TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

April 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 april 2026

April medförde inte någon betydande ändring i cybervädret

Det varma vårvädret kyldes ner i synnerhet av kapningar av M365-konton, som rapporterades till Cybersäkerhetscentret i större omfattning än föregående månad. Under månaden föll också ”regndroppar” i form av sårbarheter som publicerades i flera olika produkter.

Utnyttjandet av AI-baserade lösningar vid kartläggandet och utnyttjandet av sårbarheter blev månadens samtalsämne.

Utnyttjandet av artificiell intelligens har också konstaterats ha ökat i bedrägerier.

- Enligt Cybersäkerhetscentret känner man hittills endast till enstaka fall där AI-genererade röster och bilder har använts, till exempel i vd-bedrägerier och investeringsbedrägerier.

Traficom har publicerat cybersäkerhetsscenarier som sträcker sig till år 2035 och beskriver fyra alternativa framtidsbilder

Ur ett cybersäkerhetsperspektiv lyfter samtliga scenarier fram centrala frågor såsom artificiell intelligens, leveranskedjor, tillförlitligheten i informationsmiljön samt sammankopplingen av kritisk infrastruktur.

Scenarierna stöder beredskap, beslutsfattande och strategisk diskussion i en situation där säkerheten i det framtida digitala samhället bygger på allt mer komplexa beroenden.

Traficoms webbsidor uppdaterades

Vi har uppdaterat Cybersäkerhetscentrets webbsidor som en del av reformen av Traficoms webbplattform. Ändringen förbättrar webbplatsernas funktion och möjliggör utvecklingen av dem i framtiden. Det kan förekomma enstaka brister på webbplatserna, t.ex. trasiga länkar. Vi fixar dem kontinuerligt. Vi beklagar de tillfälliga störningar som uppdateringen medför.

Månadens hagelskur
AI-baserad sårbarhetsskanning ändrar spelfältet

AI-baserad sårbarhetsskanning blev ett brett diskussionsämne i april på grund av de möjligheter tekniken erbjuder.

Avancerade AI-lösningar bedöms effektivisera kartläggningen av sårbarheter i skadligt syfte och öka antalet sårbarheter som kan utnyttjas. Med hjälp av artificiell intelligens är det möjligt att hitta nya sårbarheter som man inte känt förut och artificiell intelligens kan utnyttja dem självständigt.

I AI-lösningar kommer analys av angreppsvägar (attack path analysis) också att bli avsevärt lättare. Genom att utnyttja AI-lösningar kan angriparen hitta och kedja samman olika faktorer som möjliggör utnyttjande av sårbarheter, till exempel identifierings-, konfigurations- och logikfel i den utsatta nätmiljön.

Detta utmanar traditionella skanningsmetoder som inte nödvändigtvis identifierar den totala risken för hittade sårbarheter.

Man tror dock att avancerade AI-lösningar inte helt kommer att ersätta sårbarhetsskanning som baserar sig på traditionella identifierare utan de förändrar verksamhetens karaktär till en mer självständig, snabbare och mer heltäckande förmåga som beaktar hot och riskfaktorer.

AI-baserade applikationer är samtidigt en möjlighet att förbättra organisationernas riskhantering och cybersäkerhet. Enligt vissa prognoser är det möjligt att med AI-applikationer täcka till och med hälften av skydds- och avvärjningsåtgärderna i nuvarande cyberangrepp före år 2028.

Cybersäkerhetscentrets åtgärder och tips för förberedelser

Anmäl dig till infotillfället om ikraftträdandet av EU:s cyberresiliensförordning (CRA), som ordnas av Traficom, kommunikationsministeriet och Kyberala ry den 3 juni. I evenemanget framför EU-kommissionens, de nationella myndigheternas och företagens representanter sina åsikter om innehållet och skyldigheterna i regleringen samt det nationella genomförandet av den.

Organisationer uppmuntras att övergå till metoder som är resistenta mot nätfiske, t.ex. FIDO2/WebAuthn eller certifikatbaserad identifiering. Den traditionella multifaktorsautentiseringen (MFA) kan allt oftare kringgås genom Adversary-in-the-Middle (AiTM)-angrepp, med missbruk av Oauth och med genom att stjäla sessionstoken.

FINMISP-tjänsten publicerad! FINMISP är Cybersäkerhetscentrets nationella tjänst för delning av nationell cyberhotsinformation som baserar sig på MISP-plattformen (Malware Information Sharing Platform). Med hjälp av tjänsten effektiviseras delning av teknisk hotinformation om de informationssäkerhetsincidenter som observerats nationellt och internationellt. Cybersäkerhetscentret fungerar som navet i nätverket och delar information med tjänstens användare.

Fenomen i cybervädret

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

Fenomen i cybervädret
april 2026

1 mån.

Dataintrång och dataläckor

Antalet anmälda dataintrång var 14 % mer än i mars. Informationsläckor rapporterades dock mindre i april. Orsaken till flera rapporterade fall av informationsläckor var en felaktig konfiguration.

