TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

Mars 2026

Cybervädер

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 cybervädret i mars 2026

Cybervädret fortsatte att vara regnigt

Flera angrepp mot leveranskedjor via programvarukomponenter drog in regnmoln över vårens cyberhimmel. Hotaktören TeamPCP genomförde angreppen via programvara med öppen källkod (Trivy, Kicks, och Python-paket LibLLM).

Vågen av intrång i M365-konton verkar ha minskat jämfört med föregående månad.

I mars publicerade vi tre sårbarhetsmeddelanden om kritiska sårbarheter.

Cybersäkerhetscentret har fått exceptionellt få anmälningar om utpressningsprogram. Internationellt ökar antalet utpressningsprogram kontinuerligt, så situationen kan förändras snabbt även i Finland.

Det blev ljusglimtar mellan regndropparna när Cybersäkerhetscentret och skyddspolisen deltog i en internationell operation där man avvärjde spionage från den ryska militära underrättelsetjänsten GRU. I operationen förhindrades användningen av ett globalt cyberspionasnätverk som bestod av knäckta routrar i TP-länkar.

GRU hade använt sårbara routrar åtminstone för att spionera på användare genom att ändra enheternas namnserverinställningar. Detta har möjliggjort genomförandet av ett man-in-the-middle-angrepp (adversary-in-the-middle, AitM) och dekryptering av krypterad nätverkstrafik.

Cybersäkerhetscentrets åtgärder och tips för förberedelser

Cybersäkerhetscentret publicerade situationskort som hjälper organisationer att kommunicera om cyberincidenter. Korten ger en allmän bild av olika incidenter och konkret stöd för att kommunicera om dem.

Vi bjuder in organisationer att delta i det avgiftsfria pilotprojektet Vartijatonttu (”väktartomten”) som kartlägger finländska företags förmåga att identifiera och hantera aktuella cyberhot. Deltagarna får jämförelsedata om sin egen cybermognadsnivå, en analys av verkliga hotscenarier samt konkreta utvecklingsförslag.

Cybersäkerhetscentrets nya guide Ohjelmistoturvallisuuden johtaminen - Roolit ja osaamistarpeet erbjuder stöd för systematisk ledning av programvarusäkerhet under programmets hela livscykel. Med detta tryggas organisationers och hela samhällets verksamhets kontinuitet och störningsfrihet i den digitala miljön.

Webbinarieserien Kritisk kod som är speciellt avsedd för programvaruutvecklare börjar 17.4. I den serie av webbinarier som Cybersäkerhetscentret arrangerar behandlas programvarusäkerhet ur praktisk synvinkel: hur gör man en bättre och tryggare kod.

Månadens hagelskur
Konton för snabbmeddelandeapplikationer föremål för kapningsförsök

Under början av året har Cybersäkerhetscentret fått ett flertal anmälningar om incidenter som hänför sig till snabbmeddelandeapplikationer. Målen har varit Telegram-, WhatsApp- och Signal-konton.

Flera olika typer av incidenter har anmälts. I de rapporterade fallen har konton skapats med ett nummer som används av en annan person eller med ett nummer som tagits ur bruk. Man har genomfört kontokapningar och olovlig användning åtminstone med länkningsfunktion som gör det möjligt att använda samma konto på en annan enhet. För länkningen krävs en kod som man försöker lura genom nätfiske.

Konton för snabbmeddelandetjänster kan skyddas med multifaktorautentisering samt genom att säkerställa att inga okända enheter har kopplats till ditt konto. Den förvalda pin-koden i telefonsvararen ska bytas. Det lönar sig för organisationer att ge anvisningar för sina medarbetare om hur man använder snabbmeddelandeapplikationer i arbetskontext.

Internationellt rapporterade kampanjer visar att vid kontokapningar i snabbmeddelandeapplikationer finns det risk för även allvarliga incidenter.

Observationer om incidenter i snabbmeddelandeapplikationer internationellt

- I Tyskland varnade myndigheterna för nätfiske i snabbmeddelandeapplikationer, särskilt Signal, som sannolikt utförts av en statlig aktör. Nätfisket har riktats mot högt uppsatta politiker, tjänstemän, företrädare för försvarsmakten och journalister.
- Nederländska myndigheter publicerade uppgifter om en global kampanj där cyberhotaktörer med koppling till den ryska staten försökte ta över framstående personers Signal- och WhatsApp-konton.
- I Italien har man i en Signal-kampanj försökt fiska efter människors personliga uppgifter med hjälp av social manipulation.

Fenomen i cybervädret

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

Fenomen i cybervädret
januari 2026

1 mån.

Dataintrång och dataläckor

Mars var en rätt jämn månad när det gäller dataintrång. Under månaden förekom det dock några betydande dataintrång och informationsläckor. Angreppen genomfördes i regel genom att utnyttja sårbarheter.

Skadliga program

I mars fick leveranskedjeangrepp som en hotaktör riktade mot programvara med öppen källkod omfattande konsekvenser både nationellt och internationellt.

Sårbarheter

I mars rapporterades fortfarande en hel del sårbarheter. Konsekvenserna var ganska begränsade i Finland.

Bedrägerier och nätfiske

I mars observerades en hel del bedrägerimeddelanden med skatt som tema som hänförde sig till skatteåterbäring, skattebeslut eller efterskatt.

Med hjälp av gruppdiskussioner i WhatsApp-grupper samlar man in uppgifter om företag för fakturabedrägerier.

Automation och IoT

USA förbjöd import av konsumentroutrar som tillverkats utomlands till marknaden i USA med hänvisning till den nationella säkerheten.

Nätens funktion

I mars rapporterades något fler överbelastningsangrepp än under de första månaderna av året, men inga betydande konsekvenser observerades.

Vid sidan av tekniska överbelastnings-angrepp kan störningar i mänskliga gränssnitt vara på väg att öka.

Fenomen i cybervädret
januari 2026 1/2

1 mån.

Dataintrång och dataläckor

- I myndigheternas gemensamma operation avvärjdes cyberspionage från den ryska militära underrättelsetjänster där man utnyttjade en sårbarhet i TP-Links routrar (CVE-2023-50224) för dataintrång i enheter. Med hjälp av dataintrånget använde angriparna speciellt ouppdaterade routrar som verktyg för spionage, till exempel genom att styra nättrafiken via sin egen infrastruktur.
- Digitalist Experience Oy:s system utsattes för ett dataintrång som omfattade Viking Lines kunduppgifter.
- Antalet anmälningar till Cybersäkerhetscentret om dataintrång i M365-konton var nästan hälften färre än i februari.

Skadliga program

- Hotaktören TeamPCP lyckades genomföra ett leveranskedjeangrepp mot programvara med öppen källkod, dvs. Trivy-informationssäkerhets-skanner, LiteLLM och Cehckmarx. Genom angreppet installerade hotaktören en bakdörr i programvaran. Skadliga versioner av programmen spreds offentligt i stor omfattning. Angreppet medförde dataintrång runt om i världen.
- Under mars fick Cybersäkerhetscentret anmälningar om skadliga program mer än normalt.

Sårbarheter

- I mars publicerades en kritisk sårbarhet i Citrix NetScaler ADC och NetScaler Gateway-produkterna (CVE-2026-3055) som gör det möjligt för information i minnet att läcka från ett sårbart system. Vi rekommenderar att du uppdaterar omedelbart för att åtgärda problemet.
- Kritisk sårbarhet publicerades också i F5 BIG-IP APM-åtkomsthanterings-systemet (CVE-2025-53521). Det rekommenderas att systemet uppdateras till den korrigerade versionen och att man granskar miljön för eventuell exploatering.
- Kritisk sårbarhet hittades också i npm-distributionen av Axios JavaScript-paket.

Fenomen i cybervädret
januari 2026 2/2

1 mån.

Bedrägerier och nätfiske

- Bedrägerimeddelanden med skatt som tema har i mars skickats under förevändning av skatteåterbäring, skattebeslut eller efterskatt.
- Man har fiskat efter betalkorts-uppgifter i bostadsuthyrningstjänsters namn.
- Företagens interna uppgifter har samlats in för fakturabedrägerier med hjälp av diskussioner i WhatsApp-grupper. Bedragaren har förfalskat e-postmeddelanden i direktörens namn och begärt att den anställda skapar en gruppchatt och skickar en inbjudningslänk i svarsmeddelandet. Cybersäkerhetscentret har inte tidigare fått information om motsvarande metod.

