TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

Maj 2022

#cyberväder

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

28.6.2022

Cybervädret maj 2022

Dataintrång och dataläckor

- Konton för sociala medier har blivit utsatta för dataintrång eller intrångsförsök.
- Lyckade nätfiskekampanjer har resulterat till dataintrång i Office 365-konton. Kontona har använts för att skicka meddelanden.

Bluff och nätfiske

- Flera tusen textmeddelanden med falska orderbekräftelser har skickats ut i namnen på bakgrundsbilden Wallpaper och speltjänsten Dorgames.
- Nätfiske efter bankkoder i Skatteförvaltningens namn.

Skadeprogram och sårbarheter

- Infrastrukturen som spridit det skadliga programmet FluBot är inte längre aktiv, och varningen om FluBot har tagits bort.
- Ny anvisning hjälper organisationer som drabbats av ett utpressningsprogram.

Automation och IoT

- Den tyska cybersäkerhets-myndigheten BSI har publicerat ett informationssäkerhetscertifikat för konsumenternas smarta enheter.
- Kriminell verksamhet kan döljas genom att utnyttja IoT-system som inte omfattas av normala informationssäkerhetskontroller.

Nätens funktion

- Näten fungerade mycket bra i Finland i maj.
- Överbelastningsangrepp rapporterades men det blev inte några större effekter.

Spionage

- APT41, eller Winnti, har försökt spionera på industriella företag på olika håll i världen.
- Grupper som rapporterats ha samband med Ryssland har fortsatt vara aktiva i Europa, och det finns fortfarande cyberangrepp även i Ukraina.

TRAFICOM

28.6.2022

Top 5 cyberhot - betydliga fenomen över en längre period

1

De ekonomiska och politiska fenomenen reflekteras även i cybersäkerheten.

Digitaliseringen är en övergripande fråga i hela organisationen och ändringarna i det internationella säkerhetsläget påverkar avsevärt organisationens kontinuitet och riskhantering.

2

Bristfälligt informationsutbyte försvagar den heltäckande lägesbilden av cybersäkerheten.

Cyberhotet som en organisation möter kan följande dag drabba andra organisationen.

3

Ouppdaterade sårbarheter öppnar en rutt till organisationen för de kriminella.

De kriminella utnyttjar sårbarheterna snabbt. Man lämnar enheter öppna mot internet utan att ha beaktat deras informationssäkerhet och även skyddsåtgärderna och underhåll är bristfälliga.

Symboler

Ny

Uppdaterad

4

Cybersäkerhet är beroende av experter och cybersäkerhetskunskaperna hör till alla!

Det finns ett allt större behov av allt mångsidigare cybersäkerhetsexperter och den nya regleringen och cybersäkerhetens inkludering som en del av förtagens dagliga rutiner ökar behovet ytterligare.

5

Åtkomsträttigheter är nycklar till en organisation.

Kontroll av åtkomsträttigheter är mycket viktigt i en organisation. Koder kan stjälas med hjälp av olika angrepp, och detta kan ha en betydande inverkan på organisationens verksamhet om koderna hamnar i orätta händer.

TRAFICOM

28.6.2022