TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

Maj 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 maj 2021

Dataintrång och dataläckor

- Antalet rapporterade Office 365-dataintrång började öka igen vid början av sommaren.
- Flera betydande dataintrång som innebär utpressningsprogram har rapporterats utomlands.

Bluff och nätfiske

- SMS-bedrägerier infekterade mobiltelefoner i Finland.
- Det skadliga programmet FluBot, som spridits aggressivt, stjäl även bankuppgifter.
- Utpressningsmeddelanden på finska blev mer aktiva igen mot slutet av månaden.

Skadeprogram och sårbarheter

- Skadliga program mot mobilapparater har varit aktiva.
- Vi publicerade en gul varning om Flubot den 4 juni.
- Microsofts månatliga uppdateringar omfattade korrigeringar för 55 sårbarheter, av vilka 4 var kritiska

Automation och IoT

- Utpressningsprogrammet i Colonial Pipelines kontorsnät påverkade även produktionssystem.
- En inspelning av Traficoms webbseminarium om informationssäkerhetskrav för IoT-apparater finns nu tillgänglig.

Nätens funktion

- I maj förekom det bara tre betydande störningar i nätens funktion i Finland.
- Avbrott i användningen av Salesforce-tjänsterna berodde på ett mänskligt misstag.
- Antalet överbelastningsangrepp som rapporterades till oss minskade i maj men angreppen var bland de största någonsin.

Spionage

- APT29-gruppen har skickat riktade skadliga e-postmeddelanden till en stor grupp av mottagare.
- Den amerikanska NSA anklagas för spionage mot tjänstemän och politiker i Tyskland, Frankrike, Sverige och Norge via Danmark åren 2012–2014.

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Top 5 cyberhot - betydliga fenomen över en längre period

1 ↑

Sårbarheter som inte åtgärdas öppnar vägen för brottslingar till organisationen. Sårbarheter utnyttjas snabbt. Man lämnar enheter och tjänster öppna på nätet, utan att ha beaktat deras informationssäkerhet eller sett till att skyddsåtgärderna och underhållet är tillräckliga.

2 →

Användningen av olika typer av cyberangrepp för utpressning blir allt vanligare och hotar affärsverksamheternas kontinuitet. I Finland kommer det att ske allt fler webbattacker, där tiotusentals euro är småpengar.

3 ↓

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.

↑ *ökat*

↓ *minskat*

→ *oförändrat*

Gult = nytt/ uppdaterat*

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