Multifaktor-Authentifizierung:

Einfach, flexibel und stark in der Sicherheit

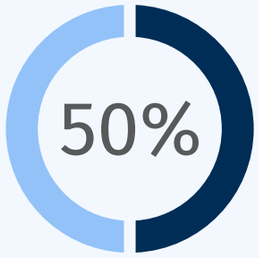
Unverzichtbarer Schutz
für kleine und mittlere
Unternehmen

E-BOOK

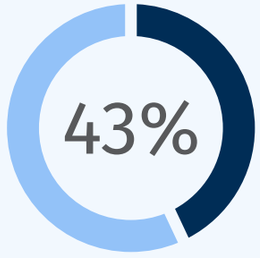
Die hohen Kosten für niedrige Sicherheit

Cyberangriffe werden jeden Tag raffinierter. Versierte Cyberkriminelle nutzen schwache, veraltete Sicherheitsmethoden und -standards, um in alarmierendem Tempo auf Konten und sensible Daten zuzugreifen.

Die dramatische Zunahme von Cyberangriffen bedeutet, dass verstärkte Sicherheitsmaßnahmen nicht nur empfehlenswert, sondern unerlässlich sind. Dies gilt insbesondere für kleine und mittlere Unternehmen (KMUs), die mehr denn je unter den finanziellen, reputationsbezogenen und operativen Auswirkungen leiden.

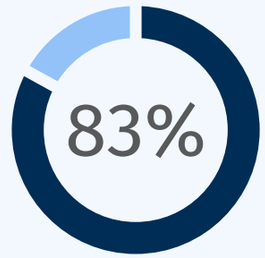


Zunahme von Cyberangriffen im vergangenen Jahr [1]



von Cyberangriffen, die auf kleine Unternehmen abzielen

Stundenlange unnötige Ausfallzeit nach einem typischen Verstoß



der KMU sind finanziell nicht in der Lage, sich von einem Angriff zu erholen [2]

Diese Statistiken sind beängstigend, aber es gibt eine Lösung: **80–90 %** [3] aller Cyberangriffe können durch den Einsatz von Multifaktor-Authentifizierung (MFA) verhindert werden.

[1] https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=5cdc68866b61

[2] https://cybersecurity-magazine.com/10-small-business-cyber-security-statistics-that-you-should-know-and-how-to-improve-them/

[3] https://www.infosecurity-magazine.com/news/tech-execs-mfa-prevent-90-of

Multifaktor-Authentifizierung (MFA) verstehen

Anstatt einen einzigen Authentifizierungsfaktor zu verwenden, verifizieren Multifaktor-Authentifizierungslösungen die Identität mit einer Kombination aus mindestens zwei verschiedenen Methoden, darunter:

ETWAS, DAS SIE HABEN
- SmartCard
- Sicherheitsschlüssel
- Zugangsausweis
- OTP-Token
- Mobiltelefon

ETWAS, DAS SIE WISSEN
- PIN-Code
- Passwort
- Sicherheitsfragen

ETWAS, DAS SIE SIND
- Fingerabdruck
- Gesichtserkennung
- Spracherkennung

Unternehmen können eine beliebige Kombination von Authentifizierungsmethoden in beliebiger Reihenfolge verlangen.

Karte + Passwort + Fingerabdruck

Mobiltelefon + PIN + Sicherheitsfrage

FIDO-fähiger Sicherheitsschlüssel + PIN

Diese Authentifizierungsebenen arbeiten zusammen, um das Risikoniveau zu reduzieren. Selbst wenn ein Authentifizierungsfaktor kompromittiert wird, muss der Benutzer einen weiteren angeben, bevor er Zugang erhält. Die geschützten Daten und Vermögenswerte bleiben somit sicher geschützt.

Schneller mit FIDO

Fast IDentity Online (FIDO) ersetzt die reine Passwortanmeldung durch eine sichere und einfache Authentifizierung auf Websites und in Anwendungen. Es nutzt kostenlose und offene Standards, um die Sicherheit und den Komfort für Verbraucher und Unternehmen gleichermaßen zu erhöhen. Weitere Informationen finden Sie unter

MFA: Sichern, was Ihnen wichtig ist

MFA kann und sollte überall dort eingesetzt werden, wo der Zugang zu sensiblen Ressourcen vor Cyberangriffen und menschlichem Versagen geschützt werden muss. Kleine und mittlere Unternehmen setzen MFA ein, um Folgendes zu sichern:

- **Datenbanken und Anwendungen –** Sicherer Zugriff auf Datenbanken, Buchhaltungs- und HR-Software, Cloud-, Web- und On-Premise-Anwendungen mit Smartcards, Sicherheitsschlüsseln, OTP-Token oder mobilen Authentifizierungsgeräten
- **Mitarbeitercomputer und -geräte –** Schützen Sie Geräte zu Hause und in Remote-Büros, indem Sie zusätzlich zum traditionellen Passwort eine zweite Authentifizierungsebene mit einem Sicherheitsschlüssel oder einer Smartcard hinzufügen
- **Mehrbenutzergeräte –** Ermöglicht es Mitarbeitern, sich schnell und sicher an gemeinsam genutzten Computern und Geräten in Umgebungen wie Einzelhandel, Produktion, Gesundheitswesen und mehr anzumelden
- **Netzwerke und Server –** Sichere VPNs und Server erleichtern Mitarbeitern den Zugriff auf die Ressourcen, die sie für die Arbeit von überall benötigen – auch bei Verwendung eines öffentlichen Netzwerks

