Sicherheit im Netz

07.12.2019 08:37:32 | AH-WEB | 0 Kommentare

Passwörter waren gestern und was ist heute und morgen? Mails checken, online shoppen, Cloud-Applikationen öffnen oder über Bezahldienste Finanztransaktionen abwickeln: Erstaunlich oft ist dabei nach wie vor die überholte Kombination von User-Name und Passwort gefragt. Bei vielen Menschen ist das aus Bequemlichkeit immer die gleiche Eingabe. Zeitgemäß ist diese Verifizierungsmethode aber nicht.

Jedes Mal, wenn Nutzername und Passwort eingegeben werden, bieten sich Hackern Gelegenheiten, die Daten abzugreifen. Die Tendenz geht deshalb hin zu passiver Authentifizierung und Zero Login. Das verspricht einerseits hohe Benutzerfreundlichkeit und andererseits mehr Schutz vor Passwort-Spähern. Aber Vorsicht, es gibt auch Schattenseiten.

Der Status quo

Wer einen neuen Online-Account anlegt und ein Passwort festlegen soll, kennt den Prozess: Während der Eingabe der Zeichenreihe signalisiert eine Anzeige in Ampelfarben, ob ein Kennwort dem System als halbwegs sicher gilt. Andere Dienste verlangen zur Verifizierung einfach, die gewählte Zeichenfolge nochmals einzugeben, sehen im Zweifel Überprüfungsfragen vor und dergleichen mehr. Auch wenn solche Minimal-Mechanismen zur scheinbaren Identitätsüberprüfung eingesetzt werden, bleibt es bei der aktiven Authentifizierung. Und diese bietet Spähern bei jedem Eintippen aufs Neue Gelegenheiten zum Zugreifen.

Liegen die Zugangsdaten erst einmal dem Anbieter eines Webshops, Cloud-Dienstes, Bezahlservice oder Ähnlichem vor, sind sie noch immer nicht unbedingt sicher. Die Datenschutz-Panne von Twitter aus dem diesjährigen Frühsommer illustriert das. Der Social-Media-Dienst musste eingestehen, dass aufgrund eines Systemfehlers die Passwörter seiner Nutzer unverschlüsselt in einer internen Datenbank gelagert waren. Damit lagen sie nicht nur für Mitarbeiter, sondern auch für potenzielle Cyber-Angreifer offen.

Anmelden, ohne sich anzumelden

Was aber folgt auf die anfälligen reinen Zeicheneingaben? Zero Login heißt die aktuelle Richtung, das heißt im Grunde: Anmelden, ohne sich anzumelden. Wie funktioniert das in der Praxis? Einige Geräte sind bereits per Design darauf ausgelegt, anders zu verfahren als mit Zeicheneingaben zur Authentifizierung. Smartphones etwa, die mit hochauflösenden Kameras, Scanner-Apps oder berührungsempfindlichen Oberflächen biometrische Verfahren unterstützen. Darunter fallen beispielsweise Fingerabdruck, Gesichtserkennung, Iris-Scan und so weiter. Standort-, Bewegungs- und Geodaten-Analyse von Mobilgeräten oder typische Muster im Tippverhalten können dazukommen.

Apple bietet beispielsweise schon seit dem iPhone 5s mit der Entsperrungsfunktion per Fingerprint eine Möglichkeit der passwortlosen Identifizierung. Bei neueren Modellen ab dem iPhone 7 kann zudem der Klickwiderstand des Home-Buttons individuell angepasst werden. Zwar dient das in dem Fall nur der Nutzerfreundlichkeit, stellt aber bereits einen Schritt in Richtung Verhaltensanalyse dar.

Mit dem iPhone X kam dann die Einführung der Face ID-Funktion. Die Gesichtserkennung ermöglicht seither nicht nur die Entsperrung des Geräts, sondern auch das Öffnen von Apps, das automatische Ausfüllen von Benutzername sowie Passwort im Netz und sogar Bezahlvorgänge via Apple Pay.

Neben diesen Funktionen speichert und "erinnert" sich das iPhone an Signale von weiteren Geräten, wie etwa vom Auto oder von Fitness-Trackern, die üblicherweise in territorialer Nähe verortet sind. Es deutet sich eine Entwicklung hin zu mobilen Devices an, die einen Anwender erkennen, sobald er das Gerät nur in die Hand nimmt.
Mehrfaktoren- und adaptive Authentifizierung

Amazon sieht zum Beispiel das typische Verhalten eines Kunden als einen Aspekt der Multi-Faktor-Authentifizierung (MFA). Individuell typischer Druck auf die Oberfläche beim Bedienen eines Mobilgeräts etwa, übliche Standortdaten oder auch die Tippgeschwindigkeit können aussagekräftige Parameter für eine Authentifizierung sein. Derartige Charakteristika zu replizieren - zumal in Kombination der einzelnen Bausteine - ist für Betrüger, die es auf Identitätsklau oder -manipulation abgesehen haben, kaum darstellbar.

Weicht innerhalb eines MFA-Prozesses das Verhalten des aktuellen Users von der Norm ab, passiert das, was bereits vom Online-Banking bekannt ist, wenn beispielsweise eine auffällige Transaktion, eine Abhebung im Ausland oder eine Anmeldung über ein fremdes Gerät stattfindet. Der Kunde erhält eine Benachrichtigung und wird in der Regel zu einer zusätzlichen Authentifizierung aufgefordert. Allerdings gilt es hierbei häufig wieder ein Passwort einzugeben oder eine Sicherheitsfrage (schriftlich) zu beantworten.

Neue Faktoren der Identifikation verbessern die Sicherheit der Authentifizierung. Allerdings stellen sich auch Fragen, wohin sich die Technologie entwickeln kann: Wenn die Geräte unser Verhalten registrieren, Informationen über uns sammeln, sie transportieren und eventuell zur Verbesserung eines Algorithmus an eine KI-Engine weitergeben - kann dann nicht auch eine Software entscheiden, was überhaupt einer Authentifizierung unterliegt? Und auf welchem Level? Wird eine Authentifizierung benötigt, wenn man beispielsweise nur eine Terminzusage verschickt?

Zum Teil finden solche adaptiven Authentisierungstechnologien schon jetzt Verwendung. Dabei wird eine Matrix an Variablen zusammengefasst und daraus ein Profil erstellt, das Risiken einschätzt und je nach Situation zum Handeln auffordert. In der Folge könnten adaptive Technologien ermöglichen, dass das Gerät über die Notwendigkeit einer weniger- oder mehrschichtigen Identitätsüberprüfung entscheidet.

Läuft die Authentifizierung in risikoarmen Fällen einfach im Hintergrund, erhöht sich das Nutzererlebnis. Fällt die Risikobewertung hoch aus, muss die Authentifizierung durch mehrere Faktoren erfolgen, was auch das Sicherheitsmanagement eines Unternehmens verbessern kann.

Klärungsbedarf bei Schutz und Handhabung biometrischer Daten

Soweit klingt das alles ganz praktisch. Keine versteckten Zettel mit unzähligen verschiedenen Passwörtern für verschiedene Accounts mehr. Kein Chaos und keine E-Mails, weil das Passwort vergessen wurde. Aber die neuen Trends werfen auch Fragen auf, die künftig von immer größerer Bedeutung sind und noch nach Klärung verlangen. Ein kritischer Aspekt ist beispielsweise der Datenschutz.

Was passiert auf Dauer mit Identifikationsdaten über Verhalten, Standorte, benachbarte Devices und Co.? Wie erkennt ein Benutzer, dass er nicht ohne sein Wissen auf sein Verhalten hin geprüft wird? Durch biometrische Daten wird das Bild, das vom Konsumenten gezeichnet wird, noch detaillierter. Gerade die Tatsache, dass neue Identifikations-Indikatoren eben deshalb so wirksam sind, weil sie personenbezogen sind, machen diese Fragen besonders sensibel.

Zusätzlich zur Technologie, zur Verarbeitung von Bild-, Ton- und Sensordaten oder zur Leistungsfähigkeit von KI-Engines, die in Echtzeit mit dutzenden Faktoren operieren und dabei selbstlernend immer präziser werden, müssen daher auch konsequente Bewusstseinsbildung in Unternehmen und fundierte Big-Data-Strategien bei IAM-Herstellern kommen. Das Verständnis, dass Daten nicht nur Informationen sind, sondern extrem sensible Einsichten über Personen liefern und dass deren Schutz im Vordergrund steht, muss sich auf Seite der Anbieter entwickeln. Dies muss wiederum von legislativer Seite durch klare Regulierungen gefordert sein.