Skadliga program

Månaden var aktiv med tanke på observationer av skadliga program. Cybersäkerhetscentret fick anmälningar bland annat om skadliga program som spreds med ClickFix-teknik, samt om enstaka skadliga program Magecart och infostealer.

Sårbarheter

Antalet publicerade sårbarheter förblev på hög nivå även i april. Snabb uppdatering av enheter och tjänster som är synliga i nätet framhävs fortfarande för att minska möjligheter att utnyttja sårbarheter.

.

Bedrägerier och nätfiske

Myndighetskommunikationen flyttades helt till suomi.fi-tjänsten i april. Bedragare följer läget och skickar länkar till förfalskade tjänster.

Bedrägerier med hotell- och resebokningstjänster som tema blir vanligare när semesterperioden närmar sig.

Automation och IoT

Amerikanska myndigheter publicerade en anvisning om tillämpning av nolltillitsprinciper i OT-system.

IoT-enheter och konsumenternas nätverksenheter är intressanta angreppsföremål också för statliga aktörer.

Nätens funktion

Om man tillhandahåller AI-tjänster utanför organisationen ska man beakta möjligheterna till deras belastning.

Genom användningen av AI-tjänster kan de ökade antalen programsårbarheter visa sig som en ökning av botnät som används för överbelastningsangrepp.

Fenomen i cybervädret
april 2026 1/2

1 mån.

Dataintrång och dataläckor

- I april anmäldes klart flera kapade M365-konton än i föregående månad. För nätfiske efter koderna användes för det mesta AiTM-tekniken, så det är inte längre tillräckligt att enbart använda MFA-skyddet för att förhindra kontointrång.
- Från kapade konton skickades flera tusen nya nätfiskemeddelanden, vilket bedöms öka antalet dataintrång i maj.
- Flera WordPress-webbsidor hackades genom att utnyttja sårbarheter i deras tillägg. Det är viktigt att uppdatera WordPress och dess tillägg regelbundet. Det lönar sig också att säkerställa huruvida ansvaret för uppdateringen hör till leverantören av webbhotelltjänsten eller till administratören av webbplatsen.

Skadliga program

- Det skadliga programmet Magecart observerades i enstaka webbutiker. Med hjälp av det skadliga programmet försöker man stjäla person- och bankuppgifter som man matat in i webbutiken.
- Cybersäkerhetscentret fick också anmälningar om skadliga program som spreds med ClickFix-teknik.
- Med hjälp av nätfiske och sårbarheter har man också försökt sprida skadlig programvara samt skadliga infostealer-program.
- Leveranskedjeangrepp i mars mot bibliotek med öppen källkod syns fortfarande som angreppsvektor vid spridning av skadliga program.

Sårbarheter

- CVE-2026-31431 ”Copy Fail” - sårbarhet i Linux-kärnan, med vilken en vanlig användare kan få huvudanvändarrättigheter.
- CVE-2026-41940 i cPanel- och WHM-produkter med vilken det är möjligt för en icke-autentiserad angripare att få administratörsrättigheter till kontrollpanelen. Utnyttjande av dem har observerats och omedelbar uppdatering rekommenderas.
- CVE-2026-35616 sårbarhet i FortiClient EMS med vilken angriparen kan ta kontroll över enheten. Sårbarheten utnyttjas aktivt.

Fenomen i cybervädret
april 2026 2/2

1 mån.

Bedrägerier och nätfiske

- Myndighetskommunikationen flyttades helt till suomi.fi-tjänsten i april. Bedragare följer läget och skickar länkar till förfalskade tjänster. När människor får information i förväg blir det lättare att känna igen bedrägerier. Medvetenhet ger möjlighet att stanna upp och bedöma om ett sms, e-postmeddelande eller telefonsamtal är äkta eller en bluff. Följ inte länkar i textmeddelanden till stark autentisering.
- Bedrägerier med hotell- och resebokningstjänster som tema blir vanligare när semesterperioden närmar sig. Tänk efter två gånger och kontrollera hos tjänsten innan du betalar överraskande extra avgifter.

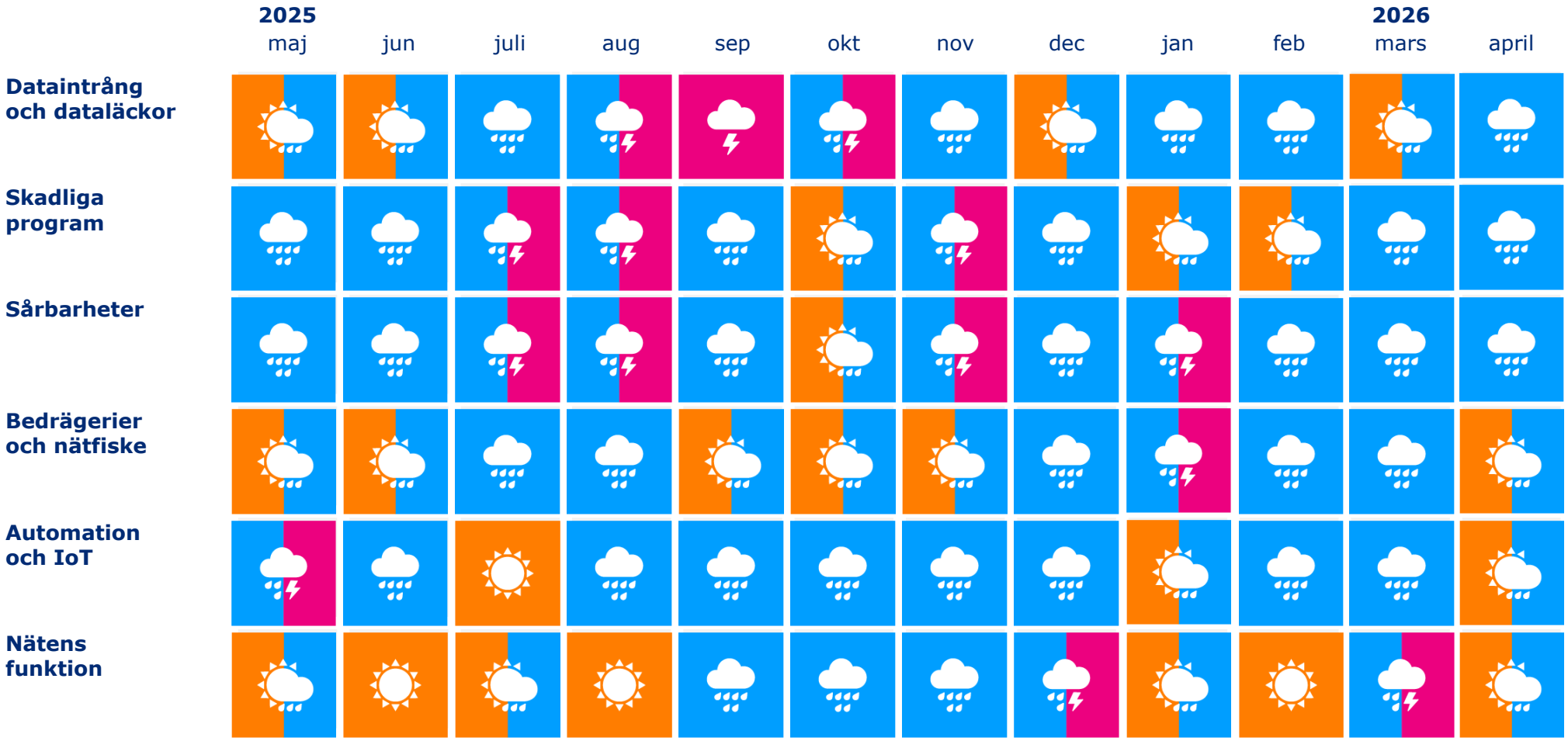
Automation och IoT

- En amerikansk myndighetsarbetsgrupp publicerade ett dokument om tillämpningen av nolltillitsprinciperna på OT-system och -miljöer.[13]
- Bristfälligt skyddade internetanslutna kameror är en bra informationskälla också för underrättelsetjänster. Till exempel uppges information om Irans ajatollah Khameneis rörelser ha inhämtats från bilder från trafikövervakningskameror.[14]
- USA:s cybersäkerhetsmyndighet varnade om att kinesiska cyberhotsaktörer bygger dolda nätverk av knäckta IoT-enheter.[15]

Nätens funktion

- Det observerades inte några allvarliga störningar i allmänna kommunikationsnät i april.
- AI-genererat innehåll kan också användas för att överbelasta AI-baserade tjänster som organisationen erbjuder aktörer utanför organisationen. Till exempel vid införandet av en chatbot som hjälper kunder på webbplatsen måste man beakta begränsningarna i de resurser som den använder.
- Utöver överbelastning av tjänsten kan massiva mängder indata orsaka organisationen extra kostnader.

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.

Cyberväderprognos
Cyberhoten förblir normala

1 mån.

De fortsatt ökade M365-kontointrången och de uppföljande nätfiskemeddelanden som skickas från kapade konton leder sannolikt till kontointrång även i maj.

AI-teknologier och deras tillämpning utvecklas snabbt, vilket kan leda till plötsliga förändringar i angriparnas tillvägagångssätt. Den kontinuerliga kartläggningen av verksamhetsmiljön och anpassningen till den är viktig för organisationers säkerhet.

Organisationens beredskap

- Sårbarhetshanteringen fortsätter att betona vikten av snabba uppdateringar av enheter och tjänster som är synliga på nätet för att minska utnyttjandet av sårbarheter.
- Känn till din egen nätverksmiljö, de system du använder och deras beroenden, och ersätt system som närmar sig slutet av sin livscykel i tid.
- Upplysning och multifaktorsautentisering (MFA) är inte tillräckliga för att skydda medarbetare mot avancerade försök för kontointrång, t.ex. nätfiske som använder AiTM-teknik.

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.