Mythos nie je zázračný hackovací robot, ale magické zkradlo

21.7.2026 - Martin Lohnert | SOITRON

Odkedy spoločnosť Anthropic predstavila Mythos a projekt Glasswing, môže sa zdať, že polovica internetu už vidí neodvratnú tsunami 0-day zraniteľností a druhá polovica rovno apokalyptický koniec kybernetickej bezpečnosti ako takej. Model, ktorý nikto z nás zatiaľ nemal v rukách, sa stal strašiakom roka. A ako to pri takýchto oznámeniach býva, niekde medzi neobmedzeným nadšením a panikou sa stratil zdravý rozum.

Mythos nie je hackerský zázrak, ktorý cez noc zmenil pravidlá hry. Áno, dokáže autonómne hľadať zraniteľnosti a reťaziť exploity rýchlejšie, než by to zvládol tím skúsených výskumníkov, ale nevymýšľa nové vektory útoku. Nachádza tie isté kategórie chýb, ktoré poznáme, analyzujeme a vieme opraviť už roky. Mení sa rýchlosť a objem, nie podstata.

Skutočné úzke miesto nikdy nebolo v hľadaní chýb, ale v ich oprave. Väčšina zraniteľností zostáva neopravená mesiace či roky po vydaní záplaty, nie z neznalosti, ale pre chýbajúce procesy, ľudí, čas a priority.

Preto je Mythos skôr zrkadlo než hrozba: firmám so zodpovedným prístupom dá náskok, tým, ktoré bezpečnosť zanedbávajú, len zvýši cenu nahromadeného dlhu. Rozhodujúca sa stáva detekcia a reakcia – schopnosť zachytiť problém dosť skoro, aby ste naň stihli reagovať.

V článku nájdete aj 4 otázky, podľa ktorých zistíte, či je vaša firma na túto éru pripravená.

Inovácia hodná pozornosti

Mythos dokáže (údajne) autonómne hľadať zraniteľnosti a hlavne reťaziť „exploity“, vďaka čomu v testoch zvládol cez noc to, čo by tímu skúsených výskumníkov trvalo týždne. Nie je to málo a bolo by chybou to zľahčovať. Ale povedzme si aj to druhé: nie je to zázračný hackovací robot, ktorý zo dňa na deň zmenil pravidlá hry.

Prečo? Lebo zraniteľnosti, ktoré takýto nástroj nájde, spadajú prevažne do tých istých kategórií, aké už roky poznáme, analyzujeme a vieme ošetriť. Mythos nevymýšľa nové vektory útoku. Áno, môže zásadne zmeniť rýchlosť a objem v akom sú zraniteľnosti odhalené. Zmenšuje aj časové okno medzi odhalením chyby a jej zneužitím. Útočníkov tak môže byť viac a budú rýchlejší. Ale stále budú útočiť na to isté.

Navyše, úzke miesto ani dosiaľ nebolo v hľadaní chýb. Bolo a stále je v ich oprave.

Patch management ako priorita?

Väčšina zraniteľností ostáva nezaplátaná mesiace či roky po tom, čo výrobca vydal opravu. Nie však preto, že by ste o nich nevedeli. Ale preto, že na to nie sú procesy, ľudia, čas či priority.

Nástroj, ktorý rýchlejšie nájde viac chýb, na podstate tohoto problému nič nemení. Len ho ešte viac zvýrazní, ak na vašej strane „patchovanie“ viazne.

Ak ste však bezpečnosť brali vážne aj doteraz a pravidelne „patchujete“, rozumne segmentujete, zálohujete, monitorujete a máte ešte aj pripravený dobrý plán reakcie na incident, tak sa pre vás v zásade nemení nič. Áno, budete pod väčším časovým tlakom. Áno, detekcia a reakcia budú dôležitejšie než kedykoľvek predtým. Ale základy, na ktorých celé odvetvie kybernetickej bezpečnosti stavia, fungujú ďalej.

Houston, we have a problem

Problém nastáva, ak ste bezpečnostnú „hygienu“ doteraz zanedbávali. Ak žijete s deravými systémami, plochou sieťou, starým antivírusom a bez akéhokoľvek dohľadu. Doteraz vás možno chránilo len to, že útočníci si vyberali väčšie ryby. To sa teraz vďaka AI a lepšej automatizácii na strane útočníkov môže zmeniť. A vy si poviete: „Houston, we have a problem.“

Čo sa naozaj posúva, je hodnota detekcie a reakcie. Keď útočník dokáže premeniť zraniteľnosť na funkčný „exploit“ za hodiny namiesto týždňov, prevencia sama nestačí – pretože časové okno, v ktorom záplatu nemáte k dispozícii (lebo ešte neexistuje), bude väčšie.

Rozhodujúce tak bude, či vo svojej infraštruktúre v reálnom čase vidíte, čo sa deje a či dokážete podozrivú aktivitu zachytiť a zastaviť skôr, než spôsobí väčšiu škodu.

Mythos je zrkadlo

Lebo nástroj ako Mythos nie je hrozba sám o sebe. Je to zrkadlo. Bez filtrov ukáže, ako na tom naozaj ste. Firmám so zodpovedným prístupom dá náskok, ktorý vedia využiť na rýchlejšiu remediáciu.

No tým, ktoré bezpečnosť zanedbávajú, zvýši cenu nahromadeného dlhu. Navyše, technológia nie je všeliekom, a tak situáciu nevyrieši kúpa ďalšej licencie či „krabice.“ Najväčším rizikom zostáva to, čo ním bolo vždy – organizácie, ktoré bezpečnostné opatrenia odkladajú dovtedy, kým sa niečo nedeje.

Pozornosť preto nepatrí len inováciám ako Mythos, ale stále najmä základným otázkam: vie vaša organizácia, čo má chrániť? Má nasadené a konzistentné bezpečnostné základy? Dokáže prípadný problém zachytiť dosť skoro na to, aby naň stihla reagovať? A je jasné, kto má v prípadnej kríze čo robiť?

Tam, kde na tieto otázky existujú odpovede, nepredstavuje éra umelej inteligencie dôvod na paniku. Tam, kde chýbajú, nie je na vine žiadny nový model – Mythos iba zviditeľnil to, čo vo firmách existovalo celý čas.

https://www.soitron.sk/mythos-nie-je-zazracny-hackovaci-robot-ale-magicke-zkradlo