TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Cyberväder

November 2025

Cybervädret november 2025

Dataintrång och dataläckor

- Varningen som gällde intrång i Microsoft 365-konton togs bort den 27 november 2025. Trots detta har hotet om kontointrång förblivit högt. Multifaktorsautentisering räcker inte ensamt för att avvärja hotet.
- Genom att utnyttja sårbarheter genomfördes dataintrång:
  - Microsoft WSUS Remote Code Execution CVE-2025-59287
  - Adobe Commerce and Magento Open Source CVE-2025-54236
  - ASUS AiCloud - CVE-2025-2492

Automation och IoT

- CRAs genomförandeförordning (EU) 2025/2392 om den tekniska beskrivningen av viktiga och kritiska produkter har publicerats i EUR-lex.
- Multifunktionella botnät som Aisuru ger angripare en bred uppsättning kapabiliteter. Även om botnät kan göras obrukbara förblir enheterna fortfarande sårbara och kan användas för att skapa nya botnät.

Bedrägerier och nätfiske

- Falska nätbutiker fiskar efter konsumenternas pengar i kölvattnet av årets slutreaerbjudanden. Julhandelns kampanjer är populära bland bedragare.
- Lösningen för att förhindra bedrägerisamtal som utvecklats i samarbete mellan Traficom och finländska teleoperatörer vann den europeiska brottsförebyggande tävlingen. Lösningen för att förhindra bedrägerisamtal valdes tidigare i höst också till vinnare i Finlands brottsförebyggande tävling.

Nätens funktion

- De största botnäten som används för överbelastningsangrepp växer ständigt och allt större angrepp rapporteras. Ökningen av osäkra IoT-enheter driver på detta fenomen, och samma utveckling lär fortsätta även i framtiden.
- Microsoft rapporterar att de framgångsrikt har stoppat ett rekordstort överbelastningsangrepp från Aisuru-botnätet på över 15 Tbps, där angreppstrafik skickades från mer än 500 000 källadresser. Aisuru består av kapade hemroutrar och IoT-enheter, såsom övervakningskameror.

Skadeprogram och sårbarheter

- Kritisk och utnyttjad sårbarhet i Fortinet FortiWeb-produkten (CVE-2025-64446)
- Den andra vågen av det skadliga programmet Shai-Hulud har i stor utsträckning infekterat npm-paket och samlat in autentiseringsuppgifter samt känslig information från system som använder dem. Organisationer bör granska sin utvecklingsinfrastruktur för misstänkta tecken.
- Det skadliga programmet Magecart som gömts i komprometterade nätbutiker stjäl kundernas kortuppgifter.

Spionage

- Cyberhotaktörer utnyttjar fortfarande både redan kända och nya sårbarheter vid dataintrång som riktas mot nätverksenheter. I november riktades intrång bland annat mot Cisco-enheter.
- En dataläcka kopplad till en iransk cyberaktör avslöjade detaljer om gruppens verksamhet.
- I rapporteringen kopplad till Iran framkom även ett intresse för bland annat försvarsindustrin och flygbranschen.

Cybersäkerhetscentrets
åtgärder och tips för förberedelser

OWASP, som kartlägger säkerhetshot mot webbapplikationer, håller på att uppdatera sin Top 10-lista. I den nya listan förändras både rubrikerna och hotens placeringar något. Hot kopplade till leveranskedjor är också på väg att inkluderas som en ny kategori.

Risken för digital skimming ökar inför stora reor och högtider. Vid digital skimming installerar brottslingar skadlig kod i nätbutiker och stjäl därigenom uppgifter som lämnas under betalningsprocessen. Även om Black Friday redan är förbi bör risken beaktas vid julklappsinköp. Läs mer i Informationssäkerhet Nu- artikeln *”En osynlig tjuv i din nätbutik – digital skimming kan få betydande ekonomiska konsekvenser”* (på finska).

Vi publicerade en artikel i serien Informationssäkerhet Nu! om administratörskonton i molntjänster i början av december. Läs tips om hur du skyddar huvudadministratörskonton i artikeln
”Hantering av huvudadministratörskonton för molntjänster – bästa praxis”.

Allmän översikt över cybersäkerheten i november

Cybersäkerhetsläget i november var överlag regnigt, men samtidigt ganska lugnt. Under månaden observerades några anmärkningsvärda fenomen i Finland och världen.

I de rapporter som anmäldes till Cybersäkerhetscentret omfattade angrepp med ClickFix-teknik och skadeprogrammet Shai-Hulud 2.0. Det finns fortfarande observationer av skadeprogrammet BadBox 2.0 som blev vanligare under sommaren.

- I ClickFix-angrepp luras internetanvändare att köra den skadliga programvaran på sin enhet. I angreppsmetoden imiteras små uppgifter av typen ”Bekräfta att du är människa” och CAPTCHA-kontroller, vilka användare är vana vid att lösa i samband med vardaglig webbsurfning.
- Shai-Hulud 2.0 är en datormask som sprider sig i utvecklingsmiljöer. Masken har spridit sig mycket snabbt och den har infekterat flera populära npm-paket. Dessa har omfattat en hel del paket som publicerats av Zapier, ENS, Domains, PostHog och Postman. Nya paket som innehåller en skadlig kod identifieras kontinuerligt. I Finland har man gjort några anmälningar om det skadliga programmet.

Ökningen av dataintrång som riktats mot Microsoft 365-konton avtog i november och i början av november vi tog bort den allvarliga varningen som varit i kraft sedan september. Antalet M365-rapporter om dataintrång har tills vidare återgått till augustinivån, men hotet som är kopplat till fenomenet har inte försvunnit.

Det förekom en internationell störning i CloudFlares tjänster den 18 november, vilket påverkade tillgängligheten för flera populära tjänster. Störningen märktes ganska brett bland vanliga internetanvändare, eftersom den tillfälligt hindrade användningen av till exempel X och ChatGPT.

Trenderna inom cybersäkerhet
de gångna 12 mån.