TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

Juli 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 helheltsbild 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 juli 2026

I julis cyberväder rapporterades det om sommarskurar

Under högsommaren fick Cybersäkerhetscentret in färre anmälningar om informationssäkerhetsincidenter än under en vanlig månad, men antalet anmälningar har åter börjat öka. Det följer det välbekanta vädermönstret från tidigare somrar, då semesterperioden påverkar anmälningsaktiviteten.

Mörka moln drog ändå in över cyberhimlen i juli i form av utpressningsprogramsattacker. Ett fåtal sådana attacker genomfördes i Finland. Under början av året var vädret förhållandevis stabilt när det gäller utpressningsprogram, men i takt med att temperaturen steg blev också cyberbrottslingarna mer aktiva.

I linje med årets trend offentliggjordes åter flera sårbarheter i juli. Cybersäkerhetscentret lyfte fram fyra av dem i sina sårbarhetsmeddelanden. En viktig orsak till att antalet sårbarheter har ökat markant är att artificiell intelligens används för att söka efter sårbarheter.

Intrång i M365-konton har redan i flera år kommit i vågor. Under sommaren har läget varit lugnare, men framåt hösten väntas kampanjer med kontointrång åter ta fart.

Den snabba utvecklingen av AI-systemens kapacitet och de potentiella hot som är förknippade med systemen och användningen av dem var aktuella också i juli. Samtidigt är det bra att komma ihåg att generativ artificiell intelligens också erbjuder försvararna betydande möjligheter.

Cybersäkerhetscentrets åtgärder och tips för förberedelser

Vi påminde om riskerna med dåligt skyddad nätverksutrustning. Nätverksutrustning som är bristfälligt skyddad eller övervakad kan ge en direkt väg in i organisationens interna nätverk och kritiska system. Det är viktigt att avsätta tillräckliga resurser för att skydda nätverksutrustningen, och det är också bra att öva på hur incidenter som gäller utrustningen ska hanteras.

I snabbmeddelandeappen WhatsApp infördes användarnamn, vilket kan göra trovärdiga bedrägerier möjliga och öka antalet sådana bedrägerier. Organisationer bör överväga att reservera sina officiella användarnamn så tidigt som möjligt.

Antalet skadeprogramsfall där ClickFix-metoden har använts för spridningen ökade åter i juli. Organisationer kan förebygga och begränsa konsekvenserna av attacktekniken ClickFix med tekniska åtgärder som vi berättade om i fjol.

Fenomen i cybervädret

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

Fenomen i cybervädret
juli 2026

1 mån.

Dataintrång och dataläckor

Cybersäkerhetscentret har fått många anmälningar om intrång på WordPress-webbplatser. Antalet anmälningar om utpressningsprogram har ökat jämfört med början av året.

Antalet M365-kontointrång har minskat betydligt under semesterperioden.

Skadliga program

Under juli har spridning av skadeprogram, särskilt med hjälp av ClickFix-tekniken, förekommit oftare än normalt. Intrång på WordPress-webbplatser har gjort webbplatserna sårbara för den här typen av spridning av skadeprogram.

Sårbarheter

Sårbarheter har fortsatt att upptäckas i allt snabbare takt. I juli passerades gränsen på 40 000 CVE-identifierare för 2026, medan det under hela 2025 utfärdades något över 45 000 CVE-identifierare.

Bedrägerier och nätfiske

Under juli har bedragare försökt lura anställda som vikarierat under semesterperioden genom vd-bedrägerier.

Observationerna tyder på att AI-verktyg används i allt större utsträckning för att genomföra bedrägerier.

Automation och IoT

Automationssystem vid flera vattenverk i USA har utsatts för attacker. Systemen har varit bristfälligt skyddade eller helt saknat skydd. Systemägarna bör förbättra skyddet tillsammans med systemleverantörerna.

Nätens funktion

Några överbelastningsattacker har riktats mot finländska organisationer, men de hade endast små konsekvenser för tillgängligheten.

Fenomen i cybervädret
juli 2026 1/2

1 mån.

