TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädер

Juni 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 juni 2023

Dataintrång och dataläckor

- Antalet intrång i företagens e-postkonton har under hela första halvåret varit högt jämfört med år 2022.
- Antalet anmälningar om intrång i konton för sociala medier fortsätter att vara på en hög nivå.

Bluff och nätfiske

- Nätfiskesidor gömmas allt oftare bakom QR-koder.
- Personuppgifter som stulits eller som läckt ut används för många olika slags brott, till exempel för det mer skräddarsydda nätfisket efter bankkoder.

Skadeprogram och sårbarheter

- Zyxel åtgärdade en kritisk sårbarhet i sina NAS-enheter, man har redan rapporterat om att sårbarheten har utnyttjats.
- Cybersäkerhetscentret har fått rätt att bevilja CVE-koder, dvs. att vara en CVE Numbering Authority (CNA)-aktör.

Automation och IoT

- IoT-lösningar kan sluta fungera oväntat, vilket kan medföra betydande problem för användare.
- En enskild kunds förmåga att påverka tjänsteleverantören eller åtgärda problemet är liten.
- Beslutet om tjänstens upphörande kan omfatta svåra etiska frågor.

Nätens funktion

- I maj förekom det tre betydande störningar i allmänna kommunikationstjänster.
- Hamnoperatörer blev igen utsatta för överbelastningsangrepp.
- Namntjänst som tillhandahålls en operatörs företagskunder drabbades av ett överbelastningsangrepp.

Spionage

- Skadliga program som sprids via USB-minne blir vanliga igen även inom cyberspionage.
- Informationssäkerhetsforskare berättar om flera fall där infekterade USB-minnen har spridit skadliga program som sedan har utnyttjas för insamling av information och hålla fotfäste i olika mål.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Cybersäkerhetscentret har blivit godkänt som CNA-aktör (CVE Numbering Authority) som tilldelar CVE-identifierare (Common Vulnerabilities and Exposures) till sårbarheter.

Det nationella samordningscentrumet vid Cybersäkerhetscentret (NCC-FI) har öppnat sin första ansökan om stöd för finansiering av moderna cybersäkerhetslösningar och -innovationer i små och medelstora företag.

Vi publicerade en ny anvisning om att genomföra en övning via e-post.

Förberedelserna inför Post-Quantum Crypto-tiden pågår också i Finland.

Allmän överskit över cybersäkerheten i juni

- I juni fick Cybersäkerhetscentret anmälningar om att sårbarheten i Zyxel hade utnyttjats även i Finland. Internationellt har sårbarheten utnyttjats aktivt och i offentligheten har det bl.a. konstaterats att botnätet Mirai gör angrepp mot Zyxels brandväggar.
  - Zyxel tackar i sitt meddelande Cybersäkerhetscentrets (NCSC-FI) hjälp för att sårbarheten hittades.
- Nolldagarssårbarheten i filöverföringsprogrammet MOVEit utnyttjades i stor utsträckning internationellt. I Finland förekom det inte många fall, eftersom enligt våra uppgifter används systemet inte i stor utsträckning.
- M365-nätfiske blir allt snabbare. För tillfället är fördröjningen mellan en lyckad nätfiskehändelse (där användaren ger sina koder) och utnyttjandet som snabbast bara några minuter.
  - Cybersäkerhetscentret fick över 100 anmälningar om M365-dataintrång under det andra kvartalet.

Trenderna inom cybersäkerhet
de senaste 12 mån.