TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyberväder

April 2025

Cybervädret april 2025

Dataintrång och dataläckor

- Antalet dataläckor var mindre än i början av året.
- Hackade användarnamn för hotell- och resebokningstjänster, speciellt på Booking.com, användes igen för nätfiske efter betalkortsuppgifter.
- Intrång i M365-koder fortsatte och ATM-nätfiskemeddelanden med Dropbox som tema förekom ofta.

Bedrägerier och nätfiske

- Aktivt nätfiske efter nätbaknskoder. SMS-bedrägerimeddelanden har haft Tullen och Skatteverket som tema, och man har lurat offret att klicka på länkarna till nätfiskesidor.
- Nätfiskebedrägerier har också använts för att skrämma mottagare med en parkeringsbot.
- Användare av mobilcertifikat har blivit utsatta för bedrägeriförsök med avsikt att godkänna okända identifieringstransaktioner.

Skadeprogram och sårbarheter

- Kritisk sårbarhet i SAP NetWeaver programkomponent (CVE-2025-31324) har utnyttjas och bör uppdateras utan dröjsmål.
- En kritisk sårbarhet i Ivanti Connect Secure (CVE-2025-22457) har utnyttjas. Gamla versioner bör uppdateras utan dröjsmål.

Automation och IoT

- För automation och IoT-system medförde april bra vårväder och det rapporterades inte några betydande observationer under granskningsperioden.
- Amerikanska myndigheter publicerade anvisningen "Primary Mitigations to Reduce Unsophisticated Cyber Threats to Operational Technology" den 6 maj.

Nätens funktion

- Det observerades 6 funktionsstörningar i allmänna kommunikationsnät i april, av vilka en var av allvarlighetsklass A (hög).
- Under veckan med region- och kommunval riktade en pro-ryska hacktivistgrupp överbelastningsangrepp mot finska webbsidor, bland annat mot politiska partiers webbsidor. Angreppen hade inte någon betydande inverkan på valens genomförande.

Spionage

- Apple har skickat varningar till sina användare som har blivit spionerade med kommersiella skadliga spionprogram.
- Frankrike kombinerade flera cyberangrepp som landet undersökt med det ryska aktören APT28.
- Polen and Rumänien upptäckte spionage mot statsförvaltningen och den privata sektorn. I spionage användes en sårbarhet i Microsoft.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Traficom publicerade i april en ny anvisning om förfaranden för bedömning och godkännande av informationssystemens informationssäkerhet. Anvisningen är avsedd för myndigheter och företag som behandlar nationellt eller internationellt säkerhetsklassificerad information i elektronisk form.

Skyldigheterna i NIS2-direktivet och cybersäkerhetslagen trädde i kraft i Finland den 8 april 2025. Den nya lagen skapar en mer strukturerad ram för cybersäkerheten i Finland och uppställer samtidigt skyldigheter för samhällets kritiska aktörer gällande cybersäkerhetsincidenter.

Flera sårbarheter har observerats under våren, speciellt i kantdatorsystem. Hantering av sårbarheter är svårt om en organisation inte tillräckligt känner till sin miljö. System bör kartläggas och dokumenteras regelbundet.

Allmän översikt över cybersäkerheten i april

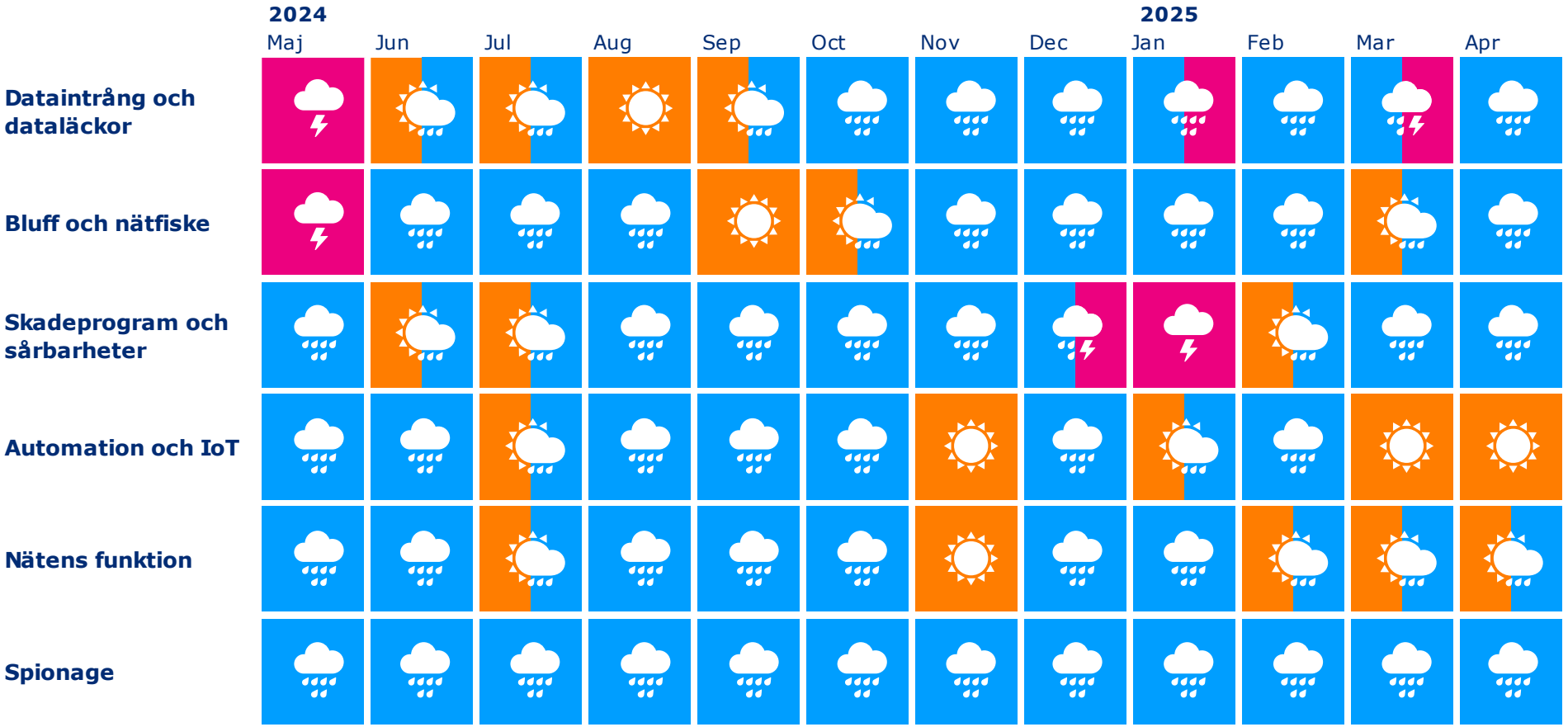
April var en ganska lugn månad med tanke på följande cybersäkerhetsfrågor:

