TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

November 2021

#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

30.12.2021

Cybervädret november 2021

Dataintrång och dataläckor

- DVV har publicerat en elektronisk guide på webbtjänsten Suomi.fi för organisationer som drabbats av dataintrång eller dataläckage.
- Ett danskt företag som tillverkar och opererar vindturbiner drabbades av ett dataintrång.

Bluff och nätfiske

- Antalet textmeddelandebedrägerier har ökat explosionsartat.
- Förutom bankkoder är nätfiskarna intresserade av användarkoder och e-post vid universitet.

Skadeprogram och sårbarheter

- Sårbarheten i den aktivt utnyttjade Log4j-komponenten kräver omedelbara åtgärder av administratörerna.
- Det skadliga programmet FluBot sprids flitigt i Finland. I spridningsmeddelanden har man använt postpaket och röstmeddelanden som tema.

IoT och automation

- Strategier och anvisningar för cybersäkerheten i IoT och automation blir allt vanligare och berättar om ökande medvetenhet om ämnesområdets viktighet.

Nätens funktion

- 6 betydande funktionsstörningar med betoning på ändringsarbeten och programfel.
- Hackade servrar användes för överbelastningsangrepp.
- HUS berättade att det hade drabbats av ett överbelastningsangrepp.

Spionage

- Iranska aktörer är allt mer intresserade av aktörerna på IT-branschen och om leverantörer av internettjänster.
- En nordkoreansk grupp försöker spionera på informationssäkerhetsforskare igen.
- Olika nätverksutrustningar är ett kontinuerligt mål för cyberspionage eller i valet av dess medel.

TRAFICOM

30.12.2021

Top 5 cyberhot - betydliga fenomen över en längre period

1

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.

2

Användarkoder är värdefull information i organisationer
Kontroll över användarkoder är viktigt i alla organisationer. Koder kan stjälas med hjälp av olika angrepp, och detta kan ha en betydande inverkan på organisationens verksamhet.

3

Det blir allt vanligare att använda olika cyberangreppsmetoder för utpressning och de hotar affärsverksamhetens kontinuitet. I Finland kommer man att se allt fler nätangrepp där tiotusentals euro är småpengar.

Symboler

Nytt

Uppdaterat

4

Molntjänster är nya för många organisationer, och angripare är ofta bästa experter på informationssäkerhet i molnet. Organisationer har snabbt övergått till molntjänster men de förstår ofta inte sin egen miljö och dess förmågor tillräckligt bra.

5

Informationssäkerheten i leverans- och servicekedjor blir allt mer kritisk. För att garantera cybersäkerhet ska organisationerna förstå sina egna leveranskedjor.