Citadelo zveřejnilo Ethical Hacking Report 2023. U klientů objevilo nejvíce zranitelností v historii

12.3.2024 - | PROTEXT

Etičtí hackeři v průměru odhalili v každém projektu více než 7 zranitelností, které se dělí do 4 kategorií podle míry závažnosti. Kritických, tedy těch s nejvyšší mírou rizika zneužití, objevili etičtí hackeři celkem 192, což je nejvíce od založení společnosti. "Zranitelnosti s vysokým a kritickým dopadem představují přímé a akutní riziko a musí být neprodleně odstraněny. Drtivý dopad na chod systémů či celé organizace nemá potenciálně pouze jediná kritická zranitelnost, ale i vícero těch méně závažných, které útočník zřetězí do neméně destruktivní kombinace, kterou zneužije. V extrému až ke kompletnímu převzetí moci nad cílovým systémem společnosti," řekl Vojtěch Sláma, country manažer pro Českou republiku.

Nalezené typy zranitelností mohou typicky vést např. k Remote Code Execution - vzdálenému spuštění škodlivého kódu, eskalaci privilegií nebo dosažení ultimátního cíle při simulaci útoku na IT infrastruktury firem, získání role doménového administrátora, s jehož oprávněními útočník přebírá kontrolu nad celou sítí.

U webů je velmi ohrožující možností zranitelnost "SQL injection", kdy útočník využije bezpečnostních nedostatků k proniknutí do databázové vrstvy webové aplikace prostřednictvím vložení vlastního SQL příkazu. SQL je programovací jazyk sloužící k manipulaci s daty v relačních databázích, které často obsahují citlivé informace, jako jsou například přístupové údaje uživatelů.

Nejčastěji se takový útok provádí prostřednictvím neošetřených vstupních formulářů. Útočník může do takto nezabezpečeného přihlašovacího formuláře na internetovém obchodě vložit SQL příkaz, který mu umožní volně zapisovat (injektovat) do databáze. Jinými slovy, útočník má možnost manipulovat s daty uloženými v databázi, což může způsobit vážné dopady na chod a provoz aplikace, jejího serveru a nakládání s citlivými údaji uživatelů. Experti společnosti se zaměřili také na prověřování lidského faktoru, na který nejčastěji míří vektory útoků hackerů, které využívají metody sociálního inženýrství, jako vishing, phishing a smishing. Ty jsou velmi rizikové jak pro jednotlivce, tak pro firmy ve kterých pracují. Efektivitu těchto útoků dokumentují i interní nezveřejněné statistiky společnosti. Úspěšnost simulovaných útoku, které Citadelo v loňském roce provedlo využitím těchto technik, je až 40%. Skoro každá druhá oběť v nově testovaných společnostech tak podlehla nástrahám etických hackerů. "*Proto klientům poskytujeme pravidelná a důkladná bezpečnostní školení, na kterých jim kromě samotné teorie, ukazujeme také praktické ukázky různých hackerských technik, aby se dokázali co nejlépe bránit,*" popisuje důležitost prevence Sláma.

Velký počet nalezených zranitelností poukazuje na nezbytnost komplexního penetračního testování a posouzení bezpečnosti. Zejména v současném době, kdy se četnost a sofistikovanost kybernetických útoků neustále zvyšuje a stále více míří na komerční průmyslový sektor, telekomunikace a dopravu. Potvrzují to i nároky nové evropské legislativy DORA a NIS2. "*Tyto nařízení zásadním způsobem rozšiřují povinnosti firem, které budou muset kybernetickou bezpečnost bezodkladně řešit. Penetrační testy jsou účinným nástrojem, které pomohou tyto nové, zákonem stanovené normy dodržet, a zároveň jim pomoci účinně chránit své klienty, zaměstnance i infrastrukturu,*" dodal Sláma.

https://www.ceskenoviny.cz/tiskove/zpravy/citadelo-zverejnilo-ethical-hacking-report-2023-u-klientu-objevilo-nejvice-zranitelnosti-v-historii/2491731