TRAFICOM
Liikenne- ja viestintävirasto

Liikenne- ja logistiikkasektorin kyberturvallisuus

Juuso Selin
Liikenne- ja logistiikkasektorin toimialavastaava
Kyberturvallisuuskeskus

TLP:CLEAR

Kyberturvallisuuslaki

- Traficom valvoo, että kyberturvallisuuslaissa edellytetyt velvoitteet täyttyvät
- **Traficom voi valvoa ainoastaan NIS2-toimijoita** - ei alihankkijoita, kumppaneita, palveluntuottajia, urakoitsijoita (paitsi, jos he itse ovat NIS2-toimijoita)
- Traficom valvoo, että 9 §:n mukainen **toimitusketjun yleinen laatu ja häiriönsietokyky**, hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt ovat riittävät
  - Traficom edellyttää, että NIS2-toimijat toteuttavat yo. 9 §:n mukaisia menettelyjä riittävällä tavalla
  - Traficom tulee pyytämään todennusta siitä, että kerrotut tai dokumentoidut menettelyt todella toteutuvat

TLP:CLEAR

Välillisiä vaikutuksia toimitusketjuun?

- NIS2-toimijan tulee huolehtia ja myös kyetä osoittamaan, että se **huolehtii lain edellyttämällä tavalla toimitusketjunsa kyberturvallisuudesta**.
- Valvova viranomainen osoittaa poikkeamat ja puutteet NIS2-toimijalle. Tämän tulee tarvittaessa **ryhtyä toimenpiteisiin toimitusketjunsa kyberturvallisuuden, laadun ja häiriönsietokyvyn parantamiseksi**.
- Valvova viranomainen voi velvoittaa NIS2-toimijan julkistamaan puutteet. Tästä voi **aiheutua mainehaittaa myös toimitusketjun jäsenille**, mikäli he ovat osallisina tapahtumissa.
- Kyberrikolliset ja ns. heikoin lenkki –trendi.

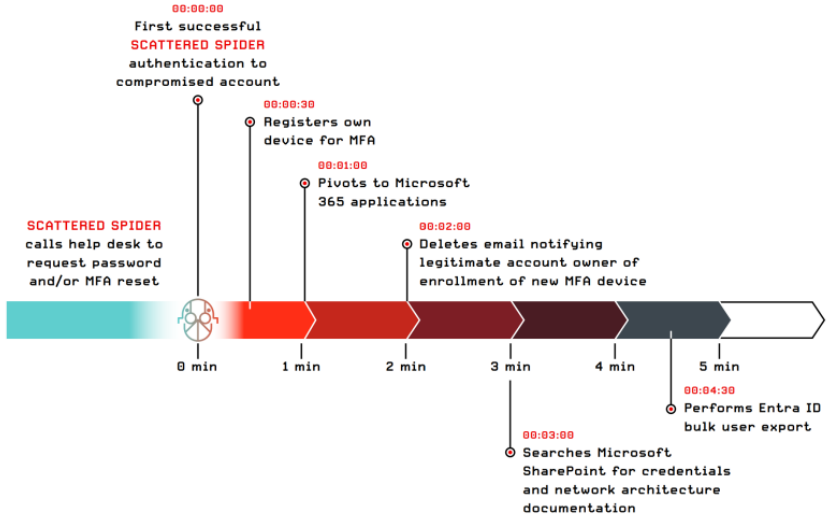
TLP:CLEAR

Iberian niemimaan sähkökatkot

- Espanjan, Portugalin ja Ranskan huhtikuiset sähkökatkot vaikuttivat myös paikalliseen liikennesektoriin.
  - Espanjan lentokenttäyhtiö Aena kertoi, että maan lentokentillä sattui katkon vuoksi useita ongelmatilanteita.
  - Ilmailutietoyhtiö Ciriumin mukaan jopa 205 Espanjan lentoasemilta lähtevää lentoa ja 208 saapuvaa lentoa peruttiin
  - Espanjan rautatieyhtiö Adif kertoi sähkökatkon pysäyttäneen junaliikenteen koko maassa. Junavuorojen peruminen vaikutti yli 35 000 junamatkustajaan ja jätti ainakin 11 suurnopeusjunaa jumiin.
  - Liikennevalot ja rautatiesignaalit olivat pois käytöstä Madridissa ja sen ympäristössä, josta aiheutui pahoja liikenneruuhkia.
- Suomessa esimerkiksi turvakellot lakkasivat toimimasta

