TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cyberväder

September 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

Cybervädret september 2021

Dataintrång och dataläckor

- Det finländska börsbolaget Adapteo berättade om dataintrång i början av september.
- Koder för underhåll av brandväggar till finländska organisationer fanns till salu på ett hackarforum.

Bluff och nätfiske

- Nätfiske efter bankkoder och betalningsuppgifter är aktivt i alla bankers namn både per e-post och per sms.
- Sökresultat till nätbanker och till Mina Kanta har förfalskats i sökmotorer för att visa till nätfiskesidor.

Skadeprogram och sårbarheter

- Vi publicerade en ny sida med mer information om Autoreporters observationer av de vanligaste skadliga programmen.
- Microsofts autodiscover-funktion hade en sårbarhet som utnyttjades.

IoT och automation

- Cybersäkerhetscentret vid Traficom och cybersäkerhetsmyndigheten i Singapore publicerade sitt samarbete om ömsesidigt godkännande av IoT-cybersäkerhetsmärken.
- Det hittades nya IoT-sårbarheter, och även sårbarheter i industriautomation.

Nätens funktion

- Det förekom två betydande störningar i nätens funktion i Finland.
- Problem på Facebook påverkade också användningen av Instagram och WhatsApp under flera timmar.
- Överbelastningsangrepp påverkade tillgången till tjänsterna i viss mån i september.

Spionage

- ProxyShell-angreppet hotar lokalt administrerade Microsoft Exchange-servrar.
- Tyskland och EU anklagar Ryssland för den så kallade Ghostwriter-verksamheten.
- Enligt Skyddspolisen förekommer det kontinuerliga försök till cyberspionage mot Finland.

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.