TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

Februari 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 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 februari 2026

Februari fortsatte att vara regnig

Isigt duggregn kom från flera håll. På basis av de incidenter som anmäldes till Cybersäkerhetscentret utnyttjade brottslingar flera kanaler, t.ex. utpressningsmeddelanden, bedrägerisamtal i bankers och myndigheters namn, robotsamtal, välgjorda nätfiske-meddelanden samt investerings- och kryptobedrägerier.

Dataintrång i M365-konton fortsatte och AiTM-angreppens förmåga att förbigå multifaktorsautentisering betonade behovet för starkare skyddsmekanismer.

Under februari rapporterades det om flera kritiska sårbarheter i program och tjänster i allmänt använda programvaror och tjänster. Även om sårbarheter är tekniskt betydande och i värsta fall skulle möjliggöra besittningstagande av system eller olovlig användning av uppgifter har deras nationella konsekvenser än så länge förblivit små.

Trots detta följer vi lägesbilden intensivt eftersom försök till utnyttjandet av sårbarheterna har observerats i olika miljöer.

Flera observerade sårbarheter har fått höga punkter i CVSS, vilket betonar betydelsen för att uppdateringen och skyddsåtgärderna ska hållas uppdaterade.

Värt att notera om sårbarheter

- Organisationer uppmanas att säkerställa att kritiska system är uppdaterade och att loggnings- och övervakningsmekanismerna fungerar för att kunna identifiera eventuella försök till utnyttjande.
- Dessutom är det viktigt att beakta att sårbarheter ofta utnyttjas snabbt efter att de har offentliggjorts, vilket innebär att snabb respons är avgörande för riskhanteringen.

Månadens hagelskur
Cyberdimensionen med i USAs och Israels angrepp mot Iran

USA och Israel gjorde ett angrepp mot Iran den 28 februari 2026. På de första dagarna av angreppet observerades cyberaktiviteter vid sidan om kinetiska slag.

- Iranska nättjänster och applikationer störddes, och flera hacktivistgrupper inledde i sin tur överbelastningsangrepp (DDoS-agrepp) och störning av webbsidor.
- Kapningen av en iransk böneapplikation, där applikationens innehåll gjordes regimkritiskt, väckte särskild uppmärksamhet.
- Den nationella internettrafiken i Iran sjönk till omkring fyra procent av normal nivå till följd av omfattande nedstängningar av internetförbindelser i landet.
- Flera stater har publicerat bedömningar av hur situationen i Iran påverkar cybersäkerheten. [4]
- Enligt bedömningarna anses Iran och aktörer med kopplingar till Iran dock fortsatt ha förmåga att genomföra cyberoperationer, vilket ökar risken för indirekta cyberhot, särskilt för organisationer med verksamhet eller leveranskedjor i Mellanöstern. [5]
- Hittills har inga betydande cybersäkerhetseffekter riktats mot Finland till följd av situationen i Iran.

Cybersäkerhetscentrets åtgärder och tips för förberedelser

Cybersäkerhetscentret har publicerat en vägledande webbplats som behandlar det hot som utvecklingen av kvantdatorer utgör mot nuvarande krypteringsmetoder. Kvanthotet gäller särskilt information som måste förbli konfidentiell långt in i framtiden. Sådan information omfattar till exempel personuppgifter, hälsouppgifter, affärshemligheter samt uppgifter som omfattas av myndigheters sekretess. [6]

Webbläsartillägg kan förbättra funktionaliteten, men de medför betydande informationssäkerhetsrisker eftersom de ofta beviljas omfattande behörigheter till webbläsarens innehåll. Risken kan minskas genom att hålla antalet tillägg lågt, ta bort onödiga tillägg samt endast installera nya från officiella källor och genom att bedöma utvecklarens tillförlitlighet och de begärda åtkomsträttigheterna. [7]

Myndigheten för digitalisering och befolkningsdata (DVV) har en ny guide ”Säkerställande av övningars effekter och genomförande av utvecklingsåtgärder i praktiken” som betonar att övningar endast ger nytta om lärdomar och utvecklingsområden dokumenteras, analyseras och förankras i organisationens verksamhet. Därför bör det skapas en tydlig process för övningar, där respons, dokumentation och uppföljning av utvecklingsåtgärder stöder den kontinuerliga utvecklingen av beredskap och cybersäkerhet.

Fenomen i cybervädret

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

Fenomen i cybervädret
februari 2026

1 mån.

