TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

December 2022

#cyberväder

Cyberväder berättar om betydande säkerhetsincidenter och -fenomen under månaden. Läsaren får en snabb helhetsbild av vad som hänt på cybersäkerhetsfältet under perioden i fråga. Läget kan vara:

lugnt oroande allvarligt

TRAFICOM

18.1.2023

Cybervädret december 2022

Dataintrång och dataläckor

- Övertagande av konton för sociala medier är fortfarande vardag.
- En sårbarhet i Microsoft Exchange används aktivt för att lägga in utpressningsprogram i systemen.

Bluff och nätfiske

- Användningen av .fi-domännamn är sällsynta undantag i nätfiske efter bankkoder. Majoriteten av bedrägerierna använder fortfarande internationella domäner.
- Försök till vd-bedrägerier sker ofta men de flesta försöken har till all lycka misslyckats.

Skadeprogram och sårbarheter

- Utpressningsprogram har anmälts mer än tidigare.
- I december publicerades flera sårbarhetsmeddelanden med information om flera korrigeringar till kritiska sårbarheter i olika produkter.

Automation och IoT

- Kontinuitet i funktionen och underhåll av medicintekniska implantat är etiskt viktigt. Tillverkarens konkurs kan även äventyra patienternas cybersäkerhet.

Nätens funktion

- I december förekom det två betydande störningar i allmänna kommunikationstjänster.
- Överbelastningsangrepp görs mer än tidigare.
- 25 % av alla överbelastningas-angrepp år 2022 anmäldes i december.

Spionage

- Spionagekampanjer försöker kringgå mekanismer som planerats för att varna användare.
- Intrångsrutter som APT-aktörer använder omfattar sårbarheter i VPN-lösningar och i andra produkter för nättrafik.

TRAFICOM

18.1.2023

Top 5 cyberhot i den närmaste framtiden (6 månader - 2 år)

1

De ekonomiska och politiska fenomenen reflekteras även i cybersäkerheten.

Digitaliseringen är en övergripande fråga i hela organisationen och ändringarna i det internationella säkerhetsläget påverkar avsevärt organisationens kontinuitet och riskhantering.

2

Det anses att nivån för cyberhot har ökat i Finland.

På grund av ökad skadlig trafik och förhöjd hotnivå blir organisationernas beredskap allt viktigare.

3

Brister i vanliga avvärjningsåtgärder orsakar fortfarande majoriteten av informationssäkerhetsincidenterna.

Till exempel hantering av åtkomsträttigheter, upprätthållande av programvara och god informationssäkerhetskultur utgör grundvalen för cybersäkerheten.

Symboler

Ny

Uppdaterad

4

Bristfälligt informationsutbyte försvagar den heltäckande lägesbilden av cybersäkerheten.

Cyberhotet som en organisation möter kan följande dag drabba andra organisationen. Effektivt informationsutbyte förbättrar cybersäkerheten för alla.

5

Cybersäkerhet är beroende av experter och cybersäkerhetskunskaperna hör till alla!

Det finns ett allt större behov av allt mångsidigare cybersäkerhetsexperter och den nya regleringen och cybersäkerhetens inkludering som en del av förtagens dagliga rutiner ökar behovet ytterligare.

TRAFICOM

18.1.2023