Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zraniteľnosť IoT zariadení

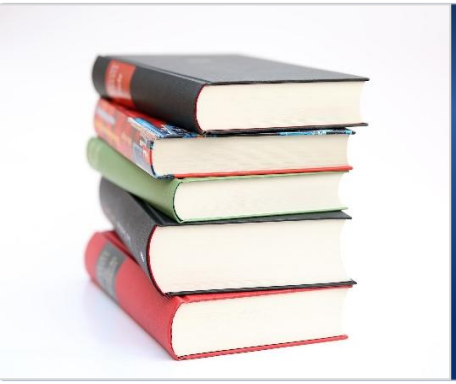
Bezpečnosť pri bezdrôtovej komunikácii, vzdialenom prístupe, využívaní cloudu a IoT zariadení (Blok VI)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Doc. Ing. Jozef Papán, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

jozef.papan@uniza.sk



Obsah

- Aké sú zraniteľnosti IoT zariadení?
- Zraniteľnosti v softvéri tretích strán
- Kybernetické útoky IoT zariadení
- Štatistiky o bezpečnosti IoT v roku 2025
- Bezpečnostné odporúčania a návrhy opatrení

Úvod - IoT

- Internet vecí (Internet of Things – IoT) predstavuje rýchlo sa rozvíjajúcu oblasť technológií, ktorá prináša nové možnosti automatizácie, zberu dát a vzdialeného riadenia zariadení.
- IoT zahŕňa široké spektrum zariadení – od inteligentných domácich spotrebičov, cez nositeľné technológie, až po priemyselné senzory a zariadenia v oblasti zdravotníctva.
- Ich spoločným menovateľom je schopnosť komunikovať prostredníctvom siete a vytvárať prepojený ekosystém.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Aké sú zraniteľnosti IoT zariadení?

Aké sú zraniteľnosti IoT zariadení?

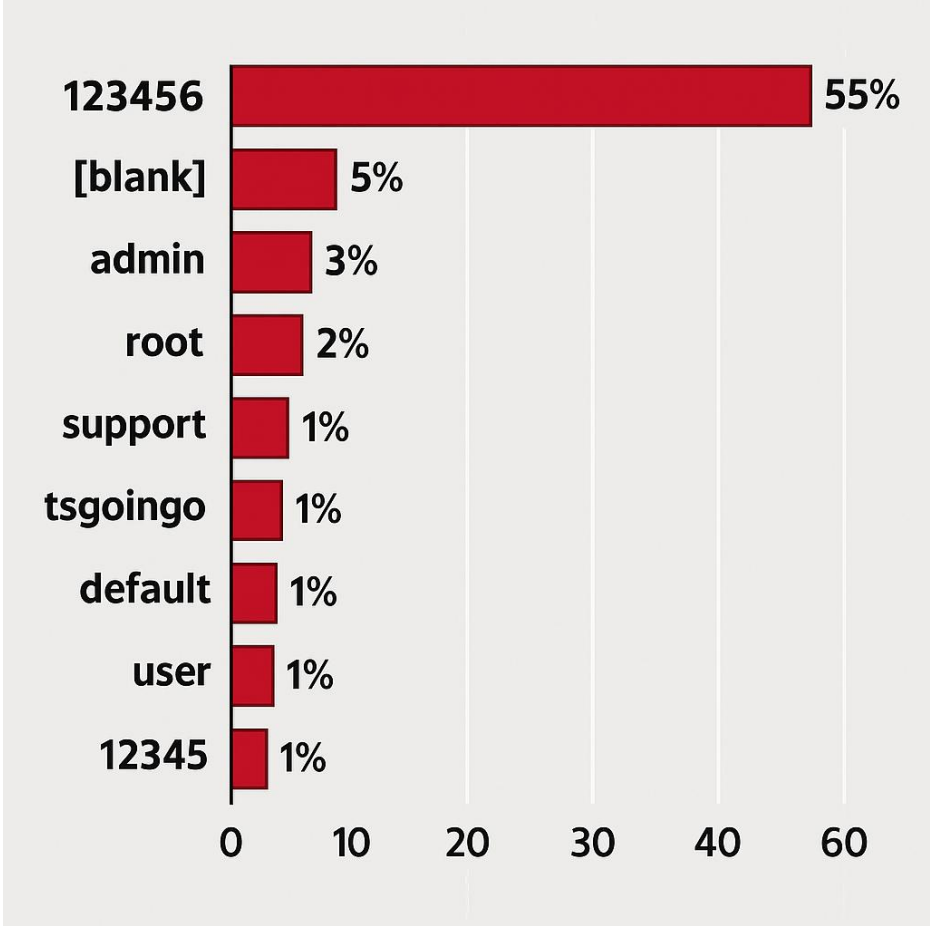
- Zraniteľnosti IoT zariadení sú pomerne časté a rôznorodé, keďže tieto zariadenia často nebývajú dostatočne zabezpečené.
- Ich hlavný cieľ je často zameraný na funkcionalitu a jednoduchosť používania, nie však na kybernetickú bezpečnosť. Typy zraniteľností:
  - 1. Slabé autentizačné mechanizmy
  - 2. Nešifrovaná komunikácia
  - 3. Zastaraná alebo žiadná aktualizácia systému
  - 4. Nedostatočné zabezpečenie fyzického prístupu
  - 5. Zraniteľnosti v softvéri tretích strán

