RESOURCE CENTER

Bericht zum Stand der Passwortsicherheit 2024

Wie Bundesbehörden die Passwortsicherheit angehen

Get the full interactive view at
https://bitwarden.com/de-de/resources/the-state-of-password-security/

bitwarden

Bewertung des Zustands der Passwortsicherheit innerhalb der US-Bundesbehörden

In den letzten Jahren wurde ein intensiver Fokus auf die Cybersicherheit in der gesamten Bundesregierung der Vereinigten Staaten gelegt, wobei viele Behörden bei der Aufklärung von Regierungsorganisationen und großen und kleinen Unternehmen sowie von Verbrauchern führend waren.

Wenn es jedoch um die Passwortsicherheit geht, singt nicht jede Agentur die gleiche Melodie. Eine der führenden Gruppen, das National Institute of Standards and Technology (NIST), "entwickelt Cybersicherheitsstandards, Richtlinien, Best Practices und andere Ressourcen, um die Bedürfnisse der US-Industrie, der Bundesbehörden und der breiten Öffentlichkeit zu erfüllen."

Auf der NIST-Cybersicherheitsseite heißt es weiter: „Einige NIST-Cybersicherheitsaufgaben werden durch Bundesgesetze, Durchführungsverordnungen und Richtlinien definiert. Zum Beispiel schreibt das Office of Management and Budget (OMB) vor, dass alle Bundesbehörden die Cybersicherheitsstandards und -richtlinien von NIST für nicht-nationale Sicherheitssysteme umsetzen."

Leider wurden die Empfehlungen von NIST noch nicht von allen Bundesbehörden allgemein akzeptiert und umgesetzt. Und während NIST die Standards festlegt, denen Agenturen angeblich folgen, hat selbst NIST seine eigene Schwäche in Form einer unorganisierten Website.

2024 ist das dritte Jahr, in dem Bitwarden diese Analyse durchgeführt hat. Im Laufe von drei Jahren ist die NIST-Website unorganisiert geblieben, obwohl ihr Inhalt sehr solide ist. Es gab auch einige positive Entwicklungen. Das Weiße Haus hat die Verbreitung von Ratschlägen zur Passwortsicherheit verbessert und von einem „Raum für Verbesserungen“ zu einer „guten“ Bewertung übergegangen. Andere Agenturen, die sich in Bezug auf ihre Empfehlungen zur Passwortsicherheit und die allgemeine Cybersicherheitslage in eine bessere Richtung entwickelt haben, sind die Cybersecurity and Infrastructure Security Association (CISA), das Federal Bureau of Investigation (FBI), die Federal Trade Commission (FTC) und die Small Business Administration (SBA).

In diesem Jahr hat Bitwarden auch die Securities and Exchange Commission (SEC) zu diesem Bericht hinzugefügt. Im vergangenen Jahr verabschiedete die SEC Vorschriften, nach denen Unternehmen wesentliche Cybersicherheitsvorfälle offenlegen müssen. Angesichts der Rolle der SEC bei der Durchsetzung der Cybersicherheits-Compliance wird in diesem Bericht die eigene Passwortsicherheitsempfehlung der SEC bewertet.

Die Technologie bewegt sich schnell. Für Unternehmen und Privatpersonen ist ein Großteil unseres Lebens jetzt auf einer Vielzahl von Konten online, die von unterhaltsamen Unterhaltungsseiten bis hin zu ernsthaften Finanzgeschäften wie unseren Bankkonten reichen.

Das Ziel dieser Bewertung ist es, jeden, der Passwörter verwendet, über die besten Praktiken der Bundesregierung zu informieren und aufzuklären, wo es Raum für Verbesserungen gibt. Es gibt viele in der Bundesregierung, die einen soliden pädagogischen Ansatz zur Passwortsicherheit haben, und es gibt andere, die möglicherweise ein wenig Unterstützung bei der Modernisierung benötigen.

Glücklicherweise baut der Konsens auf Best Practices für die Passwortsicherheit auf. Dieser Bericht konsolidiert und bewertet die Details.

The State of Password Security: How federal agencies are addressing password security

Download

Zeigen Sie den Status der Passwortsicherheitspräsentation an

Inhaltsverzeichnis

Richtlinie zum Passwortsicherheitsbewertungssystem

Das Bewertungssystem stuft Agenturen nach der Einhaltung der folgenden Kriterien ein:

Excellent

- Empfiehlt die Verwendung eines Passwort-Managers
- Weist auf die Bedeutung von starken Passwörtern hin
- Zitate benötigen 2FA/MFA, um die Passwortsicherheit weiter zu unterstützen
- Die allgemeine Sicherheitsberatung ist auf dem neuesten Stand und entspricht den NIST-Richtlinien
- Legt Passwortsicherheitsempfehlungen klar, verständlich und leicht zu finden fest

Very Good

- Empfiehlt die Verwendung eines Passwort-Managers
- Weist auf die Bedeutung von starken Passwörtern hin
- Zitate benötigen 2FA/MFA, um die Passwortsicherheit weiter zu unterstützen
- Die allgemeine Sicherheitsberatung ist auf dem neuesten Stand und entspricht den NIST-Richtlinien
- Legt Passwortsicherheitsempfehlungen nicht klar, verständlich und leicht zu finden dar

Good

- Empfiehlt nicht die Verwendung eines Passwort-Managers
- Weist auf die Bedeutung von starken Passwörtern hin
- Zitate benötigen 2FA/MFA, um die Passwortsicherheit weiter zu unterstützen
- Die allgemeine Sicherheitsempfehlung ist nicht auf dem neuesten Stand und entspricht nicht den NIST-Richtlinien
- Legt Passwortsicherheitsempfehlungen nicht klar, verständlich und leicht zu finden dar

Fair

- Empfiehlt nicht die Verwendung eines Passwort-Managers

- Weist auf die Bedeutung von starken Passwörtern hin
- Zitiert nicht konsequent die Notwendigkeit von 2FA/MFA, um die Passwortsicherheit weiter zu unterstützen
- Die allgemeine Sicherheitsempfehlung ist nicht auf dem neuesten Stand und entspricht nicht den NIST-Richtlinien
- Legt Passwortsicherheitsempfehlungen nicht klar, verständlich und leicht zu finden dar

Room for Improvement

- Empfiehlt nicht die Verwendung eines Passwort-Managers
- Weist nicht auf die Wichtigkeit von starken Passwörtern hin
- Nennt nicht die Notwendigkeit von 2FA/MFA zur weiteren Unterstützung der Passwortsicherheit
- Die allgemeine Sicherheitsempfehlung ist nicht auf dem neuesten Stand und entspricht nicht den NIST-Richtlinien
- Legt Passwortsicherheitsempfehlungen nicht klar, verständlich und leicht zu finden dar

Nationales Institut für Standards und Technologie (NIST)

NIST-Risikomanagement-Framework | IA-5(18)

Agenturberatung:

- Authenticator Management | Passwort-Manager
  - Stellen Sie [Assignment: Organization-defined password managers] ein, um Passwörter zu generieren und zu verwalten; und
    - Schützen Sie die Passwörter mit [assignment: organization-defined controls].
    - Für Systeme, in denen statische Passwörter verwendet werden, ist es oft eine Herausforderung, sicherzustellen, dass die Passwörter angemessen komplex sind und dass nicht dieselben Passwörter auf mehreren Systemen verwendet werden. Ein Passwort-Manager ist eine Lösung für dieses Problem, da er automatisch starke und unterschiedliche Passwörter für verschiedene Konten generiert und speichert. Ein potenzielles Risiko bei der Verwendung von Passwort-Managern besteht darin, dass Gegner die Sammlung von Passwörtern, die vom Passwort-Manager generiert werden, gezielt einsetzen können. Daher muss die Sammlung von Passwörtern geschützt werden, einschließlich der Verschlüsselung der Passwörter und der Offline-Speicherung der Sammlung in einem Token.

