TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret

September 2024

#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

Månadens nyckeltal

1 år

Den nationella kartläggningen av angreppsytan (Hyöky) som Cybersäkerhetscentret vid Traficom tillhandahåller fyllde ett år i september! Tjänsten är avsedd för kommuner och organisationer inom den offentliga förvaltningen, men vi håller på att utöka möjligheten så att även beredskapskritiska organisationer kan beställa tjänsten. [1, 14]

100/100

Finland fick fulla poäng och placerade sig på nivå 1 i Internationella teleunionen ITU:s globala cybersäkerhetsindex. [2]

1.

Transport- och kommunikationsverket Traficom har beviljat det första godkännandet av kryptoprodukter för krypteringslösningen Insta SafeLink som skyddar Natos säkerhetsklassificerad information. [3]

Cybervädret i september 2024

Dataintrång och dataläckor

- Antalet anmälda dataintrång har fortsatt vara lugnt.
- M365-nätfiske med Dropbox som tema och dataintrång till följd av detta är den största enstaka kategorin.
- Jämfört med förra året har antalet angrepp med utpressningsprogram varit lägre.

Bluff och nätfiske

- Textmeddelandebedrägerier som gjorts i Traficoms namn började minska när registreringen av SMS sender ID trädde i kraft vid slutet av september.
- Bedrägerier som förfalskats i PRS namn ledde till en nätfiskesida som liknade suomi.fi-identifikation.

Skadeprogram och sårbarheter

- Det skadliga programmet Lumma Stealer har spridits på ett nytt sätt sedan augusti.
- Två kritiska sårbarheter har hittats i Red Hat Open Shift.
- Sårbarheterna i utskriftssystemet CUPS möjliggör körning av godtycklig kod.

Automation och IoT

- Brottslingar använder en hel del fjärranvändningsprogram [4] som användare av industriautomation har installerat i sina system.
- Enligt informationssäkerhets-bolaget Claroty har 55 % av de internetanslutna indstriautomationsmiljöerna minst fyra olika fjärranvändningsprogram [5].

Nätens funktion

- I september observerades två funktionsstörningar i allmänna kommunikationsnät.
- Inhemska organisationer var mer aktiva att anmäla överbelastningsangrepp jämfört med året innan.
- På finansbranschen förekom störningar som fick synlighet också i medierna. Nordea berättade att störningarna hade delvis berott på överbelastningsangrepp [6].

Spionage

- Myndigheterna i USA körde ned ett omfattande botnät som ansågs ha samband med Kina. [7]
- APT-aktörerna utnyttjar botnäten bland annat för att fördunkla ursprunget för illvillig nättrafik eller att observera den.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Genom NIS2-direktivet får organisationerna en skyldighet att anmäla betydande cybersäkerhetsincidenter till tillsynsmyndigheten. Vi publicerade en artikel där vi ger tips för utvecklingen av incidenthanteringsprocesserna i organisationer (på finska) [8]

Organisationer ska fortfarande på olika sätt vara förberedda för överbelastningsangrepp. Hacktivisters överbelastningsangrepp på applikationsnivå och den nya vågen av *carpet bombing*-tekniken är bra exempel på att angriparna kontinuerligt försöker utveckla sina metoder.

Verksamhetsmiljön som förändras kontinuerligt ställer förväntningar och krav såväl för organisationernas som för samhällets beredskap. Med hjälp av regelbundna övningar är det möjligt att förbättra samhällets cyberresiliens och funktionssäkerhet. Cybersäkerhetscentret deltar årligen i flera övningar och stödjer försörjningsberedskapskritiska organisationers cyberövningar som myndighetstjänst. [9]

Allmän översikt över cybersäkerheten i september

- I september förekom det något flera cybersäkerhetsincidenter efter de lugna sommarmånaderna.
- I det annars ganska klara höstvädret har det varit dimma på grund av överbelastningsangrepp samt olika nätfiske- och bedrägerikampanjer mot finländska organisationer.
  - I början av hösten har Cybersäkerhetscentret fått ett större antal rapporter om överbelastningsangrepp än tidigare. Bland annat Nordea har berättat om att störningar under de senaste tiderna har delvis berott på överbelastningsangrepp. Än så länge har konsekvenserna i övriga fall blivit små. [10, 11]
  - Nätfiske efter M365-koder med Dropbox som tema har varit aktivt vid början av hösten. Cybersäkerhetscentret har fått en hel del anmälningar om dataintrång i M365-konton till följd av Dropbox-nätfiske. [12]
  - Textmeddelandebedrägerier som gjorts i Traficoms namn syns i polisens riksomfattande lägesbild över bedrägeribrott. Enligt polisen var det sammanlagda brottsliga vinningen från bedrägerier över 560 000 euro enbart i september. Samma fenomen observerades i lägesbilden redan tidigare under sommaren men enligt polisen har fenomenet ökat under hösten. [13]
- Dessutom gjorde vi flera observationer än normalt om två olika botnät i Finland.
  - Det ganska nya botnätet Quad7 tar över speciellt Asus- och TP-Link-routrar avsedda för hushåll. Det har också gjorts observationer om botnätet Mirai som varit aktivt i flera år. [14]

Trenderna inom cybersäkerhet
de gångna 12 mån.