Tietoturvatoiminta kampuksilla

Samuli Komokallio
Tietotekniikkaosasto

Tietotekniikkaosastolla on jokaisella kampuksella tietoturvakoordinaattori. Hänen päätehtävinään on suunnitella ja kehittää tietoturvallisuutta kampuksella sekä toimia yksiköiden tukena tietoturvatyössä. Tukea jaetaan muun muassa kouluttamalla, ohjeistamalla ja antamalla ongelmatilanteissa teknistä konsultointiapua. Laitosten atk-henkilöstön kanssa toimitaan vuorovaikutuksessa ja palveluita kehitetään yksiköiltä saadun palautteen mukaan.

Tietoturvallisuuden suunnittelu ja kehittäminen kampuksilla käynnistyi reilu vuosi sitten kullakin niistä toteutetulla tietoturvakartoituksella. Tietoturvakoordinaattorit kävivät läpi valtaosan yksiköistä ja arvioivat niiden tietoturvan tason. Tämän tuloksena suunniteltiin kehittämistarpeet. Ensimmäisen kartoituksen perusteella arvioitiin yleistä tietoturvallisuuden hallinnointitapaa ja yksiköiden resursseja tietoturvatyöhön. Myös toiveita tietoturvakoordinoinnin kehittämiseksi kyseltiin.

Koulutusta ja ohjeistusta

Tietoturvallisuuden edistäminen on järkevintä aloittaa henkilöstöstä. Kampuksilla tietoteknisen turvallisuuden kehittäminen on luonnollisinta aloittaa kouluttamalla ja sitouttamalla atk-henkilöstöä. Jo sisäistämällä tietoturvan perustaidot ylläpito sujuu huomattavasti turvallisemmin ja häiriötilanteita voidaan vähentää. Resurssien puutteilla usein selitettävää tietoturvallisuuden laiminlyöntiä pyritään vähentämään erilaisin koulutustilaisuuksin. Tietoturvallisen ympäristön ideahan on häiriötön käyttö, jolloin tukipyyntöjen määräkin on vähäisempi.

Henkilöstöä koulutetaan mm. atk-tukihenkilön peruskursseilla, jonne ovat lämpimästi tervetulleita myös vanhat työntekijät. Tänä syksynä aloitetaan myös kampuksilla järjestettävät tietoturvailtapäivät, joissa osaamista syvennetään tietyn, vaihtuvan teeman mukaan. Tilaisuuksien on tarkoitus olla vuorovaikutteisia tapahtumia, joissa ylläpitäjät voivat vaihtaa arvokkaita kokemuksia myös keskenään.

Tietoturvakoordinointiin kuuluu kouluttamisen lisäksi myös ohjeistuksen parantaminen, sekä tietoturvaan liittyvä tiedottaminen. Näitä pyritään kehittämään ohjaamalla tietoa eteenpäin. Yksiköiltä saatua palautetta välitetään esimerkiksi tietotekniikkaosastolla palveluiden vastuuhenkilölle. Luonnollisesti tietotekniikkaosaston uutisista kerrotaan vastavuoroisesti yksiköille. Tietoturvakoordinaattorit tekevät toki myös testaustyötä. Sen perusteella laaditaan ohjeita ja suosituksia.

Uusia tietoturvapalveluita

Tietoturvallisuuden kehittämiseen kampuksilla liittyy kiinteästi uusien palveluiden suunnittelu. Usein kuitenkaan yksittäisellä laitoksella ei pienen kokonsa tai ylläpitäjien vähäisyyden vuoksi ole mahdollisuutta toteuttaa järkevästi tarvitsemaansa tietoturvatuotteiden hallinnointia. Tällaisissa tapauksissa tietotekniikkaosaston kautta tehty keskitetty hankinta ja hallinnointi ovat tärkeä apu. Keskitetty toiminta auttaa myös vähemmän tietoturvaorientoituneita tai -resursoituja yksiköitä. Tietoturvatuotteiden käytön leviäminen parantaa useimmissa tapauksissa yhteisesti kaikkien tietoturvaa. Yliopistollakin tietoturva on yhtä vahva kuin sen heikoin lenkki.

