TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

Februari 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

Cybervädret februari 2020

Dataintrång och dataläckor

- Antalet anmälda dataintrång i Office 365 ökar fortfarande.
- Sårbarheten i Exchange-servern som framkom i februari utnyttjas vid dataintrång.

Bedrägerier och nätfiske

- Finländarna har utsatts för hundratusentals telefonbedrägerier som utger sig för att vara tekniskt stöd.
- Nätfisket av Office 365-koder fortsätter och leder till dataintrång nästan dagligen.

Skadliga program och sårbarheter

- Försummelse av kritiska uppdateringar äventyrar företagsverksamhetens kontinuitet.
- Är bärbara datorers mobilförbindelser företagens blinda fläck?

Automation

- EKANS-utpressningsprogram har observerats i världen. Eventuell kontakt med tidigare MEGACORTEX-utpressningsprogram identifierad.

Nätverkens funktion

- Det har rapporterats om stora mängder överbelastningsangrepp, men de har inte haft någon betydande inverkan på tjänsternas funktion.
- Sex betydande funktionsstörningar i februari.
- Omfattande störning i Microsoft Teams; Microsoft glömde förnya certifikat.

Spionage

- Logghanteringen är i allmänhet inte på tillräcklig nivå för att utreda dataintrång.

Top 5 cyberhot - betydande långsiktiga fenomen

1

Utnyttjandet av sårbarheter blir snabbare, vilket kräver snabba uppdateringar. Apparater och tjänster vars datasäkerhet inte har beaktats lämnas öppna på nätet och skyddsåtgärderna samt underhållet är bristfälliga.

2

Nätfiske är väldigt vanligt och mottagaren kan ha svårt att upptäcka att det är fråga om ett bedrägeri. Detta utnyttjas också i riktade attacker och spionage.

3

Utpressningsangrepp med omfattande konsekvenser hotar affärsverksamhetens kontinuitet. Skadorna i enskilda fall har ökat till tiotals miljoner euro.

4

En otydlig ansvarsfördelning mellan tjänsteleverantören, underleverantörerna och beställaren försämrar hanteringen av datasäkerheten. Brister i kontrollen av loggar gör det svårare att upptäcka hot.

5

Organisationer kan inte hantera sina cyberrisker. Man kan inte förutse hur hoten påverkar verksamheten och därför underskattas riskerna. Det finns brister i återhämtningsplanerna.