TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret

December 2023

#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 december 2023

Dataintrång och dataläckor

- Antalet anmälningar om dataintrång minskade till mediannivån för år 2023, men antalet anmälningar om dataintrång med allvarliga konsekvenser ökade i december.
- I flera fall hade man fått tillgång till system och konfidentiella uppgifter via hackade administratörsuppgifter.

Bluff och nätfiske

- Redan i början av december såg vi tusentals bedrägerimeddelanden i MinSkatt-tjänstens namn där man utlovade skatteåterbäringar.
- I meddelandetjänsten Whatsapp förekom det en hel del bedrägerier som gällde arbetserbjudanden.
- Signeringstjänster användes som förevändning för nätfiske.

Skadeprogram och sårbarheter

- Vi fick ett exceptionellt stort antal anmälningar om utpressningsprogrammet Akira (6 st. i december).
- En hel del sårbarheter som möjliggör fjärrkörning av godtycklig kod har åtgärdats i Atlassians produkter.
- Två utnyttjade nolldagarssårbarheter i Ivantis VPN-produkt.

Automation och IoT

- Den ukrainska säkerhetstjänsten SBU berättade att den hade hittat hackade IoT-videokameror som har använts för militär underrättelseändamål i Ukraina.

Nätens funktion

- I december förekom det inte några störningar i allmänna kommunikationstjänster.
- Olika sektorer rapporterade om överbelastningsangrepp. Största delen av dem hade inte några konsekvenser på tjänsternas funktion.
- HRT berättade offentligt om överbelastingangrepp som ägde rum på nyårsafton och som påverkade tjänster.

Spionage

- Gruppen Callisto, som i offentligheten har kopplats till Ryssland, har försökt spionera föremål i västländerna gnom att skicka riktade nätfiske-meddelanden till personers privata e-post. Detta görs för att kringgå organisationernas egna informationssäkerhetskontroller.
- Callisto är också känd bland annat under namnen Star Blizzard och Coldriver.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Multifaktorsautentisering skyddar användarnamn också i nätinfrastrukturen och kan förhindra till exempel ett brute force-angrepp. Bekanta dig med vår anvisning om multifaktorsautentisering.

Cybersäkerhetscentret har öppnat ansökan om stöd för finansiering av moderna informationssäkerhetslösningar och -innovationer. Finansieringsstöd kan sökas av mikroföretag samt av små och medelstora företag. Ansökan är öppen till 1.3.2024 kl. 16:15.

Traficom håller på att utarbeta en rekommendation om riskhanteringsåtgärderna för cybersäkerhet enligt NIS2-direktivet.

Allmän överskit över cybersäkerheten i december

- Utnyttjande av kända sårbarheter för dataintrång fortsatte, vilket återspeglades i ett ökat antal utpressningsprogram som anmälts till oss.
  - Majoriteten av anmälningarna gällde utpressningsprogrammet Akira. Det har observerats att Akira fortfarande utnyttjar Ciscos nätutrustningssårbarhet (CVE-2023-20269) som möjliggör ett *brute force*-angrepp. Det är möjligt att förebygga angreppet genom att använda flerfaktorsautentisering i Ciscos VPN-tjänst.
- I början av januari publicerade Ivanti två kritiska sårbarheter som påverkar två av dess produkter. Sårbarheterna har redan utnyttjats. Flera inhemska organisationer har skäl att omedelbart reagera på sårbarheterna.
  - På basis av Cybersäkerhetscentrets kartläggning finns det flera hundra sårbara servrar i Finland. Än så länge finns det inte några korrigerande programuppdateringar tillgängliga, men programfixar som förhindrar utnyttjandet av sårbarheterna har publicerats.
  - Även om man inför åtgärder som begränsar sårbarheternas konsekvenser är de ändå skäl att analysera systemet med tanke på ett dataintrång som eventuellt skett.
  - Enligt IT-säkerhetsbolaget Volexity har man observerat att sårbarheten utnyttjats sedan början av december 2023.

Trenderna inom cybersäkerhet
de senaste 12 mån.