TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyberväder

Februari 2025

#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 februari 2025

Dataintrång och dataläckor

- Intrång i M365-konton med meddelanden med Dropbox-tema fortsatte i stor omfattning. Från kapade konton gjordes faktureringsbedrägerier och skickades nya nätfiskemeddelanden.
- Organisationer utsattes för brute force-angrepp, varav några var exceptionellt massiva.
- Facebook-konton kapades genom att fråga efter telefonnummer och bekräftelsekod under förevändning av en tävling på Messenger.

Bedrägerier och nätfiske

- Finländare litar på polisen. Bedragare har utnyttjat detta och skickat bedrägerimeddelanden i polisens namn, ringt samtal där de utgett sig för att vara Europol-tjänstemän och förfalskat textmeddelanden i rättsväsendets namn.
- Bedrägerier i Skatteförvaltningens namn har använts för att försöka komma åt bankkoder.

Skadeprogram och sårbarheter

- Flera anmälningar om Magecart-angrepp mot finländska webbutiker.
- Anmälningar om e-postmeddelanden med bifogade filer som innehåller QR-koder.

Automation och IoT

- De mest sålda IoT-enheterna i Finland uppfyller för närvarande inte alla krav i radioutrustningsdirektivet (RED)[4]. Tillämpningen av direktivet börjar 08/2025.
- IoT-enheter glöms kvar på fältet. En övervakningsplan för lokalerna, dokumentation av livscykeln för installerade enheter samt processer för att upptäcka enheter som inte hör till lokalerna är till hjälp.

Nätens funktion

- I februari observerades fyra funktionsstörningar i allmänna kommunikationsnät.
- En liten minskning kan observeras i antalet anmälda överbelastningsangrepp.
- Överbelastningsangreppen orsakade inga betydande störningar i finländska nättjänster i februari.

Spionage

- APT-grupper som offentligt kopplats till Ryssland använder en nätfiskemetod riktad mot Microsofts molnbaserade e-postkonton, där offret luras att godkänna kopplingen av angriparens enhets-ID till offrets konto, vilket ger angriparen tillgång till kontot.[5] Ryska aktörer har även utnyttjat enhetskoppling vid nätfiske riktad mot Signal-konton.[6]

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Riskhantering är nyckeln till programvarubaserat skydd - och en konkurrensfördel. Säker programvaruutveckling är inte bara ett tekniskt krav, utan den säkerställer kontinuiteten i affärsverksamheten, programvarornas tillförlitlighet och därmed upprätthållandet av kundernas förtroende. Förutseende riskhantering hjälper till att i tid identifiera risker i programvaruutvecklingen och i upphandlingar, vilket minskar reparationskostnaderna och informationssäkerhetshoten.

Cybersäkerhetscentret har fått anmälningar om Magecart-angrepp riktade mot finländska webbutiker, där skadliga tilläggsprogram läggs till i webbutiken eller skadlig kod läggs till i dess källkod. Om du driver en webbutik, se till att skydda dina administratörsuppgifter och uppdatera webbutiken regelbundet. Kontrollera vid behov din webbutik för skadlig kod eller skadliga tilläggsprogram.[8].

Företagens interna nätverksutrustning och certifikat som är synliga från det offentliga nätverket bör granskas regelbundet. Till exempel kan tjänsten Censys användas för att söka efter egna enheter. Resultaten bör beakta hur enheternas certifikat har undertecknats, vilka tjänster som upptäcks och var enheterna är belägna.

Utredning: Satellitbredband erbjuder ett betydande alternativ och en ytterligare resurs för organisationers beredskap för störningar i telekommunikationsnät. En ny utredning av Cybersäkerhetscentret och Försörjningsberedskapscentralen syftar till att ge en översikt över användningen av satellitbredbandsteknologier och -tjänster i beredskapen hos försörjningsberedskapskritiska organisationer. Utredningen kan även användas av andra organisationer som vill använda satellitbredbandsteknologier och -tjänster.[9]

Allmän översikt över cybersäkerheten i februari

- Februaris snöblandade regn orsakades av kritiska sårbarheter i Ivanti Connect Secure och Policy Secure-produkter, vilka möjliggjorde körning av godtycklig kod på sårbara enheter[10]. En allvarlig sårbarhet i Palo Altos PAN-OS-system möjliggjorde att autentiseringen kunde kringgås och kommandon köras på enheterna.[11]
- VD-bedrägerier pågår från adresser med formen *fornamn.efternamn.organisation/domain[at]outlook[.]com.* [12]
  - Finskan som används i bedrägerierna har varit mer felfri än tidigare och de tilltalar ofta mottagaren med förnamn. Bedrägeriet inleds med ett meddelande där mottagaren ombeds göra en tjänst och svara via e-post på grund av situationen. Om man svarar på bedrägerimeddelandet, ber bedragaren offret att köpa presentkort till organisationen som företagsgåvor.
- Nätfiske i myndigheternas namn cirkulerar i stor omfattning:[13]
  - Cybersäkerhetscentret fick i februari flera anmälningar om bedrägerimeddelanden och -samtal i olika myndigheters namn. Målet med bedrägerierna har varit att få offret att lämna ut känsliga uppgifter, som till exempel bankuppgifter. En myndighet ber aldrig om att lämna ut bankkoder eller betalkortsuppgifter per telefon.
  - Äktheten av ett samtal från en myndighet kan verifieras till exempel via myndighetens kundtjänst eller växel. Kontaktuppgifter finns på myndigheternas webbplatser. Olika myndigheter informerar även aktivt på sina webbplatser om bedrägerikampanjer som sker i deras namn. Du kan också läsa om aktuella bedrägerier i Cybersäkerhetscentrets veckoöversikter.
- M365
  - I de M365-dataintrångsfall som Cybersäkerhetscentret fått kännedom om har försök att logga in på användarkontot gjorts till och med inom några minuter efter att användaridentifikationen har matats in på nätfiskesidan. I många fall har faktureringsuppgifter sökts från kontot efter intrånget och försök gjorts att ändra mottagarens kontonummer till bedragarens kontonummer.[14]
  - Även om de flesta fall syftar till ekonomisk vinning, är det viktigt att komma ihåg att användarkonton också kan intressera andra än opportunister. Bland annat har informationssäkerhetsföretagen Microsoft och Volexity rapporterat om en färsk kampanj av en cyberhotsaktör som kopplats till en stat, som syftar till att samla in Microsoft 365-molntjänstuppgifter. Kampanjen har riktats åtminstone mot följande sektorer: statsförvaltningen, ICT- och teletjänstleverantörer, hälso- och sjukvården, försvaret och energibranschen.[15]

Trenderna inom cybersäkerhet
de gångna 12 mån.