TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyberväder

Augusti 2025

#cyberväder

Cybervädret berättar om betydande säkerhetsincidenter och -fenomen under månaden.

Denna produkt är i första hand avsedd för dem som arbetar med informationssäkerhetsfrågor på olika nivåer i organisationer. Läsaren får en snabb helheltsbild av vad som har hänt och vad som kommer att hända på cybersäkerhetsfältet.

Cybervädret kan vara:  lugnt  oroande  allvarligt

Månadens nyckeltal

I en myndighetsoperation som koordinerades av INTERPOL åtgärdades cyberbrottslighet på olika håll i Afrika. Vid en internationell samarbetsoperation greps totalt 1 209 personer misstänkta för cyberbrott, och en betydande mängd infrastruktur som använts av brottslingar beslagtogs. [1]

Antalet anmälningar om dataintrång i Microsoft 365 som gjordes till Cybersäkerhetscentret tredubblades jämfört med juli. Det ökade antalet anmälningar beror huvudsakligen på att semestersäsongen tagit slut, men ökningen har varit ovanligt kraftig jämfört med tidigare år, särskilt när det gäller M365.

Cyberväder augusti 2025

Dataintrång och dataläckor

- Antalet dataintrång ökade mer än tredubbelt efter en lugn juli. Antalen fall har typiskt ökat i början av hösten när medarbetare kommer tillbaka till jobbet.
- I flera fall var bakgrunden till dataintrång fortfarande ett lyckat M365-nätfiske, när en skadlig länk kom från en bekant avsändare.
- Teams-samtal har också blivit vanligare som grundorsak för dataintrång i augusti. [2]

Bedrägerier och nätfiske

- Textmeddelandebedrägerier som gjorts i barnskyddets namn har gett betydande brottsvinst. Förlusterna för medborgare och organisationer uppgick i augusti till hundratusentals euro.
- Förutom e-post, textmeddelanden och telefonsamtal använder brottslingar numera också Microsoft Teams-samtal för bedrägerier. Bedragare som utger sig för att vara IT-support försöker få offret att installera en fjärrhanteringsprogramvara på sin enhet.

Skadeprogram och sårbarheter

- En kritisk sårbarhet i produkterna Citrix Netscaler ADC och NetScaler Gateway utnyttjas aktivt.
- I Finland och i världen har skadlig programvara som maskerar sig som en PDF-editor upptäckts. När man laddar ner program är det viktigt att beakta både det nedladdade programmets och webbplatsens tillförlitlighet.
- Världen över har det rapporterats om det första AI-baserade utpressningsprogrammet. Skadlig programvara kan med hjälp av AI skriva skadlig kod på en infekterad enhet, vilket försvårar dess identifiering och upptäckt.

Automation och IoT

- I Polen utsattes ett bristfälligt skyddat fjärrhanteringssystem för en liten elproducerande damm för missbruk. I Ukraina utsattes däremot öppet synliga webbkameror och ouppdaterade IoT-enheter på Internet för missbruk. [3 & 4]
- Incidenterna påminner om hur viktigt det är att skydda IoT- och automationssystem med grundläggande åtgärder.

Nätens funktion

- Överbelastningsangreppen orsakade inga betydande konsekvenser i finländska nättjänster.
- I världen rapporteras det dock fortlöpande om rekordstora överbelastningsangrepp. [5]

Spionage

- Myndigheter i flera länder varnade för cyberspionage utfört av en APT-grupp med kopplingar till Kina, med bland annat följande mål: teleoperatörer och leverantörer av internettjänster.
- Gruppen har i offentligheten kallats bland annat Salt Typhoon, Operator Panda och Ghost Emperor.
- Också Skyddspolisen från Finland deltog i publikationen.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Ansökan om finansieringsstöd för att stödja genomförandet av cybersäkerhetslagen öppnades i augusti. Transport- och kommunikationsverket Traficom kan bevilja stöd till mikroföretag samt små och medelstora organisationer som omfattas av tillämpningsområdet för att uppfylla kraven i cybersäkerhetslagen och höja aktörernas cybersäkerhetsnivå inom organisationen. Ansökan är öppen till 16.10.2025 kl. 16:15. [6]

Traficom publicerade tillsammans med Skyddspolisen ett meddelande om hotnivån för Finlands cybersäkerhet. Hotnivån steg i och med kriget i Ukraina år 2022 och har förblivit förhöjd. Antalet allvarliga incidenter som utretts av Cybersäkerhetscentret har mer än fördubblats jämfört med i fjol. [7]

EU:s informationssäkerhetskrav för radioutrustning började tillämpas i början av augusti. Regleringen omfattar utrustning som använder radiofrekvenser, såsom telefoner, smartklockor och babyvakter. De nya spelreglerna förbättrar konsumenternas informationssäkerhet, eftersom endast radioutrustning som uppfyller informationssäkerhetskraven får släppas ut på EU-marknaden i fortsättningen. [8]

Allmän översikt över cybersäkerheten i augusti

Augusti markerade slutet på den lugna sommarsäsongen. Att semestrarna tog slut och att folk återvände till sina arbetsplatser syntes tydligt i form av ett ökat antal incidenter samt en återgång till vardagen i antalet anmälningar som Cybersäkerhetscentret tog emot.

- Betydande fenomen i augusti var bland annat sårbarheter och dataintrång, vilka även betonades i den internationella nyhetsrapporteringen om cybersäkerhet. Den globala SharePoint-sårbarheten som oroade under juli och augusti väckte även bekymmer i Finland, men antalet lyckade utnyttjanden har förblivit relativt lågt. Cyberangreppen mot dammanläggningar i Norge och Polen understryker vikten av att beakta säkerhetsaspekter och skydda sårbara system – oavsett bransch eller mål. [3 & 9]

Det totala antalet anmälningar om dataintrång som togs emot i augusti nådde årets toppnivå. På grund av flera lyckade dataintrång kan man även i september förvänta sig många observationer av nätfiske och försök till dataintrång.

- I vissa dataintrångsfall som upptäckts i Finland har tekniken Adversary-in-the-Middle (AiTM) använts för att kringgå multifaktorautentisering. Vid kapningen i ett angrepp kan det till exempel skapas en regel i e-postkontot som automatiskt flyttar inkommande meddelanden till mappen för borttagna eller arkiv och markerar dem som lästa. Med hjälp av omdirigeringsregler försöker brottslingen dölja aviseringar och förfrågningar om uppföljningsmeddelanden som skickats från kontot för användaren. [10]

Nätfiske har varit ett betydande hot under hela sommarsäsongen. Augusti var inget undantag från trenden, och en ökning observerades särskilt i nätfiske riktat mot Microsoft 365-konton. Det totala antalet anmälningar relaterade till nätfiske verkar dock ha stabiliserats efter sommarens kraftiga uppåtgående trend.

- Cybersäkerhetscentret tog emot flera anmälningar om nätfiskefall där meddelandet kom från en för avsändaren känd part. Rubriken i ett nätfiskemeddelande kan till exempel hänvisa till en delad fil. Länken i meddelandet leder ofta till ett dokument som delas via organisationens Online SharePoint- eller OneDrive-tjänst. Den egentliga nätfiskelänken är dock en ny länk som är inbäddad i det delade dokumentet och den leder till en falsk inloggningssida för Microsoft 365. [11]

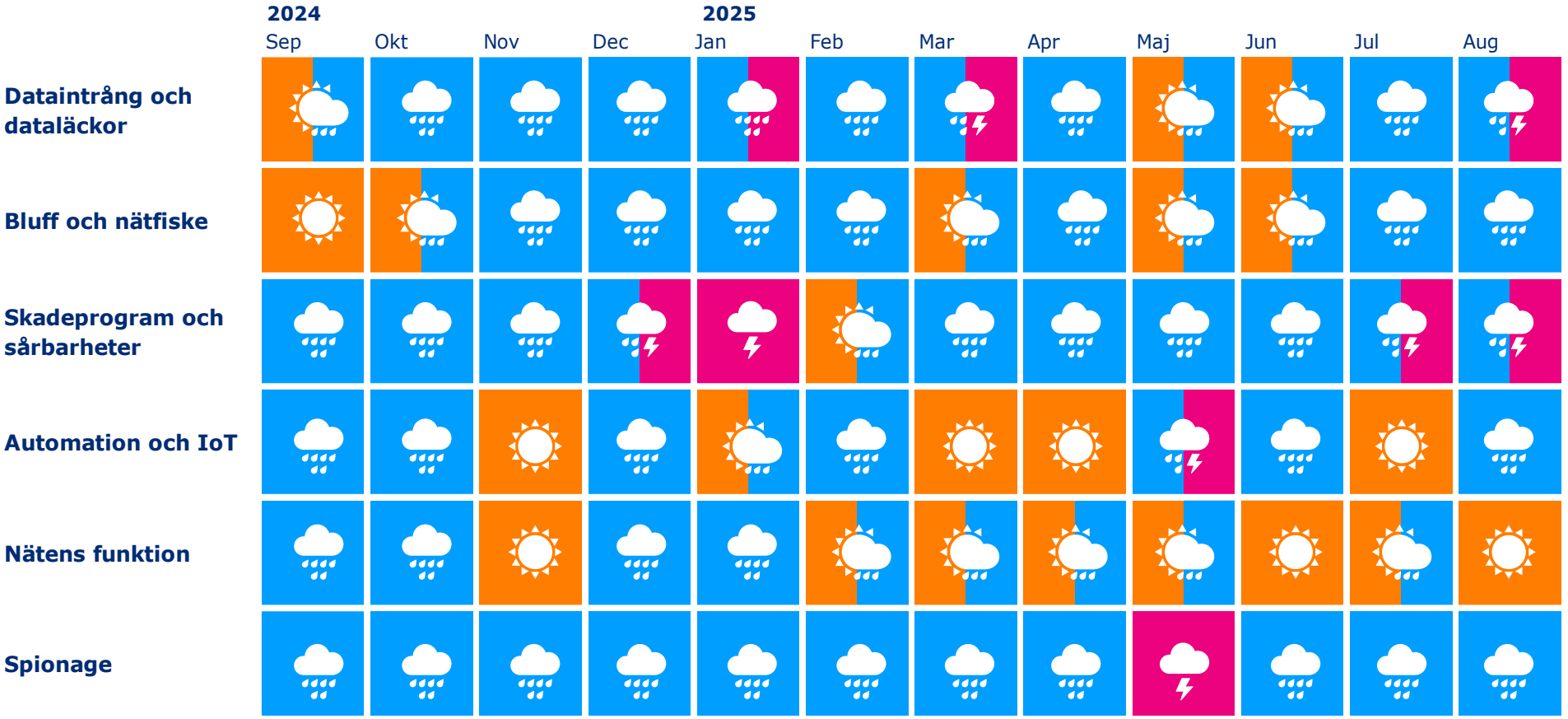
- När semestern är över är det skäl att påminna personalen om faran med nätfiske. I början av hösten är det bra att gå igenom till exempel gemensamma spelregler samt olika sätt att identifiera potentiella nätfiskemeddelanden och bedrägeriförsök. Att till exempel kontrollera länkar och webbadresser är en enkel men viktig färdighet för att undvika många hot. [11] Cybersäkerhetscentret har publicerat anvisningar bland annat för identifiering av nätfiske där AiTM-tekniken utnyttjas [10]

Trender inom sektorer och fenomen

I denna sektion går vi igenom utvecklingen och trender inom cybersäkerhetsfenomen på olika perioder. De sektorspecifika delarna beskriver läget på olika sektorer på allmän nivå.

1 kk

Trenderna inom cybersäkerhet
de gångna 12 mån.



