TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

Månad år

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 januari 2026

Internationellt betydande incidenter medförde blixtar även i Finland

Bland de betydande incidenterna i oktober fanns de kritiska sårbarheter som upptäcktes i programmeringsspråket PHP. Programmeringsspråket PHP används som grund för många webbplatser och webbtjänster världen över. Organisationernas skyddsåtgärder orsakade omfattande avbrott i webbtjänster.

I Europa genomfördes i oktober cyberangrepp mot styrsystem för kylutrustning i livsmedelsbutiker. Motsvarande angrepp spreds även till Finland i början av november. Informationssäkerheten i OT-enheter har redan under en längre tid varit ett aktuellt ämne bland annat på grund av angrepp mot energi- och vattenförsörjningssektorerna.

Ett stort antal sårbarheter publicerades fortfarande.

Mörka moln hopar sig på cyberhimlen när användningen av artificiell intelligens ökar i bedrägerier

I de anmälningar som Cybersäkerhetscentret fått har det blivit vanligare med videosamtalsbedrägerier där man utger sig för att vara polis eller bankanställd. Deepfake-teknik, det vill säga teknik för djupförfalskningar, misstänks utnyttjas i bedrägerier. Syftet är att komma över bankkoder, betalkortsuppgifter och andra personuppgifter.

På tapeten i oktober var också bedrägerimeddelanden som skickats i hotell- och inkvarteringstjänsters namn. I meddelandena utnyttjades riktiga bokningsuppgifter som kan ha läckt ut via en inkvarteringstjänst eller ett bokningssystem.

Cybersäkerhetscentrets åtgärder och tips för förberedelser



Oktober var den europeiska cybersäkerhetsmånaden. Syftet med EU:s kampanj är att öka medborgarnas och organisationernas medvetenhet om cybersäkerheten. Cybersäkerhetscentret deltog i kampanjen genom att dela tips för informationssäkerhet för alla på sociala medier via nätverket Nyt valppaana (Var försiktig på webben).



Genom Traficoms föreskrift blev det svårare att genomföra textmeddelandebedrägerier. Från och med den 2 november 2026 ska operatörerna ändra meddelandets avsändaridentifikation till "Skräppost" eller förhindra att sms-meddelandet levereras, om meddelandets avsändare inte har bekräftad behörighet till avsändaridentifikationen.



Betydelsen av att skydda IoT- och OT-enheter har lyfts fram särskilt under de senaste månaderna. Vi publicerade en heltäckande artikel där vi går igenom skyddsprinciper och senaste incidenter.

Månadens hagelskur
Kritiska sårberheter i PHP-programmeringsspråket

PHP-sårbarheterna utgjorde ett internationellt avsevärt incident

I programmeringsspråket PHP, som används i stor utsträckning för att genomföra webbtjänster, hittades kritiska sårbarheter som gör det möjligt att fjärrköra kod. Genom att utnyttja sårbarheter kan angriparen lyckas exekvera kommandon på en sårbar server och eventuellt få kontroll över servern.

Uppgiften om sårbarheterna publicerades den 20 oktober, och korrigeringsuppdateringar den 21 oktober. Efter att sårbarheterna offentliggjorts stängdes tillfälligt upp till miljontals webbplatser ned världen över. Man kan utveckla angreppsmetoder för sårbarheter mycket snabbt speciellt efter det att den programversion som korrigerar sårbarheten har publicerats.

Det förekom omfattande skanning efter och försök att utnyttja PHP-sårbarheterna. De första bekräftade fallen där sårbarheterna framgångsrikt utnyttjades upptäcktes snabbt världen över.

Cybersäkerhetscentret vet inte om utnyttjandeförsök eller dataintrång skulle ha gjorts i Finland med dessa PHP-sårbarheter. Hantering av sårbarheter medförde dock avbrott i många tjänster när sårbara tjänster avstängdes eller begränsades som försiktighetsåtgärd.

Sårbarheterna utgjorde en internationellt avsevärd incident, och deras potentiella påverkningsområde var mycket stort. PHP används i ett stort antal webbtjänster världen över, vilket innebär att sårbarheterna kan beröra många olika slags organisationer och tjänsteleverantörer. Riskpotentialen utökas av att PHP också kan användas i programvaror och enheter från tredje parter.

Fenomen i cybervädret

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

Fenomen i cybervädret
oktober 2026

1 mån.

Dataintrång och dataläckor

Antalet anmälningar om dataintrång ökade klart i oktober. WordPress-sårbarheter utnyttjades för att sprida ClickFix-innehåll, vilket betonar att uppdateringar är viktiga. Dataintrång i Microsoft 365-konton ökade kraftigt.

Skadliga program

Under oktober har man observerat skadliga program och spridning av dem bland annat som bilagor till enstaka e-postmeddelanden och på webbplatser som hackats med ClickFix-tekniken.

Sårbarheter

I oktober publicerades 6 sårbarhetsmeddelanden.

Antalet sårbarheter fortsatte att öka och under oktober beviljades över 17 000 nya CVE-koder när antalet var 4 273 i oktober 2025.

Bedrägerier och nätfiske

Antalet bedrägerier som gjorts i bokningstjänsters, myndigheters och bankers namn ökade.

Bekämpning mot textmeddelandebedrägerier blev effektivare: i stället för den oregistrerade avsändarens namn står det nu ”Skräppost”.

Automation och IoT

I Europa orsakade cyberangrepp mot kylutrustning betydande produktsvinn och ekonomiska förluster.

Angreppen avslöjade riskerna med sårbara fjärrstyrda enheter som gäller alla lösningar som är synliga i det offentliga internet.

Nätens funktion

Oktober var normal med tanke på överbelastningsangrepp. Överbelastningsangrepp har funnits och de har medfört tillfälliga, begränsade konsekvenser för tillgången till tjänster.

Fenomen i cybervädret
månad år 1/2

1 mån.

Dataintrång och dataläckor

- Antalet anmälningar om dataintrång ökade klart från september, även om månaden annars var mycket normal.
- Sårbarheter i programvara utnyttjades på ett omfattande sätt i en del av de anmälda dataintrången. I de flesta fall användes sårbarheter i WordPress för att lägga till ClickFix-innehåll på webbsidorna. Det lönar sig för organisationer att satsa på uppdatering av WordPress-webbplatser och hantering av sårbarheter.
- Antalet dataintrång i Microsoft 365-konton ökade kraftigt i oktober. Flest fall rapporterades inom små organisationer inom fastighets- och byggbranschen.

Skadliga program

- Under granskningsperioden har man observerat skadliga program och spridning av dem speciellt med hjälp av ClickFix-tekniken. Till exempel har intrång på WordPress-webbplatser ofta lett till att skadlig kod eller annat skadligt innehåll laddats upp på den komprometterade webbplatsen, varefter webbplatsen har använts för vidare spridning av skadliga program.
- Cybersäkerhetscentret har fått en anmälan om en incident där organisationen hade mottagit ett USB-minne från en kund. USB-minnet visade sig innehålla ett skadligt program. Det skadliga programmet identifierades innan det hade medfört några konsekvenser.

Sårbarheter

- Mest diskussion i oktober väcktes av PHP-sårbarheter CVE-2026-109618 och CVE-2026-109619 (PHP2Shell).
- Genom att utnyttja sårbarheter kan angriparen eventuellt på distans köra godtyckliga kommandon på servern och ta fullständig kontroll över servern.
- Flera organisationer, t.ex. Valtori, stängde ned sina tjänster innan korrigeringen till sårbarheten publicerades.
- Än så länge har man inte observerat att sårbarheten i PHP hade utnyttjas i Finland.

Fenomen i cybervädret
juli 2026 2/2

1 mån.

Bedrägerier och nätfiske

- Oktober var den europeiska cybersäkerhetsmånaden. Myndigheter, utbildningsorganisationer och andra organisationer delade praktiska tips för en trygg och säker digital vardag i nätverket Nyt valppaana (Var försiktig på webben). Nätverkets cyberrådgivning fortsätter i november.
- Antalet bedrägerier som man gjort i boendebokningstjänsters, i myndigheters och i bankers namn ökade i oktober.
- Till all lycka blev även bekämpningen mot textmeddelandebedrägerier effektivare: i stället för den oregistrerade avsändarens namn står det nu "Skräppost".

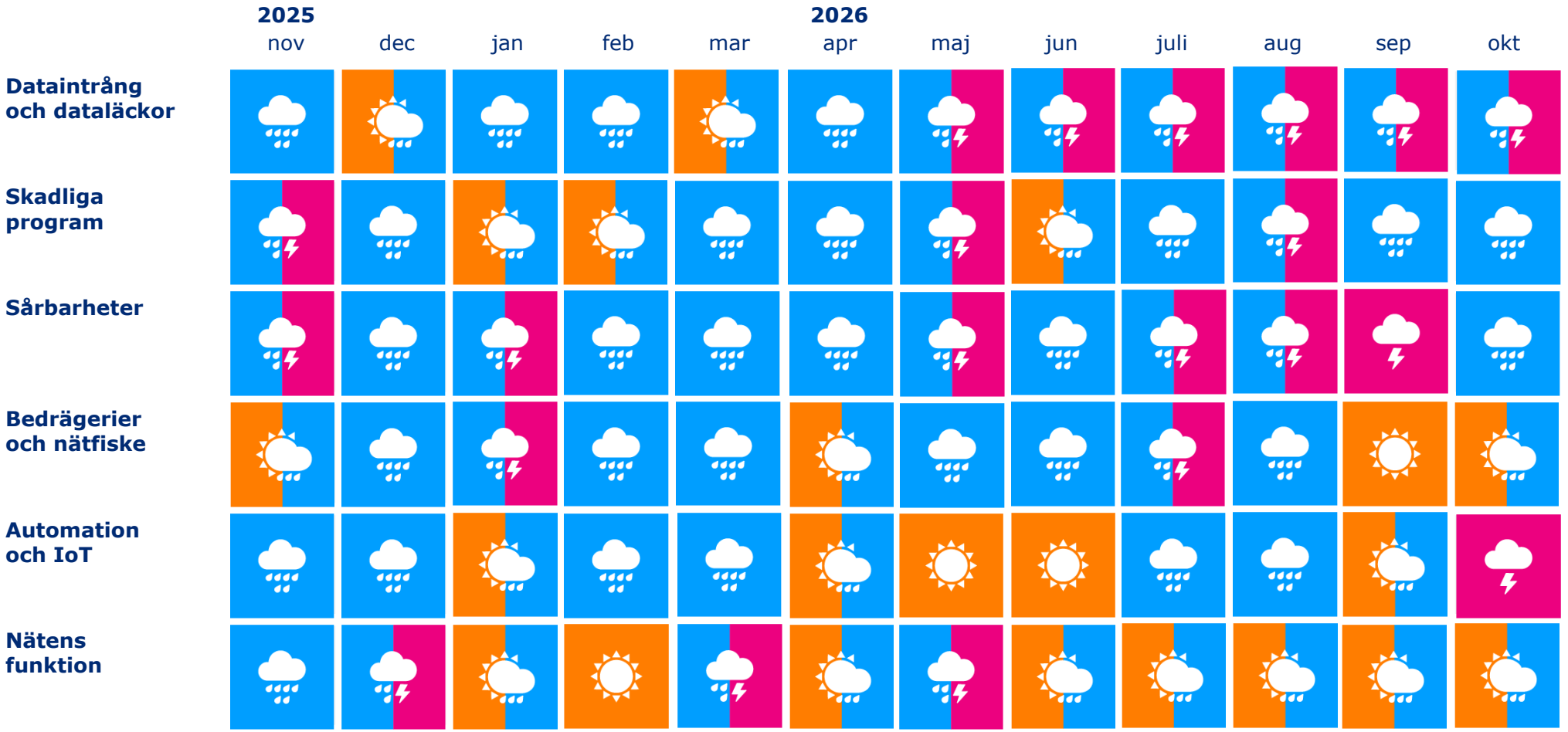
Automation och IoT

- Cyberangrepp mot kylutrustning i Europa visade i praktiken riskerna med fjärrstyrningslösningar som kan ses på det offentliga nätet. Angrepp observerades också i Finland.
- Frankrike attribuerade angreppen mot landets kylutrustning till Iran. Det är ännu inte känt vilka aktörer som ligger bakom angreppen mot andra länder.
- Det inträffade lyfter fram betydelsen av riskhantering och cybersäkerhet i lösningar som styr eller påverkar den fysiska världen. IoT- och OT-enheter ska inte exponeras direkt mot det offentliga internet om det inte är absolut nödvändigt.

Nätens funktion

- Överbelastningsangrepp behöver inte enbart bygga på stora trafikvolymer, utan kan också genomföras genom att utnyttja sårbarheter eller svagheter i programvara.
- Föreskriften om störningar i televerksamheten uppdaterades och har meddelats den 15 oktober. Föreskriften påverkar de störningsanmälningar som teleföretagen ger till både konsumenter och Traficom. Föreskriften träder i kraft den 1 januari 2027.

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

Ordspråket att cybersäkerhet inte känner några nationsgränser har blivit tydligt även för medborgarna, särskilt under oktober, och kommer sannolikt att fortsätta vara det även framöver. Det är sannolikt att cyberpåverkanskampanjer med konsekvenser för flera länder samtidigt samt incidenter till följd av kritiska sårbarheter kommer att fortsätta.

Kontokapningar av M365-konton väntas sannolikt fortsätta även under resten av året.

Organisationens beredskap

- Det lönar sig för en organisation att satsa på utbildning så att användare kan identifiera M365-nätfiskeförsök och anmäla dem till IT-stödet.
- Organisationer bör fortfarande förbereda sig för snabba uppdateringar när kritiska sårbarheter publiceras i snabb takt.
- 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.

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.