TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

Januari 2026

Cybervädret

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

Det allmänna läget i cybervädret i januari 2026

Januari var regnigt

I månadens cyberväder syntes åter sårbarheter som upptäckts i olika tillverkares kantenheter, och vars utnyttjande har observerats globalt.

Dessutom förekom fortfarande rikligt med nätfiskemeddelanden som syftade till att kapa M365-konton. Det är svårt att upptäcka intrång i M365-konton utan aktiv övervakning av systemet och uppföljning av inloggningsloggarna.

Under granskningsperioden avslöjades ett exceptionellt dataintrång där angriparen uppges ha haft obehörig åtkomst till ett energibolags onlinetjänst i nästan ett års tid. Fallet avslöjades när innehåll som inte hörde hemma på företagets webbplats upptäcktes där.

- Enligt de uppskattningar som framförts offentligt ska angriparen ha fått tillgång till uppgifter om cirka 31 000 elavtal i Finland.

I januari diskuterades också den växande användningen av AI-assistenter i organisationer samt de informations- och cybersäkerhetsutmaningar som behöver beaktas vid både införande och användning. Vi publicerade en artikel om ämnet som sammanfattar de centrala perspektiven och rekommendationerna för en säker och ansvarsfull användning av AI-assistenter.

Vi publicerade en översikt över år 2025

Publikationen Cybersäkerheten 2025, sammanställd av experter vid Cybersäkerhetscentret, ger en helhetsbild av årets centrala cyberhot i Finland. Dessutom ger översikten riktlinjer för organisationer om vad år 2026 eventuellt kan föra med sig och vilka åtgärder det föränderliga hotlandskapet kräver.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Autonoma AI-agenter omges just nu av stora förväntningar. Den mer avancerade automation som bygger på språkmodeller innebär samtidigt nya risker för cybersäkerheten. Traficoms och Försörjningsberedskapscentralens nya anvisningar hjälper organisationer att planera, bygga och förvalta agentbaserade AI-system på ett säkert sätt.

Traficoms trendrapport lyfter fram tre trender för transport, kommunikation och cybersäkerhet som kräver särskild uppmärksamhet under de närmaste åren. I takt med att samhället digitaliseras blir cybersäkerhet en allt viktigare del av den övergripande säkerheten.

Det EU-finansierade projektet SECURE beviljar finansieringsstöd för små och medelstora företag för att stödja genomförandet av cybersäkerhetsförordningen (CRA). Europeiska små och medelstora företag som omfattas av skyldigheterna i CRA kan ansöka om stöd. Ansökan är öppen till och med den 29 mars 2026.

Det utvärderingskriterium för offentliga förvaltningens molntjänster (Nationella kriteriebanken, KriPa), som har beretts i samarbete mellan finansministeriet och Traficom, syftar till att stödja myndigheternas riskhantering vid användning av molntjänster samt att främja ett korrekt skydd av säkerhetsklassificerad, sekretessbelagd och offentlig information. Kriterierna förväntas bli färdiga under hösten 2026.

Månadens hagelskur
Polens energiinfrastruktur utsattes för omfattande cyberangrepp

I slutet av december (29.12) utsattes flera objekt inom Polens energiinfrastruktur för ett omfattande, koordinerat cyberangrepp som förstörde system och information. Det är sannolikt att angriparna hade fått fotfäste flera månader innan de skadliga aktiviteterna genomfördes. Den polska cybersäkerhetsmyndigheten publicerade en rapport om fallet i januari.

Angreppen riktades i synnerhet mot anslutningspunkterna mellan anläggningar för produktion av förnybar energi och distributionsnätsföretag för el (DSO), där det finns kantenheter och industriella automationsenheter som används för styrning av elnätet. Distributionsnätsföretagen miste sin överblick och kontroll över anslutningspunkterna. På värme- och elproduktionsanläggningens arbetsstationer och servrar förstördes data, och vissa enheter gjordes odugliga för fortsatt användning.

Även om fallet var allvarligt påverkade det varken el- eller värmeproduktionen eller tillståndet i Polens elsystem.

Fallet har väckt stor uppmärksamhet

- Enligt den rapport som offentliggjorts av Polen har angreppen visat indikationer på angriparinfrastruktur som förknippas med statliga hotaktörer.
- Det är fråga om det första storskaliga angreppet med avsikt att förstöra system inom energiinfrastrukturen i en EU-medlemsstat. Motsvarande cyberangrepp har förekommit tidigare i Ukraina.
- Fallen har väckt diskussion om betydelsen av att skydda den kritiska infrastrukturen, stärka riskhanteringen och omsätta bra praxis i praktiken även i Finland.

Fenomen i cybervädret

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

Cybervädret januari 2026

1 mån.

Dataintrång och dataläckor

Januari var främst lugn. Anmälningar om dataintrång i M365-konton ökade vid slutet av månaden. Webbplatser inom energisektorn utsattes för intrång och personuppgifter äventyrades.

Skadliga program

Under januari har Cybersäkerhetscentret fått anmälningar om skadliga program som förmedlats i samband med olika nätfiskekampanjer. Antalet anmälningar har dock varit måttligt.

Sårbarheter

I januari förekom det flera nolldagarssårbarheter som utnyttjades vid dataintrång.

Bedrägerier och nätfiske

Företagare hade utsatts för förtroendegivande bedrägerier i Patent- och registerstyrelsens namn. I bedrägerimeddelandena uppmanades de att uppdatera företagets uppgifter.

Ett nytt textmeddelandebedrägeri skrämmer mottagare med ett misstänkt banktransaktion för att få dem genom att ringa det angivna telefonnumret.

Automation och IoT

Cybersäkerhetsmyndigheterna i Australien och sex andra länder har i samarbete utarbetat riktlinjer för cybersäker uppkoppling av industriella automationssystem. Riktlinjen är en del av en gemensam publikationsserie som fokuserar på att stärka cybersäkerheten i produktionsmiljöer.

Nätens funktion

De största botnäten som används för överbelastningsangrepp, liksom deras förmåga att utföra angrepp, växer ständigt. En betydande faktor är otillräckligt skyddade konsumentenheter.

Cybervädret januari 2026 1/2

1 mån.

Dataintrång och dataläckor

- Med tanke på anmälningar om dataintrång var januari en lugn månad.
- Anmälningar om dataintrång i M365-konton ökade vid slutet av månaden.
- Det gjordes intrång i webbsidorna för en organisation inom energibranschen, på sidorna publicerades olovliga artiklar och en del av personuppgifterna äventyrades.
- Cybersäkerhetscentret fick anmälningar om kapade WhatsApp- och Telegramkonton samt om kapningsförsök. Antalet anmälningar minskade mot slutet av månaden.
- Dessutom förekom det dataintrång där man utnyttjat nolldagarssårbarheter.

Skadliga program

- Januari har varit en lugn månad med tanke på observationer om skadliga program. Cybersäkerhetscentret har dock fortfarande fått anmälningar om infostealer-program som varit som bilaga till olika nätfiskemeddelanden. De har distribuerats till exempel via meddelanden i Discord-tjänsten.
- Trafik av skadlig programvara i anslutning till olika botnät observeras fortfarande i Finland. Utrustningens säkerhet ökar när den hålls uppdaterad och skaffas av pålitliga tillverkare. Det är viktigt för användaren att undvika obehövliga distansförbindelser och installera program endast från tillförlitliga källor.

Sårbarheter

- En sårbarhet i MongoDB-databasprogrammet gör det möjligt att avslöja konfidentiell information. (CVE-2025-14847)
- Kritisk sårbarhet i produkterna FortiOS, FortiManager, FortiProxy och FortiAnalyze. De har utnyttjats även i Finland. (CVE-2026-24858)
- Kritiska sårbarheter i produkten Ivanti Endpoint Manager Mobile (EPMM). Utnyttjande av sårbarheten har observerats globalt. (CVE-2026-1281 och CVE-2026-1340)

Cybervädret januari 2026 2/2

1 mån.

Bedrägerier och nätfiske

- Företagare hade utsatts för förtroendegivande bedrägerier i Patent- och registerstyrelsens namn. I bedrägerimeddelandena uppmanades de att uppdatera företagets uppgifter, men länken förde till brottslingars webbtjänst i stället för PRS.
- SMS-bedrägerier har fått ett nytt tema där offret skräms med en misstänkt banktransaktion och uppmanas att ringa ett angivet telefonnummer. Det är inte banken som svarar på numret, utan en kriminell bedragare.

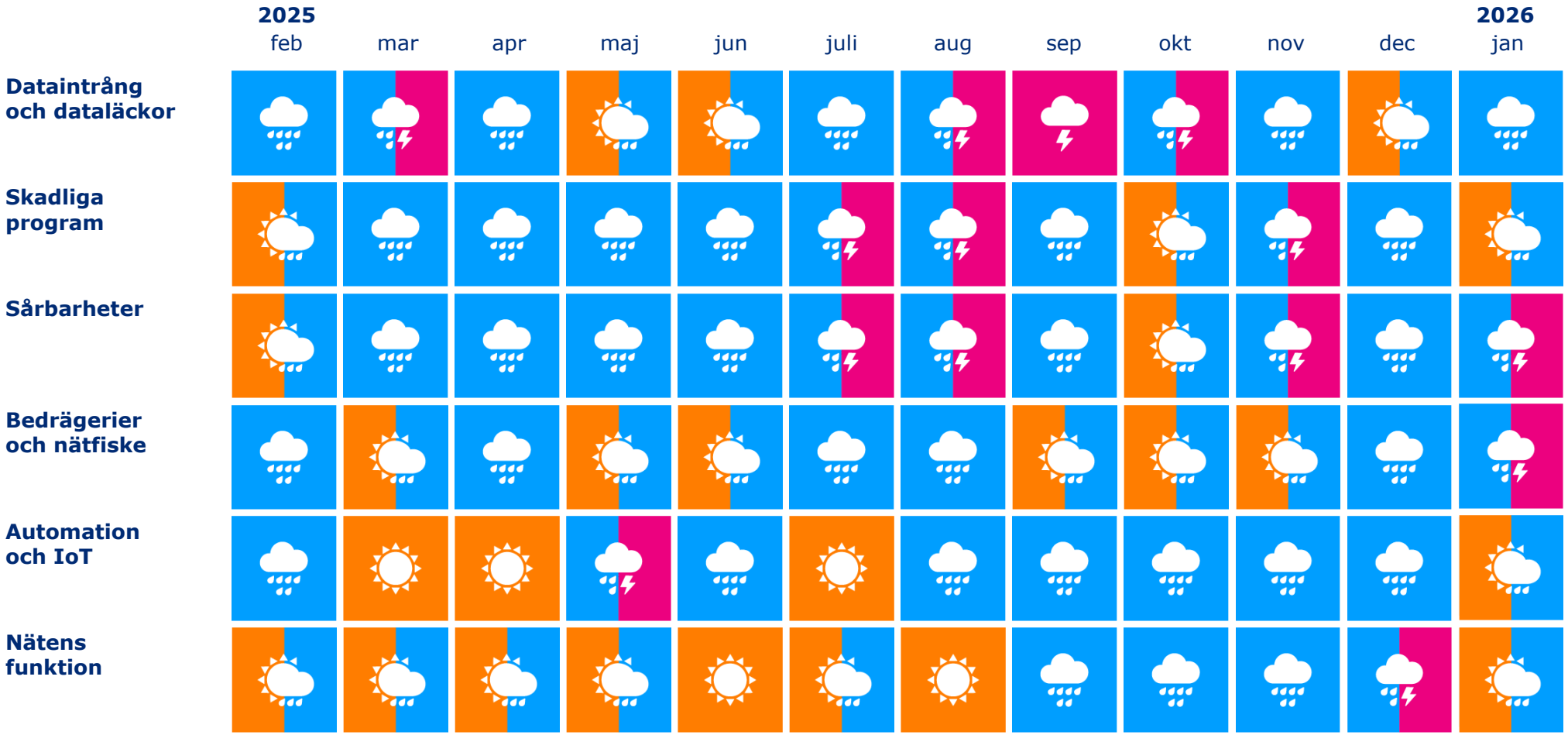
Automation och IoT

- Den anvisning som tagits fram genom internationellt samarbete presenterar åtta eftersträvansvärda cybersäkerhetsprinciper för planering och skapande av nätverksförbindelser inom industriell automation. De behandlar bland annat riskhantering, anslutningsprinciper och hantering av nätverksförbindelser samt begränsning av konsekvenserna av ett angrepp.
- Bristfälligt eller felaktigt skyddade nätverksförbindelser i produktionsmiljöer har orsakat informationssäkerhetsincidenter även i Finland.

Nätens funktion

- Det observerades inte några allvarliga störningar i de allmänna kommunikationsnätens funktion i januari.
- Under de senaste åren har infrastrukturer som möjliggör hypervolumetriska DDoS-angrepp på över 1 Tb/s blivit allt vanligare. I Finland har det ännu inte förekommit några kända exempel.
- Många botnät utnyttjar dåligt skyddade konsumentenheter, såsom medieenheter eller surfplattor som köpts från billiga nätbutiker.
- Virtuella maskiner som drivs i molntjänster kapas också och används i botnät. Botnät som består av sådana resurser kan vara ännu mångdubbelt kraftigare.

Cybervädret
de gångna 12 mån.



Cybervädерprognos

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 på normal nivå

Det kan förväntas att nätfiske efter koder för användarkonton och kontointrång, som drabbat organisationer, medför multiplikatoreffekter under de närmaste månaderna. Brottslingar använder kapade konton för att begå fakturabedrägerier, t.ex. VD-bedrägerier. Dessutom skickar man fortsatta nätfiskemeddelanden från konton.

Semestersäsonger syns upprepade gånger i vår statistik över kontointrång: när personalen kommer tillbaka från semester och öppnar sin fulla e-postlåda ökar risken för nätfiske. Vintersemestersäsongen i februari-mars kan också öka antalet nätfiskemeddelanden med inkvartering och semester som tema.

Sårbarheter i edge-enheter ökar angreppsytan för illvilliga aktörer. Sårbarheter som hittats i dem kan leda till dataintrång eller försök till intrång.

Organisationens beredskap

- Upplysning och multifaktorautentisering (MFA) är inte tillräckliga för att skydda medarbetare mot avancerade försök för kontointrång, t.ex. nätfiske som använder AiTM-teknik.
- Det lönar sig för organisationerna att införa avancerade säkerhetsegenskaper, t.ex. praxis för villkorad tillgång (conditional access), riskbaserad autentisering (risk-based authentication) och kontinuerlig evaluering av åtkomst (continue access evaluation).

Oroande

Antalet cyberhot och deras allvar är på normal nivå.

Cyberhoten kan dock förändras snabbt, även mot negativ riktning.

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.