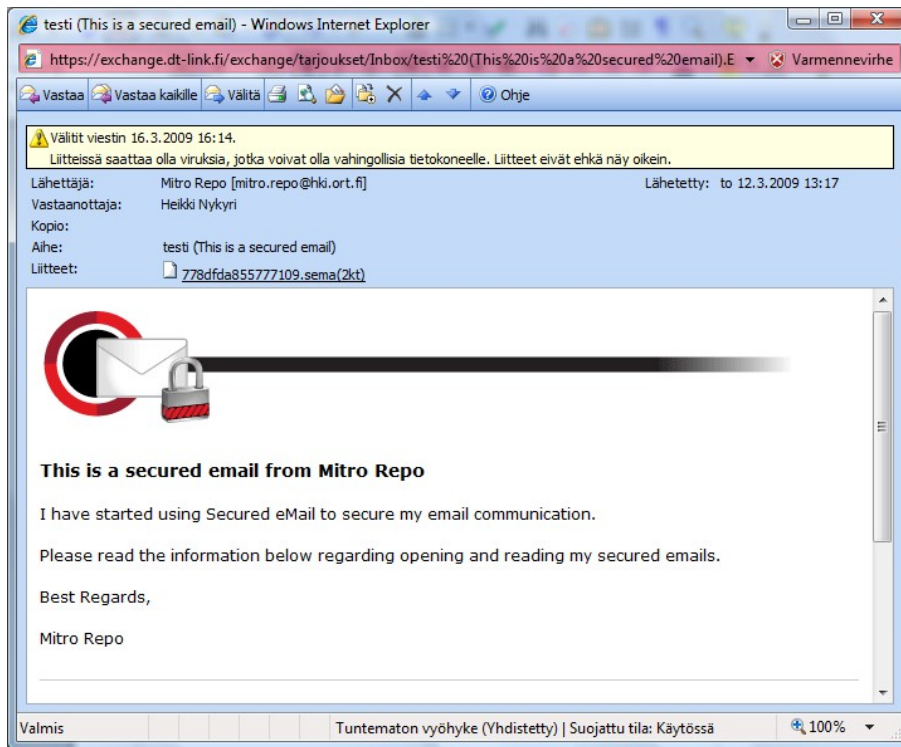


Päivän sana: salausta

Teksti: Ida Hakola



Tietoturvaan ja yksityisyydensuojan vaikut-tavat sähköiset sovellukset ovat tällä erää ajankohtaisia puheen-aiheita niin Suomessa kuin ulkomaillakin.

Tietosuojavaivaan on keksitty myös tehokas lääke. Salaustekniikan avulla kaikki muistitikuilla, tietokoneilla ja sähköposteissa piilevä tieto voidaan turvata salasanan taakse.

Tapahtui Englannissa: Verohallinnolle työskentelevä mies menee käymään pubissa työpäivän jälkeen. Taskuun on jäänyt muistitikku, joka sisältää verohallinnon verkkopalvelua käyttävien ihmisten salasanoja sekä palvelun lähdekoodi. Tikku häviää illan aikana ja massiivinen tietokanta pitää sulkea välittömästi. Kulut ovat suuret: 12 miljoonan ihmisen käyttämä tietokanta pitää luoda uudestaan ja salasana täytyy luoda toiseen kertaan.

Vastaavia suuria tietoturvahinkoja tapahtuu jatkuvasti ympäri maailmaa, sillä erilaiset mobiiliratkaisut, puhelimitse käytettävä sähköposti, taskussa kulkeva muistitikku ja

kannettava tietokone katoavat helposti haltijaltaan. Riskitekijöitä on monta ja muun muassa kadonneet henkilötiedot väärin ihmisten käsissä voivat tuottaa kinkkisiä tilanteita.

Tietoturvalle on nyt enemmän tarvetta kuin koskaan.

Yleisimmät salaustekniikat: sähköposti, muistitikku, kiintolevy

Salaustekniikka perustuu salauskoodiin, joka asetetaan joko muistitikulle tai esimerkiksi kovalevyille talletetun tiedon päälle. Salaustoimenpiteen jälkeen tietoon pääsee käsiksi ainoastaan salasanan turvin.

”Yleisimmän salaustoimenpiteitä teh-dään sähköposteille, USB-tikuille sekä kiintolevyille. Yhdellä tuotteella salataan yksi osa-alue”, **Toni Mäkinen** Getaware oy:stä selvittää.

Erityisen tärkeää salatun tiedon turvaaminen on yrityksille, jotka käsittelevät luottamuksellista tietoa. Usein salainen tieto kulkee tiedostamattakin sangen julkisissa ympäristöissä.

”Nykyään käytössä on paljon kannettavia tietokoneita, joita

liikutellaan ja unohdetaan paikasta toiseen”, Mäkinen muistuttaa.

Viime vuosina myös yritykset itse ovat heränneet salaustuotteiden tarpeellisuuteen.

”Cryptzone alkoi kehittää USB-tikun salausta nimenomaan asiakkaan pyynnöstä. Muistitikut ovat nykyään yleisiä tiedonsäilytyskohteita ja ne katoavat helposti”, Mäkinen toteaa.

Miten salausta toimii?

Salaustuotteet eroavat hieman toisistaan. Perusidea on kuitenkin sama: kunkin osa-alueen (kiintolevyille, kansiolle, sähköpostille, yms.) salaukselle määritetään oma salasana, joka mahdollistaa tietojen käytön. Malliesimerkkeinä mainittakoon sähköpostin ja USB-tikun salausta.

Muistitikun salauksen yhteydessä USB-tikku laitetaan koneeseen sisään, jonka jälkeen sille pyydetään luomaan salasana. Valitulla salasanalla pääsee käsiksi tikkuun missä tahansa Windows-koneessa. Ilman salasanaa ei tietoihin pääse käsiksi.

Sähköposti salataan aktivoimalla omaan sähköpostilokeroon ilmaantuva viesti. Posti salataan ennen lähettämistä ja puretaan vastaanottajan koneella, eli posti kulkee koneelta toiselle salattuna.

Tämän jälkeen viestin vastaanottaja aukaisee viestejä lähettäjän kanssa yhteisesti sovitun salasanan avulla. Viestien aukaisuun tulee hakea netistä Windows-pohjainen ilmainen reader-ohjelma.

Sähköpostin, muistitikun ja kiintolevyn lisäksi salaustuotteita on kehitetty yksittäisille tiedostoille ja kansioille sekä koneeseen liitettäville ulkoisille medioille.

Yhteydenotto:

DTLink
DATA- JA TELEALAN PALVELUT

<http://www.dt-link.fi>