TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyberväder

Juli 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

Cybervädret juli 2025

Dataintrång och dataläckor

- Antalet dataintrång minskade något under perioden, men försöken ökade.
- 70–80 procent av de rapporterade fallen var kopplade till en sårbarhet i SharePoint. Detta visar på vikten av regelbundet underhåll och uppdateringar av systemen.
- I de fall där intrången lyckades ökade mängden dataläckor.
- I många intrångsförsök lyckades dock säkerhetsåtgärderna förhindra åtkomst.

Bedrägerier och nätfiske

- Bedrägerimeddelanden skickades i Traficoms och Centralkriminalpolisens namn, med hot om böter och barnpornografianklagelser. Genom dessa bedrägerier försökte man komma över bankkoder.
- Ett aggressivt e-postbedrägeri krävde betalning i bitcoin och hotade att avslöja känsliga bilder av offret. Alla påståenden i meddelandet var falska, och utpressaren skickade samma hot till tusentals mottagare. De påstådda bilderna existerar inte.

Skadeprogram och sårbarheter

- En sårbarhet i Microsoft SharePoint-produkter (CVE-2025-53770) har utnyttjats i stor omfattning globalt.
- Exploatering av sårbarheterna i Citrix NetScaler-produkter (CVE-2025-5777 och CVE-2025-5349) har fortfarande observerats runt om i världen.
- Skadeprogrammet Android.BadBox2 upptäcks fortfarande i den finländska nätverkstrafiken. Denna programvara påverkar Android-baserade smarta enheter och ansluter dem till ett botnät.

Automation och IoT

- Cybersäkerhetsförordningen enligt radioutrustningsdirektivet (RED) trädde i kraft i februari 2022 och började tillämpas den 1 augusti 2025.
- Förordningen inför de första obligatoriska cybersäkerhetskraven för trådlösa internetanslutna enheter inom EU. Produkter som inte uppfyller kraven kan dras tillbaka från marknaden.
- Traficom ansvarar för marknadstillsynen av förordningen i Finland.

Nätens funktion

- En internationell polisoperation genomfördes mot den pro-ryska hacktivistgruppen NoName057(16). Operationen resulterade i arresteringsorder, genomsökningar och beslag, samt avstängning av kriminell IT-infrastruktur.
- Trots den framgångsrika operationen har NoName057(16) fortsatt sin verksamhet under juli.

Spionage

- Sårbarheter i SharePoint har också utnyttjats i Finland i dataintrång och intrångsförsök.
- Enligt Microsoft har både APT-aktörer och kriminella dragit nytta av sårbarheten.
- Storbritannien har infört sanktioner mot aktörer kopplade till den ryska militära underrättelsetjänsten. Även EU och Nato har fördömt Rysslands agerande.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Organisationen för säkerhet och samarbete i Europa (OSSE) höll sin jubileumskonferens Helsinki +50 i Finlandiahuset den 31 juli. Cybersäkerhetscentret följde cybersäkerhetsläget under hela evenemanget. Både konferensdagen och veckan före förlöpte lugnt, utan att några betydande avvikelser observerades.

I slutet av juli observerades flera fall av en aggressiv utpressningskampanj i Finland. Pornografitemade utpressningsmeddelanden har skickats till både privatpersoner och organisationer, med krav på betalning i bitcoin. Meddelandets ämnesrad var ofta ”samarbetserbjudande”, och avsändarens e-postadress hade förfalskats till mottagarens egen adress. Det rör sig om ett bedrägeri — angriparen har ingen åtkomst till enheten.

