nevis®

Making security an experience

White Paper

Credential Stuffing

Credential Stuffing hat sich aufgrund der cleveren Automatisierungsmöglichkeiten in den letzten Jahren zu einer der bevorzugten Methoden von Cyber-Kriminellen entwickelt. Lesen Sie, was Credential Stuffing so gefährlich macht und wie Sie sich dagegen schützen können.

Inhalt

Einleitung

Jedes Unternehmen und jede Behörde hat das Ziel, seinen Kunden ein einzigartiges, individuelles und sicheres User-Erlebnis zu bieten. Aus gutem Grund: Hoher Komfort beim Zugang zum Online-Benutzerkonto und zu den damit verbundenen Services fördert die Kundenbindung und stärkt den wirtschaftlichen Erfolg. Daneben muss aber auch dafür gesorgt sein, dass die Sicherheit individueller User-Accounts zu jeder Zeit gewährleistet bleibt.

Leider ist der optimale Schutz der Benutzerdaten von Online-Konten in vielen Fällen nach wie vor nicht gegeben. Ein Grund dafür liegt oft im Fehlen wirkungsvoller Sicherheitsmassnahmen bei der Nutzer-Authentisierung. Aber auch die User selbst nehmen den Schutz ihrer persönlichen Anmeldedaten in vielen Fällen nicht ernst genug – und gehen damit ein unnötiges Risiko ein.

In den letzten Jahren hat sich Credential Stuffing deshalb zu einer der effektivsten Methoden von Cyber-Kriminellen entwickelt, an die sensiblen Daten in fremden Online-Accounts zu gelangen und diese zu manipulieren oder zu missbrauchen. Nicht nur für die betroffenen User selbst kann dies verheerende Folgen haben. Es fügt auch Dienste-Anbietern und Unternehmen enormen Schaden zu. Dieser lässt sich in handfesten finanziellen Verlusten beziffern, wirkt sich aber auch auf die Unternehmensreputation aus. Nicht wenige Kunden ziehen sich nach einer Kompromittierung ihrer Daten zurück und sind für künftige Geschäfte für immer verloren.

Auf den folgenden Seiten erläutern wir, wie Credential Stuffing funktioniert und stellen Strategien vor, wie sich die Gefahr von Account Takeovers (ATO) minimieren lässt.

Was ist Credential Stuffing?

Als „Credentials" bezeichnet man die Anmeldedaten, die User beim Einloggen in ein Online-Benutzerkonto eintippen. „Stuffing" steht für das automatisierte „Füllen" solcher Login-Eingabemasken.

Bei Credential Stuffing probieren Cyber-Kriminelle einfach eine Vielzahl von Kombinationen aus Benutzernamen und Passwörtern durch, um sich Zugang zu User-Accounts zu verschaffen. Das machen sie natürlich nicht per Hand, sondern gehen systematisch vor: Sie nutzen automatisierte Bots, die in kürzester Zeit Tausende von Möglichkeiten abarbeiten können.

Warum gewinnt ausgerechnet die Betrugsmasche des Credential Stuffing in letzter Zeit so sehr an Bedeutung? Weil sie so einfach anzuwenden ist und den Cyber-Kriminellen keinen nennenswerten Aufwand abfordert. **Allein im Jahr 2019 erfolgten 80 Prozent der Angriffe auf Web-Anwendungen mit gestohlenen User-Anmeldedaten**.

Was unterscheidet Credential Stuffing von einem Brute-Force-Angriff?

Während bei Brute-Force-Attacken einfach zufällige Passwort-Kombinationen durchgetestet werden, um nach vielen Versuchen einige Treffer zu landen, kommen beim Credential Stuffing von Anfang an tatsächlich existierende Kombinationen aus User-Namen und Passwörtern zum Einsatz. Deshalb stellen bei dieser Methode auch komplizierte Passwörter für die Cyber-Kriminellen kein Hindernis dar. Die gestohlenen Anmeldedaten sind nicht immer aktuell und führen nicht zwangsläufig zum Ziel. Trotzdem ist die Wahrscheinlichkeit erstaunlich hoch, damit einen oder gar mehrere Treffer zu landen. Insider rechnen bei Angriffen mit Credential Stuffing mit einer Erfolgsquote von 0,5 bis 3 Prozent.

