Produktové novinky

Viac hodnoty.
Viac dôvery.

IIoT & OT Penetračné testovanie

Prečo je dôležité vykonávať penetračné testovanie?
Postup smerom k Priemyslu 4.0 a prepojeným výrobným systémom vytvára neustále sa zväčšujúcu útočnú plochu pre kybernetické útoky vo výrobných prostrediach a kritických infraštruktúrach. Ide najmä o priemyselný internet vecí (IIoT) a operačné technológie (OT).

Jedným dôležitým spôsobom, ako reagovať na túto hrozbu, je vykonávanie penetračného testovania, ktoré môže pomôcť včas identifikovať bezpečnostné zraniteľnosti a predchádzať útokom. Penetračné testovanie bude navyše v budúcnosti vyžadované zákonom pre mnohé priemyselné výrobky ako súčasť legislatívnych zmien. Napríklad prostredníctvom zákona EÚ o kybernetickej bezpečnosti alebo prostredníctvom delegovaného aktu ku smernici o rádiových zariadeniach.

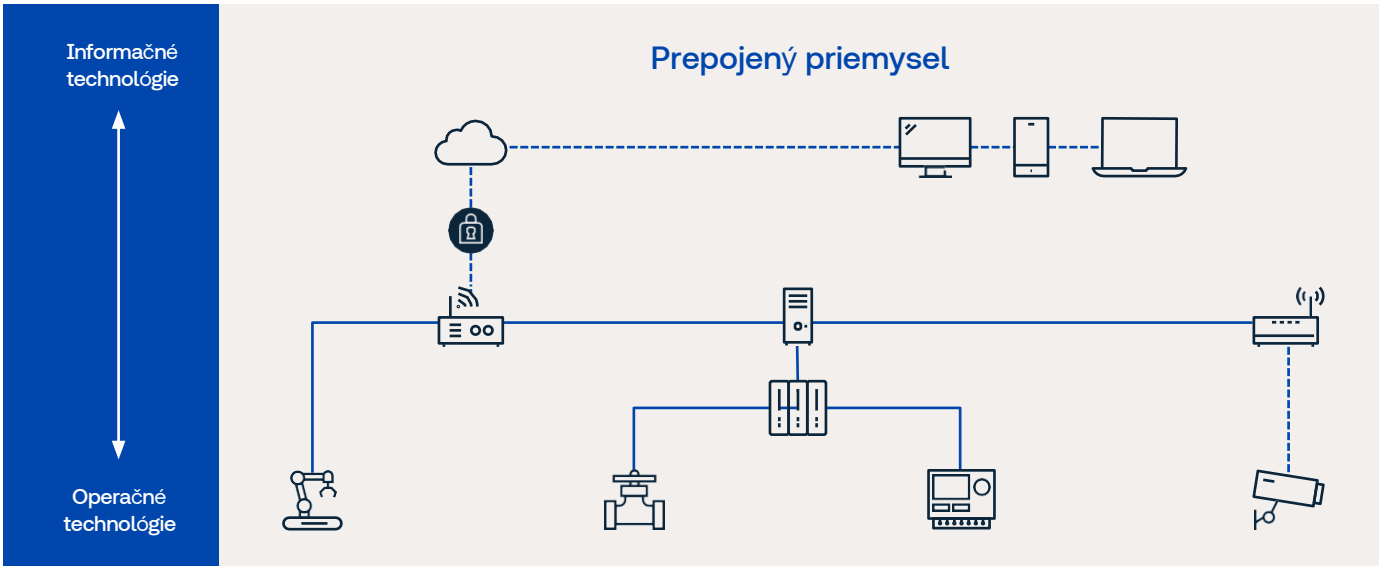
Čo je penetračný test?
V penetračnom teste naši bezpečnostní experti napodobňujú metódy potenciálnych útočníkov s cieľom odhaliť bezpečnostné zraniteľnosti v komponentoch a systémoch IIoT a OT. Používajú sa napríklad metódy získavania informácií, statické a dynamické testovanie. Okrem toho testujeme aj logický alebo konceptuálny návrh vášho produktu alebo systému.