HID

MFA ist der Goldstandard, aber die Akzeptanz hinkt hinterher

Angesichts des hohen Risikos und der einfachen Lösungen könnte man meinen, dass die meisten kleinen und mittleren Unternehmen die Vorteile von MFA nutzen würden. Tatsächlich hat eine aktuelle Studie des Cyber Readiness Institute (CRI) [4] ergeben, dass nur 46 % eine Richtlinie umgesetzt haben, weil:

1. SIE WISSEN NICHT, DASS ES SIE GIBT

55 % der KMU bleiben ungeschützt, weil sie MFA und seine Vorteile einfach nicht kennen.

2. SIE VERSTEHEN ES NICHT

30 %der Geschäftsinhaber gaben an, dass sie MFA nicht nutzen, weil sie nicht wissen, wie es funktioniert. Tatsächlich gibt es viele verschiedene Arten von MFA, von einfachen, leicht zu implementierenden Plug-and-Play-Optionen bis hin zu komplexeren eingebetteten Modulen. Darüber hinaus können Unternehmen aus einer Vielzahl von Formfaktoren (wie Karten, Schlüssel und mobile Apps) und Methoden (wie FIDO, PKI, OTP, Push-Benachrichtigungen oder Biometrie) auswählen.

3. SIE DENKEN, ES SEI UNPRAKTISCH

20 % der KMU halten MFA für zu unpraktisch. In Wirklichkeit sind wir alle mehr damit vertraut, als wir denken. Denn wer schon einmal an einem Geldautomaten PIN und Karte genutzt hat, nutzt MFA. Der gesamte Prozess dauert eine Handvoll Sekunden und kann kostspielige Cyberangriffe verhindern, die den Ruf eines Unternehmens schädigen oder sogar dessen vollständige Schließung erfordern könnten.

[4]https://cyberreadinessinstitute.org/resource/global-small-business-multi-factor-authentication-mfa-study/

MFA als KMU-Lösung: Die Vorteile

MFA kann als Eckpfeiler eines starken Cybersicherheitsprogramms für Unternehmen jeder Größe dienen, aber insbesondere für kleine und mittlere Unternehmen mit einzigartigen Herausforderungen und Bedingungen. Durch die Implementierung können Unternehmen die Sicherheit und den Komfort auf vielfältige Weise erhöhen.

OHNE PASSWORT ARBEITEN

Im Privat- und Berufsleben muss der Durchschnittsmensch über 100 Passwörter [5] im Auge behalten. Um sich das Leben leichter zu machen, verwenden viele Benutzer Passwörter, die leicht zu merken sind, oder sie benutzen dasselbe Passwort an mehreren Stellen – von der Anmeldung im Firmennetzwerk bis zu ihren persönlichen Bankkonten. Leider macht dies auch denjenigen das Leben leichter, die versuchen, Informationen zu stehlen. Auch das Vergessen von Passwörtern bedeutet, Passwörter zurückzusetzen, und das Zurücksetzen von Passwörtern kostet Zeit und Ressourcen.

Mit MFA können Sie die Abhängigkeit von Passwörtern beseitigen und Ihre Daten schützen – und gleichzeitig die Benutzerfreundlichkeit verbessern.

SICHERES MOBILES ARBEITEN FÖRDERN

Die Mitarbeiter von heute arbeiten von überall und zu jeder Zeit. Mehr denn je nutzen Mitarbeiter heute private und geschäftliche Geräte für den Zugriff auf Netzwerke und Anwendungen, manchmal über weniger sichere Internetverbindungen. Da selbst das versierteste Cybersicherheitsteam nicht immer kontrollieren kann, wo sich die Mitarbeiter einloggen, ist es das einzig Richtige, Sicherheitsmaßnahmen zu ergreifen, die das System sicherer machen, egal wo die Mitarbeiter sind.

BÖSE AKTEURE AUSBREMSEN

Die Multifaktor-Authentifizierung erschwert es potenziellen Cyberkriminellen, Unternehmensdaten zu stehlen, indem sie sich Zugang zu wichtiger Software und Hardware, einschließlich Netzwerkgeräten, verschaffen. Es verschließt alle schwachen Zugangspunkte eines ungesicherten Systems und kann laut Microsoft 99,9 % der Angriffe auf das Konto verhindern[6].

[5] https://tech.co/password-managers/how-many-passwords-average-person

[6] https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

Die perfekte Lösung und den passenden Anbieter finden

Die Entscheidung, MFA einzusetzen, ist einfach; die Auswahl der richtigen Lösung und des richtigen Anbieters kann entmutigend erscheinen. MFA ist keine Pauschallösung und es gibt viele Variablen im Auswahlprozess. Stellen Sie sicher, dass Sie mit einem Anbieter zusammenarbeiten, der alles bietet, was Sie benötigen, einschließlich:

- **Benutzerfreundlichkeit –** Ihre MFA-Lösung sollte nicht nur eine Auswahl an Authentifizierungsmethoden bieten, einschließlich kennwortloser und Phishing-resistenter Optionen auf der Grundlage von FIDO oder PKI, sondern auch einfach zu übernehmen und zu verwenden sein. Schließlich ist diese Schutzmaßnahme zu Ihrer Sicherheit und zur Benutzerfreundlichkeit da – nicht um das Leben komplizierter zu machen.
- **Mehrere Methoden und Formfaktoren –** Beschränken Sie sich nicht auf eine kleine Auswahl an Authentifizierungsmethoden (wie OTP und Push-Benachrichtigungen) oder Formfaktoren (wie Karten oder Mobiltelefone). Entscheiden Sie sich für einen Anbieter, der eine Vielzahl von beiden und die Möglichkeit bietet, verschiedene Optionen für verschiedene Benutzer und Sicherheitsanforderungen zu nutzen.
- **Einfache Bereitstellung und Verwaltung –** Einige Lösungen benötigen Monate, um einsatzfähig zu werden. Ihre Sicherheit kann nicht so lange warten. Andere Lösungen erfordern umfangreiche Schulungen, eine neue Serverinstallation oder Codeänderungen an bestehenden Anwendungen. Wählen Sie eine Lösung, die in Tagen und nicht in Monaten einsatzbereit ist.
- **Eine Komplettlösung –** Stellen Sie sicher, dass Ihr neues Sicherheits-Setup alle Ihre Ressourcen abdeckt, von Ihren PCs über Ihre Telefone bis hin zu allen integrierten Anwendungen und Netzwerken.
- **Compliance –** Insbesondere in regulierten Branchen ist Compliance von entscheidender Bedeutung. Wählen Sie eine Lösung und einen Anbieter, der in der Lage ist, sich ständig weiterentwickelnde Branchenanforderungen und -vorschriften zu erfüllen, einschließlich Datenschutz wie DSGVO und CCPA.
- **Anpassungsfähigkeit –** Ihre Sicherheitsanforderungen werden sich im Laufe der Zeit wahrscheinlich ändern, und einige Benutzer oder Teile Ihres Unternehmens benötigen möglicherweise eine höhere Sicherheit als andere. Stellen Sie sicher, dass Ihr Anbieter es Ihnen ermöglicht, sich entsprechend anzupassen.

Erweiterte Authentifizierung: Wichtige Kriterien, die bei der Auswahl eines Anbieters zu berücksichtigen sind

Weitere Informationen zur Auswahl des richtigen Anbieters finden Sie im HID Whitepaper

Ausgewogene Sicherheit und Benutzerfreundlichkeit mit starker Multifaktor-Authentifizierung von HID

Als weltweit führender Anbieter vertrauenswürdiger Identitäten bietet HID ein breites und robustes Portfolio an MFA-Lösungen, darunter FIDO- und PKI-fähige Crescendo® Smartcards und Sicherheitsschlüssel sowie MFA-Software wie DigitalPersona®.

Die preisgekrönte Software hilft Unternehmen im Gesundheitswesen, in der Fertigung, im Einzelhandel, in Call-Centern, bei der Strafverfolgung und vielen mehr, die Anmeldung bei Desktops, Websites, VPNs, Netzwerken sowie Cloud- und On-Premise-Anwendungen zu sichern. Diese einfach zu implementierende und zu verwaltende Multifaktor-Authentifizierungslösung ermöglicht die Einhaltung sich entwickelnder Sicherheitsstandards, Mandate und Vorschriften und unterstützt eine breite Palette von Authentifizierungsmethoden und Formfaktoren, einschließlich biometrischer Daten, mobiler Geräte, Zugangsausweise, Smartcards und Sicherheitsschlüssel.

Die hochsicheren Smartcards von sichern nicht nur den Zugriff auf sensible Daten, Anwendungen und E-Mails, sondern können auch als Sichtausweis für Mitarbeiter dienen, um den Zugang zu Gebäuden zu sichern. So können Unternehmen den physischen und logischen Zugang zusammenführen und sowohl Einrichtungen als auch Daten mit einem einzigen Authentifikator schützen.

Sind Sie bereit für ein Upgrade Ihrer Sicherheit? Fordern Sie noch heute eine Testversion an und erfahren Sie, wie MFA für Ihr Unternehmen funktionieren kann.

HID

hidglobal.com

Nordamerika: +1 512 776 9000
Gebührenfrei: 1 800 237 7769
Europa, Naher Osten, Afrika: +353 91 506 900
Asien-Pazifik: +852 3160 9800
Lateinamerika: +52 55 9171–1108

Weitere globale Telefonnummern finden Sie hier

2022-11-15-iams-multi-factor-auth-smb-eb-de
PLT-07033

Part of ASSA ABLOY