TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyberväder

Januari 2025

#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 helheltsbild av vad som har hänt och vad som kommer att hända på cybersäkerhetsfältet.

Cybervädret kan vara:

 lugnt

 oroande

 allvarligt

Cybervädret i januari 2025

Dataintrång och dataläckor

- Flera tillverkares kantenheter har använts som en del av dataintrång. Grundorsaken är ofta användares dåliga informationssäkerhets-kunskaper som utsätter sårbarheter för snabbt utnyttjandde.
- M365-konton har hackats till följd av en lyckad Dropbox-nätfiskekampanj.

Bluff och nätfiske

- Bedrägerier med beskattning som tema har blivit vanligare igen efter årsskiftet. Textmeddelanden med skatt som tema har använts för att locka offer att ge sina bankkoder till bedragare.
- Bedragare har köpt sökmotorreklam vilka har lett till nätfiske. Falska reklam har förekommit i sökmotorer där man som sökord har använt bland annat bankers namn och Traficom.

Skadeprogram och sårbarheter

- Kritisk sårbarhet i Fortinets FortiOS- och FortiProxy-produkter. Enligt Fortinet har sårbarheten utnyttjats aktivt.
- Åtminstone på Tori.fi och Facebooks Marketplace har det förekommit bedrägerier där säljaren har lockats att installera ett skadligt program.

Automation och IoT

- Europeiska kommissionen godkände den 20 januari 2025 en standardiseringsbegäran gällande cyberresliensakten.
- Undersökningen The BlinkenCity om användningen av oskyddade radiosignaler inom energisektorn i Centraleuropa lyfte fram risker och behovet att införa bättre skyddade trådlösa kommunikationsmetoder.

Nätens funktion

- I januari observerades sju funktionsstörningar i allmänna kommunikationsnät.
- Antalet anmälda överbelastningsangrepp ökar.
- En pro-ryska hacktivistgrupp riktade överbelastningsangrepp mot finska webbsidor och berättade att orsaken var Statsrådets försvarsredogörelse som publicerades i december. Effekten av angreppen blev liten.

Spionage

- En sårbarhet som hittades i Ivanti Connect Secure VPN har utnyttjas runtom i världen på dag noll åtminstone från mitten av december för att göra intrång i organisationer.
- Utrustning som misstänks ha hackats har också undersökts i Finland.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Kantdatorsystem som syns på och är öppna mot internet ökar angreppsytan för illvilliga aktörer. I vår Informationssäkerhet Nu!-artikel påminde vi alla om hur viktigt det är att ständigt säkerställa kantdatorsystem.

Ett skadligt program som installerats i telefoner sprider sig för närvarande via marknadsplatser på internet, och med vilket bedragarna kan komma åt allt som finns på telefonen. Vi påminde om säker handling på nätet och att man enbart ska ladda ner appar från officiella appbutiker.

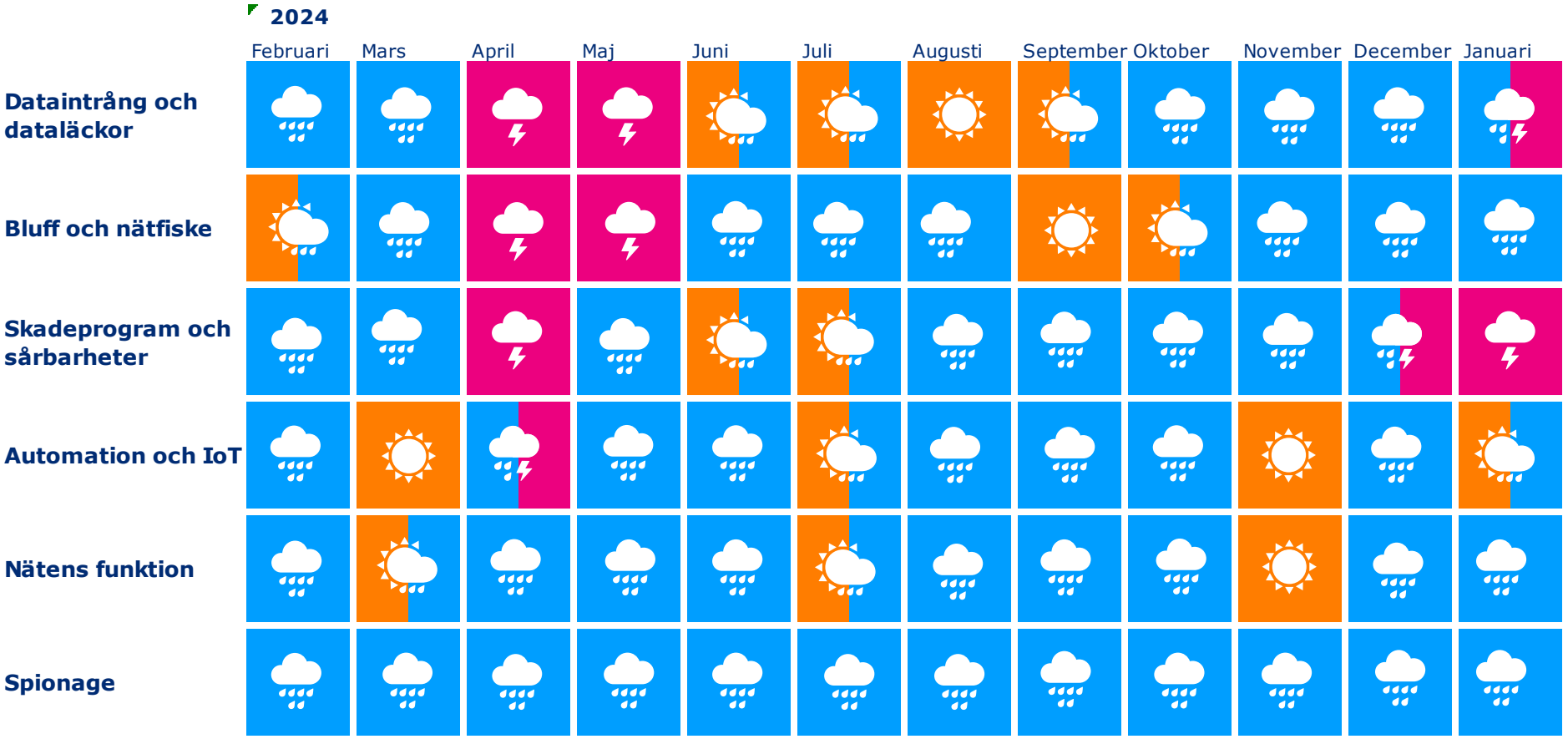
Cybersäkerhetscentret höjde sin beredskapsnivå på grund av toppmötet för Nato-medlemsländerna i Östersjöområdet som ordnades i Helsingfors den 14 januari. Med tanke på cybersäkerheten förlöpte allt lugnt.

Seminariet Informationssäkerhet 2025 ordnas i år den 12 mars. Temat är hur det digitala samhället kan skyddas. Seminariet organiseras av Traficom och Försörjningsberedskapscentralen. Programmet och registreringsblanketten finns på adressen tietoturvaseminaari.fi.

Allmän översikt över cybersäkerheten i januari

- Det blev regnmoln på himlen på grund av allvarliga sårbarheter i Ivantis, Fortnets och SonicWalls produkter. Alla sårbarheter har utnyttjats aktivt. Cybersäkerhetscentret rapporterades om flera dataintrång i Ivanti- och Fortinet-utrustning.
  - En del av sårbarheterna användes av angriparna redan innan produktägarna hade fått veta om dem.
  - Utnyttjandet av två sårbarheter kunde förhindras helt när man begränsade administrationsgränssnittets visibilitet från offentliga nät.
- En Microsoft 365-nätfiskekampanj som utnyttjar Dropbox blev mycket aktiv igen i januari. Kampanjen har resulterat i flera dataintrång på olika sektorer och i nya nätfiskeförsök.
  - För att komma åt e-postanvändarnamn utnyttjar brottslingarna i synnerhet pdf-filer som delas via Dropbox och vars rubrik är till exempel "LASKU_INV_PO300125.PDF". I de fall som Cybersäkerhetscentret fått kännedom om har man försökt logga in på användarkontot till och med inom några minuter efter att användaridentifikationen har matats in på nätfiskesidan.
  - I de fall som Cybersäkerhetscentret fått kännedom om har det kapade e-postkontot försetts med en meddelandehanteringsregel som flyttar alla meddelanden som kommer som ordet "dropbox" till mappen RSS-flöde. Målet är att användaren inte ska märka suspekt verksamhet på kontot.
  - Cybersäkerhetscentrets anvisningar för vad man ska göra vid dataintrång ger råd för förebyggande åtgärder och hur man kan försäkra säkerheten på ens eget M365-konto.

Trenderna inom cybersäkerhet
de gångna 12 mån.



Top 5-hot i den närmaste framtiden (6 månader–2 år)

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.

Utpressningsprogram - Betydande hot mot organisationer

Under det senaste året har flera organisationer i Finland drabbats av ett utpressningsprogram, och antalet ökar kontinuerligt också globalt.

3.

Informationssäkerheten och kontinuiteten i leverans- och servicekedjor är allt mer kritiska.

Att förstå underleverantörskedjan är centralt för organisationernas egen cybersäkerhet. De flesta organisationer är mer eller mindre beroende av utlagda digitala tjänster.

Ny

Uppdaterad

Symboler

4.

Organisationer bör vara förberedda för AI-relaterade utmaningar.

Det skulle vara bra för organisationer att identifiera de utmaningar som artificiell intelligens medför och förbereda sig på dem till exempel genom att utbilda sin personal.

5.

Skyddet av kommunikationsinfrastruktur blir allt viktigare

Skyddet av kommunikations- och systeminfrastruktur är viktigt utomlands och i Finland, både på grund av de skador och naturfenomen som de blir utsatta för samt på grund av avsiktliga störningar orsakade av utomstående.