RESOURCE CENTER

Rapport over wachtwoordbeveiliging 2024

Hoe federale instanties wachtwoordbeveiliging aanpakken

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

bitwarden

De status van wachtwoordbeveiliging binnen Amerikaanse federale agentschappen beoordelen

De afgelopen jaren heeft de federale overheid van de Verenigde Staten veel aandacht besteed aan cyberbeveiliging, waarbij veel instanties het voortouw hebben genomen in het opleiden van overheidsorganisaties en grote en kleine bedrijven, evenals consumenten.

Maar als het op wachtwoordbeveiliging aankomt, zingt niet elk bureau hetzelfde liedje. Een van de belangrijkste groepen, het National Institute of Standards and Technology (NIST), "ontwikkelt cyberbeveiligingsnormen, richtlijnen, best practices en andere middelen om te voldoen aan de behoeften van de Amerikaanse industrie, federale instanties en het bredere publiek."

De NIST-pagina over cyberbeveiliging zegt verder dat "sommige NIST-opdrachten op het gebied van cyberbeveiliging worden gedefinieerd door federale wetten, uitvoerende orders en beleid. Het Office of Management and Budget (OMB) schrijft bijvoorbeeld voor dat alle federale agentschappen de cyberbeveiligingsnormen en -richtlijnen van NIST voor niet-nationale beveiligingssystemen moeten implementeren."

Helaas zijn de aanbevelingen van NIST nog niet door alle federale agentschappen geaccepteerd en geïmplementeerd. En hoewel NIST de standaarden opstelt die instanties beweren te volgen, heeft zelfs NIST zijn eigen zwakke punt in de vorm van een ongeorganiseerde website.

2024 is het derde jaar dat Bitwarden deze analyse uitvoert. In de loop van drie jaar is de NIST-website ongeorganiseerd gebleven, hoewel de inhoud zeer degelijk is. Er zijn ook een paar positieve ontwikkelingen geweest. Het Witte Huis heeft de verspreiding van beveiligingsadviezen voor wachtwoorden verbeterd en is van 'Ruimte voor verbetering' naar 'Goed' gegaan. Andere instanties die zich in een betere richting hebben ontwikkeld wat betreft hun aanbevelingen voor wachtwoordbeveiliging en algemene cyberbeveiligingshouding zijn de Cybersecurity and Infrastructure Security Association (CISA), het Federal Bureau of Investigation (FBI), de Federal Trade Commission (FTC) en de Small Business Administration (SBA).

Dit jaar heeft Bitwarden ook de Securities and Exchange Commission (SEC) aan dit rapport toegevoegd. Vorig jaar heeft de SEC regels aangenomen die bedrijven verplichten om materiële cyberbeveiligingsincidenten openbaar te maken. Gezien de rol van de SEC bij het afdwingen van de naleving van cyberbeveiligingsregels, zal dit rapport het eigen wachtwoordbeveiligingsadvies van de SEC beoordelen.

Technologie gaat snel. Voor bedrijven en particulieren is een groot deel van ons leven nu online in een groot aantal accounts die variëren van leuke entertainmentsites tot serieuze financiële zaken zoals onze bankrekeningen.

Het doel van deze beoordeling is om iedereen die wachtwoorden gebruikt te betrekken en voor te lichten over de best practices van de federale overheid en waar ruimte is voor verbetering. Er zijn velen binnen de federale overheid die een solide educatieve aanpak hebben voor wachtwoordbeveiliging, en er zijn anderen die misschien een beetje hulp nodig hebben om te moderniseren.

Gelukkig groeit er consensus over best practices voor wachtwoordbeveiliging. Dit rapport consolideert en beoordeelt de details.

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

Download

Bekijk de Presentatie over wachtwoordbeveiliging

Inhoudsopgave

Richtlijn voor wachtwoordbeveiligingsclassificatiesysteem

Het beoordelingssysteem rangschikt bureaus op basis van de volgende criteria:

- Raadt het gebruik van een wachtwoordmanager aan
- Wijst op het belang van sterke wachtwoorden

- Noemt behoefte aan 2FA/MFA om wachtwoordbeveiliging verder te ondersteunen
- Het algemene beveiligingsadvies is up-to-date en voldoet aan de NIST-richtlijnen
- Geeft aanbevelingen voor wachtwoordbeveiliging op een duidelijke, begrijpelijke en gemakkelijk te vinden manier

Very Good

- Raadt het gebruik van een wachtwoordmanager aan
- Wijst op het belang van sterke wachtwoorden
- Noemt behoefte aan 2FA/MFA om wachtwoordbeveiliging verder te ondersteunen
- Het algemene beveiligingsadvies is up-to-date en voldoet aan de NIST-richtlijnen
- Geeft geen duidelijke, begrijpelijke en gemakkelijk te vinden aanbevelingen voor wachtwoordbeveiliging

Good

- Raadt het gebruik van een wachtwoordmanager niet aan
- Wijst op het belang van sterke wachtwoorden
- Noemt behoefte aan 2FA/MFA om wachtwoordbeveiliging verder te ondersteunen
- Het algemene beveiligingsadvies is niet up-to-date en voldoet niet aan de NIST-richtlijnen
- Geeft geen duidelijke, begrijpelijke en gemakkelijk te vinden aanbevelingen voor wachtwoordbeveiliging

Fair

- Raadt het gebruik van een wachtwoordmanager niet aan
- Wijst op het belang van sterke wachtwoorden
- Noemt niet consequent de behoefte aan 2FA/MFA om wachtwoordbeveiliging verder te ondersteunen

- Het algemene beveiligingsadvies is niet up-to-date en voldoet niet aan de NIST-richtlijnen
- Geeft geen duidelijke, begrijpelijke en gemakkelijk te vinden aanbevelingen voor wachtwoordbeveiliging

- Raadt het gebruik van een wachtwoordmanager niet aan
- Het belang van sterke wachtwoorden wordt niet genoemd
- Noemt niet de noodzaak van 2FA/MFA om wachtwoordbeveiliging verder te ondersteunen
- Het algemene beveiligingsadvies is niet up-to-date en voldoet niet aan de NIST-richtlijnen
- Geeft geen duidelijke, begrijpelijke en gemakkelijk te vinden aanbevelingen voor wachtwoordbeveiliging

Nationaal instituut voor standaarden en technologie (NIST)

NIST-raamwerk voor risicobeheer | IA-5(18)

Advies van het agentschap:

- Authenticatiebeheer | Wachtwoordbeheerders
  - Gebruik maken van [Opdracht: door organisatie gedefinieerde wachtwoordbeheerders] om wachtwoorden te genereren en te beheren; en
    - Bescherm de wachtwoorden met [opdracht: organisatiegedefinieerde controles].
    - Voor systemen waar statische wachtwoorden worden gebruikt, is het vaak een uitdaging om ervoor te zorgen dat de wachtwoorden voldoende complex zijn en dat dezelfde wachtwoorden niet op meerdere systemen worden gebruikt. Een wachtwoordmanager is een oplossing voor dit probleem omdat het automatisch sterke en verschillende wachtwoorden genereert en opslaat voor verschillende accounts. Een potentieel risico van het gebruik van wachtwoordbeheerders is dat aanvallers zich kunnen richten op de verzameling wachtwoorden die door de wachtwoordbeheerder zijn gegenereerd. Daarom moet het verzamelen van wachtwoorden worden beschermd, inclusief het versleutelen van de wachtwoorden en het offline opslaan van de verzameling in een token.

- Referentie

Richtlijnen digitale identiteit

Advies van het agentschap:

- Opgeslagen geheimen DIENEN minstens 8 tekens lang te zijn indien gekozen door de abonnee. Opgeslagen geheimen die willekeurig door de CDV of verificateur worden gekozen DIENEN minstens 6 tekens lang te zijn en mogen volledig numeriek zijn. Indien het CDV of de verificateur een gekozen geheime code weigert op basis van de zwarte lijst van gecompromitteerde waarden, DIENT de abonnee een andere geheime code te kiezen. Er ZOU geen andere complexiteitsvereisten voor gememoriseerde geheimen opgelegd moeten worden. Een reden hiervoor wordt gegeven in Bijlage A Sterkte van gememoriseerde geheimen.

- Verificateurs DIENEN te eisen dat de door de abonnee gekozen gememoriseerde geheimen ten minste 8 tekens lang zijn. Verificateurs ZOUEN door de abonnee gekozen gememoriseerde geheimen met een lengte van ten minste 64 tekens moeten toestaan. Alle ASCII [RFC 20] afdruktekens en het spatieteken ZOU acceptabel moeten zijn in opgeslagen geheimen. Unicode [ISO/ISC 10646] tekens ZOUDEN ook geaccepteerd moeten worden. Om rekening te houden met mogelijke typefouten, mogen verificateurs meerdere opeenvolgende spaties vóór de verificatie vervangen door een enkele spatie, op voorwaarde dat het resultaat ten minste 8 tekens lang is. Het geheim DIENT NIET te worden ingekort. Voor de bovenstaande lengtevereisten DIENT elk Unicode-codepunt als een enkel teken te worden geteld.

- Opgeslagen geheimen die willekeurig gekozen worden door de CDV (bv. bij de inschrijving) of door de verificateur (bv. wanneer een gebruiker een nieuwe PIN-code aanvraagt) DIENEN minstens 6 tekens lang te zijn en DIENEN gegenereerd te worden met een goedgekeurde willekeurige bitgenerator [SP 800-90Ar1].

- Geheime verificateurs DIENEN NIET toe te staan dat de abonnee een "hint" opslaat die toegankelijk is voor een niet-geauthenticeerde eiser. Verificateurs DIENEN abonnees NIET te vragen om specifieke soorten informatie te gebruiken (bijv. "Wat was de naam van uw eerste huisdier?") bij het kiezen van gememoriseerde geheimen.

- Bij het verwerken van verzoeken om opgeslagen geheimen vast te leggen en te wijzigen, DIENEN verificateurs de toekomstige geheimen te vergelijken met een lijst die waarden bevat waarvan bekend is dat ze vaak gebruikt, verwacht of gecompromitteerd zijn. De lijst KAN bijvoorbeeld bestaan uit, maar is niet beperkt tot:
  - Wachtwoorden verkregen uit eerdere inbreuken.
  - Woordenboekwoorden.
  - Herhalende of opeenvolgende tekens (bijv. 'aaaaaa', '1234abcd').
  - Contextspecifieke woorden, zoals de naam van de service, de gebruikersnaam en afgeleiden daarvan.

- Indien het gekozen geheim op de lijst staat, DIENT het CDV of de verificateur de abonnee te informeren dat hij een ander geheim moet kiezen, DIENT de reden voor de weigering te geven en DIENT van de abonnee te eisen dat hij een andere waarde kiest.

- Verificateurs ZOU de abonnee begeleiding moeten bieden, zoals een wachtwoordsterktemeter [Meters], om de gebruiker te helpen bij het kiezen van een sterk in het geheugen opgeslagen geheim. Dit is vooral belangrijk na de afwijzing van een gememoriseerd geheim op de bovenstaande lijst, omdat het triviale wijzigingen van op de lijst voorkomende (en waarschijnlijk zeer zwakke) gememoriseerde geheimen ontmoedigt [Zwarte lijsten].

- Verificateurs DIENEN een snelheidsbeperkend mechanisme te implementeren dat effectief het aantal mislukte authenticatiepogingen beperkt die kunnen worden gedaan op de rekening van de abonnee, zoals beschreven in paragraaf 5.2.2.

- Verificateurs ZOUDEN GEEN andere samenstellingsregels mogen opleggen (bijv. het vereisen van mengsels van verschillende soorten tekens of het verbieden van opeenvolgend herhaalde tekens) voor gememoriseerde geheimen. Verificateurs ZOU NIET mogen eisen dat opgeslagen geheimen willekeurig worden gewijzigd (bijv. periodiek). Verificateurs DIENEN echter een wijziging af te dwingen als er bewijs is van compromittering van de authenticator.

- Verificateurs ZOU moeten toestaan dat eisers de functionaliteit "plakken" gebruiken bij het invoeren van een gememoriseerd geheim. Dit vergemakkelijkt het gebruik van wachtwoordmanagers, die veel gebruikt worden en in veel gevallen de kans vergroten dat gebruikers kiezen voor sterkere onthouden geheimen.

- Om de eiser te helpen bij het succesvol invoeren van een gememoriseerde code, ZOU de verificateur een optie moeten bieden om de code weer te geven - in plaats van een reeks punten of sterretjes - totdat deze is ingevoerd. Hierdoor kan de aanvrager zijn invoer verifiëren als hij zich op een locatie bevindt waar zijn scherm waarschijnlijk niet wordt waargenomen. De verificateur KAN ook toestaan dat het apparaat van de gebruiker individuele ingevoerde tekens korte tijd weergeeft nadat elk teken is ingetikt om de juiste invoer te verifiëren. Dit is vooral van toepassing op mobiele apparaten.

- De verificateur DIENT goedgekeurde encryptie en een geauthenticeerd beveiligd kanaal te gebruiken bij het opvragen van gememoriseerde geheimen om weerstand te bieden tegen afluisteren en MitM-aanvallen.

- Verificateurs DIENEN opgeslagen geheimen op te slaan in een vorm die bestand is tegen offline aanvallen. Gememoriseerde geheimen DIENEN gezouten en gehasht te worden met een geschikte eenrichtingssleutelafleidingsfunctie. Functies voor het afleiden van sleutels nemen een wachtwoord, een salt en een kostenfactor als invoer en genereren vervolgens een hash van een wachtwoord. Hun doel is om elke poging om een wachtwoord te raden door een aanvaller die een hashbestand met wachtwoorden heeft verkregen, duur te maken en daardoor de kosten van een aanval om het wachtwoord te raden hoog of onbetaalbaar te maken. Voorbeelden van geschikte sleutelafleidingsfuncties zijn wachtwoordgebaseerde sleutelafleidingsfunctie 2 (PBKDF2) [SP 800-132] en Balloon [BALLOON]. Een geheugenharde functie ZOU gebruikt moeten worden omdat het de kosten van een aanval verhoogt. De sleutelafleidingsfunctie DIENT een goedgekeurde eenrichtingsfunctie te gebruiken zoals Keyed Hash Message Authentication Code (HMAC) [FIPS 198-1], elke goedgekeurde hashfunctie in SP 800-107, Secure Hash Algorithm 3 (SHA-3) [FIPS 202], CMAC [SP 800-38B] of Keccak Message Authentication Code (KMAC), Customizable SHAKE (cSHAKE), of ParallelHash [SP 800-185]. De gekozen uitgangslengte van de sleutelafleidingsfunctie ZOU dezelfde MOETEN zijn als de lengte van de uitgang van de onderliggende eenrichtingsfunctie.

