OUCH! | October 2015

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

Password Managers

Overzicht

Een van de belangrijkste maatregelen die je kan nemen om jezelf online te beveiligen is een uniek en sterk wachtwoord te voorzien voor iedere account die je gebruikt. Jammer genoeg hebben we zodanig veel accounts, dat het herinneren van al deze wachtwoorden een haast onmogelijke opgave wordt. Een passwoord manager, ook gekend als een wachtwoordkluis, biedt een eenvoudige oplossing. Deze toepassingen zijn ontworpen om op een veilige manier al jouw logingegevens te bewaren. Bovendien maken ze het eenvoudig om in te loggen op websites, mobiele apps en alle andere toepassingen.

Gast redacteur

Lenny Zeltser focust zich op het veilig houden van IT-operaties bij NCR Corp en traint security professionals bij het SANS-instituut. Lenny is actief op Twitter als **@lennyzeltser** en schrijft blogberichten op **zeltser.com**.

Hoe Password Managers Werken

Een password manager werkt als een virtuele kluis, het bewaart op een veilige manier jouw gebruikersnamen, wachtwoorden en andere gevoelige informatie. Wanneer een website aan jou vraagt om in te loggen met jouw account, kan de password manager automatisch jouw wachtwoord opzoeken en jou laten inloggen op de website. Dit maakt het eenvoudig om honderden unieke, sterke wachtwoorden te hebben, zonder dat je ze dient te onthouden.

Password managers bewaren jouw gegevens in een database, die soms de kluis wordt genoemd. De password manager versleutelt de inhoud en beveiligt het met een master wachtwoord, die enkel jij kent. Wanneer je wachtwoordgegevens wilt opzoeken of wil inloggen op jouw online bank of e-mail account, geef je jouw master wachtwoord in om de password manager kluis te openen.

Sommige password managers plaatsen de kluis op jouw systeem of smartphone, terwijl andere dit plaatsen op een website, die onderhouden wordt door het bedrijf dat de password manager heeft ontwikkeld. Ook bieden de meeste password managers de mogelijkheid om de gegevens van de kluis automatisch te synchroniseren tussen de verschillende toestellen, die je instelt. Op deze manier zullen de wijzigingen, indien je een wachtwoord aanpast op jouw laptop, zich automatisch synchroniseren naar jouw smartphone, tablet of ander toestel dat je gebruikt. Ongeacht waar de database zich bevindt, moet je enkel de password manager toepassing installeren op het systeem of toestel om het te gebruiken.

Wanneer je de password manager voor een eerste keer instelt, dien je jouw gebruikersnamen en wachtwoorden manueel of automatisch te importeren. Daarna kan de password manager detecteren wanneer je een nieuwe online account wil

© SANS Institute 2015

Password Managers

registreren of een bestaand wachtwoord aanpast en dit automatisch aanpassen in de kluis. Dit is mogelijk omdat de meeste password managers nauw samenwerken met jouw web browser. Deze integratie laat het toe om automatisch in te loggen op websites.

Password managers zijn ontworpen om op een veilige manier gevoelige gegevens op te slaan. Het is echter belangrijk dat het master wachtwoord, dat je gebruikt om de gegevens van de kluis te beveiligen, sterk en moeilijk te voorspellen is. We raden aan om van jouw master wachtwoord een wachtzin te gebruiken, dit is het sterkst mogelijke type wachtwoord. Indien jouw password manager twee-staps-verificatie ondersteunt, gebruik dit dan als master wachtwoord. Ten slotte zorg ervoor dat je jouw master wachtwoord niet gebruikt op andere systemen of voor andere accounts. Op deze manier voorkom je dat wanneer een hacker een kopie van jouw kluis bemachtigt, hij jouw wachtwoord niet kan voorspellen en geen toegang heeft tot de inhoud. Zorg ervoor dat je jouw master wachtwoord niet vergeet. Indien je het vergeet, heb je geen toegang meer tot jouw andere wachtwoorden.

Password managers zijn een handig middel om al jouw wachtwoorden veilig te bewaren en gebruiken.

Een Password Manager Kiezen

Er zijn verschillende gratis en commerciële password managers die je kan kiezen. Wanneer je op zoek gaat naar een oplossing, gebruik dan de volgende tips:

- Ga na of de password managers al jouw systemen en mobiele toestellen ondersteunt. De oplossing dient op een gemakkelijke manier de gegevens op al jouw toestellen te synchroniseren.
- Gebruik enkel bekende en vertrouwde password managers. Wees voorzichtig met oplossingen die nog niet lang bestaan en weinig tot geen recensies hebben. Net als bij valse antivirus software, ontwikkelen cybercriminelen soms nep-password managers om jouw persoonlijke gegevens te stelen.
- Jouw password manager moet eenvoudig in gebruik zijn. Indien je de oplossing te complex vindt, zoek dan naar een alternatief die beter past bij jouw stijl en kennisniveau.
- Kijk of er regelmatig patches en updates voor het programma uitkomen, en zorg dat je altijd over de laatste versie beschikt.
- De password manager moet het voor jou gemakkelijk maken om sterke wachtwoorden voor je verschillende accounts te kiezen. Ook moet het mogelijk zijn om automatisch sterke wachtwoorden te genereren en het de sterkte aangeeft van het gekozen wachtwoord.
- De password manager moet ook andere gevoelige gegevens kunnen bewaren zoals antwoorden op beveiligingsvragen, kredietkaarten of frequent flyer nummers.

© SANS Institute 2015

Password Managers

- Wees voorzichtig met password managers die eigen gepatenteerde of onbekende encryptie methodes gebruiken, in plaats van de gekende en standaard methodes. Indien de verkoper vermeldt dat er gebruik wordt gemaakt van zelf ontwikkelde encryptiemethodes, vermijdt dan zeker hun oplossing.
- Vermijd iedere password manager die claimt dat het jouw vergeten master password kan herstellen. Dit betekent dat ze jouw master wachtwoord kennen, dit stelt je bloot aan te veel risico's.

Password managers bieden een goede oplossing om op een veilige manier al jouw wachtwoorden te bewaren. Net omdat ze zulke belangrijke informatie opslaan, dien je een sterk master password te kiezen die niet eenvoudig te raden is, maar wel eenvoudig is om te onthouden.

Meer Weten?

Ga naar http://www.securingthehuman.org om je te abonneren op de maandelijkse OUCH! Security awareness nieuwsbrief, toegang te krijgen tot het OUCH! archief en kom meer te weten over SANS security awareness oplossingen.

Over Cegeka Groep

Cegeka Groep is een onafhankelijke ICT-dienstverlener opgericht in 1992. Cegeka heeft zijn hoofdkantoor in België en heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Tsjechië en Slovakije. Het bedrijf levert diensten aan klanten in heel Europa: enterprise cloud- en securitydiensten, applicatiediensten, agile coaching en outsourcingdiensten. Cegeka stelt 3.200 mensen tewerk en haalde in 2013 een omzet van 330 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Bronnen (Engels)

Wachtzinnen:	http://www.securingthehuman.org/ouch/2015#april2015
Twee-factor Authenticatie:	https://www.securingthehuman.org/ouch/2015#september2015
Top Five Password Managers:	http://lifehacker.com/5529133/five-best-password-managers
SANS Security Tip of the Day:	http://www.sans.org/tip_of_the_day.php

OUCH! Is een publicatie van SANS Securing The Human en wordt verdeeld onder de Creative Commons BY-NC-ND 4.0 license. Deze nieuwsbrief mag verder verdeeld worden en gebruikt worden in uw eigen security awareness programma, zolang u de inhoud niet wijzigt. Stuur een bericht naar ouch@securingthehuman.org voor meer informatie en voor vertalingen.

Redactie: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Vertaald door: Sven Jacobs, Tom Palmaers