TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

Juni 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 juni 2020

Dataintrång och dataläckor

- Omfattande dataintrångkampanjer riktades mot e-post också i Finland.
- Företagens stamkundssystem blev utsatta för dataintrång och försök till dataintrång.

Bedrägerier och nätfiske

- Man ringer i namn av tekniskt stöd aktivt igen.
- VD-bedrägerier och andra faktureringsbedrägerier ökar igen under semesterperioden.

Skadliga program och sårbarheter

- Många kritiska sårbarheter som inverkar på bl.a. VPN-lösningar av Palo Alto Networks och F5 och Citrix-produkter Application Delivery Controller (ADC), Citrix Gateway och Citrix SD-WAN WANOP.

Automation

- EKANS-attacker med skadliga program riktades mot Honda och ENEL Group.
- I juni publicerades ett par viktiga undersökningar om automation och IoT.

Nätverkens funktion

- 12 betydande störningar, därav 3 förorsakades av stormen Päivö.
- Minskningen av antalet betydande störningar som pågått i flera år verkar ha stannat av och antalet har stigit något.
- För överbelastningsangrepp var det lugnt i Finland i juni.

Spionage

- Sociala medietjänster kan också utnyttjas i förmedlingen av skadliga meddelanden och bilagor.
- Organisationens system som hänför sig till genomförandet av nätet och organisationens säkra förbindelser är intressanta mål för intrång av angriparen som är ute efter information eller försöker få fotfäste.

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Top 5 cyberhot - betydande långsiktiga fenomen

1 →

Nätfiske
är väldigt vanligt och mottagaren kan ha svårt att upptäcka att det är fråga om ett bedrägeri. Detta utnyttjas också i riktade attacker och spionage.

2 ↑

Utnyttjandet av sårbarheter blir snabbare,
vilket kräver snabba uppdateringar. Apparater och tjänster vars datasäkerhet inte har beaktats lämnas öppna på nätet och skyddsåtgärderna samt underhållet är bristfälliga.

3 ↓

Utpressningsangrepp med omfattande konsekvenser
hotar affärsverksamhetens kontinuitet. Skadorna i enskilda fall har ökat till tiotals miljoner euro.

↑ *ökat*
↓ *minskat*
→ *oförändrat*

4 →

En otydlig ansvarsfördelning
mellan tjänsteleverantören, underleverantörerna och beställaren försämrar hanteringen av datasäkerheten. Brister i kontrollen av loggar gör det svårare att upptäcka hot.

5 →

Organisationer kan inte hantera sina cyberrisker.
Man kan inte förutse hur hoten påverkar verksamheten och därför underskattas riskerna. Det finns brister i återhämtningsplanerna.

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret