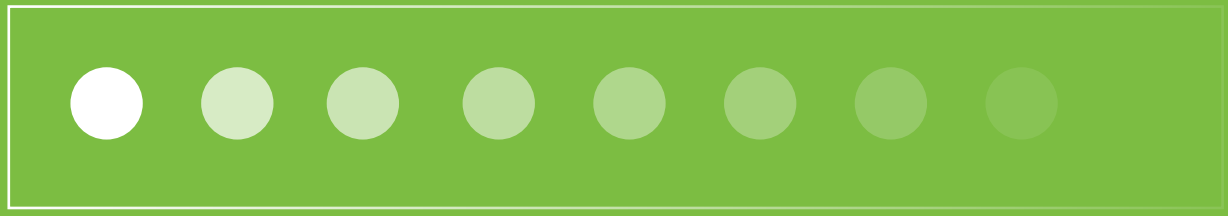
yubico

EIN WHITEPAPER VON YUBICO
OKTOBER 2020

Kennwortlose Authentifizierung

mit FIDO2 und WebAuthn



Inhalt

Kurzdarstellung

Stellen Sie sich eine Welt vor, in der niemand mehr ständig unzählige Kennwörter einrichten und zurücksetzen muss, die anschließend wieder vergessen werden und erneut zurückgesetzt werden müssen. Kennwörter gelten als größte Schwachstelle in der Sicherheit von Unternehmen. Sie erschweren den Kunden die Benutzung und behindern reibungslose interne Prozesse. Mit der Einführung der kennwortfreien Authentifizierung ändert sich das. In einer weltweiten Umfrage des Ponemon Institute unter 2.507 IT-Sicherheitsexperten und 563 Einzelanwendern wurde festgestellt, dass 49 Prozent der befragten IT-Sicherheitsexperten und 51 Prozent der Einzelanwender Passwörter für den Zugriff auf Geschäftskonten mit Kollegen teilen. Dies veranschaulicht die schlechten Praktiken, die die Sicherheitsprobleme, die durch Passwörter entstehen können, noch verschärfen.[1]

Die neuen Authentifizierungsstandards FIDO2/WebAuthn ermöglichen Unternehmen, Probleme, die ein auf Kennwörter basierendes Sicherheitskonzept mit sich bringt zu beseitigen. FIDO2 ist ein offener Standard, der von Yubico, Microsoft und weiteren Mitgliedern der FIDO Alliance entwickelt wurde und erweiterte Optionen für eine starke Authentifizierung bietet, darunter jetzt zusätzlich zur bestehenden Zwei-Faktor-Authentifizierung die Möglichkeit zur kennwortfreien Einzel- und Multi-Faktor-Authentifizierung.

Die kennwortfreie Authentifizierung verbessert die Sicherheit in Unternehmen und vereinfacht die Benutzung in allen Branchen, vom Gesundheitswesen, der Industrie bis zum Einzelhandel sowohl für Mitarbeiter, Geschäftspartner und Lieferanten. So wird die Registrierung von Benutzern vereinfacht. Bedenkt man, dass das Zurücksetzen von Kennwörtern heute die meisten Kosten für IT-Support verursacht, könnte eine kennwortfreie Anmeldung die Belastung von IT-Callcentern deutlich reduzieren, die für das Einrichten und Zurücksetzen von Kennwörtern viel Zeit investieren.

Wie können die Prozesse für Kunden und Mitarbeiter durch die kennwortfreie Anmeldung verschlankt werden? Welche neuen Produkte und Dienste sind möglich, wenn keine Kennwörter mehr gebraucht werden?

In diesem Whitepaper werden die Hintergründe der kennwortfreien Anmeldung und die Fragen beleuchtet, die sich Unternehmen bei der Umsetzung stellen sollten.

Zeit- und Kostenaufwand durch Kennwörter

Unternehmen nutzen heute Cloud- und mobile Technologien, um verbesserte Produkte und Dienste schneller und effizienter anbieten zu können. Allerdings stoßen sie bei dem Wunsch nach schlankeren Verfahren für Kunden und Mitarbeiter auf Herausforderungen auf dem Gebiet der Sicherheit.

Sicherheitsverfahren und -kontrollen schützen das Unternehmen, können aber gleichzeitig ein Hindernis für die Benutzer sein. Dabei stehen Kennwörter ganz oben auf der Liste der lästigsten Sicherheitsmaßnahmen.

Seit den 1950er-Jahren sind Kennwörter ein täglicher Begleiter sowohl für Benutzer in der Wirtschaft wie auch für Konsumenten. Nahezu jede digitale Anwendung erfordert ein Kennwort, seien es soziale Netzwerke wie Facebook, Banken und Einzelhändler wie H&M und Zara oder Business-Anwendungen wie Salesforce und QuickBooks Online.

Der durchschnittliche Konsument in den USA muss sich 70 verschiedene Kennwörter für alle von ihm genutzten Web-Anwendungen und Sites merken[2]. Benutzer in Unternehmen müssen sich sogar noch mehr Kennwörter merken, nämlich 191.[3] Laut einer Studie von IBM sind die so genannten „Millennials“, die einen immer größeren Anteil der Angestellten ausmachen, weniger bereit, sich all diese geheimen Codes zu merken. Sie werden stattdessen eher Kennwörter wiederverwenden und sich so nicht mehr als insgesamt acht merken – eine Bequemlichkeit auf Kosten der Sicherheit.[4]

Ständiges Recycling von Kennwörtern führt zu Datenlecks

Die Benutzer sind immer weniger bereit, sich für jeden Onlinedienst alle paar Monate ein neues Kennwort zu überlegen, wie Sicherheitsrichtlinien häufig vorschreiben. Um sich weniger merken zu müssen, verlassen sich viele auf einfache Kennwörter, die leider leicht zu knacken sind, oder sie verwenden dasselbe Kennwort für verschiedene Webseiten, wobei ein einziges geknacktes Kennwort die Tür zu vielen weiteren Onlinediensten öffnet.

Laut dem Verizon Data Breach Investigations Report (DBIR) von 2019 sind 80% der Hacker-Verletzungen immer noch mit kompromittierten und schwachen Anmeldeinformationen verbunden.[5] Es ist unglaublich, dass nach Jahren hochgradig publizierter Datenverletzungen die meisten davon mit einem schwachen Passwort verbunden sind. Die Analyse von Sicherheitsverletzungen im Rahmen der NCSC 2019 UK Cyber Survey ergab, dass weltweit 23,2 Millionen Opferkonten 123456 als Passwort verwenden.[6]

Vergessene Kennwörter führen zu hohen Kosten für Support

Wenn Benutzer ein Kennwort vergessen haben, rufen Sie oft bei Help Desks und Support-Centern an, was wertvolle Zeit kostet. Das Zurücksetzen von Kennwörtern macht bis zu 6% der Arbeit von Call Centern aus und kostet große Unternehmen zwischen 5 und 20 Millionen US-Dollar jährlich.

80% der Hacker-Verletzungen betreffen immer noch kompromittierte und schwache Anmeldeinformationen.[5]

Verizon Data Breach
Investigations Breach

Da die Unternehmen immer mehr Geschäftsanwendungen in ihre Portfolios aufnehmen, steigen die Kosten für Passwörter nur noch weiter an. Tatsächlich widmen Unternehmen 30 bis 60 Prozent ihrer Support-Desk-Anrufe dem Zurücksetzen von Passwörtern.

Das IT-Team von Microsoft ist auf kennwortlose Authentifizierung umgestiegen, und inzwischen melden sich 90 Prozent der Microsoft-Mitarbeiter ohne Eingabe eines Kennworts an. Infolgedessen sanken die Kosten für die Unterstützung von Passwörtern für Hard- und Software um 87 Prozent. Da Unternehmen immer mehr Geschäftsanwendungen in ihr Portfolio aufnehmen, steigen die Kosten für Passwörter nur noch weiter an. Tatsächlich widmen Unternehmen 30 bis 60 Prozent ihrer Support-Desk-Anrufe dem Zurücksetzen von Passwörtern.[7]

Phishing-Angriffe zielen auf Login-Daten ab

Phishing ist aufgrund sich weiter entwickelnder Angriffstechniken nach wie vor ein massives Sicherheitsproblem. Mit Fake-E-Mails, in denen die Benutzer aufgefordert werden, ihre Anmeldedaten erneut einzugeben, können Online-Accounts gekapert werden. Ungefähr 30% aller Phishing-Mails wurden von den Empfängern geöffnet, und über 7% aller Empfänger öffnen einen Anhang oder klicken auf einen Link, der häufig ein Anmelde-Link ist. Die meisten Phishing-Angriffe führen dann zur Installation von Malware, mit der die Datenverletzung durchgeführt werden soll.[8] Selbst, wenn komplexe Kennwörter verwendet werden, können Hacker durch Phishing Zugang auf die Benutzerkonten erlangen.

Listen mit gestohlenen Anmeldedaten werden verkauft

Wenn Hacker in die IT eines Unternehmens eindringen und Anmeldedaten stehlen, haben sie dadurch nicht nur Zugriff auf die Konten des Unternehmens, sondern auch auf Konten bei anderen Organisationen, bei denen dieselbe Kombination von Benutzername und Kennwort verwendet wurde. Als beispielsweise 2016 eine Milliarde Anmeldedaten für Yahoo! gestohlen wurden, konnten sich die Angreifer damit auch Zugang zu allen anderen Konten sichern, bei denen dieselbe Kombination aus Benutzername und Kennwort hinterlegt war. Milliarden gestohlener Anmeldedaten sind im Dark Web zum Kauf erhältlich. Zudem starten Cyberkriminelle jetzt mit den gestohlenen Kennwörtern automatische Anmeldeversuche. Heute sind neun von zehn Anmeldeversuchen auf beliebten Online-Shops und Banking-Sites Angriffe mit Bots.[9]

So lange sich Unternehmen für die Authentifizierung auf Kennwörter verlassen, sind kostenaufwendiger Support, hohe Sicherheitsrisiken und frustrierte Benutzer unvermeidlich. Vergessene und gestohlene Kennwörter verschlechtern die Benutzererfahrung, senken die Markentreue und führen zu Umsatzverlust.

Lösung des Kennwort-Problems mit FIDO2

Stellen Sie sich vor, Sie könnten verschiedenste Dienste schnell, bequem und sicher für Ihre Kunden und Angestellten bereitstellen, ohne Kennwörter und den damit verbundenen Aufwand. Stellen Sie sich vor, Ihre Kunden, Partner und Mitarbeiter könnten von PCs aus oder mobil sofort auf Inhalte und Dienste zugreifen, ohne dass sie sich an irgendwelche Kennwörter erinnern oder beim Help Desk anrufen müssen. Stellen Sie sich neue Dienste vor, die unmittelbar nach einer unkomplizierten Authentifizierung zur Verfügung stehen. Stellen Sie sich vor, wie IT-Unternehmen sich endlich nicht mehr mit der Verwaltung und dem Zurücksetzen von Kennwörtern beschäftigen müssen und diese Kosten sparen.

Der Authentifizierungsstandard FIDO2 bietet die Möglichkeit einer kennwortlosen Authentifizierung.

Die Vorteile der kennwortfreien Authentifizierung

Verbesserte Nutzbarkeit

Durch die kennwortfreie Authentifizierung müssen sich Benutzer keine Kennwörter mehr merken und nirgends mehr welche eingeben.

Erhöhte Sicherheit

Die kennwortfreie Authentifizierung schließt Sicherheitsrisiken wie gestohlene Kennwörter und Brute-Force-Angriffe gegen Anmeldedialoge aus.

Gesteigerte Effizienz

Durch die kennwortfreie Anmeldung müssen IT-Abteilungen sich nicht mehr um die Verwaltung von Kennwörtern kümmern.

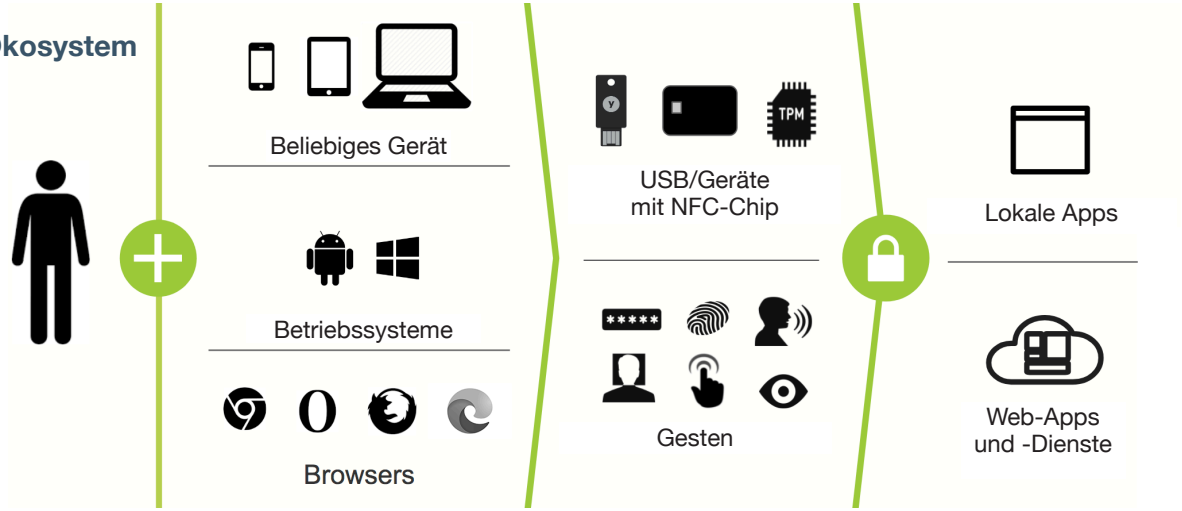
Diese Vorteile bieten jetzt die offenen FIDO2/WebAuthn-Authentifizierungsstandards.

Die kennwortfreie Authentifizierung

Der Authentifizierungsstandard FIDO2, der von Yubico, Microsoft und Mitgliedern der FIDO Alliance in Zusammenarbeit mit dem World Wide Web Consortium (W3C) mitverfasst wurde, unterstützt verschiedene Anwendungsszenarien und Erfahrungen.

FIDO2 besteht aus zwei standardisierten Komponenten: einer Web-API (WebAuthn) und einem Client to Authenticator Protocol (CTAP). Beide arbeiten zusammen und sind notwendig für eine kennwortfreie Anmeldung. WebAuthn definiert eine Standard-Web-API, die in Browser und in Web-Plattform-Infrastrukturen integriert werden kann, um Benutzern neue Methoden zur sicheren Authentifizierung im Netz bereitzustellen. CTAP ermöglicht es einem externen Authentifizierungsgerät, etwa einem Sicherheitsschlüssel, starke Authentifizierungsdaten lokal per USB, NFC oder Bluetooth an den PC oder das mobile Gerät des Benutzers zu übertragen.

Das FIDO2-Ökosystem



FIDO2 nutzt zur Authentifizierung der Benutzer ein asymmetrisches Paar kryptographischer Schlüssel (öffentlich/privat). Der öffentliche Schlüssel wird auf einem beliebigen Service- bzw. Computergerät mit FIDO2-Unterstützung gespeichert, während der private Schlüssel beim Benutzer bleibt und durch einen physischen Sicherheitsschlüssel geschützt ist, etwa den YubiKey der Serie 5 oder den Security Key von Yubico. Die Authentifizierung selbst geht schnell und einfach: Es muss lediglich der Sicherheitsschlüssel eingeführt bzw. darauf getippt werden – schon ist die Authentifizierung abgeschlossen und die Anmeldung erfolgt sofort.

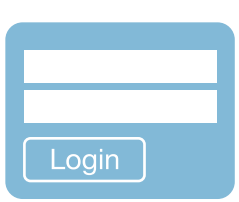
Mit FIDO2 kann der Sicherheitsschlüssel alleine oder in Verbindung mit einem PIN oder einer Geste für besonders sichere kennwortfreie Anmeldung verwendet werden. Des Weiteren wird die Zwei-Faktor-Authentifizierung per Kennwort nach wie vor unterstützt.

Das World Wide Web Consortium (W3C) unterstützt FIDO2

Mit der Web Authentication (WebAuthn)-API-Spezifizierung stehen Browsernutzern neue Methoden zur sicheren Authentifizierung im Netz auf Grundlage der FIDO2-Spezifizierung bereit. Die Browser Microsoft Edge, Google Chrome und Mozilla unterstützen die WebAuthn-API-Spezifikation.

Optionen für die Authentifizierung mit FIDO2/WebAuthn

Ein-Faktor-Authentifizierung (ohne Kennwort)
Verwendung des Sicherheitsschlüssels allein als starker erster Faktor zur Authentifizierung, wobei nur der Besitz des Geräts notwendig ist, das eine kennwortfreie Anmeldung in einem Schritt erlaubt.



Zwei-Faktor-Authentifizierung (Kennwort + Authentifizierungsgerät)
Verwendung des Sicherheitsschlüssels als zweiter Faktor bei einer Zwei-Faktor-Authentifizierung.

Mehrfaktor-Authentifizierung (kennwortfrei + PIN oder Biometrie)
Verwendung des Sicherheitsschlüssels für die Mehrfaktor-Authentifizierung, die den Besitz des Geräts UND einen PIN-Code oder eine biometrische Identifizierung erfordert, für Anwendungen mit hohem Sicherheitsniveau

FIDO2 wird auf der neuesten Version von Windows 10-Geräten, einschließlich Windows-Desktop- und Mobilsystemen, unterstützt. Damit ist FIDO2 weltweit auf über 700 Millionen Geräten und Milliarden von Azure AD-Konten verfügbar.

Die Vorteile durch Verzicht auf Kennwörter

Verbesserte Nutzbarkeit

Die kennwortfreie Anmeldung mit FIDO2 sorgt für eine schnelle und einfache Authentifizierung.

Die Authentifizierung mit FIDO2 erfolgt schnell und einfach, ohne dass Kennwörter eingesetzt werden müssen. Mit FIDO2 können sich die Benutzer mit einem einzigen Hardware-Authentifizierungsgerät, zum Beispiel einem YubiKey, bei allen Onlinediensten, die sie nutzen authentifizieren. Dazu zählen Business-Anwendungen und Dienstleistungen, soziale Netzwerke und andere Kundenanwendungen zu Hause, ohne dass Geheimnisse preisgegeben werden müssen.

