TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

Augusti 2020

#cyberväder berättar om betydande säkerhetsincidenter och -fenomen under månaden. Denna produkt är i första hand avsedd för personer som svarar för informationssäkerheten. 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 augusti 2020

Dataintrång och dataläckor

- Norska stortinget utsatt för dataintrång.
- Data från över 900 hackade Pulse Secure VPN-servrar har läckt ut till internet.
- Antalet Office 365-dataintrång ökar till följd av lyckat nätfiske.

Bluff och nätfiske

- Bedragarnas hänsynslös vet inga gränser: ”Tjänsten att returnera pengar som förlorats genom bedrägeri” bluffar redan drabbade offer igen.
- Nätfiske är ett verktyg som professionella brottslingar använder aktivt.

Skadeprogram och sårbarheter

- EMOTET sprider sig i Finland och i andra länder, och vi publicerade en gul varning om det.
- Flera kritiska sårbarheter, snabb uppdatering rekommenderas.

Automation

- Informationssäkerhetsforskare hittade flera hundra tusen sårbara skrivare på nätet.
- Den första officiella standarden om IoT-säkerhet i konsumentapparater publicerades.

Nätens funktion

- Endast fyra betydande störningar i allmänna kommunikationstjänster.
- Störning i CenturyLink den 30 augusti hade globala effekter.
- Internet censurerat i Vitryssland.
- Lugnt med tanke på överbelastningsangrepp i Finland men hot om angrepp ökar.

Spionage

- Riktade angrepp som görs på uppdrag kan i synnerhet hota information som är kritisk för affärsverksamheten, men beställda angrepp är möjliga även mot statsförvaltningen och diplomatkårer.
- För ett statligt cyberangrepp kan motivet också vara att tjäna pengar.

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

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