IBM Security

Digitale Identitäten: Anleitung zur optimierten Abwägung von Risiko und Benutzererlebnis mit adaptivem Zugriff

Die Macht der Identität

Unsere digitalen Identitäten sind von grundlegender Bedeutung für unsere Interaktion mit anderen und mit der Onlinewelt.[1] Wenn wir nachweisen können, wer wir sind, erhalten wir Kontrolle und Zugang zu Personen, Informationen und Vorteilen. Digitales Vertrauen in diese Identitäten ist Macht.

Es kann jedoch schwierig sein, eine vertrauenswürdige digitale Identität zu schaffen. Es handelt sich dabei um ein komplexes Netzwerk von traditionellen Instrumenten der Identifizierung wie Name, Adresse, Geburtsdatum und Sozialversicherungsnummer sowie Datenpunkten wie E-Mail-Adresse, Benutzername und Kennwort, Suchgewohnheiten, Kaufverhalten und mehr.

Diese personenbezogenen Daten bestehen aus den eindeutigen Merkmalen, die einer Person zugeordnet sind, und öffnen die Tür zu jeder Onlineinteraktion. Diese Aktionen sind auf Kontext zur Identitätserkennung angewiesen.

Je mehr diese Interaktionen zunehmen, desto größer werden jedoch die Sicherheitslücken.[2] Angreifer finden ständig neue Wege, um personenbezogene Daten dafür zu nutzen, Identitäten zu stehlen oder an wertvolle Daten von Unternehmen zu gelangen. Im Jahr 2018 erhöhte sich die Zahl der kompromittierten Kundendatensätze mit sensiblen personenbezogenen Daten um 126 %.[3] Im Jahr 2019 stiegen die Kosten einer Datenschutzverletzung auf fast 4 Mio. US-Dollar.[4]

Das Problem wird aufgeschoben

Das Problem: Viele verstehen das Konzept der Cybersicherheit nicht genau[5] und zahlreiche Unternehmen schützen geschäftskritische Anwendungen nach wie vor nur per Benutzername und Kennwort, obwohl es eine bessere Möglichkeit gibt. Die Mehrfaktorauthentifizierung (MFA) sorgt für eine zusätzliche Ebene der Sicherheit und macht es Unbefugten viel schwerer, sich Zugriff zu verschaffen. Also warum verschließen alle die Augen vor dem Problem und schieben die Lösung auf die lange Bank?

Nur ein Bruchteil der Unternehmen nutzt die Mehrfaktorauthentifizierung, obwohl sie sicherer ist und ihre Nutzung laut Prognosen zunehmen wird.

Sie glauben häufig (irrtümlich), dass das Risiko, Endbenutzer, Mitarbeiter und Kunden zu frustrieren, größer ist als das Risiko einer Datensicherheitsverletzung. Nur ein Bruchteil der Unternehmen nutzt die Mehrfaktorauthentifizierung, obwohl sie sicherer ist und ihre zunehmende Nutzung prognostiziert wurde. Gartner schreibt: „Bis 2022 werden 60 % der Implementierungen für das Zugriffsmanagement UEBA-Funktionen (User and Entity Behavior Analytics) für die Analyse des Verhaltens von Benutzern und Systemen und weitere Kontrollmechanismen für die kontinuierliche Authentifizierung, Autorisierung und Erkennung von Onlinebetrug verwenden – heute sind es weniger als 10 %."[6]

KERNPUNKT

Nur ein Bruchteil der Unternehmen nutzt die Mehrfaktorauthentifizierung, obwohl sie mehr Sicherheit bietet und ihre Nutzung laut Prognosen zunehmen wird.

Benutzererlebnis versus Sicherheit

Durchschnittliche Geschäftsanwender managen 191 Kennwörter[7] – in der Regel eher schlecht, da sie dasselbe Kennwort immer und immer wieder verwenden. Falls diese enorme Zahl noch nicht ärgerlich genug ist, versuchen Sie, sie zum Warten auf einen Text oder eine E-Mail mit einem Code für die Anmeldung zu bewegen.

