Tisíce bezpečnostních děr odhaleny včas. Citadelo ochránilo desítky firem před útoky hackerů

25.4.2025 - | PROTEXT

"Na první pohled může působit znepokojivě, že náš tým v uplynulém roce objevil tolik děr v systémech našich klientů. Já to ale vidím jinak - dokázali jsme odhalit tisíce slabin dřív, než je mohli zneužít skuteční hackeři," říká Tomáš Zaťko, CEO společnosti Citadelo. "Počet kritických zranitelností navíc klesl o 30 %. To je jasným důkazem, že jedině pravidelné testování zajistí firmám z nejrůznějších odvětví větší obranu proti kybernetickým útokům."

Nejčastěji testovanou a zároveň nejzranitelnější kategorií byly v roce 2024 webové aplikace, které tvořily více než polovinu všech projektů (53 %). Následovalo rozhraní API (10 %), interní infrastruktura (8 %), mobilní aplikace (7 %) a cloudová prostředí (7 %), které se rovněž ukázaly jako časté zdroje slabin.

Významným trendem bylo také rozšíření o testování velkých jazykových modelů (LLMs). Tyto pokročilé AI technologie přinášejí revoluci v komunikaci, programování i analýze dat a zároveň zásadně proměňují dnešní svět. Jejich využívání však zároveň otevírá nové bezpečnostní hrozby – například v podobě manipulace vstupních požadavků (prompt injection) či záměrného ovlivnění trénovacích dat.

Klíčové statistiky z roku 2024:

- 9 nových projektů týdně

- 6 zranitelností je průměrný počet nalezený v každém testovaném projektu

- 28 % testovaných projektů obsahovalo alespoň jednu kritickou zranitelnost

- 62 % testovaných projektů mělo vysoké riziko, 95 % střední závažnost

Citadelo se rovněž soustředilo na testování **sociálního inženýrství**, které simuluje nejčastější útoky na lidský faktor v organizacích - například phishing (podvodné e-maily), vishing (manipulativní telefonáty) či smishing (škodlivé SMS zprávy). **Právě tyto typy útoků zůstávají jedním z nejrozšířenějších a přesto nejpodceňovanějších.** "*Naše interní data ukazují, že u organizací testovaných poprvé došlo k prolomení zabezpečení až ve 40 % případů. Díky pravidelnému školení a testování lze ale toto číslo udržet na jednociferných hodnotách,*" uvedl Zaťko.

Z hlediska odvětví dominoval sektor **bankovnictví a financí**, který tvořil přes 56 % všech projektů. Následovaly společnosti z oblasti systémové integrace, telekomunikací, softwarového vývoje a energetiky.

Závěry reportu podtrhují nutnost pravidelného, komplexního a odborně vedeného testování – nejen pro splnění regulatorních požadavků, ale především pro ochranu dat, důvěry zákazníků a samotného fungování podniků v digitální době.

Trendy a výhled pro rok 2025:

Threat-Led Penetration Testing (TLPT) bude v roce 2025 jedním z nejvýznamnějších trendů v oblasti kybernetické bezpečnosti, zejména ve vysoce regulovaných odvětvích, jako je finanční sektor. Citadelo je připraveno podpořit velké instituce v implementaci tohoto pokročilého přístupu, který vychází z reálných hrozeb a rámců jako TIBER-EU, a pomoci jim zajistit obranu na nejvyšší úrovni. "*Jedním z klíčových témat letošního roku bude Threat-Led Penetration Testing – komplexní testy pro největší bankovní instituce v EU, kde kybernetický útok může znamenat ohrožení celého finančního trhu. My jsme na tuto výzvu připraveni,*" dodává Zaťko.

Kompletní Ethical Hacking Report 2024 najdete zde.

O společnosti Citadelo

Společnost Citadelo se od roku 2013 specializuje na etický hacking a patří k předním hráčům v oblasti kybernetické bezpečnosti v Evropě. Pomáhá firmám identifikovat bezpečnostní slabiny dříve, než je zneužijí skuteční útočníci – prostřednictvím penetračních testů, bezpečnostních auditů, školení zaměstnanců a pokročilých simulací útoků (red teaming). Citadelo má kanceláře v Bratislavě, Praze a švýcarském Zugu a důvěru jí svěřili klienti napříč odvětvími, včetně firem z žebříčku Fortune 500. Od roku 2023 je součástí skupiny Boltonshield AG.

https://www.ceskenoviny.cz/tiskove/zpravy/tisice-bezpecnostnich-der-odhaleny-vcas-citadelo-ochranilo-desitky-firem-pred-utoky-hackeru/2665539