TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

Juni 2021

#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

Cyberväder juni 2021

Dataintrång och dataläckor

- Dataläckor kan även inträffa oavsiktligt eller utan att någon utomstående aktör orsakar dem.
- Det är viktigt att vara noggrann med säkerhetskopior, duplicering av data spelar en nyckelroll.

Bluff och nätfiske

- Aktivt nätfiske igen i bankernas namn. Ekonomiska förluster till följd av nätbedrägerier har enligt polisen uppgått till miljoner euro i år.
- FluBot-kampanjen var mycket aktiv i juni.

Skadeprogram och sårbarheter

- Det norska företaget Axiell AS har blivit offer för ett utpressningsprogram.
- Kaseya-distributionskedjeattacken påverkade hundratals organisationer.
- Skadeprogram som sprids med hjälp av länkar i textmeddelanden har varit mycket aktiva.

Automation och IoT

- Det har upptäckts en kritisk sårbarhet i IP-kamerorna tillverkade av Bosch. En uppdatering finns tillgänglig.
- Flera aktörer har publicerat instruktioner som syftar till att hjälpa organisationer att förbereda sig på cyberhot på ett mer systematiskt sätt.

Nätens funktion

- 14 betydande funktionsstörningar i allmänna kommunikationstjänster i juni.
- Stormar och serviceavbrott ökade antalet funktionsstörningar jämfört med de föregående månaderna (2 stycken i april och 3 stycken i maj).
- Utpressningsmeddelanden med överbelastningsangrepp som tema.

Spionage

- De västerländska informationssäkerhetsmyndigheterna meddelade att den omfattande bruteforce-kampanjen hade anknytning till Rysslands militära underrättelseverksamhet.
- Nyheterna om cyberspionage handlade ofta om länderna i Asien.

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Top 5 cyberhot - betydliga fenomen över en längre period

1

Ouppdaterade sårbarheter öppnar en rutt till organisationen för de kriminella. De kriminella utnyttjar sårbarheterna snabbt. Man lämnar enheter och tjänster öppna mot internet utan att ha beaktat deras informationssäkerhet och även skyddsåtgärderna och underhåll är bristfälliga.

2

Det blir allt vanligare att använda olika cyberangreppsmetoder för utpressning och de hotar affärsverksamhetens kontinuitet. I Finland kommer man att se allt fler nätangrepp där tiotusentals euro är småpengar.

3

Molntjänster är nytt för organisationer och det är angriparna som har bästa förståelse av informationssäkerheten hos molntjänster. Organisationer har övergått till molntjänster i rask takt men saknar tillräcklig förståelse av den egna miljön och dess förmågor.

Symbolerna

Ny

Uppdaterad

4

Informationssäkerheten hos distributions- och servicekedjor är alltmer kritisk. Att förstå underleveranskedjorna är centralt för organisationens egen cybersäkerhet.

5

Distansarbete är här för att stanna – och så är också riskerna. Enheternas distansuppkopplingstjänster som är öppna mot internet utsätter organisationer för dataintrång. Det lönar sig att administratörerna kontrollerar skyddet på distansarbetarnas enheter samt att brandväggsinställningarna är ändamålsenliga.

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret