TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

Oktober 2020

#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:

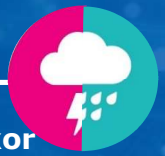
lugnt

oroande

allvarligt

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret oktober 2020



Dataintrång och dataläckor

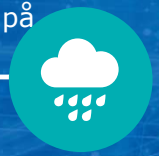
- Det kommer fortfarande in anmälningar om Office 365-intrång
- Psykoterapicentret Vastaamo och dess kunder var föremål för utpressning med hot om dataläckage. Både patient- och personuppgifter läckte ut.
- Närmare anvisningar finns på https://tietovuotoapu.fi.

Bluff och nätfiske

- Man har fiskat efter Office 365-koder med mycket trovärdiga Zoom-inbjudanden.
- COVID19-temat har blivit aktuellt igen i samband med porrbedrägerier, donationsbedrägerier, nigeriabrev och många andra nätfiskekampanjer.

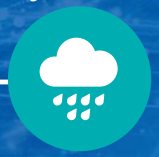
Skadeprogram och sårbarhe

- Utpressningsprogram har riktats på hälsovårdssektorn
- Ett skadeprogram för Android sprids i Postis namn.



Automation och IoT

- Enligt Nokias hotrapport gällde en tredjedel av alla observationer av skadliga program IoT-apparater.
- Andelen ökade med 17 procentenheter från i fjol, vilket berättar om IoT-apparaternas svaga informationssäkerhetsnivå och att antalet sådana apparater ökar.



Nätens funktion

- Endast tre betydande störningar i inhemska kommunikationstjänster
- Globala störningar i Microsofts och Slacks tjänster
- Cybersäkerhetscentret fick anmälningar om överbelastningsangrepp som också hade omfattande konsekvenser på tjänsternas funktion.

Spionage

- Norge anklagar Ryssland för ett cyberangrepp mot Norges parlament tidigare under denna höst.
- Enligt Skyddspolisen har coronaviruspandemin ökat cyberspionage i förhållande till övrigt spionage. Skyddspolisen anser att i synnerhet Ryssland och Kina är intresserade av Finland.

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Top 5 cyberhot - betydliga fenomen över en längre period

1 ↑

Det blir allt vanligare att använda olika cyberangreppsmetoder för utpressning och de hotar affärsverksamhetens kontinuitet. Skadorna för enskilda fall har gått upp till tiotals miljoner euro.

2 →

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.

3 →

Sårbarheter utnyttjas snabbt, vilket förutsätter snabba uppdateringar. Man lämnar enheter öppna mot internet utan att ha beaktat deras informationssäkerhet och även skyddsåtgärderna och underhåll är bristfälliga.

↑ *ökat*
↓ *minskat*
→ *oförändrat*

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