TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyberväder

Oktober 2025

Cybervädret oktober 2025

Dataintrång och dataläckor

- M365-dataintrång har fortsatt att öka. Försök till dataintrång rapporterades mindre än tidigare.
- I oktober rapporterades om globala informationsläckor som hänt redan tidigare och som även omfattade finska offer.
- Sveriges stamnätsbolag Svenska kraftnät drabbades av ett dataintrång där hotaktören Everes har påstått att ha läckt ut 280 Gt data. I offentligheten bekräftades att intrånget gäller en begränsad extern dataöverföringslösning.

Automation och IoT

- Dragos årsrapport och ENISAs rapport Threat Landscape 2025 publicerades i oktober.
- I ENISAs rapport konstateras att mobilapparater fortfarande är det gränssnitt som angriparna använder mest. Antalet OT-angrepp mot industri och kritisk infrastruktur ökar.

Bedrägerier och nätfiske

- I bedrägerisamtalen har man utgett sig för att vara myndighetsföreträdare. Brottslingar har påstått att de ringer från Cybersäkerhetscentret och att utrustningen har blivit smittade av ett skadligt program och snokat efter bankkoder eller betalkortsuppgifter.
- Vid en internationell polisoperation stängdes mobilservrar som användes av kriminella, misstänkta greps och över 1200 SIM-boxar samt annan brottsvinster togs i beslag. Det uppskattades att bedrägerierna hade minst 3 200 offer.

Nätens funktion

- Finska organisationer blev igen utsatta för överbelastningsangrepp av en proryska aktör. Angreppen hade inte någon betydande inverkan.
- När du förbereder dig på överbelastningsangrepp behöver du ta hänsyn till helheten i de system som ska skyddas och deras inbördes beroenden.

Skadeprogram och sårbarheter

- Runt om i världen har det rapporterats omfattande om olika utpressningsprogramangrepp. I Finland hade angreppen ännu inte haft någon större inverkan under oktober.
- När antalet nätfiske och bedrägerier har ökat har man upptäckt riktad spridning av skadlig programvara som har gömts i e-postbilagor.
- En allvarlig sårbarhet har hittats i programmet CVE-2025-49844 Redis. Vi rekommenderar att man lokaliserar och uppdaterar sårbara instanser omedelbart.

Spionage

- En kinesisk hotaktör försökte spionera på diplomatiska mål i Europa. I kampanjen försökte man sprida det skadliga programmet PlugX till målet bl.a. med EU och NATO som tema.
- En hotaktör med koppling till Nordkorea har försökt spionera på europeiska försvarsorganisationer genom en kampanj som inleds med en rekryteringsinriktad kontakt.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

I slutet av september informerade vi om kritiska sårbarheter i Ciscos FTD- och ASA-produkter, och i oktober tog vi kontakt med ägarna till de enheter som identifierats som sårbara. Du kan läsa om dessa sårbarheter och uppdateringsbehov på våra webbsidor.

Vi har fått veta om incidenter där brottslingar har utgett sig för att vara medarbetare vid Cybersäkerhetscentret. Vi publicerade ett meddelande om ämnet där vi berättar hur du kan identifiera huruvida samtalet eller e-postmeddelandet kommer från en riktig person. Kom ihåg att vi aldrig ber dig till exempel att betala en faktura, installera programvara eller lämna ut bank- och inloggningsuppgifter.

Microsoft avslutade den 14 oktober 2025 det officiella stödet för Windows 10. Att stödet upphör betyder att operativsystemet inte längre får säkerhetsuppdateringar eller officiell teknisk support. Operativsystemet fungerar fortfarande, men användningen medför ökade informationssäkerhetsrisker eftersom nya sårbarheter inte längre åtgärdas.

Allmän översikt över cybersäkerheten i oktober

Ur Cybersäkerhetscentrets perspektiv var oktober ganska livlig.

