Příliš chytré budovy

(o dalších věcech nemluvě)

Bezpečnostní rizika „Internetu věcí“

RNDr. Marian Kechlibar, PhD.
CircleTech, s.r.o.

Spousta věcí se změnila v počítače

- Telefon dříve:

- Telefon dnes: počítač, který umí také telefonovat.
- V tomto případě je aspoň transformace fyzicky zjevná.

U jiných objektů to není tak patrné

- Automobil – dříve mechanické zařízení.
  - Nyní v podstatě počítač se čtyřmi koly, jedoucí rychlostí až 150 km/h, u dobrodruhů i více.
  - Dobrá okolnost: automobilky jsou na kvalitu software docela přísné, i když to není jejich hlavní činnost.
- Dům – dříve prostě nemovitost.
  - Postupně se mění v komplikovaného, decentralizovaného robota se zajímavými a někdy nebezpečnými periferiemi – třeba sporákem.
  - Špatná okolnost: výrobci takových zařízení kvalitu software až zas tak moc neřeší.

Tři části „chytrého“ vybavení domu

- Senzory.

  (teploměr, tlakoměr, čidlo detekující světlo nebo pohyb) - potenciální narušení soukromí.

- Processing (počítač).

  Ukládání údajů, jejich analýza. Část napadnutelná z Internetu. **Čím propojenější ven, tím hůře.**

- Periferie.

  Světla, klimatizace, topné zařízení, dálkově ovládané dveře garáže nebo domu, sporáky, trouby, domácí pekárny, televize…

  Právě tyto periferie mohou napáchat **nejvíce škod**.

2011: „Hackování“ laserové tiskárny

- Výzkumníci z Kolumbijské univerzity Salvatore Stolfo a Ang Cui zjistili, že někteří výrobci, včetně Hewlett-Packardu, digitálně nepodepisují svoje updaty firmware.
- Výsledek:

2013: Supermarkety Target

- Druhý největší obchodní řetězec v USA (po Walmartu), přes 1800 obchodů.

2013: Supermarkety Target

- V roce 2013 odborně „hacknuty“ nejspíš z Ukrajiny.
- Vstupní bod: dálkově ovládaná klimatizační zařízení.
- Útočníci ovládli pokladny, mrazáky, světla…
- Naštěstí šlo o profesionály, kteří šli „jen“ po údajích z platebních karet.

2015: Ovládnutí džípu Cherokee

- Dva „white hat“ hackeři, Charlie Miller a Chris Valasek, nainstalovali do džípu jedoucího po dálnici malware a spustili:
  - Maximální výkon klimatizace.
  - Palubní rádio přeladěné na hiphopovou stanici.
  - Přední i zadní stěrače a ostřikovače.
  - Vypnuli motor za jízdy.
  - Na parkovišti (kvůli bezpečnosti) deaktivovali brzdy.
- Tentýž hack by v USA fungoval na 471 000 dalších aut.
- Slabým bodem byl uConnect, systém stahující navigační údaje a média.

Video ilustrující hack vozidla

2016: Nemocnice v Los Angeles

- Hollywood Presbyterian Medical Center napaden hackery.
- Pachatelé zaheslovali databáze s údaji pacientů a vyřadili z provozu některé lékařské přístroje připojené k Internetu.
  - Laboratorní přístroje, tomografy.
- Nemocnice zaplatila za jejich znovuzprovoznění 17 tisíc dolarů v bitcoinech.
- Pachatelé nebyli odhaleni.

Základní problém software

- Bugy. Bugy. Bugy.
- Nevyhnutelný důsledek komplexity dnešních systémů.
- Velké firmy jako Apple, Microsoft a Google mají peníze a lidi na to, udržovat systém časných updatů.
- Menší firmy … škoda mluvit.
  - Příklad: nezáplatované routery.

Druhý základní problém software

- Uživatel. Uživatel. Uživatel.
- Bezpečnost vyžaduje od lidí určitou pozornost a námahu. Což se jim nelíbí.
- Výchozí PIN, heslo: 0000, 1234, admin/admin.
- Zůstávají nezměněny celá léta. Někdy změnit ani **nejdou!**
- Připojit takové zařízení na internet = riziko.

Podobenství cedníku

- V hrubém stavu se téměř jakýkoliv software podobá cedníku – tolik je v něm bezpečnostních chyb.
- Jednu po druhé musíte najít a „zaletovat“, přitom nevyrobit další. Navíc nejsou pouhým okem vidět.
- Pak vypustíte „cedník“ na moře internetu.
- „Vodě“ (hackerům) stačí jedna zapomenutá dírka, aby jej potopila.
- Internet usnadňuje všechno, tedy také útoky.

Následky jsou různě závažné

- Smazaná sbírka MP3 je nepříjemnost.
  - U běžného PC jsou škody obecně omezeny na digitální data uložená na disku, nanejhůře ovládnutí kamery.
  - Může jít o vážné poškození soukromí nebo obchodních zájmů, ale málokdy jde o život.
- Na dálku zapnutý spotřebič může být vysloveně nebezpečný svému okolí.
- Na dálku ovládaná zdravotní pomůcka…

Schází regulační rámec

- Na software (firmware) „chytrých“ zařízení nejsou kladeny v podstatě žádné zákonné požadavky.
  - Pozůstatek krásných dob, kdy se toho nedalo moc zkazit.
- Časem se to bude muset změnit.
- Do té doby je na uvážení architekta systému, co vlastně online být musí a co ne.

Děkuji za pozornost