PENETRAČNÉ TESTOVANIE IOT

IoT (Internet vecí) v súčasnosti patrí medzi najnovšie trendy v oblasti technológií. Na trh prichádzajú každý mesiac nové zariadenia. Avšak ich bezpečnosti a bezpečnostným rizikám sa doteraz nevenovalo veľa pozornosti.

Popularita týchto zariadení urobila z IoT vysoko lukratívny cieľ pre každého potenciálneho útočníka. Počet pripojených zariadení sa v posledných rokoch zvýšil a z niektorých napadnutých zariadení začali hackeri vytvárať botnety. Takéto botnety sa často používajú na útok typu Distributed Denial of Service (DDoS). Taký bol aj Mirai, napádajúci IP kamery a domáce routre, ktoré sa stali súčasťou botnetu používaného pri útokoch typu DDoS.

IoT zahŕňa všetky produkty, ktoré sú pripojené k internetu. Mnoho IoT zariadení zhromažďujú a ukladaju údaje počas používania a často zdieľajú tieto informácie so svojimi výrobcami bez toho, aby si to užívatelia uvedomili. Zariadenia IoT často bývajú aj súčasťou kritickej infraštruktúry (IIoT).

PREHĽAD SLUŽBY

Cieľom penetračného testu je identifikovať bezpečnostné zraniteľnosti a nedostatky v IoT zariadeniach (inteligentné domáce zariadenia, hračky, inteligentné domy, priemyselné zariadenia, SOHO zariadenia, atď.), určiť ich riziko a odporučiť riešenia ako eliminovať nájdené zraniteľnosti.

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/zariadení), GREY BOX (čiastočné informácie o testovanej infraštruktúre/zariadení) alebo WHITE BOX (úplne informácie o testovanej infraštruktúre, vrátane zdrojových kódov, konfiguračných súborov zariadení/popis nastavení).

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

Bezpečnosť internetu vecí (IoT) je významnou výzvou, ktorá si vyžaduje zhodnotenie bezpečnosti mnohých vektorov, od webových a mobilných aplikácii, firmvéru zariadenia, sieťových služieb/protokolov, hardvéru, šifrovania a cloudových služieb až po problémy týkajúce sa ochrany súkromia.

Binary House vytvoril a používa komplexnú metodológiu na vykonávanie penetračných testov IoT, ktorá simuluje útok tak, ako by postupoval skutočný útočník. Testovanie je možné prispôsobiť špecifickým požiadavkam alebo konkrétnej požadovanej metodológií. Každý test IoT je prispôsobený konkrétnemu testovanému zariadeniu. Využívame kontrolný zoznam, ktorý zabezpečuje, že sa počas testovania nevynechajú žiadne dôležité témy.

V závislosti od konkrétneho zariadenia a rozsahu môžete očakávať vykonanie týchto úloh:

- Hodnotenie/test bezpečnosti aplikácií a cloudu (web/API, mobilné aplikácie)
- Hodnotenie/test bezpečnosti infraštruktúry
- Hodnotenie/test bezpečnosti hardvéru
- Hodnotenie/test bezpečnosti hardvéru
- Analýza komunikačných protokolov/firmware/zdrojového alebo binárneho kódu
- Hodnotenie/test bezpečnosti bezdrôtovej komunikácie
- Všeobecné zhodnotenie bezpečnosti