Penetrační testy

Obstojí váš podnikový software před útokem hackerů? Odhalte a posilte svou kybernetickou odolnost.

Penetrační (simulace reálného hackerského útoku) a bezpečnostní testy odhalí slabiny v zabezpečení vašich informačních a komunikačních technologií a umožní vám tak jejich rychlou a efektivní nápravu. Zároveň ověří odolnost vaší organizace vůči kybernetickému útoku.

Bezpečnostní testování je nezbytné pro organizace podléhající kybernetické bezpečnosti a GDPR, vhodné je ale i pro ty, kdo outsourcují informační systémy a spoléhají na bezpečnost služeb. To platí také pro dopravní, zdravotní, výrobní a energetické sektory, stejně jak pro správu nemovitostí.

Nabízíme vám různé typy testů podle vašich požadavků, ať už se jedná o testování webových nebo mobilních aplikací, síťové a aplikační infrastruktury, nebo klientských a průmyslových zařízení.

Nečekejte, až bude pozdě. Objednejte si penetrační test ještě dnes a ujistěte se, že je váš systém bezpečný.

V roce 2022 bylo v Česku evidováno 18 554 trestných činů v oblasti kyberkriminality. Meziročně tak vzrostla o 94,9 %

Ochrana vašich firemních dat před kybernetickými hrozbami

Výrazná úspora nákladů oproti vlastnímu řešení

Špičkové nástroje k detekci zranitelnosti vaší infrastruktury

Tým bezpečnostních specialistů sledující aktuální trendy

Pravidelný reporting stavu zabezpečení vaší sítě

Co testujeme?

- **Infrastrukturu** – IT a OT sítě, síťové a bezpečnostní prvky, operační a podpůrné systémy, IoT zařízení, virtualizační platformy
- **Aplikace** – webové a speciální aplikace OWASP Top 10
- **Služby** – telekonferenční a e-mailové služby, úložiště, cloudové aplikace
- **Zaměstnance** – sociální inženýrství, phishingové kampaně cílené na klíčové osoby, procesy nebo informace
- **Bezpečnostní technologie** – účinnost šifrování komunikace, síťových firewallů, IDS, DLP a SIEMu
- **Bezpečnostní procesy** – fungování identifikace a zvládání bezpečnostních incidentů
- **Ochranu významných osob** – provádíme monitoring úniku citlivých dat do veřejného prostoru
- **Sociální inženýrství** – provádíme útoky na osoby i technologie za pomoci sociotechnik a veřejně dostupných informací

Ing. Filip Lang | filip.lang@ictnwt.cz | +420 724 707 417 **ictnwt.cz**

Penetrační testy – případová studie

Sociální inženýrství, neaktualizované technologie a fyzická infiltrace vedly k úplnému převzetí kontroly nad organizací veřejné správy.

Během penetračních testů externí a interní infrastruktury v organizaci veřejné správy byly nalezeny velmi závažné nedostatky, které vedly ke kompletní kompromitaci několika serverů. V určitých případech se nám podařilo zřetězit několik zranitelností, konkrétně chybějící bezpečnostní záplaty, slabou politiku hesel a nedodržování best practices. Dokonce se nám povedlo dostat k utajovaným informacím přímo z Internetu.

Naše taktika zahrnovala využití zranitelností v externí VPN infrastruktuře, která nebyla aktualizována a tudíž byla otevřena pro útoky. Přes tuto slabost jsme pronikli do vnitřní sítě. Našli jsme další problémy, tentokrát na intranetovém serveru, který obsahoval zranitelnost, umožňující vzdálené spouštění kódu. K úspěšnému útoku jsme však potřebovali legitimní přihlašovací údaje, které jsme již měli v rukou. To nám umožnilo kompletně ohrozit tento server.

Další problém se ukázal ve webové aplikaci pro „HelpDesk“. Chybná validace uživatelských vstupů a hardcoded přihlašovací údaje nám poskytly cestu k útoku typu SQL Injection, což nám umožnilo získat citlivá data uložená v databázi. Tímto způsobem jsme mohli ovládnout i databázový server.

Pomocí sociotechnik jsme získali plný přístup ke stanicím uživatelů, se kterými jsme byli v přímém fyzickém kontaktu. Tito uživatelé nás ke svým stanicím sami pouštěli. Dostali jsme se dokonce do zamčené serverovny a za přítomnosti vedoucího IT týmu jsme si tam umístili své zařízení. Vše jen díky obecně známým informacím (OSINT) a umění klamu.

Pro zaměstnance jsme připravili v rámci sociálního inženýrství i různé ankety, falešné WIFI sítě a ti s námi velmi „ochotně“ spolupracovali. Sociální inženýrství bylo využito v útocích na WIFI i OSINT. Využívali jsme i SPEAR Phishingové kampaně.

Postupně jsme ovládli celou organizaci – byli jsme schopni ji odpojit od sítě, Internetu a vyřadit zabezpečovací systémy či vypnout servery.

Během testů fyzické bezpečnosti jsme se pohybovali v objektech a prostorách se zakázaným vstupem veřejnosti, dostávali se do uzamčených místností, obcházeli zabezpečovací a kamerové systémy. Objevili jsme i další „živé“ ethernetové zásuvky v nestřežených prostorách organizace, kam jsme umístili další naše zařízení, která nám umožňovala vstup do infrastruktury.

Postupně jsme získali plnou vládu nad celou organizací – a to jak po stránce kybernetické, tak i po stránce fyzické. Byli jsme schopni celou organizaci odpojit od sítě, 230 V, Internetu. Byli jsme schopni vyřadit zabezpečovací systémy či vypnout servery. Měli jsme kontrolu nad uživatelskými stanicemi.

Výsledkem našich testů byla podrobná, 730stránková zpráva obsahující návrhy na nápravu zjištěných nedostatků. Organizace měla štěstí, že jsme odhalili tyto bezpečnostní trhliny před skutečným útočníkem. Naše závěrečná zpráva obsahovala statistiky, manažerské zhodnocení a technické detaily o nejzávažnějších problémech a jejich opravách.

Je alarmující, že před námi organizaci zkoušela jiná firma a tyto závažné nedostatky zůstaly nepovšimnuty. Tato situace zdůrazňuje důležitost pravidelných a důkladných penetračních testů, aby organizace mohla efektivně reagovat na hrozby a zajistit svou kybernetickou a fyzickou bezpečnost.

Ing. Filip Lang | filip.lang@ictnwt.cz | +420 724 707 417 **ictnwt.cz**