TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

# Cybervädret

Juni 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 juni 2024

## Dataintrång och dataläckor

- Juni var en ganska lugn månad i fråga om dataintrång och dataläckor.
- Facebook-användarkonton knäcktes genom bedrägerier som fiskade efter bekräftelsekoder med IKEA som tema.
- Dataintrång i M365-konton rapporterades i synnerhet i slutet av månaden. Konton hackades till exempel med nätfiskemeddelanden där man "delade en fil".

## Bluff och nätfiske

- Bedrägerier som skickats i Traficoms namn med böter som tema dök upp på ”trafcom.info”, en adress som skrivits på lite annorlunda sätt än tidigare.
- I juni började man igen se bedrägerimeddelanden som skickats i Skatteförvaltningens namn med skatteåterbäring som tema.

## Skadeprogram och sårbarheter

- Som helhet  var juni en lugn månad för dessa fenomen.
- Vi fick några anmälningar om försök att sprida det skadliga programmet Vultur som man hade fått per textmeddelanden.

## Automation och IoT

- Operatörernas enheter i rubriker: I USA gick 100 000 routrar sönder till följd av ett angrepp. I Finland får oskyddade enheter inte tillgång till nätet på grund av att certifikat för vissa modem gått ut.
- En mycket allvarlig brist i små apparater, bland annat i automations-enheternas FreeTROS-operativsystem kan medföra problem över en lång tid.

## Nätens funktion

- I juni förekom det 10 störningar i allmänna kommunikationstjänster.
- Antalet överbelastningsangrepp som rapporterades i juni var måttligt, och de anmälda incidenterna hade inte några avsevärda konsekvenser för tjänster.

## Spionage

- TeamViewer som är känt för sin lösning för distanshantering berättade om ett dataintrång i sitt företagsnät. För detta anklagas Midnight Blizzard (Nobelium, APT29). Intrånget lär inte ha gällt kundförbindelser eller produktionsmiljön.
- Microsoft har skickat anmälningar till sina kunder för vilka dataintrånget, som associerats med Midnight Blizzard i vintras, har kunnat påverka.

# **Cybersäkerhetscentrets**
# åtgärder och tips för förberedelser

Vi publicerade en ny anvisning om kvantsäkra algoritmer och om övergången till dem.

Vi påminde om att man ska vara beredd för fakturerings- och VD-bedrägerier som kan öka under sommaren. Det effektivaste sättet att skydda sig mot fakturabedrägerier är att i oklara fall säkerställa saken per telefon och genom att använda fakturerarens ursprungliga kontaktuppgifter. Det är också viktigt att påminna sommararbetare och även långvariga medarbetare om det korrekta sättet att hantera inkommande fakturor i organisationen.

Statsrådet har den 27 juni 6024 tillsatt en delegation för nätsäkerhet för en ny mandatperiod. Delegationen för nätsäkerhet har till uppgift att följa utvecklingen av kommunikationsnäten och kommunikationstekniken och tillämpningspraxisen för lagstiftningen om nätsäkerhet samt att stödja myndigheternas beslutsfattande. Delegationens mandattid är 1.7.2024–31.12.2027.

I juni godkände Traficom två sammanslutningar till betrodda anmälare som avvärjer olagligt innehåll på internet speciellt för barn och unga. Statusen beviljades Rädda Barnen rf samt Somis Enterprises Oy som tillhandahåller tjänsten Someturva.

# Allmän översikt över cybersäkerheten i juni

- Via ett konsultbolags system gjorde man i våras tiotusentals ogrundade sökningar i till exempel myndigheters register. Angriparen misstänks ha gjort sökningarna med hjälp av hackade användarnamn till ett bilverkstad och till en bogseringstjänst.
  - Det är fråga om ett så kallat leveranskedjeangrepp.
  - Det är viktigt att upptäcka och hantera leveranskedjeangrepp, inte bara för den egna verksamhetens kontinuitet utan också därför att de har stor betydelse för organisationens anseende och förtroendet i nätverket. Vid leveranskedjeangrepp är både leverantören och kunden offer. För att hantera situationen krävs det ofta öppenhet och samarbete mellan de olika parterna.
  - Nätfiske kan användas för leveranskedjeangrepp.
- Cybersäkerhetscentret har under de senaste tiderna fått ett flertal anmälningar om nätfiske efter Microsoft 365-användarkonton riktat mot organisationer. En del av nätfiske har lett till ett dataintrång i ett e-postkonto.
  - Nätfiske sker med olika, ofta aktuella teman. Ibland kan man för nätfiske även använda sådana teman för vilka objektet väntar på en kontakt, och då ska man vara speciellt uppmärksam för att kunna identifiera nätfiske.
  - Bekanta dig med vår anvisning Gör så här vid dataintrång i ett Microsoft 365-konto.

# Trenderna inom cybersäkerhet
de senaste 12 mån.