TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret

Augusti 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 helheltsbild av vad som har hänt och vad som kommer att hända på cybersäkerhetsfältet.

Cybervädret kan vara:

 lugnt

 oroande

 allvarligt

Cybervädret i augusti 2023

Dataintrång och dataläckor

- I augusti kunde man se att sårbarheten i programmet Citrix Netscaler, som publicerades i sommar, hade utnyttjats. Sårbarheten har antagligen utnyttjats mycket snabbt och på ett automatiserat sätt.
- I övrigt har antalet anmälningar sjunkit till samma s.k. normala nivå som i början av året.

Bluff och nätfiske

- Nätfiske var mycket aktivt i augusti.
- Meddelanden som hotelltjänsten booking.com skickat används för nätfiske efter betalkortsuppgifter.
- Nätfiske efter bankkoder pågår igen både genom det aktuella skatteåterbäringstemat och genom textmeddelanden som förfalskats så att de verkar komma från posten.

Skadeprogram och sårbarheter

- Sårbarheten Citrix Netscaler från juli ledde till flera dataintrång i Finland.
- Uppdateringarna ska fortfarande installeras så snabbt som möjligt efter att de blivit tillgängliga.
- Amerikanska myndigheter berättar att det skadliga programmet Qakbot har förhindrats med hjälp av en internationell operation.

Automation och IoT

- Harmoniserade standarder för informationssäkerhets-bestämmelsen i EU:s radioutrustningsdirektiv (RED) har sänts på remiss.

Nätens funktion

- I augusti förekom det nio betydande funktionsstörningar i de allmänna kommunikations-tjänsterna.
- En del av störningarna berodde på elavbrott.
- För överbelastningsangreppens del var augusti en lugn månad och de observerade incidenterna hade inte några betydande effekter på tjänsterna.

Spionage

- Ett riktat nätfiske kan också ske via Teams.
- Enligt Microsofts rapport utnyttjade en kampanj nätfiskemeddelanden som skickats via Teams och syftet var att kapa objektets användarkonto. I meddelanden gav man sig ut för att vara från IT-stöd eller informationssäkerhetsteam.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

- Cybersäkerhetscentret har publicerat ett nytt verktyg för att underlätta planeringen av cyberövningar.
- Vi publicerade en anvisning för hur man kan radera sina uppgifter från taxitjänsten Yango.
- Seminariet Informationssäkerhet 2023 anordnas den 12 oktober 2023. Du kan följa evenemanget avgiftsfritt på webben. Anmäl dig nu!
- Ketjutonttus öppna webbinarium om översikt över resultaten anordnas den 5 oktober 2023.
- Traficom har publicerat internetsidorna om sjöfartens cybersäkerhet.

Allmän överskit över cybersäkerheten i augusti

- I augusti såg man en hel del bedrägerimeddelanden med säker e-post som tema. Man försökte igen lura uppgifter och pengar av mottagarna i kända aktörers namn, till exempel i Polisens, Postis och Skatteförvaltningens namn.
- I augusti utnyttjades sårbarheten Citrix Netscaler mycket snabbt och automatiskt över webben. Utnyttjandet möjliggjorde en bakdörr (ett webbskal) i systemet vilket förblev där även efter att systemet hade uppdaterats.
- 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.

Trenderna inom cybersäkerhet
de senaste 12 mån.