

Bezpečnosť Internetu vecí (IoT)

Základy pre prax

Ing. Matej Skulský

KC KB - FEI STU Bratislava

13. februára 2026



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ
CENTRUM
KYBERNETICKEJ
BEZPEČNOSTI

STU

SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE

- 1 Úvod do Internetu vecí (IoT)
- 2 Architektúra a technológie IoT
- 3 Hrozby a útoky na IoT
- 4 Bezpečnostné princípy pre IoT
- 5 Ochrana domácich IoT zariadení
- 6 Kto naozaj vlastní vaše IoT?
- 7 IoT v organizáciách a priemysle
- 8 Normy a regulácie pre IoT
- 9 Zhrnutie a praktické odporúčania

Čo je Internet vecí (IoT)?

Definícia

Internet vecí (IoT) je sieť fyzických zariadení, ktoré zbierajú, spracúvajú a vymieňajú si dáta cez komunikačné siete **bez priamej účasti človeka**.

Príklady IoT zariadení:

- Smart TV, hlasoví asistenti
- Inteligentné žiarovky, zásuvky, termostaty
- Bezpečnostné kamery, alarmy, zvončky
- Nosená elektronika (hodinky, náramky)
- Senzory v priemysle, mestách (parkovanie, osvetlenie)

Typické vlastnosti:

- Neviditeľne bežia na pozadí
- Sú trvalo pripojené k sieti/internetu
- Zbierajú a odosielajú veľké množstvo dát
- Často majú obmedzené možnosti správy a aktualizácie

Prečo je bezpečnosť IoT kľúčová?

Dopady na používateľov:

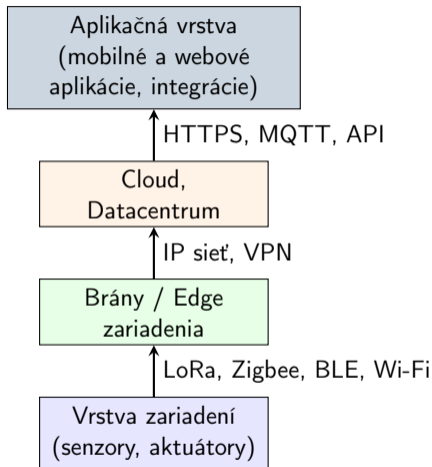
- Únik osobných údajov (zdravotné, lokalizačné, návyky)
- Zneužitie kamier a mikrofónov na sledovanie
- Ovládnutie zámkov, alarmov a iných bezpečnostných prvkov
- Zneužitie IoT ako vstupnej brány do firemnej siete

Dopady na infraštruktúru:

- Botnety z kompromitovaných IoT zariadení (napr. Mirai)
- DDoS útoky na služby a kritickú infraštruktúru
- Sabotáž priemyselných procesov (IIoT, SCADA)
- Reputačné škody a finančné straty

Kľúčové zistenie

IoT zariadenia sú často **najslabším článkom** siete, ale útočníkom poskytujú **veľmi silnú páku**.



Bezpečnostný pohľad

Každá vrstva má svoje **špecifické zraniteľnosti** a vyžaduje iné bezpečnostné opatrenia.

Prístupové technológie:

- Wi-Fi, Ethernet
- Bluetooth, BLE
- Zigbee, Z-Wave
- LoRaWAN, Sigfox
- Mobilné siete (4G/5G, NB-IoT, LTE-M)

Protokoly:

- **MQTT** – publish/subscribe, vhodné pre senzory
- **CoAP** – „HTTP pre malé zariadenia“
- **HTTP(S)** – webové API
- **Proprietárne protokoly** výrobcu

Bezpečnostné dôsledky

Rôzne technológie majú rôznu úroveň šifrovania, autentizácie a správy kľúčov – pri návrhu je potrebné to zohľadniť.

Na úrovni zariadenia:

- Predvolené alebo slabé heslá
- Neaktualizovaný firmware, známe zraniteľnosti
- Chýbajúce šifrovanie komunikácie
- Nezabezpečené debug porty (UART, JTAG)
- Nedostatočne chránené úložisko (plain-text konfigurácie)

Na úrovni systému:

- Neoddelené siete (IoT v tej istej sieti ako firemné PC)
- Slabé alebo chýbajúce logovanie
- Chýbajúci inventár IoT zariadení („nevieme, čo máme“)
- Slabé riadenie prístupu k cloudovým účtom a aplikáciám

Problém

Mnohé IoT zariadenia boli navrhnuté s dôrazom na **cenu a jednoduchosť**, nie na bezpečnosť.

Čo bol Mirai?

Mirai bol malvér, ktorý automaticky vyhľadával a infikoval IoT zariadenia s predvolenými prihlasovacími údajmi a vytváral z nich botnet.

Zneužívané zariadenia:

- Domáce routery
- IP kamery a rekordéry
- Iné jednoduché IoT zariadenia

Dôsledky:

- Masívne DDoS útoky na veľké služby (DNS poskytovatelia, hostingy)
- Nedostupnosť mnohých populárnych webov
- Ukážka, že **domáce zariadenia** môžu mať globálny dopad

Poučenie

Jednoduché veci ako zmena predvoleného hesla výrazne znižujú riziko.

Ciele útočníkov:

- Sledovanie domácnosti cez kamery
- Získanie prístupu k domácemu Wi-Fi/routeru
- Získanie prístupu k firemným zdrojom (home office)
- Vytvorenie botnetu z domácich zariadení

Typické chyby používateľov:

- Nezmena predvoleného hesla
- Vypnuté alebo chýbajúce aktualizácie
- Pripojenie IoT do tej istej siete ako pracovný notebook
- Inštalácia neoverených aplikácií na správu IoT

Príklad

Smart kamera s továrenským heslom je dostupná z internetu – ktokoľvek si môže pozerať prenos z vašej obývačky.

Myšlienka

Najlacnejšia a najefektívnejšia bezpečnosť je tá, ktorá je **zabudovaná už pri návrhu**, nie doplnená na konci.

Pre výrobcov a architektov:

- Bezpečné predvolené nastavenia (žiadne default „admin/admin“)
- Povinná zmena hesla pri prvom použití
- Podpora bezpečných aktualizácií (OTA)
- Šifrovanie komunikácie a úložísk

Pre prevádzkovateľov:

- Zohľadniť bezpečnosť už v požiadavkách na projekt
- Hodnotenie rizík pri nasadzovaní IoT
- Testovanie (aj bezpečnostné) pred nasadením do produkcie

Dôvernosť (Confidentiality):

- Šifrovanie komunikácie (TLS, VPN)
- Bezpečné ukladanie citlivých údajov
- Riadenie prístupu k dátam (autentizácia, autorizácia)

Integrita (Integrity):

- Podpisy a kontrolné súčty firmvéru
- Ochrana proti manipulácii s konfiguráciou
- Detekcia neautorizovaných zmien

Dostupnosť (Availability):

- Ochrana proti DDoS a preťaženiu
- Redundancia kritických prvkov
- Bezpečné obnovenie po výpadku

Špecifikum IoT

Pri IoT je často kritická **bezpečnosť** a **spoľahlivosť fyzického procesu** (vykurovanie, výroba, doprava).

Nastavenia a aktualizácie:

- Vždy zmeňte **predvolené heslá**
- Používajte **silné a jedinečné** heslá, ideálne s password manažérom
- Zapnite **automatické aktualizácie** firmvéru, ak sú dostupné
- Pravidelne kontrolujte, či výrobca stále vydáva záplaty

Sieť a pripojenie:

- Vytvorte samostatnú **Wi-Fi sieť pre IoT** zariadenia (guest/IoT VLAN)
- Neprepájajte IoT priamo s pracovným notebookom
- Vypnite vzdialený prístup, ak ho nepotrebuje
- Prístup na konfiguráciu obmedzte len z internej siete

Vedome rozhodujte, čo zbierate:

- Skontrolujte, aké oprávnenia má mobilná aplikácia
- Vypnite zbytočné senzory (mikrofón, kamera), ak ich netreba
- Obmedzte zber lokalizačných údajov a históriu
- Prečítajte si aspoň stručný súhrn podmienok spracovania dát

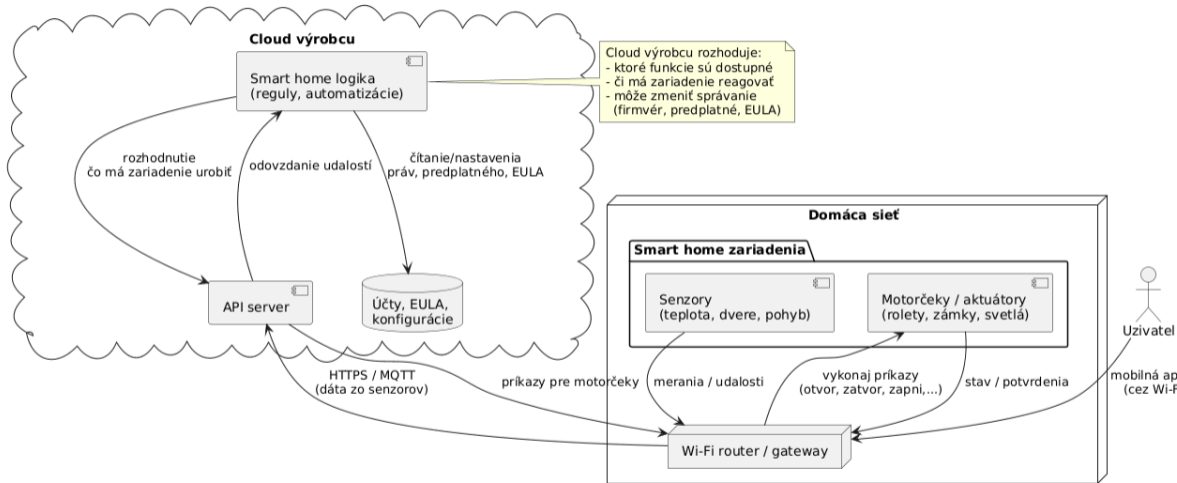
Praktické tipy:

- Umiestnite kamery tak, aby nenesímali viac než je potrebné
- Zvážte, či naozaj potrebujete cloudový záznam, alebo stačí lokálne úložisko
- Pri predaji/darovaní zariadenia urobte **factory reset** a odstráňte ho z účtu

Dôležité

Ochrana, bezpečnosť a súkromie v dizajne ... to je síce pekné, ALE, ...

Architektúra smart home závislá od cloudu



Problém

Pri mnohých IoT riešeniach **nevlastníte službu**, iba zariadenie a prístup k účtu, ktorý môže výrobca kedykoľvek zmeniť alebo vypnúť.

Typický model:

- Zariadenie funguje len cez **cloudový server výrobcu**
- Funkcie sú viazané na **účet a EULA/podmienky používania**
- Výrobca si vyhradzuje právo meniť funkcie a ceny
- Bez servera → „hlúpe“ alebo nefunkčné zariadenie

Dôsledky pre používateľa:

- Firma ukončí službu → zariadenie prestane fungovať
- Zmena predplatného → za funkciu, ktorú ste mali, **zrazu platíte mesačne**
- Zrušený účet (napr. porušenie EULA) → strata prístupu k „vlastným“ zariadeniam

Príklady „vypnutých“ služieb:

- Výrobca ukončí cloud pre smart kamery → kamery bez záznamu a notifikácií
- Smart hub pre dom automatizácie prestane byť podporovaný → žiadne aktualizácie, výpadok integrácií
- Zmena obchodného modelu: funkcie, ktoré boli v cene, prejdú na **predplatné**

Čo to učí používateľov:

- „Ak je moje bývanie závislé na cudzom serveri, **nemám nad ním plnú kontrolu.**“
- EULA často umožňuje výrobcovi meniť funkcie a podmienky jednostranne.
- „Smart“ sa môže v jednej noci zmeniť na „hlúpe“, hoci hardvér je fyzicky v poriadku.

