TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

April 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 april 2020

Dataintrång och dataläckor

- Office 365–dataintrång har ökat till samma nivå som vid början av året.
- O365-koder som erhållits genom nätfiske används även för andra dataintrång.

Bedrägerier och nätfiske

- Vid avancerade bedrägerier används offrets verkliga personuppgifter, kontouppgifter, e-post och textmeddelanden.
- Det kapade kontot används tillsammans med återställningsfunktionen för lösenord för att stjäla lösenord i flera tjänster.

Skadliga program och sårbarheter

- Under april har det förekommit en hel del kritiska sårbarheter, nya metoder för utnyttjande och tjänster utsatta för angrepp.
- Försumma inte kritiska uppdateringar, speciellt om tjänsten är öppen mot internet.

Automation

- Cybersäkerhetscentret har börjat sin årliga utredning av oskyddade automationsenheter i finländska datanät.
- Ouppdaterade enheter, t.ex. industriautomationsenheter eller medicinska enheter har blivit infekterade av kända skadliga program.

Nätverkens funktion

- Det förekom osedvanligt mycket störningar i nätens funktion och de hade omfattande verkningar.
- En störning i Telias internetförbindelser 25.4 hade en inverkan på många av samhällets verksamheter.
- För överbelastningsangrepp var det lugnt i april.

Spionage

- Teman som hänför sig till coronaviruset, t.ex. vaccinforskning och övrig forskning, kan vara utsatta för spionage.
- Statligt beslutsfattande och beredning av det är traditionella mål som blivit aktuella också under epidemin.

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.