RESOURCE CENTER

Five Best Practices for Enterprise Password Management

Learn the best practices for enterprise password management in this white paper.

Get the full interactive view at https://bitwarden.com/nl-nl/resources/five-best-practices-for-password-management-white-paper/

bitwarden

Terwijl organisaties van beveiliging een prioriteit blijven maken, bestaat een belangrijk deel van die inspanning uit het opleiden en informeren van algemene gebruikers over best practices. Kijk eens naar enkele van deze statistieken uit het Yubico 2019 State of Password and Security Authentication Security Behaviors Report:

- 2 op de 3 respondenten deelt wachtwoorden met collega's
- 51% van de deelnemers zegt wachtwoorden te hergebruiken voor persoonlijke en zakelijke accounts
- 57% zegt zijn wachtwoord niet te hebben gewijzigd na een phishingpoging

Om verandering te brengen in een onderneming, moeten beveiligings- en IT-teams werknemers informeren over best practices. Wat betreft wachtwoordbeheer is een van de eenvoudigste manieren om een goede wachtwoordhygiëne aan te moedigen het inzetten van een oplossing voor wachtwoordbeheer op uw werkplek. Hier zijn enkele best practices om toe te passen.

1. Gebruik een oplossing voor wachtwoordbeheer

Gedurende de dag bezoeken de meeste mensen veel verschillende sites waarvoor wachtwoorden nodig zijn. Het onthouden van veel unieke en voldoende sterke wachtwoorden (of wachtzinnen) is vrijwel onmogelijk. Een wachtwoordmanager vereenvoudigt het gebruik van wachtwoorden op verschillende sites om gebruikers veiliger te houden. Er zijn een aantal goede wachtwoordmanagers. Geef de voorkeur aan platformonafhankelijke diensten die gratis of tegen een zeer lage prijs aan particulieren worden aangeboden. De meeste wachtwoordbeheerders zijn in de loop der jaren ook uitgebreid.

2. Kies een tool die je gemakkelijk in je hele organisatie kunt inzetten

Wachtwoordmanagers moeten eenvoudig te gebruiken zijn voor elk gebruikersniveau, van beginner tot gevorderde. Als je een groot of verspreid personeelsbestand overweegt, moeten de applicaties intuïtief in gebruik zijn en gemakkelijk te implementeren. Of u nu kiest voor de Bitwarden Cloud of voor uw eigen zelf gehoste Bitwarden-instantie, het opstarten van Bitwarden is eenvoudig. En Bitwarden Directory Connector werkt met de meest gebruikte directoryservices van dit moment, zoals Azure, Active Directory, Google, Okta en anderen, om uw Bitwarden-gebruikers in-sync te houden met uw teams en medewerkers.

3. Wijzig wachtwoorden alleen als u mogelijk bent gecompromitteerd

De dagen dat je je wachtwoord elke drie maanden moest veranderen zijn voorbij. Je zou ze nu alleen moeten veranderen als je denkt dat je bent gecompromitteerd. Het National Institute of Standards and Technology (NIST) raadt gebruikers niet aan om wachtwoorden vaak te veranderen. Dit leidt in feite tot gedrag dat na verloop van tijd kan resulteren in zwakkere wachtwoorden. U kunt bepalen of een wachtwoord gecompromitteerd is door te verwijzen naar tastbaar bewijs, zoals creditcardfraude, of door een hulpmiddel te gebruiken (zoals uw wachtwoordmanager) dat kan vertellen of uw wachtwoord blootgesteld is bij een inbreuk.

4. Gebruik sterke, unieke wachtwoorden

Door sterke, unieke wachtwoorden te gebruiken voor elke service die je online gebruikt, beperk je de impact van datalekken. Een sterk wachtwoord betekent niet per se het toevoegen van speciale tekens of cijfers aan een gewoon woord of naam, het betekent het vergroten van de entropie, of willekeurigheid van het wachtwoord. Een eenvoudige tactiek voor het maken van een sterk wachtwoord is het gebruik van een wachtwoordzin. Een wachtwoordzin combineert schijnbaar ongerelateerde woorden of zinnen die de gebruiker gemakkelijk kan onthouden, maar die anders moeilijk te raden zouden zijn door een aanvaller. Wachtzinnen hebben een hoge mate van entropie en zijn tegelijkertijd makkelijk te onthouden.

5. Schakel waar mogelijk authenticatie met twee factoren in

Nu authenticatie met twee factoren (2FA) steeds gebruikelijker wordt op websites van consumenten en bedrijven, bevat een goede wachtwoordmanager manieren om deze functie uit te breiden. Het gebruik van 2FA verhoogt de veiligheid van je account door je te verplichten om een ander token in te voeren dan alleen je hoofdwachtwoord. Zelfs als iemand uw hoofdwachtwoord ontdekt, kan hij niet inloggen op uw wachtwoordmanager zonder toegang tot het extra token. Als u aan de slag wilt met een wachtwoordmanager, kunt u zich hier aanmelden voor een gratis Bitwarden-account.