TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

September 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 september 2020

Dataintrång och dataläckor

- Vi har fått fler anmälningar än vanligt om hackade inhemska webbplatser.
- I andra länder har man gjort många observationer om utpressningsprogram mot hälsoaktörer.
- Office 365-dataintrång fortsätter.

Bluff och nätfiske

- Flera tusen sms har skickats i Postis namn. Dessa sms leder till en abonnemangsfälla, nätfiske och ett skadlig program.
- Bakom den avslöjade nätfiskesidan hittades uppgifter om flera tiotals offer. Uppgifterna bidrog till att dessa dataintrång kunde avbrytas.

Skadeprogram och sårbarheter

- Emotet sprider sig aktivt via e-postbilagor också i Finland.
- Sårbarheten Zerologon utnyttjas aktivt. Se till att alla styrservrar är uppdaterade.

Automation

- I Microsofts undersökning observerades sårbarheter i 71 % av de undersökta näten för automationssystem.
- Kasperskys statistik för första halvåret 2020 visar att antalet angrepp mot automationssystem var lägst i Nordeuropa.

Nätens funktion

- Nio betydande störningar i nätens funktion; tre av dem berodde på stormen Aila. Orsaken till de övriga störningarna var oftast ett fel i elmatningen eller i underhållsarbeten.
- Ganska lugnt med tanke på överbelastningsangrepp i Finland men hot om angrepp ökar.

Spionage

- Microsoft berättade om APT28-gruppens kampanj vars syfte är att samla in lösenord från ett flertal organisationers anställda.
- Olika avgiftsfria tjänster eller tjänster med försöksperiod kan utnyttjas som kommandokanaler för att dölja skadlig trafik.

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