Interní penetrační test ICS/SCADA systémů

Obecné požadavky

- Zhotovitel provede identifikaci všech otevřených portů a služeb, popis slabin pro všechny potenciálně zranitelné služby a návrh doporučení.
- Zhotovitel provede manuální prověření nálezů tak, aby byly vyfiltrovány false-positive nálezy.
- Zranitelnosti budou prozkoumány až na úroveň identifikace konkrétních exploitů, nicméně jejich použití, které by mohlo narušit důvěrnost, integritu či dostupnost systémů musí být konzultováno s objednatelem.
- Penetrační testování bude prováděno v souladu s volně dostupnými standardy např.: OSSTMM (Open-Source Security Testing Methodology Manual), OWASP (Open Web Application Security Project), NIST SP800-115, ISSAF, NESCOR Guide to Penetration Testing for Electric Utilities.
- Provedení pen. testu v režimu „black-box test“

Rozsah:

Testovat se budou 3 lokality.
VD Lovosice
VD Josefův Důl
VD Rozkoš

Příprava testovacího plánu

Zhotovitel připraví a navrhne rozsah testu, jeho typ, naplánuje čas a datum provedení testu a určí cílové komponenty nebo systémy. Objednatel poskytne potřebnou součinnost.

Zhotovitel předloží plánovaný test a jeho rozsah objednateli ke schválení. V rámci schválení penetračního testu se objednatel seznámí s rozsahem testu, cílovými systémy, které jsou předmětem testu a souvisejícími riziky. Objednatel může k posouzení žádosti vyžadovat další informace od zhotovitele. Objednatel může omezit rozsah testu, stanovit a implementovat další opatření před provedením penetračního testu.

Provedení penetračního testu

V této fázi zhotovitel provede cílený penetrační test dle metodiky a schváleného testovacího plánu objednatelem.

Test bude probíhat na produkčním prostředí objednatele v pracovních dnech v době od 8:00 – 15:00. Objednatel musí být vždy minimálně 24h předem informován.

Vyhodnocení penetračního testu

Zhotovitel vyhotoví Závěrečnou zprávu o nálezech zranitelností, která popisuje zjištění na základě provedeného penetračního testu. Zpráva u každé zranitelnosti klasifikuje její závažnost, místo výskytu, postup ověření zranitelnosti a jednoznačný odkaz testu v metodice, resp. ve standartu, který je součástí metodiky. Součástí zprávy je také doporučená strategie nápravy, tj. jak zranitelnosti odstranit a v jakém pořadí. Zpráva bude obsahovat kvantitativní metriky měření, které musí být založeny pouze na faktech a musí se vyvarovat jakékoli subjektivní interpretaci.

Struktura závěrečné zprávy:

1. Manažerský souhrn – stručný průřez průběhem testu společně s výsledky.
2. Popis testu – popis metodiky testů a přehled všech prováděných činností a použitých nástrojů.
3. Zjištěné skutečnosti – detailní popis výsledku všech testů jednotlivých zařízení.
4. Shrnutí doporučení – přehled doporučení, kterými lze odstranit nedostatky nalezené v průběhu testu, tj. obsahuje návrh protiopatření k eliminaci identifikovaných zranitelností.
5. Závěr

Každý ve zprávě uvedený nález bude klasifikovaný dle závažnosti:

• INFO (informace),

• LOW (dopad nízkého stupně),

• MEDIUM (středně závažný nález),

• HIGH (závažný nález) a

• CRITICAL (kritický nález).

Zjištění kritického nálezu bude hlášeno objednateli okamžitě po zjištění.

Každý nález bude mít uvedené doporučení, které by mělo slabinu a riziko z ní vyplývající eliminovat nebo aspoň snížit. Nálezy/doporučení musí být ve zvláštní kapitole uvedeny přehledně v tabulce.