TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Cybervädret

Augusti 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 augusti 2024

Dataintrång och dataläckor

- I dataintrång fortsatte sommaren vara lugn och den vanliga ökningen av anmälningar på hösten har inte setts.

Bluff och nätfiske

- Skatteåterbäringar var det populäraste ämnet i bedrägerier.
- Tiotals olika textmeddelande-bedrägerier försökte stjäla nätbankskoder.
- Nätfiske efter bankoder skedde även med andra argument, till exempel i elbolags, tele-operatörers, Kanta-tjänstens, myndigheters och förstås i bankers namn.

Skadeprogram och sårbarheter

- Sårbarheten SonicWall SSL VPN utnyttjas aktivt.
- Det har gjorts flera observationer än normalt om botnäten Quad7 och Mirai.
- Uppdatering av enheter och anskaffning av nya enheter betonas fortfarande när det gäller att skydda sig mot säkerhetshot.

Automation och IoT

- Hanteringen av IoT-system flyttas allt oftare till molnet. I offentligheten togs upp att cyber-säkerheten i molnbaserade fjärrkontrollsystem för distribuerad elproduktion och förvaringen av el inte alltid är tillräckligt bra.
- För slutanvändare är situationen svår, om det inte säkra alternativ inte finns tillgängliga.

Nätens funktion

- I augusti observerades 10 funktionsstörningar i allmänna kommunikationsnät.
- Under de senaste tiderna har en hel del korta överbelastnings-angrepp rapporterats mot finländska organisationers tjänster.
- Konsekvenserna har dock varit små.

Spionage

- APT29 rapporterades ha fått åtkomst till vissa e-postmeddelanden för Storbritanniens statsförvaltning till följd av ett dataintrång mot Microsoft.
- Samma aktör använde metoder som kommersiella spionprogram i Mongoliet använt.
- En hackad webbsida för statsförvaltningen användes vid intrång i andra objekt.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Hotanalys och hotmodellering är centrala verktyg i hanteringen av cybersäkerhetsrisker. Hotanalys samt införandet och uppdateringen av hotmodellering erbjuder en systematisk metod för att identifiera cybersäkerhetsrisker och att förbereda sig för dem. Vi publicerade en artikel om ämnet.

Vår anvisning om hur man kan skydda sitt hemnät och sina personliga uppgifter är fortfrande aktuell. Under de senaste tiderna har vi observerat att två botnät har tagit över hemroutrar i Finland. Botnät används både som en del av distribuerade överbelastningsangrepp och som proxy för skadlig nättrafik i cyberangrepp.

Microsoft börjar införa i etapper tvingad flerfaktorsautentisering i Azure, Intune och Entra ID administratörsportaler. Som en del av att tvinga använda MFA rekommenderas att man skapar s.k. Break glass-ID. Mer information om tenantspecifika tidtabeller finns i Message Centers för ovan nämnda tjänster.

Allmän översikt över cybersäkerhten i augusti

- Augusti var exceptionellt lugn i fråga om incidentanmälningar vi fick.
- I de rapporterade incidenterna framhävdes olika nätfiske- och bedrägerikampanjer mot medborgare. I synnerhet meddelanden med suomi.fi som tema var ett besvär i mitten av augusti. Skatteåterbäringstemat fortsätter också.
- Betydelsen av beredskap och kontinuitetsplanering betonas speciellt vid utpressningsprogram i organisationer och företag av alla storlekar.
  - Ett dataintrång kan ha mycket allvarliga ekonomiska konsekvenser. I värsta fall kan konsekvenserna av ett utpressningsangrepp lamslå en organisation för veckor eller till och med för evigt.
  - Det är också möjligt att få bättre och effektivare hjälp i att utreda incidenten om man rapporterar den snabbt. I bästa fall kan Cybersäkerhetscentret erbjuda verktyg för dekryptering av utpressningsprogrammet.
  - I augusti publicerade vi en artikel om utpressningsprogrammens funktion och hur man kan skydda sig mot dem.

Trenderna inom cybersäkerhet
de gångna 12 mån.