TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

Maj 2026

Det allmänna läget i cybervädret i maj 2026

Maj fortsatte att vara ostadig främst på grund av sårbarheter.

Cybervädret i maj var omväxlande och tidvis ostadigt. Under månaden förekom återkommande och omfattande bedrägerikampanjer där kriminella utgav sig för att representera bland annat barn, myndigheter, banker och tjänster.

Samtidigt observerades att nätfiske utvecklades tekniskt, för Microsoft 365-konton utsattes för AI-assisterad riktning, vilket gjorde meddelandena ännu mer trovärdiga. I april förutspådde vi fortsatt nätfiske till följd av M365-kontointrång, vilket förverkligades bland annat som svårare upptäckbar device-code-phishing. I maj varnade vi också för kapningar av snabbmeddelandekonton som hade pågått under hela början av året och gav anvisningar om hur man skyddar sig mot fenomenet. Under månaden publicerades flera kritiska sårbarheter, varav vissa redan utnyttjades aktivt.

Periodvis solsken i cybervädret bidrog den förnyade Hyöky-tjänsten från Cybersäkerhetscentret till, som togs i ännu bredare bruk, samt den produktionssatta FINMISP-tjänsten, som effektiviserar delningen av teknisk cyberhotsinformation till organisationer och myndigheter som är kritiska för försörjningsberedskapen.

Informationssäkerhet har ingen semester på sommaren

Under sommarsemester ökar särskilt vd-bedrägerier och andra bedrägerier riktade mot penningtransaktioner, när organisationernas normala verksamhet går långsammare och nyckelpersoner är frånvarande.

Under semesterperioden ökar riskerna särskilt när uppgifter sköts av vikarier eller sommaranställda som ännu inte känner till organisationens rutiner. Därför har introduktion och tydliga verksamhetsmodeller stor betydelse.

Cybersäkerhetscentrets åtgärder och tips för förberedelser

Microsoft har startat en av de viktigaste informationssäkerhetsuppdateringarna under de senaste åren: Förnyelse av Windows Secure Boot-certifikat. Ändringen gäller särskilt att vissa Secure Boot-certifikat som är i bruk når slutet av sin livscykel. De rotcertifikat som togs i bruk år 2011 börjar upphöra att gälla från och med sommaren 2026. Ändringen gäller i praktiken nästan alla Windows-enheter som har tillverkats efter år 2012. Microsoft bedömer dock att majoriteten av de moderna Windows 11-enheterna får uppdateringarna automatiskt via Windows Update.

Ny våg observerats i M365-nätfiske: AI-assisterad nätfiskekampanj för enhetskod. Kampanjen är riktad mot organisationer och enskilda användare. Syftet med angreppen är att få obehörigt tillträde till konton och till företagens resurser. Ett dataintrång som gjorts med ny typ av M365 Device Code-nätfiske observeras inte genom traditionella varningar om nätfiskeangrepp. Därför har angriparen en möjlighet att göra till exempel fakturabedrägerier i all tysthet.

Organisationer rekommenderas därför att kontrollera Device Code-intrång som upptäckts via sökningar samt att begränsa användningen av Device Code Flow-funktionen med villkorsstyrda åtkomstregler (Conditional Access). På vår webbplats berättar vi mer om hur organisationer och privatpersoner kan skydda sig mot fenomenet, och i artikeln finns även anvisningar för hur man gör en sökfråga.

Fenomen i cybervädret

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

Fenomen i cybervädret
maj 2026

1 mån.

Dataintrång och dataläckor

Antalet dataintrång ökade med 24 % från april. Denna ökning beror på vågen av M365-kontointrång. Vi fick två anmälningar om utpressningsprogram. Allvarliga konsekvenser undveks.

Skadliga program

Under månaden fick Cybersäkerhetscentret anmälningar om flera observationer av skadliga program. Skadliga program har spridits till organisationer och privatpersoner som bilagor i nätfiskemeddelanden, i samband med rekryteringsbedrägerier samt via komprometterade webbplatser.

Sårbarheter

En hel del nya sårbarheter rapporterades också i maj och samma trend verkar fortsätta hela resten av året.

Bedrägerier och nätfiske

På morsdagen förekom "Hej mamma"-bedrägerier. Bedrägerier begås allt mer med verktyg för artificiell intelligens.

Vd-bedrägerier ökar under semesterperioden. Man försöker lura sommarvikarier i direktörens namn.

Automation och IoT

Den nationella cybersäkerhetslagen som kompletterar EU:s cybersäkerhetsresiliensförordning (CRA) som trädde i kraft måndagen den 1 juni 2026.

Nätens funktion

Överbelastningsangrepp orsakade inte några betydande störningar i Finland.

Störningar i nätens funktion betonades i maj.

Fenomen i cybervädret
maj 2026 2/2

1 mån.

Dataintrång och dataläckor

- Sårbarheter som publicerades i maj ledde till dataintrång i organisationer. Allvarliga konsekvenser kunde dock undvikas.
- Efter en lugn början av året fick vi anmälningar om utpressningsprogram. Företagens beredskap har blivit bättre och man återhämtar sig ganska bra från utpressningsprogram. I ett fall observerades angreppet så snabbt att angriparens verksamhet kunde följas i realtid och hindra tillträde till företagets miljö.
- Det gjordes flera M365-dataintrång när offren av misstag hade accepterat angriparens enhet med sina egna M365-koder. Med hjälp av intrång försökte angriparna begå fakturabedrägerier.

Skadliga program

- Under maj har delning av skadliga program och de dataläckage som begåtts med hjälp av dem varit en betydande olägenhet.
- Man har lyckats dela trojanska på arbetsstationer i form av rekryteringsanmälningar, vilket har lett till att uppgifterna i arbetsstationer har läckt ut till angriparen.
- Via ett leveranskedjeangrepp mot ett internationellt företag har man under maj kunnat sprida skadliga program till olika organisationer som har använt företagets produkter och tjänster.
- Med ClickFix-teknik har man under maj delat ut skadliga program via knäckta webbsidor.

Sårbarheter

- I maj gjorde man fem anmälningar om sårbarheter.
- Sårbarheterna gällde Drupal Coreen (CVE-2026-9028), Cisco Catalyst SD-WAN -produkten (CVE-2026-20182), cPanel- och WHM -hanteringsprogrammen (CVE-2026-29201, CVE-2026-29202, CVE-2026-29203), Ivanti EPMM -produkten (CVE-2026-5786, CVE-2026-5787, CVE-2026-5788, CVE-2026-7821, CVE-2026-6973) samt Palo Alto PAN-OS-programvarans User-ID Authentication Portal -tjänst (CVE-2026-0300).
- En del av sårbarheterna har utnyttjats aktivt.

Fenomen i cybervädret
maj 2026 2/2

1 mån.

Bedrägerier och nätfiske

- På morsdagen i maj försökte brottslingar få föräldrar att tro att deras barn hade en ny telefon. Med hjälp av ett bedrägerimeddelande försökte man få mamman att skicka pengar.
- Traficom har använts som förevändning i bedrägerier.
  I nätfiskemeddelanden hänvisas till obetalda böter som förfallit till betalning, och på så sätt försöker man komma över bankkoder.
- När semestersäsongen närmar sig ökar också vd-bedrägerierna.
  Semestervikarier försöks luras att godkänna betalningar till bedragarens konto genom förfalskade meddelanden i chefens namn.

