!). Eliminieren Sie komplexe Verfahren wo immer dies möglich ist, indem Sie sicherstellen, dass die MFA

– **einfach zu verwalten ist.** Halten Sie den Verwaltungsaufwand gering und vermeiden Sie die Einführung mehrerer Authentifizierungssysteme für die diversen Systeme Ihres Unternehmens.
– **benutzerfreundlich ist.** Je geringer die Benutzerfreundlichkeit, desto höher ist der Widerstand der Anwender. Ziehen Sie daher die gleichzeitige Einführung einer Single Sign-on-Lösung in Betracht. Damit müssen sich die Benutzer nicht verschiedene Passwörter merken oder sich für jedes System erneut authentifizieren.

Wenn die MFA optimal implementiert ist, macht sie den Benutzern das Leben leichter, denn es ist sicher einfacher, mit dem Finger über einen Scanner zu fahren und eine PIN einzugeben, als sich einen Benutzernamen und ein Passwort zu merken.

Worauf Sie bei der Auswahl eines MFA-Anbieters achten sollten

Die Implementierung der MFA ist ein bedeutender Schritt auf Ihrem Weg zu mehr Sicherheit und Produktivität. Daher sollte sie sich gut in Ihre Geschäftsabläufe integrieren lassen.

1. Suchen Sie nach einer Lösung, die Ihnen Wahlfreiheit und Flexibilität bei der Art der Authentifizierung und ihrer Durchführung bietet.

2. Lassen Sie sich nicht auf eine Form der physischen Authentifizierung festlegen – Ihre Authentifizierungsstrategie sollte nicht von der gewählten Hardware abhängig sein.

3. Suchen Sie nach Anbietern, die in einem offenen Framework entwickeln, das bei der Einführung neuer Technologien unverzüglich aktualisiert wird.

4. Suchen Sie nach Anbietern, die Ihnen ein einfach zu handhabendes System bereitstellen.

Ihr MFA-Anbieter sollte eine Lösung zur Verfügung stellen, die zahlreiche Anwendungen abdeckt, Plugins unterstützt und sich problemlos integrieren lässt. Die Implementierung sollte unter enger Einbeziehung eines Identitätsmanagementsystems erfolgen, und es sollten Verfahren zur Erhöhung der Benutzerfreundlichkeit, z. B. Single Sign-on, eingesetzt werden.

Da die Sicherheitsrisiken bei der Online-Authentifizierung zunehmen, müssen Sie sich als Unternehmen dieser Herausforderung stellen oder andernfalls mit den möglichen Konsequenzen rechnen.

Weitere Informationen finden Sie auf **www.netiq.com**.

www.netiq.com

NetIQ
Deutschland
Fraunhoferstr. 7
85737 Ismaning
Tel: +49 (0)89 420940
Email: infoDE@netiq.com

Schweiz
Flughafenstrasse 90
P.O. Box 253 8058 Zürich
Tel: +41 (0)43 456 2400
Email: infoCH@netiq.com

info@netiq.com
www.netiq.com/communities
www.netiq.com

Die vollständige Liste unserer Niederlassungen in Nordamerika, Europa, Nahost, Afrika, Lateinamerika sowie im asiatisch-pazifischen Raum finden Sie unter: www.netiq.com/contacts

www.netiq.com