Centria SecuLab esittää – tietoturvapodcast, osa 8 – Hyviä käytänteitä

Voihan juukeli!
Taas päivitys … meidän piti katsoa elokuva.
Vaihtoehdot tais olla saapasjalkakissa, prinsessan päiväkirja, tai Risto Räppääjä…
No voi! Se vaan työntää tuota päivitysruutua koko ajan.
Voidaankohan nyt valita elokuva, vai pitääkö se päivitys tehdä ensin?

On erittäin tärkeää pitää järjestelmien ja laitteiden päivitykset ajan tasalla. Suuri osa ohjelmistopäivityksistä sisältää haavoittuvuuksien korjauksia, joiden avulla korjataan turvallisuuspuutteita. Päivitykset on syytä asentaa mahdollisimman nopeasti niiden julkaisemisen jälkeen. Ohjelmistopäivitykset ovat saatavilla sovelluskaupasta, palveluntarjoajan sivuilta tai automaattisen päivityksen kautta – josta tietokoneesi ilmoittaa. Päivittämättömillä järjestelmillä on aina suurempi riski joutua tietomurron kohteeksi, koska rikolliset hyödyntävät vanhentuneissa ohjelmistoissa olevia turvallisuuspuutteita. Pitämällä päivitykset kunnossa pidät siis myös rikolliset loitolla.

Esimerkiksi käyttöjärjestelmä on tärkeä ohjelmisto tietokoneessasi. Se hallitsee tietokoneesi laitteistoa ja kaikkia sen ohjelmia. Siksi se on tärkeä päivittää ja pitää ajan tasalla.

Useimmat ohjelmat tarjoavat automaattisia päivityksiä, jolloin sinun ei tarvitse etsiä uusinta päivitystä ja tietää milloin sellainen on saatavilla. Samalla voit olla varma, että käyttämäsi ohjelmistot ovat ajantasaisia eivätkä päivitykset unohdu. Yleensä automaattinen päivitys otetaan käyttöön ohjelman asetuksista.

Varmuuskopio on digitaalinen kopio yrityksesi toiminnalle keskeisistä tiedoista ja palveluista, kuten asiakastiedoista. Tee tärkeimmistä tiedoista sekä palveluista varmuuskopiot. Säilytä varmuuskopiot esimerkiksi verkosta irti olevalla kiintolevyllä, jottei kiristyshaittaohjelma tee myös varmuuskopioista käyttökelvottomia. Tärkeiden tietojesi varmuuskopio voi myös olla pilvipalvelussa. Tarkista säännöllisesti – kuten esimerkiksi neljännesvuosittain – että varmuuskopioiden palauttaminen onnistuu, ja että tarvittavat tiedot on varmuuskopioitu.

Monivaiheinen tunnistautuminen on vahva turvallisuustoimenpide. Se tarkoittaa, että henkilön identiteetti varmistetaan useampaa eri tunnistautumistapaa käyttämällä. Tämä perustuu kolmelle ominaisuudelle, jotka ovat:

1. Jotain mitä tiedät (kuten esimerkiksi salasana),
2. Jotakin mitä omistat (kuten esimerkiksi puhelimeen lähetettävä muuttuva koodi), ja
3. Jotakin mitä olet (kuten esimerkiksi sormenjälki tai muu käyttäjän yksilöivä ominaisuus).

Kannattaa myös kysyä; kenellä on oikeus päästä yrityksen käyttämissä järjestelmissä olevaan tietoon. Käyttöoikeuksien antaminen erilaisille käyttäjäryhmille on tapa rajoittaa tiedon saamista sellaisilta henkilöiltä, joilla ei ole tarvetta saada kyseistä tietoa.

Päätä kuka tarvitsee mitäkin tietoa ja kenelle pääsyoikeus halutaan myöntää. Mikäli yrityksessä on useampi työntekijä, määrittele tällöin eritasoisia käyttöoikeuksia järjestelmiin ja niissä oleviin tietoihin – ja muista myös valvoa käytänteiden toteutumista.

Ota myös salalause käyttöön. Salalausetta käytetään salasanan tavoin erilaisiin palveluihin ja järjestelmiin, mutta se on pidempi. Turvallisuus parantuu yksinkertaisesti käyttämällä salalausetta ja se on erityisen tehokas, kun sitä käytetään yhdessä monivaiheisen tunnistautumisen kanssa. Salalause:

- on vaikeampi murtaa kuin tavallinen salasana, mutta se
- on helpompi muistaa kuin salasana, jossa on käytetty satunnaisesti erilaisia merkkejä, ja se

- täyttää erilaiset salasanavaatimukset vaivattomasti.

Kiire on suurin tietoturvauhkien aiheuttaja. Kiire lisää merkittävästi eri riskitekijöitä, ja huonontaa harkintakykyä. Stressi kuormittaa vuorostaan kehoa ja mieltä, sekä heikentää tietoturvaa. Ota siis rauhallisesti! Monet asiat ratkeavat, kun muistat maltin.

No hei! Antaa sen päivittää, teen samalla popparit, ja sitä paitsi saadaan miettimisaikaa mikä filmi katsotaan!