

TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

September 2026

Cyberväder

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 cyberväddret i september 2026

Regn och storm på kantnätet

Cybersäkerhetsläget i Finland i september präglades av bedrägerier, intrång i webbplatser samt kritiska sårbarheter i nätets kantenheter. Bedrägerier var igen mångsidiga och till exempel vd-bedrägerier förekom nästa varje dag. Intrång i finländska WordPress-webbplatser och spridning av skadliga program med ClickFix-tekniken fortsatte. Dessutom publicerades flera kritiska och aktivt utnyttjade sårbarheter, till exempel i Cisco-, F5-, Check Point- och GitLab-produkter.

Vid slutet av september publicerade Cybersäkerhetscentret en allvarlig varning om sårbarheter i Citrix NetScaler ADC- och Gateway-produkter som har använts för att genomföra flera dataintrång i Finland. I detta fall är uppdatering inte tillräckligt utan miljön ska inspekteras även för spår på inbrott.

Blixtar som träffar nätverkets kantenheter även utomlands

- Nolldagarssårbarheter i Citrix NetScaler-enheter utnyttjades globalt från början av september. De gällde bland annat organisationer inom den offentliga förvaltningen och finansieringen i Europa och Nordamerika.
- I Norge förekom vid slutet av augusti och i september flera omfattande överbelastningsangrepp, som delvis påstods ha utförts av en Rysslandsvänlig hacktivistgrupp.
- Motsvarande aktivitet har inte observerats i andra nordiska länder, men i september höjde Danmark sin egen cyberhotbedömning till nivån hög för förödande cyberangrepp.

Cybersäkerhetscentrets åtgärder och tips för förberedelser



Cybersäkerhetscentret publicerade årets första allvarliga varning. Varningen publicerades i anslutning till kritiska sårbarheter i Citrix NetScaler ADC- och gateway-produkterna som uppdagades i slutet av september.



Nätfiske är ett vanligt sätt att göra intrång i organisationers Microsoft 365-användarkonton. Artikeln på våra webbsidor belyser hur nätfiske efter Microsoft 365-uppgifter och kapning av Microsoft 365-konto fortskrider, hur man kan upptäcka ett dataintrång och avgränsa det samt vilka tekniska skyddsåtgärder en organisation vidta för att minska risken för att användarkonton äventyras.



Med hjälp av hotmodellering kan organisationer identifiera informationssäkerhetsrisker i programvara och system redan vid utvecklingsskedet, och de kan göra informationssäkerhet till en planerad och integrerad del av programvaruutvecklingen. På våra webbsidor publicerade vi ett materialpaket samt utbildningar som stöder det och som hjälper organisationer att komma i gång med arbetet och öva hotmodelleringen i praktiken.

Fenomen i cybervärdet

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



Fenomen i cybervädet

september 2026



Dataintrång och dataläckor

I september inkom det 81,5 % mer anmälningar om dataintrång än månaden innan. I dataintrång utnyttjade man sårbarheter i programvara och utpressningsprogram drabbade särskilt små företag.



Skadliga program

Under granskningsperioden har det observerats flera finländska webbplatser där man har delat skadliga program med hjälp av ClickFix-tekniken. I GitLab har man spridit skadliga paket samt skadliga program.



Sårbarheter

Under september gavs till och med åtta sårbarhetsmeddelanden. Antalet utnyttjade sårbarheter har ökat och exploateringen av dessa sårbarheter har blivit snabbare.



Bedrägerier och nätfiske

Enligt Finansbranschens färskaste utredning avvärjde bankerna över hälften av bedrägeriförsöken under första halvåret. Antalet bedrägeriförsök ökade ändå med nästan en tredjedel jämfört med motsvarande period året innan.



Automation och IoT

I konferenserna VehicleSec '26 och WOOT '26 presenterades forskningsresultat för svagheter som hittats i elfordonens laddningssystem och som angriparen kunde utnyttja för att få ekonomisk nytta eller störa laddningen. Videorna offentliggjordes i september.



