OUCH! | April 2015

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- **Wachtzinnen**
- **Wachtzinnen veilig gebruiken**

Wachtzinnen

Achtergrond

Wachtwoorden gebruiken we iedere dag, om e-mail te lezen, voor online banking, om online te shoppen of om je smartphone te gebruiken. Wachtwoorden zijn ook één van onze zwakste punten, als iemand jouw wachtwoord kent, kan hij jouw identiteit stelen, geld overmaken of jouw persoonlijke gegevens raadplegen. Sterke wachtwoorden zijn essentieel om jezelf te beschermen. In deze nieuwsbrief leer je hoe je sterke wachtwoorden maakt die eenvoudig te herinneren zijn door een bepaald type wachtwoorden te gebruiken, genaamd wachtzinnen.

Gastredacteur

Guy Bruneau is een senior security consultant bij IPSS Inc., een SANS-instructeur en een ISC-handler. Guy is houder van een SANS GSE en heeft het SANS Cyber Guardian programma afgemaakt. Je kan hem volgen op Twitter **@GuyBruneau** en op **handlers.sans.org/gbruneau**.

Wachtzinnen

De uitdaging is dat cyberaanvallers speciale methodes hebben ontwikkeld om jouw wachtwoord te raden of te “bruteforcen” en ze blijven er beter in worden. Dit betekent dat ze wachtwoorden kunnen kraken die zwak of eenvoudig te raden zijn. Een belangrijke stap om jezelf te beschermen is om sterke wachtwoorden te gebruiken. Hoe meer tekens jouw wachtwoord bevat, des te sterker en moeilijker het is voor een aanvaller om deze te raden. Lange en complexe wachtwoorden zijn echter moeilijk te onthouden. In de plaats hiervan raden we wachtzinnen aan, dit zijn simpele zinnen die je eenvoudig kan onthouden, maar moeilijk zijn om te hacken. Hier is een voorbeeld:

Waar is koning Julian?

Wat maakt deze wachtzin zo sterk? Het is niet enkel 22 tekens lang, maar het heeft ook grote letters en symbolen (spaties en leestekens zijn ook tekens). Je kan jouw wachtzin zelfs sterker maken door letters te vervangen met cijfers of symbolen, zoals de letter “a” te vervangen met het “@” symbool of de letter “o” met het nummer nul. Indien een website of programma het gebruik van nummers beperkt in een wachtwoord, gebruik dan het maximum aantal toegelaten tekens.

© SANS Institute 2015

Wachtzinnen

Wachtzinnen veilig gebruiken

Je moet voorzichtig zijn hoe je wachtzinnen gebruikt. Een wachtzin gebruiken helpt niet indien slechteriken ze eenvoudig kunnen kopiëren of stelen.

Het gebruik van wachtzinnen is één van de beste maatregelen die je kan nemen om jouw identiteit en gegevens te beveiligen.

1. Zorg voor een unieke wachtzin voor iedere gebruikersaccount of toestel. Gebruik bijvoorbeeld nooit dezelfde wachtzin voor jouw werk of bankactiviteiten, als die voor jouw persoonlijke accounts, zoals Facebook, YouTube of Twitter. Op die manier, als één account gehacked is, zullen de andere accounts nog veilig zijn. Als je te veel wachtzinnen hebt om te onthouden (wat vaak voorkomt), overweeg dan om een password manager te gebruiken. Dit is een speciaal programma waar je op een veilige manier alle wachtzinnen kunt opslaan. Zo hoef je enkel de wachtzinnen te onthouden van jouw computer en het password manager programma.

2. Deel nooit een wachtzin of de manier waarop je deze samenstelt met iemand anders, ook niet met collega's. Onthoud dat een wachtzin een geheim is, indien iemand anders dit kent is het niet langer veilig. Indien je per ongeluk je wachtzin deelt, of denkt dat deze gekend of gestolen is, verander ze dan onmiddellijk.

3. Net als bij wachtwoorden, vermijd dat ze eenvoudig te voorspellen zijn of veel voorkomend zijn. Bijvoorbeeld de zin "Dit is een wachtwoord" is geen goede wachtzin omdat het zo veel voorkomend en voorspelbaar is.

4. Gebruik geen openbare computer zoals die in hotels of bibliotheken om in te loggen op een werk- of bankaccount. Aangezien iedereen deze computers kan gebruiken, kunnen ze mogelijk geïnfecteerd zijn met schadelijke software die al jouw toetsaanslagen kan registreren. Log enkel in op jouw werk- of bankaccounts op vertrouwde computers of mobiele toestellen.

5. Wees voorzichtig met websites waarbij je persoonlijke vragen kan beantwoorden. Deze vragen worden gebruikt indien je jouw wachtzin vergeet en deze wil resetten. Het probleem is dat veel antwoorden te vinden zijn op het Internet; of misschien wel op jouw Facebook pagina. Als je zulke persoonlijke vragen beantwoordt, gebruik dan enkel informatie die niet publiek beschikbaar is of fictieve informatie die je verzonnen hebt. Password managers kunnen helpen met dit door de extra informatie te bewaren.

© SANS Institute 2015

Wachtzinnen

6. Veel online accounts bieden tweefactor authenticatie aan, ook gekend als tweestapsverificatie. Hier heb je meer nodig dan enkel jouw wachtzin om in te loggen, zoals een code die verstuurd wordt naar jouw smartphone. Deze optie is veel veiliger dan enkel de wachtzin zelf. Indien mogelijk, gebruik altijd deze sterkere opties van authenticatie.

7. Mobiele toestellen vereisen vaak een PIN om toegang te beveiligen. Weet goed dat een PIN niets anders dan een wachtwoord is. Hoe langer jouw PIN hoe veiliger. Veel mobiele toestellen laten toe om jouw PIN-nummer te wijzigen tot een wachtzin.

8. Ten slotte, als je een account niet meer gebruikt, zorg er dan voor dat je deze afsluit, verwijdert of uitschakelt.

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)

Two-step Verification:	http://www.securingthehuman.org/ouch/2013#august2013
Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013
Social Engineering:	http://www.securingthehuman.org/ouch/2014#november2014
Common Security Terms:	http://www.securingthehuman.org/resources/security-terms

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