TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyberväder

September 2025

Cybervädret september 2025

Dataintrång och dataläckor

- Från hackade Microsoft-konton skickar man ofta en hel del nya nätfiskemeddelanden vidare.
- I några fall har M365-dataintrång varit långvariga: angriparen håller sig i miljön och kan övervaka situationen på flera månader före användningen av offrets koder för att begå ett faktureringsbedrägeri.
- Man har även gjort dataintrång genom att utnyttja sårbarheter i kantdatorsystem, t.ex. brandväggar och VPN-lösningar.

Bedrägerier och nätfiske

- Blockering av bedrägerisamtal vann brottsförebyggande tävlingen 2025. Genom att blockera förfalskningar har man avvärjt miljontals bedrägerisamtal.
- Dataintrång i Microsoft M365-e-postkonton fortsatte att öka. I september publicerades en allvarlig varning om M365-nätfiske. Dataintrång som begås med hjälp av nätfiske är det vanligaste sättet att göra intrång i företagets system.

Skadeprogram och sårbarheter

- Flera flygplatsers verksamhet lamslogs i Europa till följd av infektionen med ett utpressningsprogram. Som indirekta konsekvenser blev flygförbindelserna till Finland försenade och de omdirigerades.
- Kritiska Cisco ASA- och FTD-sårbarheter har utnyttjats i angrepp världen över.

Automation och IoT

- Vägverket i USA uppmanade till undersökning av vägarnas digitala infrastruktur med tanke på dolda komponenter, t.ex. radio. Det skulle vara möjligt att störa eller spionera användningen av vägar med dold utrustning.
- I Europa skapar cyberresiliensförordningen (CRA) och NIS2-direktivet starka rutiner för hur man ska ingripa i sådana cyberhot som uppstår i leveranskedjorna.

Nätens funktion

- Mot finländska organisationer riktades flera överbelastningsangrepp. Betydande effekter på tjänsternas tillgänglighet undveks. God beredskap och aktiva motåtgärder minskade effekterna.
- Effekterna av överbelastningsangrepp kan också märkas i tjänster som inte är direkta mål. Delade resurser kan bli överbelastade och orsaka störningar i flera tjänster samtidigt.

Spionage

- Aktiviteten i Europa hos Iran-anknutna hotaktörer uppges ha ökat. En APT-grupp rapporterades ha försökt bryta sig in i teleoperatörers system med hjälp av ett rekryteringsbedrägeri, och en annan APT-grupp uppgavs i sin tur ha försökt skaffa information bland annat om organisationer inom satellitbranschen samt från försvarssektorn. Målgrupper fanns bland annat i Storbritannien, Frankrike, Sverige och Danmark.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

Nätfiske efter Microsoft 365-konton har fortsatt aktivt. Med anledning av den betydande ökningen av fallen och den fara som de medför publicerade Cybersäkerhetscentret en varning om fenomenet.

Ett överbelastningsangrepp kan störa affärsverksamheten och bli ett regelbundet problem utan något tillräckligt förutseende. Beredskapen omfattar förberedelser före angreppet, t.ex. administrativa och tekniska åtgärder, reagering under angreppet samt efterbehandlingen. Du kan läsa mer om ämnet i Informationssäkerhet Nu!-artikeln *”Proaktivitet är det bästa försvaret mot överbelastningsangrepp”* (på finska).

I samband med Cybersäkerhetscentrets veckoöversikter behandlas nu som nytt ämne även skadliga program! Översikten över skadliga program är särskilt avsett för läsare som ännu inte är så bekanta med skadliga program.

Allmän översikt över cybersäkerheten i september

Den påbörjade hösten var regnig också på cybersäkerhetsfronten. För antalet incidenter var september en ganska livlig månad, och under den observerades incidenter som fick synlighet i medierna både i Finland och utomlands.

- I Finland syntes överbelastningsangreppen i hotfältet efter mitten av september. Flera angrepp riktades avsiktligt mot webbsidor och organisationer som väckte uppmärksamhet i medierna. De störningar som incidenterna medförde var dock i regel kortvariga. Överbelastningsangreppen är ganska vanliga för flera organisationer och man återhämtar från dem ofta snabbt.
- Nätfiske efter och intrång i Microsoft 365-konton ökar fortfarande. Fenomenet gav också anledning för en varning.

Ett cyberangrepp med omfattande konsekvenser störde europeiska flygplatsers verksamhet fr.om. 19.9.

- Ett utpressningsprogram mot bolaget Collins Aerospace som producerar Check-in- och Boarding-tjänster störde passagerartrafiken åtminstone på Bryssels, Berlins och Heatrhows flygplatser.
- Angreppet medförde flygförseningar och inställda flygningar. En del av flygbolagen lyckades införa alternativa metoder för att betjäna sina kunder, och till exempel boarding-pass upprättades i vissa fall för hand.
- Sammantaget påverkade angreppen flygplatsernas verksamhet i cirka en vecka, med de allvarligaste störningarna under de första dagarna. På Berlin Brandenburg-flygplatsens webbplats informerades ännu den 9 oktober om störningar som orsakats av cyberangreppet.

Trenderna inom cybersäkerhet
de gångna 12 mån.