TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

December 2020

#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
Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret december 2020

Dataintrång och dataläckor

- Den version av administrationsverktyget SolarWinds som innehöll en bakdörr har också använts i Finland.
- Office 365-konton är fortfarande aktiva mål för intrångsförsök.

Bluff och nätfiske

- Textmeddelanden används för massiv spridning av bedrägerier som leder till abonnemangsfällor, nätfiske och skadliga program.
- Ankomstanmälningar har lett till nätfiske genom vilket bedragarna kan begå snabblån i offrens namn.

Skadeprogram och sårbar

- I administrationsverktyget SolarWinds hittades en bakdörr som möjliggjorde spionage och dataintrång.
- Observationer av Emotet har blivit vanligare i Finland igen efter en passiv månad.

Automation och IoT

- Flera angrepps- och spridningsmetoder har förekommit i det skadliga programmet Gitpaste.
- Brister vid uppdatering av sårbarheter i automationssystem – långa leveranskedjor gör att det tar längre tid att reagera på sårbarheter och identifiera dem.

Nätens funktion

- Endast två betydande störningar i allmänna kommunikationstjänster
- En global störning i Googles tjänster hindrade många att arbeta. Många IoT-apparater fungerade inte.
- Till exempel tjänsteleverantörer och VPN-lösningar har varit mål för överbelastningsangrepp.

Spionage

- Ett cyberangrepp mot Finland i höstas äventyrade vissa e-postkonton för riksdagen - bland dessa var också riksdagsledamöters konton.
- Det gjordes ett intrång mot olika ministerier, ämbetsverk och teknologibolag i USA med hjälp av en bakdörr i administrationsverktyget SolarWinds Orion.

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Top 5 cyberhot - betydliga fenomen över en längre period

1

Det blir allt vanligare att använda olika cyberangreppsmetoder för utpressning och de hotar affärsverksamhetens kontinuitet. Skadorna för enskilda fall har gått upp till tiotals miljoner euro.

2

Nätfiske
är mycket vanligt, och det kan vara svårt för mottagare av ett nätfiskemeddelande att observera bedrägeri. Detta utnyttjas även för riktade angrepp och spionage.

3

Sårbarheter utnyttjas snabbt, vilket förutsätter snabba uppdateringar. Man lämnar enheter öppna mot internet utan att ha beaktat deras informationssäkerhet och även skyddsåtgärderna och underhåll är bristfälliga.

ökat

minskat

oförändrat

Gult = nytt/ uppdaterat*

4

Svag hantering av cyberrisker och oklar ansvarsfördelning för hantering av tjänster Det är svårt att förutspå konsekvenserna för cyberhot, och oklarheter vid ansvarsfördelningen för hantering av tjänster försämrar informationssäkerheten.

5

Bristfällig logginformation utgör en risk i många organisationer. På grund av bristfällig insamling, uppföljning och förvaring av logginformation kan man inte observera eller utreda it-incidenter.

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret