VIER AUTHENTIFIZIERUNGSARTEN DIE JEDER SICHERHEITSPROFI KENNEN SOLLTE

Wie kann die IT-Abteilung gewährleisten, dass ein Benutzer wirklich die Person ist, für die er sich ausgibt?

ETWAS, DAS **MAN WEISS**

D.h. Passwörter, PINs, Muster, Passcodes und andere Verifizierungsmittel, die auf Informationen basieren, die nur der Benutzer kennen sollte. Passwörter sind das wichtigste Mittel zur Überprüfung der Benutzeridentität, seit Datenschutz notwendig wurde.

VORTEILE

Die Benutzer sind sie gewohnt; keine spezielle Hardware erforderlich; fast alle Anwendungen akzeptieren sie.

NACHTEILE

Leicht zu hacken durch Social Engineering, Phishing, schlechte Passwort-Hygiene und Brute-Force-Angriffe. Zudem müssen die Benutzer mehrere einzigartige, komplexe Passwörter erinnern und richtig schützen; und die IT-Admins müssen sie zurücksetzen, wenn sie vergessen wurden.

ETWAS, DAS **MAN HAT**

D.h. eine Smartcard, ein Token, eine virtuelle Smartcard – ein physischer Gegenstand, den nur der Benutzer besitzt und der während des Authentifizierungsprozesses verwendet wird.

VORTEILE

Kann in der Regel nur gehackt werden, wenn der Angreifer physischen Zugriff auf die Smartcard oder das Token hat. Bei PKI-basierter Authentifizierung werden keine Passwörter oder PINs über das Netzwerk übertragen. Smartcard-Technologien sind seit mehr als einem Jahrzehnt im Einsatz und sind eine bekannte, bewährte Strategie.

NACHTEILE

Der Benutzer muss den Überblick über die verschiedenen Hardwarekomponenten für die einzelnen Dienste behalten. Die IT muss diese bei Verlust ersetzen. Zusatzkosten für Beschaffung und Ersatz.

VIRTUELLE SMARTCARD: Gehört zu dem, „was Sie haben“; funktioniert wie herkömmliche Tokens oder Smartcards, ist aber in den PC, das Laptop, Tablet oder Telefon eingebettet.

VORTEILE

Da die Benutzer keine Extra-Komponenten brauchen, sind die Verwaltungskosten erheblich geringer. Basiert auf einer branchenüblichen Hardware, die in die meisten Unternehmensgeräte bereits integriert ist; daher keine Beschaffungskosten für Smartcards und Smartcard-Reader.

NACHTEILE

Die virtuelle Smartcard ist mit einem bestimmten Gerät verbunden und nur zur Authentifizierung über einen einzigen Endpunkt verwendbar

ETWAS, DAS **MAN IST**

D.h. ein biometrisches Merkmal. Ein Benutzer authentifiziert sich mittels eines Fingerabdrucks, seiner Stimme, seiner Iris oder eines anderen einzigartigen körperlichen Merkmals.

VORTEILE

Praktisch – nichts mitzutragen oder zu erinnern.

NACHTEILE

Kann gefälscht werden und falsch positive/negative Ergebnisse erbringen. Weniger standardisiert als andere Lösungen. Erfordert zusätzliche Lesegeräte, Scanner und Support. Hohe Beschaffungs- und Wartungskosten. Kann nicht entzogen werden, ohne dem Benutzer das biometrische Merkmal zu entziehen.

ZWEI-FAKTOR-**AUTHENTIFIZIERUNG**

Jede Kombination aus zwei dieser drei Authentifizierungsformen: etwas, das man weiß; etwas, das man hat; und etwas, das man ist. Zwei-Faktor-Authentifizierung ist eine empfohlene Best Practice zum Schutz sensibler Daten und Ressourcen und bei der Verarbeitung bestimmter Arten von Daten gesetzlich vorgeschrieben.

VORTEILE

Hacker müssen zwei Schutzschichten knacken, was einen erfolgreichen Angriff erheblich erschwert. Verringert die Abhängigkeit von Passwörtern, verbessert das Benutzererlebnis und senkt letztlich die Kosten.

NACHTEILE

Kosten und Komplexität – Unternehmen müssen mehr als eine Form von Authentifizierung implementieren und verwalten. Die Ausnahme sind dabei virtuelle Smartcards, die auch ein Passwort umfassen und daher nureine einzige Implementierung benötigen, um Zwei-Faktor-Authentifizierung zu erreichen.

wave®