TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyberväder

Mars 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 mars 2025

Dataintrång och dataläckor

- Antalet Akira-fallen har ökat under början av året. I angreppen utnyttjar man fortfarande kantenheter och MFA som saknas för att komma in.
- Från kapade M365-konton skickades fakturabedrägerier som ökade de förfalskade meddelandenas trovärdighet genom registrering av ett domännamn som liknade offrets domännamn (typosquatting).

Bedrägerier och nätfiske

- Cybersäkerhetscentrets nya anvisning hjälper att undvika bedragare på webben och i telefonen (på finska).
- Beskattning som tema har använts en hel del vid nätfiske efter bankkoder i mars.
- Konton för sociala medier kapas igen genom att skicka ett snabbmeddelande till offret där man frågar efter offrets telefonnummer och sedan ”utlottningskoden”.

Skadeprogram och sårbarheter

- Infektioner med utpressningsprogram observerades i mars, speciellt i anmälningar som gällde det skadliga programmet Akira. I angreppen har man utnyttjat sårbara kantenheter
- Det rekommenderas att kantenheterna alltid uppdateras utan dröjsmål.

Automation och IoT

- Japan har publicerat sitt eget cybersäkerhetsmärke för IoT-enheter.
- Europeiska standardiserings-organisationer har godkänt EU-kommissionens standardiserings-begäran som gäller Cyberresiliens-akten (CRA) och börjat arbetet.

Nätens funktion

- Det observerades inga störningar i de allmänna kommunikationsnätens funktion i mars.
- Köpta DDOS-tjänster blir vanligare vid överbelastningsangrepp. Till exempel det Mirai-baserade botnätet GorillaBot har använts i angrepp mot finländska objekt.

Spionage

- Kinesiska APT-grupper utnyttjar IT-leveranskedjor samt verktyg för fjärranvändning och fjärr-administration samt deras sårbarheter för att göra intrång i organisationer.
- Cyberangrepp mot Ukraina och dess leveranskedjor fortsatte aktivt. Föremålen omfattade bland annat logistik- och försvarssektorer samt statsförvaltningen.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Cybersäkerhetscentret har den 27 mars publicerat en kriskommunikationsguide riktad till organisationer. Guiden beskriver olika typer av cyberangrepp samt metoder och tillvägagångssätt som används av kriminella aktörer. Den innehåller tips för hur man kommunikationsmässigt kan förbereda sig samt hur man bör kommunicera under och efter ett cyberangrepp.

Microsoft publicerar kontinuerligt nya uppdateringar till sina molntjänster. Prenumerationers inställningar bör kontrolleras minst en gång i halvåret i Microsoft 365-prenumerationens Entra ID-inställningar (tidigare Azure Active Directory), om inte organisationens uppdateringar av Microsoft 365-prenumerationen följs kontinuerligt på något annat sätt. Cybersäkerhetscentret har publicerat en anvisning där man behandlar inställningarna för Entra ID:s katalog och användarhantering.

Cybersäkerhetscentret har uppdaterat sina tips för användning av en lösenordshanterare.

Allmän översikt över cybersäkerheten i mars

- I mars fick vi anmälningar om utnyttjande av sårbarheter i kantdatorsystem. Dessa sårbarheter är en viktig accessvektor och därför ska man hålla kantdatorsystemen uppdaterade.
  - Flera internationella informationssäkerhetsmyndigheter har varnat till exempel om sårbarheter i Fortinets brandväggsprodukter som används i stor utsträckning. Till exempel USA:s cybersäkerhetsmyndighet CISA lade till Fortinets sårbarhet CVE-2025-24472, som publicerades tidigare under detta år, i dess förteckning över utnyttjade sårbarheter. Sårbarheter har utnyttjats till exempel för att sprida utpressningsprogram. Angreppen gäller speciellt adminstrationsgränssnitt för brandväggsenheter.
  - Fortinets nätenheter har också betonats i de rapporter som Cybersäkerhetscentret har fått. Vi rekommenderar att användare av Fortinet nätenheter omedelbart kontrollerar och förhindrar att administrationsgränssnittet inte finns tillgängligt på offentliga nät och säkerställer att utrustningen är uppdaterad.
- Olika bedrägerier har fortsatt.
  - Cybersäkheretscentret har fått anmälningar om bedrägerisamtal till exempel i Cybersäkerhetscentrets namn, om nätfiske efter bankkoder i Skatteförvaltningens namn, om bedrägerimeddelanden i S-bankens namn, om bedrägeri med Neste som tema samt om nätfiske i Postens namn.
  - Facebook-användarnamn kapas också fortfarande så att man skickar meddelanden via Messenger och försöker kapa konton med hjälp av ett telefonnummer och en verifikationskod.
  - Så här identifierar du äkta webbplatser och myndigheter – undvik bedrägerier på nätet. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-yksityishenkiloille/nain-tunnistat-aidot (på finska)
- Flera M365-dataintrång som använder AiTM-tekniken har rapporterats inom flera sektorer. I många fall har angriparna försökt skicka ytterligare meddelanden från hackade konton.
  - Cybersäkerhetscentrets AiTM-anvisning finns tillgänglig här: https://https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/vid-dataintrang-i-m365-anvands-allt-oftare-natfisketekniken-aitm

Trenderna inom cybersäkerhet
de gångna 12 mån.