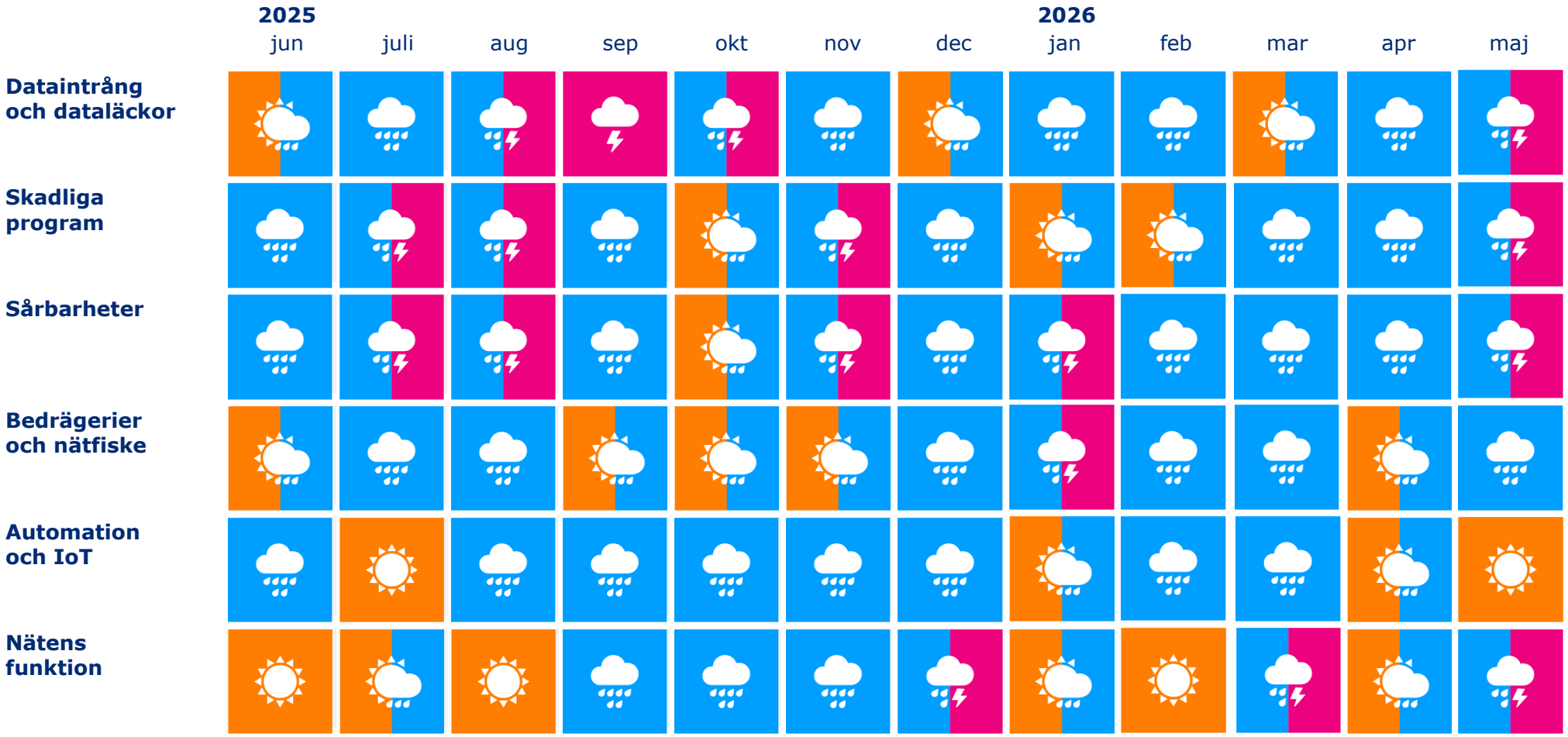
Automation och IoT

- Den nationella lagen som kompletterar CRA om cybersäkerhetsresiliens för vissa produkter samt cybersäkerhets-certifiering trädde i kraft den 1 juni 2026. Lagen behandlar marknadstillsyn, anmälan av anmälda organ samt administrativa påföljder. Dessutom kompletterar lagen den nationella regleringen om EU:s cybersäkerhetscertifieringar. Dessa uppgifter sköts centralt av Transport- och kommunikationsverket Traficom.
- Bestämmelserna om anmälda organ börjar tillämpas den 11 juni 2026, från vilket datum det är möjligt att ansöka hos Traficom om att bli anmält organ för bedömningsuppgifter enligt CRA.

Nätens funktion

- Överbelastningsangrepp är vardag på internet och därför måste tjänster som erbjuds på nätet skyddas.
  Även om angreppen inte helt kan förhindras kan de avvärjas och deras effekter minimeras.
- Antalet allvarliga funktionsstörningar i näten låg på en exceptionell nivå i maj.

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.

Det finns inga särskilda förändringar att notera i cyberläget i juni. Dataintrång och sårbarheter fortsätter sannolikt att vara på samma nivå. I juni börjar effekterna av sommarsemestersäsongen synas i cybersäkerheten i form av olika bedrägerier, såsom vd-bedrägerier och olika nätfiskeförsök kopplade till resande.

Organisationens beredskap

- Organisationernas beredskap och förmåga får inte vara beroende av informationssäkerhets-personalens semester.
- Innan du går på semester är det bra att säkerställa att de enheter och applikationer du använder är uppdaterade och uppdatera dem.

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.