Kyberturvallisuus yksilön näkökulmasta

LUENTO – KYBERTURVALLISUUDEN UHAT JA SUOJAUTUMINEN

JAN ENLUND, TIETOTURVAPÄÄLLIKKÖ

Luennoitsija

Jan Enlund

Koulutus: M.Sc 2003, eMBA 2020, kyberturvallisuusinsinöörin opinnot menossa

Tausta: IT alalla vuodesta 1997, eli kohta 30 vuotta täynnä

Työpaikat: Teknillinen korkeakoulu, YLE, Elisa, TDC, Cinia, Loihde, Suomen Asiakastieto

Tehtäviä: Tutkimusapulainen, projektipäällikkö, tuotepäällikkö, palvelujohtaja, konsutti, kehitysjohtaja…

Nykyinen työ IT security manager ~ Tietoturvapäällikkö

Tämän luennon aiheita

Tietoturva ja sen tärkeys

Peruskäsitteitä

Uhat

Huijaukset ja miten niitä voi pyrkiä tunnistamaan

Mitä pahaa ei saisi tapahtua – Kuinka varautua?

Miten menetellä jos sitten kävikin kehnosti?

Suojausmenetelmät

Tietoturva ja sen tärkeys

NEWS | SCAMS

How AI was used in an advanced phishing campaign targeting Gmail users

Posted: February 13, 2025 by Pieter Arntz

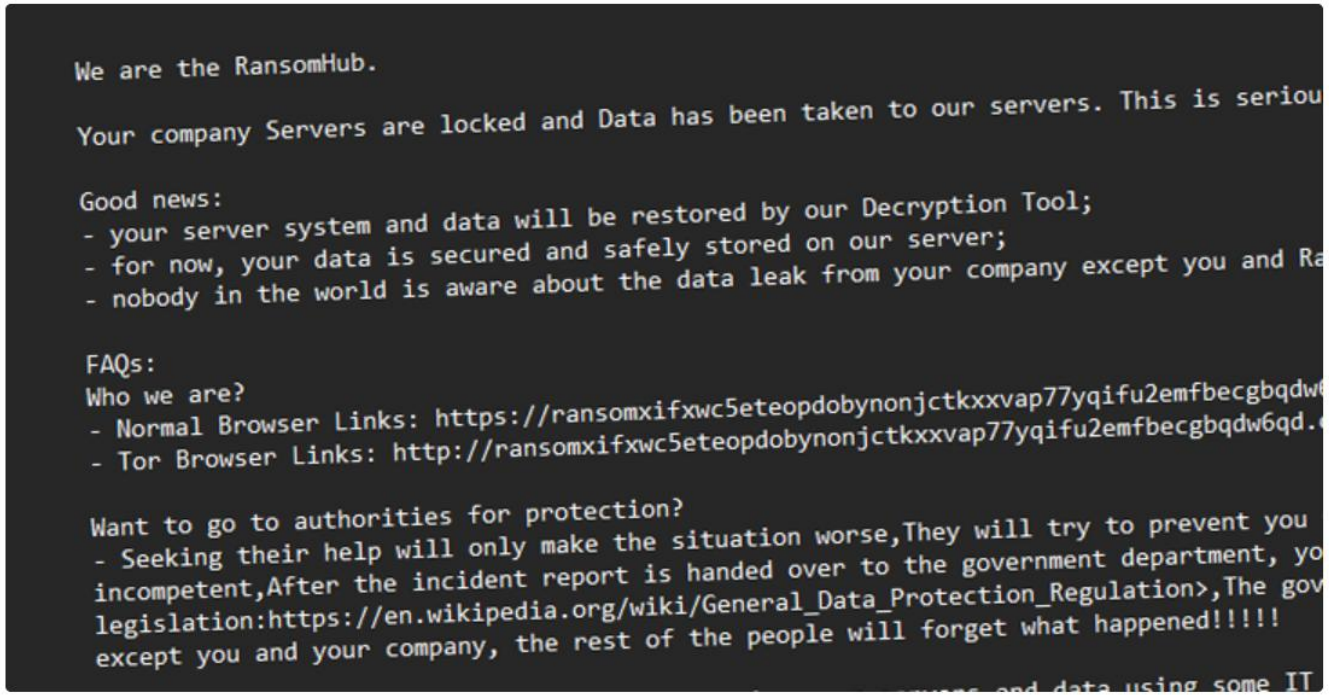
In May, 2024, the FBI warned about the increasing threat of cybercriminals using Artificial Intelligence (AI) in their scams.

At the time, FBI Special Agent in Charge Robert Tripp said:

Lähde: Malwarebytes 13.2.2025 [1.]

RansomHub Becomes 2024's Top Ransomware Group, Hitting 600+ Organizations Globally

Feb 14, 2025 Ravie Lakshmanan Ransomware / Network Security



The threat actors behind the RansomHub ransomware-as-a-service (RaaS) scheme have been observed leveraging now-patched security flaws in Microsoft Active Directory and the Netlogon protocol to escalate privileges and gain unauthorized access to a victim network's domain controller as part of their post-compromise strategy.

"RansomHub has targeted over 600 organizations globally, spanning sectors such as healthcare,

Lähde: The Hacker News, 14.2.2025 [2.]

Hackarnas hot: Läcker uppgifterna från Sportadmin om en vecka

PUBLICERAD 11 FEBRUARI 2025

Appen Sportadmin med över en miljon användare i idrotts-Sverige har hackats.
Nu hotar kriminella hackare att läcka alla personuppgifter, bland annat för barn med skyddad identitet.
– Gruppen vet om att det är det här de sitter på, säger DN:s techredaktör Linus Larsson.

Sportadmin används av idrottsföreningar i Sverige, bland annat för kallelser till träningar och kontaktuppgifter till medlemmar.

Lähde: SVT 11.2.2025 [3.]

DIGITODAY

Jos sait tämän kirjeen, tietosi on varmuudella viety

Tietomurto koskettaa kymmeniätuhansia suomalaisia.

JAA TALLENNA KOMMENTIT

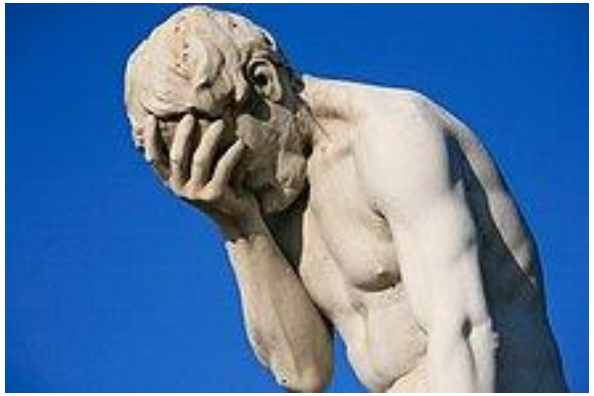
Valion eläkekassan toimitusjohtajan mukaan tietomurrosta kertovaa kirjettä ei ole voinut saada aiheetta. KUVA: RONI REKOMAA / LEHTIKUVA

Lähde: Digitoday 31.1.2025 [4.]

Tavallisia tietomurtojen syitä

1. **Haavoittuvuudet ohjelmistoissa**
2. **Päivittämättömät järjestelmät**
3. **Heikot tai varastetut salasanat**
4. **Tietojenkalastelu (phishing)**
5. **Haittaohjelmat**
6. **Puutteita verkkolaitteiden asetuksissa**
7. **Sosiaalinen manipulointi (social engineering)**
8. Palvelunestohyökkäykset (Distributed Denial of Service – DDoS)
9. Sisäpiirin uhat (insider threat)
10. Fyysinen pääsy järjestelmiin
11. Pilvipalveluiden asetusten puutoksia

[5., 6.] Lähde: ChatGPT ja Copilot



[Lähde: https://fi.wikipedia.org/wiki/Facepalm#cite_note-1]

Miksi tietomurtoja tehdään?

Raha – kyberrikollisuus on mailman kolmanneksi suurin talous.

- 2024 Kyberrikollisuus on arvoltaan 9,5 triljoonaa euroa! [Lähde: Esentire 2024]
- 2025 10,5 triljoonaa euroa [Lähde: Steve Morgan/Cybercrime Magazine 2025]

Tietoja – kiristykseen, myytäväksi…

Yrityssalaisuuksia ja patentteja sekä muita yritysvakoilun kohteita

Laskentateho

Uusi hyökkäyssuunta – toimittajaketjun kautta varsinaiseen kohteesen, asiakkaisiin tai vastaaviin

Kiusanteko

Haktivismi – hakkerointi ja aktivismi samassa

Kosto – vihaiset työntekijät, kilpailijat…

Valtiolliset toimijat – APT-ryhmä – Advanced Persistent Threat

Kyberrikolllisuus lyhyesti

Liiketoimintaa!

Ryhmät johdetaan kuten yrityksiä – mukana HR ja muut tukitoimet

- Kohteet ja tavoitteet
- “Liiketoimintalaueet”
- Omat alihankintaketjut – eri ryhmittymät/osaajat keskittyvät eri osa-alueisiin

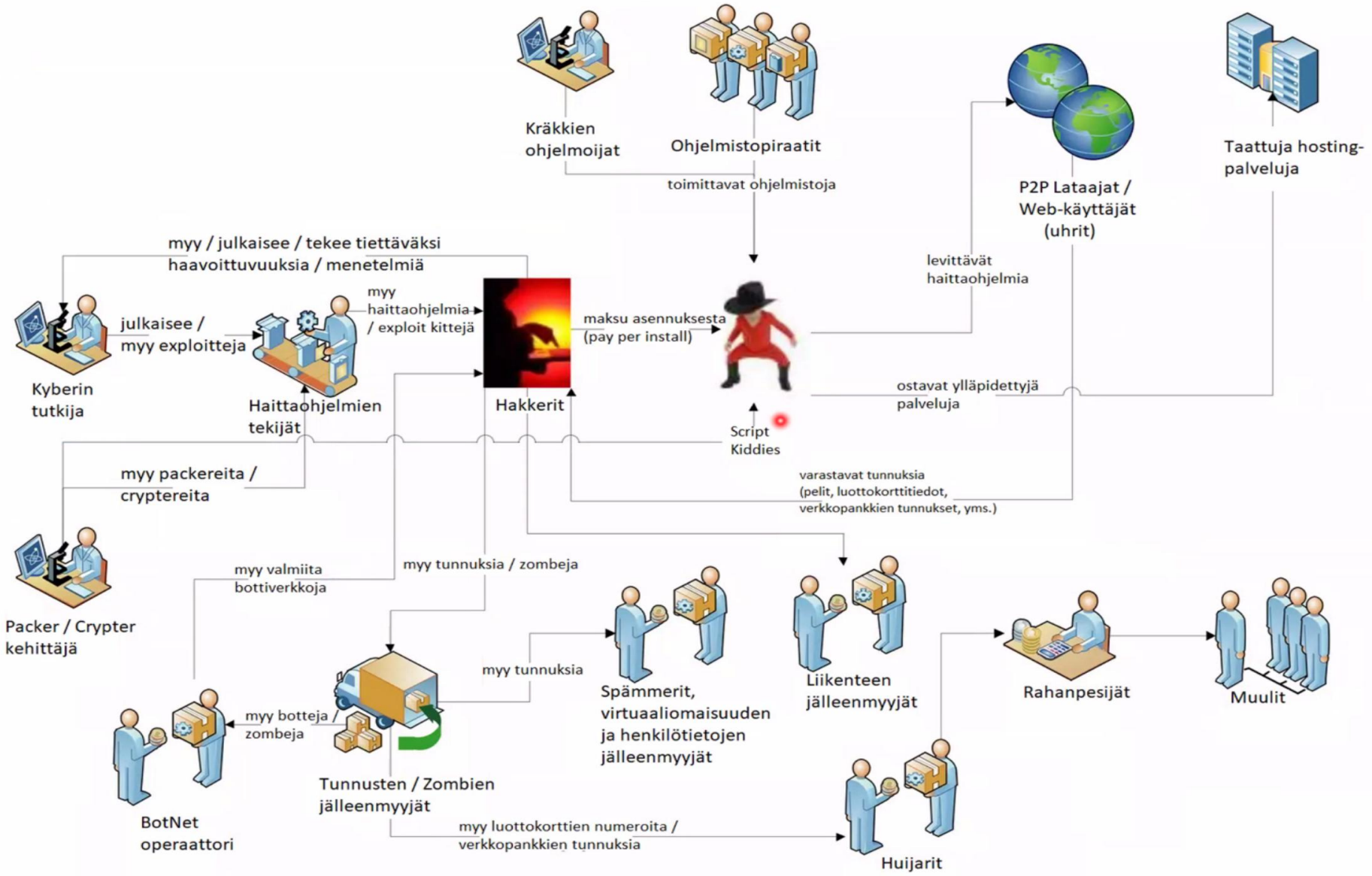
Tuomiot kohtuullisen vähäiset ja pieni kiinnijäämisen riski

- Toiminta ei välttämättä ole edes rikollista maassa, jossa rikolliset toimivat
- Rikollisia kannustetaan toimintaan kunhan se ei kohdistu maahan, jossa sijaitsevat

Laaja kirjo hyökättäviä kohteita

- Yhteisöjä, yrityksiä, valtioita, yksityiset henkilöt…
- Arviolta 20 miljardia laitetta Internetissä 2025 [Lähde: Naveem Kumar/DemandSage 2025]

Kyberrikollisten Ekosysteemi



Albert Hui (CC)

Lähde: Pätynen, Metropolia - Tietoverkkojen turvallisuus 2025

Miksi näistä pitää tietää ja ymmärtää?

Moderni yhteiskunta on riippuvainen digitaalisista järjestelmistä

- Mikä tahansa järjestelmä voi lähes million tajansa olla hyökkäyksen kohde

Kodit ja erityisesti me ihmiset olemme etenevässä määrin osa yhteiskunnan digitaalisia järjestelmiä ja niiden käyttäjiä

- Uhat kohdistuvat myös näihin järjestelmiin ja niissä oleviin tietoihin
- Henkilökohtainen tietoturva ja tietojen suojaaminen on tarpeen – identiteettivarkaudet, taloudelliset menetykset
- Turvata perhe ja lapset verkon vaaroilta – nettikiusaaminen, huijaukset, haitallinen sisältö
- Digitaaliset kansalaistaidot kyseessä ja ovat tarpeen myös työelämässä

Me käyttäjät ja meidän tiedot ovat kauppatavaraa – hyvässä ja huonossa

- “If it’s free – you are the tool” – Ei ilmaisia lounaita

Uhkia kohdistuu kaikkiin näihin osalueisiin - uhkia sekä suojautumista niitä vastaan käydään läpi tällä luennolla

Peruskäsitteitä

Peruskäsitteitä (1/2)

Tieto

- Dataa = bittejä, eli signaaleja, joita tulkitaan joko olevan 0 tai 1
- Informaatio = datan tietosisältö kuten tekstiä, kuvaa, videota...
- Tieto = informaation merkitys ihmiselle

Tietosuoja = lakisääteinen vaatimus suojata arkaluonteisia tietoja (henkilötietoja) väärinkäytöksiä vastaan

Tietoturva = Suojataan tiedot eri järjestelmissä eri tekniikoita käyttäen, esim henkilötiedot, yritystiedot, yrityssalaisuudet, ohjaustiedot…

Kyberturva = suojataan ihmisiä digitaalisten järjestelmien vaikutuksilta ja toisin pain

Lähde: Kiravuo, Timo. Kyberturva 2024 [8.]

Peruskäsitteitä (2/2)

Haavoittuvuus

- Virhe, heikkous tai vastaava tuotteen tai palvelun suunnittelussa, joka mahdollistaa hyväksikäytön pahat mielessä

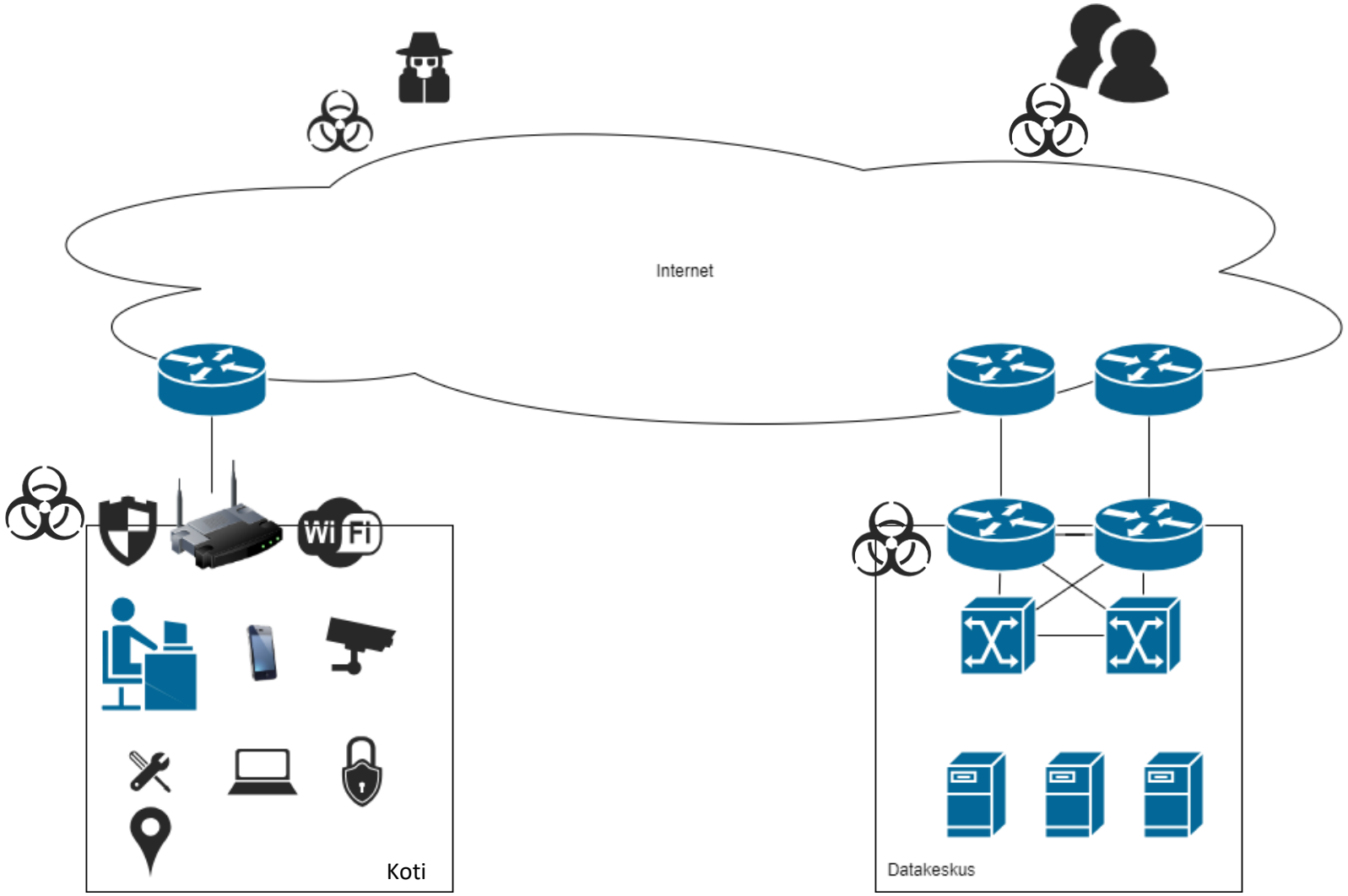
Uhka = jokin epätoivottu tapahtuma, skenaario, jolla on negatiivisa seuraamuksia. Uhkatekijä voi olla ihminen, sääilmiö, sota..

Riski = mahdollinen tappio tai vahinko, joka voi tapahtuma mikäli uhka toteutuu

Hyökkäys = Tilanne jossa hyökkäjä koittaa erilaisin keinoin saada luvaton pääsy kohdejärjestelmään tai kohdejärjestelmän tietoihin

Verkkohuijaus= Petos joka tapahtuu internetin välityksellä

Erilaiset uhkakuvat



Uhkia on monenlaisia ja usealla eri osa-alueella

Uhkia eri tasoilla

Palveluntarjoajat
- Tiedostot
- Sähköpostit
- Kalastelu
- Haavoittuvuudet

Verkko
- Verkkolaitteet
- Verkkoprotokollat
- Haavoittuvuudet

Laitteet
- Haavoittuvuudet
- Päivittämättömät laitteet
- Laitetyypit: koti vs yritykset, IoT

Muut käyttäjät
- Varomattomuus – luottosuhde ystäviin
- Sähköpostit
- Sosiaalinen media

Oman perheen laitteet ja käyttäjät
- Haavoittuvuudet
- Ohjelmistot, haittaohjelmat, tiedonkalastelu, tietojen varkaudet
- Laitesuojaukset

Omia tietoja koskevat uhat
- Luottokortit
- Henkilötiedot
- Perhetiedot
- Työtiedot

Kodin tietoliikenne/verkkolaitteet

Pääosin komponentit ovat samoja kaikissa verkossa, niiden tehokkuus, kytkentäkapasiteetti ja ominaisuudet kuitenkin vaihtelevat

Reititin – router – sananmukaisesti reitittää liikennettä eri laitteiden välillä, yleensä verkkojen välillä (esim. lähiverkosta internetiin)

Kytkin – switch – yhdistää liikennettä saman verkon sisällä

Tukiasema – Access point – Langattoman verkon kytkentäpiste, jonka toimintaa voisi verrata kytkimen toimintaan

Modeemi – modem – laite joka toimii hiukan kuin reititin, kuitenkin muutaen signaaleja tietoliikenneverkon ymmärtämään muotoon (analogiset modeemit, ISDN modeemi, xDSL modeemi, kaapelimodeemi – nykyään enää xDSL ja kaapelimodeemit käytössä)

Palomuuri – firewall – laite tai ohjelmisto joka tarkkailee tietoliikennettä ja suodattaa sitä eri keinoin

NAS – Network Attached storage – tiedontallennusjärjestelmä joka liitetään lähiverkkoon, vaikka kuvien, videoiden tallettamiseksi

IoT- Internet of Things laitteet – videovalvonta, älytermostaatteja, älyvalaistus robotti-imuri, ilmalämpöpumppu, television, yleensä pieniä erikoistuneita laitteita elinympäristön hallitsemiseen

IDS/IDP – Intrusion Detection System/Intrusion Detection and Prevention System – tietoliikenteen syvälliseen seurantaan ja hyökkäysten estämiseen tarkoitettuja järjestelmiä. Riisuttu malli löytyy uusimmista reitittimissä esim tekoälyllä toteutettuna

Lääkinnälliset laittet – CPAP, lääkerobotti ja vastaavat voivat tarvita verkkoyhteyksiä

Kodin reititin + WLAN tukiasema ja kytkin samassa
Lähde: https://www.gigantti.fi/_next/image?url=https%3A%2F%2Fmedia.elkjop.com%2Fassets%2Fimage%2Fdv_web_D1800010021602702&w=1200&q=75

8-porttinen hallitsematon kytkin
Lähde:https://cdn.broman.group/api/image/v1/image/DC3F5AB9E3E2A975081E70869072C78032504903.tp-link-tl-sg108-kytkin-47-6785.webp

Verkkolevy/tallennuspalvelin NAS
Lähde:https://cf-images.dustin.eu/cdn-cgi/image/fit=contain,format=auto,quality=75,width=828,fit=contain/image/d2000010011186855/synology-diskstation-ds223-nas-ja-tallennuspalvelimet-ty%C3%B6p%C3%B6yt%C3%A4-ethernet-lan-rtd1619b.png

Vanha modeemi
Lähde: https://www.clickitdirect.com/product/9600-bps-v-29-synchronous-and-asynchronous-modem/

WiFi tukiasema/toistin
Lähde: https://cdn.verk.net/kuvastin/w:1632/h:1020/rt:fit/q:80/sh:0.5/plain/images/9/2_259379-264x388.jpeg

Palomuuri
Lähde: https://cdn.verk.net/kuvastin/w:1632/h:1020/rt:fit/q:80/sh:0.5/plain/images/83/2_817462-784x412.jpeg

Wifi/Blutooth pistorasia

Lähde: https://pricespy-75b8.kxcdn.com/product/standard/280/10273984.jpg

Wifi/Ethernet valvontakamera

Lähde: https://static.elisa.com/v2/image/2tqybbhjs47b/3cz4J4Vq4NvacfX9kmqsmT/Tapo+C520WS+valvontakamera.jpeg?w=800&fm=avif&env=master&q=75

Wifi/Bluetooth/Zwave/Zigbee etäohjattava termostaatti

Lähde: https://www.netrauta.fi/media/catalog/product/cache/aafae4742beaf3b5b0bf669c071f6b10/N/E/NED-ZBHTR20WT_1.jpg

Wifi/Zwave/Zigbee älylamppu

Lähde: https://media.power-cdn.net/images/h-657941ebbe10ec5f270decf42573a946/products/1930694/1930694_7_900x900_t_g.webp

Wifi lääkerobotti

Lähde: https://www.uusiteknologia.fi/wp-content/uploads/2018/11/evendos_laakerobotti_www-600x475.jpg

Wifi/Blutooth älykello

Lähde: https://media.elkjop.com/assets/image/dv_web_D180001283463127

Kodin verkkolaitteet

Yleensä kuluttajille suunnatut verkkolaitteet ovat yhdistelmä edellisen kalvon laitteista

- Nykyaikainen WiFi-reititin usein sisältää 4-5 kytkinporttia – johon laitteet kytketään kaapelilla
- Sisältää WiFi tukiaseman – johon laitteet kytketään langattomasti
- Sisältää reititinosuuden – mikä reitittää WiFi:stä ja kytkinporteista ulos laitteesta tietoliikenneoperaattorin laitteelle – vaikkapa kuitupäätelaitteelle
- Uusimmat laitteet sisältävät usein myös palomuuritoiminnallisuuksia tai edistyksellisempiä tietoturvaratkaisuja

Laitteet usein massatuontoa, jotka rakennettu mahdollisimman edullisesti

- Komponentit usein vakioidut halpatuotannon komponentteja
- Laitetuki vain rajoitetun ajan (2-4 vuotta), laitepäivitykset saatavilla hitaasti uusien uhkien ilmaantuessa
- Perustuvat monesti muokatun Linux-ytimen ympärille (yleensä BSD Linux)

Mitä tietoliikennelaitteet sisältävät?

Ohjelmistoa ja komponentteja!

Keskusyksikkö – CPU (Central Prosessing Unit) suorittaa ohjelmia ja prosessoi tietoja

Muisti – Memory – Tieto tallennetaan lyhyt- tai pitkäkestoisieeen muistiin – työmuisti katoaa kun virta katkaistaan

Erilaiset muut järjestelmät (I/O) – input ja output yhdistävät laitteen maailmaan

Verkko-osuus – eri verkkoteknologian piirit/alijärjestelmät jolla kytkeydytään ko. Verkkotekniikan verkkoon

Perusasiat kuntoon!

Päivitä, päivitä ja päivitä! Pidä laitteesi ajan tasalla - aina!

- Tietoliikennelaitteiden laitteistopäivitykset – firmware update. Löytyy valmistajien sivuilta
- Tällä hetkellä laitevalmistajien tuki loppuu useimmiten 2-4 vuoden sisään laitteen hankkimisesta – valitettavasti. Tulossa EU sääntely alkaen 2027, jossa laitetta tuettava elinkaarensa ajan (Kyberkestävyyssäädöt – CRA (Cyber Resilience Act) – astunut voimaan 12/2024)

Päivitä laitteet ja niiden ohjelmistot – ota käyttöön automaattiset päivitykset ja uudelleenkäynnistä laitteet aina päivitysten jälkeen

Vaihda aina käyttöön otettaessa laitteiden oletussalasanat

Suojaustoimenpiteet (1/2)?

Toimenpide	Termi laitteessa	Miksi	Ohjeita
1. Vaihda langattoman verkon nimi	SSID, service name, network name…	Poista laitevalmistajaan viittaavat nimet, koska auttaa hyökkääjiä	Älä nimeä verkkoa osoitteesi tai sijainnin mukaan. Älä myöskään nimeä laitetta käytön mukaan “Keskustie_IOT
2. Vaihda langattoman verkon salasana	WPA, WPAv2, network password…	Laitteiden oletussalasanat johdetaan laitteiston komponenteista ja voi antaa hyökkääjille etuja	Käytä riittävän pitkää salasanaa 10-16 merkkiä, käytä isoja/pieniä kirjaimia, numeroita ja erikoismerkkejä (jos laite tukee niiden käyttöä)
3. Tarkista laitteen päivitykset	Firmware upgrade, software version….	Uudemmat versiot korvaavat mahdollisia virheitä laitteiston ohjelmistossa	Uusimmat reitittimet tarkistavat päivitykset internetistä suoraan, vanhempien osalta voi joutua lataamaan päivityksen ensin tietokoneelle ja siitä laitteelle
4. Vaihda pääkäyttäjän salasana	Administrator password, admin password, root password…	Internet täynnä listauksia laitevalmistajien oletussalasanoista ja kirjautumistiedoista (IP-osoite missä hallintaan kirjaudutaan)	Tämä mikäli vastaat itse laitteen turvasta. Valitse tarpeeksi pitkä salasana, 12-16 merkkiä, käyttäen isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä
5. Poista etähallinta käytöstä	WAN management, remote management…	Asetus sallii etäyhteyden laitteelle internetistä pain	Tämä jos vastaat itse laitteen turvasta. Salli käyttö ainoastaan sisäverkosta (langallinen, langaton) tai jos uskot laitevalmistajan omiin etäratkaisuihin (TP-link, D-Link, Asus…)
6. Aseta automaattiset päivitykset käyttöön	Automatic updates, auto-update…	Asetus sallii laitteen päivittää itsensä automaattisesti	Tämä jos vastaat itse laitteen turvasta

Lähteet: Kybertuvalisuuskeskus, Suojelupoliisi, ja Federal Trade Commission [18., 19., 20]

Suojaustoimenpiteet(2/2)?

Toimenpide	Termi laitteessa	Miksi	Ohjeita
7. Aseta laite uudelleenkäynnistymään viikottain/päivittäin	Enable automatic reboot, device reboot, reboot schedule	Tyhjentää laitteen muistin ja pitää sen näin tehokkaampana. Myöskin siihen mahdolliset ladatut haitakkeet poistuvat. Poistaa myös usein laitteen “oireilua” esim. jos siihen päivän aikana kirjautuu paljon laitteita	Aseta käynnistymään uudelleen vähintään viikottain
8. Ota NAT (Network Address Translation)-toiminne käyttöön	Network Address Translation, NAT, firewall…	Piilottaa kodin laitteet operaattorin julkisen IP-osoitteen taaksi, vaikeuttaa hyökkäämistä yksittäiseen laitteeseen	Yleensä päälle/pois asetus
Seuraavat suositukset vaativat laitteen toiminnan syvällisempää ymmärrystä, mutta eivät sinsänsä ole hankallia			
9. Erottele laitteita omiksi verkoiksi	Guest network, IoT Network, Multiple SSIDs	Erottelee eri verkot toisistaan fyysisesti	Erottele omiksi verkoikseen etätyö, pelaaminen, IoT jos laite tukee tätä. Tämä voi vaati myös todennäköisesti laitteen DHCP osoitteiden asettamista per verkko
10. Ota käyttöön palomuurisääntöjä, AI sääntöjä tai muita edistyksellisiä toimintooja	AI enhanced firewall, AI Protection, Firewall, SPI firewall	Auttaa liikenteen suodattamisessa paitsi ulkoverkosta niin sisäverkossa	Nimitys vaihtelee valmistajan mukaan. Ominaisuudet saattavat vaatia tilauspalveluiden käyttöä (kk/vuositilaus) tai rekisteröintiä valmistajan sivuilla
11. Ota käyttöön SSL suojaus pääkäyttöliittymälle	Secure admin panel, ssl, https	Auttaa suojaamaan liikennettä selaimen ja reitttimien välillä	Nimitys vaihtelee valmistajan mukaan. Yleensä päälle/pois asetus
12. Laita loktitiedot päälle	Logging, logs, log management	Auttaa selvittämään tapahtumia virhetilanteessa	Laitteesta riippuen lokitietoja voi määritellä. Tässä kiinnostavat eniten käyttäjäkirjautuminen, mikä voi olla admin panel, admin interface tai vastaavalla nimityksellä oleva. Loktiedot kannattaisi ohjata lokipalvelimelle, tai vaikkapa NAS palvelimelle

Lähteet: Kybertuvalisuuskeskus, Suojelupoliisi, ja Federal Trade Commission [18., 19., 20]

Erilaiset hyökkäykset, huijaukset ja muut uhkakuvat

Verkkohuijausten eri tyypit

Phishing - tietojen kalastelu. Huijari lähettää sähköposteja tai muita viestejä, pyrkien saamaan ne näyttämään siltä että tulevat luotetulta taholta ja pyytää henkilötietoja/pankkitietoja/luottokorttitietoja/kirjautumistunnuksia

- **Vhishing** – Voice Phishing – Soitetaan uhrille ja esiinntynään viranomaisena tai olemattoman yrityksen edustajana
- **Smishing** – SMS phishing – Sama asia mutta tekstiviestistä, klikkaa linkkiä tai lataa vaarallinen sovellus
- **Spear phishing** – kohdistettu tietojenkalastelu. Hankittu etukäteen tietoja uhrista ja kohdistetaan hyökkäystä ja viestiä niiden perusteella.

Toimitusjohtajahuijaus – Huijari esiintyy yrityksen toimitusjohtajana ja pyrkii ohjaalmaan työntekijöitä tekemään maksusuorituksia tai paljastamaan tietoja. Yleisiä kesällä ja loma-aikoina

Haittaohjelmat

Ransomware – Haittaohjelma joka lukitsee (salaa) käyttäjien tietoja ja vaaditaan lunnaita tietojen vapauttamiseksi. Voidaan myös uhata tietojen julkistamisella jos lunnaita ei makseta

Troijalainen – haittaohjelma joka naamioituu hyödylliseksi tai harmittomaksi mutta tosiasiassa suorittaa haitallisia toimintoja järjestelmässä. Voivat varastaa tietoja, sallia etäpääsy (takaportti/backdoor), ladata muita haitakkeita laitteelle

Vakoiluohjelma - Spyware. Varastaa esimerkiksi näppäinpainalluksia, tietoja sivuista joilla käydään

Mainosohjelmat – Adware. Näyttää mainoksia hidastaen toimintaa ja yleensä keräävät tietoja selainkäyttäytymisestä. Ei enää niin yleinen kuin vielä 5-6 vuotta sitten

Cryptominer – Haittaohjelma joka käyttää järjestelmää louhiakseen kryptovaluuttoja, eri varastaa konetehoja ja sähköjä.

Botti – haittaohjelmalla saadaan luotua verkko erilaisia botteja, joita käytetään hyväksy massahyökkäyksissä. Botti yleensä toiminnallisuuksiltaa rajattu.

Rootkit – Ohjelma jolla saadaan pääsy järjestelmään ja joka osaa piiloutua erittäin hyvin

Puhtaat **virukset ja madot** ovat nykyään harvinaisempia, mutta muut haitakkeet sisältävät niiden perusominaisuuksia

Kauppahuijaukset

Verkkokauppahuijaukset – online shopping scam – Luodaan uskottavan näköinen verkkokauppa, joka myy olemattomia tuotteita tai joka varastaa maksutietoja. Tyypillisesti houkutellaan halvoilla brändituotteilla ja tarjouksilla – **jos se kuulostaa liian hyvältä ollakseen totta, se todennäköisesti ei ole totta!**

Sijoitushuijaukset – investment scams. Houkutellaan ihmisiä sijoittamaan suurilla tuotoilla ja yleensä jotakuta tunnettua ihmistä hyväksi käyttäen. Suomessa Wahlroos, Lipponen, Marin on hyödynnetty. **Jos se kuulostaa liian hyvältä ollakseen totta, se todennäköisesti ei ole totta!** Käytä mieluummin pankkien ja muiden vastaavien toimijoiden palveluita

Teknisen tuen huijaukset – tech support scams. Soitetaan tai ollaan yhteydessä pikaviestimen kautta ja yritetään uskotella soitettavan vaikka Microsoftin puolesta. Myös erilaisia pop-up ruutuja käytetään tässä hyväksi – väitetään vaikka koneessa olevan haitttaohjelma Palvelusta pitäisi maksaa tai annettava pääsy laitteeseen sen “puhdistamiseksi” Yleensä tällöin varastetaan pankki ja henkilötietoja (erityisesti jos ohjataan maksusivulle palvelun “maksamiseksi”). Tukiorganisaatiot eivät soita sinulle oma-aloitteisesti – ei ikinä!

Työpaikkahuijaukset – fake job offers. Löydät elämäsi työpaikan ja kaikki näyttää hyvältä, pääset haastatteluun ja ehkä jopa tapaat online useammankin ihmisen. Kuitenkin pyritään kahteen asiaan – huijataan sinulta henkilötiedot ja CV:n tiedot, sekä Saada sinut maksamaan esimerkiksi tullimaksu tietokoneesta tai ostosta. Usein käytetään myös erilaisia “rekisteröintimaksuja” joita tulisi maksaa työpaikan saamiseksi.

Lähde: Copilot, ChatGPT [9., 10.]

Tilausansat

Pyritään samaan huijattu tilaamaan jatkuva palvelu sitä ymmärtämättään tai tietämättään

Yleisiä tapoja:

- Ilmaisnäytteet – saat ehkä ensimmäisen tuotteen ilmaiseksi mutta sitten niitä tuleekin kuukausittain. Yleensä jatkuva luottokorttiveloitus, joka onnistuu koska piti maksaa vain ensimmäisen kerran postikulut kortilla
- Sovellusten ja pelien sisään piilotetut jatkuvat tilatukset – todella hankalaa löytää kohdat mistä perua tai saada katkaistua. Yleensä lapsia ja nuoria houkutellaan lataamaan peli, joka onkin sitten maksullinen jatkossa.
- Erilaiset epämääräiset suoratoistopalvelut – houkutellaan sovelluksen pariin jollain uuden elokuvan verukkeella. Ensimäinen elokuva ilmaiseksi! Ja sitten kuitenkin halutaan maksutiedot, josta tulee tyypillisesti kuukausiveloitteinen
- SMS tilausansat ovat samantyyppisiä, mutta saatkin tekstiviestin sähköpostin tai sovelluksen sijaan. Myös “voitit kilpailun, ole hyvä ja vahvista numerosi” ovat tyypillinen esimerkki tällaisesta huijauksesta
- Arpajaiset ja kilpailut – on kiva olla voittaja, mutta jos pitää antaa puhelinnumero tai luottokorttinumero tulisi hälytyskellojen soida

Lähde: ChatGPT [11.]

Myyntihuijaukset

Suomessa on paljon huijauksia tori.fi ja huuto.net palveluiden osalta

- Olematon ostaja
  - Halutaan tehdä kaupat Whatsappin, Signalin tai Discordin kautta
  - Myös ulkomaisia puhelinnumeroista yhteydenottoja → Mieti haluatko julkaista puhelinnumeron myynti-ilmoituksessa
- Halutaan että tuotteet lähetetään ennen maksua tai luvataan maksu, tai pyydetään vahvistamaan maksutapahtuma antamalla tietoja maksujen vastaanottamiseen → tiedot varastetaan
- Halutaan käyttää postin/torin/pankin turvallista maksutapahtumaa – ei ole olemassa tällaista palvelua! ToriDiili on ainoa tori.fin maksupalvelu → varovaisuutta käytettäessä

Tarkista palveluiden varoitukset niiden omilta tuki-sivuilta (tuki.tori.fi, huuto.net/ohjeet)

Vastaavia huijauksia myös muilla myyntisivuilla kuten Facebook Marketplace, Vinted, Ebay…Vertaiskauppaa tehdessä kannattaa olla varovainen!

Lähde: tori.fi [12.]

WhatsApp huijaukset

Facebookin omistama WhatsApp on yksi mailman suosituimmista pikaviestimistä, joten on luonnollista että siihen hyökätään. Huijauksilla pyritään kaappaamaan käyttäjien tilit tai saamaan rahaa

WhatsApp-päivityshuijaus – sovelluksessa lähetetään viesti jossa pyydetään linkin kautta lataamaan päivitys. Päivitys on kuitenkin haittaohjelma.

WhatsApp vahvistuskoodihuijaus – Viestillä kerrotaan että “vahingossa olen pyytänyt vahvistuskoodin sinun numerollasi omani sijaan. Voitko lähettää minulle sen koodin, kiitos?” Tämä siirtää WhatsAppin toiselle laitteelle ja menetät tilisi.

“Hei äiti, mun puhelin katosi ja käytän kaverini puhelinta” on yksi tapa, toinen on sama viestinä/tekstinä. Uusimpina tekoäly soittaa kertoen samaa. Tekoäly tarvitsee vain noin 30sek ääninäytteen kuulostaakseen uskottavasti toiselta, lisäten ääneen hätää, itkua…Hyökkääjä pyytää rahaa lippuu, uuteen puhelimeen…

Lähde: NordVPN [13.]

Facebook huijaukset

- Erilaiset kilpailut - “Olet voittanut, vahvista tietosi”
- Erilaiset sovellukset, sovellus joka vaikka kertoo mikä on sinun kääpiönimesi tai Smurffi-nimesi syntymäpäivän perusteella todennäköisesti varastaa henkilötietosi
- Sijoitus- ja tilausansat – yleensä mainostetaan tuotteita jotka ovat kyseenalaisia tai jossa luvataan kohtuuttomia tuottoja
- Äkkirikastumista lupaavat artikkelit
- Väärennetyt tuote- ja tilaussivustot – mainostetaan esimerkiksi kokeiluja tai käyttöä ilman luottokorttia
- Erilaiset yhteydenotot, viestit Facebook Messengerissä jossa kadonnut vaikka puhelin, yhteystiedot tai pyydetään vastaavasti koodia kuin WhatsAppin kanssa → riskinä tietojen ja tilin menetys

Lähde: Iltasanomat/Digitoday [14.]

Viranomaishuijaukset

Yhteydenottoja erilaisten viranomaisten nimissä: poliisi, poliisihallitus, Vero, KELA, Suomi.fi

Yleensä sisältävät linkkejä sivustolle johon hyökkäyskohde pyritään saamaan

- Pyydetään tunnistautumista → varastetaan henkilötietoja
- Pyydetään maksamaan jokin vähäinen maksu → varastetaan pankki- tai luottokorttitietoja
- Linkit väärennettyjä → tarkkuutta niitä tarkistaltessa

Viesteissä korostuu usein kiire tai nopeuden tarve

Viestien suomen kieli parantunut, ei voi enää tunnistaa huijaukset pelkästään niiden kautta

Paketti- ja kirjelähetykset

Yleisimmät käytetyt pakettivälitysyritysten nimisssä tapahtuvat huijaukset

- Posti, DHL, TNT, PostNord

Usein tekstiviesti tai sähköposti “Pakettisi jumissa”, “pakettisi toimitus” nimillä

- Sisältää linkkejä huijausivuille
- Sanotaan paketin olevan jumissa tullissa, tai että puuttuu osa maksusta