Wo liegen die Unterschiede zu Social Engineering?

Beim Social Engineering geht es um das Phishing („Fischen", „Angeln") nach Passwörtern: User werden beispielsweise durch täuschend echt wirkende Mails auf gefälschte Websites ihrer Bank oder einer anderen wichtigen Institution gelockt, um dort beim Einloggen unwillentlich ihre Nutzerdaten an Kriminelle preiszugeben. Beim Credential Stuffing sind die Online-Betrüger hingegen bereits im Besitz von einzigartigen Kombinationen aus User-Namen und Passwörtern. Hier gilt es nur noch, verschiedene Online-Portale mit Hilfe von Botnets mit den Daten zu „füttern", bis man mit einer gültigen Kombination einen Treffer erzielt.

Wie kommen Cyber-Kriminelle an die Account-Daten anderer Nutzer heran?

Im Darknet finden sich sogenannte „Combo-Listen" (wie die berüchtigte Collection X), in denen insgesamt ca. 3,3 Milliarden einzigartige Verbindungen von Benutzernamen und Passwörtern in durchsuchbaren Datenbanken zusammengefasst sind (Stand Anfang 2021). Diese Daten stammen zum Beispiel aus grossen Cyber-Attacken auf die Online-Portale von Gmail, LinkedIn, Microsoft, Napster, Netflix, Nintendo, Zoom oder aus der Welt der Kryptowährungen. Ergänzt werden diese Listen durch komfortable Tools, mit denen sich beispielsweise Bot-Detektoren (CAPTCHA-Tests, wie etwa die Bilderreihen, bei denen man verschiedene Merkmale wie Brücken, Ampeln, Lkws oder Ähnliches identifizieren muss, bevor man sich einloggen kann) austricksen lassen.

Mit den Listen, Bots und Zusatz-Tools wird unter Cyber-Kriminellen ein lukrativer Handel betrieben. Dennoch sind diese Grundlagen für Credential-Stuffing-Angriffe in der Regel sehr günstig zu haben – manchmal sogar komplett kostenlos. So hat beispielsweise die Sicherheitsfirma Cyble im Jahr 2020 mehr als **530.000 Datensätze gestohlener Zoom-Accounts für gerade mal 0,0020 US-Cent pro Stück gekauft**. Dies macht Credential Stuffing für Betrüger umso reizvoller – denn die mögliche „Ausbeute" einer Attacke erfordert keine nennenswerte Investition.

Geld ist keine Hürde: Credential-Stuffing-Tools zum Spottpreis

Im Report Credential Stuffing 2021 machen die Sicherheitsexperten von F5 eine verblüffende Rechnung auf, was Cyber-Kriminelle durchschnittlich in ihre Credential-Stuffing-Aktivitäten investieren müssen:

Zugriff auf 2,3 Milliarden Anmeldedaten	**$ 0,00**
Tool–Konfiguration	**$ 50,00**
100.000 CAPTCHAs („Completely Automated Public Turing test to tell Computers and Humans Apart")	**$ 139,00**
10 globale IPs	**$ 10,00**

Das bedeutet: **100.000 Account-Takeover-Versuche (ATO) sind bereits für weniger als 200 US-Dollar zu haben**.

