Mars | 2019

#CYBERVÄDER

#cybervädер 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

Cybervädret mars 2019

Nätens funktion

- Det förekom färre driftstörningar än i januari och februari.
- I flera europeiska länder har man observerat överbelastningsangrepp som försökte störa valen.
- Här i Finland var läget med överbelastningsangrepp lugnt.

Dataintrång & dataläckage

- Dataintrång mot Norsk Hydro medförde betydande ekonomiska förluster.
- Användaruppgifter (t.ex. till Office 365) som nätfiskare kommit över används ofta snabbt vid dataintrång.

Skadeprogram & sårbarheter

- En hel del uppdateringar för kritiska sårbarheter publicerades.
- Ransomware-aktiviteten utvecklas.

Spionage

- Även apparattillverkare utnyttjas vid angrepp mot leveranskedjor.
- År 2018 fick Skyddspolisen veta om flera nätspionagefall bakom vilka det antagligen funnits en statlig instans.

Bluff och nätfiske

- Allt mer trovärdiga portaler har skräddarsytts för nätfiske.
- VD-bedrägerier ökar igen genom knäckta Office 365-e-postkonton.

IoT och automation

- 20 % av IKT-apparaternas sårbarheter är kritiska.
- Sårbarheter i Fidelix byggnadsautomationssystem; temat behandlades i YLEs program Docstop: Team Whack.
- I Finland finns en hel del IoT-apparater som är kopplade mot det offentliga internet.