Oder bitten Sie sie, Bilder mit Autos oder Verkehrsampeln zu identifizieren, wenn die meisten Bilder scheinbar beides enthalten. Schicken Sie ihnen dann eine weitere E-Mail, die sie vor dem Zugriff warnt, für den sie gerade mehrere Schritte durchlaufen haben – immer vorausgesetzt, dass sie überhaupt so weit kommen. Nur 28 % der Erwachsenen in den USA können ein Beispiel einer Zwei-Faktor-Authentifizierung nennen.[8]

Wenn Sie diesen mühseligen Prozess auch auf Kunden anwenden, werden Sie sie möglicherweise nie wiedersehen. Das Kundenerlebnis ist heute ein entscheidender Wettbewerbsfaktor. Wer Kunden wie Cyberkriminelle behandelt, schadet seinem Geschäftsergebnis.

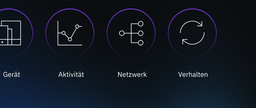
Das Zugriffsmanagement muss keine Entweder-oder-Entscheidung sein. Die Mehrfaktorauthentifizierung ist nicht umständlich, wenn sie intelligent ist. Die Benutzerfreundlichkeit und Sicherheit können optimiert werden, wenn eine Sicherheitslösung unbemerkt im Hintergrund arbeitet und Kontext über die Benutzer und ihr Verhalten erfasst. Sie nutzt dann diesen Kontext, um den richtigen Authentifizierungsprozess für die jeweilige Situation bereitzustellen – und schafft so ein reibungsloses, anpassungsfähiges Erlebnis.

KERNPUNKT

Nur 28 % der Erwachsenen in den USA können ein Beispiel einer Zwei-Faktor-Authentifizierung nennen.[8]

Mehr Freiheit für Benutzer

Mit einem Zugriffsmanagement, das die Mehrfaktorauthentifizierung nur dann einsetzt, wenn Risiken erkannt werden, können Sie Ihren Benutzern ein reibungsloses Erlebnis bieten. Für Vertrauen sorgt ein durchgehender Kontext, der beim Benutzer beginnt und bis zu dem Gerät, der Aktivität, der Netzwerkumgebung und dem Verhalten des Benutzers reicht.



Trust-Scoring

Die KI-basierte Risikoerkennung verwendet Modelle für maschinelles Lernen, um Kontext auf Mobilgeräten, in Webskripten und VPNs zu kombinieren, basierend auf Kriterien wie bekannten Betrügern, Malwareinfektionen und weiteren Anomalien, und dann in Szenarien mit hohem Risiko automatisch die Mehrfaktorauthentifizierung zu empfehlen.

Die Kontextanalyse kombiniert sowohl positive als auch negative Faktoren, um einen einzelnen Indikator für Vertrauen zu erstellen. Durch diesen Wert (Trust-Score) können Sie von einer Alles-oder-nichts-Strategie zu einem stärker nuancierten Verständnis vom Maß des Vertrauens zwischen Ihnen und Ihren Benutzern übergehen. Diese Flexibilität bildet die Grundlage einer Strategie des adaptiven Zugriffs.

Sobald Sie einen Trust-Score haben, müssen Sie keine statischen Regeln mehr für die Authentifizierung verwenden. Stattdessen können Sie eine intelligente Authentifizierungsstrategie entwickeln, die vertrauenswürdigen Benutzern frustrationsfreien Zugriff bietet und den Zugriff mit steigendem Risiko einschränken kann. Mit diesem Ansatz profitieren Benutzer, die ein geringes Risiko darstellen, von einem kennwortlosen Benutzererlebnis und erhalten Zugriff, ohne dass manueller Aufwand für die Prüfung ihrer Identitäten nötig ist.

Die intelligente Authentifizierung ermittelt Folgendes:

- Ist der Benutzer ein Mensch oder ein Bot?
- Gibt es Anzeichen böswilliger Absichten?
- Ist das Mobiltelefon ein Prepaid-Gerät? Ist es per Rooting oder Jailbreak manipuliert?
- Verfügt es über eine legitime Telefonnummer oder E-Mail-Adresse?
- Sind böswillige Muster feststellbar?
- Wurde die Out-of-Band-Authentifizierung umgangen?
- Existiert ein Anmeldeproxy?
- Ist das Benutzerverhalten bekannt?
- Wirken Mausbewegungen ungewöhnlich oder automatisiert?

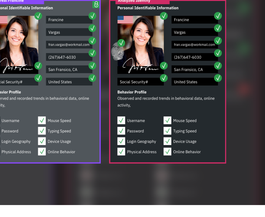
KERNPUNKT

Die Kontextanalyse kombiniert sowohl positive als auch negative Faktoren, um einen einzelnen Indikator für Vertrauen zu erstellen.

Trust Scoring: So funktioniert es

Beispielsweise erhält ein Benutzer mit einigen geringfügigen Anomalien Zugriff, wobei gewisse Einschränkungen bei Transaktionen oder Aktivitäten gelten. Benutzern, die hohes Vertrauen genießen, bekannte Geräte nutzen und positive Verhaltensbiometriewerte aufweisen, könnte ohne Kennwort Zugriff gewährt werden.

Sehen Sie sich die Demo an



Das Versprechen von adaptivem Zugriff

Statische Regeln legen die Messlatte für die Verifizierung zu niedrig oder zu hoch. IBM Cloud Identity mit adaptivem Zugriff ist eine Plattform für das intelligente Zugriffsmanagement. Sie kombiniert die innovative Risikoerkennung mit einer zuverlässigen Richtlinien-Engine, um den vollständigen Kontext der Identität eines Benutzers zu prüfen, der versucht, auf einen digitalen Service zuzugreifen. So kann das Versprechen eines frustrationsfreien digitalen Erlebnisses erfüllt werden, ohne auf die notwendige Sicherheit zu verzichten.

IBM Cloud Identity mit adaptivem Zugriff hilft Unternehmen, die Schwierigkeiten haben, die Risikobegrenzung und Benutzerfreundlichkeit bei Identitäten zu optimieren. Die Lösung vereinfacht die Authentifizierung durch Bereitstellung des frustrationsfreien, intelligenten Zugriffs auf Anwendungen und Daten.

Die Lösung lässt sich problemlos ohne oder mit nur geringem Codieraufwand über eine API für kundenspezifische Anwendungen und vordefinierte Vorlagen für häufig verwendete Cloud-Apps in Anwendungen integrieren.

KERNPUNKT

IBM Cloud Identity mit adaptivem Zugriff hilft Unternehmen, die Schwierigkeiten haben, die Risikobegrenzung und Benutzerfreundlichkeit bei Identitäten zu optimieren. Die Lösung vereinfacht die Authentifizierung durch Bereitstellung des frustrationsfreien, intelligenten Zugriffs auf Anwendungen und Daten.

Die Authentifizierung sollte intelligenter sein. Eine intelligente Authentifizierung passt sich an.

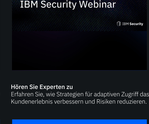
Weitere Schritte

Erfahren Sie mehr
Entdecken Sie drei unterschiedliche Möglichkeiten, mit denen Sie Ihr Identitäts- und Zugriffsmanagement verbessern können.

Lesen Sie den Blogbeitrag

Sehen Sie sich die interaktive Demo an
Sehen Sie, wie IBM Cloud Identity mit adaptivem Zugriff in der Praxis funktioniert.

Sehen Sie sich die Demo an



Hören Sie Experten zu
Erfahren Sie, wie Strategien für adaptiven Zugriff das Kundenerlebnis verbessern und Risiken reduzieren.

Nehmen Sie an dem Webseminar teil

Quellen

1. IBM, Digital identity management: How much of your personal information do you control?
2. IBM Institute for Business Value, Trust me: Digital identity on blockchain, April 2017
3. Identity Theft Resource Center, Consumers At Risk: 126% Increase In Exposed Consumer Data, 1.68 Billion Email-Related Credentials, 28. Januar 2019
4. IBM, Cost of a Data Breach, 2019
5. Pew Research Center, What the Public Knows About Cybersecurity, Aaron Smith, 22. März 2017
6. Gartner, 2019 Magic Quadrant for Access Management, Abhyuday Data, Michael Kelley, Henrique Teixeira
7. Security Magazine, Average Business User Has 191 Passwords, 6. November 2017
8. Pew Research Center, Americans and Digital Knowledge, Monica Anderson und Emily Vogels, 9. Oktober 2019

IBM