- De salt DIENT minstens 32 bits lang te zijn en wordt willekeurig gekozen om zoutwaardebotsingen tussen opgeslagen hashes te minimaliseren. Zowel de zoutwaarde als de resulterende hash DIENT voor elke abonnee te worden opgeslagen met behulp van een geheime authenticator.

- Voor PBKDF2 is de kostenfactor een iteratieteller: hoe vaker de PBKDF2-functie iteratief is, hoe langer het duurt om de hash van het wachtwoord te berekenen. Daarom ZOU het aantal iteraties zo groot moeten zijn als de prestaties van de verificatieserver toelaten, meestal minstens 10.000 iteraties.

- Daarnaast ZOU een verificateur een extra iteratie van een sleutelafleidingsfunctie moeten uitvoeren met een zoutwaarde die geheim is en alleen bekend is bij de verificateur. Indien een salt-waarde wordt gebruikt, DIENT deze te worden gegenereerd door een goedgekeurde willekeurige bitgenerator [SP 800-90Ar1] en ten minste de minimale beveiligingssterkte te bieden die is opgegeven in de laatste herziening van SP 800-131A (112 bits op de datum van deze publicatie). De geheime zoutwaarde DIENT afzonderlijk van de gehashte opgeslagen geheimen te worden opgeslagen (bv. in een gespecialiseerd apparaat zoals een hardware beveiligingsmodule). Met deze extra iteratie zijn brute-force aanvallen op de gehashte gememoriseerde geheimen onpraktisch zolang de geheime zoutwaarde geheim blijft.

- Cybersecurity Maand 2023 Blogreeks
  - Advies agentschap
    - Wachtwoorden zijn nog steeds het meest gebruikte authenticatiemechanisme om toegang te krijgen tot interessante bronnen. Wachtwoorden zijn de belangrijkste verdediging om de vertrouwelijkheid en integriteit van gegevens te beschermen tegen cybercriminelen en datalekken. Goede, sterke wachtwoorden helpen mensen om online veilig en privé te blijven.

- Referentie

bitwarden

Nationaal instituut voor standaarden en technologie (NIST)

Algehele Bitwarden beoordeling: Zeer goed

- Raadt het gebruik van een wachtwoordmanager aan
- Wijst op het belang van sterke wachtwoorden
- Noemt behoefte aan 2FA/MFA om wachtwoordbeveiliging verder te ondersteunen
- Het algemene beveiligingsadvies is up-to-date en voldoet aan de NIST-richtlijnen (NIST stelt de norm voor beveiligingsadvies van de federale overheid)
- Geeft geen duidelijke, begrijpelijke en gemakkelijk te vinden aanbevelingen voor wachtwoordbeveiliging

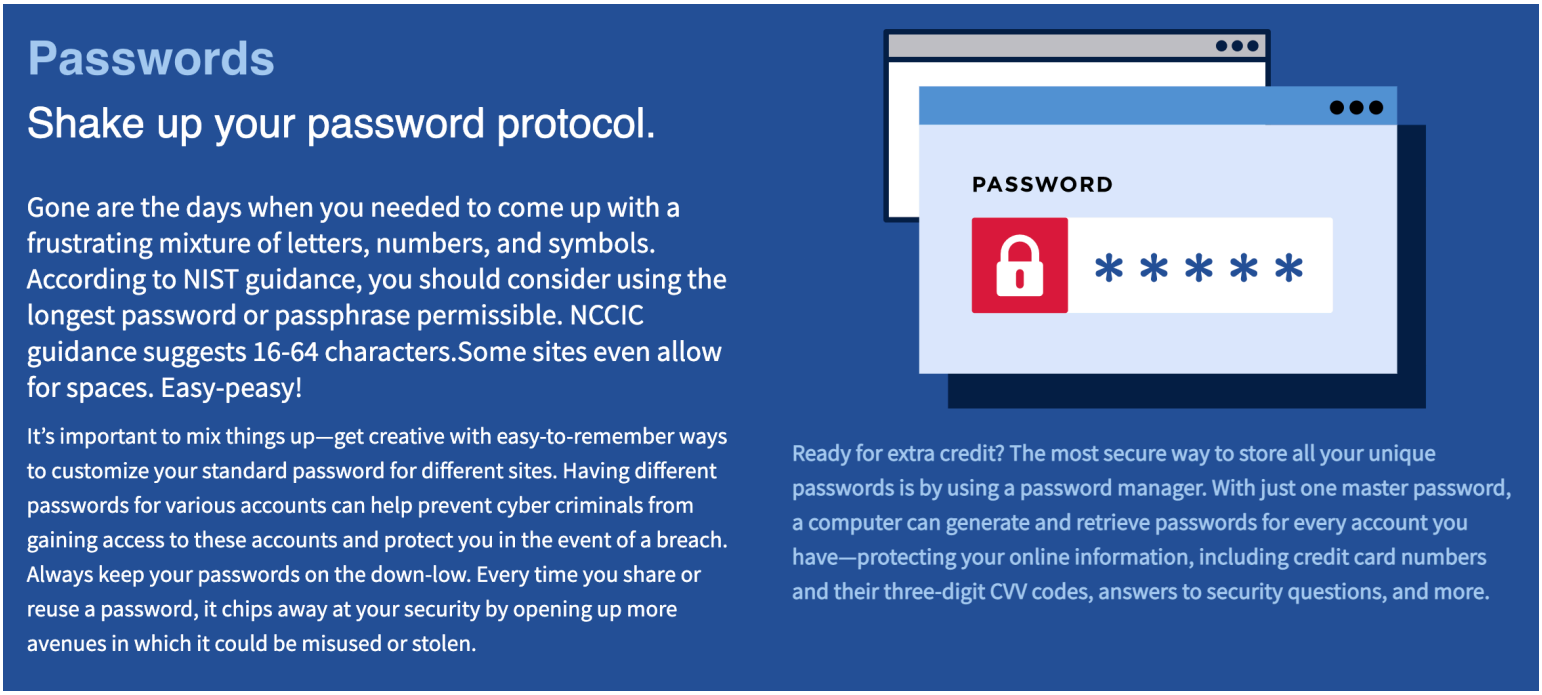
Hoewel het advies grondig is en de normen vaststelt voor instanties, is de toegang tot wachtwoordrichtlijnen via de website niet intuïtief. Het advies is verstopt in erg lange PDF's en geschreven op een manier die niet gebruiksvriendelijk is.

"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

Agentschap voor de beveiliging van cybersecurity en infrastructuur (CISA)

Cyberlessen



Cyberlessen over wachtwoorden, CISA

- Referentie

Ransomware stoppen

Advies van het agentschap:

- Een wachtwoordbeleid implementeren dat unieke wachtwoorden van minstens 15 tekens vereist
  - Wachtwoordbeheerders kunnen je helpen bij het ontwikkelen en beheren van veilige wachtwoorden. Beveilig en beperk de toegang tot wachtwoordmanagers die in gebruik zijn en schakel alle beveiligingsfuncties in die beschikbaar zijn op het product dat in gebruik is, zoals MFA.

- Referentie

Beveilig onze wereld: Sterke wachtwoorden vereisen

Advies van het agentschap:

- Kleine tot middelgrote bedrijven zijn regelmatig het doelwit van kwaadwillende hackers en een veelvoorkomend toegangspunt voor digitale dieven zijn gestolen of zwakke wachtwoorden.

- Maar het goede nieuws is dat u uw bedrijf veilig kunt houden door werknemers te verplichten sterke wachtwoorden en wachtwoordmanagers te gebruiken.

- Geef het goede voorbeeld door lange, willekeurige, unieke wachtwoorden te gebruiken voor al je persoonlijke en zakelijke accounts - en gebruik een wachtwoordmanager om ze te onthouden! Werk dan samen met je IT-medewerkers of -provider om werknemers te verplichten sterke wachtwoorden te gebruiken om toegang te krijgen tot je systemen. Zo blijven je gegevens veilig en beschermd.

- Referentie

Beveilig onze wereld: Zwakke wachtwoorden

Advies van het agentschap:

- Laat een wachtwoordmanager het werk doen! Een wachtwoordmanager maakt wachtwoorden voor ons aan, slaat ze op en vult ze automatisch aan. Dan hoeven we maar één sterk wachtwoord te onthouden - voor de wachtwoordmanager zelf. Zoek in betrouwbare bronnen voor "wachtwoordmanagers" zoals Consumer Reports, dat een selectie van goed beoordeelde wachtwoordmanagers biedt. Lees recensies om opties te vergelijken en een gerenommeerd programma voor jou te vinden.

- Referentie

Excellent

bitwarden

Agentschap voor de beveiliging van cybersecurity en infrastructuur (CISA)

Algehele Bitwarden beoordeling: Zeer goed

- Raadt het gebruik van een wachtwoordmanager aan
- Wijst op het belang van sterke wachtwoorden
- Noemt behoefte aan 2FA/MFA om wachtwoordbeveiliging verder te ondersteunen
- Het algemene beveiligingsadvies is up-to-date en voldoet aan de NIST-richtlijnen
- Geeft geen duidelijke, begrijpelijke en gemakkelijk te vinden aanbevelingen voor wachtwoordbeveiliging

De nationale veiligheidsdienst (NSA)

Ransomware stoppen

Advies van het agentschap:

- Een wachtwoordbeleid implementeren dat unieke wachtwoorden van minstens 15 tekens vereist
  - Wachtwoordbeheerders kunnen je helpen bij het ontwikkelen en beheren van veilige wachtwoorden. Beveilig en beperk de toegang tot wachtwoordmanagers die in gebruik zijn en schakel alle beveiligingsfuncties in die beschikbaar zijn op het product dat in gebruik is, zoals MFA.

- Referentie

Cisco-wachtwoordtypen: Best Practices

Advies van het agentschap:

- De toename van het aantal compromitteringen van netwerkinfrastructuren in de afgelopen jaren herinnert ons eraan dat authenticatie van netwerkapparaten een belangrijke overweging is. Netwerkapparaten kunnen in gevaar komen door:
  - Slechte wachtwoordkeuze (kwetsbaar voor brute force password spraying)
  - Routerconfiguratiebestanden (die gehashte wachtwoorden bevatten) die via niet-versleutelde e-mail worden verzonden, of
  - Hergebruikte wachtwoorden (waarbij wachtwoorden van een gecompromitteerd apparaat kunnen worden gebruikt om andere apparaten te compromitteren).

- Het gebruik van wachtwoorden op zichzelf verhoogt het risico op uitbuiting van apparaten. Hoewel NSA multi-factor authenticatie sterk aanbeveelt voor beheerders die kritieke apparaten beheren, moeten soms alleen wachtwoorden worden gebruikt. Het kiezen van goede algoritmen voor het opslaan van wachtwoorden kan uitbuiting veel moeilijker maken.

- Om zoveel mogelijk bescherming te bieden, gebruik je sterke wachtwoorden om te voorkomen dat ze worden gekraakt en omgezet in platte tekst. Voldoe aan een wachtwoordbeleid dat:
  - Bestaat uit een combinatie van kleine letters en hoofdletters, symbolen en cijfers;

- Minimaal 15 alfanumerieke tekens bevat; en
- Patronen die dat niet zijn:
  - Een toetsenbordwandeling
  - Hetzelfde als een gebruikersnaam
  - Het standaard wachtwoord
  - Hetzelfde als een wachtwoord dat ergens anders wordt gebruikt
  - Met betrekking tot het netwerk, de organisatie, de locatie of andere functie-identificatoren
  - Rechtstreeks uit een woordenboek, veelgebruikte acroniemen of gemakkelijk te raden
- Referentie

Veilig blijven op sociale media

Advies van het agentschap:

- Beveilig en versterk je wachtwoorden
  - Gebruik unieke en sterke wachtwoorden voor elke online account. Het hergebruiken van wachtwoorden voor meerdere accounts kan gegevens van alle accounts blootleggen als het wachtwoord wordt ontdekt. Zorg ervoor dat je wachtwoord lang en complex genoeg is en een combinatie van letters, cijfers en speciale tekens bevat. Implementeer waar mogelijk multi-factor authenticatie met behulp van een authenticatietoken of -app, zodat iemand geen toegang kan krijgen tot je account, zelfs niet als je wachtwoord gecompromitteerd is. Deel nooit wachtwoorden en vermijd het gebruik van informatie die geraden kan worden op basis van je social media-profielen of openbare informatie.
- Referentie

Veilige oplossingen voor multifactor-authenticatie selecteren

Advies van het agentschap:

- Eén antwoord, multi-factor authenticatiemechanismen vereisen activering van het apparaat, ofwel met een PIN/wachtwoord of biometrisch. Het apparaat biedt 'wat je hebt' en activering van het apparaat impliceert dat 'wat-je-weet' of 'wat-je-zijn' is geverifieerd.
- Aan de andere kant bevatten authenticators in meerdere stappen vaak een wachtwoord om te voorzien in 'wat-je-weet' en een andere authenticator die voorziet in 'wat-je-hebt'. Amerikaanse overheidsinstellingen moeten eisen overwegen voor PIN/wachtwoord activering en voor de wachtwoorden die direct worden gebruikt om 'wat-je-weet' te verstrekken. De richtlijnen in SP 800-63-3 Deel B geven aan dat in het geheugen opgeslagen geheimen (zowel voor activering als voor authenticatie met één factor) ten minste 6 tot 8 tekens moeten bevatten, en bevelen een hogere wachtwoordsterkte aan voor door de gebruiker geselecteerde wachtwoorden. Houd er bij het bepalen van wachtwoordvereisten rekening mee dat apparaten met meerdere factoren strenge drempelwaarden moeten integreren om aanvallen waarbij wachtwoorden worden geraden aan te pakken, terwijl verificateurs minder strenge drempelmechanismen kunnen gebruiken die garanderen dat wachtwoorden die direct worden gebruikt een hogere sterkte hebben.
- Referentie

Very Good

bitwarden

De nationale veiligheidsdienst (NSA)

Algehele Bitwarden-beoordeling: Goed

- Raadt het gebruik van een wachtwoordmanager niet aan
- Wijst op het belang van sterke wachtwoorden
- Noemt behoefte aan 2FA/MFA om wachtwoordbeveiliging verder te ondersteunen
- Het algemene beveiligingsadvies is niet up-to-date en voldoet niet aan de NIST-richtlijnen
- Geeft geen duidelijke, begrijpelijke en gemakkelijk te vinden aanbevelingen voor wachtwoordbeveiliging

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

Ministerie van Binnenlandse Veiligheid

CISA valt onder het DHS

Cyberbeveiligingspagina

Advies van het agentschap:

- President Biden heeft van cyberbeveiliging, een cruciaal onderdeel van de missie van het Department of Homeland Security (DHS), een topprioriteit gemaakt voor de regering Biden-Harris op alle overheidsniveaus.
- Om de inzet van de president kracht bij te zetten en om aan te geven dat het verbeteren van de veerkracht van het land op het gebied van cyberbeveiliging een topprioriteit is voor het DHS, heeft minister Mayorkas in zijn eerste maand als minister een oproep gedaan voor actie op het gebied van cyberbeveiliging. Deze oproep tot actie richtte zich op het aanpakken van de onmiddellijke dreiging van ransomware en op het opbouwen van een robuuster en diverser personeelsbestand.
- In maart 2021 schetste minister Mayorkas zijn bredere visie en een routekaart voor de cyberbeveiligingsinspanningen van het ministerie in een virtuele toespraak die werd georganiseerd door RSA Conference, in samenwerking met Hampton University en de Girl Scouts of the USA.
- Na zijn presentatie werd de minister vergezeld door Judith Batty, interim CEO van de Girls Scouts, voor een fireside chat over de ongekende cyberbeveiligingsuitdagingen waar de Verenigde Staten momenteel voor staan. Dr. Chutima Boonthum-Denecke van de afdeling Computerwetenschappen van Hampton University introduceerde de secretaris en leidde het programma af met vragen en antwoorden.
  - Overzicht van de cyberbeveiligingssprints van het DHS

Room for Improvement

bitwarden

Ministerie van Binnenlandse Veiligheid

Algehele Bitwarden-beoordeling: Ruimte voor verbetering

- Raadt het gebruik van een wachtwoordmanager niet aan
- Het belang van sterke wachtwoorden wordt niet genoemd
  - Biedt onnauwkeurig en misleidend advies over wachtwoordbeveiliging OF maakt geen melding van wachtwoorden of wachtwoordbeveiliging
  - Geeft niet duidelijk advies over wachtwoorden
- Noemt niet consequent de behoefte aan 2FA/MFA om wachtwoordbeveiliging verder te ondersteunen
- Het algemene beveiligingsadvies is niet up-to-date en voldoet niet aan de NIST-richtlijnen
- Geeft geen duidelijke, begrijpelijke en gemakkelijk te vinden aanbevelingen voor wachtwoordbeveiliging

Federal Bureau of Investigation (FBI)

De cyberbedreiging

Advies van het agentschap:

- Internetdelicten en cyberinbraken worden steeds geraffineerder en om ze te voorkomen moet elke gebruiker van een verbonden apparaat zich ervan bewust zijn en op zijn hoede zijn.
- Houd systemen en software up-to-date en installeer een sterk, gerenommeerd antivirusprogramma.
- Wees voorzichtig wanneer je verbinding maakt met een openbaar Wi-Fi-netwerk en voer geen gevoelige transacties uit, waaronder aankopen, wanneer je je op een openbaar netwerk bevindt.
- Maak een sterke en unieke wachtwoordzin voor elke online account en wijzig deze wachtwoordzinnen regelmatig.
- Stel multi-factor authenticatie in op alle accounts die dit toestaan.
- Bestudeer het e-mailadres in alle correspondentie en bestudeer de URL's van websites voordat u op een bericht reageert of een site bezoekt.
- Klik niet op iets in ongevraagde e-mails of sms-berichten.
- Wees voorzichtig met de informatie die je deelt in online profielen en sociale media accounts. Het delen van namen van huisdieren, scholen en familieleden kan scammers de hints geven die ze nodig hebben om je wachtwoorden of de antwoorden op de beveiligingsvragen van je account te raden.
- Stuur geen betalingen naar onbekende mensen of organisaties die op zoek zijn naar geldelijke steun en dring aan op onmiddellijke actie.
- Referentie

Oplichting en veiligheid op internet

Advies van het agentschap:

- **Houd uw firewall ingeschakeld**

  Een firewall helpt je computer te beschermen tegen hackers die toegang proberen te krijgen om de computer te laten crashen, informatie te wissen of zelfs wachtwoorden of andere gevoelige informatie te stelen. Software firewalls worden algemeen aanbevolen voor afzonderlijke computers. De software is voorverpakt op sommige besturingssystemen of kan worden aangeschaft voor afzonderlijke computers. Voor meerdere netwerkcomputers bieden hardwarerouters meestal firewallbescherming.

- **Installeer of update je antivirussoftware**

  Antivirussoftware is ontworpen om te voorkomen dat schadelijke softwareprogramma's zich op je computer nestelen. Als het schadelijke code detecteert, zoals een virus of een worm, werkt het om het onschadelijk te maken of te verwijderen. Virussen kunnen computers infecteren zonder dat de gebruiker het weet. De meeste soorten antivirussoftware kunnen zo worden ingesteld dat ze automatisch worden bijgewerkt.

- **Installeer of update uw antispywaretechnologie**

  Spyware is precies hoe het klinkt: software die stiekem op je computer wordt geïnstalleerd om anderen te laten meekijken met jouw activiteiten op de computer. Sommige spyware verzamelt informatie over u zonder uw toestemming of produceert ongewenste pop-upadvertenties op uw webbrowser. Sommige besturingssystemen bieden gratis spywarebescherming en er is goedkope software beschikbaar om te downloaden op het internet of in uw plaatselijke computerwinkel. Wees op je hoede voor advertenties op het internet die downloadbare antispyware aanbieden- in sommige gevallen kunnen deze producten nep zijn en spyware of andere kwaadaardige code bevatten. Het is net als boodschappen doen - koop waar je vertrouwen in hebt.

- **Houd je besturingssysteem up-to-date**

  Besturingssystemen van computers worden periodiek bijgewerkt om te blijven voldoen aan technologische vereisten en om veiligheidslekken te repareren. Zorg ervoor dat je de updates installeert om ervoor te zorgen dat je computer de nieuwste bescherming heeft.

- **Wees voorzichtig met wat je downloadt**

  Het achteloos downloaden van e-mailbijlagen kan zelfs de meest waakzame antivirussoftware omzeilen. Open nooit een e-mailbijlage van iemand die je niet kent en wees op je hoede voor doorgestuurde bijlagen van mensen die je wel kent. Ze kunnen onbewust kwaadaardige code hebben verspreid.

- **Schakel uw computer uit**

  Met de groei van snelle internetverbindingen kiezen veel mensen ervoor om hun computer aan te laten staan en klaar te maken voor actie. Het nadeel is dat computers kwetsbaarder worden als ze "altijd aan" staan. Naast firewallbeveiliging, die is ontworpen om ongewenste aanvallen af te weren, zorgt het uitschakelen van de computer er ook voor dat de verbinding van een aanvaller wordt verbroken, of het nu gaat om spyware of een botnet dat de bronnen van uw computer gebruikt om andere onwetende gebruikers te bereiken.

- Referentie

Good

bitwarden

Federal Bureau of Investigation (FBI)

Algehele Bitwarden-beoordeling: Goed

- Raadt het gebruik van een wachtwoordmanager niet aan
- Wijst op het belang van sterke wachtwoorden
- Noemt de behoefte aan 2FA/MFA om wachtwoordbeveiliging verder te ondersteunen
- Het algemene beveiligingsadvies is niet up-to-date en voldoet niet aan de NIST-richtlijnen
- Geeft geen duidelijke, begrijpelijke en gemakkelijk te vinden aanbevelingen voor wachtwoordbeveiliging

"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

Federale Handelscommissie (FTC)

Sterke wachtwoorden maken en andere manieren om je accounts te beschermen

Advies van het agentschap:

- Een andere optie is om een wachtwoordmanager van derden te gebruiken om een sterk wachtwoord te maken - en het te onthouden. Lees de recensies van experts om een goede wachtwoordmanager te vinden. Zorg ervoor dat het wachtwoord dat je gebruikt met de wachtwoordmanager sterk en veilig is. Een webbrowser, mobiele browser en wachtwoordmanager kunnen allemaal je wachtwoorden voor je opslaan.
- Een sterk wachtwoord is een belangrijke eerste stap in het beschermen van je account tegen hackers. Maar zelfs sterke wachtwoorden zijn kwetsbaar voor cyberaanvallen. Het gebruik van multi-factor authenticatie betekent dat een hacker die je wachtwoord steelt niet kan inloggen op je account zonder een andere authenticatiefactor.
- De meest voorkomende vorm van multifactor-authenticatie is een verificatiewachtwoord dat je per sms of e-mail ontvangt. Deze eenmalige toegangscode is meestal zes cijfers of langer en verloopt automatisch. Maar dit is de minst veilige vorm van twee-factor authenticatie, dus kies een veiligere methode zoals een authenticatie app of een beveiligingssleutel voor meer bescherming, als je de optie hebt.
- Referentie

Checklist voor wachtwoorden

Advies van het agentschap:

- **Zorg ervoor dat je wachtwoord lang en sterk is.** Dat betekent minstens 12 tekens. Een wachtwoord langer maken is over het algemeen de makkelijkste manier om het sterker te maken. Overweeg om een wachtwoordzin van willekeurige woorden te gebruiken zodat je wachtwoord beter te onthouden is, maar vermijd het gebruik van veelvoorkomende woorden of zinnen. Als de service die je gebruikt geen lange wachtwoorden toestaat, kun je je wachtwoord sterker maken door hoofdletters, kleine letters, cijfers en symbolen te combineren.

- **Gebruik wachtwoorden die je voor andere accounts hebt gebruikt niet opnieuw.** Gebruik verschillende wachtwoorden voor verschillende accounts. Op die manier, als een hacker je wachtwoord voor één account krijgt, kunnen ze het niet gebruiken om bij je andere accounts te komen.

- **Gebruik meerfactorauthenticatie als dat mogelijk is.** Sommige accounts bieden extra beveiliging door iets extra's te vereisen naast een wachtwoord om je aan te melden bij je account. Dit wordt multifactorauthenticatie genoemd. De "iets extra's" die je nodig hebt om je aan te melden bij je account vallen in twee categorieën:
  - Iets dat je hebt - zoals een wachtwoord dat je krijgt via een authenticatie-app of een beveiligingssleutel.
  - Iets wat je bent - zoals een scan van je vingerafdruk, je netvlies of je gezicht.

- **Overweeg een wachtwoordmanager.** De meeste mensen hebben moeite om al hun wachtwoorden bij te houden. Hoe langer en ingewikkelder een wachtwoord is, hoe sterker het is, maar een langer wachtwoord kan ook moeilijker te onthouden zijn. Overweeg om je wachtwoorden en beveiligingsvragen op te slaan in een gerenommeerde wachtwoordmanager. Om een goede wachtwoordmanager te vinden, zoekt u op onafhankelijke beoordelingssites en vraagt u vrienden en familie welke zij gebruiken. Zorg ervoor dat je een sterk wachtwoord gebruikt om de informatie in je wachtwoordmanager te beveiligen.

- **Kies beveiligingsvragen waar alleen jij het antwoord op weet.** Als een site u vraagt om beveiligingsvragen te beantwoorden, vermijd dan antwoorden die beschikbaar zijn in openbare documenten of gemakkelijk online te vinden zijn, zoals uw postcode, geboorteplaats of de meisjesnaam van uw moeder. En gebruik geen vragen met een beperkt aantal antwoorden die aanvallers gemakkelijk kunnen raden - zoals de kleur van je eerste auto. Je kunt zelfs onzinantwoorden gebruiken om het raden moeilijker te maken - maar als je dat doet, zorg er dan voor dat je kunt onthouden wat je gebruikt.

- **Wijzig wachtwoorden snel als er een lek is.** Als een bedrijf je vertelt dat er een datalek is geweest waarbij een hacker je wachtwoord heeft kunnen achterhalen, verander dan meteen het wachtwoord dat je gebruikt bij dat bedrijf en bij elke account die een soortgelijk wachtwoord gebruikt.

- Referentie

Excellent

bitwarden

Federale Handelscommissie (FTC)

Algehele Bitwarden-beoordeling: Uitstekend

- Beveelt het gebruik van wachtwoordbeheer aan
- Wijst op het belang van sterke wachtwoorden
- Noemt behoefte aan 2FA/MFA om wachtwoordbeveiliging verder te ondersteunen
- Het algemene beveiligingsadvies is up-to-date en voldoet aan de NIST-richtlijnen
- Geeft aanbevelingen voor wachtwoordbeveiliging op een duidelijke, begrijpelijke en gemakkelijk te vinden manier

"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

Ministerie van Handel

Nationale Maand van de Cyberveiligheid: Jezelf online beschermen

Advies van het agentschap:

- Voorheen was het gebruikelijk om wachtwoorden te maken met speciale tekens, hoofdletters, cijfers, letters en allerlei willekeurige regels, waaronder het verplichten om je wachtwoord meerdere keren per jaar te veranderen. Onderzoek toont aan dat ieder van ons hetzelfde deed als reactie - wachtwoorden gebruiken of variaties van hetzelfde wachtwoord maken omdat we tientallen unieke wachtwoorden moesten onthouden voor elke site, login of applicatie.

- Onze natuurlijke instincten creëerden een zwakke plek in onze online beveiliging en cybercriminelen profiteerden hiervan. Onderzoek naar het gebruik van wachtwoorden heeft de inherente zwakte aangetoond van de verwachting dat gebruikers willekeurig complexe wachtwoorden onthouden en het belang van het gebruik van multifactorauthenticatie (MFA) om onze privégegevens te beschermen. Wat belangrijk is, is dat ons denken over dit onderwerp is geëvolueerd en we hebben de volgende praktijken geïdentificeerd om onszelf beter te beschermen:
  - Als je een wachtwoord moet gebruiken, gebruik dan een langer wachtwoord (15 of meer tekens) of zelfs een wachtwoordzin, omdat deze meer bescherming bieden dan een korter, willekeurig complex wachtwoord. Wachtzinnen hebben als bijkomend voordeel dat ze gemakkelijk te onthouden zijn.
  - Het gebruik van MFA (zoals een eenmalige code die naar je wordt gemaild of een authenticatie-app op je telefoon) voegt een tweede, cruciale laag toe om je te beschermen tegen een gecompromitteerd wachtwoord. MFA moet worden ingesteld wanneer het beschikbaar is. Het duurt maar een paar tellen en geeft je gemoedsrust.

- Wachtwoordbeheerders, beschermd door één heel sterk, lang wachtwoord met MFA ingeschakeld, stellen ons in staat om unieke wachtwoorden aan te maken voor elke site zonder dat we ze allemaal hoeven te onthouden.

- Referentie

NIST valt onder het ministerie van Handel

Advies van het agentschap:

- Het waarborgen van de veiligheid van onze onderling verbonden wereldwijde netwerken en de apparaten en gegevens die op deze netwerken zijn aangesloten, is een van de belangrijkste uitdagingen van ons tijdperk.

- Het ministerie van Handel heeft als taak het bewustzijn en de bescherming op het gebied van cyberbeveiliging te verbeteren, de privacy te beschermen, de openbare veiligheid te handhaven, de economische en nationale veiligheid te ondersteunen en Amerikanen in staat te stellen hun online veiligheid beter te beheren.
  - NIST brengt versie 1.0 van Privacy Framework uit
  - NIST biedt 'snelstartgids' voor zijn catalogus met beveiligings- en privacywaarborgen
  - Cyberbeveiligingshoek voor kleine bedrijven

- Referentie

Very Good

bitwarden

Ministerie van Handel

Algehele Bitwarden beoordeling: Zeer goed

- Raadt het gebruik van een wachtwoordmanager aan
- Wijst op het belang van sterke wachtwoorden
- Noemt behoefte aan 2FA/MFA om wachtwoordbeveiliging verder te ondersteunen
- Het algemene beveiligingsadvies is up-to-date en voldoet aan de NIST-richtlijnen
- Geeft geen duidelijke, begrijpelijke en gemakkelijk te vinden aanbevelingen voor wachtwoordbeveiliging

Federale Communicatie Commissie (FCC)

Cyberbeveiligingstipensheet voor kleine bedrijven

- Train werknemers in beveiligingsprincipes. Stel basisbeveiligingspraktijken en -beleidsregels op voor werknemers, zoals het verplicht stellen van sterke wachtwoorden en het opstellen van richtlijnen voor gepast internetgebruik, waarin de straffen voor het overtreden van het bedrijfsbeleid voor cyberbeveiliging gedetailleerd worden beschreven. Stel gedragsregels op die beschrijven hoe om te gaan met klantinformatie en andere belangrijke gegevens en hoe deze te beschermen.
- Eis van werknemers dat ze unieke wachtwoorden gebruiken en wachtwoorden elke drie maanden wijzigen. Overweeg om multifactorauthenticatie te implementeren waarbij naast een wachtwoord aanvullende informatie nodig is om toegang te krijgen. Informeer bij uw leveranciers die gevoelige gegevens verwerken, met name financiële instellingen, of zij multi-factor authenticatie aanbieden voor uw account.
- Referentie

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

Federale Communicatie Commissie (FCC)

Algehele Bitwarden-beoordeling: Redelijk

- Raadt het gebruik van een wachtwoordmanager niet aan
- Wijst op het belang van sterke wachtwoorden
  - Koppelingen naar inhoud die zich richt op wachtwoordbeveiliging
  - De inhoud is echter duidelijk verouderd en zou overzichtelijker kunnen zijn
- Noemt niet consequent de behoefte aan 2FA/MFA om wachtwoordbeveiliging verder te ondersteunen
- Het algemene beveiligingsadvies is niet up-to-date en voldoet niet aan de NIST-richtlijnen
  - Tegen de NIST-richtlijnen in wordt aanbevolen wachtwoorden elke drie maanden te wijzigen
- Geeft geen duidelijke, begrijpelijke en gemakkelijk te vinden aanbevelingen voor wachtwoordbeveiliging

Small Business Administration (SBA)

Beste praktijken voor het voorkomen van cyberaanvallen

Advies van het agentschap:

- Medewerkers en hun werkgerelateerde communicatie zijn een belangrijke oorzaak van datalekken bij kleine bedrijven, omdat ze rechtstreeks toegang hebben tot je systemen. Door werknemers te trainen in de basispraktijken voor internetgebruik kunnen cyberaanvallen voor een groot deel worden voorkomen.
  - Andere trainingsonderwerpen die aan bod komen zijn onder andere:
    - Phishing e-mails herkennen
    - Goede internetgebruiken
    - Verdachte downloads vermijden
    - Verificatiehulpmiddelen inschakelen (bijv. sterke wachtwoorden, Multi-Factor Authenticatie, etc.)
    - Gevoelige informatie van leveranciers en klanten beschermen
- Referentie

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)

Algehele Bitwarden-beoordeling: Goed

- Raadt het gebruik van een wachtwoordmanager niet aan
- Wijst op het belang van sterke wachtwoorden
- Noemt de behoefte aan 2FA/MFA om wachtwoordbeveiliging verder te ondersteunen
- Het algemene beveiligingsadvies is niet up-to-date en voldoet niet aan de NIST-richtlijnen
- Geeft geen duidelijke, begrijpelijke en gemakkelijk te vinden aanbevelingen voor wachtwoordbeveiliging

Securities and Exchange Commission (SEC)

In juli 2023 heeft de SEC "definitieve regels aangenomen die openbare bedrijven verplichten om zowel materiële cyberbeveiligingsincidenten die ze meemaken als, op jaarbasis, materiële informatie over hun risicobeheer, strategie en bestuur op het gebied van cyberbeveiliging openbaar te maken". Gezien de rol van de SEC bij het afdwingen van cyberbeveiliging, lijkt het verstandig om het eigen wachtwoordbeveiligingsadvies van de SEC te beoordelen.

Een zoekopdracht naar "wachtwoordbeveiliging" op de website SEC.gov levert 12 documenten op, die allemaal van jaren geleden lijken te zijn. Er is een pagina gewijd aan cyberbeveiliging, maar deze biedt vrij algemene aanbevelingen die zijn overgenomen van CISA. Een risicowaarschuwing voor cyberbeveiliging uit 2020 getiteld "Cybersecurity: Safeguarding Client Accounts against Credential Compromise" leidt naar een PDF waarin credential stuffing wordt besproken. Hoewel het woord "wachtwoord" overal wordt gebruikt, wordt "wachtwoordbeveiliging" niet expliciet genoemd. In de onderstaande context wordt verwezen naar "sterke wachtwoorden":

Cyberbeveiliging: Accounts van klanten beveiligen tegen inbreuken op referenties

Advies van het agentschap:

- OCIE-medewerkers moedigen bedrijven aan om bij hun voorbereiding op aanvallen met "credential stuffing" na te denken over hun huidige werkwijzen (bijv. MFA en andere hierboven beschreven werkwijzen) en mogelijke beperkingen van die werkwijzen, en om te overwegen of de klanten en medewerkers van het bedrijf goed zijn geïnformeerd over hoe ze hun accounts beter kunnen beveiligen. Geïnformeerde klanten De meeste bedrijven verplichten klanten en personeel om sterke wachtwoorden aan te maken en te gebruiken. Het gebruik van wachtwoorden is echter minder effectief als klanten en/of medewerkers wachtwoorden van andere sites hergebruiken. Om effectiever te zijn, hebben sommige bedrijven klanten en medewerkers geïnformeerd en aangemoedigd om sterke, unieke wachtwoorden aan te maken en wachtwoorden te wijzigen als er aanwijzingen zijn dat hun wachtwoord is gecompromitteerd.

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)

Algehele Bitwarden-beoordeling: Redelijk

- Raadt het gebruik van een wachtwoordmanager niet aan
- Wijst op het belang van sterke wachtwoorden
  - Koppelingen naar gedateerde inhoud waarin sterke wachtwoorden worden erkend, maar die veel explicieter zou kunnen zijn
- Noemt niet consequent de behoefte aan 2FA/MFA om wachtwoordbeveiliging verder te ondersteunen
  - Hoewel er naar 2FA/MFA wordt verwezen in de PDF waarnaar hierboven wordt verwezen, is het geen uitgebreid advies en moet je even zoeken om het te vinden.
- Het algemene beveiligingsadvies is niet up-to-date en voldoet niet aan de NIST-richtlijnen
- Geeft geen duidelijke, begrijpelijke en gemakkelijk te vinden aanbevelingen voor wachtwoordbeveiliging

Het Witte Huis

Een proclamatie over de Maand van de Bewustwording van cyberbeveiliging, 2023

Advies van het agentschap:

- "Ik roep de mensen, bedrijven en instellingen van de Verenigde Staten op om het belang van cyberbeveiliging te erkennen en ernaar te handelen en de Cybersecurity Awareness Month in acht te nemen ter ondersteuning van onze nationale veiligheid en veerkracht. Ik roep ook bedrijven en instellingen op om actie te ondernemen om het Amerikaanse volk beter te beschermen tegen cyberdreigingen en nieuwe kansen te creëren voor Amerikaanse werknemers om goedbetaalde cyberbanen na te streven. Amerikanen kunnen ook direct actie ondernemen om zichzelf beter te beschermen, zoals het inschakelen van multifactor authenticatie, het updaten van software op computers en apparaten, het gebruiken van sterke wachtwoorden en voorzichtig zijn met het klikken op links die er verdacht uitzien."
- Referentie

Een Digital-First publieke ervaring bieden

Advies van het agentschap:

- Agentschappen moeten ervoor zorgen dat websites die authenticatie van het publiek vereisen, compatibel zijn met veelgebruikte wachtwoordbeheerders en mogen het "plakken" van wachtwoorden of andere geautomatiseerde, client-side hulpmechanismen niet verhinderen.
- Referentie

Verslag van het Witte Huis-symposium over de modernisering van multifactorauthenticatie

Advies van het agentschap:

- "Je hebt meer nodig dan een wachtwoord om online veilig te blijven en dat is waar multi-factor authenticatie een rol speelt om ervoor te zorgen dat je gegevens beter beschermd zijn tegen kwaadwillende cyberactoren," zegt CISA Executive Director Brandon Wales. "CISA heeft organisaties consequent aangespoord om MFA te implementeren voor alle gebruikers om ervoor te zorgen dat kritieke gegevens moeilijker toegankelijk zijn. Het symposium van vandaag gaat over samenkomen om de visie in kaart te brengen die we allemaal nastreven om werkelijkheid te maken."

- Referentie

De regering Biden-Harris kondigt een etiketteringsprogramma voor cyberveiligheid aan voor slimme apparaten om Amerikaanse consumenten te beschermen

Advies agentschap

- Op grond van haar bevoegdheid om draadloze communicatieapparatuur te reguleren, zal de FCC naar verwachting commentaar vragen over de uitrol van het voorgestelde vrijwillige programma voor het labelen van cyberbeveiliging, dat naar verwachting in 2024 van start zal gaan. Zoals voorgesteld zou het programma gebruikmaken van inspanningen van belanghebbenden om producten te certificeren en labelen, op basis van specifieke criteria voor cyberbeveiliging die zijn gepubliceerd door het National Institute of Standards and Technology (NIST) en die bijvoorbeeld unieke en sterke standaardwachtwoorden, gegevensbescherming, software-updates en mogelijkheden voor incidentdetectie vereisen.

- Referentie

Good

Updated January 2025

bitwarden

Het Witte Huis

Algehele Bitwarden-beoordeling: Goed

- Raadt het gebruik van een wachtwoordmanager niet aan
  - In een mededeling van 2022 over de Cybersecurity Awareness Month raadde het Witte Huis het gebruik van een wachtwoordmanager aan. Het Witte Huis had de kans om hetzelfde te doen in de 2023 Cybersecurity Awareness blog. Dat deden ze niet. Hoewel de blog 'het gebruik van sterke wachtwoorden' aanbeveelt, wordt er niets gezegd over wachtwoordmanagers.
- Wijst op het belang van sterke wachtwoorden
- Noemt behoefte aan 2FA/MFA om wachtwoordbeveiliging verder te ondersteunen
- Het algemene beveiligingsadvies is niet up-to-date en voldoet niet aan de NIST-richtlijnen
  - In eerdere mededelingen heeft het Witte Huis aanbevolen om wachtwoorden te veranderen, in tegenstelling tot het advies van NIST. Wachtwoorden moeten alleen worden gewijzigd als ze zwak, hergebruikt of gecompromitteerd zijn. Een sterk en uniek wachtwoord hoef je misschien nooit te veranderen, tenzij je vermoedt dat het gecompromitteerd is.
- Geeft geen duidelijke, begrijpelijke en gemakkelijk te vinden aanbevelingen voor wachtwoordbeveiliging
  - Geen speciale pagina over cyberbeveiliging

Samenvatting

Er zijn veel stappen die u kunt nemen om veilig online te blijven, maar de eenvoudigste actie met de grootste en meest directe impact op uw veiligheid is het gebruik van een wachtwoordmanager. Kies een cross-platform wachtwoordmanager met zero knowledge end-to-end encryptie die onbeperkt unieke en sterke wachtwoorden kan genereren en opslaan. U kunt aan de slag met Bitwarden met een gratis account of kiezen voor Premium voor minder dan $10/jaar om geavanceerde functies te krijgen.

Aanvullende bronnen

- Bekijk de presentatie over wachtwoordbeveiliging