Pri výbere riešenia:

- Preferujte zariadenia, ktoré **vedia fungovať lokálne** (LAN, lokálny controller - bez internetu)
- Overte si, či je možné použiť **otvorené štandardy** (MQTT, Matter, Zigbee, Home Assistant ...)
- Skúste sa vyhnúť kritickým funkciám (zámky, kúrenie) závislým na cudzom cloude - najmä pri domácnostiach

Prevádzkové odporúčania:

- Čítajte aspoň základ EULA – čo sa stane, ak službu zrušia?
- Pri návrhu smart home počítajte s **plánom B** (manuálne ovládanie)
- U kritických služieb zvažujte **self-hosted** alebo hybridné riešenia

1. Inventarizácia IoT:

- Zoznam všetkých IoT zariadení (čo, kde, kto je zodpovedný)
- Zahnúť aj „skryté“ prvky (TV, tlačiarne, kamery, chytré klimatizácie)
- Identifikovať výrobcu, model, verziu firmvéru

2. Segmentácia siete:

- Samostatné VLAN/subsiete pre IoT
- Obmedziť prístup IoT len na nevyhnutné systémy (princíp najmenších oprávnení)
- Použiť firewall a ACL medzi IoT a zvyškom infraštruktúry

Praktický cieľ

Ani úplné kompromitovanie IoT zóny by nemalo **ohroziť kritické systémy** organizácie.

Prevádzková bezpečnosť:

- Politika nákupu IoT (minimálne bezpečnostné požiadavky na výrobcu)
- Pravidelné kontroly aktualizácií a zraniteľností
- Riadenie prístupov k cloudovým účtom a správčovským rozhraniam

Monitoring a incidenty:

- Logovanie prístupov a udalostí z IoT zariadení
- Prepojenie na SIEM/SOC (ak existuje)
- Scenáre reakcie: čo robiť pri podozrivom správaní IoT zariadenia

Dôležité

Hlásenie incidentov (aj podozrení) je rovnako dôležité pri IoT ako pri klasických IT systémoch.

Európske a medzinárodné normy:

- **ETSI EN 303 645** – kybernetická bezpečnosť spotrebiteľských IoT
- **ISO/IEC 27402** a príbuzné normy pre IoT bezpečnosť
- **ISO/IEC 27001 + ISO/IEC 62443** (priemyselné systémy)

Legislatívny rámec:

- **GDPR** – ochrana osobných údajov z IoT zariadení
- **NIS2** – povinnosti pre prevádzkovateľov základných a dôležitých služieb
- **ZoKB** – Zákon o kybernetickej bezpečnosti
- Pripravované **Cyber Resilience Act** v EÚ

Pre prax

Nie je nutné poznať všetky paragrafy, ale je dôležité vedieť, že **pravidlá existujú** a ovplyvňujú dizajn a prevádzku IoT riešení.

- 1 IoT je všade okolo nás – v domácnostiach, mestách, priemysle.
- 2 IoT zariadenia sú často najslabším článkom bezpečnosti siete.
- 3 Bezpečnosť musí byť súčasťou návrhu, nie dodatok na konci.
- 4 Segmentácia a inventarizácia sú základné kamene ochrany.
- 5 Jednoduché návyky (zmena hesla, aktualizácie, osobitná sieť) majú veľký efekt.
- 6 IoT riešenia podliehajú reguláciám (GDPR, NIS2, normy ETSI/ISO).

Pre domácnosť:

- ✓ Zmeniť predvolené heslá na IoT zariadeniach
- ✓ Zapnúť automatické aktualizácie, kde to ide
- ✓ Vytvoriť samostatnú Wi-Fi sieť pre IoT
- ✓ Skontrolovať nastavenia súkromia aplikácií

Pre organizáciu:

- ✓ Začať inventarizáciou IoT zariadení
- ✓ Navrhnuť alebo vylepšiť segmentáciu IoT siete
- ✓ Nastaviť minimálne bezpečnostné požiadavky pri nákupe IoT
- ✓ Zahnúť IoT do existujúcich bezpečnostných politík a školení

Otázky?