Tilaus- tai maksuansoja

- Varastetaan henkilötiedot ja maksutiedot

Rakkaus- ja romanssihuijaukset

Yleensä pitkäkestoisempi huijaus, jossa huijari rakentaa tunteiden kautta otteen huijattavasta	•Tavoitteena saada henkilötietoja ja rahaa – yleensä paljon rahaa nopeassa ajassa, kun siirrytään huijauksessa “kotiuttamisvaiheeseen”
Rakennetaan sopivia profiileja tapaamispaikoille tai seuranhakupalveluille, joskus myös ollaan yhteydessä suoraan pikaviestimillä ikään kuin vahingossa. Lääkäri, sotilas, leski…sopivilla kuvilla höystettynä	•Catfishing – esiinnytään väärennetyllä profiililla ja tiedoilla ja pyritään luoda läheinen yhteys uhriin •Love bombing – pyritään psykologisin keinoin kehumalla ja antamalla tunnustusta manipuloida uhri suhteeseen •Sotilasromanssi (tai lääkäriromanssi) – luodaan profiili, jonka poissaolo ja vaikea tavoitettavuus voidaan selittää sotilasuralla, lääkäriuralla ulkomailla tai vaikka öljynporauksessa työskentelyllä. Samalla luodaan tunne, että profiilin henkilö voi olla vaarassa, mikä myös kasvattaa kiintymystä nopeasti ja voidaan edetä suhteeseen nopeasti
Tyypillistä on tunteiden nopea kehittyminen ja niiden voimakas ilmaiseminen	•Rakkaus, kiintymys ja lupaus niistä yleensä koukuttaa uhrin •Tapaamista tai vaikkapa videokeskusteluja vältetään ja usein selitykset ovat tekosyitä kuten matkat, odottomaton työkomennus tai jokin henkilökohtainen ongelma
Rahoja pyydetään jossain kohden esimerkiksi hätätilanteeseen, kuten auton rikkoontumiseen, sairastumiseen (oma tai lähiomainen), liiketoimintaa varten tai yleisimmin matkustaakseen uhrin luokse	•Rahoja ei välttämättä pyydetä edes suoraan vaan kerrotaan esim. että odottamaton rahanmeno estää matkan “rakkaan” luokse •Pyytäjä voi myös olla hujauksessa mukana oleva kolmas henkilö – ollaan yhteydessä koska väitetysti on tapahtunut onnettomuus, jossa “rakas” on loukkaantunut. Vedotaan kalliisiin hoitoihin tai ambulanssilentoon, lakiasioiden sopimiseen tai muuhun rahojen saamiseksi

Lähde: Reader’s Digest, Anna, KuntoPlus [15. , 16., 17.]

Sosiaalinen manipulointi

Sosiaalinen manipulointi – Social engineering

- “Epärehellisiä keinoja, joilla rikollinen saa uhrin paljastamaan arkaluonteista tietoa tai toimimaan omien etujensa mukaan” – Wikipedia [18.]
- “Hakkeroidaan ihmistä” – Kasperksy [19.]

Eli pyritään saamaan uhri tekemään halutut toimet (esim lataamaan haittaohjelma), paljastamaan tietoja (esim käyttäjätunnus) tai antamaan käyttöoikeuksia järjestelmiin.

“Hyökkäystapoja” useita – puhelinsoitto, viestittely, tapaaminen kasvokkain, yllättävä tapaaminen parkkipaikalla – vain kekseliäisyys rajana

Perustuu ihmisten käyttäytymiseen, tapoihin ajatella sekä toimia. Auttamishalu, empatia, ahneus, halu tehdä oikein, syyttömyyden ylläpitämistä…syitä on lukemattomia miksi autetaan tai tehdään hyökkääjän pyytämät asiat

Seksivideohuijaukset

Yleisest kiristykset – “Valtasimme koneesi ja otimme kameralla sinusta videon”.

Uhataan jakaa video työpaikalle, ystäville jne ellei lunnaita makseta. Saatetaan myös lähestyä poliisin nimissä ja pyydetään maksamaan “sakko”

- Yleensä koko materiaalia ei ole edes olemassa
- Epätodennäköistä että tunnistettaisiin sähköpostiosoitteet, kotiosoite tai nimi videokuvan perusteella

Tämä eri kuin kuva- ja videokiristykset jossa uhataan levittää henkilön jossain kohden luovuttama arkaluonteinen materiaali

Muut – lyhyet maininnat

Pelit, pelihahmot ja pelien erilaiset aseet ja asusteet

- usein myydään olemattomia tilejä ja lisäominaisuuksia

Erilaiset piraattisovellukset ja lisenssikoodit

- voi toimia, mutta ei takeita ja käyttö hyvin riskialtista
- Kenties asennetaan laitteelle takaportti tai muu haittaohjelma

Ei suoraan huijauksia mutta sisältää riskejä:

- Laitteiden mikrofonit ja kamerat
  - Haittaohjelmat ja verkkosivut voivat käyttää näitä hyödyksi.
  - Lupien kanssa kannattaa olla tarkkana! Annettuja käyttölupia voi tarkistella asetusten kautta
- Älykodin laitteet
  - voisiko osaa käyttää paikallisesti (kodin sisällä) eikä liittää nettiin?
  - Suositeltavaa käyttää isoja tunnettuja laitevalmistajia, jotta saa laitepäivityksiä ja palvelua jos jotain meneekin mönkään.
  - Laitteiden turvataso monesti heikko, eikä välttämättä ole eduksi lähettää esimerkiksi suoraa videokuvaa kotoa internetiin.
  - Erilaisia IoT laitteita voi hakea esim Shodan hakukoneella (shodan.io)
- Dark web/Dark internet
  - Verkon “pimeä” puoli - tarjolla jos jonkinmoisia haittaohjelmia, skriptejä, tietoja
  - Rikollisten käyttämiä sivuja joista herkästi myös tartutetaan varomatonta käyttäjää haitakkeilla

Nyt tiedämme huijauksista – mutta miten suojaudumme?

Suojautumisen perusteita

Kybersuojautumista voi pohtia useista eri näkökulmista mutta tehokkainta on yleensä miettiä kahta asiaa:

1. Mitä tärkeää, arvokasta minulla on – mitä minun kannattaa suojata?

2. Mitä pahaa ei saisi tapahtua tälle suojattavalle, arvokkaalle asialle?

Lähde: CISA, Cyber Insight

Suojauksen perusteita: Mitä suojata?

Mitä arvokasta minulla on?

Rahaa – kotona, lompakossa, pankissa

- Arvopapereita – nekin ovat rahaa
- Luottokortit – rahaa nekin

Asunto – harvemmin kyberrikollisten kohteena, mutta asuntoon liittyvä digitaalinen informaatio kylläkin. Osake/omistuspaperit. Osoitetiedot, tiedot naapureista

- Asuntoon liittyvä IoT materiaali – videokuvaa, etäohjaukset – mitä jos tuhotaan lämmitysjärjestelmä tai käytetään videokuvaa ihmisten seuraamiseen?

Henkilötiedot – täydellinen nimi, syntymäaika, henkilötunnus – kaikki tiedot arvokkaita rikollisille

- Perheen tiedot: kumppani, lapset, sukulaiset/sukulaisuussuhteet, lemmikit (ovat monesti turvakysymyksenä palveluissa)

Työtiedot – työnantaja, titteli, esihenkilö, kollegat, kulkukortti/kulkunappi – käytettäviä ja arvokkaita tietoja rikollisille

Auto ja muut kulkuvälineet – rekisterinumero, tyyppi – monia kulkuvälineitä voi seurata ja uusimmat autot ovat lähinnä liikkuva tietokone – voidaan käyttää vakoilemiseen!

Laitteet – tietokoneet, tabletit, puhelimet – sisältävät arvokasta tietoa ja voidaan valjastaa rikolliseen käyttöön

Tiedostot – sähköpostit, valokuvia, videoleikkeitä, ohjelmalisenssit, tilaustiedot – voidaan käyttää hyödyksi räätälöimään hyökkäyksiä tai ottaa rikollisen käyttöön

Suojauksen perusteita: Mitä pahaa ei saa tapahtua?

Rahojen menetys

Asunnon menetys

Henkilötietojen menetys

Perhetietojen menetys

Terveystietojen menetys

Työtietojen menetys

Kulkuvälineiden menetys

Asunnon menetys

Laitteiden menetys

Tiedostojen (valokuvat, videot) menetys

Testamentit ynnä muut tärkeät tiedostot

Seuraavaksi 10 teesiä suojautumiseen

Miten suojautua – Kyberulottuvuus (1/2)

1. Kaikkein tärkein - Kouluttaudu!

- Pidä itsesi ajan tasalla hyökkäksistä, uhista ja mitä ne itsellesi tarkoittavat – pitääkö lisätä turvaa vai jättää palvelu käyttämättä
- Hanki osaamista tehdä asiat oikein tai ainakin vaatia niiden tekemistä oikein, tai pyydä apuja niiden kanssa kuten laiteasennukset

2. Seuraavaksi tärkein – päivitä, päivitä ja päivitä!

- Päivitä kaikkiin laitteisiin viimeisimmät tietoturvapäivitykset – aina! Tabletit, tietokoneet, puhelimet, reitittimet…Aivan kaikki!
- Yleisimmät hyökkäykset – haavoittuvuudet ja päivittämättömät laitteet

3. Hoida tietoturva kuntoon – käytä suojausohjelmistoja

- Antivirus, haittaohjelmien suodatus, sähköpostien suodatus, palomuuri, laitteiden salaus
- Hanki suojausohjelmistot myös mobiililaitteisiin!

