satopaa_welling_korjattu_ver2

0:00
Pia: Tän kaltaiset tietoturva-aukot on hyvinkin yleisiä eli just siellä koodissa olevat virheet, konfigurointivirheet, aiheuttaa niitä aukkoja, jota sitten ne hakkerit yrittää hyödyntää.

0:15
Talk Podcast. Näkökulmia muutokseen.

Siiri: Tervetuloa uuden Talk podcastin pariin. Minä olen Siiri Welling ja tänään meillä on vieraana kyberturvallisuuden lehtori Pia Satopää ja tänään me puhutaan nyt tietysti ylläripylläri kyberturvallisuudesta. Pia sä oot ollut meillä… onko se nyt toista vuotta lehtorina?

P: Joo olen toista vuotta kyllä.

S: Sä olet sitä ennen toiminut pitkään puolustusvoimilla samojen aiheiden parissa ja sen takia ne aiheet on sulle myös tosi tuttuja. Mutta ihan nyt ensin täytyy aloittaa näistä perusasioista ja selventää että mistä tässä on kyse, niin mitä se kyberturvallisuus on, mitä sillä tarkoitetaan?

P: No kyberturvallisuuden tarkoitetaan yleensä tämmöisen sähköisen maailman eli digitaalisen toimintaympäristön turvallisuutta. Tässä on vähän eri käsityksiä, riippuen siitä keneltä kysyy, mutta mun mielestä kyberturvallisuus on sitä sähköisen tiedon turvaamista.

S: Mutta sitten puhutaan myös tästä tietoturvasta, niin miten se, miten nämä 2 eroavat toisistaan kun musta tuntuu että nää menee aika usein sekaisin ihmisillä kun puhutaan tai kun he puhuu tietoturvasta ja kyberturva.

P: No joo just näin. Eli puhutaan tietoturvallisuudesta ja kyberturvallisuudesta ja tässä niitä tulkintaeroja just sitten onkin, mutta tietoturvallisuus mun näkökulmasta ja mun mielestä on niinku laajemmin sitä tietojen turvaamista. Eli se kattaa myöskin kaiken muun tietoturvan eli tämmöisen fyysisen tietoaineiston turvaamisen, kun kyberturvallisuus sitten taas keskittyy siihen sähköisessä maailmassa olevaa tietoon.

S: Eli puhutaan esimerkiksi siitä, että minkälaisia tietoja kerätään ihmisistä, jos on erilaisia kyselylomakkeita tai tapahtumailmoittautumisia esimerkiksi, niin silloin on kyse tietoturvasta esimerkiksi.

P: Juuri näin, jos se on fyysisessä muodossa, paperimuodossa ja niitä säilytetään vaikkapa kassakaapissa tai missä muistitikuilla jos niitä joku vielä käyttää, niin tän tyyppiset materiaalit.

S: Ja tosiaan täällä Turun ammattikorkeakoulussa opetat kyberturvallisuutta ja tietysti riskienhallintaa. Mutta sitten kun puhutaan riskienhallinnasta tässä kyberturvamielessä niin mitä se oikeastaan nyt sitten tarkkaan ottaen on?

P: Riskienhallinnalla kyberturvallisuudesta tarkoitetaan sitä, että pystyttäisiin varautumaan ja ennaltaehkäisemään siihen sähköiseen tietoon kohdistuvia uhkia ja riskejä eli että ne ei pääsisi realisoitumaan ne riskit siihen tietoon kohdistuen. Ja jos me ajatellaan kyberturvallisuusriskejä, niin meidän pitäisi kysyä itseltämme, että mitä me suojataan, miksi me suojataan, keneltä me suojataan ja miten me sitä suojataan.

S: Aivan eli tässä estetään tulipalojen syttymistä siellä kyberturvamaailmassa jos niin voisi sanoa.

P: Kyllä ja nykyään niitä tulipaloja valitettavasti syntyy joka tapauksessa niin harvemmin niiltä enää voi välttyä, että sitten se jatko siihen on se, että millä tavalla sitten siitä tulipalosta selvitään ja toivutaan ja palataan takaisin normaaliin toimintaan.

3:20

S: Myös tää kyberturva, ja ehkä nyt tästä riskienhallinnastakin tulee ensimmäisenä mieleen, että tyypillisimpiä on varmasti tämmöiset tietoturva-aukot eli jostain koodin pätkässä on vaikka puute ja sitten sitä kautta niin hakkerit tulee kurkkimaan tietoja. Vaikka pankkiasioista, paljonko sulla on rahaa sun tilillä esimerkiksi tai näin. Mut et onko sulla käsitystä siitä, että miten tavallisia just tän tyyppiset tietoturva aukot on? Oliko tää huono esimerkki?

3:51
P: No ei ollut huono esimerkki, että jos me ajatellaan nyt tällaista kybertoimintaympäristöä eli tätä meidän sähköistä maailmaa, niin tän kaltaiset tietoturva aukot on hyvinkin yleisiä, eli just siellä koodissa olevat virheet, konfigurointivirheet, aiheuttaa niitä aukkoja siellä, jota sitten ne hakkerit yrittää hyödyntää. Ja just niinku tossa sunkin esimerkissä oli, niin pääosin halutaan rahaa. Ja millä tavalla siihen sitten pääsee käsiksi, niin niitä aukkoja pyritään etsimään ja jos ajatellaan tota nykymaailmaa niin tekoälyhän on todella tehokas etsimään niitä aukkoja ja toimii sitten tehokkaimmin apuna. Kyllä me ollaan aika mielenkiintoisessa maailmassa.

S: Miten tämmöisiä tietoturva-aukkoja syntyy? Johtuuko se vaan siitä, että joku on ollut huolimaton ja unohtanut tarkistaa, että se tietty koodinpätkä siellä toimii, vai onko tässä jotain muutakin taustalla?

P: No pääosin näkisin että juurikin näin, eli ne on niitä inhimillisiä virheitä. Siinä koodauksessa tai sitten auditoinnissa ei ole tullut esiin joku aukko, eli täysin pommivarmaan, täysin turvallista järjestelmää, ei ole nähdäkseni mahdollista edes tehdä eli se on kyllä hankala asia.

S: Eli hakkerit on aina kuitenkin sitten yksi äsken ehkä edellä tai jos ei edellä, mut kuitenkin tiiviisti siellä perässä tulevat ja löytävät uusia tietoturva-aukkoja.

P: No ovat tiiviisti perässä ja heillä on se motivaatio siihen aukkojen etsimiseen, että ehkä se on se heidän ajurinsa siinä.

S: Mut tavallisiin ihmisiin kohdistuu myös näitä huijausyrityksiä ja tämmöisiä tietoturvaongelmia ja itse ainakin oon aika usein itse asiassa saanut nykyisellään ihan tekstiviestejä missä pyritään sanomaan, että mulle on saapunut joku postin lähetys ja klikkaa tätä linkkiä ja sitten myös torissa. eli tori.fi:ssä on ollut vähän vastaavan kaltaisia huijausyrityksiä ja toki somessa on nää perinteiset huijauskirjeet eli joku no viimeksi vaikka on tämmöinen joku amerikkalainen afganistanin veteraanilääkäri sitten yhtäkkiä tavoittelee loppujen lopuksi rahaa, mut miten sä itse kuvailisit kun on pitkä kokemus nyt tästä kyberturvaasta ja paljon näkemyksiä niin miten tavallisia tämmöiset tavallisiin ihmisiin kohdistuvat huijausyritykset on sitten jos verrataan näitä organisaatioiden kohtaamia huijausyrityksiä.
Eli kumpaa huijataan useammin yritystä vai ihmistä?

P: No tuohon en osaa sanoa kumpaa huijataan enemmän. Mä luulen että organisaatiot on enemmän varautuneita ja valveutuneempia ja siellä myöskin sitten koulutetaan ja viestitään asioista että yksityishenkilöiden massan on hirveän iso ja laaja hyökkäyskenttä ja kuten sanoin niin näitähän tulee koko ajan ja todella paljon ja just amerikkalaiset upseerit lähestyy naisihmisiä ja kertoo, että äiti on kipeänä täällä ja toimita rahaa niin nää on tosi tyypillisiä. Ja nythän nää rekrytointi huijaukset eli tulee viestillä vaikka whatsappilla että kiitos hakemuksesta ja haluaisimme jatkaa keskustelua ja siitä se sitten etenee. Mutta me ollaan kuitenkin inhimillisiä ihmisiä ja me halutaan uskoa ihmisestä ja hän yhteydenotoista hyvää, niin se on se meidän heikko kohta. Eli pitäis aina vähän olla semmoinen epäileväinen, varsinkin kun tulee niitä linkkejä. Ei lähdetä kikkailemaan vaan selvitetään ja ajatellaan maalaisjärjellä, että jos se näyttää liian hyvältä että sieltä on nyt arabialaiselta prinssiltä tulossa miljoonia, niin se ei ehkä ole totta.

S: WhatsAppiin tulee työpaikkailmoituksia tai tämmöisiä pyyntöjä, että sut on hyväksytty haastatteluun tai eteenpäin niin niin tuleeko se suomen kielellä nykyisellään?

P: En ole törmännyt vielä suomenkielisiin, mutta englanniksi ainakin toistaiseksi on tuolla, mutta

tekoälyhän on tässäkin hyvä renki eli osaa kääntää kyllä suomen kielelle niin tehokkaasti, että ei pysty erottamaan. Ei ole niitä kielivirheitä.

S: tavoite on varmaan sitten saada niitä pankkitietoja tai tilitietoja.

P: Joko tilitietoja tai sitten pyydetään jotakin summaa, että voidaan tätä prosessia jatkaa ja.

S: Miten voi tietää ettei omia tietoja ole valunut hakkereille tai muualle tämmöisiin epäilyttäviin paikkoihin? Pystyykö tavallinen ihminen edes tarkistamaan mistään, että missä hänen tietonsa menevät tai liikkuvat`

P: On olemassa sellaisia ilmaisia palveluja, jossa sä voit käydä tarkistamassa, että onko sun käyttäjätunnus , sun sähköposti mitä usein käytetään käyttäjätunnuksena, niin onko se vuotanut jonnekin? Esimerkiksi Fsecurelta löytyy tämmöinen palvelu ja sieltä kyllä selviää sitten, että onko sitä sun tunnusta hyödynnetty.

S: Ootko sä käynyt testaamassa ikinä?

P: Oon käynyt testaamassa ja muutamasta palvelusta tuli ilmoitus että on vuotanut ja
menin kyllä hyvin nopeasti vaihtamaan salasanan tai sitten kyseessä toinenkin oli semmoinen missä oli sellainen palvelu mitä mä en enää käytä. Sitten luovuin siitä kokonaan.

S: Ehtikö mitään vahinkoa käymään näillä vuodetuilla tiedoilla, että oliko joku huijari yrittämässä esiintymässä sinuna?

P: Ei ole semmoista onneksi tapahtunut, että siltä toistaiseksi välttynyt.

S: No niin jotain positiivista.
No tuossa aikaisemmin kyllä ehkä puhuitkin jotain, sanoit sitä että miten voi erottaa niitä huijausviestejä oikeasta viestistä. Tosiaan kun puhutaan aikaisemmin sitä, että somen kautta tulee aika paljon näitä huijausviestejä ja sitten mä itse asiassa törmäsin yksi päivä tämmöiseen uutissivustoon, ihan niinku että se näytti ihan just siltä tietyltä luotettavalta uutissivustolta ja siinä oli tämmöinen klikkiotsikko mikä ei ole tietysti hirveän epätyypillinen jo journalismissa tai viestinnässä muutenkaan, mutta ei eli otsikon perusteella ei pystynyt päättelemään että on nyt kyse huijaussivustosta, mut sitten sitä tekstiä luki eteenpäin siinä on. Se on pitkä artikkeliteksti, jossa käytännössä yritettiin ajaa ihmistä toiselle sivustolle, jossa sitten olisi voinut tapahtua jotain niinku rahan siirtoa. Kun tekstiä lukee eteenpäin niin sitten kyllä huomasi että tätä ei ole oikea ihminen kirjoittanut. Miten se neuvoisit nyt tosiaan tavallista ihmistä, semmoiset jotka joilla ei ehkä ole mitään viestinnän kokemusta, että pystyy katsomaan tätä ei pidä paikkaansa niin mitä sanoisit tälle ihmiselle, mitä kannattaa tai mihin kannattaa kiinnittää huomiota kun tulee tämmöisiä epäilyttäviä viestejä?

11:26
P: Ehkä just siihen, että jos se vaikuttaa se kieliasu erikoiselta itse ainakin kiinnitän siihen huomiota tai sitten kun otsikko on tosi raflaava. Ja varsinkin jos se tulee sitten vaikka jonnekin facebookiin tämmöisenä mainos tyyppisenä niin en lähde niitä klikkaamaan, mutta toisaalta niin kauan kun sä et luovuta mitään tietoja mihinkään niin se ei ole kovin vaarallista. Ehkä siihen kohtaa kannattaa sitten herätä, että nyt mä en enää siirry sitten seuraavalle sivustolle.

S: Tarkkaavaisuutta.

P: Tarkkaavaisuutta.

S: No entäs nyt sitten jos on kuitenkin klikannu sitä epäilyttävää sivustoa ja ehkä joku rahansiirtokin on tapahtunut niin mitäs sitten? Mitä sitten voi tehdä enää? Onko peli jo menetetty?

P: Ei onneksi ole peli menetetty eli siinä kohtaa ensisijaisesti yhteyttä pankkiin ja estäisin kaikki muutkin rahasiirrot. Ja sen jälkeen ihan rehellinen rikosilmoitus.
Eli siinä kohtaa kun rahaa siirtyy ja sitä on varastettu ja viety, se on rikosasia.

Ja tää on semmoinen asia mitä monet ei ehkä osaa ajatella, että tässä rikosilmoitus tulee tehdä tämmöisessä tilanteessa.
Ja Yksi asia, mikä myöskin monesti tulee esiin, että sitten hävettää niin kovasti se, että on joutunut tämmöiseen tilanteeseen, että mennään vaan sitten lukkoon eikä osata ajatella että mitä tässä nyt on tapahtunut ja mä oon rikoksen uhri. Siitä häpeästä pitäisi päästä eroon, koska nää on todella yleisiä niin ei kannata ajatella, että minä olen toiminut tyhmästi ja ollut tässä huono ihminen vaan näitä ihan varmasti tapahtuu monelle.

S: Eli jos toimii nopeasti niin ne omat rahat voi saada takaisinkin vielä.

P: No joissakin tilanteessa joo. Pankki pystyy pysäyttämään sen rahansiirron ja palauttamaan, mutta tietysti nää on aina tapauskohtaisia, että miten sitä pysyttään toimimaan.

S: Mut sä oot enemmän perehtynyt tähän just organisaatiotasolla tähän kyberturvallisuuteen ja tietoturvaan ja IT strategiaan ja sä oot näiden asiantuntija niin osaatko sä sanoa että mikä on semmoinen yleisin virhe, mitä organisaatiot tekee just heidän IT strategiassaan?

P: No ehkä se yleisin virhe on se, että se on liian ylätasolla. Eli se ei konkretisoidu sinne organisaation toimintaan ja sitten toinen virhe voisi olla se, että se ei ole linjassa sen organisaation strategian kanssa. Eli se IT-strategian pitäisi aina tukea organisaation strategiaa ja ne vaatimukset pitäisi tulla sieltä liiketoiminnasta. Eli millä tavalla se IT ja IT strategia tukee sitä organisaation liiketoimintaa eli se voi olla sellainen erillinen oma vähän siiloutunut, omassa kuplansa ja näin sen ei pitäisi olla.

14:42
S: Onko yritykset tai organisaatiot ylipäätään mitenkä tietoisia heidän tietoturva-asioistaan tai kyberturvallisuus asioistaan tänä päivänä.

P: No tänä päivänä me eletään sellaisessa tilanteessa, että organisaatiot on kyllä hyvin heräillä ja kovasti kiinnostuneita siitä oman organisaationsa tietoturvasta. Me saadaan joka päivä lukee lehdissä erilaisista hyökkäyksistä, erilaisista uhkista ja Milloin missäkin, niin kyllä tää on tällä hetkellä asia johon organisaatiot panostaa.

S: Kun puhutaan tietoturvan testaamisesta tai kyberturvaasioiden testaamisesta, niin mä oon törmännyt siihen että on käytössä tämmöisiä valkohakkereita. Eikö niin, että valkohankkeita on?

P: Se on vastakohta tälle pahishakkerille, mutta sanoisin valkohattuhakkeri on tämmöinen joka toimii ehkä niinku eettisemmin eikä havittele sitä taloudellista hyötyä.

S: Ootko sä ikinä kuullut että joku suomalainen organisaatio olisi käyttänyt valkohakkereita staamaan heidän tietoturvaansa?

P: Ole joo, puhutaan valkohattuhakkereista.

S: Aivan joo sulla on nää termit oikein.

P: Joo niitä valkohattuhakkereita, eli he toimivat niin, että auttavat organisaatiota löytämään sieltä omista tietojärjestelmästä niitä aukkoja, jotta niitä sitten pystytään korjaamaan ja varautumaan paremmin ja liiketoiminnan jatkuvuuteen ja panostamaan. Eli näkisin että tää on kyllä organisaatioilla tiedossa ja tällä hetkellä hyvinkin kiinnostava asia.

S: Oletko sä itse aikaisemmin vaikka nyt kun sä opetat meillä näitä master- opiskelijoita, elikkä ylemmän ammattikorkeakoulututkinto opiskelijoita, niin ootko kuullut heiltä, että he olisi vaikkapa heidän organisaatioissaan ihan käyttänyt siis näitä valkohattuhakkereita.

P: No ei ole näissä tullut esiin opiskelijan kautta, mutta tiedän kyllä organisaatioita, jotka ovat käyttäneet. Ja nythän jossakin näin tämmöisen haasteenkin, että organisaation haastoi valtakunnan hankkeita vähän tällaiseen kilpailutyyppiseen. Kuka löytää ja mitä löytää ja siitä saa sitten palkkion.

S: Eli kyllä sitten myös taloudellinen hyöty myös voi motivoida valkohattuhakkereitakin.

P: Ei ole se ensisijainen ajuri, vaan puhtaasti tosiaan auttaa organisaatiota.

S: Eli heistä on ihan hyötyäkin sitten näistä valkohattuhakkereista.

P: On heistä kyllä hyötyä.

S: Mitä yrityksen tulee tehdä, jos se huomaa jonkun tämmöisen tietoturva aukon tai muun tämmöisen ongelman?

P: Oma toivomukseni on, että tilannetta organisaatioissa olisi harjoiteltu eli olisi pohdittu niitä mahdollisia skenaarioita mitä voi tapahtua, jolloin sitten kun jotakin tapahtuu, niin osattaisiin toimia ja minimoida niitä haittoja ja vaikutuksia ja sitten tietysti kyberturvallisuuskeskus on taho, joka organisaatioita suomessa auttaa ja monella varsinkin isommalla organisaatiolla on myös oma palveluntuottaja, joka sitten tulee aluksi siinä kohtaa kun jotain yhtäkkiä tapahtuu.

S: Pitääkö kyberturvallisuuskeskukseen tehdä joku ilmoitus jos on tämmöisiä tietoturvaongelmia tai huomaa näitä aukkoja, siellä?

P: On hyvä tehdä ilmoitus, koska kyberturvallisuuskeskus kerää sitä tilannekuvaa ja sitten jakaa muille organisaatioille tiedoksi, että tällaista on liikkeellä, tällaista on löydetty, että katsokaa ja varautukaa. Ja se, että me pystytään jakamaan sitä tilannekuvaa täällä kansallisesti, niin se hyödyttää kyllä kaikkia organisaatioita.

S: Totta nyt kun itse asiassa puhuit just tosta että jakaa tietoa eteenpäin. Tuli mieleen, että ihan normi ihmisen arjessakin on tätä. Tätä haastattelua tehdään Applen puhelimella, niin tota kyllä tänä vuonnakin on ollut näitä ilmoituksia, että päivittäkää applen käyttöjärjestelmää, että siellä on ollut jotain tietoturva aukkoja. Niin näitä varmaan voi verrata sitten tähän tähän asiaan. Eli jos on joku valkohattuhakkeri käynyt testaamassa ja sitten on tullut tämmöinen tieto niin sitten jaetaan tietoa eteenpäin, että muutkin voi estää sen saman asian ja ongelma. Ootko muuten muistanut päivittäin sun applen käyttöjärjestelmä?

P: mulla ei ole applea tällä hetkellä, mutta kyllä mä pyrin päivittämään mun laitteet ja pitämään ne ajat tasalla, että siellähän ne tulee korjatuksi ne löydetyt aukot. Se on se ensisijainen syy miksi ne kannattaa pitää ajan tasalla.

S: eli päivittäkää laitteita.

P: päivittäkää.

S: Myös siellä organisaatioissa. Ja jos tosiaan nyt kyberturva ja riskienhallinta kiinnostaa, niin sinua Pia voi tulla kuuntelemaan nyt sitten keväällä toukokuun lopussa, shiftissä turussa vierailukeskus joessa, niin onko sulla jo minkälaisia tunnelmia nyt tätä sun puheenvuoroa kohtaan?

P: No tietysti vähän jännittää, nää on aina kivoja tälläiset puheenvuoron mahdollisuudet ja tilaisuudet vielä tää joki on hieno paikka. Hieno stage päästä puhumaan ja riskienhallinnasta siellä puhutaan

aika samoja teemoja mitä tänään tässä keskusteltu, mutta ehkä vielä enemmän sitten sieltä organisaationäkökulmasta.

S: Eli sinne vaan nyt kaikki shiftiin kuuntelemaan Pia Satopäätä. Turun ammattikorkeakoulu on siellä myös muutenkin vahvasti mukana ja edustettuna, joten jos kiinnostaa tällainen kyberturvallisuusasia niin sinne vaan kaikki ihmiset.

P: Tervetuloa kyberriskejä kuuntelemaan.

S: Hei kiitos vierailusta Pia Satopää, oli mukava jutella sun kanssa kyberturvaasta ja tietoturvasta. Nää on asioita jotka koskettaa kaikkia ja kaikkioen n kyllä hyvä päivittää ne laitteet.

Lisää näkökulmia muutokseen löydät Turun ammattikorkeakoulun verkkolehdestä talk.turkuamk.fi