TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret

December 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 december 2024

Dataintrång och dataläckor

- I december fick vi anmälningar om försök till dataintrång mot kantdatorsystem. Om försöken lyckas kan de resultera till exempel i att utpressningsprogrammet smittas.
- Kryptovalutakonton hackades med hjälp av nätfiskemeddelanden som utgav sig vara från olika kryptotjänster.

Bluff och nätfiske

- Bedragare fiskar efter nätbankskonder också i myndigheters namn. Reklamutrymme i sökmotorer har köpts för förfalskade sidor.
- Bedrägerier som genomförts med QR-koder beror ofta på skadliga skanningapplikationer. Det är ändå klokt att se till att man inte har petat på koden eller täckt den med ett klistermärke.

Skadeprogram och sårbarheter

- Flera anmälningar om utpressningsprogram i december.
- Enstaka rapporter om Lumma Stealer-infektioner i datorer.
- Sårbarheten (CVE-2025-0282) i Ivanti Connect Secure-produkten har redan utnyttjats. Uppdatera omedelbart.

Automation och IoT

- Det skadliga programmet IOCONTROL har observerats i flera israeliska och amerikanska automationssystem. De som skrivit det skadliga programmet antas agera för Iran.[4]
- Oskyddad positionshistorik och uppgifter om ägare av elbilar lagrade på offentliga servrar avslöjade exakta körrutter och stopplatser för privatpersoner och även till exempel för politiker och polisbilar. [5]

Nätens funktion

- Skadorna i undervattenskablar hade inte några avsevärda konsekvenser för Finlands telekommunikationsförbindelser.
- Det förekom några överbelastningsangrepp som orsakade korta avbrott i tjänsten genom ett flöde av webblanketter.

Spionage

- Cyberangrepp mot Ukraina fortsatte. I december rapporterades bland annat störningar i Befolkningsdatasystemet.
- Till exempel grupperna Turla och Sandworm, som kopplats till Ryssland, har varit aktiva i Ukraina.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Den amerikanska cybersäkerhetsmyndigheten CISA upprätthåller webbplatsen #StopRansomware. Webbplatsen innehåller utmärkt och aktuell information om utpressningsprogram.[6]

Europeiska unionens cybersäkerhetsbyrå Enisa publicerade en slutrapport om den europeiska cyberövningen. I övningen deltog cirka 5 000 personer från olika delar av Europa. Cirka 50 av dem var från Finland. Cybersäkerhetscentret ansvarade för den nationella planeringen och genomförandet av övningen. [7]

Cybersäkerhetscentret organiserade ett webbinarium om de krav som anges i cyberresiliensakten (Cyber Resilience Act, CRA) för att berätta om de produkter som omfattas av akten samt för att ge tips för att hjälpa organisationer att bereda sig för akten i förväg. En inspelning av webbinariet kommer att finnas tillgänglig för att dela informationen med dem som inte kunde delta i evenemanget. [8], [9]

Allmän översikt över cybersäkerheten i december

- Antalet anmälningar om utpressningsprogram började öka något mot slutet av 2024.
  - I alla rapporterade fall var det fråga om olika varianter av utpressningsprogram.
  - Kantdatorsystem används fortfarande för att att komma in. Sårbarheter, brister i processer och konfigurationsfel utsätter organisationer för angriparna. Regelbundna övningar hjälper organisationer att vara förberedda för olika cyberincidenter. Vi skrev om detta också i mars 2024. [10]
  - Säkerhetskopior hjälpte många organisationer att återhämta sig från ett angrepp med ett utpressningsprogram förra året.
  - Organisationer bör också betrakta utgående trafik från sina interna nät eftersom i en del av fallen kan man upptäcka och förhindra aktiveringen eller installeringen av utpressningsprogram för utgående trafik.
- Såsom i november blev telekommunikationskablar skadade i december.
  - Den 25 december fick Cybersäkerhetscentret rapporter om flera skador i el- och telekommunikationskablar i Finska viken. Cybersäkerhetscentret inledde en särskild uppföljning i anslutning till fallen.
  - Det inträffade har inte påverkat Finlands försörjningsberedskap och de flesta skadade kablar har redan åtgärdats. Finland har förberett sig väl för olika störningar i elöverföringen och telekommunikationen. De olika samhällssektorerna samarbetar intensivt när det gäller beredskap för olika störningar och myndigheter samt företag ordnar regelbundna övningar tillsammans.

Trenderna inom cybersäkerhet
de gångna 12 mån.