TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

# Cyberväder

December 2025

# Cybervädret förnyas 2026

Utseendet och innehållet i Cybervädret uppdateras från och med januariutgåvan 2026. Med förändringarna strävar man efter en mer tillgänglig, enhetlig och samtidigt mer informativ publikation än tidigare.

Vi beaktade kundresponsen i samband med utvecklingsarbetet och vi har behållit de bästa delarna av Cybervädret. Vid sidan av detta utlovas också nytt innehåll och mer proaktivitet.

Framöver kommer vi att publicera mer omfattande analysbilder, såsom Top 5 hoten, som en del av Cybersäkerhetsvädret i mars och september.

# Cybervädret december 2025

## Dataintrång och dataläckor

- December var lugn när det gäller dataintrång och -läckor. Jämfört med november kom det nästan 30 % färre anmälningar.
- I dataintrången syntes utnyttjanden av sårbarheterna i Ciscos produkter och i Reacts React Server Components.

## Bedrägerier och nätfiske

- Under decemberledigheten har det förekommit omfattande nätfiske riktat mot inkvarteringsföretag och deras kunder. Brottslingar försöker komma över inloggningsuppgifter till inkvarteringstjänster och använder dem sedan för att fiska efter betalkortsuppgifter.
- Konton i snabbmeddelandetjänster har kapats oftare än tidigare. Konton bombas med kontinuerliga inloggningsförsök, eller så försöker man skapa ett nytt konto med offrets telefonnummer. Man ska inte godkänna bekräftelsemeddelanden och inte heller öppna länkarna i dem. Det är viktigt att skydda sina egna konton genom att aktivera multifaktorsautentisering.

## Skadeprogram och sårbarheter

- Kritisk sårbarhet i Reacts funktion React Server Components (CVE-2025-55182)
- I TOTOLINK X5000R-hemroutern har man hittat en sårbarhet som under vissa förhållanden möjliggör kapning av enheten. Det finns ingen korrigering tillgänglig till sårbarheten (CVE-2025-13184).
- Kritisk sårbarhet i produkterna Cisco Secure Email Gateway och Secure Email and Web Manager (CVE-2025-20393)

## Automation och IoT

- Utifrån våra observationer har fjärranslutningarna till OT-system i Finland genomförts på ett informationssäkerhetsmässigt osäkert sätt. Orsaken är bland annat standardinställningarna i de edge-enheter som används i distansförbindelser. Dessa lämpar sig inte för OT-miljöer, eftersom de möjliggör obegränsad trafik mot internet.

## Nätens funktion

- Under julveckan riktade den Rysslandsvänliga gruppen NoName återigen sina överbelastningsangrepp mot finländska mål. Betydande konsekvenser kunde undvikas, men hanteringen av angreppen medförde extra arbete.
- USA:s justitiedepartement har väckt åtal mot en person som kopplats till gruppen NoName. I samband med publiceringen av åtalet uppges det att gruppen NoName har fått ekonomiskt stöd från den ryska staten.
- I slutet av december orsakade skador på undervattenskablar i Östersjön samt stormen Hannes flera driftstörningar.

## Spionage

- Enligt USA står den ryska staten bakom hacktivistgrupperna Cyber Army of Russia Reborn (CARR)/Z-Pentest och NoName057(16) som genomfört cyberangrepp och -störningar i västländerna. Även flera andra länder deltog i uttalandet. CARR/Z-Pentest är länkad till GRU i Ryssland.
- Även Danmark och Tyskland har offentligt anklagat Ryssland för cyberangrepp. Förutom överbelastningsangrepp gjordes det ett angrepp även mot ett vattenförsörjningsverk i Danmark. I Tyskland gjordes angrepp mot flygledningssystemet, och man försökte även störa valen.

# **Cybersäkerhetscentrets**
# åtgärder och tips för förberedelser

Transport- och kommunikationsverket Traficom har utfärdat en ny version av föreskriften om kommunikationsnätets kritiska delar. Den reviderade föreskriften utvidgar regleringen så att den delvis även omfattar 5G-nätets basstationer.

Hanteringen av administratörskonton för molntjänster är en viktig del av molntjänsternas säkerhet. I artikeln Informationssäkerhet Nu! *”Hantering av administratörskonton för molntjänster – bästa praxis*” går vi igenom de tre vanligaste molntjänsterna – Amazon Web Services (AWS), Microsoft Azure och Google Cloud Platform (GCP) – och berättar hur deras administratörskonton ska skyddas och underhållas.

Efter julen kan det finnas nya routrar och andra nätverksanslutna enheter i många hushåll, och deras inställningar bör kontrolleras för att förbättra säkerheten. Du kan läsa anvisningar för routerns inställningar och säker koppling i vår anvisning *”Informationssäkerheten i hemnätet och routern”.*

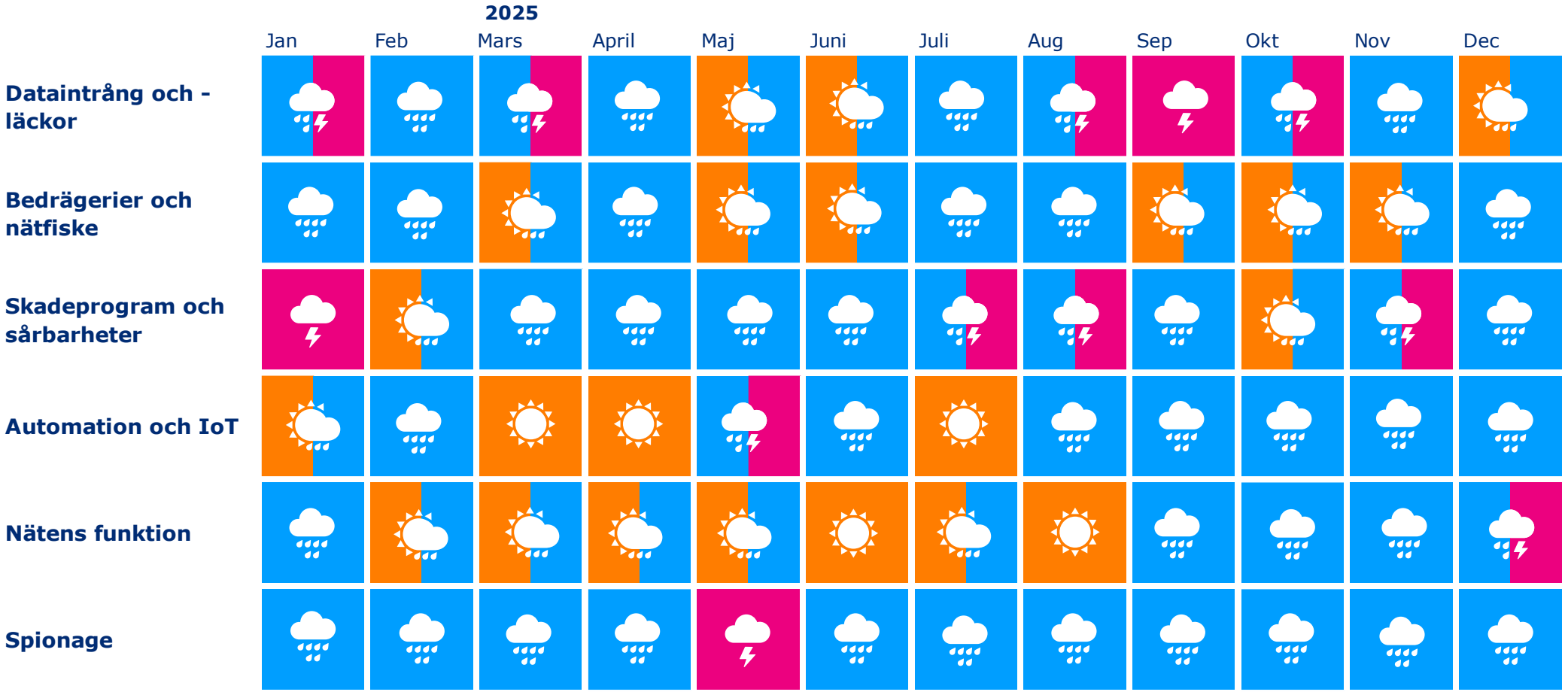
# Allmän översikt över cybersäkerheten i december

December inleddes ur ett cybersäkerhetsperspektiv relativt lugnt, men läget försämrades något mot slutet av månaden.