Gleichzeitig unterstützt FIDO2 mehrere Identitäten für einen einzigen Benutzer. Derselbe YubiKey kann sowohl für Business- als auch für Konsumentenanwendungen genutzt werden. Dazu zählen Websites, Onlinedienste, Server und Geräte mit FIDO2-Unterstützung – von Gebäuden bis hin zu Fahrzeugen.

Mit der kennwortfreien Authentifizierung können sich Geschäftsleute auf Flugreisen oder in der U-Bahn, wo es möglicherweise kein W-LAN oder mobiles Internet gibt, immer noch auf ihren Laptops authentifizieren und sicher und produktiv arbeiten – selbst dann, wenn sie wegen schlechtem Netz keine SMS- oder OTP-Anmeldedaten für die Authentifizierung empfangen können.

Dank FIDO2 ist kein Netzwerkzugang (mobil oder Internet) mehr notwendig, um Zweitfaktoren zu empfangen. Zusätzlich zur verbesserten IT-Sicherheit erleichtert FIDO2 den Benutzern den Zugang zu den Geräten, die sie brauchen, um überall und jederzeit arbeiten zu können.

FIDO2 wird auf der neuesten Version von Windows 10-Geräten, einschließlich Windows-Desktop- und Mobilsystemen, unterstützt. Windows 10 hat weltweit mehr als 1 Milliarde Benutzer, was etwa 700 Millionen Geräte FIDO2-kompatibel macht.[10]

Da FIDO2 als ein offener Industriestandard entwickelt wurde und umfassend von Microsoft und dem World Wide Web Consortium (W3C) beworben sowie von Google und Mozilla unterstützt wird, hängt die Implementierung nicht von einer einzigen Institution ab. Mit FIDO2 sparen sich Unternehmen die Kosten für Entwicklung und Pflege individueller Sicherheitskonzepte zum Bekämpfen der Probleme durch Kennwörter. Jetzt können Unternehmen aus allen Branchen die Vorteile eines offenen Industriestandards zur Authentifizierung nutzen, der von führenden IT-Organisationen unterstützt wird.

Erhöhte Sicherheit

FIDO2 verbessert die Sicherheit bei Benutzerauthentifizierung und Zugangsmanagement deutlich

FIDO2 verbessert die Sicherheit bei Benutzerauthentifizierung und Zugangsmanagement deutlich.

Durch die kennwortfreie Anmeldung können die Benutzer nicht mehr Opfer von Kennwort-Phishing werden. Die Benutzer bestätigen ihre Identität mit einem Hardware-Authentifizierungsgerät wie etwa einem YubiKey, der auf einem hohen Niveau wie folgt funktioniert:

- Der YubiKey erstellt und verwaltet die FIDO2-Anmeldedaten (ein Paar mit öffentlichem und privatem Schlüssel) und bindet die Anmeldedaten an einen bestimmten Dienst, der als Ursprung („origin“) bezeichnet wird.
- Die Bindung des Ursprungs verhindert Man-in-the-middle-Angriffe.
- Wird die Authentifizierung von einem Dienst wie etwa Azure AD angefordert, wird die Antwort mit dem privaten Schlüssel unterzeichnet und zum Netzwerk gesandt, um vom Onlinedienst mit Hilfe des öffentlichen Schlüssels bestätigt zu werden.

Die FIDO2-Anmeldedaten, die auf einem sicheren Chip im YubiKey gespeichert werden und die das Gerät nie verlassen, wurden so entwickelt, dass ein Diebstahl der Daten bei der Anmeldung auf Websites verhindert wird.

FIDO2 verringert das Risiko für Anwendungen, Websites, Onlinedienste, Server und Geräte, indem die zentrale Speicherung und Verwaltung von sensiblen Anmeldedaten abgeschafft wird. FIDO2-Konten benötigen kein Kennwort, daher kann es auch nicht mehr zu Passwortklau kommen. Websites und andere Online-Dienste speichern nur die öffentlichen Schlüssel, die die Benutzer dort registriert haben. Der geheime (private) Schlüssel wird sicher auf dem Hardware-Authentifizierungsgerät aufbewahrt und, anders als ein herkömmliches Kennwort, nie über ein Netzwerk übermittelt. Mit diesen öffentlichen Schlüsseln lassen sich von den privaten Schlüsseln generierte Signaturen validieren, alleine sind sie aber nutzlos für den Zugriff auf andere Ressourcen. Nur ein Endbenutzer mit dem privaten FIDO2-Schlüssel kann sich erfolgreich für einen Onlinedienst authentifizieren. So wird die Sicherheit verbessert und gleichzeitig der Anmeldevorgang für die Endbenutzer schneller, einfacher und zuverlässiger.

Authentifizierungsrechte können in Übereinstimmung mit den Sicherheitsrichtlinien der Organisationen bzw. mit Branchenvorschriften (z. B. GLBA und HIPAA, s. USA) oder behördlichen Vorschriften (z. B. die US-amerikanische NIST SP800-63) gewährt werden. Durch die Einhaltung von NIST SP800-63 entspricht FIDO2 automatisch einer Vielzahl anderer Vorschriften, die auf NIST-Normen beruhen. IT-Administratoren und Compliance Officers können sicher sein, dass die Benutzer die Authentifizierungsprüfung nicht durch geteilte Kennwörter umgehen. Jeder Benutzer erhält einen einmaligen Schlüssel, mit dem die Authentifizierung für registrierte Onlinedienste und Anwendungen erfolgt.

Einhaltung der Authentifizierungs-standards des NIST (National Institute of Standards and Technology)

FIDO2 ist ein kryptographischer Token (mit einem oder mehreren Faktoren). Laut der NIST Special Publication 800-63 wird der Mehrfaktor-Kryptographie-Token als Authentication Assurance Level 3 (Authentifizierungs-Sicherheitsstufe 3) klassifiziert, die höchste Stufe gemäß dieser Norm. Der Einsatz von FIDO2 entspricht demzufolge den höchsten Anforderungen an die sichere Authentifizierung in NIST SP800-63 verpflichtend ist.[11]

„FIDO2 erfordert keine komplexe PKI-Umgebung zur Verwaltung von Zertifikaten“

Gesteigerte Effizienz

Mit FIDO2 müssen IT-Abteilungen sowie Help Desks und Call Center keine Kennwörter mehr erstellen, speichern, aktualisieren und zurücksetzen.

