

TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Syyskuu 2026

Kybersää

Kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä.

Tämä tuote on suunnattu ensisijaisesti eri tasoilla organisaatioiden tietoturvallisuuden parissa työskenteleville.

Kybersää tarjoaa nopean kokonaiskuvan, mitä kyberturvallisuuskentällä on tapahtunut ja mitä on tulossa.

Kybersää voi olla:



rauhallinen



huolestuttava



vakava

Kuukauden tunnuslukuja



Kyberturvallisuuskeskus julkaisi syyskuussa kahdeksan haavoittuvuustiedotetta kriittisistä haavoittuvuuksista. ^[1]



Kyberturvallisuuskeskus julkaisi vuoden 2026 ensimmäisen keltaisen varoituksen NetScaler ADC- ja NetScaler Gateway –tuotteisiin liittyen. Ongelma koskee Citrix-asiakkaita maailmanlaajuisesti ja Kyberturvallisuuskeskus on saanut ilmoituksia haavoittuvuuksien hyväksikäytöstä, eli tietomurroista myös Suomessa. ^[2,3]



Lähes yhdeksän kymmenestä suomalaisesta pitää arkeaan digitaalisessa ympäristössä turvallisena, vaikka digihuijaukset ovat Suomessa yleisempiä kuin EU:ssa keskimäärin. ^[4]



Kybersään yleistilanne syyskuussa 2026

Sadetta ja myrskyä verkon reunalla

Syyskuun kyberturvallisuustilanne Suomessa painottui huijauksiin, verkkosivustojen murtoihin sekä verkon reunalaitteiden kriittisiin haavoittuvuuksiin. Huijaukset olivat jälleen monipuolisia ja esimerkiksi toimitusjohtajahuijauksia nähtiin lähes päivittäin.

Suomalaisiin WordPress-sivustoihin kohdistuneet murrot ja haittaohjelmien levittämiset ClickFix-tekniikalla jatkuivat. Lisäksi syyskuussa julkaistiin useita kriittisiä ja aktiivisesti hyväksikäytettyjä haavoittuvuuksia esimerkiksi Ciscon, F5:n, Check Pointin ja GitLabin tuotteissa. [5,6,7,8]

Syyskuun lopussa Kyberturvallisuuskeskus julkaisi vakavan varoituksen Citrix NetScaler ADC- ja Gateway-tuotteiden haavoittuvuuksista, joiden kautta on tehty useita tietomurtoja Suomessa. Pelkkä päivittäminen ei tässä tapauksessa riitä, vaan ympäristö on tarkastettava myös murtojälkien varalta. [9]

Salamoita verkon reunalaitteisiin myös ulkomailta

- Citrix NetScaler -laitteiden nollapäivähaavoittuvuuksia hyödynnettiin globaalisti syyskuun alusta lähtien. Kohteina oli muun muassa julkishallinnon ja rahoitusalan organisaatioita Euroopassa ja Pohjois-Amerikassa. [10]
- Norjassa esiintyi elokuun lopulla ja syyskuussa useita laajoja palvelunestohyökkäyksiä, joista osan takana väitti olevansa Venäjä-mielinen haktivistiryhmä. [11]
- Muissa Pohjoismaissa samanlaista toimintaa ei ole havaittu, mutta Tanska nosti syyskuussa oman kyberuhka-arvionsa tuhoisten kyberhyökkäysten osalta tasolle korkea. [12]



Kuukauden raekuuro

Kvanttisiirtymä tulee, oletko valmis?

Kyberturvallisuuskeskus julkaisi tammikuun lopulla ohjesivuston, joka käsitteli kvanttietokoneiden aiheuttamaa uhkaa nykyisille salausmenetelmille.

Jatkona ohjesivustolle on nyt julkaistu lyhyt esitys otsikolla "Kvanttiturvalliseen salaukseen siirtyminen", jossa käydään neljällä selkeällä kalvolla läpi asioita, joita organisaatioiden johtoportaissa tulisi huomioida kvanttisiirtymään liittyen.
[13]

Kvanttitietokoneiden kehittyminen muuttaa nykyisten salausmenetelmien turvallisuusoletuksia. Kvanttiuhka koskee erityisesti tietoja, joiden on säilyttävä luottamuksellisina pitkälle tulevaisuuteen. Tällaisia ovat esimerkiksi henkilötiedot, terveystiedot, liikesalaisuudet sekä viranomaisten salassa pidettävät tiedot.

Kvanttiuhka ei ala Q-päivästä

- Kvanttiuhkaa kuvataan toisinaan käsitteellä **Q-päivä (Q-day)**, jolla tarkoitetaan ajankohtaa, jolloin kvanttietokoneet kykenevät murtamaan laajasti käytössä olevat klassiset epäsymmetriset salausmenetelmät käytännössä.
- Q-päivä ei kuitenkaan ole selkeä rajapyykki, jonka jälkeen uhka vasta syntyy. Merkittävä osa kvanttiuhkasta liittyy tilanteeseen, jossa hyökkääjä kerää salattua tietoa jo ennen Q-päivää ja säilyttää sitä myöhempää purkamista varten. Tätä kutsutaan strategiaksi "*talleta salattu aineisto nyt, pura salaus myöhemmin*" (harvest now, decrypt later).

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen



Kyberturvallisuuskeskus julkaisi vuoden ensimmäisen vakavan varoituksen. Varoitus julkaistiin syyskuun lopulla ilmi tulleisiin Citrix Netscaler ADC- ja Gateway tuotteiden kriittisiin haavoittuvuuksiin liittyen. ^[14]



Tunnusten kalastelu on yleinen tapa murtautua organisaatioiden Microsoft 365 -käyttäjätileille. Verkkosivuillamme julkaistu artikkeli valottaa sitä, miten Microsoft 365 -tunnusten kalastelu ja tilikaappaus etenevät, miten tietomurron voi tunnistaa ja rajata sekä millä teknisillä suojaustoimenpiteillä organisaatio voi pienentää käyttäjätilien vaarantumisen riskiä. ^[15]



Uhkamallinnuksen avulla organisaatiot voivat tunnistaa ohjelmistojen ja järjestelmien tietoturvariskejä jo kehitysvaiheessa, ja ottaa tietoturvan suunnitelmalliseksi osaksi ohjelmistokehitystä. Julkaisimme verkkosivustollamme materiaalipaketin ja sitä tukevia koulutuksia, jotka auttavat organisaatioita pääsemään alkuun ja harjoittelemaan uhkamallinnusta käytännössä. ^[16]

Kybersään ilmiöt

Osiossa käymme läpi
kyberturvallisuuden ilmiöiden
kehitystä ja trendejä.



Kybersää syyskuu 2026



Tietomurrot ja -vuodot

Syyskuussa tietomurtoilmoituksia tuli 81,5 % enemmän kuin edellisvuonna. Tietomurroissa hyödynnettiin ohjelmistojen haavoittuvuuksia ja kiristyshaittaohjelmat iskivät etenkin pieniin yrityksiin.



Haittaohjelmat

Tarkastelujaksolla havaittu useita suomalaisia verkkosivustoja, joissa on jaettu haittaohjelmia ClickFix -tekniikkaa käyttäen. GitLab:issa levitetty haitallisia paketteja sekä haittaohjelmia.



Haavoittuvuudet

Syyskuun aikana annettiin peräti kahdeksan haavoittuvuustiedotetta. Hyväksikäytettyjen haavoittuvuuksien määrä on kasvanut ja näiden haavoittuvuuksien hyväksikäyttö on nopeutunut.



Huijaukset ja kalastelut

Finanssialan tuoreen selvityksen mukaan pankit torjuivat yli puolet alkuvuoden huijausyrityksistä. Huijausyritysten määrä silti kasvoi lähes kolmanneksella edellisvuoden vastaavaan ajanjaksoon verrattuna.



Automaatio ja IoT

VehicleSec '26 ^[17] ja WOOT '26 – konferensseissa esiteltiin tutkimustuloksia sähköajoneuvojen latausjärjestelmistä löytyneistä heikkouksista, joita hyödyntämällä hyökkääjä pystyisi saamaan taloudellista hyötyä tai häiritsemään lataamista. Videot tulivat syyskuussa julki.



Verkkojen toimivuus

Syyskuun aikana havaittiin joitain haktivismin motivoimia palvelunestohyökkäyksiä suomalaisia organisaatioita kohtaan.



Kybersää

syyskuu 2026 1/2



Tietomurrot ja -vuodot

- Ohjelmistojen haavoittuvuuksia hyödynnettiin edelleen monissa tietomurroissa. Yli puolessa näistä tapauksista hyödynnettiin WordPress-sivuston haavoittuvuuksia.
- Kiristyshaittaohjelmat iskivät etenkin pieniin yrityksiin. Hyökkääjät pääsivät järjestelmiin haavoittuvuuden tai ilman monivaiheista tunnistautumista käytettyjen VPN-tunnusten kautta.
- Microsoft 365 -tilien tietomurrot lisääntyivät voimakkaasti kuukauden loppupuolella.



Haittaohjelmat

- Syyskuun aikana Kyberturvallisuuskeskus on vastaanottanut useita ilmoituksia suomalaisista verkkosivustoista, joissa on jaettu haittaohjelmia tai haitallista koodia ClickFix-tekniikkaa hyödyntämällä. Verkkosivustot on usein murrettu WordPress-haavoittuvuuksia hyväksikäyttäen.
- Kyberturvallisuuskeskus vastaanotti havaintoja ja ilmoituksia, joissa kerrottiin GitLab-palvelussa olevan jaossa haitallisia repositorioita. Nämä poistettiin kuitenkin saatavilta nopeasti.



Haavoittuvuudet

- Syyskuun haavoittuvuustiedotteista varsinkin Citrix Netscaler nousi vahvasti esille.
- Haavoittuvuuksien hyväksikäytön jatkuvan nopeutumisen vuoksi, oman ympäristön ja hyökkäysrajapinnan tunteminen on entistä tärkeämpää ja turvallisuuspäivitysten asentaminen kiireellisempää varsinkin verkon reunalaitteissa.
- Päivittämisen lisäksi usein on syytä varmistaa, ettei haavoittuvuutta ole ehditty käyttämään hyväksi ennen päivittämistä.



Kybersää

syyskuu 2026 2/2



Huijaukset ja kalastelut

- Finanssialan tuoreen selvityksen mukaan pankit torjuivat yli puolet alkuvuoden huijausyrityksistä. Huijausyritysten määrä silti kasvoi lähes kolmanneksella edellisvuoden vastaavaan ajanjaksoon verrattuna. ^[18]
- Perinteisten tietojenkalastelu- ja sijoitushuijausten lisäksi rikolliset pyrkivät hyödyntämään pankkitunnuksia esimerkiksi uusien pankki- ja puhelinpalveluiden avaamiseen sekä lainojen ja osamaksujen hankkimiseen.
- Selvityksen tärkein viesti on, että huijaukset ovat yhä yleisempiä ja menetelmät kehittyvät nopeasti.



Automaatio ja IoT

- Latausinfrastruktuurin riskit eivät rajoitu vain tietomurtoihin.
- Sähköajoneuvojen latausohjelmistovirheet voivat aiheuttaa sen, että lataus ei pysähdy silloin kun sen pitäisi tai lataus menee toiselle henkilölle maksettavaksi. Vanhoissa viestintäprotokollissa olevien tietoturvapuutteiden takia akun voi purkaa tai sähköä voi ladata luvottomasti. ^[19,20,21]
- Suomessa Kyberturvallisuuslaki asettaa vaatimuksia latauspisteoperaattoreille, jos ne ovat kooltaan riittävän suuria tai niiden toiminta katsotaan muuten kriittiseksi.



Verkojen toimivuus

- Syyskuun aikana havaittiin joitain haktivismin motivoimia palvelunestohyökkäyksiä suomalaisia organisaatioita kohtaan. Joillakin yksittäisillä hyökkäyksillä oli korkeintaan pieniä vaikutuksia aiheuttaen lyhyitä käyttökatkoja.
- Europolin operaatio PowerOFF toimii sulkeakseen palvelunestohyökkäyksiin käytettäviä, ostettavia palveluja yhteistyössä kansainvälisten viranomaiskumppanien kanssa. Operaation osana viranomaiset pyrkivät puuttumaan tällaisten palvelujen ylläpitoon ja käyttöön. ^[22]



Kybersään ilmiöt kulunut 12 kk

	2025 Loka- kuu	Marras- kuu	Joulu- kuu	2026 Tammi- kuu	Helmi- kuu	Maalis- kuu	Huhti- kuu	Touko- kuu	Kesä- kuu	Heinä- kuu	Elo- kuu	Syys- kuu
Tietomurrot ja -vuodot												
Haittaohjelmat												
Haavoittuvuudet												
Huijaukset ja kalastelut												
Automaatio ja IoT												
Verkkojen toimivuus												

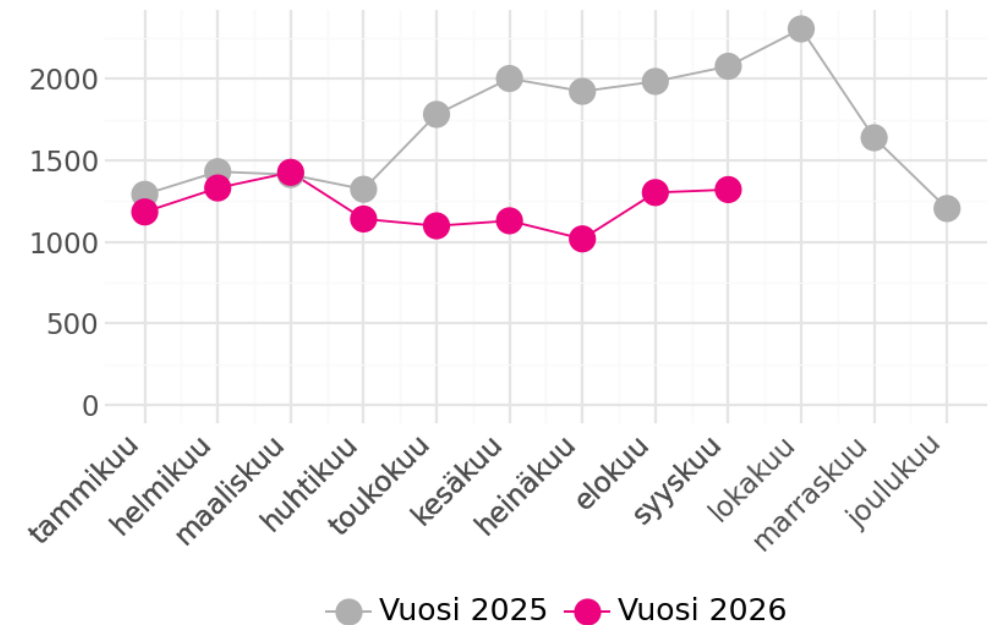


Tapaukset

- Kyberturvallisuuskeskus käsitteli syyskuussa 1320 tapausta.
- Ilmoitusten määrä on 12 kuukauden keskiarvoon nähden 1,5 % koholla.
- Syyskuun aikana tapausmäärissä näkyi erityisesti WordPress-julkaisualustan haavoittuvuuksien kautta tehdyt verkkosivustojen tietomurrot sekä haittaohjelmien levittämiset ClickFix-tekniikkaa käyttäen. Lisäksi M365-tilimurtoja on havaittu edelleen suurissa määrin.
- Syyskuun lopussa Citrix NetScaler ADC & Gateway – tuotteisiin julkaistiin kriittisiä haavoittuvuuksia, joiden välityksellä on tehty useita tietomurtoja tai niiden yrityksiä, mikä on aiheuttanut useassa organisaatiossa merkittäviä toimenpiteitä omien ympäristöjensä suojaamiseksi.

Tapaukset

Kyberturvallisuuskeskuksen käsittelemät tapaukset, lukumäärä kuukausittain



Kybersääennuste

Kybersääennuste on aiempiin havaintoihin perustuva yhteenveto ja suuntaa-antava arvio lähikuukausien kyberuhista ja niiden kehityskuluista.

Osiossa käsitellään myös puolivuositain ilmiöiden pitkän aikavälin kehitysnäkymiä ja lähitulevaisuuden top 5 kyberuhat.



Kybersääennuste

Kyberuhat pysyvät tavanomaisina

Lokakuu on alkanut epävakaisena ja sellaisena se todennäköisesti eteneekin. Syyskuun lopun Citrix-myrsky ei ole vielä ohi ja sen vaikutuksia seurataan lokakuun aikana. On mahdollista, että haavoittuvuuden opportunistinen hyväksikäyttö jatkuu. Huijaukset todennäköisesti jatkuvat sateisina ja sivustomurtojen osalta on odotettavissa paikallisia kuuroja.

Kyberkestävyyspäädöksen ilmoitusvelvoite alkoi 11.9.2026, joten lokakuussa nähdään ensimmäisiä kokemuksia valmistajien ilmoituksista. Käyttäjille tämä tarkoittaa ajantasaisempaa tietoa laitteiden haavoittuvuuksista.



Kybersääennuste on aiempiin havaintoihin perustuva yhteenveto ja suuntaa-antava arvio kyberuhkien tilasta. Arviota ei tule käyttää sellaisenaan kyberuhkiin varautumisessa, vaan sen tukena on käytettävä organisaatiokohtaista tietoa ja analyysiä. Cyberuhat voivat muuttua nopeasti, myös negatiiviseen suuntaan.



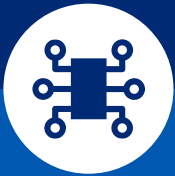
Huolestuttava

Kyberuhkien määrä ja vakavuus ovat tavanomaisella tasolla.



Pitkän aikavälin kybersää

Ilmiöt, joita seuraamme



Murrokselliset teknologiat

esimerkiksi tekoäly, 6G, kvantti-teknologia



Infrastruktuuriin ja yhteiskunnan kriittisiin toimintoihin

kohdistuvat kyberuhat



Laaja-alaisiin kyberhyökkäyksiin ja -häiriöihin

varautuminen



Tietoturva-loukkausten muutos

esimerkiksi tietomurrot ja -vuodot



Digitaalisen yhteiskunnan sääntelykehitys



Pitkän aikavälin kybersää

Haavoittuvuudet 1/2

Suurin osa (31 %) tietomurroista alkaa nykyisin haavoittuvuuden hyväksikäytöllä. Aikaisemmin globaalisti yleisin murtautumiskeino on ollut tietojenkalastelulla varastettujen kirjautumistunnusten käyttäminen. ^[23]

Löydettyjen haavoittuvuuksien määrän kasvu kuormittaa organisaatioita. Yli 20 % CVE-historian (1999-2026) haavoittuvuuksista on löydetty vuoden 2026 aikana. ^[24]

Myös hyväksikäytettyjen haavoittuvuuksien määrässä on kasvua, ja haavoittuvuuksien hyväksikäyttöä esiintyy aiempaa nopeammin.

Erinäiset kehittyneet tekoälyratkaisut ovat laskeneet eri toimijoiden tarvittavaa osaamiskynnystä uusien haavoittuvuuksien löytymiselle ja haavoittuvuuksien hyväksikäytölle, kun tekoäly pystyy käskyn saatuaan itsenäisesti tekemään haavoittuvuuden kartoituksen ja hyväksikäytön.

Tekoälyratkaisujen avulla hyökkäyspolkujen mallinnus (attack path analysis) helpottuu huomattavasti. Tämä mahdollistaa hyökkääjälle erilaisten haavoittuvuuksien hyväksikäytön mahdollistavien tekijöiden, kuten tunnistus-, konfiguraatio- ja logiikkavirheiden löytämisen ja ketjuttamisen. Tällöin yksittäin vähäpätöisiltä näyttävät puutteet voivat yhdessä muodostaa vakavan hyökkäyspolun.

Arvio lähitulevaisuudesta

- Haavoittuvuuksien määrä ja niiden hyväksikäytön nopeus tulevat erittäin todennäköisesti jatkamaan kasvuaan lyhyellä ja keskipitkällä aikavälillä, kun tekoälytyökalut kehittyvät ja leviävät laajemmin myös rikollisten ja vähemmän osaavien toimijoiden käyttöön.
- Haavoittuvuuksien priorisointi niiden aiheuttaman uhan perusteella tulee yhä tärkeämmäksi. Tämä edellyttää organisaatioilta varautumista yhä nopeampaan päivitysrytmiin ja niiden oman infrastruktuurin tuntemista.



Pitkän aikavälin kybersää

Haavoittuvuudet 2/2

EU:n Kyberkestävyyssäädöksen mukainen aktiivisesti hyödynnettyjen haavoittuvuuksien ja vakavien tietoturvaan vaikuttavien poikkeamien ilmoitusvelvollisuus alkoi 11.9.2026.

Valmistajan on ilmoitettava kyseisistä haavoittuvuuksista ja poikkeamista Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle ja EU:n kyberturvallisuusvirasto ENISAlle. Tämän lisäksi valmistajalla on velvollisuus tiedottaa tuotteen käyttäjiä näistä haavoittuvuuksista ja poikkeamista.

Kaikki ilmoitukset tehdään ENISAn ylläpitämän keskitetyn raportointialustan (Single Reporting Platform, SRP) kautta.

Valmistajan on seurattava tuotteidensa tietoturvaa ja tutkittava välittömästi epäilyttävät tapahtumat ja niistä saadut ilmoitukset. Ilmoitusvelvollisuus astuu voimaan, kun valmistaja on saanut luotettavaa näyttöä haavoittuvuuden hyödyntämisestä

Valmistajan on annettava 24 tunnin kuluessa ensivaroitusilmoitus. Varsinainen haavoittuvuus- ja poikkeamailmoitus tehdään 72 tunnin kuluessa.

Haavoittuvuuksien ja poikkeamien ilmoitusvelvoite koskee myös sellaisia tuotteita, joiden valmistus on lopetettu.

Lisätietoja CRA:sta löydät Kyberturvallisuuskeskuksen CRA – sivuilta. ^[25]



Top 5 uhat lähitulevaisuudessa

1

Vakavia haavoittuvuuksia hyödynnetään yhä nopeammin

Haavoittuvuuden korjaavan päivityksen asentamisen lisäksi on usein tarpeen tutkia, onko haavoittuvuutta hyödynnetty jo ennen päivityksen asentamista.

2

Tekoälyn käytön lisääntyminen edellyttää riskienhallintaa

Organisaatioiden varautuminen ja aktiiviset riskienhallinnan toimet ovat tärkeitä nopeasti lisääntyvän tekoälyn käytön myötä.

3

Toimitus- ja palveluketjujen tietoturva ja jatkuvuus

Alihankintaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä. Valtaosa organisaatioista on enemmän tai vähemmän riippuvaisia ulkoistetuista digitaalisista palveluista.

4

Kriittisen infrastruktuurin suojaamisen tärkeys korostuu

Nopeasti muuttuva kybertoimintakenttä vaikuttaa kriittisen infrastruktuurin suojaamiseen.

5

Kiristyshaittaohjelmat ovat merkittävä uhka organisaatioille

Kiristyshaittaohjelmien määrä kasvaa globaalisti jatkuvasti.

