MONTAKO TIETOTURVAN KEHÄÄ SUOJELEE LIIKETOIMINTAASI?

TIETOTURVAOPAS

3/2018

BLC

BLC

OPPAASI TURVA- JA TIETOTEKNIIKASSA

SISÄLTÖ

TIETOTURVASSA ON MONTA SISÄKKÄISTÄ KEHÄÄ

Älykkäällä ja moniulotteisella tietoturvalla on koko ajan kasvava merkitys. Esimerkiksi erilaiset IoT-laitteet ovat hyvinkin haavoittuvaisia, koska niihin ei välttämättä saada lainkaan omaa suojausta tai edes päivityksiä. Tällöin uhat on torjuttava jo kauan ennen itse laitteita ja muun tietoturvan merkitys kokonaisturvallisuuden kannalta korostuu.

Myös pilvimaailman myllerrys vaikuttaa kokonaisturvallisuuteen. Virtuaalipalvelimiin ja pilvipalveluihin pätevät nimittäin ihan samat tietoturvan lainalaisuudet, kuin muuhunkin yrityksen ICT-infraan. On erityisen tärkeää tietää, kuka on vastuussa ja miten asiat on hoidettu, elleivät ne ole omissa käsissäsi.

Omissa käsissäkin on aika paljon tekemistä. Moderni tietoturva voi pitää sisällään lukemattomia eri työkaluja yrityksen tietoturvaan ja suojaamiseen. Mistä ylipäätään voi tietää, mitä tietoturvaa yrityksen pitäisi ottaa käyttöön?

Yksi hyödyllinen ajattelumalli on fyysisen maailman puolelta tuttu kehäsuojausperiaate. Tietoturvassa sen sisimpänä osana on päätelaite ja sitä käyttävä ihminen ja uloimpana on verkon tietoturva. Unohtamatta kaiken perustana olevaa fyysistä tilaa, joka myös liittyy tietoturvaan.

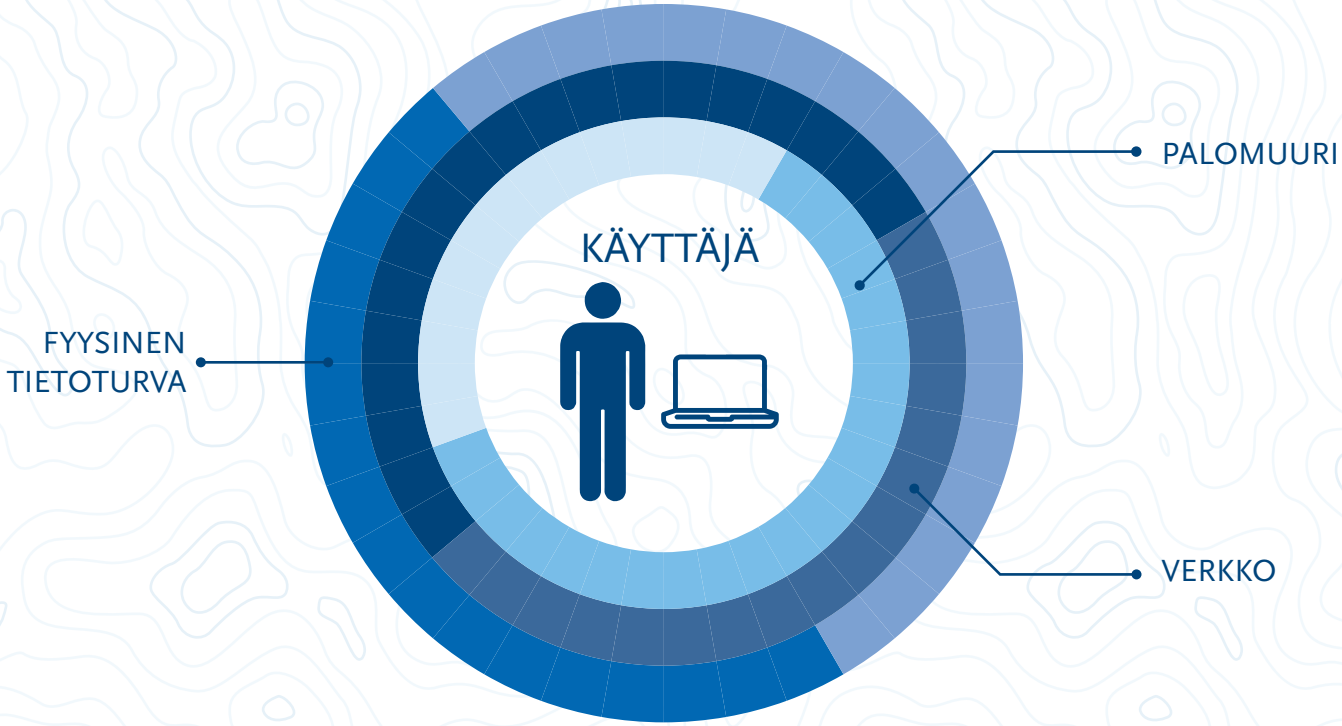
Mistä kehistä yrityksen tietoturvan kokonaisuus siis muodostuu?

Me opastamme aiheeseen

Tuomas Karhula

Jukka Nevalainen

SISIMPÄNÄ ON PÄÄTELAITE



Selkeintä on lähteä liikkeelle itse päätelaitteesta eli työasemasta, palvelimesta tai mobiililaitteesta. Fyysisen laitteen suojauksen perusta on toimiva virustorjunta ja palomuuri. Kun virustorjunnan suojaus on ajan tasalla, sillä pystytään havaitsemaan ja hallitsemaan päätelaitteelle asti päässeet haittaohjelmat. Palomuuri torjuu omalta osaltaan ulkopuolelta tulevaa uhkaa.

Näiden lisäksi merkittävä tekijä päätelaitteen tietoturvassa ovat ajantasaiset ohjelmistot. Yleensä käyttöjärjestelmien päivitykset ovat melko hyvin ajan tasalla, mutta varsinkin työasemissa erilaisia kolmannen osapuolen ohjelmistoja on todella runsaasti. Vanhenevissa ohjelmistoissa on usein haavoittuvuuksia, jotka tarjoavat mahdolliselle hyökkääjälle hyökkäyspintaa ja tietoturva-aukkoja.

Virustorjunnan ja palomuurin rinnalle tarvitaan siis toimiva sovellusten päivitysjärjestelmä. Näin turvataan päätelaitteet mahdollisimman monipuolisesti ulkopuolelta tulevilta hyökkäyksiltä.

Yrityksen tietoturvakokonaisuudessa päätelaitteiden suojaamista voi verrata kotiin, jossa jokainen kaappi on lukittu. Näin vaikka ovet jäisivät sepposen selälleen, on varkaalla melkoinen työ murtautua jokaiseen kaappiin yksitellen.

SISÄKEHÄLLÄ ON PALOMUURI

Sisäkehän palomuurilla estetään ja hallinnoidan ulkoverkosta sisäverkkoon saapuvaa liikennettä. Sisäverkko on pienimmillään se mokkula tai wifi-reititin, johon kaikki päätelaitteet kytkeytyvät. Suurimmillaan se on valtava yrityksen sisäinen verkko, joka kattaa satoja laitteita ja useita toimitiloja.

Tämän verkon ulkoreunalla on siis laite, jonka kautta liikenne kulkee ja tämän laitteen palomuuri hallinnoi, mitä sisäverkkoon saapuu. Verkkopäätelaitteen avulla hallinnoidaan myös, mitä sisäverkon palveluita tai portteja näytetään ulkoverkkoon. On nimittäin hyvä pitää mielessä, että kaikki mitä ulkoverkkoon näytetään, on myös alttiina hyökkäykselle. Siksi palomuurien konfigurointiin on syytä kiinnittää erityistä huomiota.

Uuden sukupolven laitteet osaavat myös itsessään jo tunnistaa hyökkäyksiä ja reagoida tietoverkossa tapahtuviin epämääräisyyksiin. Palomuurin älykkyydellä voidaan vaikuttaa paitsi itse sisäkehään, niin myös sisäkehän ja päätelaitteen väliseen suojaukseen.

Sisäkehän palomuuria voi verrata kodin lukitukseen ja ikkunaverhoihin. Kun palomuuri on kunnossa, ovet saa lukkoon ja asukas voi itse valita, minkä verran verhoja raottaa ohikulkijoiden silmille.

SISÄKEHÄN VOI RAKENTAA MYÖS ITSE

Aina ei olla kodin tai yrityksen seinien suojassa tekemässä töitä eikä päästä itse vaikuttamaan verkkopäätelaitteen palomuuriin ja tietoturvaan. Tällaisia tilanteita ovat esimerkiksi avoimet langattomat verkot, toimisto-hotellit ja muiden toimijoiden vierasverkot. Kannattaakin miettiä, haluaako rakentaa itselleen varmuuden vuoksi oman ylimääräisen tietoturvan kehän.

Kuljettamalla verkkoliikenteen oman väliaseman kautta, jossa on oma tietoturva, voi ainakin olla varma, että verkon palomuuri on kunnossa. Virtual Private Network -sovellukset (VPN) salaavat verkkoliikenteen sekä suojaavat salakuuntelulta ja vakoilulta, mutta ne eivät välttämättä toimi työaseman näkökulmasta palomuurina.

ULKOKEHÄLLÄ ON VERKON TIETOTURVA

Ulkokehällä pyritään torjumaan uhkia jo ennen kuin ne ovat yrityksen omissa järjestelmissä. Ulkokehä alkaa oman tietoverkon ulkopuolelta ja sitä on hyvin vaikea hallita, koska se on julkista internetiä. On silti tapoja aloittaa suojaaminen jo selkeästi aikaisemmin, kuin perinteisesti ajatellaan.

Näistä tutuin on ehkä sähköpostin virustorjunta. Sähköpostin virustorjunnalla ja tarkastuksilla voidaan estää sähköpostin haitakkeita pääsemästä päätelaitteille, eli sähköpostiohjelmistoihin tai -palvelimiin. Näin käyttäjä ei edes saa sellaisia liitetiedostoja klikattavaksi mitkä voisivat saastuttaa työaseman.

Ulkokehällä voidaan tehdä myös muuta torjuntaa. Kun käyttäjä klikkaa linkkiä, Domain Name Systemille (DNS) eli nimipalvelimille lähtevät kyselyt voidaan ohjata tietoturvalliseen järjestelmään, joka tekee kaikelle web-liikenteelle mainetarkastuksen. Tällöin käyttäjän klikkaama haitallinen sisältö voidaan estää jo ennen sen aukeamista.

Jopa osa ransomware-ohjelmistoista voidaan torjua tällä tavalla. Ne usein ”soittavat kotiin” heti tarttumisen jälkeen. Tuo soitto ohjautuu yrityksen DNS-kyselyn kautta ulkomaailmaan ja ajantasainen DNS-suojaus pystyy estämään varsinaisen ohjelmiston latautumisen itse järjestelmään.

Sähköpostin virustorjuntaa ja DNS-kyselyitä voi verrata oman piha-alueen tarkkailuun. Kuka tahansa voi liikkua kaduilla ja yrittää poiketa pihaan, mutta päästämällä ovesta sisään vain luotetut lähetit ja vieraat, ei pahantekijöitä sujahda sisälle taloon. Myös posteljoonilta voi kysäistä etukäteen, että minkäslaista kirjettä ja keneltä olet postilaatikkooni kuljettamassa.

PERUSTANA ON FYYSINEN TIETOTURVA

Hyvin usein tietoturvasta puhuttaessa jätetään fyysinen puoli vähemmälle, vaikka sen merkitys on todella suuri. Iso osa yrityksistä ei pysähdy miettimään, kuinka heidän yrityksensä tilat on suojattu ulkopuolisilta. Tietoturva alkaa karkeasti ottaen jo parkkipaikalta ja siihen liittyy kaikki fyysinen suojaus kameravalvonnasta kulunvalvontaan.

Verkon reunan palomuureista ei nimittäin ole hyötyä, jos tunkeutuja kävelee suoraan toimistolle ja laittaa koneensa kiinni yrityksen sisäverkkoon. Myös virustorjunnalla ja sovelluspalomuurilla suojellun palvelimen tietoturva huononee merkittävästi, jos se kannetaan yöllä pois toimistolta tai konesalista.

Usein helpoin tapa tunkeutua toimistolle on tehdä se päivällä DHL:n lippis päässä. Kuka on viimeksi tarkastanut kuriirilta, onko tällä oikeutta tulla toimistolle? Moniko on avannut oven, jos hän on kantanut suurta pakettia?

> Erilaiset viranomaismääräykset ja ohjeistukset (kuten VAHTI ja KATAKRI) ottavat kantaa myös fyysiseen turvallisuuteen ja prosesseihin. Tietoturvamielessä näitä on hyvä käyttää viitekehyksinä tavallisessa yritystoiminnassakin.

KESKIÖSSÄ ON LOPULTA IHMINEN

Jos tietoturvaa halutaan viedä vielä pidemmälle, ja aina pitäisi haluta, aletaan kehittää myös organisaation omaa tietoturvaa. Hyvin usein tietoturvan heikoin lenkki on itse ihminen. Lukko ovessa ei auta, jos ihminen tunkkaa oven auki. Eikä palomuuri auta, jos käyttäjä klikkaa itse epämääräistä vilkkuvaa banneria. Ja jos kaikista muureista ja suojauksista huolimatta toimitusjohtajan nimissä saapuu huijauskirje, joka pyytää talousjohtajaa siirtämään sata tonnia tietylle tilille, nojaamme ihmisen neuvokkuuteen huomata tämä huijaus ajoissa.

Aikojen muuttuessa ja henkilöstön vaihtuessa ihmisten tietoturvatietoisuuden pitäminen riittävällä tasolla vaatii paljon. Puhutaan prosesseista ja dokumenteista. Siksi käyttäjiä tulisi kouluttaa säännöllisesti ja yrityksille tulisi luoda huolellista tietoturvapolitiikkaa sekä -ohjeistuksia.

> Koulutuksen lisäksi on tärkeää todentaa, miten tietoturva oikeasti toimii. Tietoturvan toimivuutta voidaan nykyään testata erilaisilla työkaluilla verkon eri osissa. Testaus voi olla joko moniulotteista, manuaalista penetraatiotestausta tai automatisoitu toiminta säännöllisesti toteutettuna prosessina oikeilla työkaluilla.

KUN KAIPAAT LISÄÄ OPASTUSTA

Miten IT-päällikkö pystyy ottamaan kantaa jokaiseen tietoturvan kehään ja sen lisäksi vielä prosesseihin ja fyysiseen turvallisuuteen? Valitsemalla avukseen oikeanlaisen kumppanin. BLC-konsernissa on vankan IT-taustan lisäksi myös syvällistä osaamista fyysisestä turvallisuudesta.

OTA YHTEYTTÄ

Tuomas Karhula

Tuotepäällikkö

BLC Taito Oy

+358 44 502 1214

tuomas.karhula@blc.fi

Jukka Nevalainen

Toimitusjohtaja

BLC Turva Oy

+358 40 067 5272

jukka.nevalainen@blc.fi

www.blc.fi

facebook.com/blckonserni
youtube.com/BLCgroup