

TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

Augusti 2026

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 helhetsbild av vad som har hänt och vad som kommer att hända på cybersäkerhetsfältet.

Cybervädret kan vara:



lugnt



oroande



allvarligt



Det allmänna läget i cybervädet i augusti 2026

Cybervädet fortsätter vara regnigt

Cybersäkerhetsläget i Finland i augusti präglades särskilt av nätfiske, intrång i webbtjänster och nya skyldigheter till följd av EU-regleringen. Som väntat ökade även antalet Microsoft 365-kontointrång efter sommarsemestertiden.

Nätfisket tog sig många olika uttryck: lönebedrägerier, bedragare som utgav sig för att vara cybersäkerhetsexperter och bedragare som utgav sig för att vara support för snabbmeddelandeappen Signal.

I augusti fortsatte utnyttjandet av sårbarheten i kärnprogramvara som offentliggjordes i juli. I angreppen har komprometterade webbplatser använts för att sprida skadlig programvara till webbplatsbesökare. Sårbarheten har utnyttjats för att genomföra ett mycket stort antal dataintrång i finländska webbplatser.

Utomlands har det verkligen åskat ordentligt

- Den offentliga sektorn har drabbats av cyberangrepp i flera länder.
- Lettlands fordonsregistersystem drabbades av ett dataintrång och dataläcka i augusti. I dataintrånget fick angriparna personuppgifter för 1,2 miljoner människor från flera år.
- I Tyskland blev två ministerier i delstaten Berlin offer för ett angrepp med utpressningsprogram, och till följd av detta tvingades ministerierna koppla bort sig från nätet.
- I Frankrike fortsatte de omfattande dataintrång som präglat hela året genom ett angrepp mot skatteförvaltningen som blev offentlig i augusti. Vid angreppet röjdes uppgifter om cirka 680 000 personer eller företag.

Cybersäkerhetscentrets åtgärder och tips för förberedelser



Håll webbplatserns publiceringssystem (såsom WordPress) och deras tillägg uppdaterade hela tiden, och ta bort onödiga tillägg samt användarkonton. I somras uppdaterade vi vår guide för informationssäkerhet i Wordpress.



Myndigheter och organisationer har tillsammans inlett en kampanj för säker internetanvändning inför det nya läsåret. Traficoms och polisens webbplats Var försiktig på webben erbjuder praktiska tips för vårdnadshavare och barn för informationssäkerheten i vardagen.



Vi publicerade anvisningar som hjälper företag att förstå när de måste berätta användare om användningen av artificiell intelligens eller om innehållet som det producerat. I praktiken gäller det till exempel chatbotar som skapas på webbsidorna och för vilka man alltid ska berätta användare att de pratar med AI-chattbot. Vi rekommenderar att företagen utnyttjar kommissionens anvisningar, uppförandekoder och ikoner vid genomförandet av skyldigheterna.

Fenomen i cybervärdet

I denna sektion går vi igenom
utvecklingen och trender
inom cybersäkerhetsfenomen.



Fenomen i cybervädret augusti 2026



Dataintrång och dataläckor

- I augusti anmäldes en hel del dataintrång.
- I det största dataintrånget utnyttjade angriparna sårbarheter som angreppsvektor.
- I Microsoft 365-dataintrång framhövdes nätfiske med enhetskoder.



Skadliga program

- Under augusti observerades många webbsidor där man delade skadliga program med hjälp av ClickFix-tekniken.
- Under granskningsperioden rapporterades till Cybersäkerhetscentret två incidenter om utpressningsprogram.



Sårbarheter

Antalet sårbarheter fortsatte att öka också i augusti.
I augusti observerades dataläckor som skett via sårbarheter.



Bedrägerier och nätfiske

- Brottslingar lurade igen organisationers anställda som kom tillbaka från semestern.
- Tro inte på en bedragare som ringer och som utger sig för att vara från tekniskt stöd eller på grund av cybersäkerhet.



Automation och IoT

- De trafikkameror som Slovakien köpt in visade sig ha brister i informationssäkerheten och vara rysktillverkade, vilket medför en risk för att de kan utnyttjas i militärt underrättelsesyfte.
- I routrar som tillverkats av den kinesiska tillverkaren ZBT har flera bakdörrar identifierats.



Nätens funktion

- Överbelastningsangrepp orsakade inte några betydande störningar i Finland.
- Näten fungerade normalt.



