Smart Cities

Chytrá města budoucnosti

Lukáš Bláha

Slovní spojení Smart City, v českém překladu chytré město, se posledních několik let skloňuje ve všech možných směrech a patrně každý z nás se s ním již v nějakém významu setkal. Jelikož se však jedná o velmi mladý obor, neexistuje doposud žádná jeho přesná a ustálená definice. Souhrnně můžeme říct, že primárním cílem Smart City je nalézt jakýsi koncept, který bude schopný městům zajistit trvale udržitelný model rozvoje, vysokou kvalitu života, bezpečnost obyvatel a maximální efektivitu využití energie. To vše pomocí využití těch nejmodernějších technologií.

Než se však pustíme do více technické diskuse o chytrých městech, uvedeme si na začátek samotnou motivaci pro jejich vznik. Města hrají velkou roli v sociálních a ekonomických aspektech našeho života a mají obrovský dopad na životní prostředí. Za posledních 35 let došlo na celém světě k nárůstu populace přibližně o 60 %, což odpovídá navýšení počtu obyvatel o více než 2,8 miliardy. Další výzkumy ukazují, že tento trend bude i nadále pokračovat. S tímto tvrzením jde ruku v ruce i fakt, že čím dál více lidí se stěhuje do městských aglomerací, především kvůli větší nabídce pracovních příležitostí. Pro zajímavost, v České republice je míra urbanizace přibližně 75 %, tudíž pouze čtvrtina obyvatel žije mimo město. Především tyto dva důležité faktory jsou odpovědí na otázku, proč se v poslední době tak velké množství vědeckých institucí na celém světě orientuje právě na výzkum v oblasti Smart City. Na druhou stranu musíme uvést, že další obrovskou motivací především pro komerční sféru je bezesporu vytvoření nového průmyslového odvětví, které povede k dosažení nemalých finančních zisků. Dle dosavadních analýz a předpovědí bude v této oblasti do roku 2020 zapojeno přibližně 600 měst po celém světě a náklady spojené s vybudováním chytrých měst se budou pohybovat okolo 400 miliard amerických dolarů.

Jak již bylo naznačeno v úvodu, pojem Smart City se zabývá především efektivitou a optimalizací využití energií, dopravní infrastruktury či zlepšení funkce městské správy např. prostřednictvím veřejné online dostupnosti informací a dat s cílem umožnit občanům přehled o hospodaření a službách nabízených veřejnosti. Pro názornost uvedeme několik konkrétních případů, ke kterým mohou být systémy chytrých měst využívány:

- Sledování a optimalizace dopravy – indikace cesty, která se vede mimo zácpu
- Inteligentní cestování v MHD – inteligentní jízdné, informace o změnách v dopravě a mimořádných spojích
- Chytré parkování pomocí mobilní aplikace, která ukáže cestu na nejbližší volné místo
- Spravování pouličního osvětlení – rozsvícení lamp při identifikaci pohybu či nastavení intenzity podle počasí
- Správa odpadu – automatické lisování, indikace zaplnění a optimalizace svozu
- Využití mobilní aplikace pro lepší orientaci občanů na úřadech, navigaci turistů městem či hlášení závad

Je důležité zdůraznit, že Smart City není čistě technický obor. Zahrnuje propojení velkého množství různých profesí, a i když jsou nejmodernější technologie jeho nedílnou součástí, vystupují zde pouze jako jeden z nástrojů, který má obyvatelům města zajistit kvalitní život a zefektivnit využívání energií a služeb. To, že má město inteligentní a energeticky efektivní pouliční osvětlení, ještě neznamená, že je zároveň Smart. Základním technickým prvkem chytrých měst jsou koncová zařízení, ve většině případů senzory nebo též čidla či snímače. Senzory jsou ve své podstatě velmi jednoduchá zařízení, která umí měřit určitou fyzikální nebo technickou veličinu. Ty se dále spojují do senzorových sítí, které dokážou vygenerovat velké množství informací o nejrůznějších změnách v prostředí. Důležitou funkcí v rámci chytrého města je sdílení nasbíraných informací mezi různými systémy. Pokud chceme vylepšit vzájemnou spolupráci jednotlivých komponent, potřebujeme sdílet informace s uživateli a poskytovat data mezi jednotlivými systémy, ideálně v reálném čase. To, co poté dělá celý koncept Smart City opravdu chytrým, je analýza obrovského množství dat (tzv. Big Data) a následné provedení definovaných akcí. Vzájemné propojení produktů, služeb a osob do jednoho celku prostřednictvím takzvaného Internetu věcí (Internet of Things – IoT) umožnily především následující faktory:

- Díky novým technologiím umíme čidla a další zařízení levně připojit k internetu

- Ceny čidel a potřebného hardwaru jsou mnohem dostupnější
- Velká část populace používá chytré telefony, které se do řešení dají vhodně zapojit
- Internet je nyní dosažitelný i v dříve hůře dostupných oblastech

Tento velmi rychlý a téměř neřízený rozvoj a technologická komplexnost integrace stávajících infrastruktur s poměrně mladými internetovými technologiemi, jako jsou například cloudové služby, chytré telefony a mobilní aplikace, nositelná elektronika (wearables), bezdrátové technologie (Wi-Fi, RFID, NFC) či nová fyzická rozhraní, otevírají dveře potenciálním kybernetickým hrozbám.

Nové technologie jsou kvůli nutnosti jednoduchého použití a rychlého uvedení na trh často vytvářeny bez ohledu na bezpečnost a jsou doslova zamořeny bezpečnostními zranitelnostmi. Častým nedostatkem je nedostatečná ochrana bezdrátové komunikace. Ta je dostupná komukoliv v blízkém dosahu a je náchylná na odposlech. V kombinaci s použitím vlastních protokolů, které jsou často nešifrované nebo obsahují chybně implementovanou kryptografii, může docházet k modifikaci probíhajícího provozu a tím pádem i k nebezpečí kritického zásahu do celého systému. Další komplikací je aktualizace systémů a nasazení bezpečnostních záplat. Výrobci zařízení reagují na nalezené nedostatky velmi pomalu, a aktualizace jsou tak vydávány s velkým zpožděním. U některých výrobců méně známých značek se záplaty dokonce ani nedočkáte. A co dělat v případě, když aktualizace není k dispozici? Jedinou bezpečnou možností je danou službu dočasně vypnout, což může mít vážný dopad na fungování celého systému. Navíc je nutné mít na paměti, že celý systém chytrého města je značně komplikovaný a vzájemně provázaný. Je v něm použito velké množství různorodých senzorů a zařízení, které představují širokou škálu možných vektorů útoku. Další typickou chybou je například nedostatečná kontrola fyzického zabezpečení koncových prvků. Útočník s přímým přístupem k zařízení může poměrně snadno podvrhnout měřené hodnoty či prvky úplně odstavit. Chyby se však

mohou vyskytovat ve všech částech informačního systému, nejen v koncových zařízeních. Častým cílem jsou nezabezpečené webové a mobilní aplikace, které jsou používány ke správě systémů či komunikaci s občany. Nesmíme také zapomenout na zastaralé infrastrukturní prvky, na jejichž výměnu nebývá v rozpočtu myšleno.

V případě Smart City, jejichž podstatou jsou složité vazby a závislosti nejrůznějších systémů, je nezbytný proaktivní přístup a nastavení spolupráce a předávání informací v celoměstském, ne-li celostátním měřítku. O tuto především procesní bezpečnost by se měl starat lokální CERT (Cyber Emergency Response Team), který však kvůli finančním důvodům většinou neexistuje. Tým by se měl zabývat problematikou koordinace bezpečnostních incidentů a sdílení informací. Měl by zároveň zajišťovat záložní služby či postupy v případě mimořádných událostí, definovat formální komunikační kanály, omezit přístup k veřejně dostupným údajům a monitorovat pohyb a přístup ke zpracovávaným informacím. Jeho existence by měla být zajištěna už při výběru jednotlivých komponent systému, kde by od výrobce před zakoupením měla být vyžádána a důkladně analyzována veškerá bezpečnostní dokumentace. Žádný systém či zařízení by nemělo být nasazeno bez provedení bezpečnostních testů. Splnění požadavků jednoduchého seznamu obsahujícího základní kontroly šifrování, autentizace, autorizace a softwarových aktualizací dokáže výrazně zvýšit úroveň bezpečnosti celého systému. V rámci SLA by měla být s dodavatelem pevně stanovena doba na vydání kritických záplat a zajištěna dostupnost 24/7 v případě vzniku bezpečnostních incidentů. Bezpečnostní politika by měla zahrnovat i pravidelné provádění penetračních testů všech sítí a zařízení po určité době či po jakémkoliv větším zásahu do systému. Vývoj v této oblasti je velmi rychlý, proto by měly být pravidelně aktualizovány modely hrozeb a možné scénáře, jak na ně reagovat.

Přestože nástup chytrých měst bude především tématem blízké budoucnosti, zavádění inteligentních systémů můžeme pozorovat již v současné době. Velké evropské metropole jako Amsterdam, Barcelona či Stockholm mají již dnes implementovány systémy pro chytré parkování, kontrolu intenzity veřejného osvětlení, optimalizaci dopravy či zavlažování parků. V České republice je průkopníkem v této oblasti město Písek a postupně se připojují i ostatní města, jako například Pardubice, Brno a některé části Prahy. Díky rychlému rozvoji v této oblasti je pouze otázkou času, kdy se kybernetické útoky na městskou infrastrukturu a služby stanou reálnou hrozbou. Chytrá města se velmi snadno mohou stát hloupými, či dokonce životu nebezpečnými, pokud zpracovávaná data a související infrastruktura nebude dostatečně zabezpečena. ■

Lukáš Bláha

Autor článku působí jako Senior IT Security Consultant ve společnosti AEC, a. s.