4. Hyvät salasanakäytönnöt käyttöön!

- Vahva, ainutkertainen salasana - jokaiseen palveluun omansa
- Vahva tunnistaminen (MFA) käyttöön jokaisessa paikassa missä mahdollista
- Vaihda pankkitunnusten käyttö mobiilivarmenteeseen – jätä pankkitunnukset vain pankkikäyttöön
- Käytä salasanahallintaohjelmistoa – tulee monen suojausohjelmiston kyljessä

5. Suojele henkilötietojasi

- Älä jaa liikaa tietoja somessa – tiedot ovat kauppatavaraa!
- Käytä vain suojattuja viestintävälineitä arkaluontoiseen viestintään – pankkiposti, salattu sähköposti, Signal, MS Teams

Miten suojautua – Kyberulottuvuus (2/2)

5. Mieti mitä ja miksi palveluita käytät

- Tarvitsetko varmasti sovellusta
- Tarkista sovellusten oikeudet, erityisesti mobiililaitteissa

6. Terve epäluulo käyttöön

- Onko viesti oikea? Miksi sillä on kiire? Onko linkki turvallinen? Onko lähettäjä turvallinen? Käytä asiakaspalvelua ja virallisia applikaatioita sen sijaan että luotat saatuun viestiin
- Jos tarjous kuulostaa liian hyvältä ollakseen totta, se tuskin on totta
- Be a STAR – Stop, Think, Ask, React – eli hidasta, mieti, kysy neuvoa ennen kuin teet mitään

7. Ota käyttöön turvasana perheen kesken

- Jokin sana tai lause millä voitte varmistua että soittaja/viestijä on juuri oikea henkilö ja että hätä on todellinen

8. Hoida varmuuskopiot kuntoon!

- Varmista että dokumentit, valokuvat ja videot ovat turvassa
- 3-2-1 menetelmä, kolme kopiota, kahdella eri mentelmällä ja 1 kopio fyysisesti eri paikassa
- Palautumissuunnitelma
  - Miten saan tietoni takaisin varmuuskopiolta tai jos laite katoaa

9. Seuraa laitteiden elinkaarenhallintaa

- Laitteet vanhenevat 3-4 vuodessa, eikä niihin enää tulee päivityksiä → Päivitä uudempaan!

10. Tee omaehtoinen/vapaaehtoinen luottokielto

- Positiivinen luottorekisteri, Suomen Asiakastieto, Biznode tarjoaa mahdollisuuden ilmaiseen vapaaehtoiseen luottokieltoon
- Saat todistuksen jolla voit luototustilanteessa todistaa että kyseessä on itsesi asettama kielto, tai voit ottaa sen pois päältä väliaikaisesti

Muita hyviä käytänteitä

Salaa kaikki laitteet ja niiden tiedot
- Levysalaus, tiedostosalaus
- Huolehdi salausavaimesta hyvin

Rajoita käyttöoikeuksia jos mahdollista
- Käytä erillistä tiliä laitteiden hallintaan jos mahdollista – käytä vähintä mahdollista oikeutta asioiden hoitamiseen

Käytä VPN palveluita
- Varsinkin julkisissa verkoissa (tai älä käytä niitä ollenkaan)
- Valitse tarjoaja huolella – paljon huijauksia liikkeellä
- F-secure Freedome, Norton, BitDefender VPN

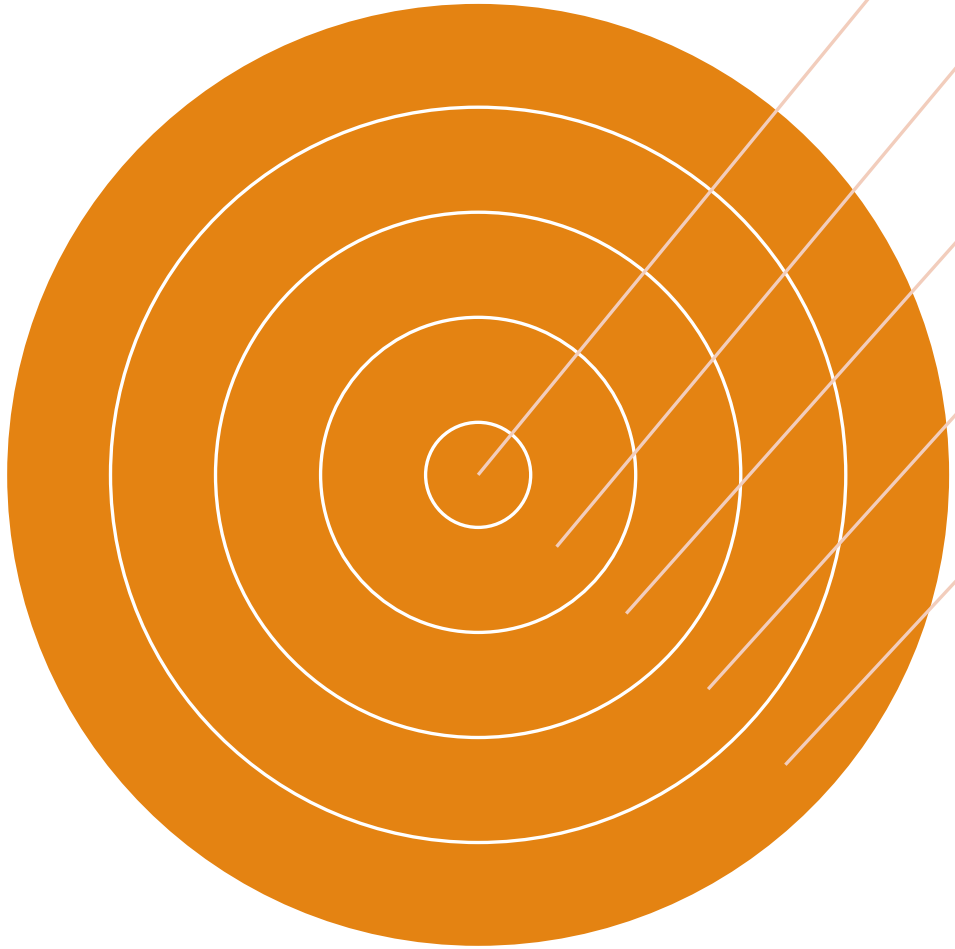
Käytä kertakäyttöluottokortteja
- Revolut ainoa Suomessa
- Jos tiedot varastetaan on kortinnumero käyttökelvoton
  - Tai ainakin oma luottokortti nettiostoja varten, jonka aktivoi vai tarvittaessa
- Maksunvälittäjiä: Klarna, Paypal…

Seuraa onko tietojasi varastettu
- Antivirusvalmistajilla usein tällainen palvelu
- Have I've been pwned - https://haveibeenpwned.com/
- Maksullisia palveluita useita jossa tätä voi myös seurata

Seuraa luottotietojasi
- Kerran vuodessa voi kysellä ilmaiseksi (Suomen Asiakastieto, Biznode)
- Positiivinen luottorekisteri kertoo luottokyselyt ilmaiseksi – tiedot näkee kirjautumalla

Varoita muita kohtaamistasi vaaroista
- Tietous lisää varautumista ja opettaa muita varomaan ongelmia

Usein puhutaan kerrossuojautumisesta tai sipulisuojautumisesta.
Yksittäinen keino ei ole riittävä vaan pitää käyttää useita suojautumismenettelyjä, jotta suojataan se tärkein – minä itse, minun henkilökohtaiset tiedot ja perheen tiedot



Henkilökohtaiset tiedot
- Salaukset
- Kertakäyttöluottokortit

Uniikit vahvat salasanat jokaisessa palvelussa
- Kaksivaiheinen tunnistus

Varmuuskopiot
- Riittävän usein
- Riittävän suojattu

Päätelaitteen suojaus
- Päivitykset
- Antivirus/suojausohjelmisto
- Käyttörajoitukset (oma pääkäyttäjä)

Verkkolaitteen suojaus
- Päivitykset
- Verkon jaottelu käytön mukaan
- Hyvät salasanat wifiverkossa
- Liikenteen suodatus ja palomuuri (jos laite tukee)

Entä jos käy huonosti?

"EI OO HÄPEE SAADA HOPEE"

“Ei oo häpee saada hopee”

Rikolliset ovat kekseliäitä ja uusia huijauksia ilmestyy jatkuvasti

Tekoäly vielä lisää riskejä hyökkäysten, hyväksikäyttöjen ja hyökkäyskeinojen suhteen

On todennäköistä että ennen pitkää sortuu virheeseen, jossa tulee paljastaneeksi hyökkääjälle esimerkiksi salasanan tai henkilötietoja

Tällöin on tärkeää ymmärtää tapahtunut ja ryhtyä toimenpiteisiin vahinkojen minimoimiseksi

Entä jos käy huonosti?

Muistisääntönä:
STAR – Stop, Think, Ask, React!

Älä panikoi! Hengitä syvään ja tee asiat järjestelmällisesti ja järjestyksessä.