Nätens funktion

Under september observerades några hacktivistiskt motiverade överbelastningsangrepp mot finländska organisationer.



Fenomen i cyberväddret

september 2026 1/2



Dataintrång och dataläckor

- Sårbarheter i programvara utnyttjades fortfarande i flera dataintrång. I mer än hälften av dessa incidenter utnyttjade man sårbarheter på webbplatsen WordPress.
- Utpressningsprogrammen riktade sig i synnerhet mot små företag. Angripare kom in i systemen via en sårbarhet eller via VPN-konton som använts utan multifaktorsautentisering.
- Dataintrång i Microsoft 365-konton ökade kraftigt vid slutet av månaden.



Skadliga program

- Under september har Cybersäkerhetscentret fått motta flera anmälningar om finska webbsidor där man delat ut skadliga program eller skadlig kod genom att använda ClickFix-tekniken. Webbplatserna har ofta komprometterats genom utnyttjande av WordPress-sårbarheter.
- Cybersäkerhetscentret fick observationer och anmälningar där man berättade att man delar skadliga repositorer i GitLab-tjänsten. Repositorierna togs dock snabbt bort från GitLab.



Sårbarheter

- Vad gäller sårbarhetsmeddelanden i september framträdde Citrix NetScaler tydligt.
- På grund av ett allt snabbare utnyttjande av sårbarheter är det allt viktigare att känna sin egen miljö och angreppsgränssnittet och installation av säkerhetsuppdateringar är allt mer brådskande i synnerhet i kantenheter.
- Förutom att uppdatera system är det ofta motiverat att säkerställa att sårbarheten inte har hunnit utnyttjas innan uppdateringen genomfördes.



Fenomen i cybervädret

september 2026 2/2



Bedrägerier och nätfiske

- Enligt Finansbranschens färskta utredning avvärdade bankerna över hälften av bedrägeriförsöken under första halvåret. Antalet bedrägeriförsök ökade ändå med nästan en tredjedel jämfört med motsvarande period året innan.
- Utöver traditionellt nätfiske och investeringsbedrägerier försöker kriminella utnyttja bankkoder till exempel för att öppna nya bank- och telefontjänster samt för att ta lån och göra avbetalningsköp.
- Det viktigaste budskapet i utredningen är att bedrägerier blir allt vanligare och att metoderna utvecklas snabbt.



Automation och IoT

- Laddningsinfrastrukturens risker begränsas inte bara till dataintrång.
- Programvarufel i laddare för elfordon kan medföra att laddningen inte avbryts när den skulle eller laddningen debiteras en annan person. På grund av informationssäkerhetsbrister i gamla kommunikationsprotokoll kan batteriet urladdas eller el kan användas obehörigen.
- I Finland uppställer cybersäkerhetslagen krav på laddningspunktsoperatörer om de till storleken är tillräckligt stora eller om deras verksamhet annars anses vara kritisk.

