

Tekoälyn vaikutus tietoturvaan

25.11.2026

Viime aikoina erilaiset ohjelmisto- ja käyttöjärjestelmäpäivitykset ovat lisääntyneet merkittävästi. Osa päivityksistä joudutaan myös asentamaan käyttäjille pakotetusti, koska ne sisältävät kriittisiä tietoturvakorjauksia.

Hyvä esimerkki tästä on noin kuukauden takainen PHP-haavoittuvuus. Haavoittuvuudet olivat niin vakavia, että korjaavat päivitykset tuli asentaa viipymättä. Meillä SEAMKissa tämä näkyi esimerkiksi siinä, että Moodlen ylläpitäjä Mediamaisteri joutui ilmoittamaan ympäristön alasajosta noin puolen tunnin varoitusajalla. Tämän lisäksi useat SEAMKin ja SEDUn asiantuntijat joutuivat etsimään ja päivittämään paikallisia PHP:ta hyödyntäviä järjestelmiä välittömästi päivitysten ilmestymisestä. Mutta jo tieto siitä, että haavoittuvuus on olemassa, se on vakava ja kohtuullisen helposti hyödynnettävissä aiheutti kansallisestikin sitä, että järjestelmiin jouduttiin rajoittamaan pääsyä, kunnes varsinainen päivitys tuli saataville ja saatiin asennettua.

Päivitystarve ei koske pelkästään työasemia ja palvelimia. Myös henkilökunnalla käytössä olevat SEAMKin hankkimat puhelimet ja muut laitteet tulee pitää ajan tasalla. Viimeaikainen esimerkki mobiililaitteisiin kohdistuvista uhkista on osuvasti nimetty *SMS of Death* -haavoittuvuudeksi. Haavoittuvuuden avulla voidaan käytännössä häiritä vanhoja Android-versioita tai pahimmassa tapauksessa jumittaa puhelin niin että se joudutaan palauttamaan tehdasasetuksiin.

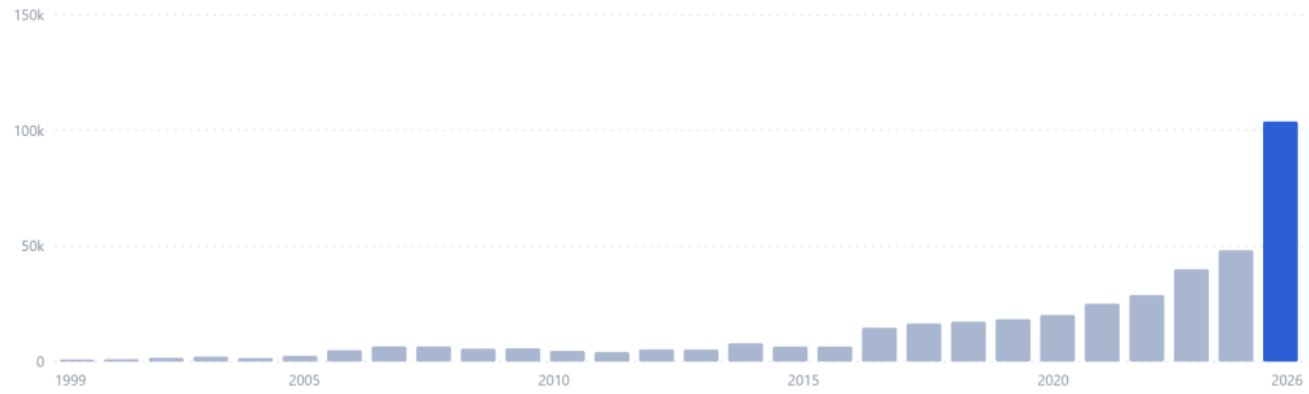
Käyttäjän oma vastuu laitteistaan ja niiden ajantasaisuudesta korostuu jatkuvasti. Tietohallinto pystyy hallitsemaan päivityksiä tiettyyn pisteeseen asti, mutta esimerkiksi pitkään pöytälaatikossa ollut puhelin voi olla useita päivityksiä jäljessä.

Tietoturva ei myöskään ole ilmaista. Tässä tulee väistämättä vastaan peiliin katsomisen paikka meille kaikille: organisaatio voi käyttää tietoturvaan paljon rahaa ja resursseja, mutta yksikin huolimaton toiminta voi heikentää suojausta merkittävästi. Tekniikka ja palvelut eivät siis yksin ratkaise tietoturvaa.