Credential Stuffing – leichtes Spiel für Cyber-Kriminelle

Auch technisch wenig versierte Cyber-Kriminelle können sich mit Credential Stuffing sehr schnell unbefugten Zugriff auf die Online-Konten nichtsahnender Konsumenten oder Firmen-Mitarbeiter verschaffen. Das ist besonders effektiv bei B2C-Unternehmen, deren Kundenkommunikation zu einem grossen Teil über die Website, den Online-Shop und Smartphone-Apps stattfindet – und der Zugang zum Benutzerkonto ohne weitere sichere Authentisierungsverfahren via User-Name und Passwort erfolgt.

Warum man Credential Stuffing nicht auf die leichte Schulter nehmen sollte

Credential-Stuffing-Angriffe machen heute mit 29 Prozent den grössten Teil der Attacken auf Benutzerkonten aus. Laut Aberdeen Strategy Research verzeichneten im vergangenen Jahr **76 Prozent der B2C-Unternehmen im EMEA-Wirtschaftsraum erfolgreiche Kompromittierungen von Account-Daten ihrer Online-Kunden**. Es wird geschätzt, dass auf etwa 20 Login-Versuche ein Credential-Stuffing-Angriff kommt. Das IT-Sicherheitsunternehmen Shape Security geht sogar davon aus, dass durchschnittlich 80 bis 90 Prozent des Login-Traffics von beliebigen Online-Shops auf Credential-Stuffing-Angriffe zurückzuführen sind.

Attacken bleiben oft unerkannt

Viele Credential-Stuffing-Angriffe werden nicht einmal bemerkt, weil sie nicht in die technische Infrastruktur eingreifen und beispielsweise keine IT-Sicherheitslücken ausnutzen. Zudem gehen die Angriffe meist über Botnets von mehreren IP-Adressen aus, so dass es schwieriger wird, Übeltäter zu identifizieren und zu sperren.

Cyber-Kriminelle profitieren von unserer Bequemlichkeit

Arglose User von Online-Konten machen es den Angreifern selbst oft noch leichter, verheerenden Schaden anzurichten: Laut Nevis Sicherheitsbarometer 2021 nutzen zum Beispiel 44 Prozent der deutschen Konsumenten ihre Passwörter über Jahre hinweg mehrfach für unterschiedliche, teils längst stillgelegte Benutzerkonten. Besonders erschreckend: **Selbst wenn eine Datenschutzverletzung aufgedeckt wurde, ändern laut einer CyLab-Studie der Carnegie Mellon University nur 33 Prozent der Anwender ihre Zugangsdaten**. Mit einem geleakten Passwort werden den Online-Verbrechern somit Tür und Tor geöffnet – oft zu mehreren Accounts bei unterschiedlichen Online-Diensten.

Was machen die Cyber-Kriminellen mit den gestohlenen Login-Daten?

In der Studie von Aberdeen Strategy Research wurde festgestellt, dass die Folgen von Credential Stuffing sehr vielfältig sein können: Betroffene B2C-Unternehmen in der EMEA-Region hatten vor allem zu kämpfen mit:

- *Einrichtung neuer Konten (z.B. Kreditanträge)* – ***34%***
- *Betrügerischen Transaktionen* – ***39%***
- *Falschen Rückbuchungen* – ***18%***
- *Falschen Ablehnungen* – ***34%***
- *Übertragung von Geld und anderen Werten (z.B. Prämien oder Treuepunkte)* – ***11%***
- *Betrügerischen Käufen (z.B. Konsumartikel oder Wertkarten)*
- *Diebstahl von digitalen Inhalten und Services (z.B. Downloads oder Nutzung von Streaming-Diensten)*

Welche Branchen sind von Credential Stuffing besonders betroffen?

Eigentlich kann Credential Stuffing alle Branchen treffen, in denen die Customer Journey zu einem gewissen Teil auf Online-Kunden-Accounts basiert:

Traditionelles Finanzwesen
Alle Anbieter von Finanzdienstleistungen (Giro-, Spar- und Geschäftskonten, Einlagenzertifikate, Unternehmens- und Privatkredite, Hypotheken…) für Unternehmen und Privatpersonen

- Geschäftsbanken
- Kreditgenossenschaften
- Regionale Sparkassen

FinTech
Anbieter technologiebasierter Finanz- und Versicherungsdienstleistungen wie

- Kryptowährungsbörsen
- Digitale Kreditvergabe
- Mobile Zahlungssysteme

Versicherungswesen
Anbieter von Versicherungsleistungen für Verbraucher

- Sach- und Haftpflichtversicherungen
- Hausratversicherungen
- Kfz-Versicherungen

Telekommunikation
Anbieter von Telefon-, Internet-, Kabel-TV- und Streaming-Diensten, die mit Online-Konten verknüpft sind

Energieversorger
Strom-, Wasser- und Gasanbieter mit Online-Kunden-Accounts

Gesundheitswesen
Kliniken, Ärzte und andere Leistungsanbieter aus dem Gesundheitsbereich, die Kosten- und Verwaltungsaufwand der Therapien ihrer Patienten über Krankenversicherungen abwickeln. Hier spielen auch Online-Behandlungsangebote wie TeleHealth oder mobile Apps zum Erreichen von Gesundheitszielen eine Rolle

Online-Shopping-Portale & Online-Marktplätze
Amazon, eBay & Co.

Social-Media-Plattformen
Facebook, Instagram, LinkedIn, Xing etc.

Consumer Electronics
Anbieter von modernen TV-Geräten, Smart-Home-Infrastrukturen und smarten Hausgeräten, die mit Online-Accounts verbunden sind

Computer- und Videospielebranche
Anbieter von Computer- und Videospielen, die mit einem Online-Zugang verknüpft sind

Online-Glücksspiele
Anbieter von Online-Poker- und Casino-Games oder Sportwetten

Wie Credential Stuffing Unternehmen schadet

Aberdeen Strategy Research untersuchte in seiner Studie die Auswirkungen von Credential Stuffing auf zehn verschiedene B2C-Branchen. Das Fazit: **Account Takeovers (ATO) haben mittlerweile ein Ausmass angenommen, das in allen betrachteten B2C-Kategorien in der EMEA-Region signifikanten wirtschaftlichen Schaden anrichtet**. Interessant ist auch, dass sich in den **drei Branchen mit der vergleichsweise niedrigsten Profitabilität – Sach- und Unfallversicherungen, Gesundheitsdienstleister und Online-Glücksspiele – die ATOs am gravierendsten auswirken**.

Credential-Stuffing-Angriffe verursachen nicht nur finanziellen Schaden, sondern auch Mehrarbeit und bürokratischen Zusatzaufwand. Hinzu kommen Langzeitfolgen wie der Vertrauensverlust bei Kunden oder eine angeschlagene Unternehmensreputation:

- Datenschutzverletzungen bei Kunden
- Mehrkosten für Service- und Support-Leistungen
- Ausfälle durch IT-Wartungsarbeiten und Downtimes
- Einbindung von Call-Centern zur Bearbeitung von Kundenanfragen zu Datenschutzverletzungen, Hilfe beim Passwort-Reset etc.
- Rückgang der Gesamtzahl der monatlich aktiven User. Nutzer, die aus Sicherheitsgründen abwandern und ihre Accounts schliessen
- Verlust von Marktanteilen an Wettbewerber
- Verstärkte Kontrollen durch Branchen-Aufsichtsbehörden

Wie man sich als User vor Credential Stuffing schützen kann

Der erste Sicherheits-Check

Viele User fragen sich, ob ihre Zugangsdaten zu diversen Online-Konten noch sicher sind. Mittlerweile bieten diverse Sicherheitsunternehmen einfache Online-Tools an, mit denen sich schnell überprüfen lässt, ob Mail-Adressen, Passwörter oder auch Mobilfunknummern in den Combo-Listen auftauchen, die von Cyber-Kriminellen für Credential-Stuffing-Angriffe genutzt werden. Sehr zuverlässig, vielfach bewährt und absolut sicher ist beispielsweise der Dienst **haveibeenpwned.com**, mit dem man in Sekundenschnelle herausfinden kann, ob die eigenen Anmeldedaten bereits kompromittiert wurden und in den einschlägigen Listen kursieren. Falls ja, gilt es, die betroffenen Passwörter schnellstmöglich zu ändern!

Möglichst viele unterschiedliche Passwörter verwenden

Wer ein Passwort für mehrere User-Konten einsetzt, riskiert, dass Internet-Kriminelle mit einem Credential-Stuffing-Angriff gleich mehrere Accounts knacken können. Deshalb empfiehlt es sich, für jedes Online-Konto ein eigenes, einzigartiges Passwort anzulegen. Dieses sollte zudem so komplex wie möglich gestaltet sein.

Passwörter regelmässig ändern

Je öfter man Passwörter ändert, desto geringer ist die Wahrscheinlichkeit, dass die aktuellen Anmeldedaten für Credential-Stuffing-Angriffe genutzt werden können.

Passwort-Manager – die komfortable Merkhilfe

Zugegeben, es ist schwierig, sich komplexe Passwörter zu merken – zumal die meisten Menschen über eine ganze Reihe von Online-Konten verfügen. Viele User nutzen deshalb oft aus Bequemlichkeit ein und dasselbe Passwort für mehrere Accounts – und machen sich damit besonders verletzlich für die Attacken dreister Online-Betrüger.

Abhilfe schaffen Passwort-Manager, die selbst komplexe Passwörter generieren und diese für die nächsten Logins speichern. Das entlastet das Gehirn – man muss sich nur noch die Zugangsdaten für den Passwort-Manager merken. Natürlich bieten Passwort-Manager auch keine hundertprozentige Sicherheit – auch sie können unter Umständen von Betrügern geknackt werden. Deshalb ist es immer gut, wenn Unternehmen neben dem Online-Zugang via Passwort weitere Sicherheitsmechanismen vorsehen, die für Cyber-Kriminelle kaum zu überwinden sind…

Sicherheits-Checkliste für Online-User

- ☑ Regelmässig über vertrauenswürdige Online-Services wie **haveibeenpwned.com** prüfen, ob die genutzten User-Namen, E-Mail-Adressen, Passwörter und Mobilfunknummern bereits kompromittiert sind.
- ☑ Für jedes Online-Konto ein eigenes, einzigartiges und komplexes Passwort wählen.
- ☑ Passwörter häufig ändern.
- ☑ Passwort-Manager für vereinfachte Logins mit automatisch generierten, komplexen Passwörtern benutzen.

Wie Unternehmen Credential-Stuffing-Angriffe abwehren können

Passwörter sind ein uraltes Instrument, um Daten vor dem Zugriff Unbefugter zu schützen – und unter heutigen Gesichtspunkten weder sicher noch anwenderfreundlich. Mit einem User-Namen und einem Passwort allein ist ein Online-Account für Betrüger mittlerweile leicht zu knacken. Dieses Problem wird sich in den kommenden Jahren mit den Möglichkeiten von Quanten-Computing weiter verstärken. Viele Unternehmen setzen deshalb schon heute auf den Komfort moderner Customer-Identity- und Access-Management-Pakete, die für die Erfassung und Verwaltung von Kundendaten erweiterte Sicherheitsfunktionen bieten.

Ausweg aus dem Passwort-Dilemma: Biometrie

Angesichts der technischen Möglichkeiten moderner Computer und Smartphones ist das Passwort als „Sicherheitsfaktor" für User-Accounts eigentlich längst passé. Biometrische Merkmale wie Fingerabdrücke, Iris-Scans oder Gesichtserkennung bieten einen kaum überwindbaren Schutz gegen Online-Betrüger – und die meisten Geräte verfügen heute längst über die Möglichkeit, derartige Technologien für die User-Authentisierung einzusetzen.

