(Ne)bezpečnost IoT

aneb Stále podceňované riziko

Michael Kupka

V minulosti, kdy moderní technologie jako internet či mobilní zařízení pronikly do všech sfér našeho života, tak i internet věcí (IoT) zaznamenává v posledních letech velmi vzrůstající popularitu. Zabezpečení těchto technologií tak zaujímá v našich životech čím dál tím důležitější roli. Navzdory několika výhodám, které jsou nám nabízeny, stále existují zranitelnosti, které vedou k možnému kybernetickému útoku. Důsledkem mohou být obrovské škody na majetku i na životě. Aby se šance na možný útok eliminovaly, musí být v tomto kontextu technologie přijaty s odpovídajícími bezpečnostními opatřeními v celém ekosystému.

Rozšíření sítě IoT

Za posledních několik let výrazně vzrostlo nasazení chytrých zařízení. Jejich přijetí není omezeno pouze na kancelářské prostory a výrobní haly, ale téměř na každou oblast života, kdy složité úkony nyní můžeme provádět jednodušeji. Stále více se nasazují například zdravotnická zařízení a prostředky připojené k internetu. Tato zařízení změnila život pacientů. Možnost měření zdravotních statistik doma bez nutnosti lékaře zlepšila jejich životní pohodu. Kromě segmentu zdravotnictví jsou přijímána další zařízení IoT ve finančních, průmyslových a mnoha dalších odvětvích. Je například možné propojit jednotlivé stroje a zařízení, získaná data v reálném čase vyhodnocovat a podle toho řídit stav zásob, tok objednávek a související servis (dnes nazýváno termínem Průmysl 4.0) – možnosti jsou nekonečné.

Hrozby

Kybernetické útoky vedené na veškerou k internetu připojenou techniku na sebe samozřejmě nenechaly dlouho čekat, a zdůrazňují tím převážně riziko spojené s používáním těchto chytrých zařízení. Jeden takový incident byl ohlášen například v Los Angeles, kde kybernetický útok zastavil tisk novin jednoho z předních nakladatelství - Los Angeles Times. Zařízení napadená malwarem také v minulosti ochromila části infrastruktury, jako jsou elektrárny. I oblast zdravotnictví zaznamenala bezpečnostní incidenty – zdravotnické prostředky, které jsou připojeny k síti, mají většinou nízkou odolnost vůči kybernetickým útokům. Pokud jsou například kardiostimulátory, infuzní pumpy, dávkovače inzulinu a jiné ovládnuty hackery, diskutujeme zde o vážných dopadech na zdraví pacienta. Kybernetické útoky mohou mít za následek vyřazení celé nemocniční IT infrastruktury z provozu. Jedním z takových útoků byl ransomware WannaCry, který v nemocnici na Ukrajině ochromil celou počítačovou síť na několik týdnů.

Nová zařízení, stejné chyby

V druhé polovině roku 2018 varoval Interpol i FBI spotřebitele, že domácí IoT zařízení (routery, kamery, televize...) musí být vlastníky zabezpečeny stejně tak, jako je tomu u počítačů a mobilních telefonů.

V praxi se ale setkáváme s tím, že útočníci i v dnešní době stále typicky kompromitují zařízení se slabou autentizací či zastaralým firmwarem, který obsahuje zranitelnosti, nebo se velice jednoduše na zařízení přihlásí výchozími uživatelskými jmény a hesly. Přeci jen útoky na IoT cílí na slabá hesla již od jejich vzniku. Výrobci zařízení na toto téměř nereagují. Situaci nenahrává ani fakt, že zdrojové kódy některých malware pro IoT jsou dostupné na internetu. Mohou se tak navzájem zdokonalovat a výchozí hesla si předávat – čímž je možné vytvořit velice objemné databáze s přihlašovacími údaji do velkého počtu různých zařízení.

10 nejčastějších bezpečnostních chyb IoT

Jaká jsou tedy největší nebezpečí, kterým IoT právě teď čelí? Tuto otázku si firmy a koncoví uživatelé pokládají nejčastěji. Zjednodušeně se dá říci, že v dnešní době existuje mnoho hrozeb pro veškerou IoT techniku. Abychom udrželi všechna zařízení mimo nebezpečí, musíme veškeré tyto hrozby identifikovat a řešit.

Útokům je možné částečně předcházet již stávajícími technologiemi – aktivními monitoringy a inteligentními firewally, avšak tato řešení jsou často nákladná a nepokrývají

zabezpečení IoT zařízení jako takového. Každé zařízení by mělo být nastaveno a zabezpečeno individuálně, tak jako systémoví administrátoři spravují své servery.

Níže je uveden seznam deseti nejběžnějších bezpečnostních chyb či hrozeb, se kterými se při každodenní práci setkáváme a které řešíme s našimi zákazníky. Vždy prvním krokem je si tato nebezpečí uvědomit, protože jedině v reakci na ně můžeme přijmout vhodná ochranná opatření.

1. Nedostatečné aktualizace

Odhaduje se, že v tuto chvíli je na světě kolem 23 miliard zařízení IoT. Do roku 2020 by toto číslo mohlo vzrůst na téměř 30 miliard. Takový masivní nárůst počtu připojovacích zařízení samozřejmě nemůže zůstat bez následků.

Největším problémem všech domácností a společností, které IoT nasazují, je, že se starají převážně o jejich funkčnost a zapomínají na bezpečnost. Většina těchto připojených zařízení postrádá nové aktualizace. Nezřídka se stává, že zařízení nejsou aktualizovaná vůbec a v provozu jsou přesně v tom stavu, ve kterém byla zakoupena. Zařízení, která tak byla kdysi považována za bezpečná, se stávají naprosto zranitelná a s postupem časů čím dál náchylnější ke kybernetickým útokům. Skutečnosti nahrává i fakt, že vysoce konkurenční trh s různými IoT produkuje stále nová a nová zařízení, přičemž ta stará rychle ztrácejí podporu a bezpečnostní aktualizace.

Přitom právě výrobci by měli být na prvním místě tohoto článku – k tomu, aby lidé zařízení aktualizovali, musí mít tyto aktualizace k dispozici. Většina výrobců poskytuje například OTA (over-the-air) aktualizace, ale jen velmi omezenou dobu – jakmile vydají na trh nové zařízení, nechají starou generaci vystavenu útokům.

2. Nedostatečně zabezpečená autentizace

S obrovským množstvím IoT na trhu výrobci přehlížejí také fakt, že každé zařízení potřebuje řádný a silný autentizační mechanismus.

Chyby v těchto mechanismech často vedou k tomu, že neoprávnění uživatelé získají vyšší přístup, než by měli mít.

Velmi často se v praxi setkáváme s nedostatky v mnoha různých částech týkající se autentizace: většina zařízení postrádá požadavky na složitost hesla či dvoufaktorovou autentizaci, dovoluje uživatelům zvolit si jednoduché výchozí přihlašovací údaje, nevyžaduje buďto žádné nebo jen slabé šifrování a obsahuje chyby v procesu obnovení zapomenutého hesla.

Nesmíme zapomínat také na stále často se vyskytující zastaralé autentizační mechanismy, jako je například Telnet, či Basic HTTP autentizace, které nejsou žádným způsobem chráněny proti útokům hrubou silou.

3. Použití výchozích přihlašovacích údajů

Většina výrobců dodává zařízení s nastavenými výchozími přihlašovacími údaji a své zákazníky důrazně neinformuje, že je mají změnit. Jedná se opět o jednu z největších hrozeb zabezpečení IoT, protože výchozí hesla jsou veřejně dohledatelná a útočníci je mohou velice snadno zneužít.

Podobné je to s hesly, která nejsou dostatečně komplexní. Existuje mnoho zařízení, do kterých se lze přihlásit hesly „1234“ či „password“ – takto slabé přihlašovací údaje představují pro útočníky velmi snadnou kořist.

4. Vzdálený přístup

V minulosti byly na serveru WikiLeaks publikované dokumenty, které poukazovaly na to, že centrální zpravodajská agentura Spojených států (CIA) cíleně útočila na IoT zařízení s cílem sledovat kamery a odposlouchávat mikrofony bez vědomí jejich vlastníků. Možnost, že nejen útočníci, ale i vláda mohou vniknout do různých zařízení a sledovat majitele, aniž by tito o tom měli sebemenší tušení, je děsivá.

Hrozba vzdáleného přístupu k zařízení zahrnuje nejen přítomnost bezpečnostních zranitelností v síťových službách, které jsou na zařízení spuštěny, ale také, že tyto služby jsou často vystavené ven do prostředí internetu i v situacích, kdy to vůbec není nutné.