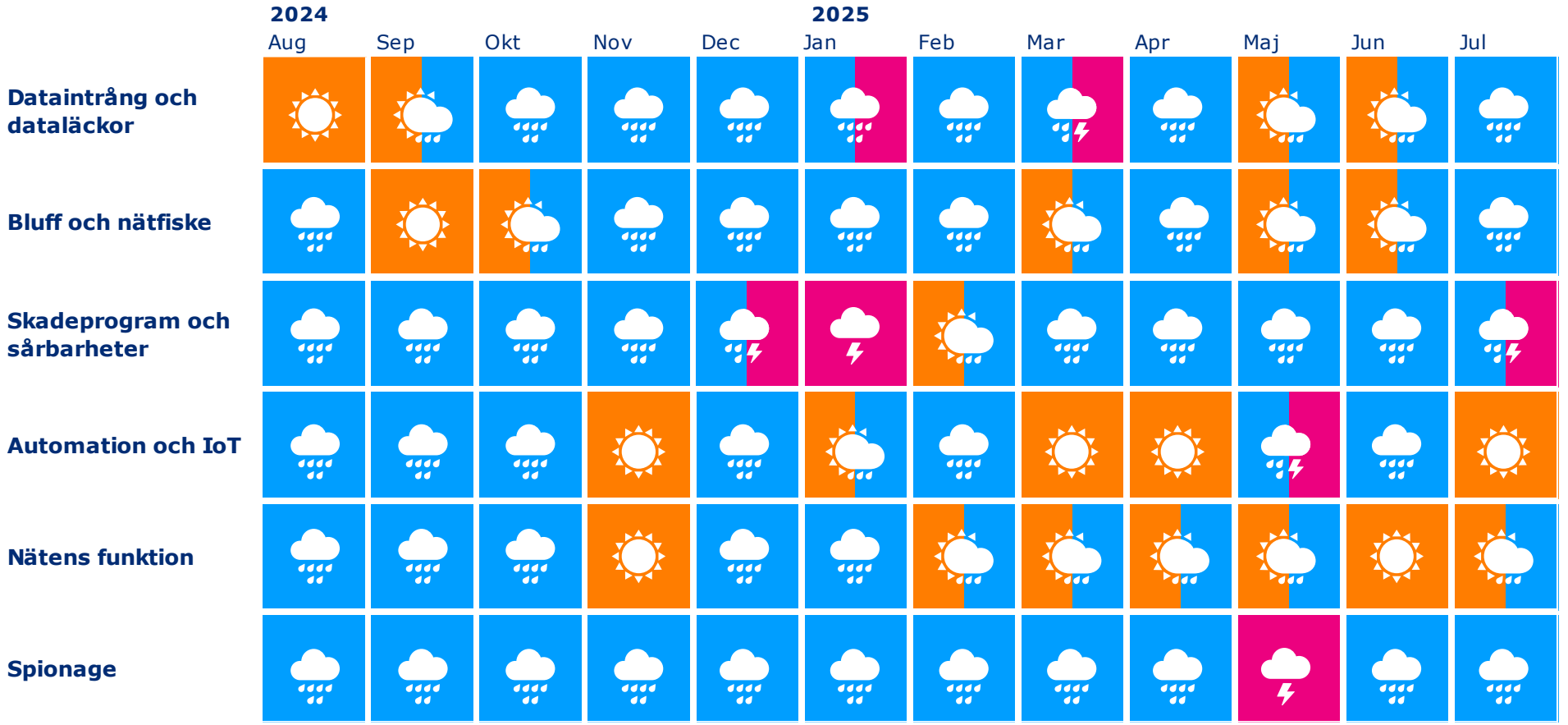
En allvarlig sårbarhet har upptäckts i Microsoft SharePoint-tjänsten, som påverkar lokala SharePoint Server-produkter. Sårbarheten har utnyttjats globalt.

Allmän översikt över cybersäkerheten i juli

Juli inleddes lugnt ur cybersäkerhetssynpunkt, men väderläget försämrades mot månadens slut:

- Under månaden observerades dataintrång som försvagade den allmänna bilden av cybersäkerheten jämfört med tidigare sommarmånader.
  - I Finland riktades intrång mot ett antal företag inom olika sektorer. Vid intrången lyckades man stjäla data som omfattade personuppgifter. I de flesta fall innehöll dock data inte de mest känsliga uppgifterna, såsom personbeteckningar.
- Allvarliga globala sårbarheter har bidragit till olika typer av cyberattacker.
  - Under juli upptäcktes en allvarlig sårbarhet i Microsoft SharePoint-tjänsten, som har utnyttjats globalt. Sårbarheten berör lokalt drivna SharePoint Server-tjänster och påverkar inte den molnbaserade versionen.
  - Sårbarheten har utnyttjats i betydande dataintrång runtom i världen. Utnyttjandet av sårbarheten framträder också i cirka 70–80 procent av de nationella dataintrångsfallen i juli.
- Angripare använder Microsoft 365:s Direct Send-funktion för att skicka meddelanden som ser ut att komma inifrån organisationen. Metoden gör det möjligt att kringgå e-postens skräppostfilter och regler. Det rekommenderas att kontrollera inställningarna för funktionen Reject Direct Send samt att använda strikta SPF/DMARC-konfigurationer och multifaktorautentisering.
- Observationer av skadeprogram jämnades ut något jämfört med juni.
  - Observationerna av skadeprogrammet BadBox 2.0 stabiliserades efter juni. Hotet som skadeprogrammet utgör har dock inte försvunnit, eftersom Google rapporterar att det har infekterat upp till 10 miljoner enheter globalt.

Trenderna inom cybersäkerhet
de gångna 12 mån.



Top 5-hot i den närmaste framtiden (6 månader– 2 år)

1.

Allvarliga sårbarheter utnyttjas allt snabbare

Förutom att installera en korrigerande uppdatering är det ofta nödvändigt att undersöka om sårbarheten redan utnyttjats innan man installerar uppdateringen.

2.

Informationssäkerheten och kontinuiteten i leverans- och servicekedjor är allt mer kritiska.

Att förstå underleverantörskedjorna är centralt för organisationernas egen cybersäkerhet. De flesta organisationer är mer eller mindre beroende av utlagda digitala tjänster.

3.

Organisationer bör vara förberedda för AI-relaterade utmaningar.

Det skulle vara bra för organisationer att identifiera de utmaningar som artificiell intelligens medför och förbereda sig på dem till exempel genom att utbilda sin personal.

Ny

Uppdaterad

Symboler

4.

Utpressningsprogram - Betydande hot mot organisationer

Under det senaste året har flera organisationer i Finland drabbats av ett utpressningsprogram, och antalet ökar kontinuerligt också globalt.

5.

Skyddet av kommunikationsinfrastruktur blir allt viktigare

Skyddet av kommunikations- och systeminfrastruktur är viktigt utomlands och i Finland, både på grund av de skador och naturfenomen som de blir utsatta för samt på grund av avsiktliga störningar orsakade av utomstående.