



**TRAFICOM**

Transport- och kommunikationsverket  
Cybersäkerhetscentret

# Cyberväder

December 2021

# #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 december 2021



## Dataintrång och dataläckor

- ▶ Flera anmälningar om övertagande eller försök till övertagande av konton för sociala medier.
- ▶ Flerfaktorsautentisering bör i mån av möjlighet införas i alla tjänster för sociala medier.



## Bluff och nätfiske

- ▶ Försäljningsspalter lockar bedragare.
- ▶ Poppuppeddelanden pressar användare till nya typer av abonnemangsfällor.
- ▶ Antalet olika telefonbedrägerier har ökat.



## Skadeprogram och sårbarheter

- ▶ Kritisk Log4shell-sårbarhet i Apache Log4j-komponenten.
- ▶ Flera miljoner textmeddelanden har filterats i Finland i anslutning till FluBot-kampanjen.



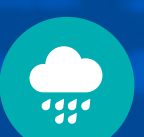
## IoT och automation

- ▶ I Storbritannien finns ett lagförslag om smarta apparater som skulle tvinga att radera enkla lösenord och att anmäla om tillgängliga säkerhetsuppdateringar efter försäljningen.
- ▶ Forskarna har använt cyberfällor för att utreda motivationen att göra angrepp i IoT-apparater.



## Nätens funktion

- ▶ I november förekom det 4 betydande störningar i allmänna kommunikationstjänster.
- ▶ Det förekom störningar i AWS-tjänster.
- ▶ Överbelastningsangrepp påverkade bl.a. ICT-tjänsteleverantörer.



## Spionage

- ▶ Microsoft tog över webbsidor som NICKEL-aktören använde och minskade då 29 spionoperationer mot landet.
- ▶ Spionage på mobilapparater väckte rubriker igen.
- ▶ APT31 har utnyttjat hackade småroutrar för routning av skadlig trafik.

# Top 5 cyberhot - betydliga fenomen över en längre period

1 

**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.

2 

**Användarkoder är värdefull information i organisationer.** Kontroll över användarkoder är viktigt i alla organisationer. Koder kan stjälas med hjälp av olika angrepp, och detta kan ha en betydande inverkan på organisationens verksamhet.

3

**Det blir allt vanligare att använda olika cyberangreppsmetoder för utpressning och de hotar affärsverksamhetens kontinuitet.** I Finland kommer man att se allt fler nätangrepp där tiotusentals euro är småpengar.

4

**Molntjänster är nya för många organisationer, och angripare är ofta bästa experter på informationssäkerhet i molnet.** Organisationer har snabbt övergått till molntjänster men de förstår ofta inte sin egen miljö och dess förmågor tillräckligt bra.

5

**Informationssäkerheten i leverans- och servicekedjor blir allt mer kritisk.** För att garantera cybersäkerhet ska organisationerna förstå sina egna leveranskedjor.

Symboler

Nytt



Uppdaterat

