



**TRAFICOM**

Transport- och kommunikationsverket  
Cybersäkerhetscentret

# Cyberväder

Oktober 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 oktober 2021



## Dataintrång och dataläckor

- ▶ Twitch upplevde ett dataintrång där kritiska data om tjänsten läcktes ut.
- ▶ Det gjordes ett dataintrång mot ett statligt informationssystem i Argentina och personliga uppgifter om tiotusentals miljoner medborgare hamnade i kriminella händer.



## Bluff och nätfiske

- ▶ Kampanjer för att stjäla bankkoder var mycket aktiva i oktober.
- ▶ Förutom e-postbedrägerier lurar man människor också med falska textmeddelanden.



## Skadeprogram och sårbarheter

- ▶ Det skadliga programmet QakBot sprids aktivt.
- ▶ Informationssäkerhet Nu!-artikel: Beroendekonflikter (dependency confusion) exponerar företag för angrepp.



## IoT och automation

- ▶ Strategier och anvisningar för cybersäkerheten i IoT och automation blir allt vanligare och berättar om ökande medvetenhet om ämnesområdets viktighet.



## Nätens funktion

- ▶ 10 betydande störningar
- ▶ En del av störningarna berodde på olika ändringsarbeten eller konfigurationsfel.
- ▶ Kommunsektorn rapporterade om överbelastningsangrepp mot skolors adresser. Angreppen har även haft en indirekt inverkan på andra tjänster.



## Spionage

- ▶ Cyberspioner är intresserade av teleoperatörer: Gruppen LightBasin har gjort intrång i flera teleoperatörers system runtom i världen.
- ▶ NOBELIUM utnyttjade IT-tjänsteleverantörers underhållskoder för att göra intrång i deras kundorganisationer.

# 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

