TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

Juni 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

18.7.2022

Cyberväder juni 2022

Dataintrång och dataläckor

- O365-dataintrång har inträffat som vanligt även i juni.
- I Kina gjorde man ett dataintrång i polisens databas och uppgifterna för en miljard människor hamnade i orätta händer.

Bluff och nätfiske

- Nätfiske efter nätbankskoder fortsätter i så gott som alla finländska bankers namn.
- Bedrägerimeddelanden sprids i Polisstyrelsens namn.

Skadeprogram och sårbarheter

- En sårbarhet i Microsofts verktyg möjliggör angrepp med hjälp av skadliga Microsoft Office-dokument.

Automation och IoT

- Även en uppmärksam användare kan inte alltid skydda sina smartapparater om sårbarheten finns i tillverkarens molntjänst.
- Sårbarheter hittas hela tiden även i automationsmiljöer, och sårbarheterna kan utnyttjas allt mer i cyperoperationer.

Nätens funktion

- I näten har man upptäckt 6 betydande störningar som dock inte hade några större verkningar.
- För överbelastningsangrepp är läget lugnt i Finland.

Spionage

- Soft Cell-kampanjen har utvidgat sina mål förutom till teleoperatörer även till finanssektorn och statsförvaltningar.
- APT-aktörer utnyttjar sårbarheten Follina.
- Hemmaroutrar och routrar för små företag är fortfarande mål för APT-aktörer.

TRAFICOM

18.7.2022

Top 5 cyberhot - betydliga fenomen över en längre period

1

De ekonomiska och politiska fenomenen reflekteras även i cybersäkerheten.

Fenomenen kan ses snabbt i den digitala miljön och de kan medföra svårförutsebara händelser i cybersäkerheten.

2

Ledning och riskhantering.

De snabba förändringarna i verksamhetsmiljön testar organisationernas riskhantering i cybersäkerheten. Det ankommer på ledningen säkerställa riskhanteringens inverkan.

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

18.7.2022