- Zeugnis

Richtlinien zur digitalen Identität

Agenturberatung:

- Auswendig gelernte Geheimnisse MÜSSEN mindestens 8 Zeichen lang sein, wenn sie vom Abonnenten ausgewählt werden. Auswendig gelernte Geheimnisse, die vom CSP oder Verifizierer zufällig ausgewählt werden, MÜSSEN mindestens 6 Zeichen lang sein und KÖNNEN vollständig numerisch sein. Wenn der CSP oder Verifizierer ein ausgewähltes gespeichertes Geheimnis aufgrund seines Auftretens auf einer schwarzen Liste kompromittierter Werte ablehnt, muss der Abonnent ein anderes gespeichertes Geheimnis auswählen. Es SOLLTEN keine anderen Komplexitätsanforderungen für auswendig gelernte Geheimnisse auferlegt werden. Eine Begründung dafür finden Sie in Anhang A Strength of Memorized Secrets.

- Verifizierer MÜSSEN verlangen, dass die vom Abonnenten gewählten gespeicherten Geheimnisse mindestens 8 Zeichen lang sind. Verifizierer SOLLTEN vom Abonnenten ausgewählte gespeicherte Geheimnisse mit einer Länge von mindestens 64 Zeichen zulassen. Alle Druckzeichen ASCII [RFC 20] sowie das Leerzeichen SOLLTEN in auswendig gelernten Geheimnissen akzeptabel sein. Unicode-Zeichen [ISO/ISC 10646] SOLLTEN ebenfalls akzeptiert werden. Um wahrscheinliche Tippfehler zu berücksichtigen, KÖNNEN Verifizierer vor der Verifizierung mehrere aufeinanderfolgende Leerzeichen durch ein einzelnes Leerzeichen ersetzen, vorausgesetzt, das Ergebnis ist mindestens 8 Zeichen lang. Eine Kürzung des Geheimnisses DARF NICHT vorgenommen werden. Für die Zwecke der oben genannten Längenanforderungen WIRD jeder Unicode-Codepunkt als ein einzelnes Zeichen gezählt.

- Auswendig gelernte Geheimnisse, die vom CSP (z. B. bei der Registrierung) oder vom Prüfer (z. B. wenn ein Benutzer eine neue PIN anfordert) zufällig ausgewählt werden, MÜSSEN mindestens 6 Zeichen lang sein und mit einem genehmigten Zufallsbitgenerator [SP 800-90Ar1] generiert werden.

- Auswendig gelernte geheime Verifizierer DÜRFEN dem Abonnenten NICHT erlauben, einen "Hinweis" zu speichern, auf den ein nicht authentifizierter Antragsteller zugreifen kann. Verifizierer DÜRFEN ABONNENTEN NICHT auffordern, bestimmte Arten von Informationen zu verwenden (z. B. „Wie hieß Ihr erstes Haustier?“), wenn sie auswendig gelernte Geheimnisse auswählen.

- Bei der Bearbeitung von Anfragen zur Einrichtung und Änderung gespeicherter Geheimnisse müssen die PRÜFER die potenziellen Geheimnisse mit einer Liste vergleichen, die Werte enthält, von denen bekannt ist, dass sie häufig verwendet, erwartet oder kompromittiert werden. Zum Beispiel KANN die Liste umfassen, ist aber nicht beschränkt auf:
  - Passwörter, die aus früheren Verstößen stammen.
  - Wörterbuchwörter.
  - Wiederholte oder aufeinanderfolgende Zeichen (z. B. ‘aaaaaa’, ‘1234abcd’).
  - Kontextspezifische Wörter, wie der Name des Dienstes, der Benutzername und Ableitungen davon.

- Wenn das gewählte Geheimnis in der Liste gefunden wird, TEILT der CSP oder Verifizierer dem Abonnenten mit, dass er ein anderes Geheimnis auswählen MUSS, GIBT den Grund für die Ablehnung an und fordert den Abonnenten auf, einen anderen Wert zu wählen.

- Verifizierer SOLLTEN dem Abonnenten eine Anleitung bieten, z. B. ein Kennwortstärkemessgerät [Meter], um den Benutzer bei der Auswahl eines starken gespeicherten Geheimnisses zu unterstützen. Dies ist besonders wichtig nach der Ablehnung eines auswendig gelernten Geheimnisses auf der obigen Liste, da es triviale Modifikationen von gelisteten (und wahrscheinlich sehr schwachen) auswendig gelernten Geheimnissen [Blacklists] verhindert.

- Die VERIFIZIERER MÜSSEN einen Ratenbegrenzungsmechanismus implementieren, der die Anzahl der fehlgeschlagenen Authentifizierungsversuche, die auf dem Konto des Abonnenten durchgeführt werden können, wie in Abschnitt 5.2.2 beschrieben, wirksam begrenzt.

- Verifizierer SOLLTEN für gespeicherte Geheimnisse KEINE anderen Regeln für die Zusammensetzung aufstellen (z. B. Mischungen verschiedener Zeichentypen erfordern oder aufeinanderfolgend wiederholte Zeichen verbieten). Verifizierer SOLLTEN NICHT verlangen, dass gespeicherte Geheimnisse willkürlich (z. B. in regelmäßigen Abständen) geändert werden. DIE Verifizierer erzwingen jedoch eine Änderung, wenn es Hinweise auf eine Kompromittierung des Authentifizierers gibt.

- Verifizierer SOLLTEN es den Antragstellern ermöglichen, die "Einfügen" -Funktionalität zu verwenden, wenn sie ein gespeichertes Geheimnis eingeben. Dies erleichtert die Verwendung von Passwort-Managern, die weit verbreitet sind und in vielen Fällen die Wahrscheinlichkeit erhöhen, dass Benutzer stärkere gespeicherte Geheimnisse wählen.

- Um den Antragsteller bei der erfolgreichen Eingabe eines gespeicherten Geheimnisses zu unterstützen, SOLLTE der Prüfer eine Option anbieten, das Geheimnis — und nicht eine Reihe von Punkten oder Sternchen — anzuzeigen, bis es eingegeben wird. Dies ermöglicht es dem Antragsteller, seine Eingabe zu überprüfen, wenn er sich an einem Ort befindet, an dem sein Bildschirm wahrscheinlich nicht zu sehen ist. Der Verifikator KANN es dem Gerät des Benutzers auch ermöglichen, einzelne eingegebene Zeichen für kurze Zeit anzuzeigen, nachdem jedes Zeichen eingegeben wurde, um die korrekte Eingabe zu überprüfen. Dies gilt insbesondere für mobile Endgeräte.

- Der Verifizierer verwendet eine genehmigte Verschlüsselung und einen authentifizierten geschützten Kanal, wenn er gespeicherte Geheimnisse anfordert, um Widerstand gegen Abhören und MitM-Angriffe zu leisten.

- Verifizierer speichern gespeicherte Geheimnisse in einer Form, die gegen Offline-Angriffe resistent ist. Auswendig gelernte Geheimnisse MÜSSEN mit einer geeigneten Einweg-Schlüsselableitungsfunktion gesalzen und gehasht werden. Schlüsselableitungsfunktionen nehmen ein Passwort, ein Salt und einen Kostenfaktor als Eingaben und generieren dann einen Passwort-Hash. Ihr Zweck ist es, jede Passwort-Rätselraten-Testversion durch einen Angreifer, der eine Passwort-Hash-Datei erhalten hat, teuer zu machen und damit die Kosten für einen Rätselraten-Angriff hoch oder unerschwinglich zu machen. Beispiele für geeignete Schlüsselableitungsfunktionen sind die passwortbasierte Schlüsselableitungsfunktion 2 (PBKDF2) [SP 800-132] und der Ballon [BALLON]. Eine Memory-Hard-Funktion SOLLTE verwendet werden, da sie die Kosten eines Angriffs erhöht. Die Schlüsselableitungsfunktion verwendet eine genehmigte Einwegfunktion wie Keyed Hash Message Authentication Code (HMAC) [FIPS 198-1], jede genehmigte Hash-Funktion in SP 800-107, Secure Hash Algorithm 3 (SHA-3) [FIPS 202], CMAC [SP 800-38B] oder Keccak Message Authentication Code (KMAC), Customizable SHAKE (cSHAKE) oder ParallelHash [SP 800-185]. Die gewählte Ausgabelänge der Tastenableitungsfunktion SOLLTE gleich der Länge der zugrunde liegenden Einwegfunktionsausgabe sein.