1

Vakavia haavoittuvuuksia hyödynnetään yhä nopeammin

Rikolliset ja valtiolliset toimijat pyrkivät hyväksikäyttämään haavoittuvuuksia ennen kuin niitä on ehditty korjata. Tammi-kesäkuussa 2026 valtaosa havaitusta hyväksikäytöstä alkoi kahden vuorokauden sisällä siitä, kun hyökkäyskoodi julkaistiin. [26]

- Järjestelmien nopea päivittäminen on erityisen tärkeää. Valmius päivittämiseen on syytä ylläpitää jatkuvasti, myös viikonloppuisin ja loma-aikoina.
- Haavoittuvan järjestelmän päivittämisen lisäksi on tärkeää tutkia, onko haavoittuvuutta jo ehditty hyväksikäyttää ennen sen korjaamista.

Myös vanhoja haavoittuvuuksia hyödynnetään edelleen onnistuneesti. Viimeaikaisissa kartoituksissa verkkolaitteista on löytynyt jopa viisi vuotta vanhoja korjaamattomia haavoittuvuuksia. [27]

Tekoälytyökalut mahdollistavat massamaisen ja automatisoidun haavoittuvuuksien etsimisen. Samalla tekoälytuotteista itsestään on tullut uusi hyökkäyspinta.

Tekoälyllä todennäköisesti kehitettyjä nollapäivähyökkäyksiä on jo havaittu. [28]

Löydettyjen haavoittuvuuksien määrä on kasvanut voimakkaasti vuonna 2026.

Verkon reunalaitteet muodostavat merkittävän rajapinnan hyökkäyksille, joita toteutetaan usein nollapäivähaavoittuvuuksien kautta. Pelkästään syyskuussa 2026 aktiivisesti hyväksikäytettyjä kriittisiä haavoittuvuuksia löytyi useamman toimittajan tuotteista. [29,30,31,32]

- Haavoittuvuuksiin liittyvien uhkien hallinnassa korostuvat sekä havainnointi että reagointikyky. Järjestelmäympäristön valvonta ja haavoittuvuuksien etsiminen edistää hyökkäysten rajoittamista. On hyvä seurata valmistajan ohjeita tietomurtojen ja hyväksikäytön havaitsemiseksi.
- Organisaatioilla tulee myös olla suunnitelma hyökkäyksestä ja sen vaikutuksista palautumiseen.

2

Tekoälyn tuomiin haasteisiin on hyvä varautua organisaatioissa

Organisaatioiden riskit kasvavat erityisesti tekoälyagenttien myötä, kun tekoäly ei vain vastaa kysymyksiin vaan toimii itsenäisesti organisaation järjestelmissä ja työkaluissa.

Etenkin tekoälyn hallitsematon käyttöönotto, ”varjo-AI”, luo organisaatioille haasteen. Moniin tuotteisiin on integroitu yllättäviä tekoälytoiminnallisuuksia, joita työntekijät voivat ottaa käyttöön epävirallisesti, organisaation tietoturvapolitiikan vastaisesti.

Organisaatioiden on tekoälyn käytössä hyvä ottaa huomioon erityisesti tietosuoja- ja salassapitonäkökulmat, ja pohtia näihin liittyviä linjauksia organisaatiossa.

- Tekoälyn käyttöön tulisi laatia organisaation sisäinen käyttöpolitiikka ja ohjeistus henkilöstölle siitä, miten tekoälyä voi sallitulla tavalla hyödyntää työssä. Tekoälyn huoleton käyttö on yleinen riski. Arkaluontoista tietoa saattaa päätyä käyttäjien välityksellä erilaisiin tekoälypalveluihin.^[33]
- Integroiduilla tekoälysovelluksilla saattaa olla laaja pääsy organisaation dataan. Riskit korostuvat, jos sovellus säilyttää tai käsittelee dataa organisaation ulkopuolisella palvelimella.^[34]

Tekoälytyökalut mukana kyberrikollisten työkalupakissa

Kyberuhkatoimijat käyttävät yhä aktiivisemmin tekoälypalveluita haittaohjelmien ja hyökkäysten jalostamiseen. Tekoälyä hyödynnetään esimerkiksi kalasteluviestien laatimiseen, haittaohjelmien kehittämiseen tai haitallisen koodin tulkittavuuden hankaloittamiseen (obfuscation).

- Uudet tekoälytyökalut myös mahdollistavat massamaisen ja automatisoidun haavoittuvuuksien etsimisen, tunnistamisen ja hyväksikäytön.^[35]

Rikolliset käyttävät syvävääreännöksiä eli deepfake-teknologiaa huijausten tekemiseen. Suomessakin on havaittu syvävääreännysvideoita, joissa esiinnyttään esimerkiksi organisaation toimitusjohtajana petosten yritysten yhteydessä.

- Epätavalliset maksu- ja hankintapyynnöt kannattaa aina varmistaa toista kanavaa pitkin, esimerkiksi soittamalla tai tapaamalla henkilö kasvotusten.

3

Toimitus- ja palveluketjujen tietoturva ja jatkuvuus ovat yhä kriittisempiä

Alihankkijaketjun ymmärtäminen on organisaatioiden kyberturvallisuuden kannalta keskeistä. Valtaosa organisaatioista on enemmän tai vähemmän riippuvaisia ulkoistetuista digitaalisista palveluista.

- Toimitusketjuihin liittyvä uhka ei kohdistu pelkästään komponentteihin, vaan saattaa konkretisoitua esimerkiksi ohjelmistojen ja ohjelmointikirjastojen kautta.

Kyberturvallisuuskeskukselle ilmoitetuissa tapauksissa vaikuttaa usein siltä, että alihankintaketjuihin liittyvät vastuut ovat organisaatioille epäselviä. Vastuut tulisi määritellä selkeästi etukäteen myös mahdollisia poikkeamatilanteita varten.

- Toimintakulttuurilla ja prosesseilla on suuri merkitys uhkien havaitsemisessa, tunnistamisessa ja tiedon jakamisessa.

Tekoälyn käyttöönoton lisääntyessä myös toimitusketjuihin kohdistuva riski kasvaa, sillä tekoälyjärjestelmien integrointi organisaatioiden ympäristöihin luo uuden, potentiaalisesti haavoittuvan hyökkäyspinnan.