Dataintrång och dataläckor

Februari var betydligt aktivare än januari. Det förekom ett betydande dataintrång där man utnyttjade en nolldagarssårbarhet.

Antalet anmälningar om dataintrång i Microsoft 365 var 67 % mer än i januari.

Skadliga program

Februari verkade vara en lugn månad nationellt med tanke på skadliga program. Cybersäkerhetscentret fick dock några anmälningar om spridning av skadliga program med hjälp av ClickFix-teknik.

Sårbarheter

I februari anmäldes en hel del sårbarheter. Med några undantag var konsekvenserna i regel avgränsade för Finland.

Bedrägerier och nätfiske

Bedrägerisamtal ringdes i bankers och myndigheters namn.

Falska bluffakturor distribuerades via e-post.

Automation och IoT

Hotverksamheten riktad mot automationssystem blev allvarligare under 2025.

Upptäckter som gjordes med stöd av artificiell intelligens förbättrade säkerheten i robotdammsugarsystemet.

Nätens funktion

Överbelastningsangrepp orsakade inte några betydande störningar i Finland.

Botnät som används för överbelastningsangrepp utnyttjas även i annan brottslig verksamhet.

Fenomen i cybervädret
februari 2026 1/2

1 mån.

Dataintrång och dataläckor

- Valtoris system för hantering av mobila enheter utsattes för ett allvarligt dataintrång, där en tidigare okänd nolldagssårbarhet i programvaran utnyttjades.
- Webbplatser har utsatts för dataintrång där olika sårbarheter samt svaga lösenord har utnyttjats.
- I ett fall kompromitterades ett företags nät via en VPN-tjänst i ett ransomware-angrepp.
- Ett BEC-bedrägeriförsök kopplat till ett intrång i ett Microsoft 365-konto upptäcktes i tid och stoppades.

Skadliga program

- Cybersäkerhetscentret underrättades om några webbplatser där skadlig kod spreds med hjälp av ClickFix-tekniken.
- I samband med nätfiskekampanjer har det även observerats spridning av skadlig kod med DocuSign-tema, där användaren uppmanas att klicka på en länk som leder till att skadlig kod installeras på användarens enhet.

Sårbarheter

- Det har förekommit kritiska sårbarheter i Cisco Catalyst SD-WAN-produkter. Aktörer som använder produkterna bör identifiera sårbara enheter i sin nätverksmiljö, samla in tillräcklig information och ögonblicksbilder (snapshots) av de sårbara enheterna, uppdatera enheterna till den senaste versionen samt genomföra hotjakt för att upptäcka eventuell exploatering (CVE-2026-20127 och CVE-2026-20129).
- Utnyttjande och försök till utnyttjande av sårbarheterna i Ivanti EPMM (CVE-2026-1281 och CVE-2026-1340) observerades också aktivt under februari.

Fenomen i cybervädret
februari 2026 2/2

1 mån.

Bedrägerier och nätfiske

- I telefonbedrägerier har uppringarna utgett sig för att vara representanter för banken eller en myndighet.
- Med mobilabonnenternas telefonnummer har konton öppnats i snabbmeddelandetjänster såsom Telegram och WhatsApp. I flera fall har det misstänkts att den till abonnemanget hörande röstbrevlådetjänsten har utnyttjats vid registreringen.
- Förfalskade fakturor har skickats via e-post, där mottagarens kontonummer har ersatts med ett bankkonto som kontrolleras av bedragaren.

