TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

Juni 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 juni 2026

I cybervädret i juni syntes mörka moln, men stormen uteblev tills vidare

Den globala FortiBleed-angreppskampanjen påverkade även Finland, där cirka 20 enheter utsattes för intrång. Även om kampanjen förde med sig mörka moln vid horisonten har det än så länge inte förekommit några betydande konsekvenser.

Månaden medförde med sig för sommarsemesterperioden typiska bedrägerier som framför allt nya sommarjobbare bör vara vaksamma mot. Mot slutet av juni började anmälningar om intrång i M365-konton däremot minska, såsom väntat.

Förnyande av Microsofts Secure Boot-certifikat blev aktuellt i juni, eftersom certifikatens utgång krävde åtgärder från organisationernas sida för att säkerställa en säker uppstart av enheterna.

Cybersäkerhetscentret bedömer situationen för första halvåret 2026

Cybersäkerhetsläget i Finland har varit stabilt under första halvåret 2026. Även om hotbilden inte har förändrats på något betydande eller plötsligt sätt har cyberhoten utvecklats i takt med tekniken och angriparnas arbetssätt. Särskilt användningen av artificiell intelligens i angrepp, ökningen av M365-kontointrång och risker som riktas mot leveranskedjor har blivit centrala bekymmer.

Månadens hagelskur
Sommarsemestertiden och vikariearrangemang skapar en gynnsam grogrund för vd-bedrägerier

Under sommarperioden arbetar fler vikarier och nya anställda än vanligt i organisationerna. De känner inte nödvändigtvis till etablerade rutiner eller verifieringsprocesser. Det gör perioden särskilt lockande för kriminella.

Typiskt för bedrägerierna är att bedragaren utger sig för att företräda företagets ledning och begär brådskande åtgärder, såsom kontoöverföringar, inköp av presentkort eller betalning av fakturor. Som förevändning kan bedragaren använda till exempel ett brådskande företagsaffär eller någon annan avvikande situation.

Kriminella utnyttjar aktivt telefonsamtal, textmeddelanden, e-post, snabbmeddelanden och sociala medier. Därför räcker det inte som bevis på äkthet att någon påstår sig kontakta dig från till exempel en bank, en myndighet eller ett känt företag.

För att minska riskerna uppmanas organisationer att

- säkerställa att processerna för godkännande och kontroll av betalningar är kända på alla nivåer i organisationen
- alltid kontrollera avvikande förfrågningar via en annan kommunikationskanal
- undvika ekonomiska beslut som fattas i brådska
- vid behov verifiera identiteten ansikte mot ansikte.

Cybersäkerhetscentrets åtgärder och tips för förberedelser

Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom har sammanställt en checklista för semesterfirare för att hjälpa dem att upprätthålla en god cybersäkerhet under semestern.

Skydda nätets kantenheter: Ta bort kantdatorsystemens kontrollpaneler och andra gränssnitt från att vara synliga på internet. Håll enheterna alltid uppdaterade och övervaka deras funktion. Aktivera multifaktorsautentisering även för VPN-inloggning alltid när det är möjligt.

Sommarsemesterperioden är högsäsong för bedragare.
Ta del av våra tips för att undvika att bli utsatt för bedrägerier.

Fenomen i cybervädret

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

Fenomen i cybervädret
juni 2026

1 mån.

Dataintrång och dataläckor

Olika kantdatorsystem utsattes för dataintrång där man utnyttjade sårbarheter samt utläckta användarnamn. Trots det stora antalet intrång kunde allvarliga konsekvenser undvikas.

Skadliga program

Under månaden har skadliga program spridits ut i e-postbilagor samt via skadliga webbsidor med användning av ClickFix-teknik. Till antalen har observationer av skadliga program varit måttliga.

Sårbarheter

Under juni har trenden med att nya sårbarheter upptäcks fortsatt att öka. Användningen av artificiell intelligens för att hitta sårbarheter har väckt mycket diskussion globalt.

Bedrägerier och nätfiske

I bedrägerimeddelanden som skickades i barnskyddets namn försökte man komma över bankkoder genom nätfiske. Man försökte lura företag med teman som gällde förnyelse av domännamn. I bedrägerisamtal som gjordes i Klarnas namn försökte man få offret att installera fjärrstyrningsprogrammet UltraViewer på sin dator.