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

1. Slabé autentizačné mechanizmy

- Mnohé IoT zariadenia používajú predvolené prihlasovacie údaje ako „admin/admin“ alebo „user/password“.
- Používatelia ich často nemenia a niektoré zariadenia dokonca ani neumožňujú zmenu prihlasovacích údajov.
- Útočníci môžu veľmi jednoducho automatizovane prehľadávať sieť a získať prístup k zariadeniam pomocou tzv. brute-force alebo dictionary útokov.
- **Odporúčanie: používať komplexné heslá, pravidelne meniť**

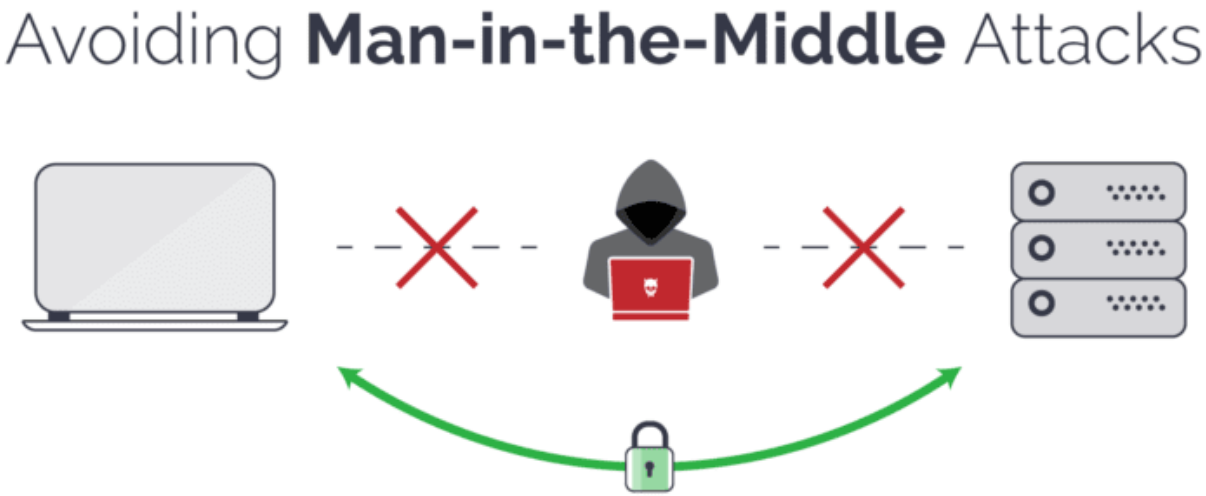
Najčastejšie používane hesla na IoT



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

2. Nešifrovaná komunikácia

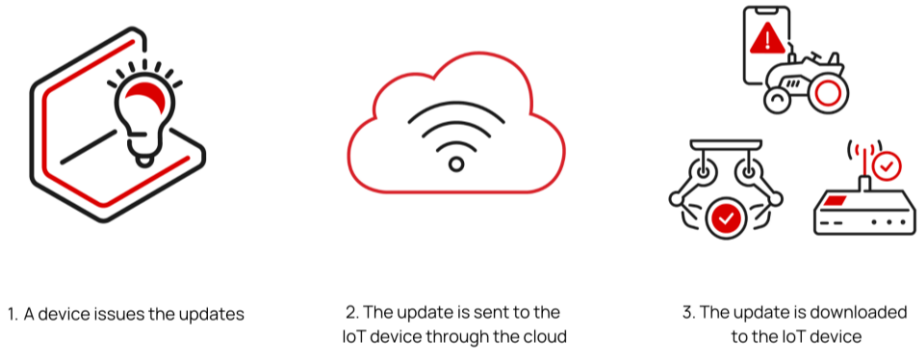
- Prenos údajov medzi IoT zariadením a centrálnym serverom často prebieha bez šifrovania (napr. cez HTTP namiesto HTTPS).
- Takéto spojenia sú zraniteľné voči **man-in-the-middle** útokom, pri ktorých útočník zachytí alebo modifikuje prenášané údaje.
- **Odporúčanie: šifrovaná komunikácia (HTTPS namiesto HTTP) , dôveryhodné certifikáty**