Die kennwortfreie Anmeldung sorgt für ein unkompliziertes Onboarding von Mitarbeitern und temporären Dienstleistern, wodurch die Support-Kosten durch Vergabe und Verwaltung von Kennwörtern entfallen. Anstelle von neuen Kennwörtern, die gleich nach Erstellung oder nach einer bestimmten Zeit wieder geändert werden müssen, benötigen neue Mitarbeiter und temporäre Dienstleister dank FIDO2 lediglich einen FIDO2-Sicherheitsschlüssel, wobei die Benutzer bei der Ausgabe optional einen PIN-Code festlegen können. Die Berechtigungen zur Authentifizierung mit FIDO2 können einfach entzogen werden, sobald ein Mitarbeiter das Unternehmen verlässt oder ein Dienstleister seinen Auftrag abgeschlossen hat.

Mit dem FIDO2-Sicherheitsschlüssel können sich die Benutzer bei einem zentralen Dienst wie Azure AD authentifizieren und ihre Identität für die Registrierung neuer Geräte (z. B. Smartphones) feststellen lassen. In Organisationen, in denen Rechner von mehreren Benutzern verwendet werden, kann sich der einzelne Benutzer schnell und einfach authentifizieren, ohne sich Kennwörter merken und eintippen zu müssen. Durch einfaches Einstecken oder Hinhalten eines YubiKey mit aktivierter NFC-Funktion können die Benutzer die Geräte entsperren und auf ihre Konten zugreifen.

Außerdem benötigt FIDO2 keine komplexe PKI-Umgebung für die Verwaltung von Zertifikaten. Die IT-Abteilung kann ihre Zeit so wieder strategischen und produktiven Aufgaben zuwenden.

Einhaltung der Authentifizierungs-Anforderungen von Unternehmen

FIDO2 erfüllt alle der folgenden entscheidenden Anforderungen an die Benutzerauthentifizierung:

- **Bereitstellung von Anmeldedaten, die nicht gehackt oder gefälscht werden können**
- **Bereitstellung einer Authentifizierungsmethode, die Phishing vorbeugt**
- **Ein bequemes Verfahren für die Endbenutzer im Vergleich zu Kennwörtern**
- **Maschinengebundene Authentifizierung und Autorisierung – die Authentifizierung kann nicht zwischen Maschinen übertragen werden**
- **Unterstützung unterschiedlich starker Authentifizierungsstufen**
- **Unterstützung mehrerer Anmeldedaten**
- **Eine einzige Geste (z. B. Tippen oder Wischen), die zum Herstellen des Zugangs ausreicht**

Einfache Anmeldung steigert die Nutzung digitaler Dienste um 10–20 %

Quelle: McKinsey ClickFox-Studie[13]

So bequem wie eine EC-Karte

Wie einfach die kennwortfreie Anmeldung mit einem YubiKey ist, lässt sich gut am Beispiel der EC-Karte verdeutlichen. Vermutlich haben Sie Ihre EC-Karte überall mit dabei. Sie passen darauf auf und lassen sie nicht offen liegen. Um sie an einem Geldautomaten zu entsperren geben Sie einen kurzen PIN-Code ein. Dieser PIN-Code ändert sich nur sehr selten, falls überhaupt. Sie müssen sich kein Kennwort merken, und dennoch ist der Zugang zum Geldautomaten sehr sicher.

Bei einem kennwortfreien YubiKey ist es ganz ähnlich. Sie haben ihn überall mit dabei. Um ein Gerät zu entsperren – sei es ein PC, ein Smartphone, eine Anlagensteuerung, ein Gesundheitsportal oder irgend ein anderes Gerät – stecken Sie einfach den YubiKey in einen USB-Port oder halten ihn in die Nähe eines NFC-Sensors. Bei Aufforderung tippen Sie dann auf den Schlüssel und geben optional einen PIN-Code ein oder verwenden ein biometrisches Identifizierungsmittel, je nach Anwendung oder Dienst.

Wie beim PIN-Code auf der EC-Karte stellt der FIDO2-PIN-Code den Zugang zum Sicherheitsschlüssel-Mechanismus sicher. Durch den PIN-Code wird der FIDO2-Sicherheitsschlüssel entsperrt, wodurch ein Schlüsselaustausch mit dem Gerät oder dem Dienst gestartet wird, bei dem Sie sich authentifizieren möchten. Das kann ein lokales Gerät, ein entfernter Verzeichnisdienst, eine Website, ein soziales Netzwerk oder ein anderer IT-Dienst sein.

Optional können die Dienste so eingestellt werden, dass die Benutzer ohne PIN-Code oder Gesten authentifiziert werden. So könnte es etwa die für Authentifizierung eines Verkäufers im Einzelhandel ausreichen, wenn er zum Entsperren eines Computersystems kurz seinen Schlüssel an ein NFC-Leser hält. Wenn das Computersystem mit einem Druckpad ausgestattet ist, dass die Anwesenheit eines Benutzers erkennt, kann das System den Benutzer automatisch abmelden, sobald sich der Verkäufer davon entfernt.[12] Da FIDO2 den Authentifizierungsprozess für die Benutzer radikal verändert, sind die zusätzlichen Authentifizierungsmaßnahmen für Unternehmen durchaus sinnvoll – schließlich sind die Prozesse mit FIDO2 so einfach und schnell, dass die Produktivität damit gesteigert und gleichzeitig Supportkosten reduziert werden.

In all diesen Szenarien ist die kennwortfreie Anmeldung mit FIDO2 schneller und sicherer als mit Benutzernamen und Kennwörtern. Die kennwortfreie Anmeldung verändert das Anmeldeverfahren für Anwendungen, Websites, Onlinedienste, Server und Geräte so, wie wir es vom sekundenschnellen Verfahren beim Geldabheben kennen.

Für die kennwortfreie Anmeldung mit FIDO2 ist ein FIDO2-zertifiziertes Authentifizierungsgerät erforderlich, etwa aus der Serie 5 des YubiKey.

FIDO2, WebAuthn und FIDO U2F

Wie funktionieren FIDO2 und WebAuthn zusammen mit FIDO U2F?

U2F ist ein offener Authentifizierungsstandard, der es Hardware-Authentifizierungsgeräten, Smartphones und anderen Geräten ermöglicht, sicher auf eine beliebige Anzahl von webbasierten Diensten zuzugreifen – sofort und ohne Treiber oder Client-Software. U2F entstand in Zusammenarbeit von Google und Yubico unter Beteiligung von NXP und wird heute von der Allianz für lizenzfreie Industriestandards für die offene Authentifizierung, der FIDO Alliance, gehostet.

U2F ist eine starke Authentifizierungsmethode, die als Zwei-Faktor-Lösung auf Benutzername und Kennwort als Erstfaktor angewiesen ist. Das „2F“ in ihrem Namen bezieht sich auf den Zweitfaktor.

FIDO2 ist die zweite Generation von U2F. Es baut auf U2F auf, wobei die erforderlichen Elemente, die eine Identifizierung und Authentifizierung von Benutzern ohne Kennwort ermöglichen, ergänzt wurden. FIDO2 unterstützt starke Ein-, Zwei- und Mehrfaktor-Authentifizierung.

Die WebAuthn-Komponente von FIDO2 ist abwärtskompatibel mit FIDO U2F-Authentifikatoren. Das bedeutet, dass alle zuvor zertifizierten FIDO U2F-Sicherheitsschlüssel inklusive YubiKeys, weiterhin für die Anmeldung mit der Zwei-Faktor-Authentifizierung in Browsern und Onlinediensten, die WebAuthn unterstützen verwendet werden können.

Neue Optionen mit kennwortfreier Anmeldung

Mitarbeiter

Beim Onboarding neuer Mitarbeiter müssen Unternehmen jetzt keine temporären oder sonstigen Kennwörter mehr ausstellen. Stattdessen reicht ein Hardware-Authentifizierungsgerät wie der YubiKey. Mit dem YubiKey kann sich ein Benutzer bei Azure AD oder anderen Diensten authentifizieren, mit oder ohne PIN-Code, je nach Anwendung. Der YubiKey kann auch verwendet werden, um zusätzliche Geräte zu registrieren, zum Beispiel Smartphones oder Laptops, mit denen sich der Nutzer dann ebenfalls authentifizieren kann.

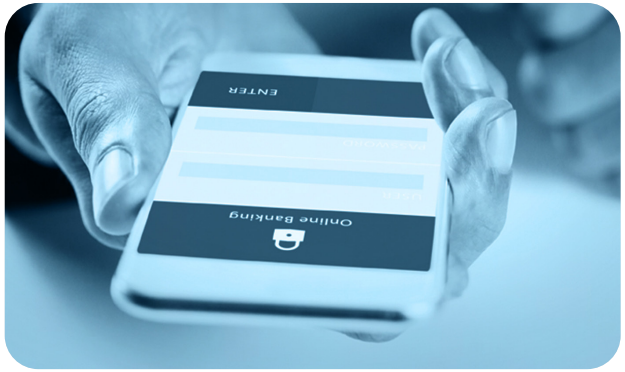
Die Authentifizierung kann so erstaunlich schnell und einfach werden. So kann ein Mitarbeiter im Büro anstatt einen Benutzernamen und ein Kennwort einzugeben sich einfach hinsetzen, den YubiKey drücken und mit der Arbeit loslegen.

Einzelhandel

Verkäufer, Abteilungsleiter, Teamleiter, Kassierer und andere Mitarbeiter im Einzelhandel benötigen schnellen und einfachen Zugang zu IT-Systemen. Die kennwortfreie Anmeldung verschlankt das Onboarding, erleichtert den Zugang und bietet gleichzeitig strenge Authentifizierung als Schutz vor Betrug.

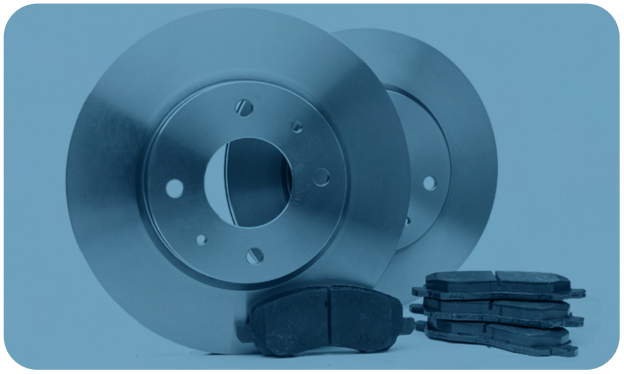
Im Einzelhandel werden häufig Saisonkräfte eingestellt. Beispielsweise gibt es einen nordamerikanischen Einzelhändler, der in der Urlaubssaison üblicherweise 30.000 Saisonarbeiter einstellt. Bisher hätte man für jeden dieser Arbeiter einen Benutzernamen und ein Kennwort benötigt. Mit FIDO2 reicht es aus, einfach Sicherheitsschlüssel zu verteilen. Die Autorisierung für Dienste kann über einen Verzeichnisdienst wie Azure AD zentral deaktiviert werden, sobald die saisonale Aktivität vorbei ist.

FIDO2 erspart der IT-Abteilung das Erstellen, Zurücksetzen und Stornieren von Kennwörtern. Wenn Angestellte wiedereingestellt werden, können ihre Sicherheitsschlüssel einfach reaktiviert und für den Zugang zu Diensten im Geschäft eingestellt werden.



Finanzwesen

Die schnelle und unkomplizierte kennwortfreie Authentifizierung verbessert die Erfahrung mit einer Marke, verschlankt Interaktionen mit Handelspartnern und Kunden und unterstützt Sie sogar bei der Entwicklung neuer Produkte und Dienstleistungen. Kreditinstitute, Genossenschaftsbanken oder andere Finanzinstitutionen, die ihren Kunden Sicherheitsschlüssel und eine kennwortfreie Anmeldung anbieten, reduzieren das Risiko von unerwünschter Anmeldung auf fremden Konten und machen gleichzeitig Kontoinhabern das Leben leichter.



Industrie

Wie bei Einzelhändlern arbeiten auch in der Industrie die Mitarbeiter im Schichtbetrieb. FIDO2 vereinfacht die Zugangsverwaltung für diese sich ständig ändernde Belegschaft. Da die Arbeiter keine Kennwörter eingeben müssen und sich dennoch individuell authentifizieren können, vereinfacht FIDO2 den Zugang zu IT-Systemen und hilft gleichzeitig bei der Einhaltung von Richtlinien zu Sicherheits- und Identitätsmanagement. Gleichzeitig wird das Risiko von Verzögerungen durch Kennwortrichtlinien (z. B. durch verpflichtende regelmäßige Kennwortänderung) und andere Probleme im Betrieb beseitigt.