5. Slabé fyzické zabezpečení

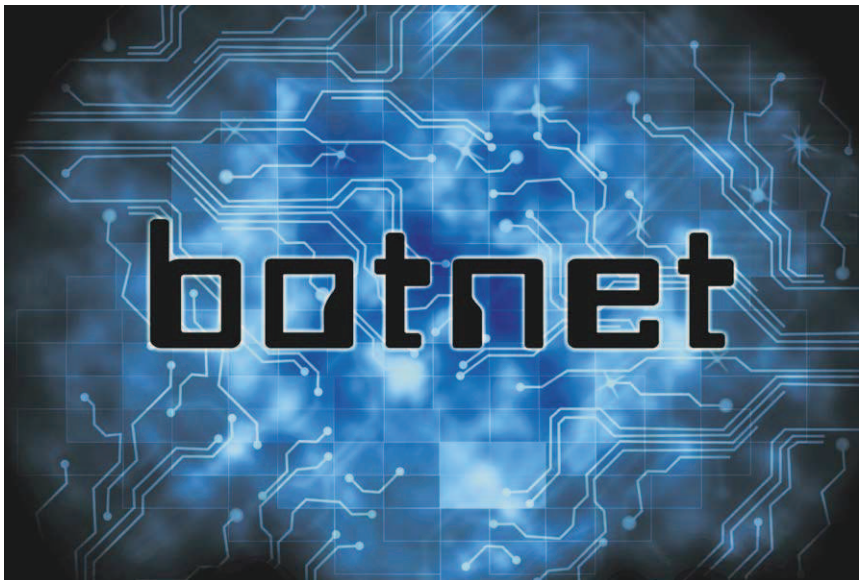
Prozatím jsme hovořili pouze o softwarovém zabezpečení, ale to není pro IoT jediná hrozba. Pokud není zařízení dostatečně zabezpečeno fyzicky, může do něj útočník snadno získat přístup bez vynaložení velkého úsilí.

Fyzická slabina zahrnuje riziko rozebrání zařízení a přístup k jeho paměťovému úložišti. Potenciální útočník je schopen získat přístup do systému i možností připojení se k USB portu či jinému konzolovému portu.

6. Nezabezpečená komunikace

Mnoho IoT zařízení nešifruje síťovou komunikaci. Toto je opět jedna z největších bezpečnostních výzev IoT. Stále se při práci s nejrůznějšími zařízeními setkáváme s takovými, jejichž administrační rozhraní i komunikace s cloudem probíhá přes nešifrovaný protokol HTTP. To, aby komunikace mezi zařízeními a cloudovými službami byla bezpečná a šifrovaná, musí zajistit převážně výrobci.

Nejlepší možnost pro zajištění bezpečné komunikace je použití šifrovaného přenosu a standardů, jako je TLS 1.2 a vyšší. Vytvářet komunikaci, která udržuje přenášená data v bezpečí a důvěrná, pomůže také izolace zařízení pomocí různých sítí (například pouze Bluetooth interně mezi jednotlivými moduly



a Wi-Fi do internetu). Vezměme si příklad z webových aplikací – za poslední roky zaznamenaly rapidní nárůst nasazení šifrování.

7. Odposlouchávání a Man in The Middle útoky

S předchozím bodem souvisí také typ útoku, kdy útočník odposlouchává komunikaci, která směřuje z i do IoT zařízení. V tu chvíli je možné s touto komunikací i manipulovat, zatímco obě komunikující strany o tom nemusí mít ani tušení. Tyto útoky mohou být pro zúčastněné strany velmi nebezpečné, protože jsou ohroženy veškeré citlivé informace uvnitř komunikace - například data senzorů.

Je dobré si uvědomit, že odposlech se nemusí týkat jen Ethernetu a Wi-Fi sítí. Pozornost při zabezpečení musí být věnována také dalším populárním bezdrátovým technologiím, jako je Bluetooth či Zigbee.

8. Únik osobních dat

Většina IoT zařízení shromažďuje data různého druhu, která obsahují citlivé informace. Pokud zařízení začnou shromažďovat osobní údaje, aniž by pro ně byla použita jakákoli vhodná metoda ochrany, považujeme to za vážné narušení soukromí. Hovoříme zde o telemetrii, zasílání diagnostických či statistických informací, které by ovšem měly obsahovat jen nutné minimum.

