TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

Januari 2021

#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 i januari 2021

Dataintrång och dataläckor

- Arbetsförmedlingsbolaget Eilakaisla har drabbats av ett dataintrång och utpressningsprogram
- Vastaamos patientinformation har delats ut igen på flera ställen i januari

Bluff och nätfiske

- Nätfiske efter bankuppgifter sker med hjälp av falska sökmotorresultat.
- Finskspråkig porrutpressningskampanj blev aktiv igen. Utpressningsmeddelanden skickas fortfarande också på engelska.

Skadeprogram och sårbarheter

- Botnätet Emotet har lagts ned genom internationellt myndighetssamarbete
- Kampanjen som spridit skadliga program via sms i mobiler med OmaPosti som tema har varit mycket aktiv

Automation och IoT

- NAT Slipstreaming v2.0: Det nya angreppssättet kan utsätta all utrustning i inomhusnätet för internet
- Cybersäkerhetscentret uppmuntrar i sitt blogginlägg att man börjar använda SBOM

Nätens funktion

- Sex betydande störningar i allmänna kommunikationstjänster
- Världsomfattande störning i Slack som är ett verktyg för tjänster och grupparbeten
- Överbelastningsangrepp har haft konsekvenser i Finland även i januari. Vi tackar alla som anmält till oss!

Spionage

- Statliga aktörer är intresserade av informationssäkerhets- och sårberhetsforskare
- Uppgifter som stulits vid dataintrånget i Europeiska läkemedelsmyndigheten har läckts ut i förändrad form.
- Tyskland varnar om att APT31-gruppen undersöker sina möjligheter att göra intrång i västerländska politiska organisationer.

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Top 5 cyberhot - betydliga fenomen över en längre period

1 ↑

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.

2 ↓

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.

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*

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