TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

December 2019

#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 december 2019

Nätens funktion

- Sårbarhet i en aktiv nätverksutrustning utnyttjades vid ett överbelastningsangrepp.
- Vinterstormen orsakade endast ringa störningar i nätens funktion.
- Minskningen av antalet betydande störningar avstannade.

Spionage

- Den skärpta politiska situationen mellan Iran och USA höjer också risken för cyberangrepp och cyberspionage.
- Tvåfaktorsautentisering hindrar cyberspioner inte att göra intrång i system.

Skadeprogram och sårbarheter

- Till exempel Citrix produkter hade en sårbarhet som saknar programfix och som utnyttjas för angrepp.
- Det skadliga programmet Lokibot har spridits aktivt via e-post bland annat i Åbo universitets namn.

Dataintrång och dataläckage

- Office 365-dataintrång betydde en förlust på tiotusentals euro för ett finländskt företag.
- Ett ganska omfattande dataintrång i Facebook-koder som dock inte omfattade lösenord eller betalkortsuppgifter.

Bluff och nätfiske

- Abonnemangsfällor är allt oftare automatiserade.
- Abonnemangsfällor sprids via sms, e-post, länkar till reklam och sökmotoroptimering.

IoT och automation

- Den årliga kartläggningen avslöjade över tusen oskyddade enheter i Finland.
- FBI rekommenderar att man håller IoT-apparaterna i separata system.

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret