TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

April 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

19.5.2022

Cybervädret april 2022

Dataintrång och dataläckor

- Brottslingar har gjort intrång i kommuners och städers e-postkonton och från dessa konton har det skickats en hel del nätfiskemeddelanden.
- Kontona för sociala medier är fortfarande utsatta för dataintrång och intrångsförsök.

Bluff och nätfiske

- I Fenton-bedrägerierna skickades flera tusen falska arbetserbjudanden och användarna lockades till ett pyramidspel.
- I Wallpaperga-meddelanden luras offret att klicka på en länk där man annullerar en avgiftsbelagd beställning.

Skadeprogram och sårbarheter

- Cybersäkerhetscentret har igen fått några observationer om det skadliga programmet Emotet.
- Det skadliga programmet FluBot som sprids via textmeddelanden i mobiler har igen blivit aktivt i Finland.

Automation och IoT

- Det finns flera tecken på att cyberangrepp mot automationssystem kommer att öka.
- Tillverkaren av smarta belysningssystem gick i konkurs - användarna kan inte längre reglera sin belysning.

Nätens funktion

- Åtta betydande fel.
- Näten fungerar fortfarande normalt och läget är bra.
- Överbelastingsangrepp mot statsförvaltningen väckte diskussion.

Spionage

- Antalet cyberangrepp i Ukraina har ökat flerfaldigt under kriget. Angreppen har även gällt industriautomation.
- Flera APT-grupper har fortsatt att spionera på västländer i april. I spionaget utnyttjar grupperna bland annat kriget i Ukraina.

TRAFICOM

19.5.2022

Top 5 cyberhot - betydliga fenomen över en längre period

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

Bristfälligt informationsutbyte försvagar den heltäckande lägesbilden av cybersäkerheten.

Cyberhotet som en organisation möter kan följande dag drabba andra organisationen.

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

19.5.2022