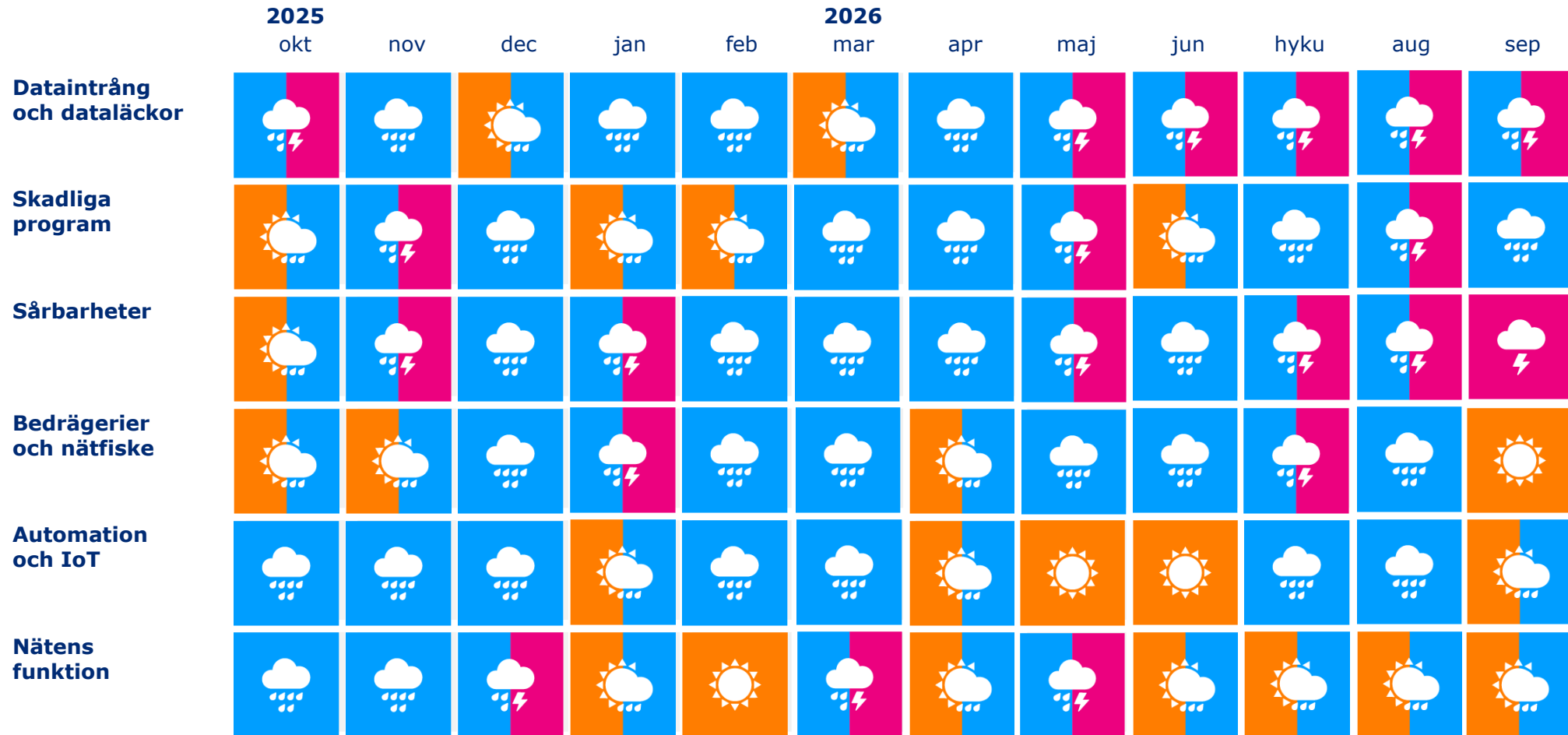


Nätens funktion

- Under september observerades några hacktivistiskt motiverade överbelastningsangrepp mot finländska organisationer. Vissa enstaka angrepp medförde högst små konsekvenser i form av korta avbrott i tjänsten.
- Europols operation PowerOFF verkar i samarbete med internationella myndighetsparter för att avstänga tjänster som man köper för överbelastningsangrepp. Som en del av operationen försöker myndigheterna ingripa i underhåll och drift av sådana tjänster.



Fenomen i cybervädret de gångna 12 mån.



Cyberväderprognos

Cyberväderprognosen 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

Oktober har börjat i ostadigt väder, och det kommer sannolikt att fortsätta så. Stormen Citrix som förekom i slutet av september är ännu inte över och dess konsekvenser följs under oktober. Det är möjligt att det opportunistiska utnyttjandet av sårbarheten fortsätter. Bedrägerierna medför antagligen fortfarande regnigt väder och för intrång i webbplatser kan man vänta lokala regnskurar.

Rapporteringsskyldigheten enligt cyberresiliensförordningen började den 11 september 2026, och i oktober får man se de första erfarenheterna av tillverkarnas anmälningar.

För användare betyder detta mer aktuell information om sårbarheter i enheter.



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.



6–24 mån.

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.