TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

Januari 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

17.2.2022

Cybervädret januari 2022

Dataintrång och dataläckor

- Det finns aktivt nätfiske efter Facebook-koder via Facebook Messenger.
- Januari har annars varit en lugn månad med tanke på anmälningar om dataintrång.

Bluff och nätfiske

- Meddelanden som förfalskats till räkning och till anmälningar om säker e-post har man kunnat fiska efter flera hundra koder och kapa konton.
- Användare luras att ge sina kreditkortsuppgifter till tjuvar på försäljningsspalterna på internet.

Skadeprogram och sårbarheter

- Den kritiska varningen om sårbarheten Log4shell har tagits bort efter att ha varit i kraft två månader.
- Varningen om det skadliga programmet Flubot har tagits bort eftersom operatörernas filtreringsåtgärder har hjälpt bra.

Automation

- Över hälften av IoT-apparaterna inom hälsovården är sårbara.
- Sårbarheter hittades i Tesla-bilar. Det är inte självklart att man anmäler om sårbarheter ansvarsfullt.
- Extra material publicerades till boken Automaation tietoturva.

Nätens funktion

- I januari förekom det fem betydande störningar i allmänna kommunikationstjänster.
- Flera överbelastningsangrepp i slutet av januari.
- Rekordsiffror i Finland igen: ett överbelastningsangrepp hade en hastighet på 379 Gbit/s.

Spionage

- Programmet Pegasus som är avsett för spionage på mobilapparater har också använts för att spionera på finländska diplomater.
- Den allt hårdare konflikten mellan Ukraina och Ryssland har synts som cyberangrepp på området.

TRAFICOM

17.2.2022

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

17.2.2022