LU03f - Zwei-Faktor Authentifizierung

Internal reference: lu/03-6.md

Einführung

Die **Zwei-Faktor-Authentifizierung** ist eine Sicherheitsprozedur, bei der ein Anwender **zwei unterschiedliche Merkmale** bereitstellt, um sich zu identifizieren. Eines der Merkmale ist meist ein **physischer Token**, wie eine Karte, während das andere beispielsweise ein Sicherheitscode ist, den sich der Anwender merken muss.

Beispiel

Ein typisches Beispiel für eine Zwei-Faktor-Authentifizierung sind Smartcards: Die Karte selbst ist der physische Gegenstand, während die PIN (persönliche Identifizierungsnummer) die dazugehörige Information ist. Die Kombination beider macht es einer fremden Person schwieriger, auf das Bankkonto des Nutzers zuzugreifen, weil dazu beide Elemente benötigt werden, also der physische Gegenstand sowie die PIN.

Vergleich Ein-Faktor- vs. Zwei-Faktor-Authentifizierung

Obwohl Benutzernamen und Passwörter zwei Merkmale sind, gehören sie doch zu demselben Authentifizierungsfaktor (Wissen), sie sind also eine **Ein-Faktor-Authentifizierung**. Es liegt an ihren geringen Kosten, der einfachen Implementierung und ihrem Bekanntheitsgrad, dass Passwörter bis heute die häufigste Form der Ein-Faktor-Authentifizierung sind. Sie sind aber nicht am sichersten. Erweiterte Anforderungen können für mehr Sicherheit sorgen, je nachdem wie sie genutzt werden. So garantieren viele biometrische Identifizierungsverfahren bereits als Standalone-Lösungen für mehr Sicherheit, selbst bei Ein-Faktor-Authentifizierungen.

Vorteil der Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung kann Identitätsdiebstahl, Phishing-Angriffe und anderen Online-Betrugsversuche reduzieren, weil es nicht ausreicht, das Zugangsgerät des Opfers zu klauen. Der Dieb benötigt auch die dazugehörige Information, eben beispielsweise die PIN – oder umgekehrt.

Nachteil der Ein-Faktor-Authentifizierung

Ein Problem der Passwort-basierten Authentifizierung ist außerdem, dass sie sowohl Wissen als auch Gewissenhaftigkeit erfordert, um sichere Passwörter zu erstellen und sich zu merken. Passwörter benötigen zudem einen Schutz vor vielen Insider-Gefahren. Dazu gehören achtlos weggeworfene gelbe Zettelchen, alte Festplatten und Social-Engineering-Attacken. Passwörter sind außerdem durch externe Hacker-Angriffe per Brute-Force-, Wörterbuch- oder Rainbow-Table-Attacken bedroht. Vorausgesetzt ein Angreifer hat genug Zeit und Ressourcen, dann kann er Passwort-basierte Systeme normalerweise knacken. Die Zwei-Faktor-Authentifizierung sorgt hier für zusätzliche Sicherheit.

Multi-Faktor-Authentifizierung für sicherere Verbindungen

Manche Sicherheitsprozesse erfordern mittlerweile eine **Drei-Faktor-Authentifizierung**, die beispielsweise aus einem Hardware-Token, einem Passwort und biometrischen Daten wie Finger abdrucken oder einer Stimmerkennung bestehen kann.

Einem Angreifer kann es etwa gelingen, einen einzelnen Authentifizierung-Faktor zu knacken. So kann eine gründliche Suche im Umfeld des Opfers beispielsweise zum Fund eines Mitarbeiterausweises oder einer Benutzerkennung samt zugehörigem Passwort führen, die im Müll gelandet sind. Oder eine unachtsam entsorgte Festplatte enthält eine Passwortdatenbank. Wenn jedoch weitere Faktoren zur Authentifizierung erforderlich sind, steht der Angreifer vor mindestens einer weiteren Hürde, die er umschiffen muss.

Der Großteil der heutigen Angriffe erfolgt über Internetverbindungen. Zwei-Faktor-Authentifizierung kann diese Distanzattacken weit weniger gefährlich machen, weil das reine Knacken des Passworts nicht mehr ausreicht, um Zugriff zu erhalten. Denn es ist sehr unwahrscheinlich, dass der Angreifer auch in den Besitz des physischen Geräts gelangt, das mit dem Benutzer-Account verknüpft ist. Jeder zusätzliche Authentifizierung-Faktor macht ein System also sicherer. Das liegt daran, dass die einzelnen Faktoren unabhängig voneinander sind. Sollte einer der Faktoren kompromittiert werden, betrifft das die anderen nicht.

Quelle: http://www.searchsecurity.de/definition/Zwei-Faktor-Authentifizierung, Zugriff 23.11.2017