1. Jos epäilet että laite on saanut haittaohjelmatartunnan: eristä laite internetistä. Tarvittaessa vedä ns töpseli irti

2. Skannaa laitteesti haitakkeista, viruksista yms. Useilla valmistajilla ladattavissa olevia versioita, joilla voi suorittaa skannauksia (lataa siis toisella laitteella vaikka muistitikulle)
   - Ole yhteydessä valmistajan asiakaspalveluun jos on tarpeen

3. Odota että skannaus valmistuu ja kykenee poistamaan haitakkeen ennen kuin käynnistät laitteen uudelleen tai liität sen internetiin

4. Ole yhteydessä huoltopalveluihin, ellet selviä itse – esim Gigantti, Power, operaattorit tarjoavat asiantuntijapalveluita.
Esimerkiksi Hyvinkäällä Napalm tarjoaa myös huoltopalveluita, joiden kautta laitteet voidaan skannata ja pelastaa tietoja

5. Ole tarvittaessa yhteydessä vakuutusyhtiöösi

Huom! Kyberturvallisuuskeskuksella kattavat ohjeet sivuillaan!

Entä jos käy huonosti?

Älä panikoi! Hengitä syvään ja tee asiat järjestelmällisesti ja järjestyksessä.

1. Jos epäilet että tunnuksesi varastettiin niin vaihda ensimmäisenä ko. palvelun salasana

2. Tarkista, että palvelun vahva tunnistaminen on edelleen käytössä

3. Päivitä salasana salasanahallintaohjelmistoon (jos käytössä)

4. Ole tarvittaessa yhteydessä palveluntarjoajan asiakaspalveluun jos sellainen on saatavilla (Microsoft, Netflix,…) ja pyydä tilisi salasanan vaihtamista

5. Tarvittaessa voit vaihtaa myös päätelaitteen salasanan tai muiden avoinna olleiden palveluiden salasanat

Muistisääntönä:
STAR – Stop, Think, Ask, React!

Entä jos käy huonosti?

Älä panikoi! Hengitä syvään ja tee asiat järjestelmällisesti ja järjestyksessä.

Jos sinulta varastettiin pankkitunnukset – ole yhteydessä pankkiisi sulkeaksesi tilisi tai tilipääsyt

Jos sinulta varastettiin luottokorttitiedot – ole yhteydessä kortin myöntäjään ja sulje korttisi.

Jos sinun identitettisi varastettiin, ole yhteydessä poliisiin sekä pankkiin ja tee vapaaehtoinen luottokielto (Suomen Asiakastieto, Bisnode ja Positiivinen luottorekisteri)

- Tee ilmoitus poliisille!
- Tee ilmoitus vakuutusyhtiölle jos tarpeen
- Ole yhteydessä tietosuojavaltuutettuun

Varoita muita – perhettä, sukulaisia, työtovereita

Myös Rikosuhripäivystys auttaa – erityisesti ensimmäisten turvaamistoimenpiteiden jälkeen

Huom! Kyberturvallisuuskeskuksella, Poliisilla ja Tietosuojavaltuutetulla kattavat ohjeet näihin tilanteisiin nettisivuillaan

Mistä saan lisätietoja ja apua?

Lähde: https://www.reactive-executive.com/en/what-are-the-4-functions-of-management/

Kyberturvallisuuskeskus

Suojelupoliisi/Poliisi

Tietosuojavaltuutettu

Internet-operaattorin asiakaspalvelu ja “guru”-palvelut

Kondikoneliikkeet, joilla asennus/huoltopalveluita – Gigantti, Power, Verkkokauppa…

Laitevalmistajan kotisivut ja asiakaspalvelu

Eri tietoturvasivuilta (hieman lähdekriittisyyttä tarpeen harrastaa)

Youtube (hieman lähdekriittisyyttä tarpeen harrastaa)

Kiitos!

KYSYMYKSIÄ?

KESKUSTELUA?

KOMMENTTEJA?

Lähteet (1/3)

[1.] Arntz, Pieter. 13.2.2025. How AI was used in advanced phishing campaign targeting Gmail users. Verkkouutinen, https://www.malwarebytes.com/blog/news/2025/02/how-ai-was-used-in-an-advanced-phishing-campaign-targeting-gmail-users, viitattu 23.2.2024

[2.] Lakshmanan, Ravie. 14.2.2025. RansomHub becomes 2024's Top Ransomware Group, Hitting 600+ organizations globally. Verkkouutinen, https://thehackernews.com/2025/02/ransomhub-becomes-2024s-top-ransomware.html, viitattu 23.2.2025

[3.] SVT. i.a. 11.2.2025. Hackarnas hot: läcker uppgifterna från Sportadmin om en vecka. Verkkouutinen, https://www.svt.se/nyheter/inrikes/hackarnas-hot-lacker-uppgifterna-fran-sportadmin-om-en-vecka, viitattu 23.2.2025

[4.] Tiihonen, Olli. 31.1.2025. Jos sait tämän kirjeen, tietosi on varmuudella viety. Verkkouutinen, https://www.is.fi/digitoday/art-2000011002936.html, viitattu 23.2.2025

[5.] OpenAi, Chatgpt. 23.2.2025. Tekoälyhaku "syitä erilaisten kyberrikosten takana". https://chatgpt.com, viitattu 23.2.2025

[6.] Copilot. 23.2.2025. Tekoälyhaku "tavallisimmat tietomurtojen syyt". https://copilot.Microsoft.com, viitattu 23.2.2025

[7.] 2NS, a.i. 1.12.2023. Threat modelling. Koulutusmateriaali, viitattu 23.2.2025

[8.] Kiravuo, Timo. 09.2024. Johdanto kyberturvallisuuteen. Luentomateriaali, viitattu 23.2.2025

Lähteet (2/3)

[9.] Chatgpt, OpenAI. 23.2.2025. Tekoälyhaku: “Yleisimmät verkkohuijaukset”. Verkkosivu, https://chatgpt.com, viitattu 23.2.2025

[10.] Copilot, Microsoft. Tekoälyhaku: “Yleisimmät verkkohuijaukset”. Verkkosivu, https://copilot.microsoft.com, viitattu 23.2.2025

[11.] Chatgpt, OpenAI. 23.2.2025. Tekoälyhaku: “Yleisimmät tilausansat”. Verkkosivu, https://chatgpt.com, viitattu 23.2.2025

[12.] tori.fi, a.i. Varo Torin nimissä tehtyjä huijauksia. Verkkoartikkeli, https://tuki.tori.fi/hc/fi/articles/22684260056722-Varo-Torin-nimiss%C3%A4-tehtyj%C3%A4-huijauksia, viitattu 23.2.2025

[13.] Augusténè, Agné. 7.5.2023. Yleisimmät WhatsApp-huijaukset – näin vältät ne. Verkkoartikkeli, https://nordvpn.com/fi/blog/whatsapp-huijaus/

[14.] Kärkkäinen, Henrik. 19.5.2024. Ilmiannoimme 10 Facebook-huijausta – sitten törmäsimme todella vastenmieliseen ilmiöön. Verkkouutinen, https://www.is.fi/digitoday/tietoturva/art-2000010409207.html, viitattu 23.2.2025

[15.] Boman, Christina. 5.6.2023. Love bombing on narsistisen persoonien keino manipuloida – näin selvität helposti, osaako kumppanisi asettua soitsen asemaan. Verkkoartikkeli, https://anna.fi/ihmiset-ja-suhteet/ihmissuhteet/love-bombing-on-narsististen-persoonien-keino-manipuloida-nain-selvitat-helposti-osaako-kumppanisi-asettua-toisen-asemaan, viitattu 23.2.2025

[16.] Stathis, Janine. 7.10.2024. How to spot Romance Scams: 7 Telltale signs to watch out for. Verkkoartikkeli, https://www.rd.com/article/romance-scams/, viitattu 23.2.2025

[17.] Langballe, Amalie. 18.8.2023. Mikä on catfishing? Verkkoartikkeli, https://kuntoplus.fi/terveys/psykologia/mita-on-catfishing, viitattu 23.2.2025

Lähteet (3/3)

[18.] Wikipedia, a.l. N/a. Käyttäjien manipulointi. Verkkoartikkeli, https://fi.wikipedia.org/wiki/K%C3%A4ytt%C3%A4j%C3%A4n_manipulointi, viitattu 23.2.2025

[19.] Kaspersky, a.l. N/a. Mitä sosiaalinen manipulointi on? Verkkosivu, https://www.kaspersky.fi/resource-center/definitions/mita-sosiaalinen-manipulointi-, viitattu 23.2.2025

[20.] Adcyber. 25.6.2023. Why assets are critical in cybersecurity – understanding the importance. Verkkosivu, https://cyberinsight.co/what-is-an-asset-and-why-is-it-important-in-cyber-security/, viitattu 23.2.2025

[21.] CISA, 07.2018. Securing High Value Assets. Verkkojulkaisu, https://www.cisa.gov/sites/default/files/publications/Securing%20High%20Value%20Assets_Version%201.1_July%202018_508c.pdf, viitattu 23.2.2025