Das US-Heimatschutzministerium hat davor gewarnt, dass die Industrie nach wie vor ein beliebtes Ziel für Phishing-Angriffe ist, nicht zuletzt, da Hacker an geistigem Eigentum interessiert sind.[14] Indem Firmen „phishbare“ Kennwörter durch FIDO2-Sicherheitsschlüssel ersetzen, schließen sie mit der starken Authentifizierung dieses Einfallstor für Phishing-Angriffe.

Gesundheitswesen

Organisationen im Gesundheitswesen sehen sich verschiedenen Arten von Verletzungen der Datensicherheit ausgesetzt. Gesundheitsdaten, einschließlich Krankengeschichte und Zahlungsinformationen, sind auf dem Schwarzmarkt zehnmal so wertvoll wie Kreditkartendaten.[15] Warum? Weil Betrug im Medizinbereich (etwa durch fälschliches Anfordern von Versicherungsleistungen) ein einträgliches Geschäft ist.

Organisationen im Gesundheitswesen werden häufig von Ransomware-Angriffen getroffen, von denen viele durch Phishing gestartet werden. Indem Kennwörter durch Sicherheitsschlüssel ersetzt werden, können diese Organisationen und ihre Geschäftspartner ihre Anfälligkeit gegenüber solchen Angriffen deutlich senken.

FIDO2 kann auch dabei helfen, sicherzustellen, dass persönliche Gesundheitsdaten nur von autorisierten Benutzern gemäß geltenden Vorschriften aufgerufen werden können. Eine aktuelle Umfrage in der Gesundheitsbranche in den USA hat ergeben, dass 73% aller Ärzte bereits mit einem Kennwort eines Kollegen persönliche Gesundheitsdaten abgerufen haben.[16] Mit einfacheren Anmeldeverfahren verwenden Ärzte eher ihre eigenen Anmeldedaten, um auf persönliche Gesundheitsdaten und andere geschützte Daten und Dienste zuzugreifen, anstatt sie zu teilen. In jedem Fall haben mit der kennwortfreien Anmeldung nur Personen Einblick in die Daten, die sich physisch beim Besitzer des Schlüssels aufhalten. Im Gegensatz dazu können geteilte Kennwörter an jedem Ort eingesetzt werden.

FIDO2 bietet noch einen weiteren wichtigen Vorteil für das Gesundheitswesen: eine schnelle und einfache Authentifizierung. Ärzte und Pflegekräfte müssen sich täglich unzählige Male für jeden einzelnen Patienten, in jedem neuen Raum und auf jedem neuen Gerät extra anmelden. Jetzt erfolgt die Anmeldung dank kennwortfreiem Login sofort und sicherer als zuvor. Das medizinische Personal kann sich auf seine Patienten konzentrieren, anstatt sich mit umständlichen Anmeldeverfahren aufzuhalten.

Anbieter- und Lieferantennetzwerke

Die Zahl der Datenschutzverletzungen im Zusammenhang mit Drittanbietern ist seit 2015 um 22% gestiegen.[17]

Die sicherere Authentifizierung in Partnerportalen mit FIDO2 vereinfacht den Zugang für Partner und beseitigt gleichzeitig das Risiko, dass Kennwörter gestohlen werden, um damit ein Unternehmen über ein Partnerportal zu infiltrieren.

Zudem müssen Unternehmen mit FIDO2 nicht die Identitäten all ihrer Lieferanten verwalten. Stattdessen reicht es, eine „Kein-Kennwort-Politik“ einzuführen und von den Lieferanten und Anbietern die Authentifizierung mit einem Sicherheitsschlüssel zu verlangen. Die Anbieter können FIDO2-Sicherheitsschlüssel leicht selbst beziehen. Diese Art der Zusammenarbeit war zuvor nicht möglich, da andere Authentifizierungsmethoden die Sicherung von Lieferanten-Netzwerken unerschwinglich machten.

Fazit

Schon zu lange haben Kennwörter Endbenutzern, Sicherheitsteams und IT-Abteilungen das Leben schwer gemacht. Durch Sicherheit ohne Kennwörter öffnet FIDO2 das Tor zu einer neuen Zeit in Unternehmens-IT und Kundendienst sowie in der Interaktion von Menschen und Maschine.

Mit der kennwortfreien Anmeldung mit FIDO2 können Unternehmen ihre Netzwerksicherheit erhöhen, IT-Ausgaben senken, die Produktivität steigern und eine neue Klasse profitabler Dienste schaffen, die erst durch die schnelle, bequeme und überall verfügbare sichere Anmeldung möglich werden. Die kennwortfreie Anmeldung bietet:

- **Verbesserte Nutzbarkeit** mit der kennwortfreien Anmeldung müssen sich Nutzer keine Kennwörter mehr merken und die Arbeit zu keiner Zeit unterbrechen, um welche einzugeben. Der Zugang wird schnell und einfach.
- **Gesteigerte Sicherheit** Der Verzicht auf Kennwörter beseitigt die Sicherheitsrisiken durch gestohlene Kennwörter, Kennwort-Phishing und Brute-Force-Angriffe auf einfache Kennwörter.
- **Gesteigerte Effizienz** In einer Welt ohne Kennwörter müssen IT-Administratoren nicht mehr hunderttausende Kennwörter bereitstellen. Die Belastung des IT-Supports nimmt ab, bei gleichzeitig verbesserter Sicherheit und Benutzerfreundlichkeit.

FIDO2 ist eine Lösung, die jetzt für hunderte Millionen Geräte mit Windows 10 mit einem Upgrade auf der letzten Version von Windows 10 verfügbar ist. Es ist eine IT-Lösung, mit der Lieferanten und IT-Abteilungen in Unternehmen arbeiten können, um nicht nur interne IT-Sicherheitsfragen anzugehen, sondern auch die der Kunden.

Wie können die Prozesse für Kunden durch die kennwortfreie Anmeldung verschlankt werden? Wie können Kundenerfahrungen ohne Kennwörter neu gedacht werden? Was, wenn Anwendungen von überall schnell, einfach und sicher aufgerufen werden können?