- Das Salz MUSS mindestens 32 Bit lang sein und willkürlich gewählt werden, um Salzwertkollisionen zwischen gespeicherten Hashes zu minimieren. Sowohl der Salzwert als auch der resultierende Hash WERDEN für jeden Teilnehmer unter Verwendung eines gespeicherten geheimen Authentifikators gespeichert.

- Für PBKDF2 ist der Kostenfaktor eine Iterationszählung: Je öfter die PBKDF2-Funktion iteriert wird, desto länger dauert es, den Passwort-Hash zu berechnen. Daher SOLLTE die Anzahl der Iterationen so groß sein, wie es die Verifizierungsserverleistung zulässt, in der Regel mindestens 10.000 Iterationen.

- Darüber hinaus SOLLTEN Verifizierer eine zusätzliche Iteration einer Schlüsselableitungsfunktion mit einem Salt-Wert durchführen, der geheim ist und nur dem Verifizierer bekannt ist. Dieser Salzwert, falls verwendet, MUSS von einem zugelassenen Zufallsbitgenerator [SP 800-90Ar1] erzeugt werden und mindestens die in der neuesten Version von SP 800-131A angegebene Mindestsicherheitsstärke (112 Bits zum Datum dieser Veröffentlichung) bereitstellen. Der geheime Salzwert WIRD getrennt von den gehashten gespeicherten Geheimnissen gespeichert (z. B. in einem speziellen Gerät wie einem Hardware-Sicherheitsmodul). Mit dieser zusätzlichen Iteration sind Brute-Force-Angriffe auf die gehashten gespeicherten Geheimnisse unpraktisch, solange der geheime Salzwert geheim bleibt.

- Cybersecurity Awareness Month 2023 Blog-Serie
  - Agenturberatung
    - Passwörter sind nach wie vor der am weitesten verbreitete Authentifizierungsmechanismus, um Zugang zu Ressourcen von Interesse zu erhalten. Passwörter sind die erste Verteidigungslinie, um die Vertraulichkeit und Integrität der Daten vor Cyberkriminellen und Datenschutzverletzungen zu schützen. Gute, starke Passwörter helfen Menschen, online sicher und privat zu bleiben.

- Zeugnis

NIST

bitwarden

Nationales Institut für Standards und Technologie (NIST)

Gesamtbeurteilung Bitwarden: Sehr gut

- Empfiehlt die Verwendung eines Passwort-Managers
- Weist auf die Bedeutung von starken Passwörtern hin
- Zitate benötigen 2FA/MFA, um die Passwortsicherheit weiter zu unterstützen
- Die allgemeine Sicherheitsberatung ist auf dem neuesten Stand und entspricht den NIST-Richtlinien (NIST setzt den Standard für die Sicherheitsberatung der Bundesregierung)
- Legt Passwortsicherheitsempfehlungen nicht klar, verständlich und leicht zu finden dar

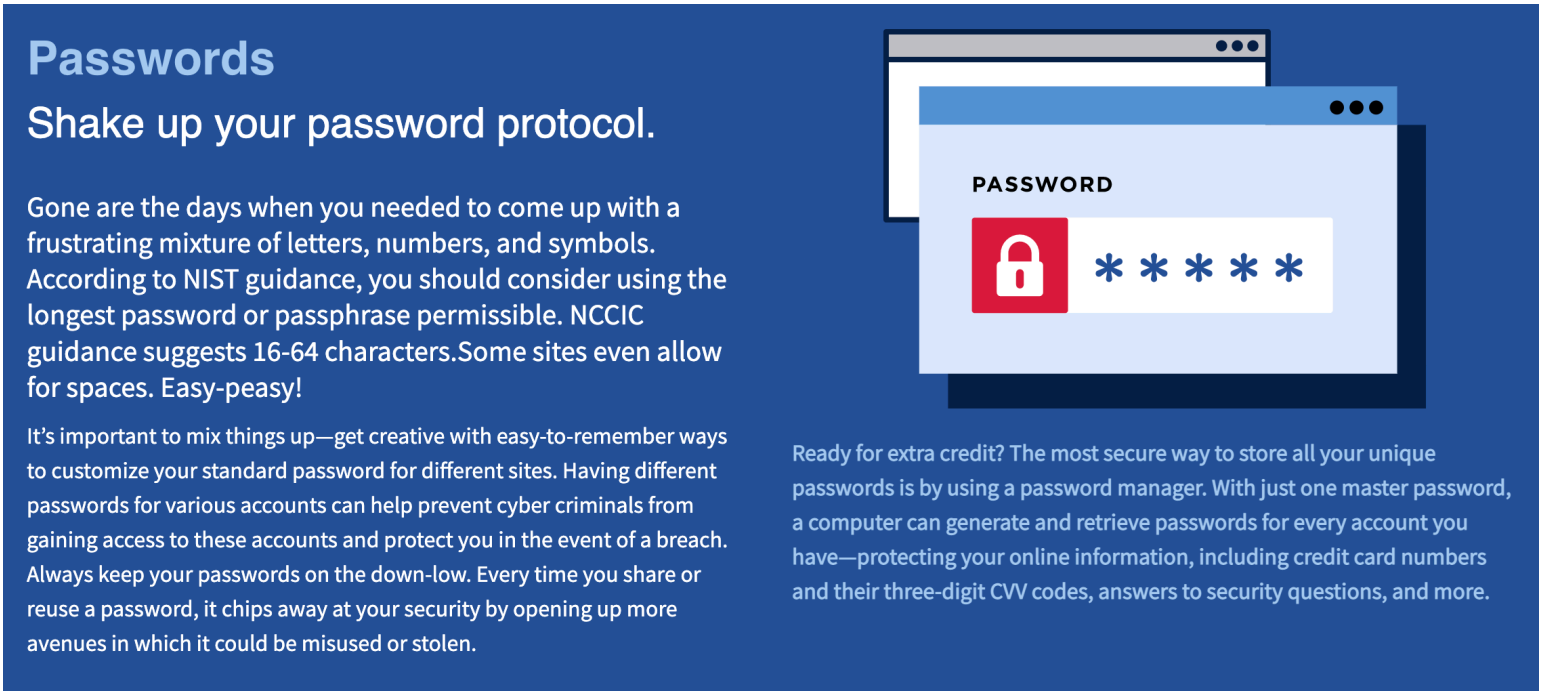
Die Beratung ist zwar gründlich und legt die Standards für Agenturen fest, die über die Website auf Passwortrichtlinien zugreifen, ist jedoch nicht intuitiv. Der Ratschlag ist in sehr langen PDFs vergraben und auf eine Weise geschrieben, die nicht benutzerfreundlich ist.

"Verifiers SHOULD permit claimants to use “paste” functionality when entering a memorized secret. This facilitates the use of password managers, which are widely used and in many cases increase the likelihood that users will choose stronger memorized secrets."

NIST

Agentur für Cybersicherheit und Infrastruktursicherheit (CISA)

Cyber-Lektionen



Cyber-Lektionen zu Passwörtern, CISA

- Zeugnis

Anleitung zum Stoppen von Ransomware

Agenturberatung:

- Implementieren Sie Passwortrichtlinien, die eindeutige Passwörter mit mindestens 15 Zeichen erfordern
  - Passwort-Manager können Ihnen helfen, sichere Passwörter zu entwickeln und zu verwalten. Sichern und beschränken Sie den Zugriff auf alle verwendeten Passwort-Manager und aktivieren Sie alle Sicherheitsfunktionen, die auf dem verwendeten Produkt verfügbar sind, wie z. B. MFA.

- Zeugnis

Sichern Sie unsere Welt: Erfordern Sie sichere Passwörter

Agenturberatung:

- Kleine bis mittlere Unternehmen sind ein regelmäßiges Ziel für böswillige Hacker und ein häufiger Einstiegspunkt für digitale Diebe sind gestohlene oder schwache Passwörter.

- Aber die gute Nachricht ist, dass Sie Ihr Unternehmen schützen können, indem Sie von Ihren Mitarbeitern starke Passwörter und Passwort-Manager verlangen.

- Gehen Sie mit gutem Beispiel voran, indem Sie lange, zufällige, eindeutige Passwörter für alle Ihre persönlichen und geschäftlichen Konten verwenden - und verwenden Sie einen Passwort-Manager, um sich an sie zu erinnern! Arbeiten Sie dann mit Ihren IT-Mitarbeitern oder Ihrem Anbieter zusammen, um von den Mitarbeitern zu verlangen, dass sie starke Passwörter verwenden, um auf Ihre Systeme zuzugreifen. So bleiben Ihre Daten sicher und geschützt.

- Zeugnis

Sichern Sie unsere Welt: Schwache Passwörter

Agenturberatung:

- Lassen Sie einen Passwort-Manager die Arbeit machen! Ein Passwort-Manager erstellt, speichert und füllt automatisch Passwörter für uns. Dann müssen wir uns jeweils nur noch ein sicheres Passwort merken - für den Passwort-Manager selbst. Suchen Sie in vertrauenswürdigen Quellen nach „Passwort-Managern“ wie Consumer Reports, die eine Auswahl an hoch bewerteten Passwort-Managern bieten. Lies Bewertungen, um Optionen zu vergleichen und ein seriöses Programm für dich zu finden.

- Zeugnis

Excellent

bitwarden

Agentur für Cybersicherheit und Infrastruktursicherheit (CISA)

Gesamtbeurteilung Bitwarden: Sehr gut

- Empfiehlt die Verwendung eines Passwort-Managers
- Weist auf die Bedeutung von starken Passwörtern hin
- Zitate benötigen 2FA/MFA, um die Passwortsicherheit weiter zu unterstützen
- Die allgemeine Sicherheitsberatung ist auf dem neuesten Stand und entspricht den NIST-Richtlinien
- Legt Passwortsicherheitsempfehlungen nicht klar, verständlich und leicht zu finden dar

Die National Security Agency (NSA)

Anleitung zum Stoppen von Ransomware

Agenturberatung:

- Implementieren Sie Passwortrichtlinien, die eindeutige Passwörter mit mindestens 15 Zeichen erfordern
  - Passwort-Manager können Ihnen helfen, sichere Passwörter zu entwickeln und zu verwalten. Sichern und beschränken Sie den Zugriff auf alle verwendeten Passwort-Manager und aktivieren Sie alle Sicherheitsfunktionen, die auf dem verwendeten Produkt verfügbar sind, wie z. B. MFA.

- Zeugnis

Cisco-Passworttypen: Best Practices

Agenturberatung:

- Der Anstieg der Anzahl von Kompromittierungen von Netzwerkinfrastrukturen in den letzten Jahren erinnert daran, dass die Authentifizierung bei Netzwerkgeräten eine wichtige Überlegung ist. Netzwerkgeräte könnten kompromittiert werden durch:
  - Schlechte Passwortauswahl (anfällig für Brute-Force-Passwortspritzen)
  - Router-Konfigurationsdateien (die gehashte Passwörter enthalten), die per unverschlüsselter E-Mail gesendet werden, oder
  - Wiederverwendete Passwörter (bei denen Passwörter, die von einem kompromittierten Gerät wiederhergestellt wurden, dann verwendet werden können, um andere Geräte zu kompromittieren).

- Die Verwendung von Passwörtern allein erhöht das Risiko der Geräteausnutzung. Während die NSA Administratoren, die kritische Geräte verwalten, dringend eine Multi-Faktor-Authentifizierung empfiehlt, müssen manchmal nur Passwörter verwendet werden. Die Wahl guter Passwortspeicheralgorithmen kann die Ausnutzung erheblich erschweren.

- Um so viel Schutz wie möglich zu bieten, verwenden Sie starke Passwörter, um zu verhindern, dass sie geknackt und in Klartext konvertiert werden. Halten Sie sich an eine Passwortrichtlinie, die:
  - Besteht aus einer Kombination von Klein- und Großbuchstaben, Symbolen und Zahlen;

- Mindestens 15 alphanumerische Zeichen umfasst; und
- Muster, die nicht:
  - Ein Tastaturspaziergang
  - Entspricht einem Benutzernamen
  - Das Standardpasswort
  - Das gleiche wie ein Passwort, das irgendwo anders verwendet wird
  - Bezogen auf das Netzwerk, die Organisation, den Standort oder andere Funktionskennungen
  - Direkt aus einem Wörterbuch, gebräuchliche Akronyme oder leicht zu erraten
- Zeugnis

Sichere Nutzung von Social Media

Agenturberatung:

- Sichern und stärken Sie Ihre Passwörter
  - Verwenden Sie eindeutige und sichere Passwörter für jedes Online-Konto. Die Wiederverwendung von Passwörtern über mehrere Konten hinweg kann Daten aus allen Konten freigeben, wenn das Passwort entdeckt wird. Achte darauf, dass dein Passwort ausreichend lang und komplex ist, indem du eine Kombination aus Buchstaben, Zahlen und Sonderzeichen verwendest. Wenn möglich, solltest du eine Multi-Faktor-Authentifizierung mithilfe eines Authentifizierungstokens oder einer -App implementieren, damit niemand auf dein Konto zugreifen kann, selbst wenn dein Passwort kompromittiert wurde. Teilen Sie niemals Passwörter und vermeiden Sie es, Informationen zu verwenden, die anhand Ihrer Social-Media-Profile oder öffentlichen Informationen erraten werden könnten.
- Zeugnis

Sichere Multi-Faktor-Authentifizierungslösungen auswählen

Agenturberatung:

- Multi-Faktor-Authentifizierungsmechanismen mit einer einzigen Antwort erfordern die Aktivierung des Geräts, entweder mit einer PIN/einem Passwort oder biometrisch. Das Gerät liefert "was Sie haben" und die Aktivierung des Geräts impliziert, dass "was Sie wissen" oder "was Sie sind" verifiziert wurde.
- Auf der anderen Seite enthalten mehrstufige Authentifikatoren oft ein Passwort, um das zu liefern, was Sie wissen, und einen anderen Authentifikator, der das bietet, was Sie haben. US-Regierungsbehörden sollten die Anforderungen für die PIN-/Passwortaktivierung sowie für die Passwörter berücksichtigen, die direkt verwendet werden, um „was Sie wissen“ bereitzustellen. Die Richtlinien in SP 800-63-3 Teil B weisen darauf hin, dass gespeicherte Geheimnisse (sowohl für die Aktivierung als auch als Einzelfaktor-Authentifikator) mindestens 6 bis 8 Zeichen lang sein müssen, und empfehlen eine höhere Passwortstärke für vom Benutzer ausgewählte Passwörter. Beachten Sie bei der Bestimmung der Passwortanforderungen, dass Multi-Faktor-Geräte strenge Schwellenwerte integrieren sollten, um Angriffe auf das Erraten von Passwörtern zu bekämpfen, während Verifizierer möglicherweise weniger strenge Schwellenwertmechanismen verwenden, die garantieren, dass Passwörter, die direkt verwendet werden, höhere Anforderungen an die Festigkeit stellen.
- Zeugnis

Very Good

bitwarden

Die National Security Agency (NSA)

Gesamtbeurteilung Bitwarden: Gut

- Empfiehlt nicht die Verwendung eines Passwort-Managers
- Weist auf die Bedeutung von starken Passwörtern hin
- Zitate benötigen 2FA/MFA, um die Passwortsicherheit weiter zu unterstützen
- Die allgemeine Sicherheitsberatung ist nicht auf dem neuesten Stand und entspricht den NIST-Richtlinien
- Legt Passwortsicherheitsempfehlungen nicht klar, verständlich und leicht zu finden dar

> "Disable the feature that allows web browsers to remember your passwords. Secure your passwords in a password manager."
>
> **NSA**

Department of Homeland Security

CISA fällt unter das DHS

Cybersicherheitsseite

Agenturberatung:

- Präsident Biden hat die Cybersicherheit, ein kritisches Element der Mission des Department of Homeland Security (DHS), zu einer obersten Priorität für die Biden-Harris-Administration auf allen Regierungsebenen gemacht.
- Um das Engagement des Präsidenten voranzutreiben und zu reflektieren, dass die Stärkung der Cybersicherheitsresilienz des Landes für das DHS oberste Priorität hat, rief Minister Mayorkas in seinem ersten Monat im Amt zu Maßnahmen auf, die sich der Cybersicherheit widmen. Dieser Aufruf zum Handeln konzentrierte sich auf die Bewältigung der unmittelbaren Bedrohung durch Ransomware und den Aufbau einer robusteren und vielfältigeren Belegschaft.
- Im März 2021 skizzierte Minister Mayorkas seine umfassendere Vision und einen Fahrplan für die Cybersicherheitsbemühungen des Ministeriums in einer virtuellen Adresse, die von der RSA-Konferenz in Zusammenarbeit mit der Hampton University und den Girl Scouts der USA veranstaltet wurde.
- Nach seiner Präsentation wurde der Sekretär von Judith Batty, Interims-CEO der Girls Scouts, zu einem Kamingespräch begleitet, um die beispiellosen Cybersicherheitsherausforderungen zu diskutieren, vor denen die Vereinigten Staaten derzeit stehen. Dr. Chutima Boonthum-Denecke von der Informatikabteilung der Hampton University stellte den Sekretär vor und ermöglichte eine Fragerunde zum Abschluss des Programms.
  - Überblick über DHS Cybersecurity Sprints

Room for Improvement

bitwarden

Department of Homeland Security

Gesamtbeurteilung Bitwarden: Raum für Verbesserungen

- Empfiehlt nicht die Verwendung eines Passwort-Managers
- Weist nicht auf die Wichtigkeit von starken Passwörtern hin
  - Bietet ungenaue und fehlgeleitete Passwortsicherheitshinweise oder erwähnt keine Passwörter oder Passwortsicherheit
  - Ruft nicht eindeutig passwortbezogene Ratschläge aus
- Zitiert nicht konsequent die Notwendigkeit von 2FA/MFA, um die Passwortsicherheit weiter zu unterstützen
- Die allgemeine Sicherheitsempfehlung ist nicht auf dem neuesten Stand und entspricht nicht den NIST-Richtlinien
- Legt Passwortsicherheitsempfehlungen nicht klar, verständlich und leicht zu finden dar

Federal Bureau of Investigation (FBI)

Die Cyber-Bedrohung

Agenturberatung:

- Internetfähige Straftaten und Cyberangriffe werden immer ausgefeilter, und um sie zu verhindern, muss jeder Benutzer eines angeschlossenen Geräts auf der Hut sein.
- Halten Sie Systeme und Software auf dem neuesten Stand und installieren Sie ein starkes, seriöses Antivirenprogramm.
- Seien Sie vorsichtig, wenn Sie sich mit einem öffentlichen WLAN-Netzwerk verbinden, und führen Sie keine sensiblen Transaktionen, einschließlich Einkäufe, durch, wenn Sie sich in einem öffentlichen Netzwerk befinden.
- Erstellen Sie eine starke und einzigartige Passphrase für jedes Online-Konto und ändern Sie diese Passphrasen regelmäßig.
- Richten Sie die Multi-Faktor-Authentifizierung für alle Konten ein, die dies zulassen.
- Überprüfen Sie die E-Mail-Adresse in der gesamten Korrespondenz und überprüfen Sie Website-URLs, bevor Sie auf eine Nachricht antworten oder eine Website besuchen
- Klicken Sie in unerwünschten E-Mails oder Textnachrichten auf nichts.
- Seien Sie vorsichtig bei den Informationen, die Sie in Online-Profilen und Social-Media-Konten teilen. Das Teilen von Dingen wie Kosenamen, Schulen und Familienmitgliedern kann Betrügern die Hinweise geben, die sie benötigen, um Ihre Passwörter oder die Antworten auf die Sicherheitsfragen Ihres Kontos zu erraten.
- Senden Sie keine Zahlungen an unbekannte Personen oder Organisationen, die finanzielle Unterstützung suchen, und fordern Sie sofortige Maßnahmen.
- Zeugnis

Betrug und Sicherheit im Internet

Agenturberatung:

- **Halten Sie Ihre Firewall eingeschaltet**

  Eine Firewall schützt Ihren Computer vor Hackern, die versuchen könnten, ihn zum Absturz zu bringen, Informationen zu löschen oder sogar Passwörter oder andere vertrauliche Informationen zu stehlen. Software-Firewalls werden allgemein für Einzelcomputer empfohlen. Die Software ist auf einigen Betriebssystemen vorkonfektioniert oder kann für einzelne Computer erworben werden. Für mehrere vernetzte Computer bieten Hardware-Router in der Regel Firewall-Schutz.

- **Installieren oder aktualisieren Sie Ihre Antivirensoftware**

  Antivirensoftware wurde entwickelt, um zu verhindern, dass bösartige Softwareprogramme auf Ihrem Computer eingebettet werden. Wenn es bösartigen Code entdeckt, wie einen Virus oder einen Wurm, funktioniert es, um ihn zu entschärfen oder zu entfernen. Viren können Computer ohne Wissen der Benutzer infizieren. Die meisten Arten von Antivirensoftware können so eingerichtet werden, dass sie automatisch aktualisiert werden.

- **Installieren oder aktualisieren Sie Ihre Anti-Spyware-Technologie**

  Spyware ist genau das, wonach es sich anhört - Software, die heimlich auf Ihrem Computer installiert wird, damit andere in Ihre Aktivitäten auf dem Computer hineinschauen können. Einige Spyware sammelt ohne Ihre Zustimmung Informationen über Sie oder erzeugt unerwünschte Popup-Anzeigen in Ihrem Webbrowser. Einige Betriebssysteme bieten kostenlosen Spyware-Schutz, und kostengünstige Software steht zum Download im Internet oder in Ihrem lokalen Computergeschäft zur Verfügung. Seien Sie vorsichtig bei Anzeigen im Internet, die herunterladbare Antispyware anbieten - in einigen Fällen können diese Produkte gefälscht sein und tatsächlich Spyware oder anderen bösartigen Code enthalten. Es ist, als würde man in einem Lebensmittelgeschäft einkaufen, dem man vertraut.

- **Halten Sie Ihr Betriebssystem auf dem neuesten Stand**

  Computer-Betriebssysteme werden regelmäßig aktualisiert, um mit den technologischen Anforderungen Schritt zu halten und Sicherheitslücken zu schließen. Stellen Sie sicher, dass Sie die Updates installieren, um sicherzustellen, dass Ihr Computer über den neuesten Schutz verfügt.

- **Seien Sie vorsichtig, was Sie herunterladen**

  Das sorglose Herunterladen von E-Mail-Anhängen kann selbst die wachsamste Antivirensoftware umgehen. Öffnen Sie niemals einen E-Mail-Anhang von jemandem, den Sie nicht kennen, und hüten Sie sich vor weitergeleiteten Anhängen von Personen, die Sie kennen. Möglicherweise haben sie unwissentlich fortgeschrittenen bösartigen Code.

- **Schalten Sie Ihren Computer aus**

  Mit dem Wachstum von Hochgeschwindigkeits-Internetverbindungen entscheiden sich viele dafür, ihre Computer eingeschaltet und einsatzbereit zu lassen. Der Nachteil ist, dass "always on" Computer anfälliger macht. Über den Firewall-Schutz hinaus, der dazu dient, unerwünschte Angriffe abzuwehren, trennt das Ausschalten des Computers effektiv die Verbindung eines Angreifers - sei es Spyware oder ein Botnetz, das die Ressourcen Ihres Computers nutzt, um andere ahnungslose Benutzer zu erreichen.

- Zeugnis

Good

bitwarden

Federal Bureau of Investigation (FBI)

Gesamtbeurteilung Bitwarden: Gut

- Empfiehlt nicht die Verwendung eines Passwort-Managers
- Weist auf die Bedeutung von starken Passwörtern hin
- Nennt die Notwendigkeit von 2FA/MFA zur weiteren Unterstützung der Passwortsicherheit
- Die allgemeine Sicherheitsempfehlung ist nicht auf dem neuesten Stand und entspricht nicht den NIST-Richtlinien
- Legt Passwortsicherheitsempfehlungen nicht klar, verständlich und leicht zu finden dar

"Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions."

FBI

Federal Trade Commission (FTC)

So erstellst du sichere Passwörter und andere Möglichkeiten zum Schutz deiner Konten

Agenturberatung:

- Eine andere Möglichkeit besteht darin, einen Passwort-Manager eines Drittanbieters zu verwenden, um ein sicheres Passwort zu erstellen — und es sich zu merken. Um einen seriösen Passwort-Manager zu finden, lesen Sie die Expertenbewertungen. Stellen Sie sicher, dass das Passwort, das Sie mit dem Passwort-Manager verwenden, stark und sicher ist. Ein Webbrowser, ein mobiler Browser und ein Passwort-Manager können Ihre Passwörter für Sie speichern.
- Ein sicheres Passwort ist ein wichtiger erster Schritt, um dein Konto vor Hackern zu schützen. Aber auch starke Passwörter sind anfällig für Cyberangriffe. Die Verwendung der Multi-Faktor-Authentifizierung bedeutet, dass sich ein Hacker, der dein Passwort stiehlt, ohne einen weiteren Authentifizierungsfaktor nicht in dein Konto einloggen kann.
- Die häufigste Art der Multi-Faktor-Authentifizierung ist ein Verifizierungspasscode, den du per SMS oder E-Mail erhältst. Dieser einmalige Passcode ist in der Regel sechs Ziffern oder länger und läuft automatisch ab. Dies ist jedoch die am wenigsten sichere Art der Zwei-Faktor-Authentifizierung. Wählen Sie daher eine sicherere Methode wie eine Authentifizierungs-App oder einen Sicherheitsschlüssel für mehr Schutz, wenn Sie die Möglichkeit haben.
- Zeugnis

Passwort-Checkliste

Agenturberatung:

- **Achte darauf, dass dein Passwort lang und sicher ist.** Das bedeutet mindestens 12 Zeichen. Ein Passwort länger zu machen, ist im Allgemeinen der einfachste Weg, es stärker zu machen. Erwägen Sie, eine Passphrase aus zufälligen Wörtern zu verwenden, damit Ihr Passwort einprägsamer wird, aber vermeiden Sie es, gängige Wörter oder Sätze zu verwenden. Wenn der von Ihnen verwendete Dienst keine langen Passwörter zulässt, können Sie Ihr Passwort stärker machen, indem Sie Groß- und Kleinbuchstaben, Zahlen und Symbole mischen.

- **Verwende Passwörter, die du für andere Konten verwendet hast, nicht wieder.** Verwenden Sie unterschiedliche Passwörter für verschiedene Konten. Auf diese Weise kann ein Hacker, der dein Passwort für ein Konto erhält, es nicht verwenden, um in deine anderen Konten zu gelangen.

- **Verwenden Sie die Multi-Faktor-Authentifizierung, wenn es eine Option ist.** Einige Konten bieten zusätzliche Sicherheit, indem sie zusätzlich zu einem Passwort etwas verlangen, um sich bei deinem Konto anzumelden. Dies wird als Multi-Faktor-Authentifizierung bezeichnet. Das „Extra“, das Sie benötigen, um sich in Ihrem Konto anzumelden, fällt in zwei Kategorien:
  - Etwas, das Sie haben — wie einen Passcode, den Sie über eine Authentifizierungs-App oder einen Sicherheitsschlüssel erhalten.
  - Etwas, das du bist — wie ein Scan deines Fingerabdrucks, deiner Netzhaut oder deines Gesichts.

- **Betrachten Sie einen Passwort-Manager.** Die meisten Menschen haben Probleme, alle ihre Passwörter im Auge zu behalten. Je länger und komplizierter ein Passwort ist, desto stärker ist es, aber ein längeres Passwort kann auch schwieriger zu merken sein. Erwägen Sie, Ihre Passwörter und Sicherheitsfragen in einem seriösen Passwort-Manager zu speichern. Um einen seriösen Passwort-Manager zu finden, durchsuche unabhängige Bewertungsseiten und sprich mit Freunden und Familie nach denen, die sie verwenden. Stellen Sie sicher, dass Sie ein starkes Passwort verwenden, um die Informationen in Ihrem Passwort-Manager zu sichern.

- **Wählen Sie Sicherheitsfragen aus, auf die nur Sie die Antwort kennen.** Wenn Sie auf einer Website aufgefordert werden, Sicherheitsfragen zu beantworten, vermeiden Sie es, Antworten anzugeben, die in öffentlichen Aufzeichnungen verfügbar oder online leicht zu finden sind, z. B. Ihre Postleitzahl, Ihren Geburtsort oder den Mädchennamen Ihrer Mutter. Und verwenden Sie keine Fragen mit einer begrenzten Anzahl von Antworten, die Angreifer leicht erraten können — wie die Farbe Ihres ersten Autos. Sie können sogar unsinnige Antworten verwenden, um das Raten zu erschweren — aber wenn Sie dies tun, stellen Sie sicher, dass Sie sich daran erinnern können, was Sie verwenden.

- **Ändern Sie Passwörter schnell, wenn ein Verstoß vorliegt.** Wenn ein Unternehmen Ihnen mitteilt, dass es eine Datenschutzverletzung gab, bei der ein Hacker Ihr Passwort hätte erhalten können, ändern Sie sofort das Passwort, das Sie bei diesem Unternehmen verwenden, und auf jedem Konto, das ein ähnliches Passwort verwendet.

- Zeugnis

Excellent

bitwarden

Federal Trade Commission (FTC)

Gesamtbeurteilung Bitwarden: Ausgezeichnet

- Empfiehlt die Verwendung des Passwort-Managers
- Weist auf die Bedeutung von starken Passwörtern hin
- Zitate benötigen 2FA/MFA, um die Passwortsicherheit weiter zu unterstützen
- Die allgemeine Sicherheitsberatung ist auf dem neuesten Stand und entspricht den NIST-Richtlinien
- Legt Passwortsicherheitsempfehlungen klar, verständlich und leicht zu finden fest

"Use a password manager. A third-party password manager also can create a strong password. To find a reputable password manager, read expert reviews. Make sure the password for your password manager is strong. And protect it like you do your other passwords."

FTC

Handelsministerium

Nationaler Monat der Cybersicherheit: Schützen Sie sich online

Agenturberatung:

- Bisher war es üblich, Passwörter mit Sonderzeichen, Groß- und Kleinschreibung, Zahlen, Buchstaben und einer Vielzahl von willkürlichen Regeln zu erstellen, einschließlich der Verpflichtung, Ihr Passwort mehrmals pro Jahr zu ändern. Untersuchungen haben gezeigt, dass jeder von uns dasselbe bei reaktionswiederverwendeten Passwörtern getan hat oder Variationen desselben Passworts erstellt hat, weil wir aufgefordert wurden, uns Dutzende von eindeutigen Passwörtern für jede Website, jedes Login oder jede Anwendung zu merken.

- Unsere natürlichen Instinkte schufen eine Schwäche in unserer Online-Sicherheit und Cyberkriminelle nutzten sie aus. Untersuchungen zur Verwendung von Passwörtern haben die inhärente Schwäche gezeigt, von Benutzern zu erwarten, dass sie sich beliebig komplexe Passwörter merken, und die Bedeutung der Verwendung von Multi-Faktor-Authentifizierung (MFA) zum Schutz unserer privaten Informationen. Wichtig ist, dass sich unser Denken zu diesem Thema entwickelt hat, und wir haben die folgenden Praktiken identifiziert, um uns besser zu schützen:
  - Wenn Sie ein Passwort verwenden müssen, verwenden Sie ein längeres Passwort (15 oder mehr Zeichen) oder sogar Passphrasen, da diese einen größeren Schutz bieten als ein kürzeres, willkürlich komplexes Passwort. Passphrasen haben den zusätzlichen Vorteil, dass sie leicht zu merken sind.
  - Die Verwendung von MFA (z. B. ein einmaliger Code, der Ihnen per E-Mail gesendet wurde, oder eine Authentifizierungs-App auf Ihrem Telefon) fügt eine zweite, kritische Ebene hinzu, um sich vor einem kompromittierten Passwort zu schützen. MFA sollte jederzeit eingerichtet werden, wenn es verfügbar ist. Es dauert nur ein paar Augenblicke und gibt Ihnen Sicherheit.

- Passwort-Manager, die durch ein sehr starkes, langes Passwort mit aktivierter MFA geschützt sind, ermöglichen es uns, eindeutige Passwörter für jede Website zu erstellen, ohne sie sich alle merken zu müssen.

- Zeugnis

NIST fällt unter das Handelsministerium

Agenturberatung:

- Die Gewährleistung der Sicherheit unserer miteinander verbundenen globalen Netzwerke und der mit diesen Netzwerken verbundenen Geräte und Daten ist eine der entscheidenden Herausforderungen unserer Zeit.

- Das Handelsministerium hat die Aufgabe, das Bewusstsein und den Schutz der Cybersicherheit zu verbessern, die Privatsphäre zu schützen, die öffentliche Sicherheit aufrechtzuerhalten, die wirtschaftliche und nationale Sicherheit zu unterstützen und die Amerikaner in die Lage zu versetzen, ihre Sicherheit online besser zu verwalten.
  - NIST veröffentlicht Version 1.0 des Datenschutz-Frameworks
  - NIST bietet eine Schnellstartanleitung für seinen Katalog zu Sicherheits- und Datenschutzmaßnahmen
  - Cybersicherheitsecke für kleine Unternehmen

- Zeugnis

Very Good

bitwarden

Handelsministerium

Gesamtbeurteilung Bitwarden: Sehr gut

- Empfiehlt die Verwendung eines Passwort-Managers
- Weist auf die Bedeutung von starken Passwörtern hin
- Zitate benötigen 2FA/MFA, um die Passwortsicherheit weiter zu unterstützen
- Die allgemeine Sicherheitsberatung ist auf dem neuesten Stand und entspricht den NIST-Richtlinien
- Legt Passwortsicherheitsempfehlungen nicht klar, verständlich und leicht zu finden dar

Federal Communications Commission (FCC)

Cybersicherheitstipps für kleine Unternehmen

- Schulung der Mitarbeiter in Sicherheitsgrundsätzen. Festlegung grundlegender Sicherheitspraktiken und -richtlinien für Mitarbeiter, z. B. die Anforderung sicherer Passwörter und die Festlegung geeigneter Richtlinien für die Internetnutzung, in denen die Strafen für Verstöße gegen die Cybersicherheitsrichtlinien des Unternehmens aufgeführt sind. Legen Sie Verhaltensregeln fest, die beschreiben, wie Kundeninformationen und andere wichtige Daten zu behandeln und zu schützen sind.

- Fordern Sie die Mitarbeiter auf, alle drei Monate eindeutige Passwörter zu verwenden und die Passwörter zu ändern. Erwägen Sie die Implementierung einer Multi-Faktor-Authentifizierung, die zusätzliche Informationen über ein Passwort hinaus erfordert, um Zugang zu erhalten. Erkundigen Sie sich bei Ihren Anbietern, die mit sensiblen Daten umgehen, insbesondere bei Finanzinstituten, ob sie eine Multi-Faktor-Authentifizierung für Ihr Konto anbieten.

- Zeugnis

10. Passwords and authentication

Require employees to use unique passwords and change passwords every three months. Consider implementing multi-factor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multi-factor authentication for your account.

Fair

bitwarden

Federal Communications Commission (FCC)

Gesamtbeurteilung Bitwarden: Fair

- Empfiehlt nicht die Verwendung eines Passwort-Managers
- Weist auf die Bedeutung von starken Passwörtern hin
  - Links zu Inhalten, die sich auf die Passwortsicherheit konzentrieren
  - Der Inhalt ist jedoch eindeutig veraltet und könnte besser organisiert sein
- Zitiert nicht konsequent die Notwendigkeit von 2FA/MFA, um die Passwortsicherheit weiter zu unterstützen
- Die allgemeine Sicherheitsempfehlung ist nicht auf dem neuesten Stand und entspricht nicht den NIST-Richtlinien
  - Empfiehlt entgegen den NIST-Richtlinien, Passwörter alle drei Monate zu ändern
- Legt Passwortsicherheitsempfehlungen nicht klar, verständlich und leicht zu finden dar

Small Business Administration (SBA)

Best Practices zur Verhinderung von Cyberangriffen

Agenturberatung:

- Mitarbeiter und ihre arbeitsbezogene Kommunikation sind eine der Hauptursachen für Datenschutzverletzungen in kleinen Unternehmen, da sie direkte Wege in Ihre Systeme darstellen. Die Schulung von Mitarbeitern in Bezug auf grundlegende Best Practices für die Internetnutzung kann einen großen Beitrag zur Verhinderung von Cyberangriffen leisten.
  - Weitere Schulungsthemen sind:
    - Phishing-E-Mails erkennen
    - Verwendung guter Internet-Browsing-Praktiken
    - Vermeidung verdächtiger Downloads
    - Aktivieren von Authentifizierungstools (z. B. starke Passwörter, Multi-Faktor-Authentifizierung usw.)
    - Schutz sensibler Lieferanten- und Kundeninformationen

- Zeugnis

Enable Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a mechanism to verify an individual's identity by requiring them to provide more than just a typical username and password. MFA commonly requires users to provide two or more of the following: something the user knows (password, phrase, PIN), something the user has (physical token, phone), and/or something that physically represents the user (fingerprint, facial recognition). Check with your vendors to see if they offer MFA for your various types of accounts (e.g., financial, accounting, payroll).

Good

bitwarden

Small Business Administration (SBA)

Gesamtbeurteilung Bitwarden: Gut

- Empfiehlt nicht die Verwendung eines Passwort-Managers
- Weist auf die Bedeutung von starken Passwörtern hin
- Nennt die Notwendigkeit von 2FA/MFA zur weiteren Unterstützung der Passwortsicherheit
- Die allgemeine Sicherheitsempfehlung ist nicht auf dem neuesten Stand und entspricht nicht den NIST-Richtlinien
- Legt Passwortsicherheitsempfehlungen nicht klar, verständlich und leicht zu finden dar

Securities and Exchange Commission (SEC)

Im Juli 2023 verabschiedete die SEC „endgültige Regeln, nach denen börsennotierte Unternehmen sowohl wesentliche Cybersicherheitsvorfälle, die sie erleben, als auch jährlich wesentliche Informationen über ihr Cybersicherheitsrisikomanagement, ihre Strategie und ihre Governance offenlegen müssen“. Angesichts der Rolle der SEC bei der Durchsetzung der Cybersicherheits-Compliance scheint es ratsam, die eigenen Ratschläge der SEC zur Passwortsicherheit zu bewerten.

Eine Suche nach "Passwortsicherheit" auf der Website SEC.gov zeigt 12 Dokumente, die alle vor Jahren zu sein scheinen. Es gibt eine Seite zur Cybersicherheit, die jedoch ziemlich allgemeine Empfehlungen des CISA enthält. Eine Cybersicherheitsrisikowarnung aus dem Jahr 2020 mit dem Titel „Cybersecurity: Safeguarding Client Accounts against Credential Compromise“ führt zu einer PDF-Datei, in der das Ausfüllen von Anmeldeinformationen besprochen wird. Während das Wort „Passwort“ durchgängig verwendet wird, wird „Passwortsicherheit nicht explizit erwähnt. "Starke Passwörter" werden im folgenden Kontext referenziert:

Cybersicherheit: Schutz von Kundenkonten vor Kompromittierung der Anmeldeinformationen

Agenturberatung:

- Während sich die Unternehmen auf Credential Stuffing-Angriffe vorbereiten, ermutigen die OCIE-Mitarbeiter die Unternehmen, ihre aktuellen Praktiken (z. B. MFA und andere oben beschriebene Praktiken) und mögliche Einschränkungen dieser Praktiken zu berücksichtigen und zu prüfen, ob die Kunden und Mitarbeiter des Unternehmens ordnungsgemäß darüber informiert sind, wie sie ihre Konten besser sichern können. Informierte Kunden Die meisten Unternehmen verlangen von Kunden und Mitarbeitern, dass sie sichere Passwörter erstellen und verwenden. Die Verwendung von Passwörtern ist jedoch weniger effektiv, wenn Kunden und/oder Mitarbeiter Passwörter von anderen Websites wiederverwenden. Um effektiver zu sein, haben einige Firmen Kunden und Mitarbeiter informiert und ermutigt, sichere, eindeutige Passwörter zu erstellen und Passwörter zu ändern, wenn es Hinweise darauf gibt, dass ihr Passwort kompromittiert wurde.

The Commission has noted that cybersecurity risks have increased alongside the ever-increasing share of economic activity that depends on electronic systems, the growth of remote work, the ability of criminals to monetize cybersecurity incidents, the use of digital payments, and the increasing reliance on third party service providers for information technology services, including cloud computing technology. In my view, artificial intelligence and other technologies may enhance both the ability of public companies to defend against cybersecurity threats but also the capacity of threat actors to launch sophisticated attacks. The Commission also observed that the cost to companies and their investors of cybersecurity incidents is rising at an increasing rate. All of these trends highlight investors' need for improved disclosure.

Fair

bitwarden

Securities and Exchange Commission (SEC)

Gesamtbeurteilung Bitwarden: Fair

- Empfiehlt nicht die Verwendung eines Passwort-Managers
- Weist auf die Bedeutung von starken Passwörtern hin
  - Links zu veralteten Inhalten, die starke Passwörter anerkennen, aber viel expliziter sein könnten
- Zitiert nicht konsequent die Notwendigkeit von 2FA/MFA, um die Passwortsicherheit weiter zu unterstützen
  - Obwohl in der oben verlinkten PDF-Datei auf 2FA/MFA verwiesen wird, handelt es sich nicht um eine produktive Beratung und es ist eine Suche erforderlich, um
- Die allgemeine Sicherheitsempfehlung ist nicht auf dem neuesten Stand und entspricht nicht den NIST-Richtlinien
- Legt Passwortsicherheitsempfehlungen nicht klar, verständlich und leicht zu finden dar

Das Weiße Haus

Eine Proklamation zum Monat des Bewusstseins für Cybersicherheit, 2023

Agenturberatung:

- "Ich rufe die Menschen, Unternehmen und Institutionen der Vereinigten Staaten auf, die Bedeutung der Cybersicherheit zu erkennen und zu handeln und den Monat des Cybersicherheitsbewusstseins zur Unterstützung unserer nationalen Sicherheit und Widerstandsfähigkeit zu beobachten. Ich fordere auch Unternehmen und Institutionen auf, Maßnahmen zu ergreifen, um das amerikanische Volk besser vor Cyber-Bedrohungen zu schützen und neue Möglichkeiten für amerikanische Arbeitnehmer zu schaffen, gut bezahlte Cyber-Jobs zu verfolgen. Amerikaner können auch sofortige Maßnahmen ergreifen, um sich besser zu schützen, z. B. die Multifaktor-Authentifizierung aktivieren, Software auf Computern und Geräten aktualisieren, sichere Passwörter verwenden und vorsichtig bleiben, wenn sie auf Links klicken, die verdächtig aussehen."

- Zeugnis

Bereitstellung einer Digital-First-Öffentlichkeitserfahrung

Agenturberatung:

- Die Agenturen stellen sicher, dass Websites, die von der Öffentlichkeit eine Authentifizierung verlangen, mit gängigen Passwort-Managern kompatibel sind und das "Einfügen" von Passwörtern oder anderen automatisierten, clientseitigen Hilfsmechanismen nicht verhindern.

- Zeugnis

Lesen Sie das White House Multifactor Authentication Modernization Symposium vor

Agenturberatung:

- "Sie brauchen mehr als ein Passwort, um online sicher zu bleiben - und hier setzt die Multi-Faktor-Authentifizierung an, um sicherzustellen, dass Ihre Daten besser vor böswilligen Cyber-Akteuren geschützt sind", sagte Brandon Wales, Executive Director des CISA. „CISA hat Unternehmen konsequent aufgefordert, MFA für alle Benutzer zu implementieren, um sicherzustellen, dass kritische Daten schwerer zugänglich sind. Beim heutigen Symposium geht es darum, zusammenzukommen, um die Vision zu entwerfen, die wir alle anstreben, um sie Wirklichkeit werden zu lassen."

- Zeugnis

Biden-Harris Administration kündigt Cybersicherheitskennzeichnungsprogramm für intelligente Geräte an, um amerikanische Verbraucher zu schützen

Agenturberatung

- Im Rahmen ihrer Befugnis, drahtlose Kommunikationsgeräte zu regulieren, wird die FCC voraussichtlich öffentliche Kommentare zur Einführung des vorgeschlagenen freiwilligen Kennzeichnungsprogramms für Cybersicherheit einholen, das voraussichtlich 2024 in Betrieb gehen wird. Wie vorgeschlagen, würde das Programm von Stakeholdern geleitete Bemühungen zur Zertifizierung und Kennzeichnung von Produkten nutzen, die auf spezifischen Cybersicherheitskriterien basieren, die vom National Institute of Standards and Technology (NIST) veröffentlicht wurden und beispielsweise eindeutige und starke Standardpasswörter, Datenschutz, Software-Updates und Funktionen zur Erkennung von Vorfällen erfordern.

- Zeugnis

Good

Updated January 2025

bitwarden

Das Weiße Haus

Gesamtbeurteilung Bitwarden: Gut

- Empfiehlt nicht die Verwendung eines Passwort-Managers
  - In einer Mitteilung zum Cybersecurity Awareness Month 2022 empfahl das Weiße Haus die Verwendung eines Passwort-Managers. Das Weiße Haus hatte die Gelegenheit, dasselbe im 2023 Cybersecurity Awareness Blog zu tun. Das taten sie nicht. Während der Blog empfiehlt, "starke Passwörter zu verwenden", werden Passwort-Manager nicht erwähnt.
- Weist auf die Bedeutung von starken Passwörtern hin
- Zitate benötigen 2FA/MFA, um die Passwortsicherheit weiter zu unterstützen
- Die allgemeine Sicherheitsempfehlung ist nicht auf dem neuesten Stand und entspricht nicht den NIST-Richtlinien
  - In früheren Mitteilungen hat das Weiße Haus im Widerspruch zu den Empfehlungen von NIST empfohlen, Passwörter zu ändern. Passwörter sollten nur geändert werden, wenn sie schwach sind, wiederverwendet werden oder kompromittiert wurden. Ein starkes und eindeutiges Passwort muss möglicherweise nie geändert werden, es sei denn, Sie vermuten, dass es kompromittiert wurde.
- Legt Passwortsicherheitsempfehlungen nicht klar, verständlich und leicht zu finden dar
  - Keine dedizierte Cybersicherheitsseite

Zusammenfassung

Es gibt viele Schritte, die Sie unternehmen können, um online sicher zu bleiben, aber die einfachste Maßnahme mit den wichtigsten und unmittelbarsten Auswirkungen auf Ihre Sicherheit ist die Verwendung eines Passwort-Managers. Wählen Sie einen plattformübergreifenden Passwort-Manager mit End-to-End-Verschlüsselung ohne Wissen, der unbegrenzt eindeutige und starke Passwörter generieren und speichern kann. Sie können mit Bitwarden mit einem kostenlosen Konto beginnen oder sich für Premium für weniger als 10 $/Jahr entscheiden, um erweiterte Funktionen zu erhalten.

Zusätzliche Ressourcen

- Zeigen Sie den Status der Passwortsicherheitspräsentation an