



TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

November 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



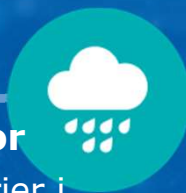
oroande



allvarligt

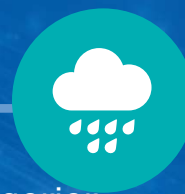
Cybervädret november 2020

Dataintrång och dataläckor



- ▶ Dataläcka hos flera ministerier i Estland.
- ▶ Office 365-dataintrång fortsätter, hackade e-postlådor utnyttjas för att skicka nätfiskemeddelanden.

Bluff och nätfiske



- ▶ Bedrägerisamtal, SMS-bedrägerier med Posten som tema och nätfiske efter O365-koder fortsätter livligt.
- ▶ Bluffsamtal (wangiri) fortsatte att öka, nu från +212.
- ▶ Nätfiske är ett viktigt verktyg också för brottslingar som begår riktade dataintrång.

Skadeprogram och sårbarheter



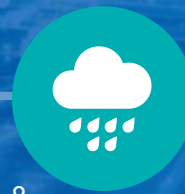
- ▶ Antalet incidenter med Emotet som tema har minskat och varningen om Emotet har raderats.
- ▶ Gamla sårbarheter i Fortinet VPN-enheter har använts.
- ▶ Skadliga program har spridits via säker e-post som låtsas komma från banker.

Automation och IoT



- ▶ Störningar i AWS skadade till exempel robotdammsugarnas funktion överallt i världen.
- ▶ Brottslingar använder IoT-apparater belägna i Finland för att routera nättrafik för kreditkortsbedrägerier.
- ▶ Det skadliga programmet Gitpaste drabbar även IoT-apparater.

Nätens funktion



- ▶ Antalet störningar i nät var något större än i genomsnitt.
- ▶ Vi fick anmälningar om överbelastningsangrepp som också hade omfattande konsekvenser på tjänsternas funktion.
- ▶ Vi har också fått anmälningar om utpressningsmeddelanden som har samband med överbelastningsangrepp.

Spionage



- ▶ Informationssäkerhetsföretaget FireEye drabbades av ett dataintrång begått av en statlig aktör vars syfte var att få tag på uppgifter om statliga kunder.
- ▶ Cyberspionage mot organisationer som utvecklar COVID-vacciner, flera aktörer bakom dem.
 - ▶ Bland dem som drabbats är t.ex. Europeiska läkemedelsmyndigheten.

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.

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.

↑ ökat
↓ minskat
→ oförändrat

Gult* = nytt/
uppdaterat