Bezpečnost internetu věcí má díky výzkumu nové účinné nástroje

Praha 13. 5. 2021

Včasné odhalení útoku na sítě internetu věcí (IoT) může znamenat doslova záchranu před mnoha nepředvídatelnými následky. V případě soukromého užití se jedná zejména o zásah do soukromí, u průmyslových aplikací může dojít k narušení funkčnosti celých systémů autonomních zařízení s rozsáhlými dopady na výrobu nebo energetiku. Tyto systémy nelze chránit antivirovými programy, proto je potřeba jiné řešení. Úkolu se zhostili odborníci ze společnosti Flowmon Networks a.s. a VUT v Brně a spolu s partnery z Jižní Koreji vyvinuli nástroje pro monitorování i diagnostiku IoT. Projekt podpořila Technologická agentura ČR více než 10,5 miliony korun v Programu DELTA.

„Internet věcí je dnes stále více využívaný a do budoucna bude jeho rozšíření větší a větší. Zasahuje nejen do průmyslové výroby, ale pomalu se stává běžnou součástí našich domácností. To přináší kromě nesporných výhod i nové problémy, zejména v oblasti bezpečnosti. Projekt Ironstone proto logicky dostal naši podporu,“ uvedl Petr Konvalinka, předseda Technologické agentury České republiky (TA ČR). Řešitelem úkolu byla firma Flowmon Networks a.s. ve spolupráci s Fakultou informačních technologií Vysokého učení technického v Brně a dalšími partnery byly výzkumníci z Jižní Koreji. Po třech letech práce čeští výzkumníci vyvinuli sadu nástrojů pro monitorování a diagnostiku komunikace internetu věcí.

„V principu jde o to, že při využívání internetu věcí mezi sebou komunikují autonomní zařízení, která mohou být infikovaná malwarem nebo pod kontrolou útočníků podobně jako počítače nebo servery. Na rozdíl od běžných systémů je však není možné chránit například pomocí antiviru. Námi vyvinutý softwarový nástroj Flowmon IoT Monitoring and Diagnostic Toolset tuto komunikaci sleduje, aby včas detekoval provozní problémy a identifikoval bezpečnostní incidenty. Druhý nástroj, Hancom GMD IoT Forensic Toolset, je určen pro forenzní analýzu získaných dat z IoT provozu a zařízení,“ vysvětlil Pavel Minařík, jeden z řešitelů projektu a technický ředitel společnosti Flowmon Networks.

Technické řešení umožňuje zvýšit viditelnost dat z komunikace a detekovat řadu útoků, jako jsou například připojení neautorizovaného zařízení k síti, přenos hesel v otevřené podobě, neautorizovaný přenos dat, útoky na síťové služby, malware, viry a desítky dalších projevů kompromitace IoT zařízení, respektive celého IoT prostředí.

Uvedením nové generace řešení pro IoT vstupuje firma Flowmon Networks na nový dynamicky se rozvíjející trh. Zatímco konkurenční řešení jsou úzce specializovaná, Flowmon Networks umožňuje v jediném systému analyzovat jak běžnou IT komunikaci v podnikových sítích, tak i komunikaci IoT

Mgr. Veronika Dostálová
tisková mluvčí TA ČR
T: 721 588 025**, E:** veronika.dostalova@tacr.cz

zařízení. Získává tím unikátní pozici výrobce řešení pro monitorování podnikových i průmyslových sítí řídicích systémů. Výsledky projektu Ironstone integrované do řešení Flowmon jsou nasazovány zejména v systémech velkých průmyslových firem nebo energetických společností.

Projekt přinesl také nalezení a ověření metod sběru a analýzy dat z IoT komunikace. Jejich využití ve formě softwarových nástrojů pro monitorování provozu a forenzní analýzy IoT v prostředí průmyslových aplikací napomohou rozšíření IoT systémů, čímž se zvýší technologická vyspělost ČR. Dalším významným přínosem je i rozvoj takzvaných chytrých domácností.

Projekt Ironstone není zdaleka poslední a již nyní společnost navazuje dalšími projekty zaměřenými různými směry, které se rovněž týkají bezpečnosti IoT. *„Jedním z nich je monitorování průmyslových systémů a zvýšení viditelnosti vnitřní komunikace se zaměřením na protokoly Modbus, DNP3 a Fieldbus. Další projekt se týká energetických sítí, kde chceme při detekci anomálií využít i metod umělé inteligence, podobně jako tomu je v našich produktech pro prostředí podnikového IT,“* upozornil Pavel Minařík.

Mgr. Veronika Dostálová
tisková mluvčí TA ČR
T: 721 588 025**, E:** veronika.dostalova@tacr.cz