OUCH!

SANS SECURITY AWARENESS

De maandelijkse Security Awareness nieuwsbrief voor jou!

Wachtwoorden Eenvoudig Gemaakt

Overzicht

Er wordt vaak gezegd dat wachtwoorden de sleutel zijn tot het beschermen van je accounts (wat waar is!), maar zelden krijg je een eenvoudige manier om al je wachtwoorden veilig aan te maken én te beheren. Hieronder behandelen we drie eenvoudige stappen om je wachtwoorden te vereenvoudigen, je accounts te vergrendelen en je toekomst te beschermen.

Wachtwoordzinnen

De dagen van gekke, complexe wachtwoorden zijn voorbij. Die wachtwoorden zijn moeilijk te onthouden, moeilijk te typen en met de huidige supersnelle computers kan het voor een cyberaanvaller alsnog gemakkelijk zijn om ze te kraken. De sleutel tot wachtwoorden is om ze lang te maken, hoe meer karakters je hebt, hoe beter. Deze worden wachtwoordzinnen genoemd, een soort sterk wachtwoord dat gebruik maakt van een korte zin of willekeurige woorden. Hier zijn twee voorbeelden

Tijd voor sterke koffie!
Verloren-slak-kruipen-strand

Beide zijn sterk met meer dan twintig karakters, gemakkelijk te onthouden en eenvoudig te typen, maar moeilijk te kraken. Je komt websites of situaties tegen waarin je symbolen, cijfers of hoofdletters aan je wachtwoord moet toevoegen, wat prima is. Vergeet niet dat de lengte het belangrijkst is.

Wachtwoordmanager

Je hebt een uniek wachtwoord nodig voor elk account. Als je hetzelfde wachtwoord hergebruikt voor meerdere accounts, loop je een groot gevaar. Het enige wat een cyberaanvaller hoeft te doen is een website die je gebruikt te hacken, alle wachtwoorden te stelen, inclusief die van jou, en vervolgens je wachtwoord te gebruiken om in te loggen op al je andere accounts. Het gebeurt veel vaker dan je je realiseert. Geloof je het niet? Kijk op de website www.haveibeenpwned.com om te zien welke sites jij gebruikt die gehackt zijn en welke wachtwoorden mogelijk gecompromitteerd zijn. Dus wat moet je doen? Gebruik een wachtwoordmanager.

Dit zijn speciale computerprogramma's die al je wachtwoorden veilig opslaan in een gecodeerde kluis. Je hoeft maar één wachtwoord te onthouden, het wachtwoord voor je wachtwoordbeheerder. De wachtwoordmanager haalt jouw wachtwoorden automatisch op wanneer je ze nodig hebt en logt je in op websites voor jou. Ze hebben ook andere functies zoals het opslaan van je antwoorden op geheime vragen, het waarschuwen wanneer je wachtwoorden hergebruikt, een wachtwoordgenerator die ervoor zorgt dat je sterke wachtwoorden gebruikt, en vele andere functies. De meeste

wachtwoordmanagers synchroniseren ook veilig op bijna elke computer of apparaat, dus ongeacht het systeem dat je gebruikt, heb je gemakkelijk en veilig toegang tot al je wachtwoorden.

Tot slot, schrijf het wachtwoord op in jouw wachtwoordmanager en bewaar het thuis op een veilige locatie. Sommige wachtwoordmanagers laten je zelfs een wachtwoordmanager recovery kit afdrukken. Op die manier heb je een back-up als je het wachtwoord vergeet. Of, als je ziek wordt of in een noodsituatie verkeert, kan je echtgeno(o)t(e) of een vertrouwd familielid de informatie namens jou opvragen.

Tweestapsverificatie

Verificatie in twee stappen (vaak Two-factor Authenticatie of Multi-factor Authenticatie genoemd) voegt een extra beveiligingslaag toe. Het vereist dat je twee dingen hebt wanneer je inlogt op je accounts, je wachtwoord en een numerieke code die wordt gegenereerd door je smartphone of verzonden naar je telefoon. Dit proces zorgt ervoor dat zelfs als een cyberaanvaller jouw wachtwoord krijgt, ze nog steeds niet in je accounts kunnen komen. Verificatie in twee stappen is eenvoudig in te stellen en je hoeft het meestal maar één keer te gebruiken wanneer je inlogt vanaf een nieuwe computer of apparaat. Schakel dit waar mogelijk in, vooral voor je belangrijkste rekeningen zoals je bank- of pensioenrekeningen of toegang tot je e-mail. Als je een wachtwoordmanager gebruikt, raden we je ten zeerste aan om deze te beschermen met een sterke passphrase EN tweestapsverificatie.

Het klinkt misschien dwaas, maar deze drie eenvoudige stappen zijn bewezen effectief voor het beschermen van jouw werk, reputatie en je financiële toekomst.

Over Cegeka Groep

Cegeka is een onafhankelijke ICT–dienstverlener die klanten in heel Europa helpt met hun digitale transformatie, agile ontwikkeling, trusted cloudoplossingen en 24/7 managed services. Cegeka heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Slowakije en Tsjechië. Cegeka heeft 3.600 medewerkers. In 2015 realiseerde Cegeka Groep een omzet van 368 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Gastredacteur

Justin Henderson *(@SecurityMapper) is medeoprichter van H & A Security Solutions, een gecertificeerd SANS Institute Instructeur en auteur voor de SANS Cyber Defense en SIEM cursussen. Hij houdt van alles wat met cyberdefensie te maken heeft en is al vijftien jaar consultant..*

Bronnen

Have I Been Pwned:	https://haveibeenpwned.com/
Two-factor Authentication Site:	https://twofactorauth.org/
NIST SP800-63B Digital Identity Guidelines:	https://pages.nist.gov/800-63-3/sp800-63b.html
Poster: You Are a Target:	https://www.sans.org/u/OGi