TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

Juli 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 juli 2020

Dataintrång och dataläckor

- Observationer om knäckta finska PulseSecure- och Netscaler-servrar och sårbara BIG-IP-servrar.
- Office 365-dataintrång har börjat öka igen efter den lugnare sommarperioden.

Bluff och nätfiske

- Nätfiske är ett verktyg som professionella brottslingar använder aktivt. Verktygets betydelse vid nätbedrägerier har ökat.
- Bedrägerisamtal är tillbaka efter en karantänpaus. Det kommer flera hundra tusen bedrägerisamtal till Finland.

Skadeprogram och sårbarheter

- Ransomwareaktörer auktionerar ut stulna data med tanke på att tjäna pengar med uppgifterna.
- I juli publicerades kritiska sårbarheter och sårbarheter avsedda för att äventyra nätverksutrustning utnyttjades aktivt.

Automation

- Amerikanska myndigheter varnade om ett ökat cyberhot mot automationssystem.
- Sårbarheter mot automationssystem hittas allt oftare.

Nätens funktion

- Endast tre betydande störningar i allmänna kommunikationstjänster.
- DigiCert ogiltigförklarade flera certifikat den 11 juli, vilket påverkade även flera finländska tjänsters funktion.
- För överbelastningsangrepp var det lugnt i Finland i juli.

Spionage

- EU har vidtagit de första aktiva motåtgärderna mot statliga cyberangrepp genom att införa sanktioner.
- Syftet med de riktade angreppen är inte bara spionage utan också påverkan och finansiering av ett kärnvapenprogram.

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Top 5 cyberhot - betydliga fenomen över en längre period

1

Omfattande utpressningsangrepp 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 Ny

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 Ny

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