- I början av månaden gjordes flera anmälningar om falska profiler som hade skapats på webbplatsen Topline.com, och i samband med detta misstänktes identitetsstölder. En betydande mängd uppgifter från LinkedIn-användarprofiler har kopierats till webbplatsen.
- Ett måttligt antal kritiska sårbarheter rapporterades. Bland dessa framhävdes sårbarheterna i Ciscos e-postsäkerhetsprodukter samt sårbarheten i Reacts funktion React Server Components, CVE-2025-55182 – den så kallade React2Shell – under den första halvan av månaden.
- På nyårsafton inträffade åter en skadlig incident som riktades mot undervattenskabeln mellan Finland och Estland, vilket ledde till en flermyndighetsinsats riktad mot fartyget Fitburg. Fartyget misstänks ha skadat Elisas kabel med sitt ankare. Fallet medförde dock inga betydande konsekvenser för dataöverföringen.
- Bland de mest betydande fallen under slutet av året återfanns något överraskande stormen Hannes, som orsakade strömavbrott runt om i landet. Enligt Meteorologiska institutet var stormen en av de värsta på årtionden och orsakade strömavbrott för upp till 180 000 kunder samtidigt.
  - Kraftiga naturfenomen samt de avbrott och fysiska skador som de orsakat hade betydande indirekta effekter på dataöverföringen.

# Trenderna inom cybersäkerhet
de gångna 12 mån.

1 kk



# **Cybervädret på lång sikt:** Cybersäkerhet inom industriautomation

Industriautomationen är i hög grad förknippad med OT-system (Operational Technology), vilket avser de enheter, system och programvaror som används för realtidsstyrning och övervakning av produktionens fysiska processer. Störningar i dessa system kan i värsta fall orsaka allvarliga och omfattande undantagssituationer som äventyrar samhällets funktionsförmåga. Baserat på de senaste observationerna är de tre allvarligaste cyberhoten mot OT-system hacktivism, spionage och sabotage:

- Hacktivisternas mål är att störa sina målobjekt samt att utnyttja insamlad information i informationspåverkan.
- Spionage kan förekomma för att uppnå konkurrensfördelar eller som stöd för politisk informationsinhämtning.
- Motivet bakom sabotage kan vara ekonomisk vinning eller statlig påverkan.

Verksamhetsfälten inom de sektorer som använder industriautomation förändras i allt snabbare takt. Digitalisering, utnyttjandet av artificiell intelligens samt IT/OT-konvergensen ökar, och automationssystemen, fjärradministrationen, övervakningen och den nödvändiga informationen sprids i allt högre grad från de så kallade traditionella anläggningsmiljöerna till ett växande antal olika platser. En risk är att man inom industriautomationsmiljöer inte hänger med i utvecklingen av cybersäkerhet och att resurserna inte räcker till i jämförelse med IT-världen.

I och med ökningen av mängden information, behovet av skyddade och driftsäkra förbindelser, leveranskedjornas längd och komplexitet, miljöernas komplexitet samt den växande angreppsytan uppstår nya utmaningar för beredskapen.

- Man satsar dock allt mer på beredskap och på att skydda produktionsmiljöerna; regleringen och kraven ökar, fler standarder tillkommer och dessa har beaktat informationssäkerhetsaspekter redan från början.
- EU:s cyberresiliensförordning CRA ålägger tillverkarna att upprätthålla en materialförteckning över sina produkter, en så kallad SBOM, software bill of materials, vars användning har främjats internationellt. Detta kommer att underlätta bland annat sårbarhetshanteringen.

Cybersäkerhetscentret samarbetar inom industriell automation i både nationella och internationella nätverk, erbjuder anvisningar och stöd vid incidenter samt kartlägger oskyddade automationssystem, inloggningsfönster och deras kontrollpaneler som är synliga på internet.