TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

April 2021

#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
Transport- och kommunikationsverket
Cybersäkerhetscentret

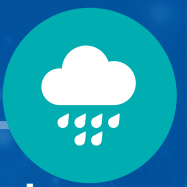
Cybervädret april 2021

Dataintrång och dataläckor

- Vi får fortfarande anmälningar om Office 365-dataintrång men antalet anmälningar har minskat år 2021.

Bluff och nätfiske

- Textmeddelandebedrägerier blir allt vanligare. Textmeddelanden används för att fiska efter bankkoder, att locka in konsumenter i abonnemangsfällor och att sprida skadliga program.
- Porrutpressningskampanjerna var mindre aktiva i april men fortsätter igen.



Skadeprogram och sårbarheter

- En uppdatering till sårbarheten i VPN Pulse Connect Secure har publicerats och ska installeras utan dröjsmål.
- Skadeprogram FluBot och FakeCop/FakeSpy sprids via textmeddelanden.

Automation

- Sårbarheterna BadAllock och NAME:WRECK påverkar hundratals miljoner inbyggda system.
- Elbilar och laddningsställen blir allt vanligare. Man talar dock inte mycket om laddningsställenas cybersäkerhet.

Nätens funktion

- Det förekom bara två betydande störningar i nätens funktion i Finland i april.
- Det förekom två större störningar i Microsofts molntjänster.
- Ungefär hälften av anmälningarna om överbelastningsangrepp gällde skolar eller undervisningsplattformar.

Spionage

- Den allvarliga sårbarheten i Pulse Connect Secure har eventuellt använts för statligt spionage.
- USA och Storbritannien anklagar den utländska underrättelsetjänsten i Ryssland för att ha hackat uppdateringskedjan för plattformen Solar Winds Orion.

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

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

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.

3

Nätfiske
är mycket vanligt, och det kan vara svårt för mottagare av ett nätfiskemeddelande att observera bedrägeri. Detta utnyttjas även för riktade angrepp och spionage.

ökat

minskat

oförändrat

Gult = nytt/ uppdaterat*

4

Svag hantering av cyberrisker och oklar ansvarsfördelning för hantering av tjänster. Det är svårt att förutspå konsekvenserna för cyberhot, och oklarheter vid ansvarsfördelningen för hantering av tjänster försämrar informationssäkerheten.

5

Bristfällig logginformation utgör en risk i många organisationer. På grund av bristfällig insamling, uppföljning och förvaring av logginformation kan man inte observera eller utreda it-incidenter.

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret