TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret

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

Cybervädret kan vara:

 lugnt

 oroande

 allvarligt

Cybervädret i juli 2024

Dataintrång och dataläckor

- Dataintrången i M365-konton orsakade mörka moln på den blå sommarhimlen. I juli var antalet dataintrång större än under föregående månader. För att komma över användar-ID användes särskilt AiTM-tekniken.
- Som helhet är antalet anmälningar om dataintrång hälften så många under sommaren som i början av året.

Bluff och nätfiske

- Bedragaren säger sig ringa från banken och skrämmer upp offren med suspekta kontoöverföringar till utlandet. Bedragaren begär offrets bankkoder för ett "återbetalningskonto".
- I textmeddelanden med namnen TRAFCOM och TRAFCORN som påminner om myndigheten skräms mottagarna med "böter som överförs till utsökning".

Skadeprogram och sårbarheter

- Störningen i CrowdStrike den 19 juli aktiverade opportunisterna: i CrowdStrikes namn görs nätfiske efter information och skadliga program som påstås åtgärda problemen med uppdateringen sprids.
- En kritisk sårbarhet upptäcktes i Cisco Secure Email Gateway (tidigare IronPort).

Automation och IoT

- Det är tekniskt enkelt att störa trådlösa inbrottsskydds- och kameraövervakningssystem. I USA har poliserna varnat för att fenomenet hela tiden blir vanligare. En bidragande orsak till detta torde vara att det finns övervakningskameror i allt fler hem.

Nätens funktion

- I juli förekom nio funktionsstörningar i de allmänna kommunikationsnäten.
- Överbelastningsangrepp rapporterades också under sommaren, men konsekvenserna för servicen har varit obefintliga.
- Alla överbelastningsangrepp kan inte kopplas till hacktivister.

Spionage

- Cyberhotaktören APT45 (Andariel), som har kopplingar till Nordkorea, har med utpressningsprogram attackerat amerikanska hälso- och sjukvårdsproducenter för att tjäna pengar till staten.
- APT45 har spionerat bl.a. på försvarsindustrin, luftfartsbranschen och organisationer med anknytning till kärnkraft.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Vi publicerade anvisningen Sometilit kuntoon, vinkit turvalliseen somettamiseen (Säkra konton i sociala medier, tips om säker användning av sociala medier). Anvisningen lämpar sig både för privatpersoner och för personer som uppdaterar företagets konton i sociala medier.

En del utpressningsprogram har försökt hitta och förstöra enhetens säkerhetskopior. Beträffande de viktigaste säkerhetskopiorna rekommenderas 3-2-1-regeln: förvara minst **tre** säkerhetskopior på **två** olika ställen och spara **en** av dessa kopior helt utanför nätet.

Utbildningen i finansieringsansökningar för programmet för ett digitalt Europa ordnas den 27 augusti 2024. I ansökningsutbildningen presenteras finansieringsansökningar till programmet för cybersäkerhetsarbete inom programmet för ett digitalt Europa. Dessutom ger erfarna experter konkreta råd och tips för hur ansökningar av hög kvalitet utarbetas och skickas till programmet för ett digitalt Europa.

Allmän översikt över cybersäkerheten i juli

- Juli var en mycket lugn månad och semestersäsongen återspeglades också i helhetsbilden.
- Uppdateringen av informationssäkerhetsprodukten CrowdStrike orsakade en störning som ledde till att Windowsenheter som använder produkten inte kunde startas. Störningen orsakade avbrott i flera tjänster globalt och påverkade bland annat betalningstrafiken, flygtrafiken, tågtrafiken, hälsovården och medieföretag. Även i Finland påverkades vissa organisationer av situationen antingen direkt eller indirekt via leveranskedjan.
- Under juli fick vi ett flertal anmälningar om nätfiske som gällde Microsoft 365-användarkonton i olika organisationer. En del av fallen hade lett till dataintrång i e-postkonton.
- Under juli skickades också olika typer av bluffmeddelanden. Brottslingarna är också med sin tid och i slutet av månaden blev bluffmeddelanden med skatteåterbäring som tema vanligare, eftersom skatteåterbäring betalas ut till många från och med augusti.
- I juli riktades överbelastningsangrepp mot olika organisationer, i synnerhet statsförvaltningen.

Top 5 hot i den närmaste framtiden (6 mån.–2 år)

1.

Allvarliga sårbarheter utnyttjas allt snabbare

Förutom att installera en korrigerande uppdatering är det ofta nödvändigt att undersöka om sårbarheten redan utnyttjats innan uppdateringen installeras.

2.

Utpressningsprogram – ett betydande hot mot organisationer

Under det senaste året har flera organisationer i Finland fallit offer för ett utpressningsprogram och utpressningsprogrammen ökar ständigt i antal även globalt.

3.

Informationssäkerheten och kontinuiteten i leverans- och servicekedjor är allt mer kritiska.

Att förstå underleverantörskedjan är centralt för organisationernas egen cybersäkerhet. De flesta organisationer är mer eller mindre beroende av utlagda digitala tjänster.

Ny

Uppdaterad

Symboler

4.

Organisationer bör vara förberedda på AI-relaterade utmaningar.

Organisationer bör försöka identifiera de utmaningar som artificiell intelligens medför och vara förberedda på dem till exempel genom att utbilda sin personal.

5.

Vikten av att skydda kommunikationsinfrastrukturen framhävs

Det är viktigt att skydda kommunikations- och informationssysteminfrastrukturen utomlands och i hemlandet, dels på grund av skador och naturfenomen som infrastrukturen utsätts för och dels på grund av avsiktliga störningar som orsakas av utomstående.

Trenderna inom cybersäkerhet
de senaste 12 mån.