Die Vorteile biometrischer Merkmale bei der Nutzer-Authentifizierung:

- **Bestmöglicher Schutz:** Biometrische Merkmale wie Fingerabdruck, Iris und Gesichtszüge sind bei jedem Menschen absolut einzigartig und damit fast fälschungssicher
- **Anmeldung ohne Passwort:** Mit dem Einsatz von biometrischen Merkmalen zur Nutzer-Authentisierung wird das unsichere Verfahren mit User-Namen und Passwörtern überflüssig
- **Maximaler Bedienkomfort:** Die biometrische Nutzer-Authentisierung erhöht die Anwenderfreundlichkeit beim Zugang zum Online-Konto: Ein sekundenschneller Fingerabdruck-Scan kann beispielsweise das umständliche Merken und Eintippen von Passörtern ersetzen
- **Höhere Kundenfrequenz und Kundenbindung:** Das Plus an Sicherheit und Usability beim Zugang zum Online-Account macht die Customer Journey attraktiver und zu einem positiven Erlebnis
- **Gut fürs Unternehmens-Image:** Zuverlässiger Schutz vor Online-Betrug gehört heute zu den wichtigsten Faktoren für eine erstklassige Unternehmensreputation

Zwei-Faktor-Authentisierung (2FA) und Multifaktor-Authentisierung (MFA)

Die Sicherheit von Online-Accounts lässt sich noch weiter steigern, wenn bei der Anmeldung zwei (2FA) oder mehr (MFA) Verfahren zur Identitätsprüfung zum Einsatz kommen: So kann der Anmeldevorgang beim Benutzer-Konto verschiedene Faktoren erfordern:

- **Etwas, das der User weiss:** zum Beispiel ein Passwort, eine PIN oder sonstige Informationen, die nur dem Nutzer zugänglich sind
- **Etwas, das der User ist:** Einzigartige biometrische Merkmale wie Fingerabdruck, Gesichtszüge oder Iris
- **Etwas, das der User besitzt:** Das Einloggen ins Benutzer-Konto erfordert die Entsperrung durch ein zweites Gerät, zum Beispiel durch eine Authentisierungs-App auf dem Smartphone oder ein externes Token

Da Online-Betrüger beim Credential Stuffing nur über gestohlene User-Namen und Passwörter verfügen, gelingt es ihnen nicht, die zusätzlichen Sicherheitsbarrieren bei der Zwei-Faktor-Authentisierung und der Multi-Faktor-Authentisierung zu überwinden.

Noch mehr Komfort und Sicherheit: der FIDO-Standard

Dank Globalisierung sind heute Business und Konsumverhalten international geworden. Wir wickeln Geschäfte mit Unternehmen auf der anderen Seite unseres Planeten ab und bestellen Waren bei global agierenden Anbietern. Kundendaten etwa mit Bankverbindungen und Kreditkartennummern liegen oft auf ausländischen Servern und werden weltweit für Transaktionen genutzt.

Aus diesem Grund entwickelt die 2012 gegründete FIDO-Allianz internationale Sicherheitsstandards für die einfache, schnelle und sichere Authentisierung im Internet. Der aktuelle Standard FIDO2 nutzt dabei konsequent die Möglichkeiten moderner Hardware: Neuere Computer und Smartphones verfügen mit Krypto-Chips und dem sogenannten Trusted Platform Module (TPM) über Technologien, mit denen sich ein Nutzer für den Zugang zu einem Online-Portal mit einem geheimen Security Key eindeutig authentisieren kann. Dieser Sicherheitsschlüssel lässt sich nicht auslesen und ist für Cyber-Kriminelle nicht zu knacken.

