Penetračné testy desktopových aplikácií

AEC

Uchovajte firemné údaje a dáta svojich klientov v bezpečí

Či už ide o krabicové riešenie tretej strany alebo výsledok vlastného vývoja, bezpečnosť je v prípade desktopových aplikácií zásadná, pretože obvykle majú prístup ku kritickým firemným dátam. Pri desktopových aplikáciách sa nebojíme ísť s pomocou dekompilácie až na úroveň zdrojového kódu vrátane jeho úprav, s cieľom identifikovať z pohľadu bezpečnosti rizikové miesta, citlivé dáta alebo iné nedostatky v autorizácii či samotnom prenose medzi klientskou aplikáciou a serverom.

www.aec.sk

Penetračné testy a audity:

Desktopových aplikácií

Vykonávame penetračné testy už kompilovaných binárnych aplikácií, písaných v ľubovoľnom jazyku voči bezpečnostným štandardom a odporúčaniam v celom rade oblastí majúcich dopad na bezpečnosť samotnej aplikácie a citlivých dát, s ktorými pracuje.

Úroveň preverenia je komplexná s cieľom identifikovať slabé miesta či priame zraniteľnosti. Oblasti pokrývajúce bezpečnosť desktopových aplikácií možno zjednodušene definovať takto:

- chyby validácie používateľských vstupov,
- nedostatky v riadení prístupov,
- slabiny autentizácie a session managementu,
- výskyt Buffer Overflow zraniteľností,
- možnosti injektáže vlastného kódu,
- nedostatočne ošetrené chybové stavy,
- nedostatky v bezpečnosti ukladania a prenosu dát,
- záťažové testy (Denial of Service),
- ostatné chyby konfiguračného charakteru.

Zdrojových kódov

Kontrolujeme zdrojové kódy aplikácií a asistujeme našim zákazníkom pri vývoji bezpečných aplikácií.

Penetračné testy desktopových aplikácií

Penetračné testy desktopových aplikácií sú v porovnaní s penetračnými testami webových aplikácií v mnohých ohľadoch pomerne špecifické. Vyžadujú komplexné znalosti tak z oblasti bezpečnej autentizácie, autorizácie prístupov a práce s citlivými dátami, ako aj hlboké znalosti programovacích jazykov vrátane assemblera, práce v dissambleri, debuggeri s priamym použitím kódov inštrukčnej súpravy (tzv. opcodes).

Výsledkom je overenie, či je aplikácia bezpečná, vhodná pre produkčné nasadenie a netrpí žiadnou zjavnou bezpečnostnou slabinou, ktorá by mohla predstavovať priame bezpečnostné riziko tak pre samotnú aplikáciu, jej používateľov, ako aj samotné dáta.

Nasleduje podrobnejší výpočet oblastí, ktoré bývajú z pohľadu bezpečnosti desktopových aplikácií aj na základe našich dlhoročných skúseností, kritické. Uvedený výpočet nie je kompletný, no podáva zreteľnejšiu predstavu o rozsahu a komplexnosti penetračných testov desktopových aplikácií, či už ide o vlastné vyvíjané riešenie alebo riešenie tretej strany, ktoré sa chystáte do svojho prostredia nasadiť. Radi vám s riešením bezpečnosti pomôžeme.

Kritické oblasti pre bezpečnosť desktopových aplikácií

- Aplikácia ukladá citlivé dáta v nešifrovanej podobe,
- vytvorené súbory majú priradené vysoké prístupové práva,
- nedostatočná kontrola vstupov na strane servera,
- zraniteľnosti komunikačnej brány,
- možné DoS testy komunikačnej brány,
- citlivé údaje sú posielané cez nešifrovaný komunikačný kanál,
- SSL/TLS nedostatky (verzie, algoritmy, dĺžky kľúčov, validita certifikátov),
- je použitý proprietárny komunikačný protokol,
- nedostatky vzájomnej autentizácie kanála,
- dlhé timeouty čakania na odpoveď servera,
- nedostatočná kontrola klientskych vstupov,
- možnosti obídenia autentizačnej schémy,
- absencia použitia viacfaktorovej autentizácie,
- možnosti brute-force útoku na autentizačné údaje,
- slabá politika hesiel,
- spustiteľné súbory nie sú podpísané,
- session tokeny nie sú generované s dostatočnou entropiou,
- dlhé trvanie používateľskej relácie,
- absencia automatického odhlásenia pri neaktivite,
- citlivé informácie ukladané v cache pamäti,
- ukladanie citlivých informácií do logov súborov,
- kryptografia použitá pri ukladaní dát nie je bezpečná,
- spustiteľný kód obsahuje citlivé údaje,
- citlivá business logika nachádzajúca sa v programe,
- vývojárske komentáre v súboroch programu,
- nie sú použité žiadne obfuskátory kódu,
- v pamäti sa nachádzajú citlivé dáta,
- nedostatky business logiky aplikácie.

Analýzy zdrojových kódov

- Kombinácia statickej analýzy pomocou automatizovaných nástrojov a manuálnej revízie kódu,
- jazyky JAVA, C#, prípadne iné, na otázku.

Naše prednosti

- Patríme medzi zavedené české security firmy, na trhu úspešne pôsobíme už dlhšie než 30 rokov.
- Máme viac než 15 rokov skúseností na poli bezpečnosti desktopových aplikácií.
- Náš tím tvoria špecialisti so skúsenosťami zo stoviek čiastkových projektov.
- Sme držiteľmi certifikácií eMAPT, CISSP, OSCP, OSCE, CEH a celého radu ďalších.
- Prevádzkujeme vlastné hackerské laboratórium na výskum v mnohých oblastiach zaoberajúcich sa bezpečnosťou rôznych riešení.
- Načúvame klientom a prispôsobujeme testy ich potrebám a časovým možnostiam.
- Sledujeme moderné trendy v oblasti bezpečnosti desktopových aplikácií.
- Pri testovaní kladieme dôraz na manuálny prístup, ktorý vedie k odhaleniu väčšieho množstva chýb najmä v business logike aplikácií oproti automatizovaným nástrojom.

Bratislava – AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283
Praha – AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
Brno – AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466