

proxion

Liikenteen ja infran kyberturvallisuus – Jokaisen toimijan vastuulla

Jarkko Ekberg

Proxion Oy

22.3.2023



Sisältö

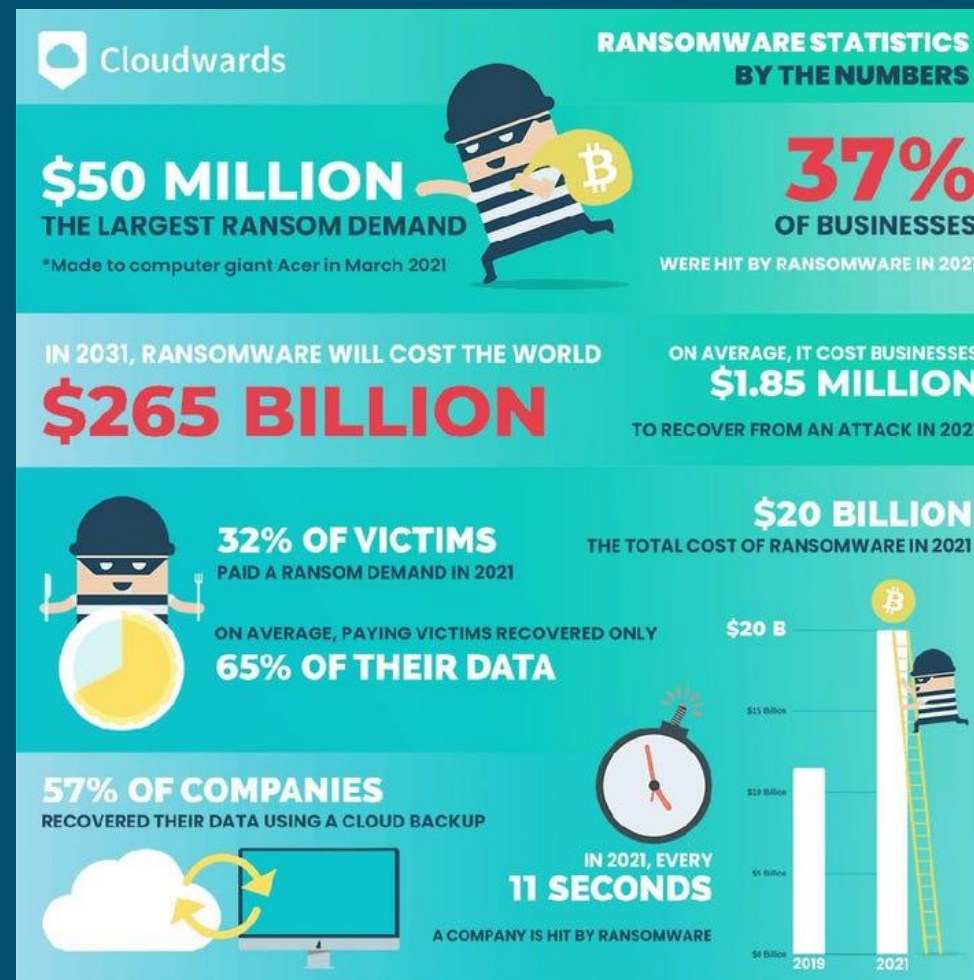
1. Liikenteen ja infran kyberturvallisuus - Miksi?
2. Mitä tieto- ja kyberturvallisuus on ja miten siitä huolehditaan?

An isometric illustration of a city scene. In the foreground, there are several buildings: a tall, light-colored tower with a crenellated top, a large building with a red roof and blue windows, and a smaller building with a blue roof. A street with traffic lights and a bench is visible. In the background, a train station with multiple tracks and platforms is shown. Several high-speed trains are on the tracks, and a bus is on a nearby road. The scene is set against a green landscape with trees and a fence.

1. Liikenteen ja infran kyberturvallisuus - Miksi?

Miksi?

- Toimintaympäristön digitalisaatio ja verkottuneisuus lisäänty → riippuvuus digitaalisesta ympäristöstä kasvaa
 - Tietoaineisto
 - Tietojärjestelmät (pilvipalvelut, etäyhteydet) & sähköinen asiointi
 - Kumppaniverkosto
 - Automaatiojärjestelmät
- Myös suojaamisen merkitys kasvaa
- Tietoturvahyökkäykset helpottuu ja lisääntyy




Liikenteen ja infran kyberturvallisuus

- Liikenne ja infra mahdollinen kyberhyökkäyksen kohde
 - Teknologia lisääntyy → alttiimpia häiriöille ja kyberhyökkäyksille
- Uhkia:
 - Palvelunestohyökkäykset
 - Kiristyshaittaohjelmat
 - Tietoliikennehäiriöt
 - Kyberhyökkäykset
 - Sabotaasi
- Mahdollisia seurauksia:
 - Vaikutukset henkilö- ja tavaraliikenteeseen
 - Henkilövahingot
 - Materiaalivahingot
 - Tarjottavien palveluiden käyttökatkot

Liikenteeseen tai infraan vaikuttaneita kyberhäiriöitä

- **Liikenne yleisesti:**
 - HSL Palvelunestohyökkäys (12/2022)
 - <https://yle.fi/a/74-20008844>
 - UK Royal Mail (1/2023)
 - <https://www.zdnet.com/article/cyber-incident-halts-royal-mails-international-export-services/>
- **Rautatie**
 - Kyberhyökkäys aiheutti junien pysähtymisen Tanskassa (2022)
 - <https://www.securityweek.com/cyberattack-causes-trains-stop-denmark>
 - Poliisi aloittaa tutkinnan kaapelivaurion aiheuttaneesta ja junaliikenteen sotkeneesta epäilyistä ilkeillä (2022)
 - <https://yle.fi/a/3-12566758>
 - Liikenteenohjausjärjestelmässä häiriö (2022)
 - <https://yle.fi/a/74-20002219>
- **Vesiliikenne**
 - Öljytankkereiden uudelleen reititys kyberhyökkäyksen takia
 - <https://www.zdnet.com/article/shell-forced-re-route-oil-supplies-after-cyberattack-on-german-companies/>
- **Lentoliikenne**
 - Tiedostojen tahaton tuhoaminen aiheutti n. 11 000 lennon peruuntumisen USA:ssa (2023)
 - https://www.theregister.com/2023/01/21/faa_outage_reasons/
- **Maantiet**
 - Liikkeessä olleen auton hakkerointi
 - <https://fossbytes.com/hackers-remotely-hacke-car-running-how-to-hack-a-car/>

An isometric illustration of a train station. In the foreground, there are several tracks with high-speed trains. To the left, there is a large, multi-story building with a clock tower and a red roof. The station platform has benches and a shelter. The background shows more tracks and a bridge.

2. Mitä tieto- ja kyberturvallisuus on ja miten siitä huolehditaan?

Eri toimijoiden rooli

- Kenen vastuulla?
 - Johto?
 - Tietoturva/IT?
 - Käyttäjät?
 - Alihankintaketju?

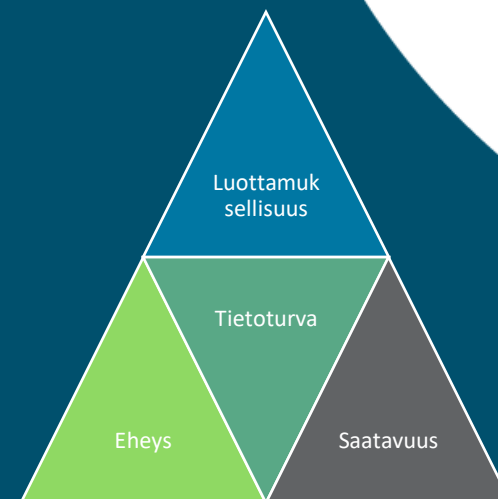


Lähde: SANS Cyber stats 10/2022

- Käyttäjä – Tietoturvallisuuden vahvin lenkki?
 - Tietoturvatietoisuuden lisääminen

