



RUOKAVIRASTO

Livsmedelsverket • Finnish Food Authority



RUOKAVIRASTO
Livsmedelsverket • Finnish Food Authority

Kyberturvallisuuslaki elintarvikealalla

Keskustelutilaisuus toimijoille

29.10.2025



Keskustelutilaisuuden aiheita

1. NIS2 –ajankohtaiset asiat
 2. Johdon vastuu, seuraamukset ja riskienhallinta
 3. Häiriönsietokykylain voimaantulo (CER-laki)
 4. Perustason tietoturvakäytännöt
 5. Lain soveltamisalaan kuuluvat elintarvikealan toimijat
 6. Kyberturvallisuuslain velvoitteet tiiviisti
 7. Juuso Selin / Kyberturvallisuuskeskuksen puheenvuoro
 8. Vapaa keskustelu ja kysely jatkoilaisuuksista
-



1. NIS2 –ajankohtaiset asiat

NIS2 –tehtävien eteneminen huhtikuun alun jälkeen Ruokavirastossa

- Ilmoittautumisia on vastaanotettu reilut puolet oletetusta määrästä
- Muistutusviestejä toimitettu yrityksille, jotka eivät vielä ole ilmoittautuneet
- Tehty runsaasti toimijoiden ohjeistusta, neuvontaa, järjestelmän kehitystä...

Kyberturvallisuuslain muutosehdotuksia

- Kyberturvallisuuslakia ollaan muuttamassa niin, että Onnettomuustutkintakeskuksen (Otkes) toimialaan lisättäisiin kyberturvallisuuteen kohdistuneiden vakavien häiriöiden turvallisuustutkinta (Helsingin kaupungin tietomurto ensimmäinen tapaus).
- Tarkoitettu tulevaksi voimaan 1.1.2027.



Ajankohtaista toimijailmoittautumisesta – tekninen käsittely

- Kaikki ilmoittautuneet on rekisteröity toimijaluetteloon
- Tekninen käsittely on vielä kesken, järjestelmän päivityksiä tulossa
- Kaikki toimijat ovat tärkeitä toimijoita
 - Ruokavirasto tekee tarvittaessa ilmoitukseen muutoksen keskeisestä toimijasta tärkeäksi toimijaksi ja ilmoittaa toimijalle
- Toimijatietojen muuttuessa toimija tekee kokonaan uuden ilmoituksen sähköiseen ilppa-järjestelmään tai ilmoittaa muutoksesta turvapostilla.

Jäsenvaltioiden välinen yhteistyö elintarvikesektorilla

- Tulossa jäsenvaltioiden Heads of Agencies –työpaja marraskuussa



Ruokaviraston valvontatoimenpiteistä

- Valvotaan parhaillaan toimijoiden ilmoittautumista
- Velvoitteiden noudattaminen jälkivalvontana; prosessien suunnittelu meneillään
- Elintarvikealan yritykset ovat ns. tärkeitä toimijoita
 - Valvova viranomainen voi kohdistaa valvontaa tärkeään toimijaan, jos on perusteltu syy epäillä, että tämä ei ole noudattanut kyberturvallisuuslakia, sen nojalla annettuja määräyksiä tai NIS2 -direktiivin nojalla annettuja säännöksiä.
- Mahdollinen tarkastus
 - Riskiperusteinen valvonta, painotus kriittisiin kyberturvallisuusriskeihin
 - Traficomin suositus pohjana, mahdollisuus käyttää myös ulkopuolista asiantuntijaa
 - Dokumenttien katselmointi, haastattelut, tekniset menetelmät, etä/läsnä



Poikkeamailmoitus

- Vastaanotettu poikkeamailmoituksia (niukasti verrattuna muihin toimialoihin)
- **Merkittävän poikkeaman määrittää aina yritys itse**
- *Merkittäväällä poikkeamalla* tarkoitetaan laissa
 - poikkeamaa, joka on aiheuttanut tai voi aiheuttaa
 - vakavan palvelujen toimintahäiriön tai
 - huomattavia taloudellisia tappioita asianomaiselle toimijalle, sekä
 - poikkeamaa, joka on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla
 - huomattavaa aineellista tai aineetonta vahinkoa.