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

3. Zastaraná alebo žiadná aktualizácia systémů

- IoT zariadenia majú často pevne zabudovaný firmvér, ktorý sa neaktualizuje automaticky.
- Výrobcovia navyše po čase prestávajú zariadenia podporovať, čo znamená, že známe zraniteľnosti zostávajú neopravené.
- Útočníci tak majú dlhodobý prístup k známym slabinám systému.
- **Odporúčanie: pravidelná aktualizácia, nakupovať od overených výrobcov**

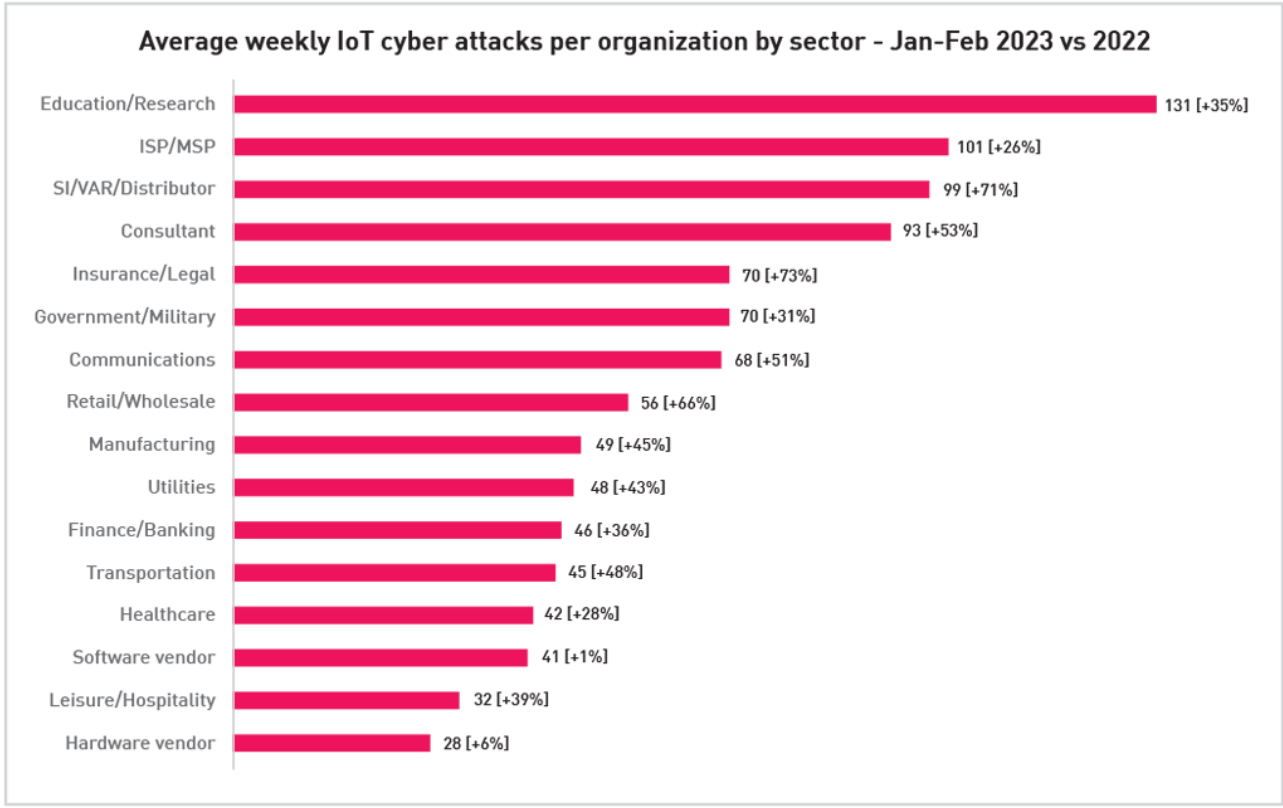


4. Nedostatočné zabezpečenie fyzického prístupu

- IoT zariadenia bývajú často umiestnené na miestach s jednoduchým fyzickým prístupom.
- Útočník môže zariadenie rozobrať, pripojiť sa priamo k hardvérovým rozhraniam (napr. UART, JTAG) a získať prístup k pamäti alebo citlivým údajom.
- **Odporúčanie: zakázať alebo zabezpečiť prístup ku konfigurácii zariadenia, šifrovanie úložiska a pamäte, použitie detekcie narušenia.**

5. Zraniteľnosti v softvéri tretích strán

- IoT zariadenia bežne využívajú:
  - Rôzne softvérové knižnice.
  - Komponenty tretích strán.
- Ak tieto komponenty obsahujú chyby, zariadenia sú automaticky zraniteľné.
- Riziko hrozí, ak sa pravidelne nevykonáva aktualizácia a bezpečnostný audit softvérových závislostí.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Dôsledky zneužitia zraniteľností

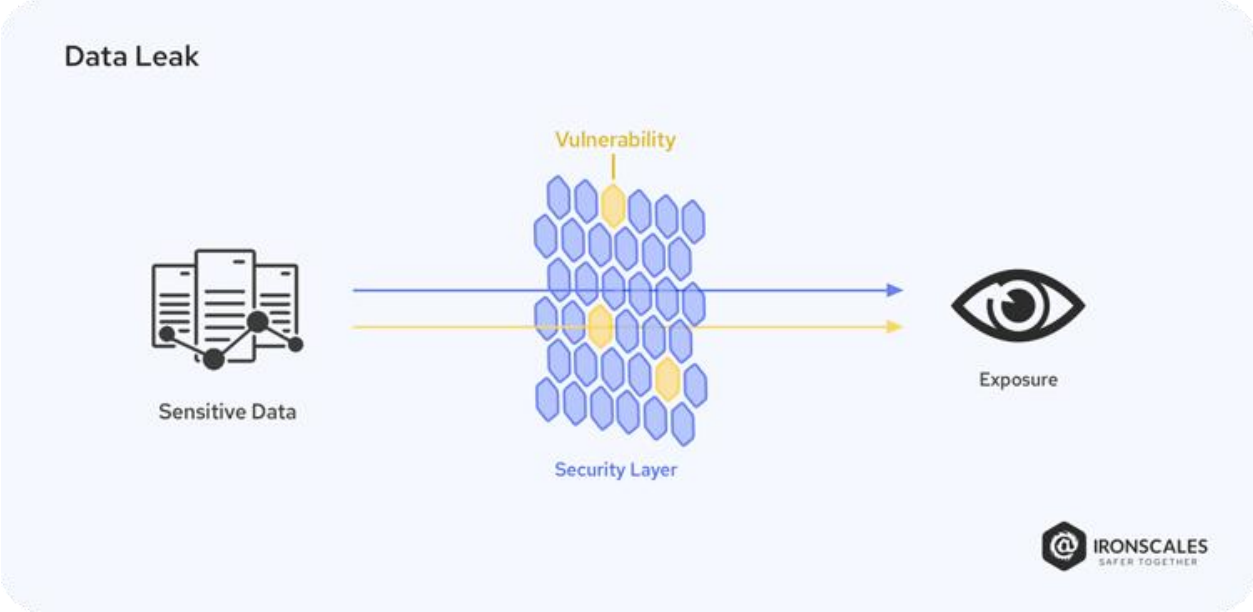
Dôsledky zneužitia zraniteľností v IoT

- Zneužitie zraniteľnosti v IoT zariadeniach môže mať závažné dôsledky – od narušenia súkromia až po ohrozenie kritickej infraštruktúry. Tu sú hlavné kategórie dôsledkov:
- 1. Únik citlivých údajov
- 2. Botnety a DDoS útoky
- 3. Narušenie funkčnosti zariadenia
- 4. Vydieranie (ransomware)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