Automation och IoT

Cybersäkerhetscentret arrangerade ett informationsmöte den 3 juni om lagen om cyberresiliens, och en sammanställning av svaren på frågorna som ställdes under evenemanget samt en inspelning av evenemanget finns på evenemangssidan.

Nätens funktion

Överbelastningsangrepp orsakade inte några betydande störningar i Finland.

Fenomen i cybervädret
maj 2026 1/2

1 mån.

Dataintrång och dataläckor

- I dataintrång utnyttjar man allt oftare sårbarheter för att komma in. Bland annat flera av Palo Altos GlobalProtect VPN-enheter hackades i maj genom att utnyttja sårbarheten CVE-2026-0257.
- I samband med FortiBleed-agreppskampanjen äventyrades över 70 000 Fortinets FortiGage-brandväggsutrurstning och SSL-VPN-utrustning runt om i världen. Till följd av det observerades dataintrång också i Finland och uppgifter om sammanlagt cirka 20 enheter läckts ut.
- Anmälningar om dataintrång i M365-konton minskade mot slutet av månaden på samma sätt som under föregående år. Enligt trenden kan följande våg av dataintrång förväntas efter sommarsäsongen, i början av hösten.

Skadliga program

- Cybersäkerhetscentret har fått anmälningar om enstaka riktade e-postmeddelanden där man gömt ett skadligt program i bilagor. Med dessa har man försökt kapa administrationen av datorn eller konton och användar-ID:n som är kopplade till datorn, t.ex. M365-konton.
- Distribution av skadliga program som görs med hjälp av ClickFix-teknik har blivit vanligare under månaden. Skadliga program sprids med ClickFix-tekniken via misstänkta eller knäckta webbsidor. Man har dock ofta observerat skadliga program tillräckligt tidigt så att det inte har blivit några skador.

Sårbarheter

- Sårbarhetstrenden har fortsatt öka och för tillfället verkar det vara så att antalet nya hittade sårbarheter kommer att vara över 50 000 år 2026.
- I början av juni publicerade Cybersäkerhetscentret ett sårbarhetsmeddelande om sårbarheten Check Point VPN (CVE-2026-50751) som utnyttjades aktivt.
- Globalt har det förts en omfattande diskussion om möjligheten att använda artificiell intelligens för att upptäcka nya sårbarheter.

Fenomen i cybervädret
juni 2026 2/2

1 mån.

Bedrägerier och nätfiske

- En hel del bedrägerier anmäldes i barnskyddets namn. Meddelanden har skickats med olika barnskyddsrelaterade teman samt via textmeddelande och e-post och till exempel genom att utge sig för att vara säker e-post. Nätfiskesidor har observerats även med .fi-domännamn. I bedrägeriet vill man få mottagarens bankkoder.
- Bedrägerimeddelanden i ”DMS Finlands” namn skickades till företag. I meddelanden skulle mottagaren förnya sitt domännamn.
- I Klarnas namn ringdes bedrägerisamtal där angriparen försökte få offret att installera fjärråtkomstprogrammet UltraViewer på sin enhet.

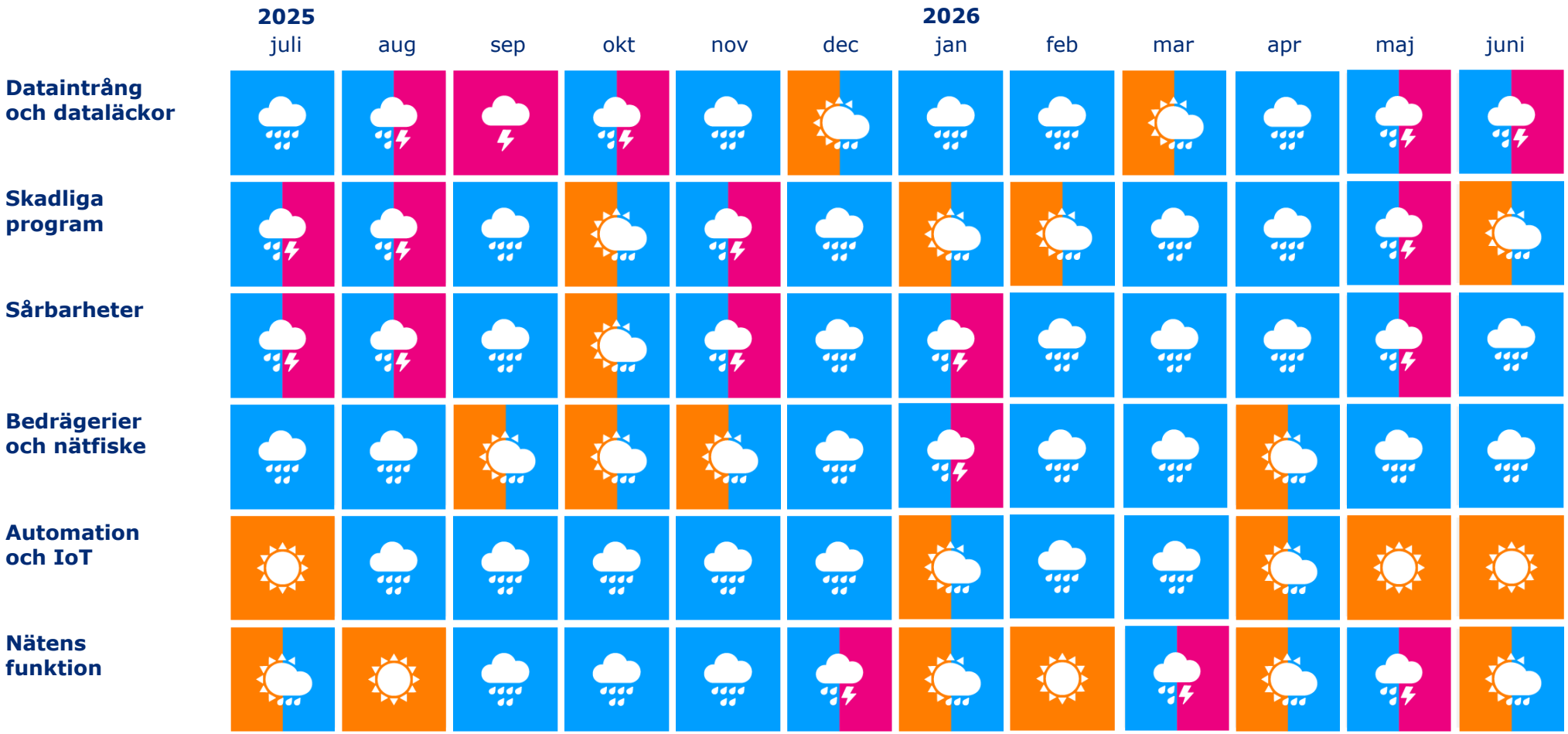
Automation och IoT

- Cybersäkerhetscentret arrangerade ett informationsmöte den 3 juni om lagen om cyberresiliens, och en sammanställning av svaren på frågorna som ställdes under evenemanget samt en inspelning av evenemanget finns på evenemangssidan.

Nätens funktion

- I allmänna kommunikationsnät observerades i juni tre lindrigare störningar och en allvarligare störning i funktionen av allmänna kommunikationsnät i Finland, varför telefontrafiken delvis var förhindrad i abonnemang som använder ett självständigt 5G-nät.
- De konsekvenser som observerades av överbelastningsangrepp i Finland begränsade sig till tillfälliga störningar.
- Även om överbelastningsangrepp har blivit vardag under de senaste åren kan de dock fortfarande ha skadliga konsekvenser och det lönar sig att skydda sig mot dem.

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

Konsekvenserna från angrepps-kampanjen FortiBleed, som blev aktiv i juni, förväntas vara måttliga i Finland. Cybersäkerhetscentret följer situationen aktivt.

Det förväntas att semesterperiodens effekter kommer att fortsätta även under juli och augusti i form av olika bedrägeriförsök.

Antalet anmälningar till Cyber-säkerhetscentret brukar minska under sommarperioden men börjar öka igen när semesterperioden i organisationerna närmar sig sitt slut i början av hösten.

Organisationens beredskap

- Skyddet av kantenheter är en central del av organisationernas cyberberedskap. Riskhanteringen förutsätter proaktiv hantering av uppdateringar, säkra konfigurationer, multifaktorsautentisering och effektiv övervakning av incidenter.
- Efter semesterperioden väntas antalet intrång i M365-konton öka. Organisationer bör vidta skyddsåtgärder mot kontointrång.

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.