



TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

Augusti 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 augusti 2022



Dataintrång och dataläckor

- ▶ Vi har fått flera anmälningar om inloggningsförsök i finska organisationers informationssystem.
- ▶ Små företags domännamn och användarkonton på sociala medier har kapats.



Bluff och nätfiske

- ▶ Nätfiske efter nätbankskoder har huvudsakligen gällt textmeddelanden medan abonnemangsfällor har bytts ut från textmeddelanden till e-post.
- ▶ Traficoms föreskrift 28 om att förhindra förfalskning av uppringarens nummer har medfört att antalet förfalskade samtal från tekniskt stöd har minskat.



Skadeprogram och sårbarheter

- ▶ Observationer av utpressningsprogram har rapporterats av finska organisationer eller organisationer med verksamhet i Finland.
- ▶ Det är fortfarande viktigt att installera uppdateringar. Sårbarheter utnyttjas snabbt efter att de läckt ut.



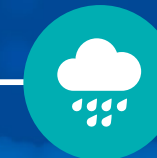
Automation och IoT

- ▶ Seminariet om cybersäkerhetsmärket den 29 september kommer att behandla framtida obligatoriska informationssäkerhetskrav för IoT-produkter inom EU.
- ▶ Forskarna hittade sårbarheter i nästan alla undersökta IoT-gränssnitt i 4G- och 5G-nät.



Nätens funktion

- ▶ Tre betydande funktionsstörningar i masskommunikationstjänster.
- ▶ Överbelastningsangrepp ökade i augusti.
- ▶ Antalet överbelastningsangrepp som rapporterats till Cybersäkerhetscentret fördubblades jämfört med sommarmånader.



Spionage

- ▶ Skadliga program som förstör data har upptäckts i åtminstone 25 länder under det första halvåret.
- ▶ APT-aktörer är fortfarande mycket intresserade av organisationers molntjänster och inloggningsuppgifter.

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 företagens dagliga rutiner ökar behovet ytterligare.