



TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

November 2022

#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

Cybervädret november 2022

Dataintrång och dataläckor

- ▶ Anmälningar om dataintrång fortsätter att öka i jämn takt. Ökningen från oktober till november 12 % och från september till november 27 %.
- ▶ Antalen utpressningsprogram samt "wipers" som är förklädda utpressningsprogram har ökat runtom i världen.

Automation och IoT

- ▶ Cyberhoten i industriella miljöer ökar igen. Antalet incidenter med utpressningsprogram har ökat under hösten.
- ▶ IoT-apparater utsatta för gamla sårbarheter på grund av försummade uppdateringar.

Bluff och nätfiske

- ▶ Polisbedrägerier och annan utpressning är fortfarande ett problem.
- ▶ Antalet bedrägeriförsök med lönebetalning har ökat.
- ▶ Black Friday i november åstadkom en hel del bedrägerier.

Nätens funktion

- ▶ I november förekom det två betydande störningar i allmänna kommunikationstjänster.
- ▶ På basis av anmälningar var november den andra mest aktiva månaden i fråga om överbelastningsangrepp. Antalet anmälningar var större bara i oktober.
- ▶ En del av angreppen hade tillfälliga konsekvenser på tjänstens funktion.

Skadeprogram och sårbarheter

- ▶ Den amerikanska informationssäkerhetsmyndigheten CISA har webbsidan Shields Up där det bl.a. finns en förteckning över utnyttjade sårbarheter och anvisningar för hantering av sårbarheter.

Spionage

- ▶ Cyberspionage- och sabotagekampanjer som har samband med kriget i Ukraina fortsätter.
- ▶ Informationssäkerhetsforskare rapporterar om Mustang Pandas aktivitet under året.

Top 5 cyberhot i den närmaste framtiden (6 månader - 2 år)

1 

De ekonomiska och politiska fenomenen reflekteras även i cybersäkerheten.

Digitaliseringen är en övergripande fråga i hela organisationen och ändringarna i det internationella säkerhetsläget påverkar avsevärt organisationens kontinuitet och riskhantering.

2 

Det anses att nivån för cyberhot har ökat i Finland.

På grund av ökad skadlig trafik och förhöjd hotnivå blir organisationernas beredskap allt viktigare.

3 

Brister i vanliga avvärjningsåtgärder orsakar fortfarande majoriteten av informationssäkerhetsincidenterna.

Till exempel hantering av åtkomsträttigheter, upprätthållande av programvara och god informationssäkerhetskultur utgör grundvalen för cybersäkerheten.

Symboler

Ny 

Uppdaterad 

4

Bristfälligt informationsutbyte försvagar den heltäckande lägesbilden av cybersäkerheten.

Cyberhotet som en organisation möter kan följande dag drabba andra organisationen. Effektivt informationsutbyte förbättrar cybersäkerheten för alla.

5

Cybersäkerhet är beroende av experter och cybersäkerhetskunskaperna hör till alla!

Det finns ett allt större behov av allt mångsidigare cybersäkerhetsexperter och den nya regleringen och cybersäkerhetens inkludering som en del av företagens dagliga rutiner ökar behovet ytterligare.