2. Johdon vastuu, seuraamukset ja riskinhallinta

Johdon vastuu

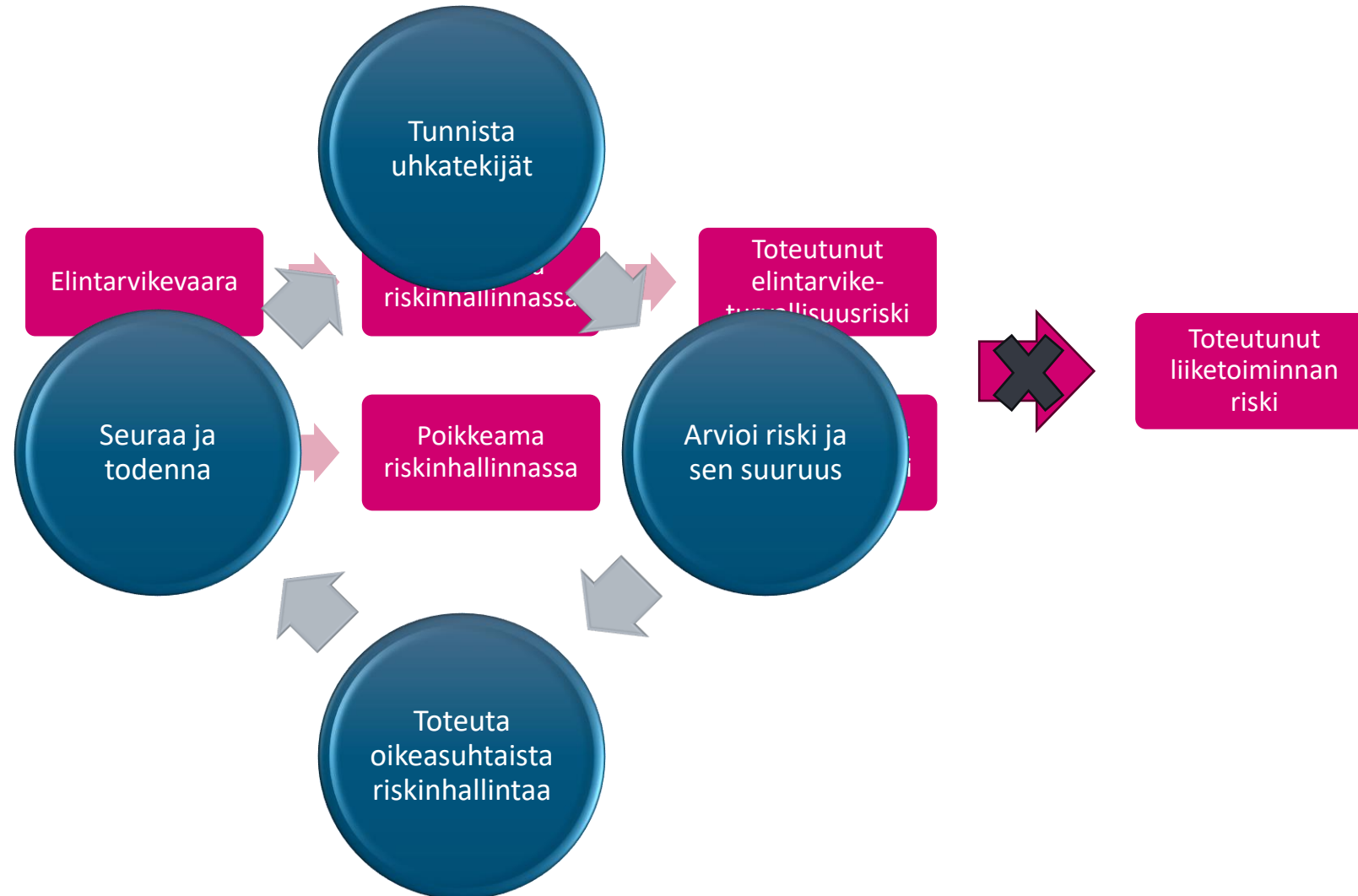
- Toimijan johto vastaa kyberturvallisuutta koskevan riskienhallinnan toteuttamisen ja valvonnan järjestämisestä sekä hyväksyy kyberturvallisuutta koskevan riskienhallinnan toimintamallin ja valvoo sen toteuttamista. Toimijan johdolla tulee olla riittävä perehtyneisyys kyberturvallisuutta koskevaan riskienhallintaan.
- Johdolla tarkoitetaan toimijan hallitusta, hallintoneuvostoa ja toimitusjohtajaa sekä muussa niihin rinnastettavassa asemassa olevaa, joka tosiasiallisesti johtaa sen toimintaa.



Seuraamukset

- Seuraamukset, mikäli velvoitteita ei noudateta
 - Varoitus
 - Uhkasakko
 - Teettämishukka
 - Keskeyttämishukka
- Hallinnollinen seuraamusmaksu
 - Tärkeälle toimijalle voidaan määrätä hallinnollinen seuraamusmaksu max 7 000 000 euroa tai
 - 1,4 prosenttia toimijan edellisen tilikauden maailmanlaajuisesta vuotuisesta liikevaihdosta kumpi on suurempi, jos se tahallaan tai törkeästä huolimattomuudesta laiminlyö velvollisuudet (124/2025 35 §).
- Seuraamusmaksulautakunta
 - Jäsenet jokaisesta valvovasta viranomaisesta

Oikeasuhtaista riskinhallintaa - toimintaympäristön muutokset huomioiden





Miksi riskinhallintaa – hyödyt monella tasolla

- Toteutuneiden riskien vaikutukset yritystasolla
 - Jatkuvuuden hallinta
 - Mainehaitta
 - Ylimääräiset kustannukset...
- Toteutuneiden riskien vaikutukset yhteiskunnan tasolla
 - Turvallisuus
 - Resilienssi
 - Talouden toimivuus
 - Yhteiskuntarauha...



Kuva: Microsoft Copilot

Kyberhyökkäyksiä tapahtuu myös elintarvikealalla – esimerkkejä maailmalta



Japan faces Asahi beer shortage after cyber-attack

1 October 2025

Demetri Chalkias



Japan is facing a shortage of Asahi products, including beer and bottled tea, as the drinks giant grapples with the impact of a major cyber-attack that has affected its operations the country.

Most of the Asahi Group's factories in Japan were brought to a standstill after the attack hit its ordering and delivery systems on Monday.

Major Japanese retailers, including 7-Eleven and FamilyMart, have now warned customers to expect shortages of Asahi products.

In a statement on Friday, Asahi said it was "unable to provide a clear timeline for

<https://www.bbc.com/news/articles/c0r0y14ly5ro> (3.10.2025)

Meat giant JBS pays \$11m in ransom to resolve cyber-attack

10 June 2021

Share Save



The world's largest meat processing company has paid the equivalent of \$11m (£7.8m) in ransom to put an end to a major cyber-attack.

Computer networks at JBS were hacked last week, temporarily shutting down some operations in Australia, Canada and the US.

The payment was reportedly made using Bitcoin after plants had come back online.

JBS says it was necessary to pay to protect customers.

In a ransomware attack, hackers get into a computer network and threaten to cause disruption or delete files unless a ransom in cryptocurrency is paid.

"This was a very difficult decision to make for our company and for me personally,"

<https://www.bbc.com/news/business-57423008> (10.6.2021)



3. CER-laki eli Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta (310/2025) voimaan 1.7.2025

- Laki toimeenpanee EU:n CER-direktiivin (2022/2557) ja koskee toimialoja, jotka tuottavat yhteiskunnan kannalta keskeisiä palveluja - mukaan lukien määritellyt elintarvikeyritykset, jotka toimivat yksinomaan logistiikan ja tukkukaupan sekä laajamittaisen teollisen tuotannon ja jalostuksen alalla.
- Samanaikaisesti tuli voimaan kyberturvallisuuslain (124/2025) muutos (369/2025), jonka myötä kyberturvallisuuslain velvoitteet ulottuvat myös CER-lain nojalla kriittisiksi määritettäviin toimijoihin. CER-lain nojalla kriittisiksi toimijoiksi määritetyt toimijat ovat kyberturvallisuuslain mukaisia ns. keskeisiä toimijoita.
- Kriittiseksi määritettyjen elintarvikealan toimijoiden on
 - ilmoitauduttava kyberturvallisuuslain mukaiseen toimijaluetteloon,
 - toteutettava kyberturvallisuuteen liittyvä riskienhallinta,
 - laadittava riskiarvio ja häiriönsietokykyä koskeva suunnitelma ja sen varmistamiseksi toteutettava toimenpiteet,
 - ilmoitettava merkittävistä poikkeamista yhteisen eurooppalaisen sääntelyn mukaisesti.



CER-laki ja kyberturvallisuuslain muutos

Tapahtuma	Päivämäärä	Kuvaus	Vastuullinen taho
Lait voimaan	01.07.2025	Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ja kyberturvallisuuslain muutos voimaan.	Valtioneuvosto
Valtakunnallinen suunnitelma ja kansallinen riskiarvio	17.01.2026	Valtioneuvosto hyväksyy kriittisten toimijoiden häiriönsietokykyä koskevan suunnitelman ja riskiarvion.	Valtioneuvosto
Kriittisen toimijan määrittäminen	17.07.2026	MMM tekee päätöksen kriittisen toimijan määrittämisestä elintarvikealalla.	MMM
CER-lain poikkeamailmoitusvelvoite	17.07.2026	Velvoitetta sovelletaan kriittiseen toimijaan päätöksen saamisesta.	Kriittinen toimija
Kyberturvallisuuslain ilmoittautumis- ja poikkeamailmoitusvelvoite	17.10.2026	Velvoitetta sovelletaan kriittiseen toimijaan 3 kk kuluttua päätöksen saamisesta.	Kriittinen toimija
Kyberturvallisuuslain riskienhallinnan toimintamallivelvoite	17.04.2027	Velvoitetta sovelletaan kriittiseen toimijaan 9 kk kuluttua päätöksen saamisesta.	Kriittinen toimija
Kriittisen toimijan riskiarviointi	17.04.2027	Riskiarviointi suoritetaan 9 kk kuluessa päätöksen saamisesta.	Kriittinen toimija
Häiriönsietokyvyn suunnitelma	17.04.2028	Häiriönsietokykyä koskeva suunnitelma laaditaan vuoden kuluessa riskiarvioinnista.	Kriittinen toimija



4. Perustason tietoturvakäytännöt

Perustason tietoturvakäytännöt eli miten pääsen alkuun

Traficom on laatinut suositusluonnoksen NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä. Suositusluonnoksessa esitetään myös perustason tietoturvakäytännöt.

Ehdotetut tietoturvakäytännöt on laadittu siten, että soveltuvat laajasti myös sellaisille toimijoille, jotka eivät kuulu NIS-säätelyn soveltamisalaan.

Perustason tietoturvakäytäntöjen avulla organisaatio voi huolehtia siitä, että tavanomaiset kybertapahtumat ovat hallittavissa.



Perustason tietoturvakäytännöt

1. Toimija on ohjeistanut perustason tietoturvakäytännöt henkilöstölle, alihankkijoille ja muille kumppaneille,
2. Toimija on tunnistanut kriittisimmän omaisuutensa,
3. Toimija on suojannut viestintäverkkonsa ja tietojärjestelmänsä,
4. Toimija on erottanut kriittiset ja haavoittuvat viestintäverkot ja tietojärjestelmät muista ympäristöistä,
5. Toimija on suojannut viestintäverkkonsa ja tietojärjestelmänsä haitallisia ja luvattomia ohjelmistoja vastaan,
6. Toimija on järjestänyt tunnistautumisen sisäisiin ja ulkoisiin palveluihinsa ja laitteisiinsa turvallisesti,
7. Toimija on erottanut järjestelmiensä pääkäyttäjätunnukset ja korotettujen oikeuksien tunnukset muista tunnuksista,



Perustason tietoturvakäytännöt, jatkuu...

8. Toimija on varmistanut, että sen luottamuksellista tietoa käsitellään turvallisesti,
9. Toimija on huolehtinut, että sen järjestelmiä päivitetään säännöllisesti ja kriittiset päivitykset asennetaan viivytyksettä,
10. Toimija on huolehtinut, että sen palvelut ja laitteet on turvallisesti konfiguroitu,
11. Toimija on huolehtinut, että sen kriittiset palvelut ja tieto-omaisuus on varmuuskopioitu,
12. Toimija on varautunut, miten sen toiminta voidaan ylläpitää vakavissa poikkeamissa ja
13. Toimijalla on käytössään kriittisten toimintojen tapahtumakirjaus.

5. Lain soveltamisalaan kuuluvat elintarvikealan toimijat



- Yrityksen toimiala: tukkukauppa, teollinen tuotanto tai jalostus.
- Ei koske esim. alkutuotantoa, elintarvikekontaktimateriaalitoimintaa, ruokapalveluita, vähittäiskauppaa tai ravintoloita.
- Yrityksen koko vähintään 50 työntekijää tai liikevaihto ja taseen loppusumma kukin ylittää 10 miljoonaa euroa.
- Tarkastelujakso 2 edellistä vuotta viimeisimmästä tilinpäätöksestä.
- Toimijakriteerit koskevat koko yrityksen liiketoimintaa, ei vain elintarviketoiminnan osuutta.



6. Kyberturvallisuuslain velvoitteet tiiviisti

Ilmoittautuminen toimijaluetteloon

- Varmistu soveltamisalasta ja toimijakriteereistä
- Ilmoittaudu ilppassa
- Anna 41§ mukaiset tiedot
- Ilmoita muutokset 2 viikon kuluessa

Riskienhallinta

- Tunnista, arvioi ja hallitse riskejä kohdistuen tietojärjestelmien ja viestintäverkkojen turvallisuuteen
- Estä tai minimoi poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin

Poikkeamailmoitus

- Ilmoita viipymättä valvovalle viranomaiselle merkittävästä poikkeamasta
- Tee ilmoitus Traficomin ilmoitussovellukseen → tieto Ruokavirastoon
- Tee ensi-ilmoitus 24 tunnin kuluessa merkittävän poikkeaman havaitsemisesta ja jatkoilmoitus 72 tunnin kuluessa merkittävän poikkeaman havaitsemisesta



Lisätietoa

Ruokaviraston sivut

- NIS2.kyberturvallisuus@ruokavirasto.fi

Traficomin sivut

- [Direktiivin kohteena olevat organisaatiot](#) (Traficomin taulukko)
- [Traficomin suositus riskienhallinnan toimenpiteistä](#)

NIS2-direktiivi (EU) 2022/2555

[Kyberturvallisuuslaki 124/2025](#) ja [Laki kyberturvallisuuslain muuttamisesta 369/2025](#)

[Laki yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta 310/2025](#) (CER-laki) ja [CER-direktiivi \(EU\) 2022/2557](#)

RUOKAVIRASTO

Livsmedelsverket • Finnish Food Authority