- Kommunal- och välfärdsområdesvalet i början av månaden vaknade den pro-ryska hacktivistgruppen NoName057(16) ur sin vintersömn när finska webbadresser blev på gruppens mållistor. Överbelastningsnagreppen riktades bland annat mot partiers, kollektivtrafikens samt den offentliga och privata sektorns webbsidor. Effekten av angreppen blev dock i sin helhet liten och hade inte någon inverkan på genomförandet av valet.
- Påsken 2025 var i år mycket lung vad gäller cybersäkerhetsobservationer. Organisationer bör dock beakta att helgdagar eller andra betydande evenemang som skiljer sig från den normala rutinen kan öka angriparnas aktivitet.

- Nätfiske var igen på tapeten i cybervädret i april då det gjordes bedrägerier speciellt i namn av banker och hotellbokningstjänster. Nätfiskemeddelanden och -webbplatser är ofta av ganska god kvalitet och några nätfiskeförsök gjordes mot mobilcertifikatet, en tjänst som används för elektronisk identifiering.
  - Angripare kontaktar ofta potentiella offer via textmeddelanden eller WhatsApp. Avsändarens namn har ofta ändrats så att meddelandet verkar komma från en verklig organisation.
  - Temana i bedrägerikampanjer varierar från månad till månad, och sommarsemesterperioden som närmar sig kommer mycket sannolikt att medföra en ökning speciellt i kampanjer som hänför sig till hotell- och bokningstjänster. I en del av bedrägeriförsöken för bokningstjänster har det funnits indikationer om dataintrång mot tjänsten när angripare har kunnat skicka meddelanden via bokningssystemet.
- Kantdatorsystem fortsätter att vara som mål för angripare:
  - Antalet angrepp mot kantdatorsystem som organisationer använder har ökat. Man kan inte nog betona vikten av att snabbt uppdatera utrustningen, eftersom angripare aktivt letar efter sårbarheter i tidigare versioner bland annat i innehållet i publicerade uppdateringar.
- Osäkerheten kring finansieringen av CVE-databasen väckte oro i april. CVE-projektet fick slutligen finansiering för följande 11 månader. Alla nuvarande verktyg för hantering av sårbarheter använder CVE-identifierare.
  - EU:s cybersäkerhetsbyrå ENISA lanserar i mitten av april en betaversion av sin databas European Vulnerability Database (EUVD). Denna databas kommer att tilldela en egen identifierare för sårbarheter och är därmed inte beroende av CVE-identifierare, även om den också använder dem i sin verksamhet. Andra internationella aktörer har också snabbt utvecklat lösningar till situationen.

1 kk

Trenderna inom cybersäkerhet
de gångna 12 mån.



Top 5-hot i den närmaste framtiden (6 månader - 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 man installerar uppdateringen.

2.

Utpressningsprogram - Betydande hot mot organisationer

Under det senaste året har flera organisationer i Finland drabbats av ett utpressningsprogram, och antalet ökar kontinuerligt också globalt.

3.

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

Att förstå underleverantörskedjorna 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 för AI-relaterade utmaningar.

Det skulle vara bra för organisationer att identifiera de utmaningar som artificiell intelligens medför och förbereda sig på dem till exempel genom att utbilda sin personal.

5.

Skyddet av kommunikationsinfrastruktur blir allt viktigare

Skyddet av kommunikations- och systeminfrastruktur är viktigt utomlands och i Finland, både på grund av de skador och naturfenomen som de blir utsatta för samt på grund av avsiktliga störningar orsakade av utomstående.