Toimintaympäristön digitalisoituminen

Tilannekatsaus nykytilanteeseen ja toimialojen haasteisiin kyberturvallisuuden näkökannalta

Prologi: kybersota Ukrainassa läikkyy yli

- **Venäjän sotilastiedustelun (GRU) osasto 74455**
  - Kyberuhkatoimija Sandworm / APT44
- **Toimintatapoja: lamauta ja tuhoa**
- **Kyberase: NotPetya (2017)**
  - Naamioitu kiristyshaittaohjelmaksi
  - Osa hybridivaikuttamista Ukrainaa vastaan
  - Levisi muualle Eurooppaan
- **Erityisen suuria vahinkoja Maerskillä**
  - Satamaterminaalien sulkeminen
  - Vahingot USD 300M
- **Myös TNT Express, Saint-Gobain, ym.**
- **Globaalit vahingot USD 4-8 mrd**
  - 200 000 työasemaa
- **Puolustuksen heikkouksia:**
  - Ei päivityksiä
  - Kouluttamaton henkilöstö

2

Venäjän GRU:n toimintatavat eivät ole kovin hienovaraisia – pääasia on, että tavoitteet saavutetaan, ja kaikenlainen “maskirovka” on sallittu puolustajan reaktioiden hidastamiseksi. Jos kohteen lisäksi tulee muita vahinkoja, se on poliittisen johdon asia.
NotPetya levitettiin Ukrainassa yleisesti käytetyn veroilmoitussovelluksen päivityksenä. Sen oli tarkoitus lamauttaa ukrainalaista yrityskenttää ja valtionhallintoa, mutta levisi Ukrainassa olevien ulkomaalaisten yritysten sivukonttorien kautta myös muualle maailmaan.
Maersk on mailman suurin varustamo ja merikuljetusyhtiö, ja NotPetya aiheutti sen, että 17 satamaterminaalia Maerskin 76:sta maailmanlaajuisesti jouduttiin sulkemaan. Haittaohjelma ei levinnyt itse aluksiin, mutta koska terminaalit olivat kiinni, alukset seisoivat satamissa tai jonottamassa pääsyä niihin turhan panttina, ja maaliikenne jouduttiin käännyttämään sataman porteilta pois.
Puolustuksen heikkouksia jälkitarkastelussa olivat nimenomaan heikosti päivitetyt IT-järjestelmät sekä kouluttamaton henkilöstö. Koulutukseksi olisi lisäksi tässä tapauksessa riittänyt se, että jos huomaa jotakin epätavallista, kytkee työaseman irti verkosta.

Tämä ei ollut ainoa tapahtuma, eikä suinkaan viimeinen tai merkittävin, mutta

toimi herätyksenä muillekin kuin perinteisen ICT:n toimijoille siitä, että kyberhyökkäykset uhkaavat nykyisin kaikkea liiketoimintaa vakavasti, toimialasta riippumatta.
Toisaalta tässä oli nähtävissä, että teknisin toimenpitein voidaan päästä vain tiettyyn puolustuksen tasoon asti, jos kyberturvallisuus on huonosti johdettu.

Koulutuksen periaatteet

Kybertoimintaympäristö

Digitalisaation toimintakenttä

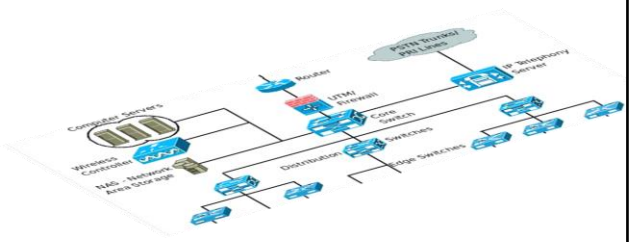
Kun puhutaan digitalisaatiosta ja uusista toimintaympäristöistä, on hyvä Saada ensin jonkinlainen käsitys, mistä oikein puhutaan. Digitalisaatio tarkoittaa löyhästi ilmaistuna digitaalisen, siis bitteihin ja kokonaislukuihin perustuvien tietokoneiden ja tietoverkkojen käyttöä arkipäivän toiminnoissa. Digitalisaatioon kuuluu lisäksi se, että eri toiminnot ovat ainakin jollain tasolla yleensä verkottuneita keskenään. Digitalisaation tärkeänä elementtinä on virtualisoitujen toimintojen joukko. Kokonaistoimintaympäristö on n. 10v sitten nimetty kybertoimintaympäristöksi, tai kybertilaksi (cyberspace).

Kyber- etuliitteenä tulee kreikan kielen sanasta ”kybereo” (”ohjata”, ”opastaa”, ”hallita”). Kybertoimintaympäristön määritelmä v. 2018 kyberturvallisuuden sanaston mukaan on: “yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö, jolle on tunnusomaista elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon viestintäverkkojen avulla. Ympäristöön kuuluvat myös datan ja informaation käsittelyyn liittyvät fyysiset rakenteet.”

Kybertoimintaympäristön rakenne

Fyysinen kerros:

Tietojenkäsittelylaitteet ja –verkot,
bittien jännitetasot, sensorit, aktuaattorit, …



5

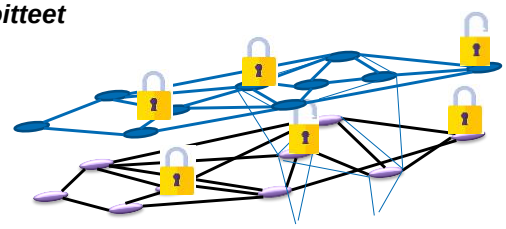
Kybertoimintaympäristö koostuu useista päällekkäisistä kerroksista verkkoja ja verkostoja. “Pohjimmaisena” ajatellaan olevan fyysinen kerros, eli erilaiset tietokoneet, reitittimet, kytkimet, puhelinvaihteet, teollisuusautomaation väylät, sensorit ja aktuaattorit. Ilman *jotakin* fyysistä ilmentymää kybertoimintaympäristön osat eivät toimi. On kuitenkin huomattava, että toiminnot eivät ole riippuvaisia jostakin tietystä laitteesta, kunhan niitä jossain on saatavilla. Fyysisellä kerroksella biteilläkin on konkreettinen olemus, esimerkiksi jännite- tai magneettikentän tasoina.

Fyysisellä kerroksella toiminnan rajoittaminen onnistuu vain jokin elementti fyysisesti poistamalla tai irrottamalla. Toiminnan synnyttämisen edellytyksenä on myös yhteyden ja yhteensopivuuden olemassa olo. Jos esimerkiksi yhteensopivuus poistuu päivityksen myötä, toiminnan tietty osa loppuu.

Kybertoimintaympäristön rakenne

Looginen / virtuaalinen kerros:

Ohjelmistot, data, tietovirrat, pääsynhallinta, Identiteetit, toiminnan rajoitteet



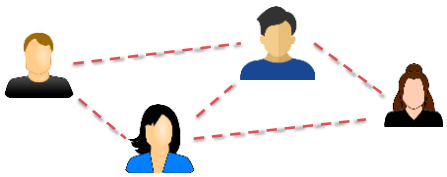
6

Kybertoimintaympäristön määräävä toiminnallisuus tulee virtuaalikerroksesta. Tämä kerros sisältää useita päällekkäisiä tasoja, jotka optimoivat omia tehtäviään eri rajapintojen kautta. Virtuaalikerroksilla on helppo asettaa estoja (lukkoja) ja tehdä pääsynhallintaa. Periaatteessa loogisella kerroksella ei pysty “murtamaan” mitään: jos toimintaa estävä mekanismi toimii oikein, ohittamattomasti ja korruptoitumatta, loogisen kerroksen toimin siitä ei ole mahdollista päästä ohitse.

Valitettavasti tosin on äärimmäisen vaikeaa

1) rakentaa kompleksisia järjestelmiä “oikein”,
2) rajoittaa kaikki mahdollinen toiminnallisuus kulkemaan kyseisen lukon kautta (ylä- ja alapuolella olevalla kerroksen osalla ei ehkä olekaan lukkoa)
3) Tehdä lukosta korruptoimaton (esimerkiksi viallisen päivityksen tai luvattoman hallintaprotokollan käytön avulla)

Kybertoimintaympäristön rakenne



Käyttäjäkerros:

Ihmiset, tieto, tavoitteet, politiikat, käyttötavat, luvat, muiden kerrosten rakentaminen ja muuttaminen

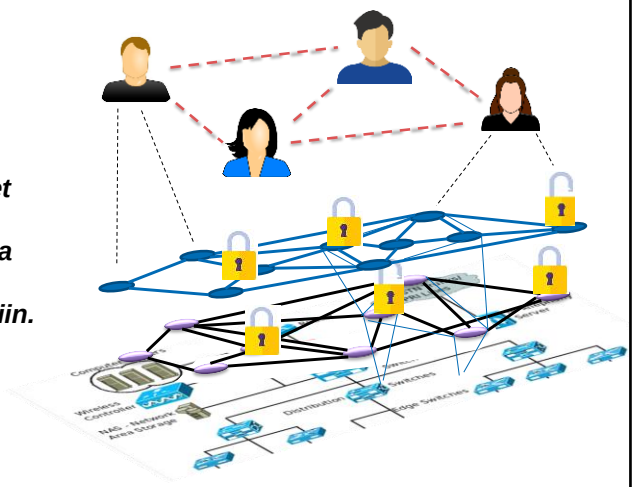
7

Vaikka virtuaalinen fyysinen kerros kykeneekin tekemään paljon asioita automaattisesti ja ilman käyttäjän ohjeistusta, varsinkin käytännön toimenpiteet järjestelmien toimimaan saattamiseksi ovat paljolti ihmisten varassa. Viime kädessä organisaation johto asettaa liiketoimintatavoitteet, jotka ohjaavat riskienhallinnan kautta tietoturvaa ja esimerkiksi tietovarantoihin pääsyä tai teollisuusautomaation luotettavuuteen sijoitettavia resursseja.

Kybertoimintaympäristön rakenne

Kerrosten yhteentoiminta:

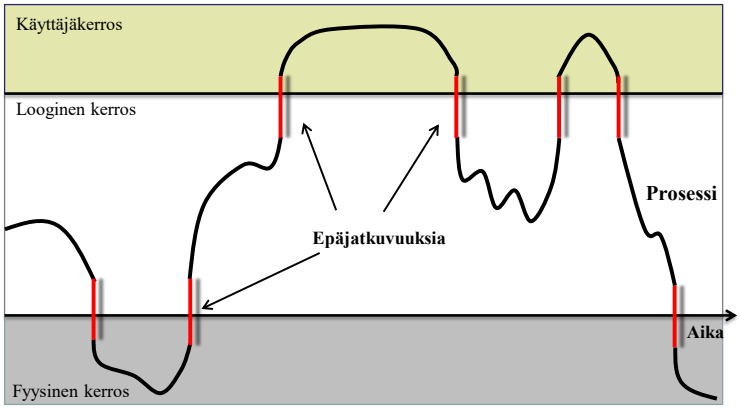
Lyhyt- ja pitkäaikaiset sidokset käyttäjiltä palveluihin (loogisella kerroksella) ja ohjelmistoilta laitteisiin.



8

Kybertoimintaympäristö on erittäin nopeasti muuttuva ja vaikeasti ennustettava johtuen verkkomaisesta rakenteesta eri kerroksilla, näiden jakautumisesta alikerroksiin ja kerroksien välisestä vuorovaikutukseta ja toiminnan rajoitusmekanismeista.

Liiketoimintaprosessin kulku kyberympäristössä



9

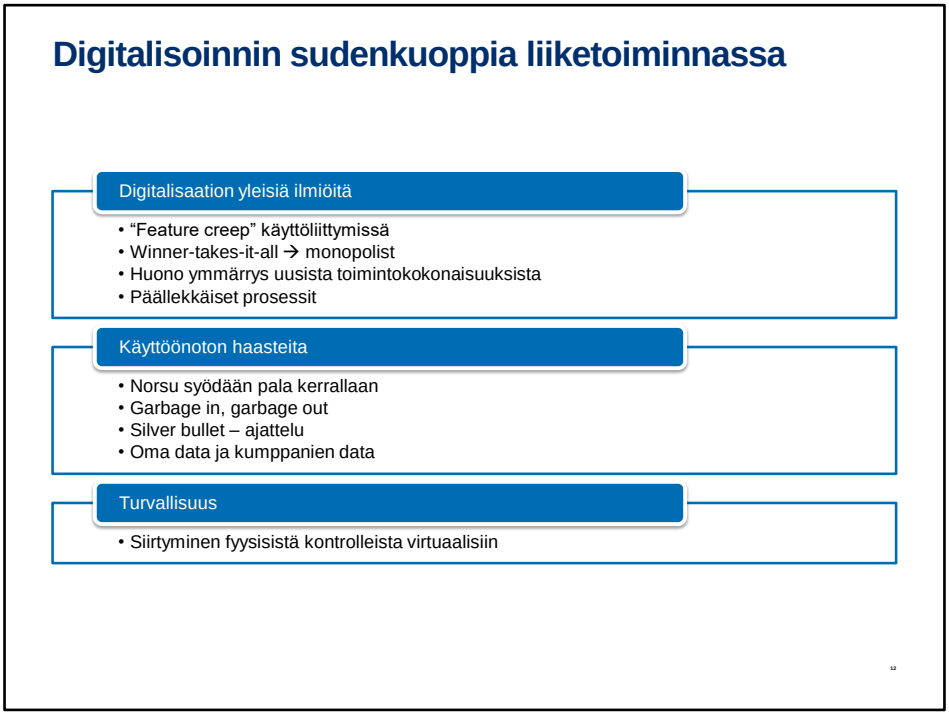
Kaikki kybertoimintaympäristössä tapahtuva toiminta, mukaanlukien liiketoimintaprosessit, ei toimi pelkästään loogisilla kerroksilla, vaan välillä ohjelmistot komentavat laitteistoja kohottamaan jännitetasoja ja käyttäjiltä pyydetään päätöksiä. Kerroksellinen toiminta on pyramidimaista sikäli, että alempien kerrosten on toimittava todella hyvin, jotta ylemmät kerrokset pystyisivät toimimaan edes kohtuullisesti. Fyysisen kerroksen ja alempien kerrosten väliset rajapinnat on nykyisin tarkkaan standardoitu ja hyvin testattu.

Suurin osa kyberturvallisuusongelmista tapahtuukin ylemällä tasolla, erityisesti kerrosten ja välikerrosten välisissä hypyissä. Käyttäjän klikatessa haittaohjelmalinkkiä tapahtuu epäjatkuvuus.

Digitalisaatio liiketoiminnassa

Teknologia toimii digitalisaation mahdollistajana. Digitaalinen tieto torjuu luonnostaan vääristymiä ja sitä voidaan myös siirtää ilman poistumaa. Digitalisaatio on poistanut aikaan, tilaan, tiedonsaantiin ja osallistumiseen liittyviä rajoituksia kansalaisten vuorovaikutuksesta ympäröivän yhteiskunnan kanssa.
Teknologioiden lisäksi digitalisaatiossa hyödynnetään digitaalisten palveluiden myötä muuttunutta asiakaskäyttäytymistä ja markkinoiden toimintatapoja. Esimerkiksi älypuhelinten

yleistyttyä ihmiset käyttävät internetpalveluita jopa kymmeniä kertoja päivässä ja uusissa käyttötilanteissa, kuten julkisissa kulkuneuvoissa. Markkinoiden toimintatapoja taas muuttavat esimerkiksi jakamistalous tai lainsäädäntö.



Digitalisaatiosta voi syntyä myös haittoja. Liiketoiminnan kannalta nämä voivat syntyä useasta syystä, esimerkiksi:

- Käyttöliittymän parantaminen siihen pisteeseen, että se tuhoaa kannattavuuden. Asiakas saa tästä paljon lisäarvoa mutta ei itse liiketoiminta
- Winner takes it all -talouden edistäminen, joka on synonyymi monopolille. Kehitystyö alalla johtaa siihen, että lopulta alalla on yksi toimija, joka hallitsee digitalisaation avulla kokonaan tai lähes kokonaan markkinaa kuten Google tai Airbnb

• Huono ymmärrys digitalisaation synnyttämistä toimintakokonaisuuksista
• Prosessien päällekkäisyyksien huomiotta jättäminen (vanha manuaalinen prosessi kuluttaa edelleen resursseja, ja prosessit vain toisinnetaan digitaaliseen ympäristöön)

Digitalisaatiosiirtymäkään ei ole ihan triviaali:
* On lähdetty ratkaisemaan liian suurta kokonaisuutta kerralla
• On lähdetty digitoimaan ja digitalisoimaan nykyinen toiminta miettimättä onko nykyinen toimintatapa (prosessit) oikein
• Ei ole ymmärretty mitä digitalisaatiolla voi oikeasti saavuttaa. Digitalisaatio ei yksin ratkaise mitään
• Ei ole kirkastettu, mitä digitalisaatiolla yritetään ratkaista. Mikä on ongelma tai parannustarve, johon haetaan ratkaisua
• Käytössä olevan tiedon laatu ei mahdollista digitalisaation hyötyjä. Oma ydintietojen hallinta ei ole kunnossa (masterdata) tai toimitusketjun muiden kumppanien tieto ei mahdollista toimintaa

Ja lopuksi tietysti virtuaalisen toimintaympäristön turvallisuus.

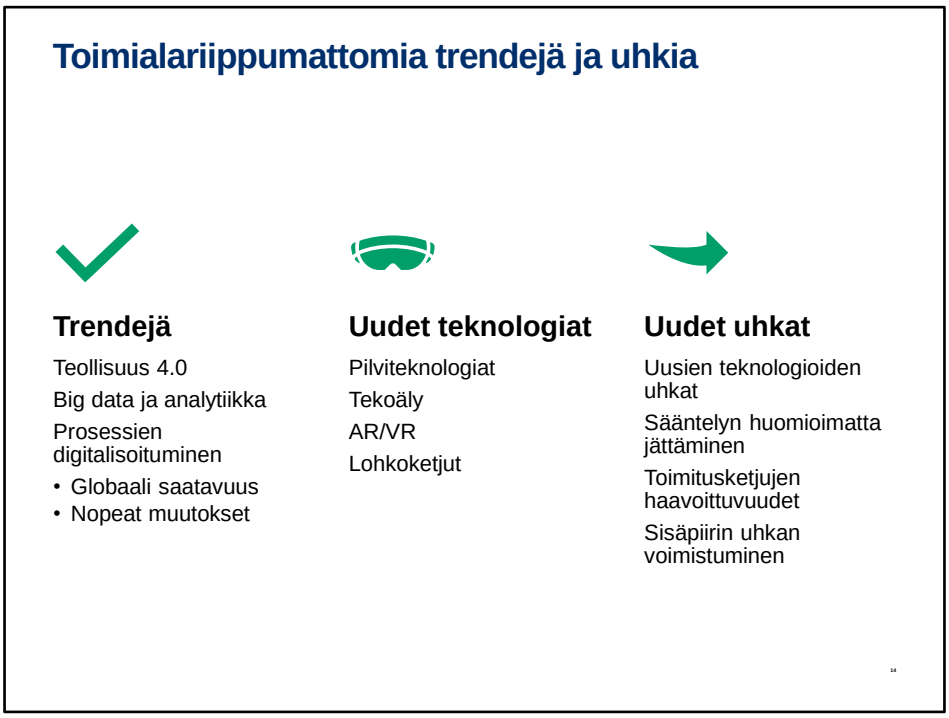
Fyysisen ja virtuaalisen ympäristön turvallisuusolettamat

- **Omaan liiketoimintaympäristöön on muiden vaikea päästä**
  - ... jos sattuu pääsemään, niin aina jälki jää
  - ... jos jotain viedään, sen huomaa helposti
  - ... syyllinen on varmaan paikallinen pikkurikollinen, tai ei varmasti ainakaan vielä ehtinyt rajan yli
- **Tuotantolaitteiston haltuunotto on fyysisesti vaikeaa**
- **Tuntemattoman henkilön henkilöllisyys on helppo varmistaa**
- **Kun on kerran tavattu, henkilöllisyys on vielä helpompi todeta (esim. kasvoista)**
- **4000km päässä on sota. Huono juttu, mutta ei meillä ole siellä asiakkaita.**

13

Ihminen tekee luonnostaan tiettyjä oletuksia turvallisuudesta havainnoidun ympäristön perusteella. Luonnollinen havainnointi vain rajoittuu fyysiseen maailmaan, ja kaikki ne turvallisuusolettamat, jotka pätevät fyysisessä ympäristössä, eivät joko päde virtuaalisessa ympäristössä ollenkaan, tai ovat löyhemmin toisissaan kiinni kuin fyysisessä ympäristössä.

Virtuaalisen ympäristö on rakennettu oletuksena niin, että eri järjestelmiin on pääsy kaukaa helposti, ajattelematta aluksi sitä, että sama pätee niin oikeutetuille kuin luvattomillekin käyttäjille. Reiät on ikäänkuin puhkottu jo valmiiksi, ja nämä pitäisi kyberturvallisuudella muuttaa lukollisiksi oviksi.



Monet digitalisaation mukanaan tuomat kyberturvallisuuden kannalta merkitykselliset trendit, teknologiat ja uhat ovat samankaltaisia suurimmalle osalle organisaatioista ja yrityksistä.

Trendeistä tämän kurssin toimialoihin vaikuttaa mm. nk. teollisuus 4.0., joka sisältää esimerkiksi teollisuusautomaation ja teollisten prosessien viemisen pilveen; Big Datan kerääminen ja sen analysoinnin mahdollisuudet liiketoiminnan optimoinnissa ja edelleen kokonaan uusissa liiketoimintamahdollisuuksissa. Big dataan sisältyy erityisesti mahdollisuus ja tarve monitoroida liiketoimintaprosesseja ja –ympäristöjä jatkuvasti niin, että se tuottaa digitaalisiin järjestelmiin yhteensopivaa ja luotettavaa tapaa. Jos bisnes on kokonaan virtuaaliympäristössä tämä on tyypillisesti pääasiassa teknologioiden yhteensopivuushaaste, mutta esimerkiksi huolinnassa, varastologistiikassa ja kaupan alalla fyysisten tuotteiden käsittely vaatii yhä monipuolisempia monitorointimenetelmiä: kameroiden tulee kyetä liikkumaan ja fyysiset paketit tai tuotteet tunnistaa automaattisesti. Tällöin esimerkiksi tekoäly ja robotiikka tulevat mukaan kuvioihin.

Itse liiketoimintaprosessitkin digitalisoituvat. Tämä tarkoittaa tiettyjen päätöspisteiden muuttumista kokonaan automaattiseksi, globaalia

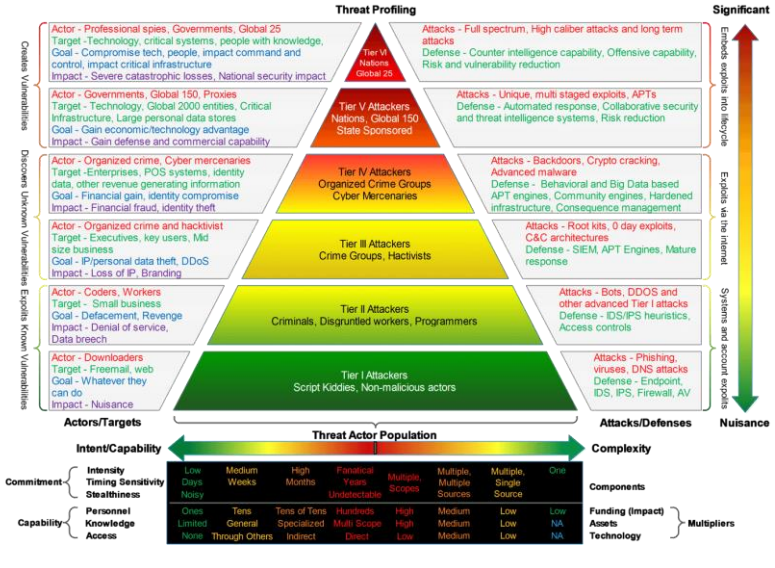
ulottuvuutta, ja nopeampaa sekä herkempää reagointia liiketoimintaympäristöön, kuten sääntelyyn, kilpailutilanteeseen ja markkinoiden liikkeisiin. Digitalisoidut prosessit ovat kylläkin tiettyjen sääntöjen puitteissa nopeita ja joustavia, mutta tarvitsevat joko hyvin mietityn sääntökannan tai oppivia tekoälykomponentteja.

Digitalisaatio liiketoiminnassa ei kykene toimimaan ilman tiettyjä avainteknologioita. Näitä ovat ensisijaisesti tekoäly ja pilviteknologiat. Tämän kurssin toimialoilla AR/VR sekä lohkoketjut näyttelevät myös toimintaa tehostavia tai varmentavia rooleja; kaupan ja rahoitusalalla lohkoketjut voivat muuttaa maksujärjestelmiä radikaalistikin.

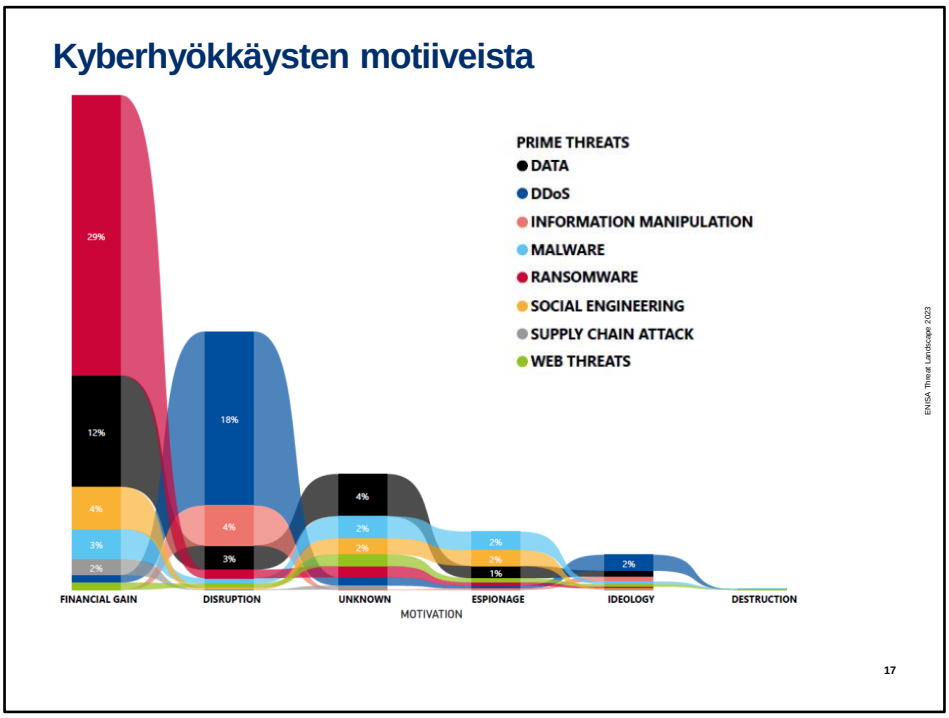
Kyberturvallisuuden trendejä

Globaali uhkatilanne

Kybertoimintaympäristön uhkatekijät

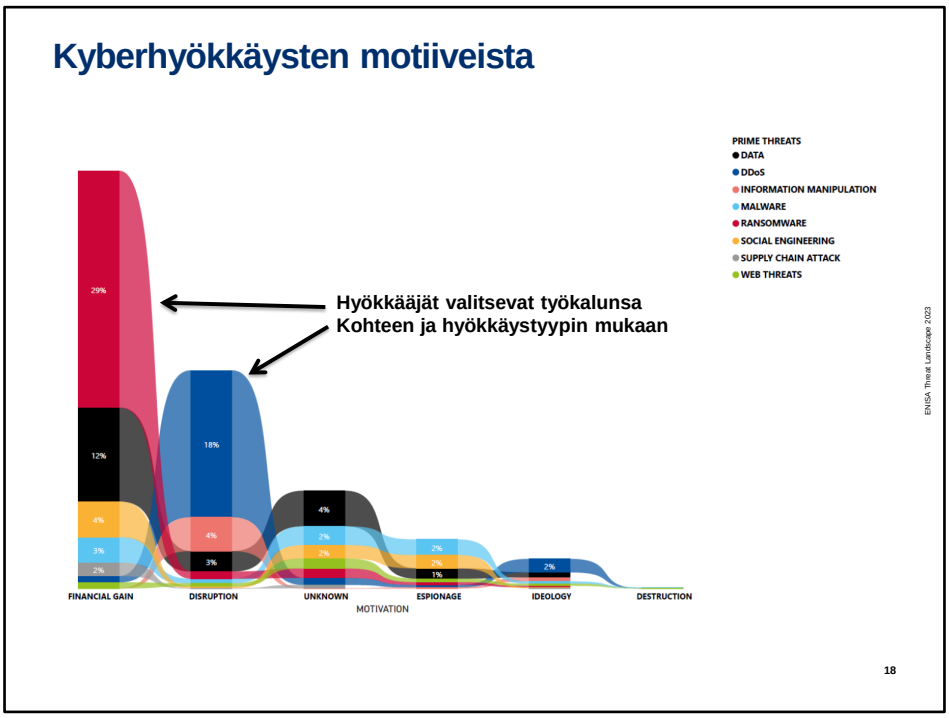


Kybertoimintaympäristö on monimutkaistunut valtavalla vauhdilla ja momentilla. Siinä, missä 1990-luvulla yksittäinen viruksen koodaaja edusti alan huippua, nykyisin haitallinen kybertoiminta muodostaa kokonaisia ekosysteemejä ja valtiollisia teollisuudenhaaroja; kyberhyökkäyksiä voidaan käyttää osana yhteiskunnan lamauttamista, teollisuusvakoilua tai laajoja huijaus- tai kiristyskampanjoita. Kaikkea vastaan on mahdoton puolustautua, mutta kaikkea vastaan on myös mahdotonta hyökätätään – tällöin on tärkeää, että rima on joka paikassa edes vähän korkeammalla kuin muualla. Uhkatoimijoiden kompleksisuuden vuoksi puolustuksessa on noudatettava järjestelmällisyyttä ja organisaation laajuista riskienhallintaa.

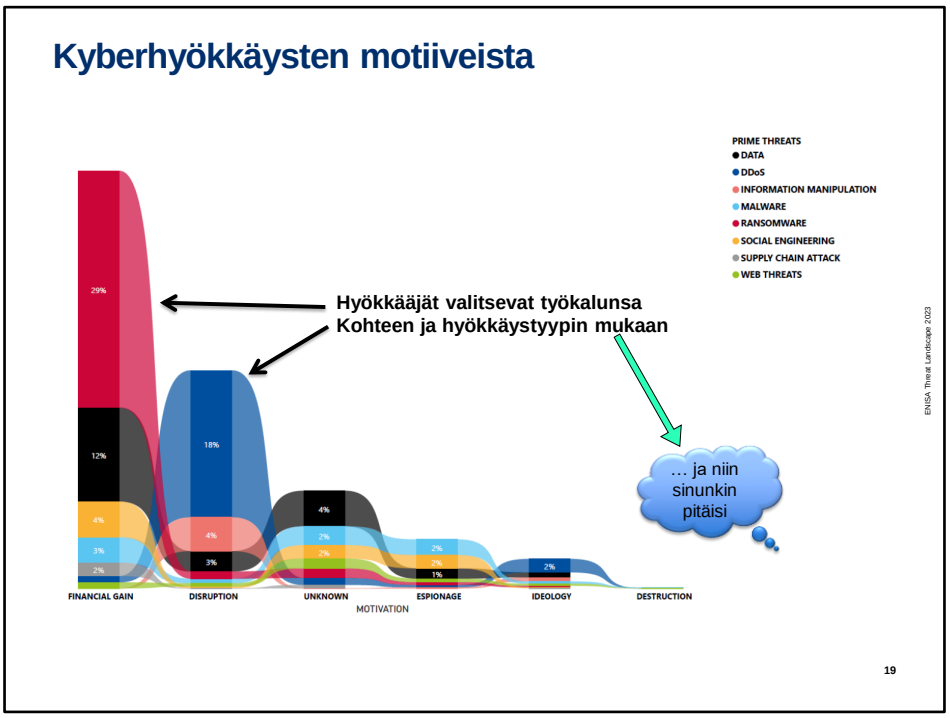


Euroopan Unionin kyberturvallisuusvirasto, ENISA (EU Network and Information Security Agency) pitää lukua kyberhyökkäyksistä vuosittain ja analysoi niitä vuosittain sekä globaalisti että EU:n tasolla ja toimialoittain. Kyberhyökkäysten motiiveissa rikolliset motiivit näyttäytyvät päällimmäisenä, joskin nykyisin valtiolliset motiivit menevät helposti päällekkäin rikollisten kanssa. Kolmas kyberhyökkäysten tekijätyyppi valtiollisen vaikuttajan ja rikollisten lisäksi on yleensä listatty haktivismi, mutta kuten tästä tilastosta näkyy, ideologiset motiivit ovat varsin pienellä prosentilla.

Kybertapahtumista ei ole usein edes helppoa selvittää motiivia, johtuen inhimillisten virheiden tuottamien tapahtumien runsaasta päällekkäisyydestä kyberhyökkäysten kanssa.

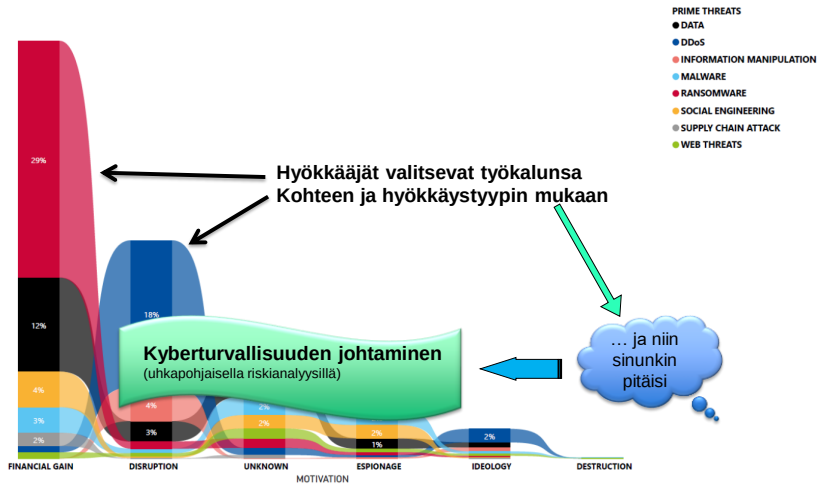


Hyökkäyksissä on huomattu motiivikohtaista tiettyjen työkalujen suosiota, esimerkiksi lunnashaittaohjelmia rahallisesti motivoiduissa hyökkäyksissä ja hajautettujen palvelunestohyökkäysten käyttöä pelkässä haitanteossa.



Koska hyökkääjä valitsee työkalunsa tapauskohtaisesti, niin myös puolustajan pitäisi tehdä niin.

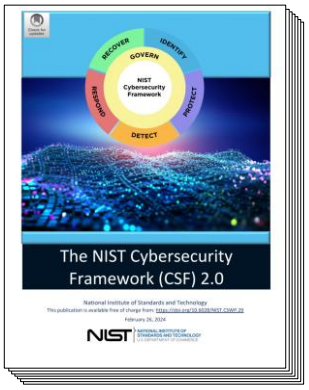
Kyberhyökkäysten motiiveista



20

Tästä tullaan kyberturvallisuuden johtamiseen uhkapohjaisella riskianalyysillä.

Kybersuositusten muutos

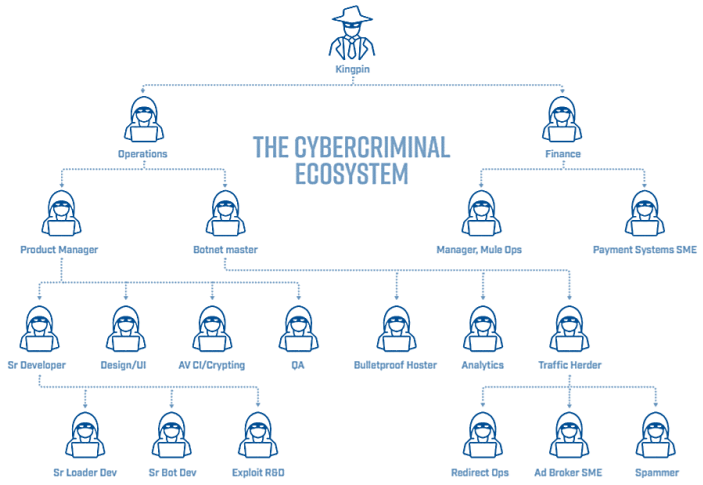


21

Kaksi Suomen kannalta tärkeintä kyberturvallisuuden suositusta on viimeisen viiden vuoden aikana muuttunut tietyllä tavalla ja samaan suuntaan. Toinen on USA:n teknologiastandardoinnin organisaatio, NISTin kyberturvallisuuden yleinen hallintakehikko CSF ja toinen Suomen kansallisen virallisen turvallisuusviranomaisen auditointityökalu, johon on koottu varsin kattavasti myös kyberturvallisuudesta tarkastettavat asiat.

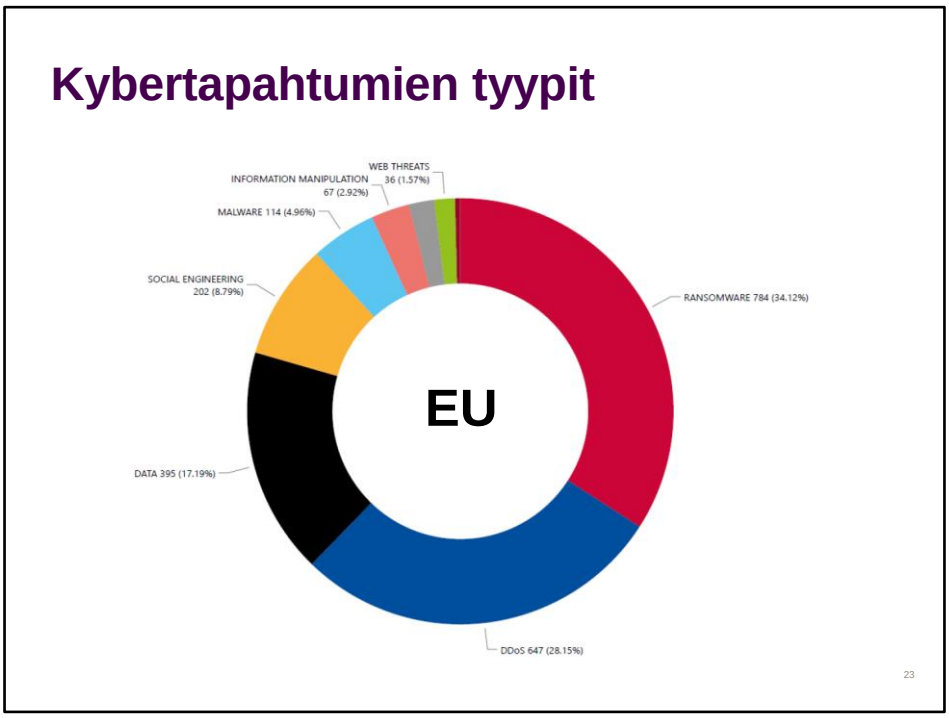
Kummassakin dokumentissa turvallisuus*johtaminen* / Governance on nostettu erilliseksi alueeksi muiden rinnalle, ja teknisiä kriteerejä on siirretty enemmän taustalle. Tämä on välttämättömäksi nähty toimenpide kyberhyökkäysten monipuolistumista ja laaja-alaistumista kohtaan.

Kyberhyökkäysten ekosysteemit



22

Nykyinen kyberuhkatekijä ei koostu muutamasta kybernerosta rokkistarasta, vaan usean eri osaamisalueen tekijästä, joita johdetaan kuin mitä tahansa organisaatiota ohjelmistonkehitysosastoineen ja rahoituspalveluineen.



Ohessa on esitetty ENISAn viimeisimmän uhkaraportin mukainen kuva tämän hetken yleisimmistä kyberuhkista.

- Lunnashaittaohjelmien käyttäminen suoranaiseen kiristykseen ja myös valtiollisessa vaikuttamisessa järjestelmien lamauttamiseen on suosituinta.
- Myös “perinteistä” lamautushyökkäystä (DDoS) voidaan käyttää varsinaisen tarkoituksensa lisäksi myös kiristykseen.
- Tietovuodot (“Data”) ovat paitsi kyberhyökkääjien ekosysteemin polttoainetta, myös eräs kiristyksen muoto
- Sosiaalinen hakkerointi, eli käyttäjän manipulointi / huijaaminen ovat merkittäviä erityisesti verkkokaupan väärinkäytöksissä.

Yleisiä trendejä (1v)

- Painopisteen siirtyminen vaikuttamisesta kybervakoiluun
  - Pääasiassa Iranin ja Venäjän toimien johdosta
- Kriittinen infra kohteena (pääsyn varmistaminen)
- Informaatiovaikuttaminen kybertilan manipuloinnilla
  - AI:n käyttö lisääntyy (fake ja deepfake)
- Jakoviivojen hämärtyminen toimijoiden ja tekotapojen / motiivien välillä
- Teknologinen kompleksisuus lisääntyy
  - “Living off the land”
- Kyberpalkkasoturien määrä kasvussa

Yleisiä trendejä (1v)

- Nousevia länsimaille vihamielisiä kybertoimijoita:
  - Iran ja Pohjois-Korea
- Kiina keskittyy vakoiluun ja informaatiovaikuttamiseen
- Venäjä keskittyy NATOon
- Euroopassa Ukraina yleisin kohde
  - UK ja FRA seuraavat
- Euroopassa yleisin kohde ajatushautomot ja siviiliorganisaatiot (NGO)
- Yksittäiset henkilöt ja reunalaitteet kohteina (esim. etätyö, BYOD)

Yleisiä trendejä (1v)

- Tärkeimpiä kyberrikostrendejä:
  - CaaS (Crime-as-a-service) lisääntyminen
  - Impersonoinnin laatu kasvaa
  - Tiedon vuotamisella kiristäminen kasvussa
- Puolustautumisen trendejä
  - Yksityisten ja yleisten organisaatioiden yhteistyö
    - → rikollisten anonymiteetin tarve kasvaa
- Uusia taktiikoita:
  - Pilvipalveluiden käyttö DDoSin lähteenä
  - “Return-customers”

26

Ransomware: tiedostojen kopiointi toiselle koneelle ja sitten takaisin, jolloin itse haittaohjelmasta ei jää jälkiä kohdekoneelle
Return-customers: jo murrettujen järjestelmien uudelleen murtaminen pelkästään sen vuoksi, että perus-intel on jo olemassa

Valtiollinen toiminta: yleisiä trendejä

- Painopisteen siirtyminen vaikuttamisesta kybervakoiluun
  - Pääasiassa Iranin ja Venäjän toimien johdosta
- Kriittinen infra kohteena (pääsyn varmistaminen)
- Informaatiovaikuttaminen kybertilan manipuloinnilla
  - AI:n käyttö lisääntyy (fake ja deepfake)
- Jakoviivojen hämärtyminen toimijoiden ja tekotapojen / motiivien välillä
- Teknologinen kompleksisuus lisääntyy
  - “Living off the land”
- Kyberpalkkasoturien määrä kasvussa

27

Venäjä

- Kybervaikuttamisen resurssit kohdennettu Ukrainan sotaan (48% tapauksista 2023)
  - Ulkomailla Ukrainan KV-kumppaneiden häirintään ja vakoiluun (36% tapauksista 2023)
  - Vakoilun kiinnostuksen kohteena informaatiovaikuttamisen pohjatiedot: Ukrainan politiikka, puolustusapu ja sotarikosten tutkinta
- Informaatiovaikuttaminen:
  - Baltiaan ja Puolaan mm. pakolaiskysymyksestä
  - Mielenosoitusten tukeminen ja järjestäminen
- Haktivistien ja valtiollisten toimijoiden yhteistyö (“vuodot”)
  - “Maskirovka”

Ryhmiä
Seashell Blizzard / Sandworm; *GRU*
Midnight Blizzard / Cozy Bear; *SVR*
Star Blizzard / Callisto; *FSB*
Aqua Blizzard / Gamaredon; *FSB-Krim*
Cadet Blizzard / [uusi]; *GRU*
Forest Blizzard / Fancy Bear; *GRU*

28

Venäjä: GRU/Sandworm

- GRU:n (sot.tied.palv.) toimija
- Vastuussa monesta kriittisen infran häirintätapauksesta
  - Esim. Ukrainan sähköverkko 2015
  - Vesilaitokset USA, Ranska, Puola
- Usein “disrupt and deny”, eli puhdasta kybervaikuttamista

29

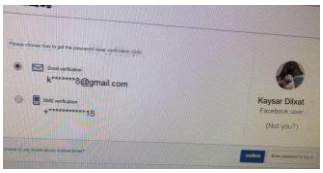
Kiina

- Kybervaikuttaminen Kiinan kommunistisen puolueen kontrolloimaa
- Pääasialliset kohteet: naapurimaat (erit.Taiwan), USA, strategiset kumppanimaat
- Kybervakoilua ja takaportittamista
- Informaatiovaikuttamisen kohteena kiinalaiset ulkomailla
  - Valetilit (tuhansia / kampanja)
  - Useat eri kielet (kymmeniä)
- Poliittinen vaikuttaminen ulkomailla (erit.USA): kansalaisten ja mediavaikuttajien impersonointi
- Trendi jatkuvaa myös 2024

Ryhmiä
Volt Typhoon / Bronze Silhouette
Raspberry Typhoon / Lotus Blossom
Flax Typhoon / [uusi]
Circle Typhoon / DEV-0322
Mulberry Typhoon / Keyhole Panda

Kiina: i-Soon/Fishmonger

- Kaupallinen kyber”turvallisuus”-yritys i-SOON
  - Ei tarvetta peitellä toimintaa (avoimia tarjouskilpailuja)
  - Keskimääräinen hakkerin palkka 1.000 € / kk
  - Oma “akatemia” (Anxun)
- Yhdistetty Fishmonger / Aquatic Panda / Charcoal Typhoon
- Sisäpiiriläisen tietovuoto i-SOONin toiminnasta
- Pääasiassa kybervakoilua kotimaan ja lähialueiden toimijoita vastaan (esim. uiguureita ja expateja)
- Myös ulkomaisia kohteita satunnaisesti
  - NATOssa: TUR, ROM, UK, FRA, NMC, BHG
- Laaja työkalusetti
  - Monelle eri käyttäjien osaamistasolle



Kuva: Murtautumista FB-kohteeseen salasana uudelleenasettamalla ja ilmeisesti verifikaatiokoodi Sieppaamalla (tekstit: Google kuvakäännös)

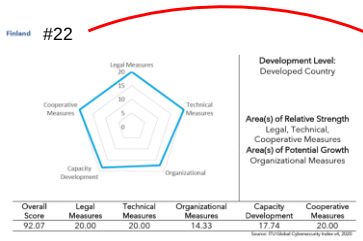
31

NMC = North Macedonia, BHG = Bosnia-Herzegovina,

Kyberturvallisuuden trendejä

Uhkatilanne Suomessa

Suomen kyberin tasosta



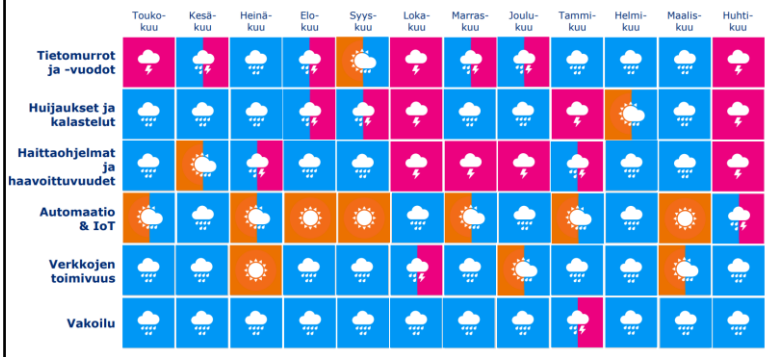
GCI, ITU

NCSI, Eesti

Yleistä kybersäästä

- Pääasiassa rikollisuutta ja valtiollisia toimijoita
  - Haktivismi pienessä roolissa, enemmän väitteitä kuin tapahtumia
  - Kyberrikollisuuden ammattimaistuminen ja “korporisaatio” (As-a-service)
- EU:ssa kyberhyökkäysten määrä 6x alkuvuodesta 2023 alkaen
- Globaalisti katsoen EU:hun kohdistuvien hyökkäysten suhteellinen määrä kasvussa
- Mobiilipäätelaitteiden perinteiset haittaohjelmat korvautuvat vakoiluohjelmilla
- DDoS ei katoa, vaan vaihtaa alustoja
- Kiinnostus toimitus- ja alihankintaketjujen hyväksikäyttöä kohti kasvaa
- Rahoitusala uudelleen kohteena, mm. sisäpiirihyökkäykset (Santander)

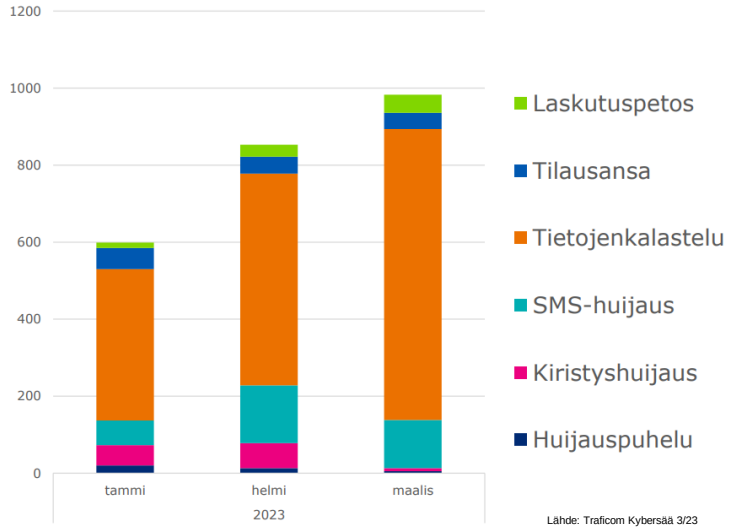
Hyökkäystyyppien trendejä



Traficom: kybersää 5/24

35

Kyberrikollisuudesta



Lähde: Traficom Kybersää 3/23

36

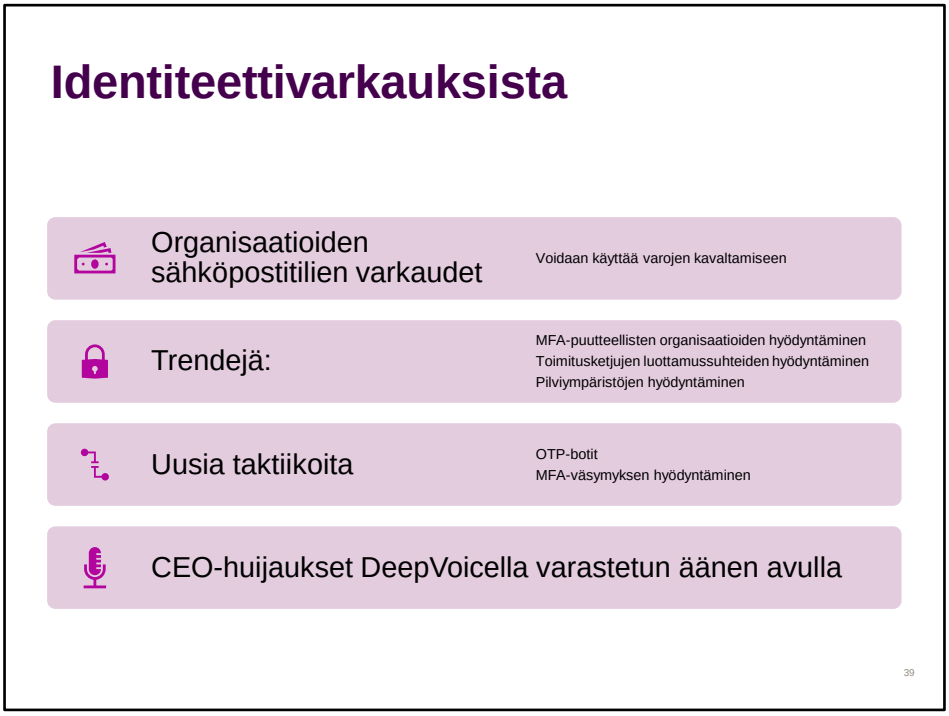
Lunnashaittaohjelmat

- 70% kohdeorganisaatioista < 500 hlö
- Kaksois- tai kolmoiskiristäminen (eri tahoilta):
  - Tiedon kryptaaminen
  - Tiedon vuotaminen
  - Palvelunestohyökkäys
- Murtautumisen kohteena erit. ylläpidon ulkopuolella olevat koneet, ja erityisohjelmistot
- Neljä haittaohjelmavarianttia vastuussa 2/3 tapauksista

Domain-huijaus

- Osoittaako linkki oikealle saitille?
  - Homoglyfit: *www.suomenpankkí.fi*
- Voitko luottaa, että linkki tuli oikeasti *ceo@mycompany.com*:ilta?
- Osoittaako N uudelleenohjausta sinne, minne piti? (Uhka nousujohteinen)
- Osoittaako linkki pilvessä olevaan aitoon dokumenttiin vaiko haittaohjelmaan?
- Lyhyet URL:t ovat käteviä? (Pysyvä uhka)

38



OTP-botit automatisoivat kertakäyttösalasanojen keruuta esim. AI:n avulla.
MFA-väsymys aiheutetaan pommittamalla uhria useilla MFA-pyynnöillä (yleensä tässä kohtaa uid/pwd on jo varastettu)