TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

Februari 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 februari 2021

Dataintrång och dataläckor

- Den franska informationssäkerhetsmyndigheten ANSSI publicerade en rapport om dataintrång i Centreonprogram
- Vi publicerade två artiklar om att förhindra och identifiera lateralt intrång

Bluff och nätfiske

- Bluffmeddelanden med OmaPosti som tema pinade finländarna dagligen.
- Bluffmeddelanden om skatteåterbäring användes för nätfiske efter oskyldiga skattebetalares kreditkortsuppgifter.

Skadeprogram och sårbarheter

- Röd varning 1/21: om sårbarheter i Exchangeservrar
- Om försök att sprida ett skadligt program via skräppost i BazarStrike-kampanjen

Automation och IoT

- Dragos publicerade en årsrapport om informationssäkerheten i industriautomation
- Det observerades att användbarhet var prioriterad på bekostnad av informationssäkerhet i automations- och IoT-tjänster som hanteras på distans

Nätens funktion

- Fem betydande störningar i allmänna kommunikationstjänster. Konsekvenserna var ganska små.
- Inhemsk teleoperatör drabbades av ett massivt överbelastningsangrepp. Angreppet betydde att kundernas internettrafik var betydlig långsammare under ungefär en timme.

Spionage

- Microsoft anser att APT-gruppen Hafnium, som är länkad till Kina, använde nolldagarssårbarheter i Microsofts Exchangeservrar för att stjäla information.
- Utländska underrättelsetjänster har använt finländska företags och privatpersoners routrar för cyberspionage.

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Top 5 cyberhot - betydliga fenomen över en längre period

1

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.

2

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.

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