TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

Maj 2020

#cyberväder berättar om betydande säkerhetsincidenter och -fenomen under månaden. Den här produkten är primärt avsedd för informationssäkerhetsansvariga. Läsaren får en snabb helhetsbild av vad som hänt på cybersäkerhetsfältet under perioden i fråga. Läget kan vara:

lugnt oroande allvarligt

Cybervädret maj 2020

Dataintrång och dataläckor

- Office 365–dataintrång på samma nivå som vid början av året.
- Aktörerna inom kommunsektorn blev utsatta för ett dataintrång och ett intrångsförsök.
- I utlandet har flera högpresenterande datorsystem blivit utsatta för dataintrång.

Bedrägerier och nätfiske

- Textmeddelandebedrägerier i Postis namn innehåller ett skadligt program som infekterar mobila enheter.
- VD-bedrägerier och andra faktureringsbedrägerier ökar igen inför semesterperioden.

Skadliga program och sårbarheter

- Utpressningsaktörer auktionerar ut stulna data med tanke på att tjäna pengar med uppgifterna.

Automation

- Ett finländskt kritiskt infrastruktursystem drabbades av ett utpressningsangrepp.
- Automationssystem har också återkommande varit utsatta för angrepp i samband med konflikter mellan staterna.

Nätverkens funktion

- Bara tre betydande störningar
- Avbruten fiber i Böle medförde en omfattande störning i tågtrafiken den 7 maj.
- För överbelastningsangrepp var det lugnt i maj.

Spionage

- Det varnas om att gruppen Sandworm har försökt göra intrång i sårbara Exim e-postservrar sedan augusti 2019, och eventuellt tidigare.
- System för kritisk infrastruktur är lockande mål för intrång av APT-grupper.

Top 5 cyberhot - betydande långsiktiga fenomen

1

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.

2

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.

3

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

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.