TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret

Mars 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 i mars 2024

Dataintrång och dataläckor

- Som ett fenomen i denna månads dataintrång var olika slags nätfiske efter e-post och dataintrång mot organisationer.
- Vi har fortfarande fått stadigt anmälningar om skanningar mot olika slags ingångar och om försök att utnyttja sårbarheter samt försök att göra intrång.

Bluff och nätfiske

- Textmeddelandebedrägerier med fordonsskatt som tema försökte fiska efter bankkoder i Traficoms namn.
- Alla banker och dessutom Posti, MittKanta och MinSkatt har varit teman i nätfiske efter bankkoder.

Skadeprogram och sårbarheter

- Versionerna 5.6.0 och 5.6.1 i fillagringsprogrammet XZ Utils för Linux-distribution innehåller skadlig kod som tillåter olovligt tillträde till systemet via en bakdörr.

Automation och IoT

- Connectivity Standards Alliance (CSA) som ansvarar för Matter-protokollet har publicerat cybersäkerhetsmärket för IoT-produkter och avtalat om ömsesidigt erkännande med cybersäkerhetsmyndigheten i Singapore (CSA).
- Även kommunikationskommissionen i USA har publicerat ett frivilligt cybersäkerhetsmärke för IoT-produkter.

Nätens funktion

- I mars förekom det 3 störningar i allmänna kommunikationstjänster.
- Hacktivister riktade igen överbelastningsangrepp mot Finland vid slutet av mars.
- Trots observationerna har överbelastningsangreppen inte medfört några betydande konsekvenser.

Spionage

- Flera länder berättade mer om cyberspionage av APT31.
- Det berättades att aktören APT31, som är kopplad till Kina, hade utnyttjat hackade svenska routrar i angrepp mot olika länder och försökt skaffa information ur brittiska politikers e-postmeddelanden.
- Centralkriminalpolisen berättade att sambandet mellan APT31 och dataintrånget i riksdagen åren 2020–2021 har bekräftats.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Traficoms och Försörjningsberedskapscentralens utredning om AI-baserade cybersäkerhetslösningar har publicerats.

Traficom fortsätter serien av evenemang om hackning av 5G-nätens cybersäkerhet med ett nytt Hack the Networks-evenemang i maj 2024. Anmäl dig till hackathonet senast den 14 april 2024!

Översikten Informationssäkerhet 2023 bedömer att hotnivån förblir förhöjd även år 2024.

Allmän överskit över cybersäkerheten i mars

- Under mars har organisationer fortfarande drabbats av såväl överbelastningsangrepp som dataintrångsförsök. Brottslingar har intresserat sig till exempel för olika ingångar.
- Efter det att en sårbarhet i programpaketet XZ Utils offentliggjordes i månadsskiftet mars-april uppmanades användarna som första hjälpen radera den kontaminerade uppdateringen. För närvarande letar man efter eventuella utnyttjanden, publicerar uppdateringar som korrigerar sårbarheten och utreder fallet ingående.
  - Tills vidare känner man inte till några allvarliga fall av missbruk av sårbarheten.
  - Brottslingar använde flera år för att bearbeta en kritisk sårbarhet i programpaketet XZ Utils och angreppet har beskrivits som ett av de mest framgångsrika angreppen mot leveranskedjor som hittills avslöjats.
  - Läs mer om fallet med programpaketet XZ Utils i vår Veckoöversikt 14/2024.
- Som en del av Cybersäkerhetscentrets Veckoöversikt började vi publicera avsnittet Aktuella bedrägerier där vi samlar in exempel på bedrägerier på basis av de anmälningar vi fått under veckan.

Trenderna inom cybersäkerhet
de senaste 12 mån.