axians

The best of ICT with a human touch

PENETRAČNÉ TESTOVANIE

Penetračné testovanie chráni vaše podnikanie a zabraňuje finančným stratám a stratám na reputácii.

My a penetračné testovanie

- 60+ testov (ročne)
- 10+ senior testerov
- Skúsenosti s testovaním OT
- Podpora v 23 krajinách
- PTaaS

Typy testovania a služieb

- **Externé** penetračné testovanie
- **Interné** penetračné testovanie
- **Testovanie webových** aplikácií, testovanie API
- **Testovanie plnohodnotných** aplikácií
- **Testovanie bezdrôtových** sietí
- Penetračné testovanie **mobilných aplikácií**
- **Poskytovanie informácií** z otvorených zdrojov (OSINT)
- **Phishingová kampaň**
- **Red/Purple Teaming**

Aké sú hlavné výhody?

- Posúdenie úrovne vystavenia spoločnosti bezpečnostným hrozbám a zraniteľnostiam
- Overenie účinnosti bezpečnostných kontrol a bezpečnostných procesov
- Prispievanie k vypracovaniu plánu na zlepšenie bezpečnosti a riadenie rizík
- Podpora dosiahnutia cieľov v oblasti dodržiavania bezpečnostných predpisov
- Zníženie rizika finančných strát a zvyšovanie dôvery vašich zákazníkov

Externý penetračný test

simuluje anonymného útočníka z internetu. Testuje zabezpečenie perimetra siete a identifikuje miesta zraniteľnosti v ďalších systémoch zákazníka, ktoré sú prístupné z internetu. Rozsah testu môže byť presne definovaný zákazníkom (napr. IP rozsah) alebo môže zahŕňať tzv. analýzu otvorených zdrojov (OSINT).

Interný penetračný test

sa zameriava na internú sieť, ktorá nie je priamo prístupná z internetu. Simuluje útok z pohľadu útočníka, ktorý získal prístup do internej siete (napr. prostredníctvom malvéru v prílohe e-mailu alebo môže ísť o útok bežného zamestnanca alebo dodávateľa). Testerom sa môže poskytnúť vzdialené pripojenie prostredníctvom siete VPN alebo testovanie prebieha priamo u zákazníka. Testeri môžu mať k dispozícii aj bežné doménové konto používateľa, aby bolo možné čo najlepšie simulovať útok používateľa alebo škodlivého softvéru spusteného na bežnej používateľskej stanici.

Penetračný test bezdrôtovej siete

simuluje útok na siete Wi-Fi. Overuje bezpečnostné mechanizmy používané na ochranu údajov pred neoprávneným prístupom prostredníctvom siete Wi-Fi. Testovanie môže zahŕňať pokusy prelomenia hesla alebo audit izolácie bezdrôtovej siete od zvyšku infraštruktúry. Testy vzhľadom na ich povahu vykonávame v priestoroch zákazníka.

Testovanie webových aplikácií

kombinuje automatizované nástroje a manuálne testovanie s cieľom identifikovať čo najviac bezpečnostných nedostatkov a minimalizovať ich vplyv. Testovanie sa môže vykonávať z pozície externého útočníka, ako aj bežného autentifikovaného používateľa. Vychádzame predovšetkým z metodiky OWASP Web Security Testing Guide.

Penetračné testovanie mobilných aplikácií

pre systémy Android a iOS preverujú zabezpečenie mobilných aplikácií proti neštandardným akciám používateľov, zabezpečenie uložených údajov a prenášanej komunikácie, vrátane možných útokov na API backend servera. Metodika testovania sa riadi OWASP Mobile Security Testing Guide.

Phishingová kampaň

sa zameriava na zamestnancov ako na zvyčajne najslabší článok v zabezpečení informačných systémov. Phishingové e-maily využívajú techniky sociálneho inžinierstva a snažia sa prinútiť používateľov, aby vykonali určitú akciu (návšteva webovej stránky, poskytnúť prihlasovacie údaje alebo spustiť súbor). Simulovaná phishingová kampaň je praktickou súčasťou školenia používateľov o IT bezpečnosti. Používatelia tak majú možnosť dozvedieť sa o potenciálnych rizikách prostredníctvom praktických príkladov a naučiť sa rozpoznávať podozrivé e-maily.

Analýza otvorených zdrojov (OSINT)

sa zameriava na zber, spracovanie a analýzu údajov z voľne dostupných zdrojov. Cieľom je poskytnúť zákazníkovi súbor informácií a údajov, ktoré sa o nich útočník môže dozvedieť. Analýza zahŕňa informácie, ktoré o sebe zákazník zverejňuje (napr. metadáta súborov na ich vlastnej webovej lokalite alebo informácie z kariérnych portálov), ale aj informácie dostupné na hackerských fórach a na darkwebe (napr. uniknuté prihlasovacie údaje).

Sme certifikovaní:

OSCE³ · OSCP · OSWE · OSED · CEH · CHFI · ECSA · GPEN · CISSP

Kontakt:

Peter Suchý
Head of Cyber Security
tel.: +421 905 558 312
e-mail: peter.suchy@axians.sk

VINCI ENERGIES