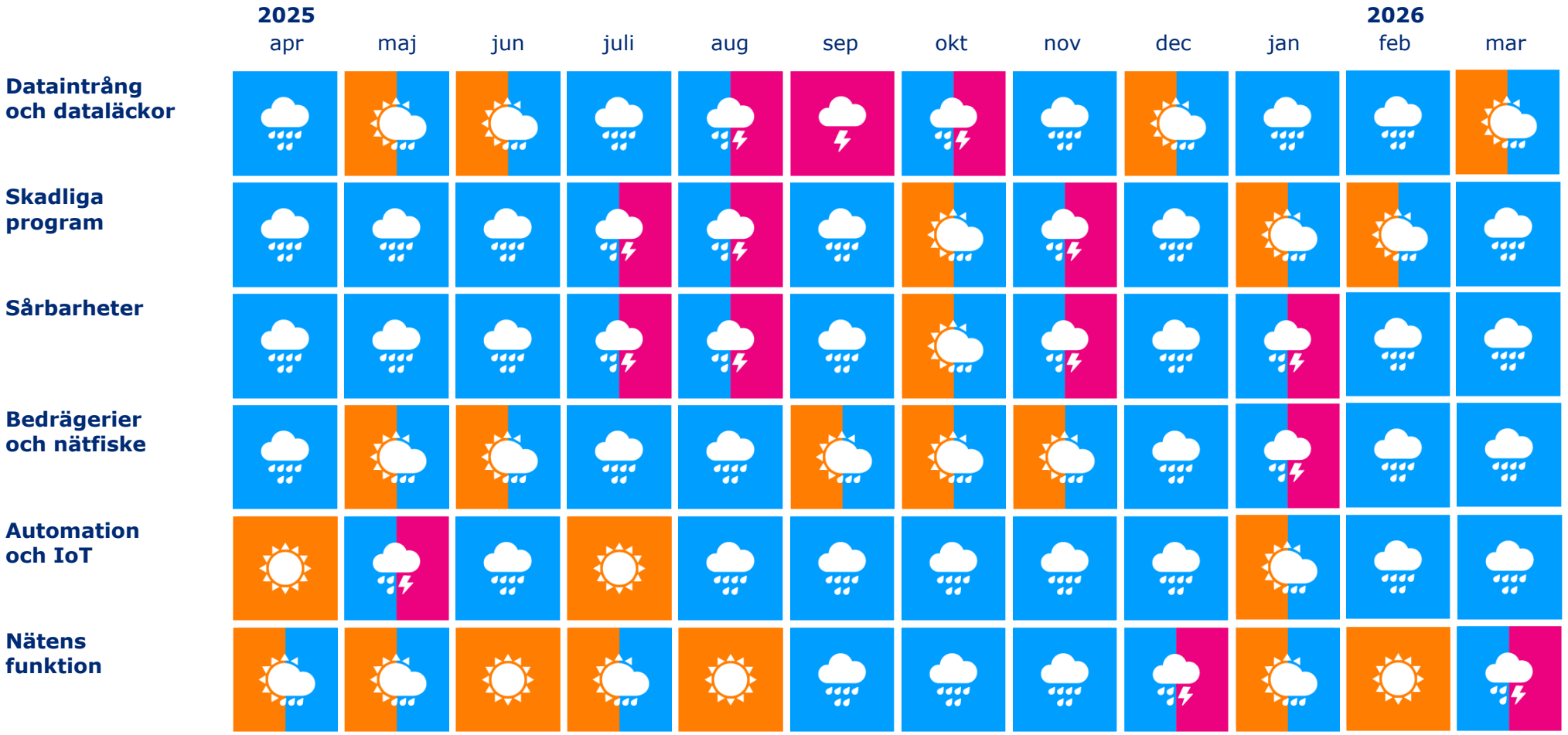
Automation och IoT

- I USA anses utländska routrar utgöra hot för hushåll och informationsnät samt möjliggöra spionage och upphovsrättsstölder.
- Kommunikationskommissionen FCC i USA förbjöd import, marknadsföring och försäljning av andra konsumentroutrar än de som tillverkats i USA.
- För att få ett försäljningstillstånd måste routrarna genomgå en myndighetsbedömning och tillverkaren ska visa en plan för att flytta produktionen till USA.
- Konsumenter kan fortsätta använda sina nuvarande enheter.

Nätens funktion

- I mars var det nyheter om att tingsrätter och förvaltningsdomstolar belastas med material som skapats med artificiell intelligens.
- Generativ AI möjliggör också belastning av många andra tjänster, t.ex. kundservice eller myndigheternas registratorskontorer.
- Cybersäkerhetscentret har också fått anmälningar om fall där kundtjänsten har belastats med bland annat fabricerade begäranden om tillsyn.

Fenomen i cybervädret
de gångna 12 mån.



Cybervädерprognos

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

1 mån.

Cyberväderprognos
Cyberhoten förblir normala

Man måste vara beredd på cyberrisker med anknytning till programvaruberoenden också i framtiden. De kampanjer med leveranskedjeangrepp som sågs i mars blir säkert inte de sista, men de understryker hur allvarligt fenomenet är.

Även den snabbt föränderliga situationen i Mellanöstern kan fortfarande medföra oväntade sekundära effekter i Finland, till exempel via komplexa leveranskedjor.

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.

Topp 5 cyberhot
i den närmaste framtiden

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 Den ökade användningen av artificiell intelligens förutsätter riskhantering

Organisationernas beredskap och aktiva riskhanteringsåtgärder är viktiga när användningen av artificiell intelligens ökar.

3 Informationssäkerhet och kontinuitet hos distributions- och servicekedjor

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

4 Vikten av att skydda kritisk infrastruktur framhävs

Det snabbt föränderliga cyberverksamhetsfältet påverkar skyddet av kritisk infrastruktur.

5 Utpressningsprogram är ett betydande hot mot organisationer

Antalet utpressningsprogram ökar ständigt globalt.

● = nytt hot på topp 5-listan