Čo obdržíte po penetračnom teste?

- **Správu z testovania vrátane hodnotenia rizika**
  V rámci našej správy z testovania obdržíte zoznam identifikovaných zraniteľností. Tento zoznam slúži ako miera bezpečnostnej úrovne vášho testovaného IIoT a OT produktu a ukazuje dôležité oblasti, na ktoré je potrebné sa zamerať.

- **Správa o hodnotení vplyvu**
  Dodatočné hodnotenie vplyvu vysvetľuje konkrétne riziká pre vaše podnikanie vyplývajúce z identifikovaných zraniteľností.

- **Návrhy na zlepšenie vrátane analýzy príčin**
  Na základe výsledkov správy z testovania naši odborníci poskytujú spätnú väzbu a návrhy na zlepšenie všeobecnej bezpečnosti vášho testovaného produktu. Voliteľne môžeme tiež vykonať analýzu príčin, aby sme identifikovali dôvody pre existujúce bezpečnostné zraniteľnosti.



Obr. A Potenciálne kybernetické útoky sa objavujú v dôsledku konvergencie IT/OT

Čo môže byť testované prostredníctvom penetračného testovania IIoT a OT?
Prostredníctvom penetračného testovania môžeme overiť všetky komponenty, systémy a rozhrania IIoT a OT, ktoré predstavujú potenciálne bezpečnostné riziko. Napríklad inteligentné senzory a aktuátory, PLC, switche, gateway a priemyselné cloudové alebo webové služby. Týmto spôsobom môžeme identifikovať zraniteľnosti v softvéri, firmware alebo hardvéri, ako sú nesprávne nastavenia, chyby v návrhu alebo softvérové chyby.

Výhody pre vaše podnikanie

- **Zabezpečenie funkčnej bezpečnosti** – Zabráňte útoku na váš produkt, ktorý by mohol spôsobiť fyzické poškodenie, pretože by bola ohrozená funkčná bezpečnosť strojov a zariadení vašich zákazníkov.
- **Ochrana výrobných prostredí a kritickej infraštruktúry** – Zachovajte integritu a funkčnosť systémov, aby sa zabránilo výpadkom a poruchám vo výrobných prostrediach a kritickej infraštruktúre.
- **Ochrana reputácie a financií** – Zabráňte útokom na vaše produkty, ktoré by mohli spôsobiť vážne poškodenie dobrého mena a finančné škody.
- **Splnenie regulačných požiadaviek** – Budete v súlade s príslušnými priemyselnými normami (napríklad IEC 62443) a regulačnými požiadavkami týkajúcimi sa kybernetickej bezpečnosti, ako napríklad nariadenie o kybernetickej odolnosti EÚ alebo vykonávajúci akt k Smernici o rádiovom zariadení.

Prečo TÜV SÜD?
V spoločnosti TÜV SÜD si uvedomujeme, že kybernetická bezpečnosť v priemyselnom prostredí prináša svoje vlastné výzvy. S našou interdisciplinárnou odbornosťou v oblasti softvéru aj hardvéru, spolu s našimi poznatkami v oblasti priemyslu a funkčnej bezpečnosti, sme schopní poskytnúť penetračné testovanie špecificky pre priemyselné komponenty a systémy. Okrem toho sú všetky testy vykonávané našimi odborníkmi v špeciálnych kybernetických laboratóriách.

Súvisiace služby

TÜV SÜD poskytuje nasledovné súvisiace služby

- Penetračné testy
- SOC – Centrum riadenia kybernetickej bezpečnosti
- Audit kybernetickej bezpečnosti

Ak ste presvedčení, že vám môžeme pomôcť eliminovať riziká kybernetickej bezpečnosti a radi by ste sa dozvedeli viac o našich ponúkaných penetračných testoch, neváhajte nás kontaktovať!

TÜV SÜD Slovakia Jašíkova 6, 821 03 Bratislava, Slovensko
0850 221 200 info.sk@tuvsud.com, www.tuvsud.com/sk