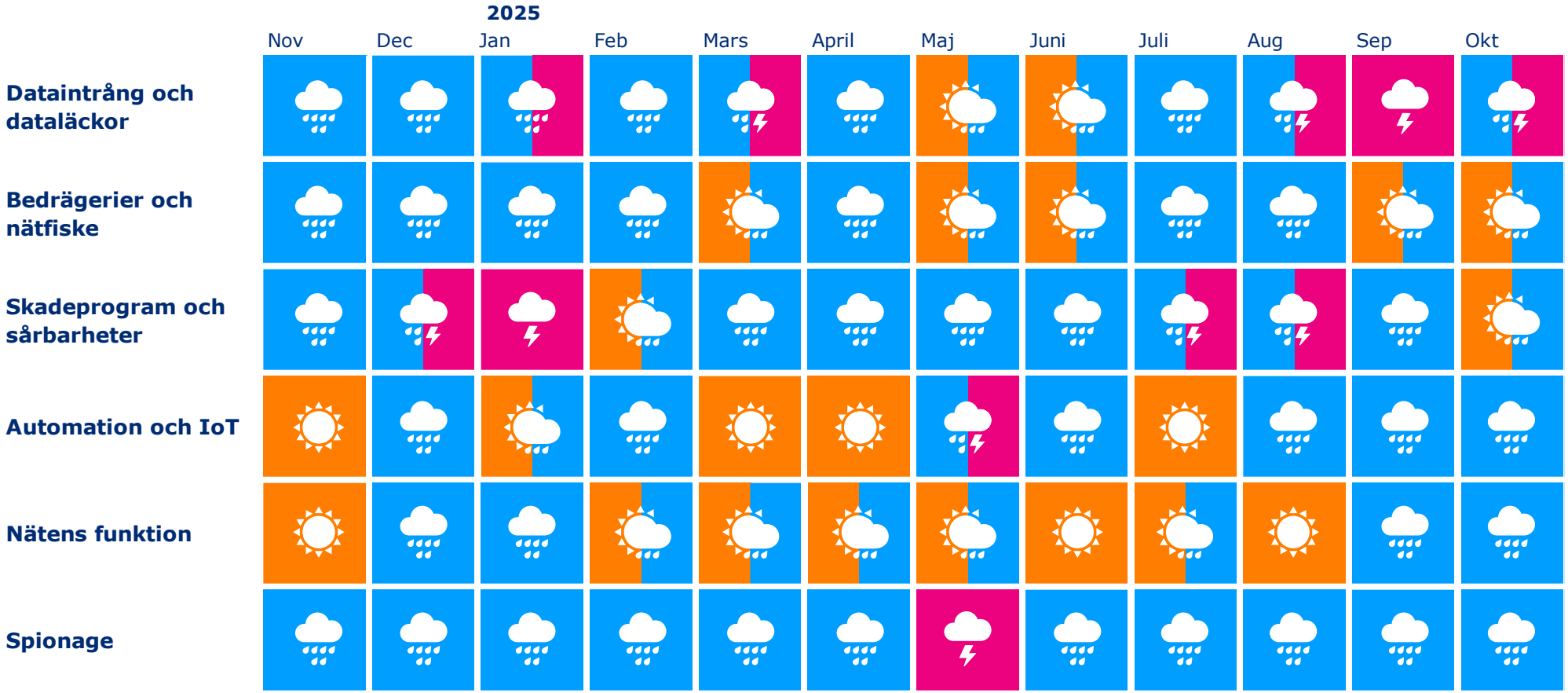
Till månadens mest betydande internationella händelser hörde bland annat ett dataintrång riktat mot det amerikanska säkerhets- och teknikföretaget F5, där en aktör som bedömts vara en statlig hotaktör hade fått åtkomst till F5:s interna system. Angriparen hade bland annat kopierat källkoden till BIG-IP-produkter samt uppgifter om ännu ej publicerade sårbarheter.

- F5:s system används i stor utsträckning i olika organisationer runt om i världen och händelsen krävde brådskande åtgärder.
- Andra internationellt betydelsefulla händelser var dataintrånget riktat mot mjukvaruföretaget Red Hat samt de kritiska sårbarheterna i Ciscos ASA- och FTD-produkter.

I Finland registrerades det fortfarande fler än vanligt anmälningar om kapade Microsoft 365-konton under oktober. Den allvarliga varningen som vi publicerade i september är fortfarande i kraft.

På hemmaplan var en positiv nyhet ur ett säkerhetsperspektiv den brottshelhet som avslöjades av polisen i Östra Finland, där pensionärer lurades på flera miljoner euro.

Trenderna inom cybersäkerhet
de gångna 12 mån.



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

1.

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.