OUCH! | June 2016

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- **Wat is Encryptie?**
- **Wat kan je Encrypteren?**
- **Correct Gebruik**

Encryptie

Wat is Encryptie?

Je hebt al vast gehoord over encryptie en hoe je jezelf en jouw gegevens hiermee kunt beschermen. Encryptie kan echter verwarrend zijn en heeft ook beperkingen. In deze nieuwsbrief leggen we encryptie uit in verstaanbare taal, hoe het jou beschermt en hoe je het correct gebruikt.

Gast redacteur

Francesca Bosca (**@francibosco**) is een onderzoeker en leidt projecten over cybercrime, cyberbeveiliging en misbruik van technologie. Ze werkt bij de United Nations Interregional Crime and Justice Research instituut en is medeoprichter van de Tech and Law Center.

Je beschikt over een grote hoeveelheid aan gevoelige informatie op jouw toestellen, zoals persoonlijke documenten, foto's en e-mailberichten. Indien er één van deze toestellen verloren raakt of gestolen wordt, kunnen deze gevoelige gegevens worden geraadpleegd door diegene die het toestel heeft. Bovendien gebruik je het om gevoelige transacties doen als online bankieren of winkelen. Als iemand deze activiteiten kan meevolgen dan kunnen ze jouw gegevens stelen zoals financiële gegevens of kredietkaartgegevens. Encryptie verdedigt je in deze situaties door ervoor te zorgen dat onbevoegde personen geen toegang krijgen tot jouw gegevens.

Encryptie bestaat al sinds duizenden jaren. Vandaag is encryptie zeer gesofisticeerd, maar heeft het hetzelfde doel – een geheime boodschap versturen en te verzekeren dat enkel bevoegde personen deze boodschap kunnen lezen. Wanneer gegevens niet versleuteld zijn, noemt men dit leesbare tekst. Dit kan iedereen lezen en raadplegen. Gegevens in een onleesbaar formaat noemt men versleutelde tekst. De hedendaagse encryptie werkt met complexe wiskundige formules en een unieke sleutel om jouw gegevens om te vormen naar versleutelde tekst. Met de sleutel kan je de gegevens leesbaar en onleesbaar maken. Vaak is de sleutel een wachtwoord of een toegangscode.

Wat kan je Encrypteren?

Er is een onderscheid tussen twee types van data om te versleutelen, data in rusttoestand (zoals de data dat op jouw mobiel toestel staat) en data in beweging (wanneer je een e-mail of bericht ontvangt van een vriend).

Encryptie

Encryptie van data in rusttoestand is cruciaal om de gegevens te beschermen wanneer jouw pc of mobiel toestel verloren of gestolen is. De hedendaagse toestellen zijn zeer krachtig en kunnen veel gegevens opslaan, maar kan je gemakkelijk verliezen. Bovendien zijn er andere draagbare media die vertrouwelijke gegevens opslaan als USB-sticks en externe harde schijven. Full Disk Encryptie (FDE) is een gangbare techniek om jouw harde schijf te encrypteren. Dit betekent dat alles op het systeem automatisch wordt geëncrypteerd, je moet niet aangeven wat je wel en niet wil encrypteren. Vandaag zijn de meeste computers voorzien van FDE, maar dien je dit manueel in te schakelen. Op Mac computers is er FileVault, terwijl op Windows, afhankelijk van de versie, heb je BitLocker of Device Encryption. De meeste mobiele toestellen ondersteunen FDE. iOS schakelt FDE in eens je een toegangscode hebt ingesteld op iPhone en iPads. Vanaf Andriod 6.0 (Marshmallow), schakelt Google FDE standaard in, als de hardware vereisten van het toestel voldoen aan de minimum vereisten.

Encryptie is een krachtige manier om jouw gegevens te beveiligen, maar is slechts zo sterk als jouw sleutel.

Gegevens zijn ook kwetsbaar als ze in beweging zijn. Als de gegevens niet geëncrypteerd zijn, kunnen deze worden gemonitored, aangepast en online worden onderschept. Daarom moet je zeker dat gevoelige onlinetransacties en -communicatie versleuteld zijn. Een veel gebruikte methode van online encryptie is HTTPS. Hiermee wordt al het verkeer tussen jouw browser en de website versleuteld. Kijk of er https:// in de URL staat, of er een hangslot icoon is in jouw browser, of dat de URL in de adresbalk groen wordt. Een ander voorbeeld is wanneer je e-mail ontvangt of verstuurt. De meeste e-mailprogramma's voorzien mogelijkheden om te encrypteren die je nog moet inschakelen. Een derde voorbeeld zijn de gegevens van een gesprek tussen twee chatgebruikers, zoals iMessage, Wickr, Signal, WhatsApp of Telegram. Deze apps zorgen voor een end-to-end encryptie waardoor derden geen toegang hebben als de data wordt verstuurd tussen de systemen of toestellen. Hierdoor kunnen enkel jijzelf en de andere persoon de gegevens lezen.

Correct Gebruik

Om er zeker van te zijn dat encryptie je beschermt, moet je het op een juiste manier te gebruiken:

- De encryptie is maar zo sterk als de sleutel. Als iemand jouw sleutel raadt of ertoe toegang heeft, kunnen ze de gegevens raadplegen. Bescherm daarom jouw sleutel. Indien je een toegangscode of wachtwoord gebruikt voor de

Encryptie

sleutel, zorg er dan voor dat deze sterk en uniek is. Hoe langer jouw wachtwoord, hoe moeilijker het is om het te raden of te bruteforcen. Vergeet jouw wachtwoord niet, zonder de sleutel kan je immers de gegevens niet meer raadplegen. Heb je moeite met de sleutel te onthouden, gebruik dan een wachtwoordkluis.

- De beveiliging van jouw toestellen speelt een grote rol. Indien jouw toestel is gecompromitteerd of besmet met malware, dan kunnen cyberaanvallers de encryptie omzeilen. Net daarom is het belangrijk dat je bijkomende maatregelen treft zoals antivirus, sterke wachtwoorden en het uitvoeren van updates.
- Veel apps en pc-toepassingen bieden sterke encryptie aan om jouw gegevens en verbinding te beveiligen. Indien er geen encryptie wordt voorzien, zoek dan een alternatief.

Meer Weten?

Ga naar securingthehuman.sans.org/ouch/archives 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)

Encryption Explained:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
Password Managers:	https://securingthehuman.sans.org/ouch/2015#october2015
What Is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016

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