CIAM: Effizientes Kundenidentitätsmanagement für Unternehmen

Customer Identity und Access Management (CIAM) ist die zeitgemässe Art, Kundenidentitäten und Kundenprofile optimal zu erfassen und zu verwalten. CIAM bündelt für Unternehmen alle Prozesse rund um User-Konten. Darüber hinaus ermöglichen derartige Systeme zum Kundenidentitätsmanagement auch eine konsistente, sichere und positive Kundenerfahrung über alle Plattformen vom Laptop bis zum Tablet und Smartphone.

Die Vorteile eines leistungsstarken CIAM-Systems:

- Kundenregistrierung
- Self-Service-Kontenverwaltung für Kunden
- Consent & Preference Management zur Personalisierung von Kunden-Konten bei gleichzeitiger Einhaltung aller Datenschutzbestimmungen
- Data Access Governance & Management zur Steuerung und Kontrolle von Zugriffsrechten auf Daten aller Art
- Optimaler Schutz vor Cyber-Kriminellen und unbefugtem Datenzugriff durch Zwei-Faktor- und/oder Multi-Faktor-Authentisierung und Single-Sign-on-Verfahren (SSO)
- Möglichkeit der Nutzung biometrischer Daten im Authentisierungsprozess
- Unterstützung der FIDO-Standards
- Berücksichtigung aller internationalen datenschutzrechtlichen Bestimmungen

Fazit: Credential Stuffing lässt sich heute wirksam vermeiden

Wer heute noch Kunden-Accounts ausschliesslich durch Kombinationen aus User-Namen und Passwörtern absichert, handelt eigentlich grob fahrlässig. Trotzdem gibt es immer noch zahllose Unternehmen, die Cyber-Kriminellen beim Credential Stuffing so ungewollt in die Hände spielen. Sie riskieren damit nicht nur unwiederbringliche Image-Verluste, sondern auch eine massive Abwanderung von Kunden. **Laut einer Studie von PriceWaterhouseCoopers kann eine einzige schlechte Erfahrung dazu führen, dass ein Fünftel bis ein Drittel der Kunden einem Unternehmen oder einer Marke für immer den Rücken kehren**. In der Tat erwarten Kunden heute vor allem drei Dinge:

- **Bestmögliches Kundenerlebnis:** Eine nahtlose, komfortable Nutzererfahrung über alle Hardware-Plattformen hinweg
- **Schnelle Reaktionen:** Prompte, perfekt aufeinander abgestimmte Services
- **Zuverlässige Datensicherheit:** Optimale präventive Massnahmen gegen Datenschutzverletzungen und die Kompromittierung kritischer persönlicher Daten

Mit Hilfe eines modernen Systems für das Customer Identity und Access Management (CIAM) gelingt es, die hohen Ansprüche heutiger Kunden optimal zu bedienen und letztere stärker an Unternehmen und Marken zu binden. Das berechtigte Verlangen nach Benutzerfreundlichkeit, Sicherheit und Datenschutz lässt sich dabei mit ausgereiften Technologien zur Zwei-Faktor- oder Multi-Faktor-Authentisierung ganz einfach erfüllen.

Die Kosten für die Implementierung einer CIAM-Lösung sind überschaubar – eine lohnende Investition gegen unvermeidliche Image- und Kundenverluste im Fall eines erfolgreichen Credential-Stuffing-Angriffs.

nevis®

Making security an experience

Über Nevis

Nevis entwickelt Sicherheitslösungen für die digitale Welt von morgen: Das Portfolio umfasst passwortfreie Logins, die sich intuitiv bedienen lassen und Nutzerdaten optimal schützen. In der Schweiz ist Nevis Marktführer für Identity und Access Management und sichert über 80 Prozent aller E-Banking-Transaktionen. Weltweit setzen Behörden sowie führende Dienstleistungs- und Industrieunternehmen auf Lösungen von Nevis. Der Spezialist für Authentisierung unterhält Standorte in der Schweiz, Deutschland und Ungarn.

Follow us

www.nevis.net