Kirsikkana kakun päällä on ystävämme tekoäly, jonka merkitys tietoturvassa on kasvanut kuluvan vuoden aikana voimakkaasti. Siinä missä tavallisessa toimistotyössä pohditaan, miten Copilotista saisi enemmän hyötyä, tietoturvan puolustavalla ja hyökkäävällä puolella tekoälyä käytetään jo haavoittuvuuksien löytämiseen, analysointiin sekä niiden hyväksikäytön ja korjausten kehittämiseen. Usein ammattilaiset käyttävät vieläpä monia kielimalleja joko rinnan tai peräkkäin löytääkseen haavoittuvuuksia mahdollisimman tehokkaasti.

Haavoittuvuuksia tunnistetaan yleisesti kansainvälisellä CVE-järjestelmällä (Common Vulnerabilities and Exposures). Se on tietoturvahaavoittuvuudelle luotu yksilöllinen tunniste. Tämän lisäksi käytetään CVE-tunnisteen yhteydessä CVSS-pisteytystä (Common Vulnerability Scoring System), joka kertoo kyseisen haavoittuvuuden vakavuuden asteikolla 0–10. Vuosien saatossa löydettyjen haavoittuvuuksien määrän kehityksen voi nähdä alla. Tänä vuonna on siis löydetty jo kaksinkertainen määrä haavoittuvuuksia viime vuoteen verrattuna ja vuotta on vielä jäljellä.

Taulukko 1. Löydetyt CVS-tunnisteen saaneet haavoittuvuudet.



Hyvä esimerkki tekoälyn tehokkuudesta tietoturvassa on aiemmin mainittu PHP2Shell. Haavoittuvuuksien taustalla oleva koodi oli ollut olemassa yli vuosikymmenen, mutta käytännössä toimivan hyväksikäyttötavan rakentaminen oli erittäin vaikeaa. Haavoittuvuuden löytäjän Wiz Researchin mukaan tekoäly muutti juuri tätä asetelmaa: monimutkaisten haavoittuvuuksien tutkiminen, testaaminen ja hyväksikäyttömenetelmien sovittaminen eri ympäristöihin nopeutui merkittävästi.

Tämä on tietoturvan kannalta merkittävä muutos. Jos tekoäly helpottaa puolustajien työtä, sama koskee myös hyökkääjiä. Aiemmin liian vaikeana tai työläänä pidetty haavoittuvuus voikin tekoälyn avulla muuttua käytännössä hyödynnettäväksi. Lisäksi se madaltaa huomattavasti osaamistasoa aiheuttaen sen, että henkilöt, jotka eivät välttämättä aiemmin osanneet näitä löytää tai hyödyntää saattavat nyt pystyä siihen tekoälyn avustuksella.

Tietohallinnossa tämä kaikki tarkoittaa jatkuvaa tasapainottelua kustannusten,

käytettävyyden ja turvallisuuden välillä

SEAMKissa ollaan nyt ensimmäistä kertaa ottamassa käyttöön CSOC-palvelua, joka antaa uudenlaista näkyvyyttä ympäristössä tapahtuviin tietoturvapoikkeamiin ja mahdollistaa niihin reagoinnin myös normaalin työajan ulkopuolella. Autuaaksi sekään ei tee, mutta se antaa hieman enemmän mielenrauhaa iltoihin, viikonloppuihin ja loma-aikoihin. Jostain syystä juuri ne tuntuvat olevan myös suosittuja ajankohtia kolkutella organisaatioiden järjestelmiä. Tästäkin löytyy hyvä esimerkki keväällä tapahtuneesta tunkeutumisesta, minkä seurauksena perjantaina työajan päättymisen jälkeen 7 asiantuntijaa selvitti alle 15 minuutin tunkeutumisen vaikutuksia yhden käyttäjän sähköpostiin iltakymmeneen asti.

Vahva oletukseni on, että olemmekin astumassa uuteen tekoälyn aikakauden normaaliin missä yksittäisen käyttäjän rooli tietoturvan yhtenä lenkkinä korostuu entisestäänkin. Muistakaa käydä suorittamassa pakollinen tietoturvakoulutus ja ottakaa yhteyttä rohkeasti, jos epäilette tietoturvapoikkeamaa. Siksi me olemme täällä. Tietoturva ei katso aikaa eikä paikkaa.

Tero Hakola
Digipalvelupäällikkö
SEAMK

Kirjoittaja toimii digipalvelupäällikkönä SEAMKin tietohallinnossa.

Lisätietoja

- Kriittisiä haavoittuvuuksia PHP:ssa | Traficom
- Ilta-Sanomat / Digitoday: SMS of Death
- Wiz Research: PHP2Shell
- CVE: Common Vulnerabilities and Exposures
- Common Vulnerability Scoring System SIG