Kyberturvallisuus – miten se koskee meitä kaikkia?

17.6.2022

Osallistuin Münchenin kyberturvallisuuskonferenssiin huhtikuussa. Konferenssissa käsiteltiin esillä olevia kyberuhkia. Digitalisaatio nähdään monella toimialalla tärkeänä kehittymisen tapana. Haasteena digitalisaatioon liittyvässä kehitystyössä on turvallisten järjestelmien kehittäminen. Kyberturvan asiantuntijoista on pulaa. Tähän on tarvetta vastata kouluttamalla uusia osaajia. Tämä haaste sopii TAMKille erittäin hyvin.

Digitaalisen infrastruktuurin suojaaminen

Luottamus tietojärjestelmiin ja digitaaliseen infraan horjuu, mikäli kyberturvallisuus heikentyy ja erilaiset hyökkäykset järjestelmiä kohtaan saavat aikaan häiriöitä, toiminnan katkoksia tai tietojen katoamisia. Nopeasti etenevä digitalisaatio tuo mukanaan riskejä ja haavoittuvuuksia. Voimassa olevat turvallisuusratkaisut vanhenevat eivätkä pysy kehityksen vauhdissa.

Koronaepidemian aikana perinteinen rikollisuus, kuten varkaudet ja murrot vähenivät. Samanaikaisesti kyberrikollisuus on lisääntynyt. Laajasti käyttöönotetut etätyöratkaisut heikoilla tietoturvaratkaisuilla ovat mahdollistaneet kyberrikollisten hyökkäyksiä.

Useimpien yritysten arvo on niiden järjestelmiin tallennetussa tiedossa omista tuotteistaan, palveluistaan ja asiakkaistaan. Näiden vuotaminen tai tuhoutuminen kyberturvallisuuden pettäessä vaarantaa yrityksen toiminnan jatkuvuuden. Esimerkkejä tästä löytyy Suomestakin.

Tietojärjestelmiin tulisi kehittää resilienssiä pelkän uhkiin reagoinnin sijaan. Security by Design – ajattelu sovelluksien ja tuotteiden kehittämisessä on tarpeen. Suunnitellaan lähtökohtaisesti järjestelmiä, jotka ovat turvallisia.

Myös Zero Trust – periaatetta on syytä käyttää, jolloin laitteet ja käyttäjät tunnistetaan joka tilanteessa sekä käytetään vahvaa tunnistautumista. Tietoturvariskit pitää tunnistaa, arvioida ja välttää mahdollisimman hyvin. TAMKissa keväällä käyttöön otettu Microsoft Intune edustaa tätä suojaustapaa.

Datan suojaamisen merkitys lisääntynyt

Nykyaikainen tietotekniikka ja mobiililaitteiden käyttö mahdollistaa laajamittaisen tietojen keräämisen. Laitteissa voi olla sovelluksia, jotka keräävät tietoja käyttäjän toiminnasta tämän tietämättä tai luvalla.

Alun perin tietojen keräämisen tarkoituksena on ollut käyttää sitä markkinointiin sovelluksen käyttäjille. Käyttäjien profiloinnin perusteella heille voidaan suunnata mieltymyksiä vastaavia mainoksia.

Kyberturvallisuuden kannalta käyttäjien ja heidän verkostonsa kannalta ongelmaksi muodostuu se, että tietoja on mahdollista käyttää väärin, mikäli tiedot vuotavat kerääjän ulkopuolelle vääriin käsiin.

Yleisesti käytettyjen sovellusten kuten Googlen ja Facebookin käyttäjien tiedot kulkeutuvat EU:n ulkopuolella oleviin servereihin, jolloin niiden käsittely ei ole Suomen tai EU:n lain hallinnassa.

Verkkorikollisuuteen varautuminen

Yleisin verkkorikollisuuden muoto on tietojen kalastelu. Tähän liittyviä viestejä tulee sähköpostilla, tekstiviesteinä, netissä tai puhelimella. Rikolliset kalastelevat sähköposti- ja verkkopankkitunnuksiasi, luottokorttitietojasi tai rahojasi useilla eri tavoilla.

Rikollinen voi kiristää ja uhkailla verkkopalvelun palvelunestohyökkäyksellä tai tietomurrolla. Saatat törmätä väärennettyyn verkkokauppaan, jossa on houkuttelevia tarjouksia.

Voit saada sähköpostiviestin, jonka liitteenä on ”lasku”, mutta se sisältää haittaohjelman. Sähköpostin lähettäjän osoite voi myös olla väärennetty.

Älä syötä luottokorttitietojasi tai verkkopankkitunnuksiasi epäilyttävän oloiselle sivustolle. Huijaussivustot on tehty muistuttamaan oikean yrityksen, vaikka pankin sivustoja. Virheellinen osoite ja muut yksityiskohdat paljastavat huijauksen. Osoite on parasta kirjoittaa suoraan selaimen osoiteriville linkin klikkaamisen sijaan.

Verkkopankit käyttävät salattua yhteyttä, jonka voi tarkistaa osoiterivin lukkoikonista ja https://-alkuisesta verkko-osoitteesta. Jos lukkoikoni puuttuu, niin kyseessä ei ole oikea verkkopankki.

Vaihda murrettu salasanasi välittömästi ja käytä jokaisessa käyttämässäsi palvelussa omaa salasanaa.

Kyberturvallisuuden kehittäminen EU:ssa

EU:ssa kyberturvallisuuden kehittämisen haetaan ratkaisua valmistelemalla Kyberresilienssisäädöstä – Cyber resilience act. Säädöksellä on tarkoitus kehittää uudet kyberturvallisuussäännöt digitaalisille tuotteille ja oheispalveluille.

Yhteiskunnan kriittinen infrastruktuuri tulee suojata kyberuhkilta. Näihin haasteisiin TAMKilla on mahdollista vastata TKI-hankkeilla.

Kirjoittaja Petri Murtomäki toimii Tampereen ammattikorkeakoulun ulkoisen rahoituksen yksikössä ja on mukana Pirkanmaan turvallisuusklusterin toiminnassa.