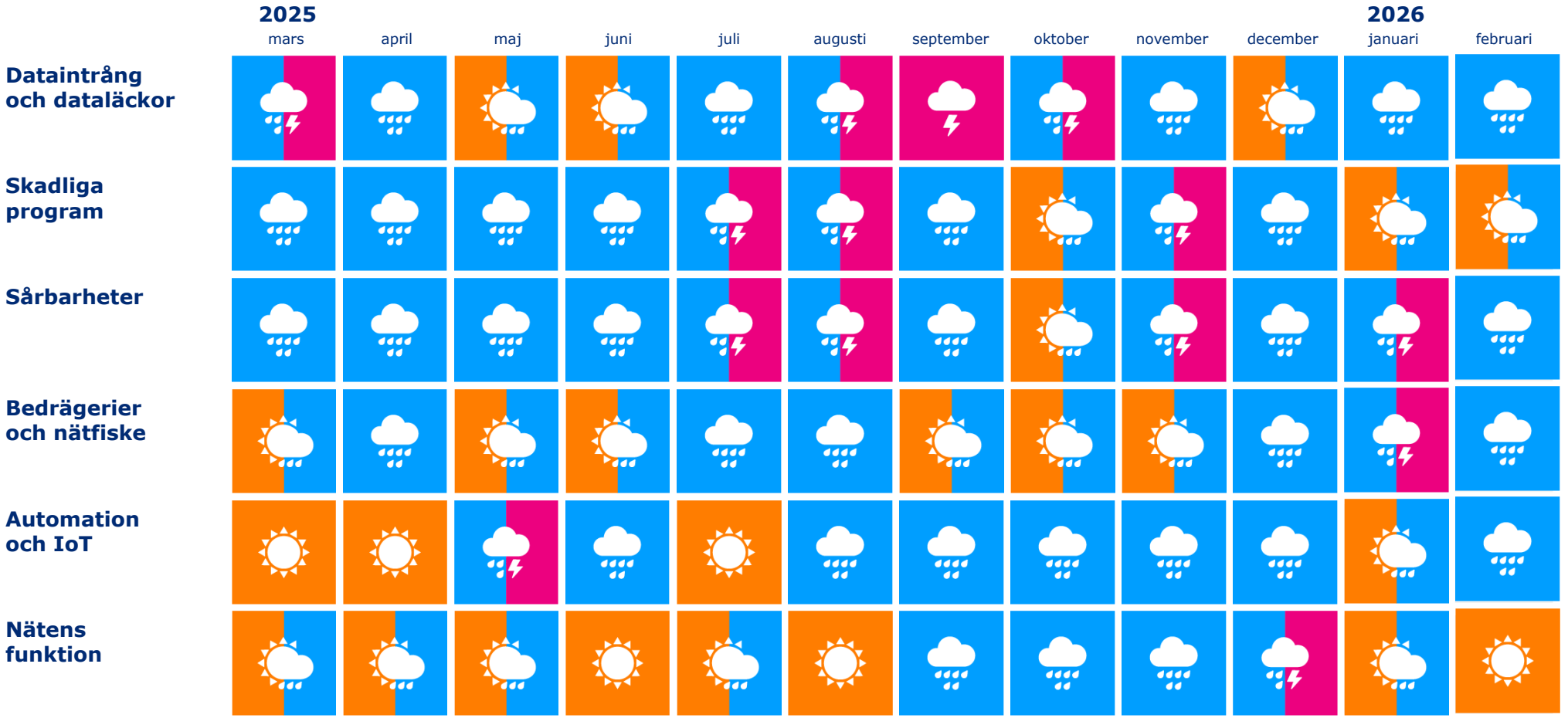
Automation och IoT

- Informationssäkerhetsföretaget Dragos, som är specialiserat på industriella automationssystem, publicerade sin årsrapport. Centrala iakttagelser var att vissa hotaktörer har gått från att etablera fotfäste till aktiv sabotageverksamhet samt att systemägare fortsatt har svårigheter att upptäcka hotverksamhet.
- I ett robotdammsugarsystem avslöjades säkerhetsbrister[10] som möjliggjorde åtkomst till 7 000 dammsugare i 24 länder. Fallet visar hur AI-verktyg kan utnyttjas för att hitta sårbarheter. Det understryker också vikten av oberoende informationssäkerhetsrevisioner, fungerande kanaler för rapportering av sårbarheter samt de grundläggande skyddsåtgärder som krävs enligt CRA.

Nätens funktion

- De konsekvenser som observerades av överbelastningsangrepp i Finland begränsade sig till tillfälliga störningar.
- Skadlig programvara som används för att ansluta nätverksenheter till botnät används också för annan cyberbrottslighet, såsom annonsbedrägerier och informationsinsamling.
- Det observerades inte några allvarliga störningar i allmänna kommunikationsnät i februari.

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.

Cybervädерprognos
Cyberhoten förblir normala

1 mån.

Den föregående prognosens bedömning av de kumulativa effekterna av utnyttjandet av sårbarheter och kontointrång realiserades i februari. Samma utveckling fortsätter: det kan förväntas att de ökande intrången i M365- och andra användarkonton leder till exempel till faktureringsbedrägerier, såsom vd-bedrägerier. Från komprometterade konton skickas också vidare nätfiskemeddelanden.

Den snabbt föränderliga situationen i Mellanöstern kan få 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.

Cybervädерprognosen 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.