TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret

Maj 2024

#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 maj 2024

Dataintrång och dataläckor

- Helsingfors stads sektor Fostran och utbildning drabbades av ett omfattande dataintrång.
- Tiotusentals olovliga ansökningar gjordes i myndigheters register som resultat av ett dataintrång mot en kundorganisation.
- Enligt uppskattningen har flera hundra tusen personuppgifter hamnat i händerna på brottslingar.

Bluff och nätfiske

- Ett nytt Microsoft Planner nätfisketema har observerats vid dataintrång i M365-konton.
- Vid slutet av maj startade en omfattande bedrägerikampanj genom textmeddelanden som hotade människor med obetalda böter i Traficoms namn. Länken ledde till nätfiske efter bankkoder.

Skadeprogram och sårbarheter

- Botnätet 911 S5 omfattar flera tusen finska IP-adresser.
- Bankuppgifter stjäls med det nya skadliga Android-programmet.
- Sårbarheten i brandväggsprodukter Check Point Quantum Gateway utnyttjades.

Automation och IoT

- Politiskt motiverade hackare runt världen riktade angrepp mot industriella kontrollsystem.
- Dataintrång förekom bland annat mot dåligt skyddade programmerbara kontrollenheter för logik och industriella routrar.
- Säkerhetskontrollerna i automationssystem bör kontrolleras regelbundet.

Nätens funktion

- I april förekom det 10 störningar i allmänna kommunikationstjänster.
- Bara några överbelastningsangrepp rapporterades under månaden och deras konsekvenser förblev lindriga.

Spionage

- Polen rapporterade om en kampanj mot statsförvaltningen där skadlig e-post hade skickats till föremålen. Perpetratoren bedömdes vara APT28-gruppen som är länkad till den ryska militära underrättelseverksamheten.
- I Tyskland rapporterades för sin del att APT28 spionerade e-post för det socialdemokratiska paritet i ett intrång som började år 2022.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Förmildrande av cyberhot med begränsade resurser - en anvisning för det civila samhället har publicerats (på finska).

Traficom har utfärdat ett utkast till rekommendation till NIS-tillsynsmyndigheter om åtgärderna för hantering av cybersäkerhetsrisker. Rekommendationsutkastet ger också den grundläggande informationssäkerhetspraxisen. Cyberhygienpraxis skapar grunden för en organisations cybersäkerhet.

Ouppdaterad kantutrustning används fortfarande i stor utsträckning i dataintrång. Organisationer bör se till att dessa produkter tas i bruk med tanke på informationssäkerhet och att de är alltid uppdaterade.

Det nationella samordningscentrumet (NCC-FI) arrangerar en avgiftsfri utbildning med två delar gällande presentation och applikation av cybersäkerhetsförslag inom programmet Digitalt Europa den 18 juni och den 28 juni 2024. Anmäl dig!

Allmän översikt över cybersäkerheten i maj

- Botnätet 911 S5 som avstängdes i maj 2024 erbjöd brottslingar tillgång till komprometterade IP-adresser och till relaterade enheter ägda av privatpersoner och företag. Tusentals finska IP-adresser drabbades också.
  - Avgiftsfria, illegala VPN-tjänster hade packats i piratvideospel och program som offren laddade ner på sina enheter. När nedladdningen var färdig laddades VPN-applikationen och proxyserverns bakdörr ner på offrens enheter utan att de visste om det, och de blev en del av 911 S5-bonätet utan att de visste om det.
- Dataintrång och dataläckage som förekommit i Finland under den senaste månaden har varit exceptionellt omfattande.
- Temat i Microsoft-planerare och applikationen för uppgiftsfördelningen används i nätfiske genom att dela en PDF-fil med en länk till nätfiskesidan.
  - Cybersäkerhetscentret fick 53 anmälningar om nätfiskeförsök på Microsoft 365-e-postkonton. 25 av dem ledde till ett dataintrång av ett Microsoft 365 e-postkonto.

Trenderna inom cybersäkerhet
de senaste 12 mån.