



**TRAFICOM**

Transport- och kommunikationsverket  
Cybersäkerhetscentret

# Cyberväder

Juli 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

# Cybervädret juli 2022



## Dataintrång och dataläckor

- ▶ Sårbara eller ouppdaterade webbservrar hackas ständigt.
- ▶ Finska Notisbyrå STT och Wärtsilä drabbades av ett dataintrång och ett utpressningsprogram till följd av dataintrånget.



## Bluff och nätfiske

- ▶ Namnen på och logotyperna för polisen har använts i bedrägerimeddelanden i vilka man hotar med rättshandlingar och kräver lösensumma.
- ▶ Nätfiske efter bankkoder sker med många olika slags bedrägerimeddelanden både via textmeddelanden och via e-post.



## Skadeprogram och sårbarheter

- ▶ I juli gjorde man inte många anmälningar om infektioner av skadliga program.
- ▶ Sambas allvarliga och Vmwares kritiska sårbarhet kräver en snabb uppdatering.



## Automation och IoT

- ▶ Cyberbrottslingar försöker hitta nya och kreativa sätt att komma åt isolerade automationssystem.
- ▶ Ett hackprogram för att knäcka lösenord kan innehålla en trojan!



## Nätens funktion

- ▶ Ett fel i klass A (störning som påverkar över 300 000 användare) på kanalen Yle TV1 under en vardagskväll.
- ▶ Bara två betydande störningar i kommunikationsnäten.
- ▶ För överbelastningsangrepp var läget lugnt i Finland.



## Spionage

- ▶ En aktör associerad med den iranska förvaltningen förstörde informationssystem för den albanska statsförvaltningen.
- ▶ Angripare associerade med den nordkoreanska förvaltningen är aktiva.
- ▶ En aktör associerad med Rysslands underrättelsetjänster fortsätter sina intrångsförsök.

# 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 företagens 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.