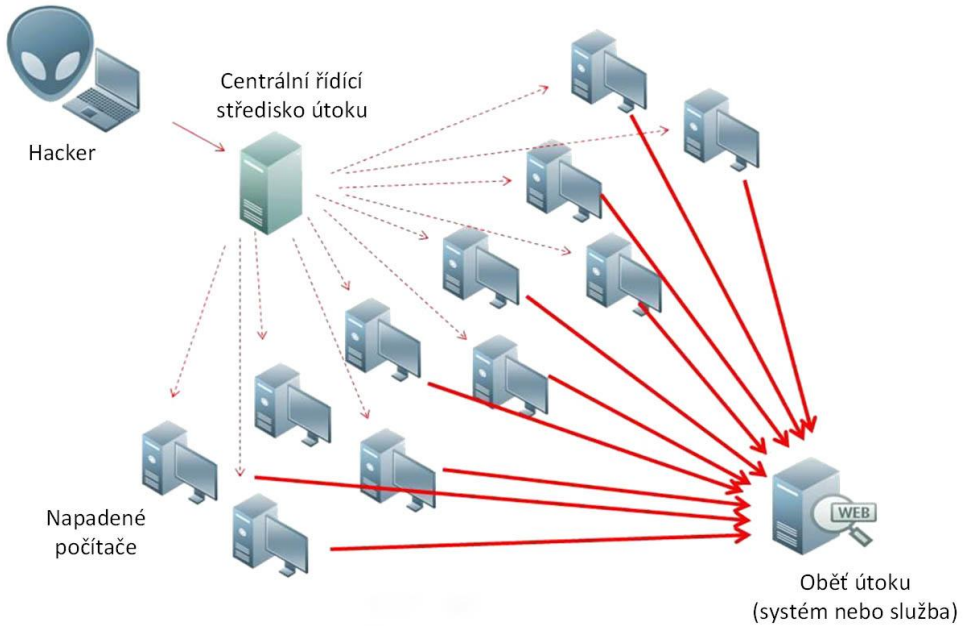
1. Únik citlivých údajov

- Mnohé IoT zariadenia zbierajú a spracúvajú citlivé informácie – od biometrických údajov (napr. nositeľné zariadenia) cez záznamy z kamier až po informácie o pohybe osôb.
- Ak dôjde k úniku týchto dát, je ohrozené súkromie jednotlivca a môže dôjsť k zneužitiu identity.



2. Botnety a DDoS útoky

- Jednou z najznámejších foriem zneužitia IoT zariadení je ich zaradenie do botnetu – siete kompromitovaných zariadení ovládaných útočníkom.
- Tieto botnety sa využívajú najmä na distribuované útoky na dostupnosť služieb (DDoS).
- Príkladom je botnet Mirai, ktorý v roku 2016 ochromil niekoľko veľkých webových služieb.



3. Narušenie funkčnosti zariadenia

- Útoky môžu viesť k znefunkčneniu zariadenia alebo jeho zneužitiu na neautorizované operácie
  - napr. otvorenie inteligentného zámku,
  - vypnutie alarmu,
  - manipuláciu so zdravotníckym zariadením a podobne.
- V priemyselných aplikáciách môže ísť o ohrozenie bezpečnosti celých výrobných liniek.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

4. Vydieranie (ransomware)

- Rovnako ako pri bežných počítačoch, aj v prípade IoT zariadení, sa môžeme stretnúť s ransomvérom.
- Ten môže napríklad zablokovať prístup k dôležitým údajom, zašifrovať záznamy zo senzorov, alebo zablokovať prístup k systémom, ktoré sú súčasťou kritickej infraštruktúry.

Zraniteľnosti IoT zariadení

Flipper Zero – multifunkčné hacker zariadenie

- je multifunkčné zariadenie pre penetračné testovanie a výskum bezpečnosti. Vyzerá ako hračka, ale v skutočnosti ide o výkonný nástroj pre interakciu s rôznymi technológiami.

Praktické príklady použitia Flipper Zero

Odomykanie dverí cez RFID/NFC

- Naklonuje prístupovú kartu (napr. do kancelárie či fitka) a emuluje ju
- Príklad: Priložením Flippera sa otvoria dvere rovnako ako originálnou kartou

Ovládanie domácich zariadení cez infračervené (IR)

- Naučí sa signály z diaľkového ovládača a potom ich vysiela
- Príklad: Prepínanie kanálov na TV alebo zapnutie klimatizácie

Zachytávanie signálu z diaľkového ovládača pre garážové brány

- Pracuje v pásmach ako 433 MHz, ktoré sa bežne používajú pre diaľkové ovládanie
- Príklad: Po načítaní signálu môže otvoriť niektoré garážové brány

Práca s iButton kľúčmi (Dallas)

- Číta a emuluje iButtony používané na prístup do budov
- Príklad: V bytových domoch alebo serverovniach

Testovanie USB HID útokov (rubber ducky štýl)

- Simuluje klávesnicu a môže automaticky písať príkazy po pripojení k PC
- Príklad: Automatické otvorenie terminálu a stiahnutie skriptu

Zbieranie dát a analýza komunikácie

- Možnosť pripojenia snímačov cez GPIO alebo zachytávanie bezdrôtovej komunikácie
- Príklad: Analyzovanie senzorov v IoT domácnosti

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kybernetické útoky IoT zariadení

Nárast kybernetických útokov na IoT v roku 2021

- **Masívny nárast útokov:** V prvom polroku 2021 zaznamenala spoločnosť Kaspersky viac ako dvojnásobný nárast útokov na IoT zariadenia v porovnaní s predchádzajúcim rokom.
- **Celkový počet:** Počas prvých šiestich mesiacov roku 2021 bolo zaznamenaných približne 1,51 miliardy útokov.
- **Hlavné vektory a ciele útokov:** * Väčšina týchto útokov zneužívala vzdialený prístup cez protokol **Telnet**.
  - Útočníci sa zameriavali predovšetkým na **ťažbu kryptomien**, realizáciu **DDoS útokov** a **krádež citlivých údajov**.
- **Metódy zhromažďovania dát:** Tieto údaje boli získané pomocou tzv. „honeypots“ – pascí (senzorov), ktoré simulujú zraniteľné zariadenia a lákajú kyberzločincov, aby odborníci mohli analyzovať ich aktivity.
- **Geografický pôvod:** Najviac útokov v tom období smerovalo z Číny, Vietnamu a Južnej Kórey.
- **Zdroj:**
- IoT Cyberattacks Escalate in 2021, According to Kaspersky: https://www.iotworldtoday.com/security/iot-cyberattacks-escalate-in-2021-according-to-kaspersky.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kybernetický útok na VšZP a NCZI (január 2025 – 2026)

- Hoci pandémia v jej najsilnejšej forme už ustúpila, v nedávnom období bol zaznamenaný ďalší **masívny kybernetický útok** na Všeobecnú zdravotnú poisťovňu (VšZP) a NCZI.
- Útočníci sa pokúšali získať **citlivé osobné údaje** vrátane diagnóz a plánovaných zákrokov miliónov pacientov.
- Podľa vyjadrení štátnych predstaviteľov by úspešný útok mohol viesť k úplnému znefunkčneniu poskytovania zdravotnej starostlivosti v krajine.
- **Zdroj:** Oficiálna správa Vlády SR: vlada.gov.sk.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Útok na objednávkový systém očkovania (2021)

- V marci 2021 čelil systém na objednávanie očkovania proti COVID-19 na stránke **korona.gov.sk** silnému **DDoS útoku**.
- **Dopad:** Útok trval takmer hodinu a spôsobil, že sa občania v kritickom čase nabehnutia nových termínov nemohli prihlásiť na očkovanie.
- **Pôvod:** Národné centrum zdravotníckych informácií (NCZI) vtedy potvrdilo, že nešlo o technickú chybu na ich strane, ale o cielenú snahu o znefunkčnenie služby.
- **Zdroj:** Národné centrum zdravotníckych informácií (NCZI) – Aktuality 2021: nczisk.sk.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zraniteľnosti IoT zariadení

Útok na vodárenský systém na Floride (2021)

- **Priebeh incidentu (5. február 2021)**
- **Vzdialený prístup:** Útočník získal prístup k počítaču operátora prostredníctvom softvéru **TeamViewer**, ktorý slúžil na vzdialenú správu.
- **Manipulácia s chemikáliami:** Operátor si všimol, že sa mu po obrazovke hýbe kurzor myši a otvára ovládacie panely. Útočník zvýšil koncentráciu **hydroxidu sodného** (lúhu) z pôvodných 100 častíc na milión (ppm) na alarmujúcich **15 000 ppm**.
- **Záchrana:** Operátor okamžite po odhlásení útočníka manuálne vrátil hodnoty na normálnu úroveň. Ak by sa tak nestalo, trvalo by približne 24 až 36 hodín, kým by sa kontaminovaná voda dostala k obyvateľom, no systém by pravdepodobne spustil aj ďalšie automatické alarmy pH.
- **Hlavné bezpečnostné zlyhania**
- Vyšetrovanie ukázalo niekoľko kritických chýb v zabezpečení mesta:
- **Zdieľané heslá:** Všetci zamestnanci údajne používali **rovnaké heslo** pre prístup k systému.
- **Zastaraný softvér:** Počítače v čistiarni vôd bežali na operačnom systéme **Windows 7**, ktorému v tom čase už skončila podpora.
- **Absencia firewallu:** Systém nebol dostatočne oddelený od verejného internetu, čo umožnilo útočníkovi nájsť vstupný bod.
- **Zdroj informácií**
- Tento prípad bol široko dokumentovaný bezpečnostnými agentúrami (FBI, CISA) aj odbornými portálmi:
- **CISA (Cybersecurity & Infrastructure Security Agency):** Zneužitie softvéru pre vzdialený prístup v Oldsmar.

Útok na spoločnosť Verkada (Marec 2021)

- Tento incident patrí medzi najväčšie narušenia súkromia v histórii IoT, pretože zasiahol zariadenia, ktoré majú byť v prvom rade bezpečnostným prvkom.
- **Priebeh:** Skupina hackerov získala prístup k interným administratívnym systémom spoločnosti Verkada, ktorá poskytuje cloudové riešenia pre bezpečnostné kamery.
- **Rozsah:** Útočníci získali kontrolu nad viac ako **150 000 kamerami**.
- **Zasiahnuté subjekty:** Hackeri mohli sledovať živé prenosy z tisícok kamier umiestnených v nemocniciach, väzniciach, školách a firemných kanceláriách (vrátane skladov spoločnosti Tesla či softvérovej firmy Cloudflare).
- **Metóda:** Útočníci využili administrátorské prístupy, ku ktorým sa dostali prostredníctvom zraniteľnosti v systéme.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

BadBox 2.0 (2024 – 2025)

- Tento útok je považovaný za jeden z najväčších v histórii televíznych sietí. Hackeri infikovali viac ako **10 miliónov zariadení** (smart TV, set-top boxy, infotainment systémy v autách) už priamo v továrni pred ich predajom.
- **Dopad:** Infikované zariadenia slúžili na podvody s reklamou a ako súčasť botnetu pre DDoS útoky.
- **Kľúčové ponaučenie:** Zraniteľnosť dodávateľského reťazca (supply chain) je kritickým bodom IoT bezpečnosti.
- Zdroj: Asimily - Top IoT Breaches 2025

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Rekordný DDoS útok botnetu Aisuru (2025 – 2026)

- V roku 2025 sa objavil botnet **Aisuru** (známy aj ako TurboMirai), ktorý vďaka miliónom kompromitovaných IoT zariadení dosiahol doteraz nevídanú silu útokov.
- **Rozsah:** Podarilo sa mu vyvinúť silu až **29,7 Tbps**, čo takmer položilo časti globálnej internetovej infraštruktúry. Microsoft Azure musel v jednom momente blokovať útok s intenzitou 15,7 Tbps.
- **Zdroj:** Vectra AI - IoT Security in 2026

Raptor Train a Flax Typhoon (2024)

- Bezpečnostné zložky (vrátane FBI) odhalili v septembri 2024 sofistikovaný botnet riadený skupinou Flax Typhoon (spájanou s Čínou).
- **Zariadenia:** Viac ako **200 000 zariadení** (routery, IP kamery, NAS úložiská) v malých kanceláriách a domácnostiach (SOHO).
- **Cieľ:** Špionáž a exfiltrácia dát z kritickej infraštruktúry USA a iných krajín.
- Zdroj: The Hacker News - Raptor Train Botnet

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Masívny únik dát Mars Hydro (2025)

- Hoci nejde o klasický botnetový útok, incident u výrobcu smart pestovateľských systémov Mars Hydro odhalil slabinu v cloudovom prepojení IoT.
- **Dopad:** Kvôli chybe v konfigurácii cloudu bolo vystavených **2,7 miliardy záznamov**, vrátane Wi-Fi hesiel a identifikátorov zariadení užívateľov po celom svete.
- **Zdroj:** Asimily Report

Útoky na zdravotnícke IoT (2025)

- V prvej polovici roka 2025 bol nahlásený incident, pri ktorom bolo cez internet voľne prístupných viac ako **1 milión medicínskych IoT zariadení** (MRI prístroje, infúzne pumpy, monitory pacientov).
- **Riziko:** Hackeri mohli nielen kradnúť citlivé údaje pacientov, ale potenciálne aj na diaľku meniť nastavenia prístrojov, čo priamo ohrozovalo životy.
- Zdroj: Device Authority - Healthcare IoT Breach

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Štatistíky o bezpečnosti IoT v roku 2025

Štatistíky o bezpečnosti IoT v roku 2025:

- **Viac ako 50 % IoT zariadení obsahuje kritické zraniteľnosti**, ktoré môžu hackeri okamžite zneužiť. *(IBM X-Force Threat Intelligence)*
- **Jedna z troch bezpečnostných incidentov s únikom dát už zahŕňa IoT zariadenie.** *(Verizon DBIR)*
- **Botnet Mirai premenil nezabezpečené IoT zariadenia na armádu útočných strojov**, ktorá spustila jeden z najväčších DDoS útokov v histórii. *(Kaspersky)*
- **IoT zariadenia v zdravotníctve sú hlavným cieľom – útoky na medicínske zariadenia medziročne vzrástli o 123 %.** *(Extra)*
- **Nezaplátaný firmvér je zodpovedný za 60 % všetkých bezpečnostných incidentov IoT zariadení.** *(IoT Security Foundation)*
- **Kompromitované inteligentné kamery a senzory viedli k veľkým narušeniam dohľadu** v podnikovej aj vládnej sfére. *(CISA)*
- **Zlyhania v zabezpečení IoT stoja firmy v priemere 330 000 dolárov na incident.** *(NIST)*

▪ Zdroj: https://jumpcloud.com/blog/iot-security-risks-stats-and-trends-to-know-in-2025

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnostné odporúčania a návrhy opatrení

Bezpečnostné odporúčania a návrhy opatrení

- V priemyselnom internete vecí (IIoT – Industrial IoT) sú bezpečnostné odporúčania a návrhy ešte dôležitejšie než v bežnom IoT, pretože ide o kritické systémy ako výroba, energetika, doprava či infraštruktúra. Prehľad bezpečnostných odporúčaní a návrhov:
- 1. Silná autentifikácia a autorizácia
- 2. Šifrovanie komunikácie
- 3. Automatické aktualizácie a podpora výrobcu
- 4. Zabezpečenie fyzického prístupu
- 5. Oddelenie IoT zariadení od hlavnej siete
- 6. Bezpečnostné testovanie pred nasadením

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

1. Silná autentifikácia a autorizácia

- Základom zabezpečenia je možnosť zmeny predvolených prihlasovacích údajov a používanie silných hesiel.
- V ideálnom prípade by IoT zariadenia mali podporovať:
  - viacfaktorovú autentifikáciu
  - obmedzenie počtu pokusov o prihlásenie.

2. Šifrovanie komunikácie

- Prenos údajov medzi zariadením a cloudom alebo aplikáciou musí byť šifrovaný pomocou moderných protokolov (TLS 1.2 a vyššie).
- To znižuje riziko zachytenia citlivých údajov.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

3. Automatické aktualizácie a podpora výrobcu

- Výrobcovia by mali zabezpečiť dlhodobú podporu zariadení, rýchlu distribúciu bezpečnostných záplat a ideálne aj automatické aktualizácie firmvéru.
- Zákazníci by mali preferovať značky, ktoré dbajú na bezpečnosť.

4. Zabezpečenie fyzického prístupu

- Ak je to možné, IoT zariadenia by nemali byť fyzicky prístupné verejnosti.
- Dôležité je tiež fyzicky zablokovať rozhrania:
  - USB, UART alebo JTAG, ktoré môžu slúžiť na neoprávnený prístup.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

5. Oddelenie IoT zariadení od hlavnej siete

- Zariadenia IoT by mali byť umiestnené v oddelenej VLAN alebo segmente siete, čím sa zníži riziko šírenia útokov do kritickej infraštruktúry. Firewally a IDS/IPS systémy by mali monitorovať komunikáciu týchto zariadení.

6. Bezpečnostné testovanie pred nasadením

- Pred nasadením zariadenia do ostrej prevádzky by malo dôjsť k jeho testovaniu z pohľadu bezpečnosti – tzv. penetration testing.
- Zariadenia so známymi zraniteľnosťami by nemali byť používané.

Záver

- Internet vecí predstavuje revolučný krok v oblasti digitalizácie a automatizácie, no zároveň otvára dvere novým bezpečnostným rizikám.
- Zraniteľnosti v IoT zariadeniach nie sú len teoretickým problémom – sú reálnou hrozbou, ktorá už viedla k viacerým vážnym incidentom.
- Vzhľadom na narastajúci počet týchto zariadení v domácnostiach, firmách aj kritickej infraštruktúre je nevyhnutné, aby bola bezpečnosť braná vážne – nielen zo strany výrobcov, ale aj koncových používateľov.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Zraniteľnosti IoT zariadení

Bezpečnosť pri bezdrôtovej komunikácií, vzdialenom prístupe, využívaní cloudu a IoT zariadení (Blok VI)
Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

doc. Ing Jozef Papán, PhD

KC KYB UNIZA, https://kc.uniza.sk/

Jozef.Papan@uniza.sk