Welche neuen Produkte und Dienste sind möglich, wenn keine Kennwörter mehr gebraucht werden, wenn Remote-PCs und -Mobilgeräte einfach bereitgestellt und als vertrauenswürdig eingestuft werden können und wenn das Risiko von Datenpannen endlich deutlich abnimmt?

Diese Fragen sollten sich vorausdenkende Unternehmen und IT-Verantwortliche jetzt stellen.

Da die kennwortfreie Anmeldung mit FIDO2 jetzt Realität ist, sind das keine spekulativen Überlegungen von Futuristen mehr, sondern ganz praktische und sogar drängende Fragen – für CISOs, Produktmanager, UX-Designer, Marketingfachleute und andere Profis, deren Ziel es ist, die bestmöglichen Produkte, Dienstleistungen und Erfahrungen bei stets sicherer Authentifizierung bereitzustellen.

Empfehlungen

Wie sollten sich Geschäftsführer, CIOs, CTOs und andere IT-Führungskräfte auf eine Welt ohne Kennwörter vorbereiten? Yubico hat folgende Empfehlungen.

Bleiben Sie auf dem neuesten Stand

Erhalten Sie Updates von Yubico unter www.yubico.com/go-passwordless

Nehmen Sie am Yubico Developer-Programm teil

Entwickler sollten am Yubico Developer-Programm teilnehmen, um Zugang zu Workshops, Open-Source-Software und Entwicklersupport zu erhalten.

Upgraden Sie die Optionen zur Zwei-Faktor-Authentifizierung noch heute

Damit werden FIDO2-Sicherheitsschlüssel unterstützt und Sie sind bereit für die kennwortfreie Anmeldung.

Entwickeln Sie eine Strategie für den „Kennwort-Ausstieg“

Bilden Sie ein Team Ihrer Führungskräfte und IT-Fachleute, um zu erörtern, wie Sie die kennwortfreie Authentifizierung am besten für sich nutzen können. Dabei sollten die Beteiligten zunächst:

- Ein Kostenmodell für Kennwörter entwickeln. Wie viele Anfragen beim Help Desk und in Call Centern stehen in Verbindung mit Kennwörtern? Wie lange dauert eine Anfrage typischerweise? Wie lange dauert es, bis Administrator neuen Benutzern ein Kennwort zugewiesen haben? Wie hoch ist der
- Produktivitätsverlust durch Sperrung von Konten? Bewerten Sie die Zeit und Ausgaben durch die aktuellen Authentifizierungsmethoden, um eine Vorstellung von der potentiellen Kosteneinsparung zu bekommen.
- Pilotprojekte planen, mit denen Ihr Team die kennwortfreie Anmeldung bei einer ausgewählten Gruppe von Benutzern einführen kann. Konzentrieren Sie sich auf Bereiche, bei denen eine starke Authentifizierung nötig ist und ein verbesserter Prozess große Vorteile bringt. Überwachen Sie den Fortschritt der ersten Einführung und beachten Sie die Erfahrungen daraus bei künftigen Einführungen.

Quellenangaben

1. ”2020 State of Password and Authentication Security Behaviors Report”. Ponemon Institute. https://pages.yubico.com/2020-password-and-authentication-report
2. “New Research: Most People Have 70-80 Passwords”. Newswire. https://www.newswire.com/news/new-research-most-people-have-70-80-passwords-21103705
3. “Average Business User Has 191 Passwords”. Security Magazine. https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords
4. Kessem, Limor. “Millennial Habits May Bring An End To The Password Era | SC Media”. SC Media. https://www.scmagazine.com/millennialhabits-may-bring-an-end-to-the-password-era/article/746144/
5. “Data Breach Investigation Report”. Verizon Enterprise. https://enterprise.verizon.com/resources/reports/dbir/2019/introduction/
6. “Most hacked passwords revealed as UK cyber survey exposes gaps in online security”. National Cyber Security Center, 2019 Cyber Security Survey. https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security
7. “Protect your accounts with smarter ways to sign in on World Passwordless Day”. Microsoft. https://www.microsoft.com/security/blog/2020/05/07/protect-accounts-smarter-ways-sign-in-world-passwordless-day/
8. Verizon, ibid.
9. Ward, Kelsey. “Credential stuffing rules the day as 90% of login attempts no longer made by humans”. Secureidnews.com. https://www.secureidnews.com/news-item/credential-stuffing-rules-the-day-as-90-of-login-attempts-no-longer-made-by-humans/
10. “Statistic: the total market share of Windows 10 version 1903/1909 edition reach 75.2%”. Meterpreter. https://meterpreter.org/statistic-the-total-market-share-of-windows-10-version-1903-1909-edition-reach-75-2/
11. “NIST SP 800-63 Digital Identity Guidelines”. Nist.Gov. https://www.nist.gov/itl/tig/projects/special-publication-800-63
12. “Pcprox® Mat | RF Ideas”. Rfideas.Com. https://www.rfideas.com/products/presence-detectors/pcprox-mat
13. “Is Cybersecurity Incompatible With Digital Convenience?” McKinsey & Company. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience
14. “Energy Sector Tops List Of US Industries Under Cyber Attack, Says Homeland Security Report - Iot Now - How To Run An Iot Enabled Business”. Iot Now - How To Run An Iot Enabled Business. https://www.iot-now.com/2015/03/12/30962-energy-sector-stays-top-of-the-list-ofus-industries-under-cyber-attack-says-homeland-security-report
15. “Your Medical Record Is Worth More To Hackers Than Your Credit Card”. Reuters. https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924
16. “Survey Reveals Sharing EHR Passwords is Commonplace”. HIPAA Journal. https://www.hipaajournal.com/sharing-ehr-passwords-commonplace/
17. “Data trust pacesetters show how to create and protect value from data”. PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity/data-trust-pacesetters.html

yubico

Über Yubico Yubico setzt weltweit neue Maßstäbe für den einfachen und sicheren Zugriff auf Computer, Server und Online-Konten. Das 2007 gegründete Privatunternehmen Yubico unterhält Niederlassungen in Australien, Deutschland, Singapur, Schweden, Großbritannien sowie in den USA. Erfahren Sie, warum die Top-10-Internetmarken und Millionen Benutzer in über 160 Ländern unsere Technologie nutzen: **www.yubico.com.**

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Schweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787
650-285-0088