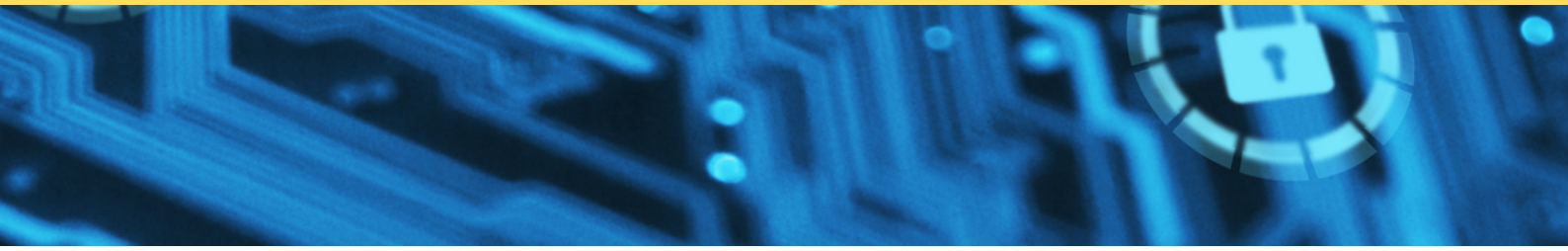
DÝCHEJTE KLIDNĚ A BUĎTE PŘIPRAVENI NA KAŽDOU SITUACI

PENETRAČNÍ TESTY



BUĎTE PŘIPRAVENI A POZNEJTE RIZIKA DOPŘEDU

KDO JSME?

Máme 6 let zkušeností s mnoha zakázkovými projekty penetračních testů a neustále sledujeme nejnovější hrozby za Vás.

CO DĚLÁME?

Díky bezpečnostním a penetračním testům pomáháme firmám preventivně předcházet výpadkům služeb a zabezpečit si infrastrukturu.

RIZIKA
rostoucí komplexita internetu zvyšuje hrozby pro všechny provozní systémy

PREVENCE
prevence je vždy lepší než řešit bezpečnostní události až když nastanou

PROVĚŘENO
používáme osvědčené metodiky a standardní nástroje a zkušenosti

solutia®
Idea & Solution Together

Spojte se s námi • +420 267 316 318 • Vršovická 1461/64, 101 00 Praha 10 • www.solutia.cz

Řešení Solutia pro penetrační testování

Společnost Solutia, s.r.o. se řídí následujícími principy při provádění penetračních testů:

- hlavní prioritou je identifikovat vysoce rizikové zranitelnosti, a to zejména takové, které nejde identifikovat automatizovanými nástroji
- další prioritou je identifikovat takové kombinace zranitelností nižšího rizika, které zneužitím v konkrétní sekvenci tvoří vysoce rizikovou zranitelnost
- s ohledem na předchozí tedy platí, že „ruční“ testování bude tvořit hlavní část testovacího procesu a testování automatickými nástroji tedy bude pouze minoritní částí procesu (případně bude sloužit jako podklad pro další ruční testování)
- výsledky testů a měření jsou kvantifikovatelné, opakovatelné a odvozené na základě skutečností zjištěných v testech
- veškeré testy jsou prováděny tak, aby bylo minimalizováno riziko dopadu na testovanou aplikaci či systém
- testování provádíme v souladu s normami ČSN ISO/IEC 27005 a ČSN ISO/IEC 27002 a dále na základě pravidel tzv. „etického hackingu“
- penetrační testy jsou realizovány jako soubor Black-Box, Grey-Box, White-Box testů prováděných z veřejné/interní sítě
- součástí testů jsou i testy infrastruktury, interních Wi-Fi sítí a např. testy neautorizovaného hardware
- součástí testování může být i použití celé škály technik sociálního inženýrství

NEJČASTĚJŠÍM ZADÁNÍM JE OVĚŘENÍ BEZPEČNOSTI WEBOVÉ APLIKACE, KDE POUŽÍVÁME METODIKU OWASP JAKO NEJVHODNĚJŠÍ CESTU, JAK OVĚŘIT JEJÍ ZABEZPEČENÍ A ODHALIT ZRANITELNOSTI TÉTO APLIKACE.

Pro prezentaci výsledků bezpečnostních testů webových aplikací je použita metrika TOP TEN (NEJ 10) s těmito kategoriemi testů:

- A1 – Injection
- A2 – Broken Authentication
- A3 – Sensitive Data Exposure
- A4 – XML External Entities (XXE)
- A5 – Broken Access Control
- A6 – Security Misconfiguration
- A7 – Cross-Site Scripting (XSS)
- A8 – Insecure Deserialization
- A9 – Using Components with Known Vulnerabilities
- A10 – Insufficient Logging & Monitoring