Avoimen lähdekoodin ohjelmistot erityisen alttiita riskille, jonka tekoälytyökalujen automaattinen haavoittuvuuksien etsintä muodostaa. Jopa 80 % ohjelmistoista hyödyntää tavalla tai toisella avointa lähdekoodia.

Toimitusketjuhyökkäys voi vaikuttaa lamauttavasti organisaation toimintaan. Kriittistä on ymmärtää omat alihankkijaketjut ja olla tietoinen sopimusyksityiskohdista palveluntarjoajien kanssa. On tärkeä selvittää kolmannen osapuolen tietoturvan taso ja ulottaa tietoturvallisuuden hallinta myös palveluihin, kattaen esimerkiksi:

- Konsultit ja heidän organisaatioidensa sisäiset järjestelmät.
- Laitteistot ja palvelut, joita voidaan käyttää joko osana omaa tuotetta, palvelukokonaisuutena tai ostettuna palveluna.

Organisaation tulee ymmärtää koko alihankintaketju, sillä myös organisaation alihankkija voi hankkia tuotteen tai palvelun seuraavana ketjussa olevalta palveluntarjoajalta.

- Varautuminen on keskiössä: Hyökkäysten vaikutusten pienentämiseksi organisaatioiden kannattaa pohtia palveluntarjoajaan tai toimitusketjun osaan kohistuvan hyökkäysten mahdollisia vaikutuksia, sekä tapoja häiriötilanteiden hallintaan.

4

Kriittisen infrastruktuurin suojaamisen tärkeys korostuu

Kriittiseen infrastruktuuriin ja organisaatioihin kohdistuvat kyberuhat ovat toimintaympäristön jatkuvan ja nopeaan muutoksen kohteina.

Suojelupoliisi ja sotilastiedustelu varoittivat heinäkuussa 2026 Venäjän FSB:n kybervakoilusta, jossa hyödynnetään huonosti suojattuja yritystason verkkolaitteita. Toiminnan kohteena on erityisesti kriittinen infrastruktuuri, kuten energia-ala ja puolustusteollisuus. ^[36]

Toimitusketjuihin kohdistuvien poikkeamien kautta kriittisen infrastruktuurin turvallisuuteen voi vaikuttaa laajan organisaation tietoturvakäytännöt.

- Verkon reunalaitteiden suojaaminen, ohjelmistojen ja laitteiden päivittäminen, toimitusketjujen tietoturvallisuuden varmistaminen ja laitteiden koko elinkaaresta huolehtiminen ovat keskeisiä suojaamistoimia.

Viimeisten vuosien aikana Suomessa on tapahtunut useita tietoliikenneinfrastruktuuriin kohdistuneita vahinkoja ja luonnonilmiöitä, sekä ulkopuolisten tekijöiden aiheuttamia tahallisia häiriöitä.

- Häiriönsietoa voidaan parantaa esimerkiksi kahdentamalla kriittisiä järjestelmiä ja yhteyksiä, sekä varmistamalla niiden sähkönsaanti lyhyen sähkökatkoksen varalta.
- Kaikkien tietoliikenne- ja tietojärjestelmäinfrastruktuurin omistajien kannattaa huolehtia viestintäverkkojen ja -palveluiden fyysisestä suojaamisesta.

5

Kiristyshaittaohjelmat ovat merkittävä uhka organisaatioille

Kiristyshaittaohjelmien määrä kasvaa globaalisti jatkuvasti. Kiristyshaittaryhmien toiminta on opportunistista, ja sen kohteet voivat muuttua nopeasti esimerkiksi uusien haavoittuvuuksien mukaan.

Kiristyshaittaohjelmien tapausmäärät voivat myös Suomessa muuttua yllättävästi. Kesällä 2026 Kyberturvallisuuskeskukselle tehtyjen kiristyshaittaohjelmailmoitusten määrä kääntyi kasvuun.^[37]

- Kiristystapaustoiminnan arviointiin pätee ns. Iceberg-viitekehys: tilastot eivät kerro koko totuutta. Toimintaa tapahtuu todennäköisesti enemmän kuin mitä sitä havaitaan ja raportoidaan.
- Suomessa kiristyshaittaohjelmien on havaittu viime aikoina kohdistuvan keskisuuriin tai pieniin organisaatioihin, joille hyökkäykset voivat aiheuttaa merkittäviä liiketoiminnallisia vaikutuksia.
- Kiristyshaittaohjelmamiö ja siihen liittyvä palvelutuotanto on jatkuvassa kehityksessä, ja esimerkiksi hyökkäysten eri osia on ulkoistettu palveluiksi.
- Heinäkuussa 2026 raportoitui ensimmäisestä täysin automatisoiduksi arvioidusta kiristyshaittaohjelmahyökkäyksestä, jossa koko kiristysoperaatio oli toteutettu tekoälyn avulla. Operaatio myös mukautui reaaliajassa ja yritti epäonnistuneita vaiheita uudelleen toisilla parametreilla. Eräessä tietoturvatutkijoiden tarkastelemassa vaiheessa kielimalli eteni epäonnistuneesta kirjautumisyrityksestä toimivaan ratkaisuun vain 31 sekunnissa.^[38]

Kiristyshaittaohjelma tartutetaan usein kalasteluviestin, infostealer-haittaohjelmien kautta vuotaneiden käyttäjätunnusten, päivittämättömien haavoittuvuuksien tai ClickFix-tekniikan kautta. Tiedostojen salaaminen ja muut hyökkääjän tekemät toimenpiteet saatetaan toteuttaa viipymättä sisäänkäynnin jälkeen.

Viime aikoina kansainvälisesti kiristyshaittaohjelma-hyökkäyksissä on korostunut tiedostojen salaamisen sijaan datan nopea varastaminen kohdejärjestelmästä. Tapauksissa kiristäjä lupaa lunnaita vastaan hävittää varastetun aineiston tai jättää sen julkaisematta.

Kiristyshaittaohjelmahyökkäys voi kohdistua toimitusketjuun ja levitä sitä kautta nopeasti useisiin organisaatioihin samalla kertaa. Varsinkin huoltovarmuuskriittisten organisaatioiden joutuessa uhriksi voivat yhteiskunnan elintärkeät toiminnot vaarantua.

- Kiristyshaittaohjelma saattaa pahimmassa tapauksessa lopettaa organisaation toiminnan kokonaan.
- Kiristyshaittaohjelmien torjunnassa ennaltaehkäisy, havainnointi ja nopea reagointi ovat avainasemassa. Varmuuskopiot voivat nopeuttaa kiristyshaittaohjelmahyökkäyksestä toipumista, mutta ne eivät kuitenkaan suojaa kiristyshaittaohjelmahyökkäyksen kohteeksi joutunutta organisaatiota tietojen vuotamiselta.

Tietoturva-alan kehitys, sääntely ja standardit

Tietoturva-alan kehitys -osiossa kerromme keskeisistä uudistuksista esimerkiksi alaa koskevan lainsäädännön tai asetusten päivityksiin liittyen. Kerromme kaikille tärkeää kyberturvallisuustietoa ja Kyberturvallisuuskeskuksen ajankohtaisista asioista.



Oikeudelliset asiat

Datakeskusrekisterilakia valmistellaan työ- ja elinkeinoministeriössä

- Työ- ja elinkeinoministeriö pyysi 3.9.2026 lausuntoja luonnoksesta hallituksen esitykseksi eduskunnalle laiksi datakeskusrekisteristä. Lausuntoja oli mahdollista antaa 2.10.2026 asti. ^[39]
- Laissa säädettäisiin datakeskusrekisteristä ja datakeskusten ilmoitusvelvollisuudesta sekä datakeskuksia koskevan tilannekuvan ylläpitämisestä.
- Rekisterin ylläpitäjänä, ilmoituksia vastaanottavana viranomaisena ja valvontaviranomaisena sekä tilannekuvan ylläpitäjänä toimisi Huoltovarmuuskeskus (HVK).
- Rekisteri ja sen perusteella ylläpidettävä tilannekuva antaisi viranomaisille kattavan kuvan Suomessa toimivista ja Suomeen suunnitelluista datakeskuksista, niiden käyttötarkoituksista, omistuksesta, sähkönkäytöstä sekä verkkovaikutuksista.
- Ehdotettu laki datakeskusrekisteristä on tarkoitettu tulemaan voimaan 1.1.2027.
- Lain voimaantulon hetkellä rakentamisvaiheessa tai toiminnassa olevasta soveltamisedellytykset täyttävästä datakeskuksesta olisi tehtävä ilmoitus 30.6.2027 mennessä.



Oikeudelliset asiat

Hallitus linjasi Suomen kannan EU:n pilvipalveluiden ja tekoälyn kehittämisen säädökseen (CADA)

- Euroopan komissio antoi 3.6.2026 ehdotuksen Euroopan teknologisen suvereniteetin paketista. Paketin yhtenä osana on ehdotus Euroopan parlamentin ja neuvoston asetukseksi pilvipalveluiden ja tekoälyn kehittämisen säädökseksi (Cloud and AI Development Act, CADA).
- Asetusehdotuksen tavoitteena on vahvistaa EU:n pilvipalvelu- ja tekoälyekosysteemiä, investointeja sekä infrastruktuuria.
- Asetus koostuisi kolmesta pilarista:
 - 1) Tutkimus-, kehittämis- ja innovointitoimet: kehittämistoimet, eurooppalaisia digitaalisia innovointihubeja (EDIH) seuraavat tekoälyn kokemus- ja kiihdyttämiskeskukset, ja jäsenvaltioiden pilvi- ja tekoälystrategiat
 - 2) Datakeskuskapasiteetti: datakeskusten nopean kehittämisen alueet, sujuvammat luvituskäytännöt, strategiset hankkeet ja keskitetyt tietopisteet
 - 3) Autonomia: luotaisiin varmuustasoja, joihin pilvipalvelujen tarjoajien tulisi vastata tarjotakseen palvelujaan julkisen sektorin toimijoille; keskusrekisteri tunnustetuista palveluista; jäsenvaltioiden riskiarvioinnit ja velvollisuus soveltaa kriteerejä; sekä velvollisuus nimetä toimivaltaiset viranomaiset
- Hallitus antoi ehdotusta koskevan kirjelmän eduskunnalle 10.9.2026 (U 54/2026 vp). Asian käsittely jatkuu eduskunnan valiokunnissa. ^[40]



Oikeudelliset asiat

Hallitus linjasi Suomen kannan 2 GHz:n satelliittiviestintää koskevaan EU-asetusehdotukseen (MSS)

- Euroopan komissio antoi 27.5.2026 ehdotuksen asetukseksi mobiilisatelliittiviestintäpalvelujen (Mobile Satellite Service, MSS) valtuuttamisesta 2 GHz:n taajuusalueella.
- Ehdotuksen tavoitteena on vahvistaa EU:n kilpailukykyä ja mahdollistaa valtiollisille toimijoille turvalliset, luotettavat ja kaikenkattavat palvelut erityisesti tilanteissa, jolloin maanpäälliset matkaviestinverkot eivät ole saatavilla tai toiminnassa.
- Hallitus antoi ehdotusta koskevan kirjelmän eduskunnalle 10.9.2026 (U 53/2026 vp). Suomi pitää tärkeänä, että tuleva sääntely turvaa kattavat satelliittiviestintäpalvelut koko EU:n alueella, myös harvaan asutuilla seuduilla. ^[41,42]
- Kattavat satelliittiyhteydet parantavat viestintäverkkojen toimintavarmuutta ja tukevat viranomaisten sekä kansalaisten mahdollisuuksia käyttää viestintäpalveluja myös poikkeus- ja häiriötilanteissa.
- EU:n tavoitteena on hyväksyä asetus vuoden 2026 loppuun mennessä.
- Nykyiset EU:n myöntämät toimiluvat 2 GHz:n taajuusalueelle päättyvät toukokuussa 2027, ja uusien toimilupien myöntäminen edellyttää asetuksen hyväksyntää.

Epäiletkö tietoturvaloukkausta?

Jos teihin on kohdistunut tai epäilette teihin kohdistuneen tietoturvaloukkauksen, olkaa yhteydessä Traficomin Kyberturvallisuuskeskukseen.

- Sähköinen lomake
www.kyberturvallisuuskeskus.fi/fi/ilmoita
- Sähköposti: cert@traficom.fi

Kyberturvallisuuskeskuksen eri toimintojen ja hankkeiden yhteystiedot löydät keskitetysti osoitteesta
www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/yhteystiedot.

Lähteet

Lähdeluettelo

1/4

1. <https://kyberturvallisuuskeskus.fi/fi/haavoittuvuudet>
2. <https://kyberturvallisuuskeskus.fi/fi/varoitukset/citrix-netscaler-adc-ja-gateway-tuotteissa-kriittisia-haavoittuvuuksia-useita-tietomurtoja-suomessa>
3. <https://www.sdxcentral.com/news/netscaler-bugs-bring-critical-sectors-down-in-europe/>
4. <https://dvv.fi/-/tuore-tutkimus-digitaalinen-luottamus-vahvistuu-vaikka-suurin-osa-suomalaisista-kohtaa-digihuijauksia>
5. <https://kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-402026>
6. <https://kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-392026>
7. <https://kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-382026>
8. <https://kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-372026>
9. <https://kyberturvallisuuskeskus.fi/fi/varoitukset/citrix-netscaler-adc-ja-gateway-tuotteissa-kriittisia-haavoittuvuuksia-useita-tietomurtoja-suomessa>
10. <https://cloud.google.com/blog/topics/threat-intelligence/defending-against-active-exploitation-of-citrix-netscaler-adc-and-gateway-appliances/>

Lähdeluettelo

2/4

11. <https://www.nrk.no/artikkel/russisk-hackergruppe-hevder-a-sta-bak-dataangrep-mot-norge-1526574>
12. <https://cert.dk/news/2026-09-24/Trusselsniveau-for-destruktive-cyberangreb-haeves-til-hoej>
13. https://www.kyberturvallisuuskeskus.fi/files/media/file/PQC%20Johdon%20tiivistelm%C3%A4_20260928.pdf
14. <https://kyberturvallisuuskeskus.fi/fi/varoitukset/citrix-netscaler-adc-ja-gateway-tuotteissa-kriittisia-haavoittuvuuksia-useita-tietomurtoja-suomessa>
15. <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/hankkeet-ja-projektit/ohjelmistoturvallisuus/opi-uhkamallintamaan>
16. <https://www.kyberturvallisuuskeskus.fi/fi/uutiset/tunnusten-kalastelusta-microsoft-365-tilikaappaukseen-nain-katkaiset-hyökkäysketjun>
17. <https://www.usenix.org/conference/vehiclesec26>
18. <https://www.finanssiala.fi/uutiset/suomalaisilta-yritettiin-alkuvuonna-huijata-60-miljoonaa-euroa-huijausyritysten-lukumaarat-hurjassa-kasvussa/>
19. <https://www.usenix.org/conference/vehiclesec26/presentation/lee>

Lähdeluettelo

3/4

20. <https://www.usenix.org/conference/vehiclesec26/presentation/low>
21. <https://www.usenix.org/conference/woot26/presentation/chen>
22. <https://www.europol.europa.eu/how-we-work/operations/operation-poweroff>
23. <https://www.verizon.com/about/news/breach-industry-wide-dbir-finds>
24. <https://www.cve.org/>
25. <https://www.kyberturvallisuuskeskus.fi/fi/kyberkestavyysaados-cra/kyberkestavyysaados-cyber-resilience-act-cra>
26. <https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-threat-hunting-report/>
27. <https://kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-372026>
28. <https://cloud.google.com/blog/topics/threat-intelligence/ai-vulnerability-exploitation-initial-access>
29. <https://kyberturvallisuuskeskus.fi/fi/haavoittuvuudet/haavoittuvuus-2026-27>
30. <https://kyberturvallisuuskeskus.fi/fi/haavoittuvuudet/haavoittuvuus-2026-28>
31. <https://kyberturvallisuuskeskus.fi/fi/haavoittuvuudet/haavoittuvuus-2026-29>

Lähdeluettelo

4/4

- 32. <https://kyberturvallisuuskeskus.fi/fi/haavoittuvuudet/haavoittuvuus-2026-30>
- 33. https://www.theregister.com/2025/10/07/gen_ai_shadow_it_secrets/
- 34. <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ole-valppaana-tekoalyn-kanssa>
- 35. <https://pudgycat.io/ai-found-500-zero-days-open-source/>
- 36. <https://supo.fi/-/suojelupoliisi-ja-sotilastiedustelu-varoittavat-yrityksia-venajan-fsb-n-verkkovakoilusta>
- 37. <https://www.kyberturvallisuuskeskus.fi/files/media/file/Kybers%C3%A4%C3%A4%20hein%C3%A4kuu%202026.pdf>
- 38. <https://www.sysdig.com/blog/jadepuffer-agentic-ransomware-for-automated-database-extortion>
- 39. <https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=968b0bcc-5f62-431c-b625-d60566c0b231>
- 40. <https://www.eduskunta.fi/asiat-ja-aanestykset/valtiopaivaasiat/U%2054%2F2026%20vp>
- 41. <https://lvm.fi/-/hallitus-linjasi-suomen-kannan-2-ghz-n-satelliittiviestintaa-koskevaan-eu-asetusehdotukseen>
- 42. <https://www.eduskunta.fi/asiat-ja-aanestykset/valtiopaivaasiat/U%2053%2F2026%20vp>