TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

Augusti 2021

#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

TRAFICOM

16.9.2021

Cybervädret augusti 2021

Dataintrång och dataläckor

- Domännamnet Vastaamohaku.com registrerades vid slutet av augusti och nedlades några dagar senare.
- Under månaden har det rapporterats flera intrång i användarkonton till följd av nätfiske.

Bluff och nätfiske

- Nätfiske efter bankkoder blir allt bättre.
- I sökmaskiner har man matat in både förfalskade resultat och annonser som i stället för rätt tjänst leder till nätfiske.

Skadeprogram och sårbarheter

- Vi tog bort varningen om skadliga program mot Android-enheter 17.8.
- PrintNightmare-sårbarheterna är fortfarande aktuella.
- Sårbarheten Atlassian Confluence utnyttjas aktivt.

Automation

- Många allvarliga sårbarheter som man försöker utnyttja aktivt.
- ETSI har publicerat en teknisk specifikation om bedömningen av IoT-säkerheten i konsumentapparater.

Nätens funktion

- Fyra betydande störningar i nätens funktion.
- Hackade Confluence-servrar användes för överbelastningsangrepp.
- Hösten kommer och medför angrepp mot inlärningsmiljöer. Påminn din skolelev att störning av informationsnät är ett brott.

Spionage

- Kinesiska aktörer har under flera år försökt göra intrång i teleoperatörernas system i Asien med hjälp av motsvarande metoder som i operationen Hafnium.
- I våras pågick det en kampanj som försökte installera det skadliga programmet Cobalt Strike på enheter via e-post; i Europa var åtminstone Slovakien utsatt för denna kampanj.

TRAFICOM

16.9.2021

Top 5 cyberhot - betydliga fenomen över en längre period

1

Ouppdaterade sårbarheter öppnar en rutt till organisationen för de kriminella. De kriminella utnyttjar sårbarheterna snabbt. Man lämnar enheter öppna mot internet utan att ha beaktat deras informationssäkerhet och även skyddsåtgärderna och underhåll är bristfälliga.

2

Det blir allt vanligare att använda olika cyberangreppsmetoder för utpressning och de hotar affärsverksamhetens kontinuitet. I Finland kommer man att se allt fler nätangrepp där tiotusentals euro är småpengar.

3

Molntjänster är nya för många organisationer, och angripare är ofta bästa experter på informationssäkerhet i molnet. Organisationer har snabbt övergått till molntjänster men de förstår ofta inte sin egen miljö och dess förmågor tillräckligt bra.

Symboler

Nytt

Uppdaterat

4

Informationssäkerheten i leverans- och servicekedjor blir allt mer kritisk. För att garantera cybersäkerhet ska organisationerna förstå sina egna leveranskedjor.

5

Distansarbete är här för att stanna – och så är också riskerna. Distanstjänster för enheter som är öppna mot internet utsätter organisationer för dataintrång. Administratörer bör se till att distansarbetarnas utrustning är skyddad och brandväggsinställningar ändamålsenliga.

3 mån.

TRAFICOM

16.9.2021