Lång sikt och den närmaste framtiden

I avsnittet visas cyberfenomen på lång sikt och i den närmaste framtiden. Ett långfristigt fenomen analyseras i mer detalj varje månad. Top 5 cyberhot berättar för sin del om hoten i den närmaste framtiden.

Cybervädret på lång sikt (5 år +): fenomen som vi följer upp

Cybervädret på lång sikt: Nätens säkerhet

Betydande incidenter som gäller nätverkens säkerhet är sällsynta, men till exempel överbelastningsangrepp utgör ett ständigt hot. På grund av hur internet fungerar går det inte att helt förhindra överbelastningsangrepp – inte heller i framtiden.

- Företag som erbjuder skyddsmekanismer mot överbelastningsangrepp rapporterar regelbundet om rekordstora överbelastningsangrepp som de har upptäckt. [12]
  - Även om allvarliga störningar uppstår sällan har återkommande överbelastningsangrepp ekonomiska och samhälleliga konsekvenser. Angreppen syftar till att belasta samhällets resurser och undergräva förtroendet för digitala tjänster. [13]
- Industrialiseringen av cyberbrottsligheten har gett upphov till ett specialiserat ekosystem för DDoS-as-a-Service, där angreppen har blivit lättillgängliga konsumenttjänster.
  - Även om internationella polisoperationer lyckas slå ut dessa tjänster, anpassar sig den kriminella marknaden som helhet snabbt och återhämtar sig. [14] Tjänsterna som erbjuds till kriminella utvecklas dessutom till att bli allt mer professionella och lättanvända.
- Vid överbelastningsangrepp används omfattande bottnätverk som består av vanliga människors enheter världen över, infekterade med skadlig programvara.
  - Hittills använder endast 68 % av världens befolkning internet, men antalet användare ökar hela tiden. [15] I framtiden innebär det sannolikt ännu fler dåligt skyddade internetanslutna enheter som brottslingar försöker kapa och använda i sina botnätverk.
  - Botnätverk som består av dåligt skyddade konsumentenheter används aktivt även för cyberspionage. [16]

Utveckling, reglering och standarder inom informations-säkerhetssektorn

I sektionen Utveckling inom informationssäkerhetssektorn berättar vi om de centrala reformer som hänför sig till exempel till uppdateringar i lagstiftningen eller föreskrifter inom sektorn. Vi ger alla viktig information om cybersäkerhet och om aktuella frågor vid Cybersäkerhetscentret.

Juridiska frågor

Delvis tillämpning av EU:s AI-förordning inleddes i början av augusti [17 & 18]

- Syftet med EU:s AI-förordning är att säkerställa att AI-system som släpps ut på marknaden och tas i bruk inom EU inte äventyrar människors hälsa, säkerhet eller grundläggande rättigheter.
- Förordningen reglerar AI-system utifrån de risker de medför. Användningsområden för AI som anses vara särskilt skadliga förbjuds, och striktare krav ställs på vissa AI-system som klassificeras som högrisk.
- AI-förordningen trädde i kraft den 2 augusti 2024 och dess tillämpning sker stegvis. Bestämmelserna i förordningen, bland annat om allmänna AI-modeller, har börjat tillämpas i EU-länderna från och med den 2 augusti 2025. Allmänna AI-modeller omfattar till exempel stora generativa AI-modeller.
- AI-förordningen är i princip direkt tillämplig rätt, men förutsätter kompletterande nationell lagstiftning.
- Regeringens proposition om kompletterande nationell lagstiftning för att genomföra EU:s AI-förordning (RP 46/2025 rd) lämnades till riksdagen den 8 maj 2025, men behandlingen av propositionen pågår fortfarande i riksdagen. Därför träder den nationella lagstiftningen om myndigheternas uppgifter, utpekandet av anmälda organ och påföljder inte i kraft ännu den 2 augusti 2025.

Misstänker du en informationssäkerhetsincident?

Om ni blivit utsatt för en informationssäkerhetsincident, vänligen kontakta oss.

- Elektronisk blankett https://www.kyberturvallisuuskeskus.fi/sv/anmal
- E-post: cert@traficom.fi
- Telefon: 0295 345 630 (vardagar kl. 9-15)

I övriga frågor kan ni kontakta oss på adressen cybersakerhetscentret@traficom.fi

Kontaktuppgifter för Cybersäkerhetscentrets funktioner och projekt hittar du centralt på: https://www.kyberturvallisuuskeskus.fi/sv/kontakta-oss/kontaktuppgifter

Källor

1) African authorities dismantle massive cybercrime and fraud networks, recover millions https://www.interpol.int/News-and-Events/News/2025/African-authorities-dismantle-massive-cybercrime-and-fraud-networks-recover-millions
2) Angriparna utger sig för att vara IT-stöd i Teams samtal https://www.cybersäkerhetscentret.fi/sv/aktuellt/cybersakerhetscentrets-veckooversikt-352025#89484-2
3) Russian Hackers Breach Polish Hydropower Plant in Major Cyberattack https://united24media.com/latest-news/russian-hackers-breach-polish-hydropower-plant-in-major-cyberattack-10882
4) The Resurgence of IoT Malware: Inside the Mirai-Based Botnet Campaign https://www.fortinet.com/blog/threat-research/iot-malware-gayfemboy-mirai-based-botnet-campaign
5) Hyper-volumetric DDoS attacks skyrocket: Cloudflare's 2025 Q2 DDoS threat report https://blog.cloudflare.com/ddos-threat-report-for-2025-q2/
6) Ansökan om finansieringsstöd för verkställandet av cybersäkerhetslagen har öppnats https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/ansokan-om-finansieringsstod-att-stoda-verkstallandet-av-cybersakerhetslagen-har-oppnats
7) Traficom och Skyddspolisen: Hotnivån mot cybersäkerhet har förblivit förhöjd - antalet allvarliga incidenter ökar https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/traficom-och-skyddspolisen-hotnivan-mot-cybersakerhet-har-forblivit-forhojd-antalet
8) Smartklockor, babyvakter och mobiltelefoner blir allt säkrare – EU skärper kraven på informationssäkerhet https://traficom.fi/sv/aktuellt/smartklockor-babyvakter-och-mobiltelefoner-blir-allt-sakrare-eu-skarper-kraven-pa
9) Norway spy chief blames Russian hackers for dam sabotage in April https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/
10) AiTM-angrepp och hur de kan avvärjas (AiTM (adversary-in-the-middle) https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/vid-dataintrang-i-m365-anvands-allt-oftare-natfisketekniken-aitmh
11) Cybersäkerhetscentrets veckoöversikt – 33/2025 https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-332025
12) https://blog.cloudflare.com/ddos-threat-report-for-2025-q2/
13) Estimating the Societal Cost of DDoS Attacks: A Dual-Lens Model for National Impact Assessment https://thegfce.org/wp-content/uploads/2025/08/Societal-Cost-DDoS-Attacks-Carlos-Alvarez.pdf
14) Assessing the Aftermath: the Effects of a Global Takedown against DDoS-for-hire Services https://www.usenix.org/conference/usenixsecurity25/presentation/vu
15) International Telecommunication Union – Statistics https://www.itu.int/en/ITU-D/Statistics/pages/stat/default.aspx
16) Hotnivån mot cybersäkerhet har förblivit förhöjd– antalet allvarliga incidenter ökar https://supo.fi/sv/-/hotnivan-mot-cybersakerhet-har-forblivit-forhojd-antalet-allvarliga-incidenter-okar
17) Det nationella genomförandet av EU:s förordning om artificiell intelligens https://https://tem.fi/sv/forordning-om-artificiell-intelligens
18) Arbetsgruppen för nationellt genomförande av EU:s förordning om artificiell intelligens https://tem.fi/sv/projekt?tunnus=TEM044:00/2024