Tietoturvallisuus

- Tietoturva suojaa ja mahdollistaa liiketoiminnan
- Riskien hallintaa
 - ➔ Tietoturvariski = Liiketoimintariski
- Tietoturvallisuus = Tiedon ja tietojärjestelmien luottamuksellisuuden, eheyden ja saatavuuden varmistaminen
 - Luottamuksellisuus = tiedot ovat vain niiden käyttöön oikeutettujen saatavilla
 - Eheys = tietoja eivät voi muuttaa muut kuin siihen oikeutetut
 - Saatavuus = tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä
- Kyberturvallisuus = Turvallisuuden osa-alue, jolla pyritään sähköisen ja verkotetun yhteiskunnan turvallisuuteen. Kyberturvallisuudessa tunnistetaan, ehkäistään ja varaudutaan sähköisten ja verkotettujen järjestelmien häiriöiden vaikutuksiin yhteiskunnan kriittisiin toimintoihin. Kyberturvallisuusajattelussa yhdistyy tietoturvallisuuden, jatkuvuuden hallinnan ja yhteiskunnan kriisivarautumisen ajattelua. Kyberturvallisuus turvallisuus tarkoittaa tapoja, joilla voit suojata digitaalisia tietoja, laitteita ja resursseja.
 - ➔ Mahdolliset vaikutukset yhteiskuntaan, kriittiseen infrastruktuuriin ja fyysiseen maailmaan!



Tietoturvallisuus

- Yksi osa yrityksen kokonaisturvallisuutta
- Tietoturvallisuus koostuu hallinnollisista, fyysisistä ja teknisistä hallintakeinoista
 - Hallinnollinen tietoturva = toimintaperiaatteet, vastuut, prosessit, koulutus, ohjeet ja niihin liittyvät resurssit ja toiminnot, joilla organisaatio suojaa hallussaan olevaa tietoa ja tietojärjestelmiä
 - Fyysinen turvallisuus = rakenteet, turvajärjestelmät, kulunvalvonta
 - Tekninen tietoturva = palomuurit, haittaohjelmasuojaus, varmuuskopiointi, tiedon salaaminen

➔ Tietoturvallisuuden hallintajärjestelmä

- Kaikista osa-alueista huolehdittava
- Monitasoinen suojaaminen



Tietoturvallisuus

- Yleisiä käytössä olevia ja sovellettavia tieto- ja kyberturvallisuuden standardeja ja viitekehyskiä
 - ISO 27001 Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden Hallintajärjestelmät. Vaatimukset
 - ISO 27001 Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot
 - NIS2-direktiivi
 - Digitaalisen turvallisuuden arkkitehtuuri, Digi- ja väestötietovirasto
 - NIST Kyberturvallisuuden viitekehys
 - Suositus kyberturvallisuuden edistämisestä raideliikenteessä
 - CLC/TS 50701 Railway applications. Cybersecurity (2021)
 - Kansallinen turvallisuusauditointikriteeristö
 - Julkisen hallinnon tietoturvallisuuden arviointikriteeristö
 - Kybermittari (Kyberturvallisuuskeskus)

Käyttäjä – Vahvin vai heikoin lenkki?



Lähde: [LinkedIn – The Cyber Security Hub](#)

Proxion Pro Oy - Yritysturvallisuuden kumppani

Riskienhallinnan palvelut:

Auditoinnit
Riskienarviointi
Riskikartoitukset
Riskianalyysit
Riskiraportit
Turvallisuustutkinnat

INPUT

UPDATE

Turvallisuussuunnittelun palvelut:

Turvallisuusosaamisen kehittäminen
Tietoturvallisuus (kyber)
Palo- ja pelastusturvallisuus
Toimitila- ja kiinteistöturvallisuus
Tuotannon ja toiminnan turvallisuus
Työturvallisuus
Varautuminen ja jatkuvuudenhallinta
VAK-kuljetukset

Kysymyksiä



Esittely

- Tietoturvapääällikkö
 - Konzernin tietoturva
 - Asiakkaiden konsultointi
- Tieto- ja kyberturvallisuus alalla n. 10v
 - Tietoturvapääällikkönä n. 6v
 - 8+ vuotta ydinvoima sektorilla
 - 7 kk rautatiealalla
- Tietoturvan hallintajärjestelmien kehitys, ylläpito ja arviointi
 - Mm. ISO 27001, Katakri, NIST kyberturvallisuuden viitekehys
- Kyberturvallisuuden suunnittelu ja arviointi
 - IEC standardit
- Tietoturvasertifikaatit
 - Certified Information Systems Security Professional
 - Global Industrial Cyber Security Professional