Dataintrång och dataläckor

- I juli observerades ett stort antal intrång på WordPress-webbplatser, som har utnyttjats för att sprida skadeprogram med hjälp av ClickFix-tekniken.
- Antalet anmälningar om utpressningsprogram har ökat jämfört med början av året. I flera fall har organisationers uppgifter läckt ut eller så har angriparna hotat med att offentliggöra dem.
- Antalet intrång i M365-konton har minskat betydligt under semesterperioden. Antalet fall väntas åter öka betydligt när semesterperioden är över.

Skadliga program

- Anmälningarna om skadeprogram som sprids med ClickFix-tekniken har ökat under juli. Skadliga program sprids med ClickFix-tekniken särskilt via hackade webbsidor.
- Det ökade antalet intrång på WordPress-webbplatser märks också i spridningen av skadeprogram, eftersom hackade webbplatser har utnyttjats för att sprida skadlig kod eller skadliga program.
- Under månaden har olika observationer av skadeprogram anmälts till Cybersäkerhetscentret, men observationerna har inte tytt på några mer omfattande skadeprogramsfenomen.

Sårbarheter

- I WordPress-produkten upptäcktes sårbarheter (wp2shell) som i kombination gör det möjligt att fjärrköra kod utan autentisering. Utnyttjande av sårbarheterna har också observerats i Finland (CVE-2026-63030, CVE-2026-60137).
- En sårbarhet publicerades i Linux Kernel-versionerna 6.0–7.1. Sårbarheten gör det möjligt för en lokal användare att höja sina behörigheter (CVE-2026-53362).
- En kritisk sårbarhet publicerades i NGINX-produkter. Sårbarheten gör det möjligt för en obehörig angripare att fjärrköra kod (CVE-2026-42533).

Fenomen i cybervädret
juli 2026 2/2

1 mån.

Bedrägerier och nätfiske

- Brottslingar har aktivt utgett sig för att vara chefer för olika organisationer. Under juli har bedragare försökt lura semestervikarier genom vd-bedrägerier.
- Observationerna tyder på att AI-verktyg används i allt större utsträckning för att genomföra bedrägerier.
- Med hjälp av AI-verktyg har bedragare också skapat förfalskade bedrägerivideor i polisens namn och riktat dem till personer med utländsk bakgrund som bor i Finland. För bedrägliga videosamtal har snabbmeddelandetjänster som WhatsApp och Google Meet använts.

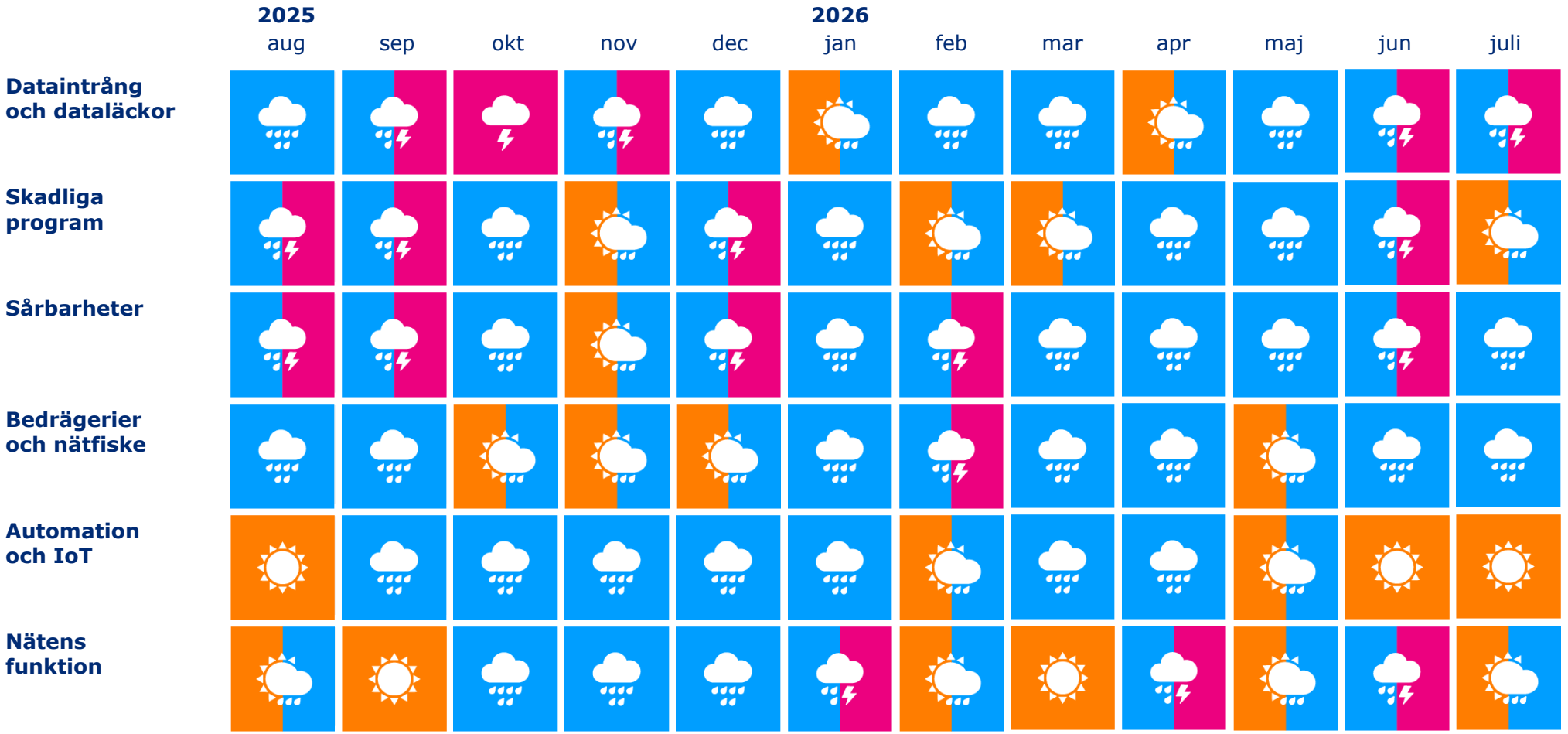
Automation och IoT

- Sedan slutet av juli har automationssystem vid flera vattenverk i USA utsatts för attacker. Attackerna har lett till driftavbrott av måttlig längd. I de aktuella fallen har systemen varit bristfälligt skyddade eller helt saknat skydd.
- Att genomföra attackerna är tekniskt enkelt. Om en attack genomförs beror i praktiken bara på angriparens motivation.
- Även i Finland finns många oskyddade automationssystem.
- Ägarna till automationssystem bör förbättra skyddet tillsammans med systemleverantörerna.

Nätens funktion

- I en rapport som publicerades i juli identifierades en ny typ av överbelastningsattack mot CDN-tjänster. Attacken utnyttjar konvertering mellan protokollen HTTP/3 och HTTP/1.1 för att få trafikmängden att öka mångfalt.
- Överbelastningsattacker kan användas som skenmanöver i mer omfattande cyberoperationer.

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

1 mån.

Antalet intrång i M365-konton som genomförs med hjälp av nätfiske med enhetskoder väntas öka kraftigt under sensommaren och början av hösten. Organisationer bör förbereda sig på situationen genom att hindra användare från att logga in med enhetskod med hjälp av en separat åtkomstkontrollpolicy för Device Code Flow (CA policy) samt övervaka de användare som behöver tjänsten.

Diskussionen om cybersäkerhet i anslutning till allt mer avancerade AI-system kommer att fortsätta vara aktuell även under hösten.

Organisationens beredskap

- På grund av det ökande antalet sårbarheter och det snabba utnyttjandet av nolldagssårbarheter bör organisationer aktivt följa sårbarhetsläget. Särskild uppmärksamhet bör fästas vid uppdateringsprocesserna.
- Skyddet av kantenheter är en central del av organisationernas cyberberedskap. Riskhanteringen förutsätter proaktiv hantering av uppdateringar, säkra konfigurationer, multifaktorsautentisering och effektiv övervakning av incidenter.

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.

- ...