PENETRAČNÝ TEST ICS/SCADA

Systémy ICS/SCADA sú súčasťou rôznych priemyslov, riadenia dopravy, verejných služieb a patria medzi najviac kritické systémy, ktoré sa dnes používajú. Veľká časť týchto systémov a ich protokolov bola vyvinutá ešte v dobe keď sa prihliadalo viac na funkčnosť a dostupnosť ako na bezpečnosť.

Nepredpokladalo sa, že tieto systémy budú dostupné z verejnej siete Internet, ale budú izolované (Air Gap). Ani fyzická izolácia ICS/SCADA systémov ešte neznamená, že útočník nemôže preniknúť do tejto siete. V závislosti od charakteru systému môže mať bezpečnostný incident fatálne následky ako napríklad ohrozenie života, možnosť sabotáže, finančných strát alebo odstavenie výroby. V minulosti sme sa mohli stretnúť s notoricky známymi útokmi na elektrické rozvodne na Ukrajine alebo STUXNET v Iráne.

PREHĽAD SLUŽBY

Cieľom penetračného testu je identifikovať bezpečnostné zraniteľnosti a nedostatky v ICS/SCADA systémoch a predísť tak útokom reálnych hackerov. Výsledkom penetračného testu je report a konzultácia so zákazníkom. Report neobsahuje žiadne "false-positive" nálezy, ale len overené zraniteľnosti a odporúčania ako ich odstrániť.

Penetračný test môže byt vykonaný pomocou metódy BLACK BOX (žiadne informácie o testovanej infraštruktúre), GREY BOX (čiastočné informácie o testovanej infraštruktúre), alebo WHITE BOX (úplne informácie o testovanej infraštruktúre, vrátane konfiguračných súborov zariadení/popis nastavení).

Cena penetračného testu záleží od hĺbky testov, veľkosti a komplexnosti testovanej infraštruktúry. Táto cena je určená po konzultácii so zákazníkom, v ktorom sa určí rozsah, typ testov a ďalšie požiadavky od zákazníka.

ICS/SCADA systémy môžu byť z časti testované rovnakými metodológiami ako pri ostatných ponúkaných službách (penetračný test infraštruktúry a webu, VA, IoT, WiFi, reverzné inžinierstvo..), ale existujú tu dôležité rozdiely. Ak má testovanie vedľajšie účinky (zmena údajov, nedostupnosť), potom sú tieto účinky závažnejšie a majú väčší dopad než v typickej firemnej sieti, hlavne ak sa testuje v produkčnom prostredí. Testovanie ICS/SCADA vyžaduje viac pochopenia ako daná infraštruktúra funguje, precízne plánovanie, aktívnu súčinnosť a tím ľudí so skúsenosťami z oblasti ICS/SCADA. Ideálne je preto testovať na záložnom/testovacom prostredí, ktoré je identické ako produkčné prostredie alebo keď je produkčné prostredie v režime offline - určené na údržbu.

Fázy testu:

- Rozhovor so zákazníkom a určenie rozsahu testu
- Test plán (Threat modeling) - identifikovanie možných zraniteľných miest v infraštruktúre (spolupracuje sa so zákazníkom na identifikácii vektorov možných útokov)
- Testovanie
- Vyhodnotenie testu, report
- Odprezentovanie výsledkov zákazníkovi

Naše penetračné testy ICS/SCADA infraštruktúry zvyčajne zahŕňajú:

- Test aplikácií
- Test infraštruktúry
- Test bezdrôtových sieti
- Hodnotenie fyzickej bezpečnosti
- Sociálne inžinierstvo
- Kontrola kódu a konfigurácie
- Všeobecné zhodnotenie bezpečnosti

Spoločnosť Binary House si uvedomuje dôležitosť odbornosti v oblasti testov ICS/SCADA a preto spolupracuje s významnou spoločnosťou z Južnej Kórei, ktorá má dlhoročné znalosti a skúsenosti s testovaním priemyselných systémov.

Referencie:

kt Singtel

ST Engineering

Ďalšie referencie poskytneme na vyžiadanie.