TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyberväder

Maj 2025

Cybervädret maj 2025

Dataintrång och dataläckor

- I maj var det lugnt med anmälningar om dataintrång på samma sätt som i april.
- Vid intrång i e-postkonton använde man tredje parters e-postapplikationer för att läsa och stjäla meddelanden på hackade M365-konton utan att användaren märkte det.

Automation och IoT

- FBI has varnat om cyberbrottslingar som utnyttjar IoT-utrustning som anslutits till hemnät för kriminell verksamhet med hjälp av botnätet BADBOX 2.0.

Bedrägerier och nätfiske

- Sommarens semesterperiod medför bedrägerier där man uppträder sig som direktör. Se till att sommarvikarierna vet hur de kan känna bedrägeriförsök, för bedragarna gör sina hemläxor omsorgsfullt och hittar på alltid nya trick.
- Kampanjen Var försiktig! erbjuder nu informationssäkerhetsanvisningar också på teckenspråk.

Nätens funktion

- I maj observerades totalt 7 funktionsstörningar i allmänna kommunikationsnät.
- Traditionella överbelastningsangrepp som baserar sig på massiva trafikvolymer är fortfarande allmänna och allt kraftigare.
- Bombmatta, angrepp på applikationsnivå och adaptering av angreppstrafiken för att kringgå de införda skydden är allt vanligare.

Skadeprogram och sårbarheter

- För bedrägerier och nätfiske med olika teman har man använt det skadliga programmet infostealer för att stjäla information. Som ett resultat av lyckade bedrägerier och nätfiskeförsök har dessa typer av skadliga program installerats på målenheten.

Spionage

- Flera västländer har varnat om aktören APT28 som är länkad till Ryssland för dess försök att spionera logistik- och teknologisektorer.
- Nederländerna och Microsoft berättade om den sannolikt Ryssland-länkade aktören Laundry Bear/Void Blizzard som har spionerat bland annat myndigheter.
- Tjeckien har länkat ett spionage mot sitt utrikesministerium med APT31-gruppen och Kina.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Europeiska sårbarhetsdatabasen EUVD (European Union Vulnerability Database) infördes den 13 maj 2025. EUVD erbjuder ett länge efterlängtat alternativ till den amerikanska CVE-databasen vars fortsättning av finansiering har varit osäker under de senaste tiderna.

Den 21 maj publicerade CISA en rapport om cyberspionage och cyberpåverkan mot teknologi- och logistikföretag i länder som stöder Ukraina. Rapporten belyser Rysslands påverkansaktiviteter som började år 2022, samt teknik, taktik och procedurer som enheter under den ryska militära underrättelsetjänsten GRU har använt mot företag i länder som stöder Ukraina.

E-postapplikationer som använts vid intrång i M365-konton begär omfattande åtkomsträttigheter till den hackade e-postlådan. Användarrättigheter som beviljas applikationer bör vara begränsade så att endast administratörer kan godkänna dem.

Det nationella samordningscentrumet för forskning, utveckling och innovation inom cybersäkerhet, som verkar i anslutning till Cybersäkerhetscentret, har beviljats delfinansiering för en fyraårig fortsättningsperiod från EU:s program för ett digitalt Europa. Europeiska kommissionen finansierar projektet med fyra miljoner euro, och nästan hela summan kommer att delas ut som finansieringsstöd till finländska aktörer. Cybersäkerhetscentret ordnar ett öppet webbinarium i juni, där aktuella utsikter för nationellt tillgängliga stödformer och EU-finansieringsmöjligheter för utveckling av cybersäkerhet presenteras.

Allmän översikt över cybersäkerheten i maj

- Början av sommaren har igen aktiverat illvilliga aktörer, speciellt i observationer om bedrägerier och nätfiske. Å andra sidan medförde den gångna månaden även enstaka stormmoln när flera västländer berättade att de hade drabbats av angrepp som kombinerats med statliga cyberhotsaktörer.
  - Mot slutet av månaden observerades nätfiskeförsök som använde adversary-in-the-middle (AiTM)-metoden där tvåfaktrosautentisering kringgås. Observationerna gällde meddelanden och bedrägerier med teman som bank, post, skatt och fordon.
- Sårbarheter i olika digitala apparater är fortfarande ett centralt bekymmer på cybersäkerhetsfältet. När man köper en apparat är det viktigt att fästa uppmärksamhet inte bara vid apparatens egenskaper och livscykel utan också vid tillverkaren.
  - Tv-sändningars övergång till högupplöst format fr.om. den 1 juli även på kommersiella kanaler gäller flera hushåll som ska skaffa en smart-tv-apparat. En del av apparaterna på marknaden kan dock äventyra hushållens informationssäkerhet. Brister i informationssäkerheten har i synnerhet observerats i billiga Android-TV-apparater som säljs av okända tillverkare via nätet. När man fattar ett köpbeslut är det värt att prioritera bekanta och tillförlitliga märken i stället för enbart priset.
  - Hotet som sårbara kantenheter utgör fortsätter att vara betydande. Utnyttjande av sårbarheter i kantenheter, t.ex. Brandväggar och VPN-utrustning har observerats i Europa och globalt — och hotet gäller också finska organisationer. Nätövervakning, snabb uppdatering av programvaran och ersättning av utrustning som nått slutet av sin livscykel med förvaltade produkter är kritiska åtgärder för att undvika hoten.
- AI-applikationer blir allt vanligare bland organisationer och privatpersoner. Cyberbrottslingar har försökt utnyttja den ökande popularitet för dataintrång och spridning av skadliga program.
  - Angripare utnyttjar förfalskade AI-applikationer och webbsidor med dolda skadliga program eller skadlig kod. Skadliga webbsidor avsedda för nedladdning av skadliga program har annonserats till exempel via sociala medier och manipulering av sökmototer. Vid nedladdning av applikationer bör användare alltid överväga deras nödvändighet och tillförlitlighet. För avgiftsfria applikationer lönar det sig i mån av möjlighet att också kontrollera utgivarens tillförlitlighet.

Trenderna inom cybersäkerhet
de gångna 12 mån.