TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

Februari 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

28.3.2022

Cybervädret februari 2022

Dataintrång och dataläckor

- Savonia yrkeshögskola berättade att skolan hade utsatts för ett cyberangrepp.
- Den kommunala sektorn utsattes för en ganska omfattande nätfiskekampanj som ledde till flera lyckade dataintrång.

Bluff och nätfiske

- Bedrägerier på försäljningsspalterna på internet har fortsatt livligt.
- Det används nya intrig för att kapa användarnas identifieringsuppgifter till sociala medier.

Skadeprogram och sårbarheter

- Skadliga program har riktats mot ukrainska organisationer.
- Operativsystemet kernel i Linux har en mycket kritisk sårbarhet som möjliggör eskalering av rättigheter.

IoT

- Många kritiska sårbarheter hittades bl.a. i en plattform som används för förvaltning och fjärrövervakning av IT-system.

Nätens funktion

- Näten fungerar för tillfället bra i Finland.
- En bank drabbades av ett överbelastningsangrepp som påverkade bankens verksamhet i stor utsträckning.
- Överbelastningsangreppen förekommer dock i allmänhet i jämna vågor.

Spionage

- I Ukraina har man efter Rysslands anfall observerat flera skadliga program som förstör uppgifter samt nätfiske och överbelastningsangrepp.
- I USA berättade man om betydliga spionagefall mot försvarsindustrin och mediebranschen.
- Den iranska gruppen MuddyWater spionerar aktivt på flera branscher.

TRAFICOM

28.3.2022

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 att 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

28.3.2022