TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

Mars 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

21.4.2022

Cybervädret mars 2022

Dataintrång och dataläckor

- Många privatpersoners konton på sociala medier har blivit utsatta för dataintrång och intrångsförsök.

Bluff och nätfiske

- Bedrägerimeddelanden skickades i polisens namn i Finland och andra europeiska länder.
- Alla organisationer från hobbyklubbar till börsbolag är igen utsatta för VD-bedrägerier.

Skadeprogram och sårbarheter

- Flera anmälningar om meddelanden med en länk till fildelningstjänsten OneDrive.
- Flera anmälningar om försök att sprida det skadliga programmet Emotet via e-post i Finland.

Automation och IoT

- Lägesrapporter om industriautomation visar att cybersäkerhetskapaciteten har ökat.

Nätens funktion

- Sju betydande funktionsstörningar.
- Störningar orsakades av elavbrott, ändringsarbeten och fel i utrustningar.
- Antalet rapporter om överbelastningsangrepp i olika sektorer var större än tidigare.

Spionage

- Cyberattacker och försök till attacker genomfört av aktörer som tros ha anknytning till Ryssland observeras i Ukraina samt västländerna.
- FBI hindrade användningen av ett botnät för illvillig verksamhet. Botnätet består av infekterade routrar och tros vara kontrollerad av APT-gruppen Sandworm.

TRAFICOM

21.4.2022

Top 5 cyberhot - betydliga fenomen över en längre period

1

De ekonomiska och politiska fenomenen reflekteras även i cybersäkerheten.

Fenomenen kan ses snabbt i den digitala miljön och de kan medföra svårförutsebara händelser i cybersäkerheten.

2

Ledning och riskhantering.

De snabba förändringarna i verksamhetsmiljön testar organisationernas riskhantering i cybersäkerheten. Det ankommer på ledningen att säkerställa riskhanteringens inverkan.

3

Ouppdaterade sårbarheter öppnar en rutt till organisationen för de kriminella.

De kriminella utnyttjar sårbarheterna snabbt. Man lämnar enheter öppna mot internet utan att ha beaktat deras informationssäkerhet och även skyddsåtgärderna och underhåll är bristfälliga.

Symboler

Ny

Uppdaterad

4

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.

5

Åtkomsträttigheter är nycklar till en organisation.

Kontroll av åtkomsträttigheter är mycket viktigt i en organisation. Koder kan stjälas med hjälp av olika angrepp, och detta kan ha en betydande inverkan på organisationens verksamhet om koderna hamnar i orätta händer.

TRAFICOM

21.4.2022