OUCH! | Augustus 2014

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- Wat is encryptie?
- Encryptie-in-rust
- Encryptie-in-overdracht

Encryptie

Wat is Encryptie?

Je hebt misschien al gehoord over het begrip 'encryptie' en hoe je het kan gebruiken om jezelf en jouw gegevens te beschermen. Hoewel het begrip encryptie verwarrend kan zijn, beschermt het niet tegen alles en zijn er beperkingen. In deze nieuwsbrief leggen we encryptie uit op een eenvoudige manier, waarom je het moet gebruiken en hoe je het juist gebruikt.

Gastredacteur

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) is een consultant in het Washington, DC gebied. Hij is hoofdinstructeur voor het SANS Instituut en geeft de cursus 'Mobile Device Security en Ethisch Hacken' (SEC575), tevens is hij auteur van de cursus 'Incident Response Team Management' (MGT535).

Jouw computer en mobiele toestellen bevatten een grote hoeveelheid aan gevoelige gegevens, zoals financiële documenten, afbeeldingen, email en medische gegevens. Als er één van jouw toestellen verloren raakt of gestolen wordt, dan kan deze gevoelige informatie worden geraadpleegd door diegene die het toestel bezit. Indien je aan online bankieren doet of online winkelt met jouw toestel, kan een cyber crimineel die jouw online activiteiten monitort, financiële gegevens stelen zoals jouw bankrekening of kredietkaartgegevens. Encryptie verdedigt je in zulke situaties zodat onbevoegde personen jouw informatie niet kunnen raadplegen of wijzigen.

Informatie die niet geëncrypteerd is, heet leesbare tekst. Dit houdt in dat iedereen de tekst kan lezen of kan raadplegen. Encryptie zorgt ervoor dat leesbare tekst wordt omgezet naar een niet-leesbaar formaat, namelijk vercijferde tekst. Encryptie past complexe wiskundige bewerkingen toe en een unieke sleutel om de leesbare tekst om te zetten naar vercijferde tekst. De sleutel zorgt voor de versleuteling of ontsleuteling van de informatie, net zoals bij het openen of sluiten van een deur. Een bekend voorbeeld is het wachtwoord, enkel diegene die het wachtwoord kent, kan jouw informatie ontsleutelen. Om jouw geëncrypteerde informatie te beschermen, dien je jouw sleutel te beschermen. In het algemeen werkt encryptie op 2 manieren, je kan jouw data-in-rust encrypteren (zoals de data op jouw laptop) alsook data-in-overdracht (zoals data die online wordt verzonden).

Encryptie-in-rust

Het hoofddoel van encryptie-in-rust is om jouw gegevens te beschermen wanneer jouw computer of mobiel toestel verloren raakt of gestolen is. 15 jaar geleden was dit geen probleem, computers waren toen immers groot, zwaar en

Encryptie

moeilijk te bewegen. Nu wegen laptops enkele kilo's en mobiele toestellen slechts honderden grammen. Deze toestellen zijn zeer krachtig en bevatten een enorme hoeveelheid gegevens, maar kunnen makkelijk verloren raken. Daarbij kunnen andere mobiele media zoals USB sticks of CD ROMs ook gevoelige gegevens bevatten. Een veel voorkomende techniek om gegevens te encrypteren is Full Disk Encryptie (FDE). Hierdoor is alles op het systeem automatisch geëncrypteerd, je kan niet beslissen wat er wel of niet wordt geëncrypteerd. De meeste besturingssystemen bevatten Full Disk Encryptie, je hoeft het enkel in te schakelen. Bijvoorbeeld Mac OS X bevat FileVault en sommige Windows versies hebben Bitlocker. Als je computer Full Disk Encryptie ondersteunt, raden we ten zeerste aan om het in te schakelen. De meeste mobiele telefoons ondersteunen Full Disk Encryptie voor hun interne opslag. Bij iOS bijvoorbeeld, het besturingssysteem voor iPhones en iPads, past automatisch Full Disk Encryptie toe wanneer er een passcode is ingesteld. Om te weten of jouw computer of mobiel toestel Full Disk Encryptie ondersteunt, contacteer dan jouw helpdesk of jouw leidinggevende. Voor persoonlijke computers, contacteer jouw fabrikant of raadpleeg de online handleiding.

Encryptie is een krachtig middel om gegevens te beveiligen, maar enkel zo sterk als jouw sleutel.

Encryptie-in-verwerking

Gegevens zijn ook kwetsbaar als ze in verwerking zijn. Indien de gegevens niet zijn geëncrypteerd, kunnen ze mogelijk worden onderschept. Hierdoor wil je dat gevoelige online communicatie, als online bankieren, e-mails versturen en zelfs het raadplegen van sociale media, geëncrypteerd is. De meest gebruikte online encryptie is HTTPS. Dit betekent dat alle verkeer tussen jouw browser en een website geëncrypteerd is. Kijk naar de https:// in de URL, of het slotje in de browser of naar de adresbalk die groen wordt. Dit zijn allemaal tekens dat de communicatie geëncrypteerd is. Afhankelijk van jouw browser en de website, kan je ze mogelijk alle drie tegelijk zien. Als je verbinding maakt met openbare Wi-Fi netwerken, zorg er dan voor dat je encryptie gebruikt indien mogelijk. Ten slotte, als je e-mails ontvangt of verzendt, zorg er dan voor dat jouw e-mail programma dit doet over een geëncrypteerd kanaal. De meeste e-mail programma's voorzien standaard encryptie, daarnaast kan jouw ISP mogelijk helpen met encryptie in te schakelen op jouw e-mail programma.

Encryptie

Encryptie correct implementeren

Ongeacht het type encryptie dat je gebruikt, voor ieder type gelden deze regels om het correct te gebruiken.

- De encryptie is zo sterk als jouw sleutel. Indien iemand jouw sleutel heeft of raadt, dan heeft men toegang tot jouw gegevens. Bescherm dus jouw sleutel.
- Indien je een passcode of een wachtwoord gebruikt voor jouw sleutel, zorg dan dat het een lang en veilig wachtwoord is. Verlies of vergeet het zeker niet, anders heb je geen toegang meer tot jouw gegevens.
- De encryptie is maar zo sterk als de beveiliging van jouw computer. Indien jouw computer is aangetast of geïnfecteerd raakt, kan de encryptie door cyber criminelen worden omzeild. Zorg er dus voor dat jouw computer of mobiel toestel beveiligd is.
- Indien je meerdere opties hebt voor encryptie, kies dan altijd voor de sterkste methode.

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.

Nederlandse Editie

Cegeka is een full-service ICT-bedrijf: u kan bij ons terecht voor advies, detachering, softwareontwikkeling, bouw van websites, on-site en remote beheer van ICT-infrastructuur en outsourcing. Voor meer informatie: http://www.cegeka.com of volg ons op Twitter via @cegeka.

Extra informatie

Mac OS X FileVault:	http://support.apple.com/kb/ht4790
iOS Encryption:	http://support.apple.com/kb/ht4175
Android Encryption:	http://www.androidauthority.com/how-to-encrypt-android-device-326700/
Windows Encryption:	http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7
Securing Your Computer:	http://www.securingthehuman.org/ouch/2012#december2012
Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013

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