Scattered Spider ja ilmailusektori

- Kesällä 2025 useat viranomaiset varoittivat Scattered Spider-ryhmän (tunnetaan myös nimillä UNC3944, Muddled Libra, Scatter Swine, Octo Tempest jne) kohdistavan toimintaansa erityisesti ilmailu- ja liikennesektorille.
- Ryhmä hyödynsi teknisten haavoittuvuuksien sijaan erittäin kohdennettua sosiaalista manipulointia.
  - He esiintyvät usein yrityksen työntekijöinä tai alihankkijoina huijatakseen IT-tukea myöntämään käyttöoikeuksia tai nollaamaan monivaiheisia tunnistautumisia.
  - Pääsyn saatuaan he hyvin nopeasti varastivat yrityksen tietoja ja joissain tapauksissa käyttivät myös kiristyshaittaohjelmia.
  - Monissa tapauksissa yrityksen IT-tuki oli ulkoistettu.



TLP:CLEAR

KNP Logistics

- Heinäkuussa 2025 158-vuotias brittiläinen logistiikkayritys Knights of Old (KNP) Logistics Group joutui lopettamaan toimintansa kiristysohjelmahyökkäyksen seurauksena.
- Hyökkääjät pääsivät yhtiön järjestelmiin arvaamalla heikon salasanan.
- Järjestelmään päästyään hyökkääjät salasivat kriittiset tiedot, mukaan lukien varmuuskopiot ja palautusjärjestelmät.
- Yritys ei pystynyt vastaamaan 5–6 miljoonan punnan lunnasvaatimukseen ja joutui lopettamaan toimintansa. Tämän seurauksena noin 700 työntekijää ja noin 500 kuorma-autoa jäi työttömiksi.
- Rikollisryhmä Akira kertoi olleensa hyökkäyksen takana

Jaguar Land Rover

- Jaguar Land Rover (JLR) ilmoitti 2. syyskuuta 2025 kärsineensä kyberhyökkäyksestä. JLR ei ole antanut yksityiskohtia tapahtuman luonteesta tai siitä vastuussa olevasta uhkatoimijasta.
  - 16. syyskuuta JLR ilmoitti tuotantotaukonsa jatkamisesta 24. syyskuuta asti meneillään olevan tutkinnan vuoksi. Tuotantotaukoa jatkettiin myöhemmin vielä 1. lokakuuta asti.
  - 25. syyskuuta JLR ilmoitti ottaneensa joitain järjestelmiään uudelleen käyttöön laskutuksen, maksujen ja osien jakelun jatkamiseksi
  - Myöhempien raporttien perusteella tuotantotoiminnan vaiheittainen uudelleenkäynnistys alkoi 7. lokakuuta ja osa järjestelmistä saatiin palautettua vasta marraskuussa.
  - Eri lähteiden mukaan tehtaat olivat alhaalla kuusi viikkoa ja taloudelliset menetykset yhtiölle satoja miljoonia euroa. Vaikutuksia joidenkin arvioiden mukaan **yli 5 000 yrityksen** toiminnalle ja Iso-Britannian kansantaloudelle yli 2 miljardia euroa
- Julkisten lähteiden perusteella Scattered LAPSUS$ Hunters-ryhmittymä otti 3. syyskuuta Telegram-kanavallaan vastuun tapahtumasta ja julkaisivat kuvakaappauksia, joiden väitettiin olevan JLR:n sisäisistä järjestelmistä.
- JLR oli tietomurtojen uhri jo keväällä 2025 (mm. HELLCAT ja APTS maalis-huhtikuussa)
  - Uhkatoimijat ilmeisesti hyödynsivät käyttäjätunnuksia, jotka oli saatu jo vuonna 2021 infostealerien avulla LG Electronicsin työntekijöiltä, joilla oli pääsy JLR:n Jira-palvelimelle

Euroopan lentokentät kyberhyökkäyksen kohteena

- Kyberhyökkäys häiritsi vilkkaiden eurooppalaisten lentokenttien toimintaa 19.9.2025 alkaen. Tapaus aiheutti merkittäviä häiriöitä matkustajaliikenteeseen etenkin Brysselin, Heathrown ja Berliinin lentoasemilla.
- Vakavimmat häiriöt kohdistuivat Berliinin lentoasemaan, jonka verkkosivuilla tiedotettiin mahdollisista viivästyksistä lokakuun puoliväliin asti. Brysselin ja Heathrown lentoasemilla vaikutuksista tiedotettiin noin kahden viikon ajan.
- Häiriöiden taustalla oli boarding- ja check-in järjestelmiä tuottavaan Collins Aerospace-yhtiöön kohdistunut kiristyshaittaohjelmahyökkäys.
  - Everest-rikollisryhmä kertoi murtautuneensa Collinsin järjestelmiin FTP-tunnuksen avulla. Tunnus oli ilmeisesti saatu haltuun jo vuonna 2022 Collinsin työntekijän laitteelta infostealerin avulla.
  - Everest kertoi julkisuudessa vain varastaneensa tietoa ja kiistivät käyttäneensä kiristyshaittaohjelmaa.

Mihin on syytä varautua?

- Kiristyshaittaohjelman uhka tulee olemaan merkittävä organisaatioille
- Verkon reunalaitteiden kriittiset haavoittuvuudet altistavat organisaatioita hyökkäyksille
- Haavoittuvuuksien hyväksikäyttö nopeutuu
- Verkkohuijaukset ja kalastelut jatkavat kasvuaan ja menetelmät kehittyvät
- Rikolliset pyrkivät naamioimaan hyökkäyksiään paremmin ja hyödyntämään organisaation omaa infraa
- Tekoälyn hyödyntäminen hyökkäyksissä kehittyy
- Kyberrikollisuuden käyttö informaatiovaikuttamisen työkaluna jatkuu

Ensiapua kyberpoikkeamatilanteessa

Traficomin Kyberturvallisuuskeskus

TILANNEKUVA

- Mitä Suomessa ja maailmalla tapahtuu?
- Millaisia hyökkäyksiä ja uhkia ja organisaatioihin?
- Miten niistä toivutaan?

TLP:CLEAR

ILMOITA MEILLE

Mahdollisimman tarkat tiedot...

- ruutukaappauksia havainnoistasi
- kokonaiset huijausviestit
- epäilyttävät linkit

kyberturvallisuuskeskus.fi

... ovat tärkeitä johtolankoja Kyberturvallisuuskeskukselle

- kartoitamme eri tavoin, mitä kybermaailmassa tapahtuu
- jaamme tietoa tilanteesta kansalaisille, organisaatioille ja valtionjohdolle
- autamme & neuvomme
- ennaltaehkäisemme
- ajamme alas rikollisten verkkosivuja

Minkä suhteen kannattaa olla erityisen valppaana juuri nyt?

Millaisia huijauksia on liikkeellä?

Mitkä laitteet ja ohjelmat on kiireellistä päivittää hetimmiten?

Mitkä turvatoimet kannattaa tarkistaa säännöllisesti?

TRAFICOM

TLP:CLEAR

Kyberpoikkeamailmoitukset viranomaisille

Kyberturvallisuus-keskuksen tilannekeskus (CERT-FI)

- Vapaaehtoiset ilmoitukset tietoturvaloukkauksista
- CERT-FI tarjoaa organisaatioille ensivaiheen tukea luottamuksellisesti ja maksutta

NIS2 valvovat viranomaiset

- Pakolliset ilmoitukset merkittävistä poikkeamista
- Ilmoitukset tehtävä oman sektorin valvovalle viranomaiselle

Tietosuoja-valtuutettu

- Pakolliset ilmoitukset henkilötietojen tietoturvaloukkauksista 72h kuluessa

Poliisi

- Rikosilmoitukset tietoverkkorikoksista
- Poliisin tehtävänä on ennalta estää, selvittää ja saattaa syyteharkintaan tietoverkkorikoksia

Kiitos!

Kysymyksiä tai kommentteja?