

Autor: Tibor Horák
Názov originál: New methods of making the internet of things safer within the concept of Industry 4.0
Názov preklad: Nové metódy zvýšenia bezpečnosti Internetu vecí v rámci konceptu Industry 4.0
Jazyk monografie: anglický
Druh monografie: vedecká
Vydavateľské údaje: 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2023. 107 s. ISBN 978-80-7380-914-0.

Anotácia

Priemyselná bezpečnosť je citlivá oblasť, ktorá bola z praktického hľadiska málo preskúmaná. Vykonávanie útokov na ovládacie prvky výrobných liniek nie je za reálnych podmienok realizovateľné. Táto publikácia sa zaoberá popisom útokov, odrazenými útokmi a metódami testovanými na modeloch výrobných liniek. Sú prezentované dve úrovne ochrany proti týmto útokom. Prvý je statický na základe definície pravidiel, ktoré je možné aplikovať na klasickú sieťovú infraštruktúru. Druhý typ je dynamický, kde sa vyhodnocuje sieťová prevádzka a zisťuje sa neštandardná sieťová prevádzka. Na základe toho je následne navrhnutá ochranná schéma a demonštrovaná komplexná ochrana pred DoS a DRDoS útokmi.

Obsah

Zoznam skratiek
Zoznam obrázkov
Zoznam tabuliek

Úvod

1 Analýza a problematika súčasného stavu

- 1.1 Otázky bezpečnosti zariadení internetu vecí
- 1.2 Útoky na priemyselné výrobné systémy
- 1.3 Štatistiky zraniteľnosti zariadení internetu vecí
- 1.4 Prehľad výskumu kybernetických bezpečnostných opatrení

2 Teória a technológia návrhu

- 2.1 Priemysel 4.0
 - 2.1.1 Technologické predpoklady
 - 2.1.2 Požiadavky na bezpečnosť a spoľahlivosť
 - 2.1.3 Normy Priemyslu 4.0
- 2.2 Internet Vecí (IoT)
 - 2.2.1 Pôvod a súčasný stav
 - 2.2.2 Požiadavky na IoT
 - 2.2.3 Charakteristika prostredia
 - 2.2.4 Využitie internetu vecí
 - 2.2.5 Priemyselný internet vecí
 - 2.2.6 Spotrebiteľský internet vecí
 - 2.2.7 Spôsoby komunikácie v rámci IoT
- 2.3 Bezpečnosť internetu vecí
 - 2.3.1 Hrozby internetu
 - 2.3.2 Kybernetické hrozby

- 2.3.3 DDoS a DRDoS útoky
- 2.3.4 Typy DDoS a DRDoS útokov
- 2.3.5 Všeobecné zásady bezpečnosti proti DDoS útokom

3 Testovanie bezpečnosti reálnej výrobnéj infraštruktúry s integrovanými IoT zariadeniami

- 3.1 Skutočná výrobná infraštruktúra
 - 3.1.1 Výrobná linka
 - 3.1.2 Komunikácia výrobnéj linky
 - 3.1.3 Bezpečnostný systém IoT Fibaro
 - 3.1.4 IoT termostat Honeywell
- 3.2 Testovanie produkčnej infraštruktúry formou DDoS útokov
 - 3.2.1 Scenáre útokov
 - 3.2.2 Prvý scenár útoku
 - 3.2.3 Druhý scenár útoku
 - 3.2.4 Tretí scenár útoku
 - 3.2.5 Štvrtý scenár útoku
 - 3.2.6 Piaty scenár útoku
 - 3.2.7 Prehľad scenárov útokov
- 3.3 Dopady DDoS a DRDoS útokov na výrobný proces

4 Návrh bezpečnostných riešení pre výrobné infraštruktúry s integrovanými IoT zariadeniami

- 4.1 Základné odporúčania pre zabezpečenie IoT zariadení
- 4.2 Navrhované riešenia na zmiernenie účinkov DDoS útokov
- 4.3 Statická bezpečnostná stratégia využívajúca transparentný firewall brige.
 - 4.3.1 Monitorovanie sieťovej prevádzky pomocou NetFlow
- 4.4 Dynamická bezpečnostná stratégia
 - 4.4.1 Získavanie dátovej komunikácie
 - 4.4.2 Strojové učenie
 - 4.4.3 Transformácia dát pre strojové učenie
 - 4.4.4 Neurónová sieť
 - 4.4.5 Zabezpečenie brány firewall

5 Overovanie a hodnotenie navrhovaných riešení

- 5.1 Overenie a vyhodnotenie statického zabezpečenia
- 5.2 Overovanie a hodnotenie dynamického zabezpečenia
- 5.3 Celkové zhrnutie a porovnanie navrhovaných riešení

Zhrnutie

Referencie

O autorovi

Index