



TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

September 2023

#cyberväder

Cybervädret berättar om betydande säkerhetsincidenter och -fenomen under månaden.

Denna produkt är i första hand avsedd för dem som arbetar med informationssäkerhetsfrågor på olika nivåer i organisationer. Läsaren får en snabb helhetsbild av vad som har hänt och vad som kommer att hända på cybersäkerhetsfältet.

Cybervädret kan vara:



lugnt



oroande



allvarligt

Cybervädret i september 2023

Dataintrång och dataläckor



- ▶ Till följd av dataintrånget i Essity/Westlog fick vi anmälningar om uppgifter som läckt ut.
- ▶ Vid dataintrång i konton för sociala medier har man också sett missbruk av kreditkortsuppgifter som sparats i systemet till exempel genom att köpa annonser.

Bluff och nätfiske



- ▶ Ett rekordantal bedrägerisamtal ringdes från förfalskade nummer i september.
- ▶ Nätfiske efter bankkoder övergick igen från textmeddelanden till e-post.
- ▶ Med faktureringsbedrägerier försökte man lura olika organisationer från fiskeklubbar till en hembygdsförening.

Skadeprogram och sårbarheter



- ▶ En kritisk sårbarhet som används på distans i libwebp-biblioteket kräver omedelbar uppdatering. Biblioteket används bland annat i flera olika webbläsare.

Automation och IoT



- ▶ NIST har uppdaterat sin anvisning 800-82 som koncentrerar sig på skyddet av industriella automationsmiljöer.
- ▶ I den nya versionen beaktas bland annat cybersäkerhetshot mot förändrade produktionsmiljöer, skyddsverktyg, rekommenderade praxis samt arkitekturer.

Nätens funktion



- ▶ I september förekom det två betydande störningar i allmänna kommunikationstjänster.
- ▶ Hacktivister fortsätter med överbelastningsangrepp och inhemska organisationer har fått sin del av angreppen.
- ▶ Överbelastningsangreppen har inte medfört några allvarliga konsekvenser för tillgången till tjänster.

Spionage



- ▶ Microsofts rapport som publiceras en gång i halvåret beskriver trenden med cyberoperationer i östra Asien.
- ▶ Microsofts rapport berättar till exempel om cyberspionage och påverkansförsök som antas ha samband med Kina samt om den nordkoreanska informationsinsamlingen och anskaffningen av kryptovaluta.

Cybersäkerhetscentrets åtgärder och tips för förberedelser



Cybersäkerhetscentrets kommunikativa tema i september var Bli bekant med informationssäkerhetsfenomen. Under månaden berättade vi i våra kanaler för sociala medier om de vanligaste informationssäkerhetshoten samt om hur man kan skydda sig mot dem.



Vi publicerade en ny anvisning om incidenthantering i molnmiljöer.



I september publicerades för kommuner tjänsten Hyöky med vilken det är möjligt att kartlägga kommunens yta för angrepp i offentliga nät.

Allmän översikt över cybersäkerheten i september

- ▶ En hacktivistgrupp meddelade att den gjort angrepp mot flera europeiska myndighetsaktörer.
 - ▶ Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom var ett av de rapporterade målen.
 - ▶ Överbelastningsangreppens effekt på tjänsternas funktion är i allmänhet tillfällig. De har ofta likställts med hög trafik eller manifestationer på nätet som syftar till att skapa nyheter.
- ▶ Centret fick ett stort antal anmälningar om bedrägerisamtal från förfalskade nummer. Traficoms föreskrift som ålägger teleoperatörerna att förhindra samtal som kommer från utlandet med falska finländska nummer även för mobilnumrens del trädde i kraft vid början av oktober.
- ▶ Under den gångna månaden har antalet anmälningar till Cybersäkerhetscentret om dataintrång, intrångsförsök och dataläckor minskat.



Trenderna inom cybersäkerhet de senaste 12 mån.

