Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

- **Mitä on kryptaus?**
- **Mitä voit kryptata?**
- **Kryptaa oikein**

Kryptaus

Mitä on kryptaus?

Olet saattanut kuulla ihmisten puhuvat ”kryptauksesta” tai tiedon salaamisesta ja siitä miten sen avulla voi suojata itseään ja tietojansa. Kryptaus on kuitenkin monimutkainen käsite ja sisältää joitakin rajoitteita. Tässä uutiskirjeessä kerromme yksinkertaisin termein mitä kryptaaminen on, miten se voi suojata sinua ja miten käyttää sitä oikein.

Vierastoimittaja

Francesca Bosco (**@francibosco**) toimii tutkijana ja projektivastaavana YK:n kansainvälisen rikollisuuden ja oikeuden tutkimuslaitoksella (United Nations Interregional Crime and Justice Research Institute). Työssään hän johtaa kyberturvallisuuteen, kyberrikollisuuteen ja tiedon väärinkäyttöön liittyviä projekteja. Hän on myös ollut mukana perustamassa Tech and Laa Center-nimistä yritystä.

Sinulla on valtavat määrät luottamuksellista tietoa laitteissasi, esim. henkilökohtaisia dokumentteja, kuvia ja sähköposteja. Jos joku laitteistasi häviäisi tai varastettaisiin, laitteen löytäjä pääsisi helposti käsiksi kaikkiin näihin tietoihin. Lisäksi saatat käyttää esim. verkkopankkia tai muita vastaavia palveluita joissa siirretään luottamuksellista tietoa. Jos joku kaappaisi verkkoliikenteesi, he voisivat varastaa kaiken tämän tiedon, sisältäen pankkitietosi tai luottokortin numeron. Kryptaaminen suojelee sinua tällaisissa tapaukissa suojaamalla tietosi niin, että kukaan valtuuttamaton ei pääse käsiksi tietoihisi tai muuttamaan niitä.

Erilaisia kryptaus- tai salakirjoitustapoja on ollut käytössä jo tuhansia vuosia sitten. Nykyisin kryptaus on totta kai huomattavasti kehittyneempää, mutta tarkoitus on edelleen sama – välittää luottamuksellinen tieto yhdestä paikasta toiseen niin, että vain ne joilla on siihen oikeus näkevät kyseisen tiedon. Kun tieto ei ole kryptattu, sitä kutsutaan selkokieliseksi ja tämä tarkoittaa että kuka tahansa pystyy näkemään tai lukemaan sen. Kryptaus muuttaa tämän tiedon ei-luettavaan, salattuun muotoon. Modernit kryptaustekniikat käyttävät monimutkaisia matemaattisia laskelmia ja ainutlaatuisia kryptausavaimia tiedon kryptaamiseksi. Tieto avataan tai siihen päästään käsiksi nimenomaan kryptausavaimen avulla ja useimmissa tapauksissa kryptausavaimenasi toimii salasanasi.

Mitä voit kryptata?

Käytännössä voidaan kryptata kahdenlaista tietoa, paikallaan olevaa (esim. mobiililaitteessasi olevat valokuvat) ja liikkeessä olevaa (esim. sähköpostin tai pikaviestin vastaanotto).

Kryptaus

Paikallaan olevan tiedon kryptaaminen on oleellinen osa tietojesi suojaamista jos laitteesi katoaa tai varastetaan. Monissa tämän päivän laitteissa on äärimmäisen paljon tietoa, mutta ne on myös helppo kadottaa. Lisäksi monet ulkoiset muistilaitteet saattavat sisältää paljon luottamuksellista tietoa. Koko levyn kryptaus (FDE, Full Disk Encryption) on yleisimmin käytetty kryptaustapa, jossa kryptataan koko muistilaitteen, esim. kovalevyn sisältö. Tämä tarkoittaa, että kaikki laitteesi tieto on kryptattu automaattisesti ja käyttäjän ei tarvitse miettiä asiaa tai päättää mitä ja miten kryptataan. Monet modernit it-laitteet toimitetaan jonkinlaisen FDE-ratkaisun kanssa, mutta sinun pitää todennäköisesti kytkeä se itse päälle. Apple-koneissa FDE on nimeltään FileVault ja Windows-koneissa versiosta riippuen Bitlocker tai ”Device Encryption”. Monet mobiililaitteet tukevat myös FDE:tä, iOS-käyttöjärjestelmä iPhone:ssa ja iPad:ssä kytkee FDE:n päälle automaattisesti kun pääsykoodi on asetettu. Android laitteissa on versiosta 6.0 (Marshmallow) eteenpäin FDE vaaditaan päälle oletuksena jos laitteen rautaominaisuudet täyttävät Google:n vaatimukset.

Kryptaus on vahva tapa suojata tietosi, mutta kryptaus on vain niin vahva kuin kryptausavaimesi.

Tieto on vaarassa myös liikkeen aikana. Jos tietoa ei ole kryptattu, sitä voidaan monitoroida ja kaapata verkossa. Tämän vuoksi sinun kannattaa varmistaa, että tieto on verkossa kryptattu kun liikutat arkaluontoista tietoa. Yleisin tapa kryptata verkossa on HTTPS. Tämä tarkoittaa, että kaikki liikenne selaimesi ja internet-sivun välillä on kryptattu. Tarkkaile verkkosivun osoitetta, jos osoite alkaa https://, osoitteen edessä on lukon kuva tai osoitepalkki on vihreä, niin liikenne on todennäköisesti kryptattua. Toinen esimerkki liittyy sähköpostiin, monet sähköpostin tarjoajat tarjoavat kryptausmahdollisuuksia jotka sinun pitää itse aktivoida. Kolmas esimerkki liittyy viestintäpalveluihin, jossa kaksi henkilöä keskustelee keskenään. Palvelussa kuten iMessage, Wickr, Signal, WhatsApp tai Telegram liikenne on oletuksena kryptattu. Nämä sovellukset käyttävät ”päästä-päähän kryptausta”, jossa koko liikenne keskustelijoiden välillä on kryptattu niin, että kukaan muu ei sitä pysty lukemaan.

Kryptaa oikein

Varmista että suojaat tietosi kryptaamalla ja että teet sen oikein:

Kryptaus

- Kryptauksesi on yhtä vahva kuin kryptausavaimesi. Jos joku pystyy arvaamaan sen tai saa sen muuten käsiinsä, he pääsevät käsiksi kaikkeen tietoosi. Jos avaimenasi toimii salasanasi (esim. iOS), varmista että salasana on ainutlaatuinen ja laadukas. Mitä pidempi salasana, sen vaikeampi on jonkun sitä arvata tai murtaa. Älä unohda itse omaa salasanaasi, ilman avaintasi et pääse tietoihisi käsiksi itsekään. Jos sinulla on haasteita muistaa ja hallita salasanojasi, suosittelemme salasananhallintasovelluksen käyttöä.
- Kryptauksesi on yhtä vahvaa kuin laitteidesi tietoturva. Jos laitteesi on infektoitunut esim. haittaohjelmalla, rikolliset saattavat pystyä ohittamaan kryptauksesi. Tämän vuoksi käytä aina antivirus sovellusta, vahvoja salasanoja ja päivitä laitteesi aina kun mahdollista.
- Monet mobiili- ja tietokonesovellukset tarjoavat nykyisin vahvaa kryptausta tietojesi suojaamiseksi. Jos käyttämäsi sovellus ei tue kryptausta, suosittelemme harkitsemaan vaihtoehtoiseen sovellukseen vaihtamista.

LUE LISÄÄ

Liity kuukausittaisen OUCH! tietoturvatietoisuus-uutiskirjeen postituslistalle, lue OUCH! arkistoja ja tutustu SANS-järjestön muihin tietoturvatietoisuuteen liittyviin ratkaisuihin osoitteessa securingthehuman.sans.org/ouch/archives.

Uutiskirjeen kääntäjä Kirill Filatov (KTM) on GIAC-sertifioitu tietoturvaa rakastava IT-johtaja. Kirill turvaa tällä hetkellä Elisa Appelsiinin liiketoimintaa vastaamalla niin yrityksen omasta kuin asiakkaiden tietoturvasta.

Lähteet

Kryptaus selitettynä:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
Salasanalausekkeet:	https://securingthehuman.sans.org/ouch/2015#april2015
Salasananhallintasovellukset:	https://securingthehuman.sans.org/ouch/2015#october2015
Mitä ovat haittaohjelmat:	https://securingthehuman.sans.org/ouch/2016#march2016
Uuden tablettisi suojaaminen:	https://securingthehuman.sans.org/ouch/2016#january2016

Lisenssi

 Toimitus: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Käännös suomeksi: Kirill Filatov, CISO, Elisa Appelsiini Oy