TOS-TOJ -konsepti on suunniteltu viranomaistehtävien prosesseihin, käytännössä vireillepano – käsittely – päätös. Ehkä joitain elinkeinoelämän järjestöjä lukuun ottamatta vastaavanlaisia asiankäsittelyn prosesseja ei ole yritysmaailmassa.

Esimerkiksi yrityksissä melko yleinen Share Point soveltuu yritysten tapaan työskennellä. Yksi syy, miksi Elkassa otimme Share Pointin käyttöön, oli se, että käyttämällä Share Pointia saamme samalla kokemusta yritysten tavasta toimia ja siitä, kuinka sen kautta saataisiin tietoa Elkaan säilytykseen.

Dokumentinhallintajärjestelmiä on toki yrityksissä käytössä, mutta kuinka moni niistä, mukaan lukien Share Point, on saanut tiedonohjausjärjestelmän kylkeensä? Tuskinpa moni, varsinkin jos asiakirjallisen tiedon hallinta ei ylipäätään perustu mihinkään suunnitelmaan. Sitten on vielä näitä levynkulmia eli vanhan ajan henkilökohtaisia arkistoja, joiden tiedonohjaussuunnitelma on työaseman käyttäjän päässä.

## Reaktiivista ja proaktiivista tiedonhallintaa

Yritysten tiedonhallinta on arkistonäkökulmasta reaktiivista ja proaktiivista. Esimerkiksi taloushallinto tietää säilytysajat ja osaa tehdä vuosittain asiakirjojen tuhoamiset. Sitten on asiakirjaryhmiä, joista vuosien päästä ei edes tiedetä, mitä ne ovat ja mikä on niiden säilytysarvo. Näiden kohdalla joudutaan toimimaan reaktiivisesti.

Jos minkäänlaista tiedonohjaussuunnitelma tai vastaava ei ole olemassa, edellä kuvattu toteutunee myös yritysten digitaalisessa tiedon hallinnassa. Ammatillisessa mielessä tämä ei vastaa tavoitetilaamme. Siksi yrityksissä tiedonhallinnan tehtävät on hoidettava käytännönläheisesti – voisi sanoa konsulttiasenteella. Emme voi muuttaa toimintaympäristöä, mutta voimme parantaa sitä.

## Ammatillinen renessanssi

Lopuksi ryhdyn minäkin ennustajaksi. Uskon, että digitaalisessa toimintaympäristössä tiedon hallinnan merkitys kasvaa. On esimerkiksi varauduttava mahdollisiin tietoturvariskeihin. Tieto on myös yhä enemmän rahaa. Tietomassat ja niiden analysointi avaavat uusia mahdollisuuksia liiketoiminnalle, elleivät peräti ole koko liiketoiminnan perustana. Immateriaalioikeuksilla on rahallinen arvo siinä missä koneilla ja kiinteistöillä.

Paineita tiedon hallintaan tulee lainsäätäjänkin taholta. Hyvä esimerkki tästä on EU:n tietotuoja-asetus, jonka säädösten rikkomisesta voi saada tuntuvat sakot. Tieto on siis monestakin syystä huomattavasti arvokkaampaa kuin aikaisemmin. Siksi tiedonhallintaan joudutaan kiinnittämään huomiota entistä enemmän myös yrityksissä. Tarvitaan uudenlaista erityisosaamista. Tämä lupaa hyvää tulevaisuutta ajatellen meille tiedonhallinnan ammattilaisille.

**Anssi Jääskeläinen**
TKI-asiantuntija
Digitalia/Xamk

Helsingissä hotelli Scandic Parkissa järjestettiin 23.11.2017 Tivin Digital & Cyber Security 2017 tietoturvaseminaari. Digitalia oli paikalla kahden osallistujan voimin. Päällimmäisenä ajatuksena seminaarista jäi mieleen toinen toistaan mullistavammat tietoturvaratkaisut – ainakin markkinointimiesten puheiden perusteella. Itse en nähnyt tai kokenut näissä sponsorien esittelemissä ratkaisuissa mitään ihmeellistä tai mullistavaa. Kaikki ratkaisut pyrkivät havaitsemaan mahdolliset uhat ja epänormaaliudet jo ennen kuin ne edes alkavat aiheuttaa haittaa.

Aruba 360 secure fabric tekee yritysverkon jokaisesta käyttäjästä riskiprofiilin, johon kaikki käyttäjän toiminnot vaikuttavat. Jos käyttäjän toiminta jossain vaiheessa alkaa poiketa normaalista, järjestelmä puuttuu peliin. Check Point Software Technologiesin automatisoitu forensiikka-analysointi puolestaan kerää jatkuvasti tietoa käyttäjärjestelmässä tapahtuvista asioista, ja jos jotain poikkeavaa tapahtuu, se markkinointipuheiden mukaan myös havaitaan. Lisäksi heidän softansa voi kuulemamme mukaan palauttaa myös ransomware-haittaohjelmien kryptaamat tiedostot, koska kaikesta otetaan varjokopioita lennossa.

# Digital & Cyber Security 2017

SentinelOne yhtiön edustaja puolestaan totesi loppukäyttäjien työpisteiden olevan 95% tapauksissa lähde tietovuodoille/tietomurroille. Heidän mukaansa käyttäjillä on taipumus klikata linkkejä, vaikka he aavistelisivatkin jotain olevan pielessä. Usean paikalla olleen toimijan mukaan uutta pahaa koodia syntyy päivittän massiivisia määriä ja perinteiset virustorjuntaohjelmistot laahaavat auttamatta perässä. Lisäksi nykyisistä uhista monet osaavat tunnistaa hiekkalaatikkoympäristöt, ja neaktivoituvat vasta päästessään sieltä pois.

## Kyberturvallisuudesta

Tilaisuuden keynoten piti "tietoturvaguru", Aalto yliopiston kyberturvallisuuden professori Jarno Limnéll, aiheenaan Kyberturvallisuuden tilannekuva 2020. Ei ollut yllätys, että puhe alkoi IoT ja muutenkin verkkoon kytkettävien laitteiden määrän räjähdysmäisellä kasvulla ja tästä väistämättä seuraavilla tietoturvaongelmilla.

Limnéll ei mennyt tarkkoihin esimerkkeihin, mutta allekirjoittanut menee. Esimerkiksi useassa kodissa löytyvän reitittimen web-käyttöliittymän käyttäjätunnus/salasana on edelleen se, joka siihen on tehtaalla asetettu. Samoin on miljoonissa muissakin laitteissa.

Vaikka IoT laitteen hakkerointi yksinään ei aiheuttaisi minkäänlaisia ongelmia laitteen haltijalle itselleen, niin yhdistämällä miljoonia hakkeroituja laitteita saadaan aikaiseksi esimerkiksi infrastruktuureita kaatava DDoS (Destributed Denial of Service) hyökkäys. Näin toteutettiin muun muassa Mirai botnet hyökkäys lokakuussa 2016, jossa laitteina käytettiin esimerkiksi perus-käyttäjänimen ja salasanan omaavia verkkokameroita. Vaikka käyttäjätunnuksen ja salasanan olisikin vaihtanut, suuressa osassa verkkoon kytkeytyviä laitteita on pohjalla edelleen reikäjuuston kaltainen Android 4.2 käyttöjärjestelmä jonka reikiä hyödyntää kuka tahansa aloittelevakin hakkeri. Ohjeistuksena kaikille lukijoille, muuttakaa oletussalasanat ja pitäkää järjestelmänne päivitettynä.

Limnéllin mukaan Darwinin teoria pätee edelleen myös teknologian kehityksessä ja toimintaympäristöjen muutoksessa; selviytyjiä ovat ne, joilla on paras kyky sopeutua muutokseen. Puheessaan hän myös totesi yhden luukun tietoturvaratkaisujen tulevan yleistymään. Uskallan olla tästä asiasta osittain eri mieltä ja perustelen näkemykseni kilpailutuslainsäädännöllä. Jos firma ei ole ostanut kerralla koko tietoturvapakettia yhdeltä toimittajalta, ei se voi myöhemmin perustella suorahankintaa tältä toimittajalta vedoten yhteentoimivuuteen, jos muutkin toimittajat pystyvät takaamaan yhteentoimivuuden. Tämä on asia, joka kannattaa pitää mielessä.

Kohta edessämme on Limnélin mukaan tilanne, jossa emme enää mieti, mitä koneet voisivat tehdä, vaan mitä voimme antaa koneiden tehdä. Lopuksi hän mainitsi Darpan raportin vuodelta 2002, jossa todettiin ihmisistä olevan kovaa vauhtia tulossa puolustusjärjestelmien heikoimpia lenkkejä. Allekirjoittaneen mielestä tästä lausahduksesta ei teoriassa ole enää kovinkaan pitkä matka Skynet-järjestelmän (Terminator elokuvasarjassa) syntymään.

## Tiedon luotettavuudesta

Yksi merkittävimmistä esiin nousseista asioista on tiedon luotettavuus, joka koskettaa läheisesti etenkin tiedonhallinnan ja arkistoinnin parissa toimijoita. Tutkimusten mukaan usko organisaation hallussa olevaan tietoon murenee, jos siitä on reilut 5% pielessä. Enää ei pelätä, että joku varastaa tiedot, vaan että joku muuttaa niiden oikeellisuutta.

Periaatteessa yhden haittaohjelman pääsy asianhallintajärjestelmään esimerkiksi PDF-tiedostoksi naamioituna liitteenä voisi aiheuttaa koko järjestelmän kryptautumisen. Luonnollisesti tällainen vaatisi järjestelmältä vakavaa haavoittuvuutta, mutta onhan näitä viime aikoina löytynyt huomattavasti paremminkin testatuista järjestelmistä kuin asianhallintajärjestelmät. Näillä viittaan luonnollisesti Spektre ja Meltdown haavoittuvuuksiin, jotka olivat olleet prosessoritasolla muutamaa poikkeusta lukuun ottamatta käytännössä


vuodesta 1995 lähtien. Näistä oli 15.2.2018 mennessä seurannut Intelin mukaan jo 30 kannetta heitä kohtaan. Olettehan te jo päivittäneet omat järjestelmänne niin, että ne eivät ole enää alttiita Spektrelle eikä Meltdownille?

## Salasanoista

Microfocus oli ottanut hieman erilaisen lähestymistavan tietoturvaan kuin muut paikalla olleet yritykset. Heidän edustajansa mukaan 81% tietovuodoista johtuu heikosta tai varastetusta salasanasta. Tästä olen täysin samaa mieltä. Esimerkiksi allekirjoittanut sai "järjestelmävastaavamme" toimesta salasanaksi kahdeksan merkkisen kuukauden nimen erääseen julkiseen verkkopalveluun. En tiennyt itkeä vaiko nauraa, koska järjestelmä ei edes pyytänyt vaihtamaan salasanaa ensimmäisellä kirjautumiskerralla, ja toisekseen järjestelmä ei ilmeisesti mahdollista itsenäistä salasanan vaihtamisesta.

Te, jotka ette tätä ymmärrä: kahdeksan merkin mittainen salasana murtuu muutamassa sekunnissa nykyisellä PC-laitteella hyödyntäen esimerkiksi vapaasti saatavilla olevia valmiiksi laskettuja hash tauluja riippumatta siitä, onko salasanassa käytetty erikoismerkkejä, numeroita, isoja kirjaimia jne.

Pelkkää raakaa laskentatehoakin käyttäen kahdeksan merkkisen salasanan tapauksessa puhutaan maksimissaan tunneista. Tämä kaikille teille tiedoksi, jotka vieläkin käytätte lapsenne syntymäaikaa tai koiranne nimeä salasanana. Hyvä salasana onkin nykyisin salasanalause eikä epämääräinen yhdistelmä erikoismerkkejä, numeroita ja kirjaimia. Esimerkiksi 16 merkin lauseen "etpäs murra tätä" murtaminen kestäisi pelkällä raa'alla laskennalla noin kaksi triljoonaa vuotta, jonka luulisi riittävän pitämään murtautujat poissa. Eri asia on tietenkin kalasteluviestit, joista myöhemmin lisää.

Osa teistä lukijoista varmasti huojentaa omaatuntoaan toteamalla, ettei teillä ei ole mitään hakkereita kiinnostavaa tietoa. Ei välttämättä olekaan, mutta hakkerit aloittavatkin heikoimmasta lenkistä ja etenevät kohti käyttöoikeustasolla korkeiden käyttäjien oikeuksia. Siinä vaiheessa, kun hakkerilla on päässyt sisäverkkoon, hänellä on käytännössä kaikki ovet auki, koska sisäverkossa liikenne kulkee usein salaamattomana, liikennettä ei juurikaan tarkkailla ja liikenteen seuraaminen ja tallentaminen muun muassa Wiresharkin kaltaisilla ohjelmilla on naurettavan helppoa.

Olen esimerkiksi kuullut tapahtumasta, jossa yrityksen tietoturva oli muuten erinomaisella tasolla, mutta sisäverkkoon kytketty tulostin oli unohdettu. Hakkeri oli yksinkertaisesti marssinut huoltomieheksi pukeutuneena tulostimelle ja päässyt sitä hyödyntäen sisäverkkoon. Siitä hän oli edennyt pikkuhiljaa organisaatiorakenteessa ylöspäin. Kyseessä oli onneksi ennalta palkatun hakkerin tekemä tietoturva-auditointi, mutta saman olisi voinut tehdä oikea ilkeämielinen hakkeri. Kaiken tasoisten käyttäjien autentikointiin kannattaa siis kiinnittää huomiota, eikä tietoturvassa kannata myöskään unohtaa niitä "vähäpätöisempiä" laitteita, joiden kautta kenenkään ei voisi uskoa saavan mitään pahaa aikaiseksi.

## Ihminen on heikoin lenkki

Koska ihminen ja hänen tekemänsä ratkaisut ovat usein tietoturvan heikoin lenkki, olisiko heitä sitten aiheellista kouluttaa. Outokummun mukaan kyllä, ja heidän ratkaisunsa erosi huomattavasti perinteisestä puolen päivän kalvosulkeisista, jonka jälkeen kaikkien oletettiin osaavan kaiken. He olivat käyttäneet kouluttamisessa huijausviestisimulaatioita, koska heidän tietojensa mukaan sähköpostilla toteutettu kalasteluviesti, joka tulee lähes omaa vastaavaa domainista, on selkeästi suosituin hyökkäysmenetelmä yrityksiä vastaan.

Outokumpu lähestyi ongelmaa itse toteutetulla huijausviestikampanjalla. He lähtivät liikkeelle kevyesti ilmiselvällä huijausviestillä ja nostivat tasoa pikkuhiljaa. Näin he saivat pidettyä käyttäjänsä innostuneina, korostaen positiivisuutta ja oppimista.

Toinen vaihtoehto olisi ollut lähteä liikkeelle täydellisellä huijausviestillä ja herättää johto esittämällä todella synkät tulokset.

Huijausviestisimulaatiolla käyttäjien tekemien virheiden ja vaarallisten klikkauksien määrää saatiin 15:llä simulaatiokierroksella pudotettua jopa 50%. Tosipaikan eteen Outokumpu oli joutunut 19.10.2017 alkaneessa huijausviestihyökkäyksessä. Ensimmäiset käyttäjät olivat reagoineet oikein alle viidessä minuutissa ja ilmoittaneet kampanjasta tietohallinnolle. Testikäyttäjiltä oli kuulemamme mukaan saatu pelkästään positiivista palautetta – yksikin oli todennut: "Now I actually think before I click/open link".

## Tietosuoja-asetus

Ei tietoturva-aiheista seminaaria ilman lakia, ei myöskään nyt. Tällä hetkellä vahvasti vaikuttava tekijä GDPR oli vahvasti esillä. Jukka Lång Dittmar & Indrenius Asianajotoimistolta valotti tilannetta. GDPR eli General Data Protection Requlation tulee täysin voimaan 25.5.2018 eli noin kolmen kuukauden kuluttua. Lyhykäisesti organisaatioilla on oltava nimettynä tietosuojavastaava, kaikkien toimintaan liittyvien henkilöiden, mukaan lukien mahdollisten alihankkijoiden, henkilötietojen käyttö ja käytänteet tulee olla GDPR:n vaatimusten mukaisia ja tietoturvakäytänteet tulee olla dokumentoituja.

Osa teistä ajattelenee jälleen, että asia ei kosketa minua, koska te ette käsittele henkilötunnuksia tai talleta muita henkilötietoja pitkäksi aikaa. Huomioittehan kuitenkin, että EU-tuomioistuimen päätöksen mukaan myös IP-osoite voidaan luokitella henkilötiedoksi[1]. Näin järjestelmän automaattisesti keräämä lokitiedosto, joka sisältää kävijän IP-osoitteen vaatii kriittisimmän tulkinnan mukaan jo kaikki GDPR:n mukaiset toimenpiteet. Myös tapahtumaa varten luotava osallistujaluettelo katsotaan GDPR:n mukaan henkilörekisteriksi.

Nyt teitä kaikkia kauhistuneita kehottaisinkin kysymään itseltänne ainakin seuraavia kysymyksiä:

- Mihin kaikkiin järjestelmiin tallennamme henkilötietoja?

- Miksi ja mihin käyttötarkoitukseen keräämme henkilötietoja, ja erityisesti tarvitsemmeko me niitä kaikkia?

- Luovutammeko henkilötietoja eteenpäin ja jos luovutamme, niin mihin?

## Turvallisuusuhkia

Seminaarin lopettavassa keynote-puheenvuorossa Cambridgen yliopiston Ross Anderson maalaili erinäisiä piruja seinille. Hän muun muassa kertoi, että Jeep Cherokee hakkeroitiin etänä Chryslerin uconnect ohjelmalla ja että CO2 päästöskandaali oli lähtöisin sisäpuolelta. Kaksituhatta ihmistä kuolee vuosittain Iso-Britannian sairaaloissa tietoteknisten laitteiden käytettävyysongelmien vuoksi. Lisäksi hän mainitsi DNP3-protokollan, jota käytettäessä pelkkä laitteen IP-osoitteen tietäminen voi riittää sen hallintaan, koska kyseinen protokolla ei tue autentikointia.

Autojen ja esim. sairaalalaitteiden tapauksessa hän totesi ongelmaksi sertifioinnin. Siinä missä PC:n käyttäjärjestelmää on helppo paikata tietoturvapäivityksillä, autojen ja sairaalalaitteiden kohdalla tilanne on toinen, koska sovelluspäivitys voi rikkoa olemassa olevan sertifioinnin. Lisäksi hän arveli, että viiden vuoden sisällä EU saattanee alkaa vaatia autovalmistajia takaamaan ohjelmistopäivitykset esimerkiksi kaksikymmentä vuotta eteenpäin auton valmistuksesta. Tämä tulisi autovalmistajille tolkuttoman kalliiksi, koska heidän tulisi säilyttää testauskykynsä kaikkiin kahdenkymmenen vuoden aikana tehtyihin automalleihin. Pelkkää koodia kun ei voi auton tapauksessa testata, vaan koko paketin eli auton toimivuus pitää todeta.

Henkilökohtaisesti en usko, että suuret autovalmistajat tällaiseen suostuvat, vaan lobbaavat tämän kaltaiset ehdotelmat kumoon, jos niitä koskaan edes syntyy. Andersonin puheenvuoro olisi voinut toimia herättelijänä heti seminaarin alussa, mutta se ei mielestäni täyttänyt tarkoitustaan keynote-puheena seminaarin viimeisenä.

Seminaari oli kaikin puolin kiinnostava, mutta se tarjosi lopultakin kohtalaisen vähän konkreettisia työkaluja tietoturvan parantamiseen. Nostaisin ensimmäisinä toimina esille verkkolaitteiden kartoituksen sekä käyttäjien autentikointiin panostamisen, jos lähdette parantamaan organisaationne tietoturvaa. Sen jälkeen käyttäjiä voisi pyrkiä kouluttamaan kalasteluviestejä vastaan. Askeleittain eteenpäin kohti parempaa tietoturvaa ja tietosuojaa. Ettehän halua joutua maksamaan 20 miljoonan euron tai 4% yrityksen globaalia liikevaihtoa vastaavaa sakkoa GDPR rikkomuksista?

1 http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1116945