Veliké opatrnosti je potřeba také, pokud je k IoT k dispozici mobilní aplikace. Téměř všechny aplikace pro chytré telefony (na platformách iOS i Android) v dnešní době vyžadují pro jejich používání určitý druh oprávnění. Tato oprávnění je zapotřebí kontrolovat a zjistit, jaký druh dat tyto aplikace shromažďují. Pokud jsou shromažďované údaje osobní a citlivé povahy, je vždy lepší aplikaci odinstalovat a hledat alternativy.

9. Nedostatek znalostí

Jedná se o hrozbu, kterou lze snadno vyřešit řádnou edukací a sdílením znalostí. Lidé buď o internetu věcí moc nevědí, nebo se o to nestarají. Přitom příčinou narušení bezpečnosti domácí či firemní sítě může být často právě jen nedostatek znalostí jejich provozovatele.

Pro každého jednotlivce by mělo být poskytování všech znalostí o internetu věcí, připojených zařízeních a hrozbách prioritou. Koneckonců právě znalosti správných a osvědčených postupů či možností nastavení zabezpečení mohou být rozdílem mezi bezpečnou sítí a kybernetickým útokem. Oproti nasazení sofistikovaných firewallů a bezpečnostních prvků se jedná o nejlevnější způsob, jak zvýšit bezpečnost IoT infrastruktury.

10. IoT botnety

Tato hrozba spojená s IoT se v poslední době vyskytuje stále častěji. Využitím některé z chyb či hrozeb charakterizovaných výše nahraje útočník do IoT zařízení malware. Tím může zařízení zcela ovládnout a připojit ho do takzvaného botnetu s ostatními napadenými zařízeními.

Typické zneužití takového botnetu je buď k provádění útoků DDoS (Distibuted Denial of Service) s cílem odstavit určitou službu, či dnes velmi populární těžba kryptoměn.

K těmto útokům lze využít téměř jakékoliv zařízení připojené do internetu, ať už se jedná o webkamery, tiskárny, televize, chytré hodinky, nebo i dětské chůvičky. Kompromitovaná zařízení mohou útočníci také přeměnit na e-mailový server. Jmenujme případ, kdy byla zdrojem šíření SPAMu chytrá lednička.

Závěrem

Inteligentní zařízení jsou na vzestupu. Prognózy naznačují, že do roku 2020 jejich počet přesáhne světovou populaci čtyřnásobně. U výrobců však stále není bezpečnost nejvyšší prioritou; některá zařízení dosud postrádají šifrování, nadále neexistují upozornění ke změně výchozího hesla během počátečního nastavení nebo oznámení o vydání nových verzí firmwaru a samotný proces aktualizace může být pro průměrného uživatele složitý. To činí IoT zařízení snadným terčem pro útočníky. Je paradoxem, že ačkoli jsou snáze napadnutelná než počítače, často hrají důležitou roli v domácí infrastruktuře – některá spravují internetový provoz, jiná pořizují videozáznamy, další ovládají domácí techniku (alarmy, vytápění, světla, atd.).

I počet malware pro chytrá zařízení se zvyšuje. A to nejen v množství, ale i kvalitě. Kromě toho, že je využíváno velkého množství exploitů, útočníci mezi sebou i velmi často spolupracují; jeden malware může mít několik autorů a využívat moduly z jiných malware.

Zde přinášíme několik jednoduchých tipů, které minimalizují riziko infekce chytrých zařízení:

- Pokud to není nezbytně nutné, zakažte přístup k zařízení z internetu. V opačném případě používejte pro přístup k zařízení vždy šifrovaný kanál.
- Pravidelně kontrolujte nové verze firmwaru a zařízení aktualizujte.
- Pro přístup do zařízení používejte složitá hesla o délce nejméně 8 znaků, včetně velkých a malých písmen, číslic a speciálních znaků.
- Změňte tovární hesla při počátečním nastavení (i když vás k tomu zařízení nevyzve).
- Zablokujte nepoužívané služby a porty, pokud je to možné. Jestliže se například k routeru nepřipojujete přes Telnet (port TCP 23), je dobré jej vypnout, abyste tím nenechali otevřená vrátka pro potenciální útočníky.
- Již nainstalovaného škodlivého malware se v některých případech můžete zbavit i jen pravidelným restartováním zařízení. ■

Michael Kupka

Autor článku je Cyber Security Specialist ve společnosti AEC.