Esimerkkinä uudesta kaivatusta palvelusta ovat tietoturvakoordinaattoreiden tekemät järjestelmien haavoittuvuustarkastukset. Näissä haavoittuvat koneet etsitään yliopiston laajasta ja heterogeenisestä verkosta jo ennen kuin ne joutuvat verkkomatojen tai krakkereiden kohteiksi. Usein verkossa tapahtuvat häiriötilanteet syntyvät vähemmälle huolenpidolle jätetyistä koneista,

joissa on murrettavia aukkoja. Erilaiset madot ja krakkerityökalut löytävät nämä aukot automaattisesti ja nopeasti. Tähän tehokas vastalääke on itse tutkia aktiivisesti verkon palveluita ja korjata mahdolliset ongelmakohdat jo ennen murtautujia. Tarkastukset tehdään tällä hetkellä vielä ylläpitäjien pyynnöstä, mutta lähitulevaisuudessa palvelu on tarkoitus määritellä automaattiseksi.

Konsultointia ja valvontaa

Yksiköt voivat pyytää kampuksen tietoturvakoordinaattorilta myös apua hankkeisiinsa. Esimerkiksi moniin ohjelmistohankintoihin olisi järkevää jo tarjouspyynnössä määritellä tietoturvavaatimuksia. Tietenkin myös jo valmiiden ympäristöjen tietoturvallisuuden kehittämiseen voi pyytää apua. Tietoturvakoordinaattori voi arvioida ympäristön turvallisuuden ja opastaa sen parantamisessa. Hankkeen tai ympäristön koolla ei ole väliä, koordinaattorit avustavat mielellään vaikka yksittäisen palvelimen turva-asetuksissa.

Tietoturvakoordinaattorin tehtäviin kuuluu myös tietoturvallisuuden valvonta ja poikkeustilanteisiin reagoiminen kampustasolla. Valvontatyöhön koordinaattorit toivovat myös ylläpitäjiä aktiivisemmin mukaan. Varsinkin useimmista häiriö- ja ongelmatilanteista ilmoittaminen on ensin tapahduttava ylläpitäjien toimesta. Itsenäisesti yksiköissä hallituista atk-järjestelmistä eivät tietoturvakoordinaattorit saa tietoa kuin laitoksien oman atk-henkilöstön kautta. Huomionarvoista on se, että yksikön häiriö on harvoin ainoa tapaus ja välittömällä tiedottamisella voitaisiin ongelman leviämistä rajoittaa. Toki valvontaa suoritetaan myös tietoliikenneverkon kautta, mutta laajan verkon liikenteessä häiriöt näkyvät usein vasta, kun epidemia on jo syntynyt.

<BOX>

Tietoturvakartoitukset

* Haastateltiin noin 70 yksiköiden atk-tuki- tai yhdyshenkilöä
* Selvitettiin yksiköiden tietoturvatyön resursseja ja yleistä tietoturvatasoa
* Tietoturvataso ja resurssit vaihtelivat suuresti yksiköiden välillä
* Tietojärjestelmien standardoiminen ja keskittäminen antaisi säästöjä ja lisäresursseja. Esim. Kumpulan kampuksella käytetään ainakin 16 erilaista käyttöjärjestelmää versioineen. Järjestelmäkantaa yhtenäistämällä ei tarvitsisi ylläpitää näin laajaa osaamista
* Tukihenkilöiden koulutukseen ja resursointiin olisi panostettava enemmän. Monissa yksikössä atk-tukena on osa-aikainen tutkija, jonka mielenkiinto ja osaaminen on tutkimuksessa, ei atk-tuessa
* Yksiköiden välinen kanssakäynti oli pientä, yhteistyöllä voitaisiin atk-tukea tehostaa
* Vanha laitekanta ja järjestelmät huomioitiin vakaviksi tietoturvauhkiksi. Käytössä on edelleen paljon jo täysin vanhentuneita ja turvattomia atk-järjestelmiä.

</BOX>