Fenomen i cyberväddret

augusti 2026 1/2



Dataintrång och dataläckor

- Dataintrång i sårbara WordPress-webbplatser stod för en betydande del av de dataintrång som utfördes genom exploatering av sårbarheter.
- I augusti meddelades att 51 % av dataintrång i Microsoft 365 genomfördes med nätfiske med enhetskoder och 44 % med AiTM-nätfiske. Brottslingar utnyttjade också Microsoft Teams-diskussioner när de tog kontakt med ekonomidirektörer och pressade på dem för att göra penningöverföringar eller betala räkningar brådskande.
- Ett dataintrång i juli visade sig vara allvarligt i fortsatt utredning: över 10 000 personers personuppgifter läckte ut.



Skadliga program

- I augusti observerades flera webbplatser i det finländska cyberrymden där man delade skadliga program genom att använda ClickFix-tekniken. Antalet dataintrång i WordPress-webbplatser har medfört att även ClickFix-incidenter har ökat avsevärt.
- I augusti fick Cybersäkerhetscentret två anmälningar om incidenter om utpressningsprogram. Bakom angreppet i båda fallen var internationellt kända kriminella grupper, t.ex. Qilin- och Krybit-grupper.



Sårbarheter

- Allvarlig och aktivt utnyttjad sårbarhet i N-able N-Central-server (på finska)(CVE-2026-18556, CVE-2026-18577)
- Metabase – en sårbarhet i programvara som gör det möjligt för en oautentiserad angripare att genomföra en SQL-injektionsangrepp på distans (CVE-2026-72898)
- Kritiska sårbarheter i Citrix Netscaler ADC och Gateway –produkter (CVE-2026-19489, CVE-2026-19490)



Fenomen i cybervädret

augusti 2026 2/2



Bedrägerier och nätfiske

- I augusti riktade cyberkriminella in sig på personer som återvände från semestern. Bland de väntande e-postmeddelandena fanns också "brådskande" nätfiskemeddelanden som syftade till att få arbetstagare som återvände från semestern att klicka på bedrägliga länkar.
- Lita inte på en bedragare som utger sig att vara en säkerhetsmyndighet. Om någon påstår sig ringa av cybersäkerhetsskäl eller erbjuda en obligatorisk applikationsuppdatering eller teknisk support, bör man inte lita på uppringaren. Man ska aldrig lämna ut lösenord, återställningsnycklar, användarkoder, PIN-koder eller andra verifieringskoder per telefon.



Automation och IoT

- Hundratals trafiksäkerhetskameror som den slovakiska staten upphandlat visade sig vara tillverkade i Ryssland. I dem upptäcktes odokumenterade bakdörrar genom vilka de kunde tas över helt och hållet. Kamerorna hade sålts av ett cypriotiskt brevlådeföretag. Osäkra trafiksäkerhetskameror har i andra delar av världen utnyttjats för spionage och militär underrättelseverksamhet, och detta väcker oro även i Slovakien.
- I routrar som tillverkats av det kinesiska företaget ZBT har flera bakdörrar upptäckts, vilka gör det möjligt att ta kontroll över dem. Utrustning som tillverkats av ZBT säljs även under många andra varumärken.

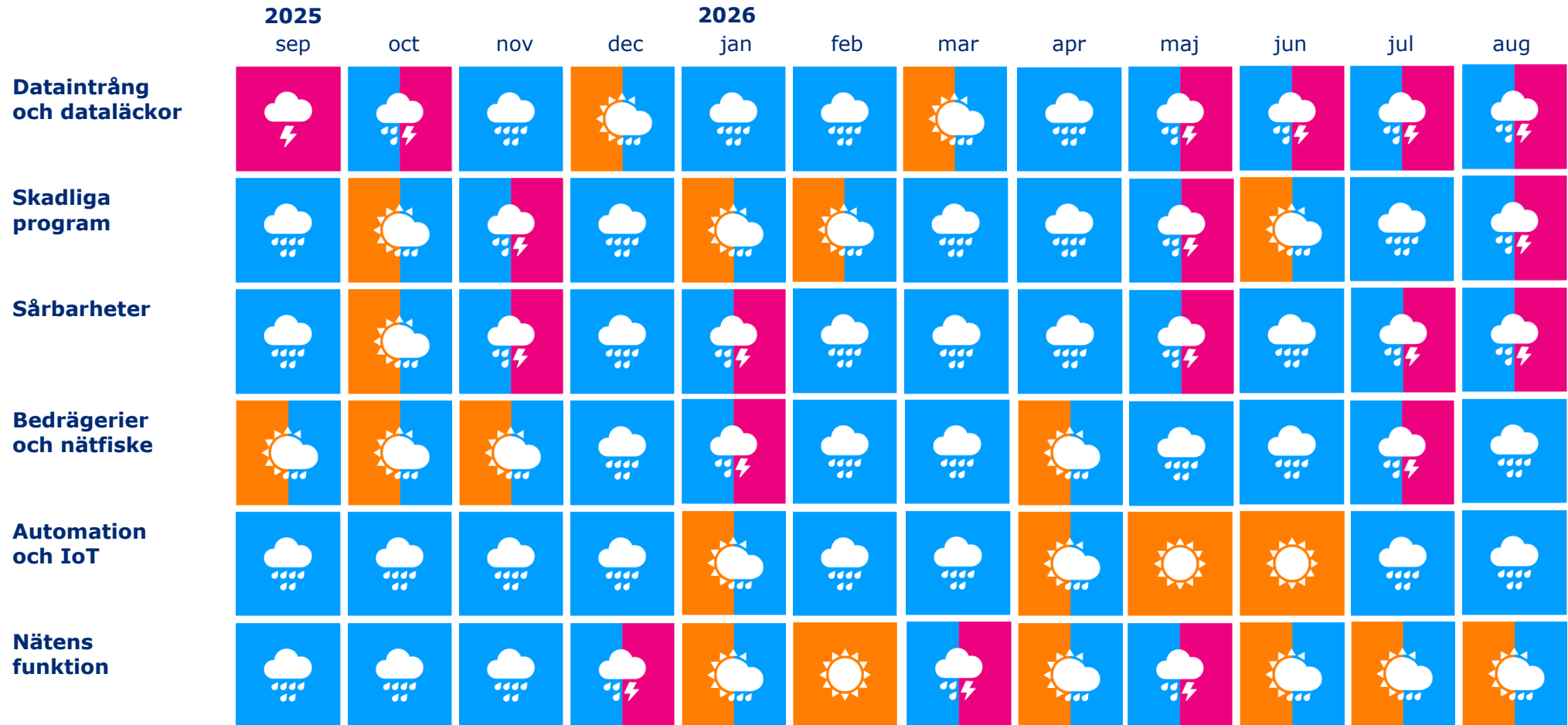


Nätens funktion

- Antalet superbotnät som består av kapade IoT-, server- och molninfrastrukturer ökar, och deras potentiella mängd angreppstrafik utgör en betydande risk för tillgängligheten hos digitala tjänster.
- Den proryska hacktivistgruppen Server Killers har tagit på sig ansvaret för flera överbelastningsangrepp runt om i Europa. Den mest betydande av dessa var angreppet mot den norska statsförvaltningen.



Fenomen i cybervädret de gångna 12 mån.



Cyberväderprognos

Cyberväderprognosen är en på tidigare observationer baserad sammanfattning och en riktgivande bedömning av de cyberhot och utvecklingstrender som kan väntas under de kommande månaderna.



Cyberväderprognos

Cyberhoten förblir normala

Inga betydande förändringar väntas i cybervädret. Det är sannolikt att utnyttjandet av de sårbarheter som observerades under sommaren kommer att fortsätta.

Det kan förväntas att antalet fall ökar när hösten närmar sig, på samma sätt som under föregående år.



Cyberväderprognosen är en på tidigare observationer baserad sammanfattning och en riktgivande bedömning av läget med cyberhoten. Bedömningen ska inte användas som sådan för beredskap inför cyberhot utan man ska använda organisationsspecifik information och analys som stöd till bedömningen.

Organisationens beredskap

- Ur sårbarhetssynpunkt är det mycket viktigt att organisationer regelbundet inventerar sina enheter och system, eftersom det i de observerade fallen förekommer exempel på föråldrad utrustning och programvara som organisationerna inte kände till fanns kvar i drift.
- Den snabba förändringen i uppdateringscykeln kräver aktiv uppföljning.
- Tillverkarna informerar ofta i förväg om kommande uppdateringar, vilket gör det viktigt att följa dessa meddelanden och planera de egna åtgärderna därefter.



Oroande

Antalet cyberhot och deras allvar är på normal nivå.

Cyberhoten kan dock förändras snabbt, även mot negativ riktning.