Jak posílit bezpečnost Internetu věcí

Jako všechno nové bude i internet věcí vystaven rostoucím hrozbám způsobeným zejména jeho bezpečnostními slabinami, jichž protivníci okamžitě využijí. Spíše než jednotlivá zařízení budou hackeři napadat a zneužívat celé sítě internetu věcí. Obrana ale existuje.

Internet věcí (Internet of Things – IoT), propojení nespočetného množství levných, jednoduše dostupných a většinou nepříliš dobře zabezpečených zařízení. Obrovské množství dat je ideální živnou půdou pro kybernetickou zločinnost. A nejde jen o zákeřné zločince v tradičním slova smyslu, ale také o skvělou příležitost pro zdatné vtipálky a škůdce bez záměru doslova z celé planety. Především je třeba si uvědomit, že mobilní zařízení, telemetrické a regulační systémy a zejména obrovskou rychlostí rostoucí množství nejrůznějších spotřebních přístrojů – od celých inteligentních domů přes domácí spotřebiče, televizory, ledničky, pračky, meteostanice, zařízení domácí automatizace, ale i pečící trouby nebo varné konvice až po inteligentní oblečení, wearables – připojených k internetu nejsou ve většině případů ničím jiným než zařízeními vybavenými určitým výpočetním výkonem a schopností komunikace. Potenciálně tudíž představují obrovskou možnost kriminálního zneužití či napadení. Propojené skupiny zařízení, z hlediska interního uspořádání téměř identických s relativně nízkou „inteligencí“ i úrovní zabezpečení, jsou navíc snadnými cíli. Je třeba učinit vše pro to, aby zařízení nebylo možné kompromitovat, ovládnout a zneužít, ukrást či modifikovat data, ale také zajistit, aby v opačném případě bylo možné vše co nejrychleji odhalit, identifikovat a přijmout opatření, která zneužití zabrání.

Ke snížení bezpečnostních rizik při provozu a poskytování IoT infrastruktury a produktů založených na mobilních komunikacích slouží i navržené řešení aktivní bezpečnosti. Původně bylo vyvinuto specialisty Security Expert Centra O2 IT Services pro zabezpečení mobilního aplikačního řešení O2. Najde však uplatnění zejména v automatizovaných systémech M2M komunikace a v rozsáhlých IoT sítích.

IoT komunikační model

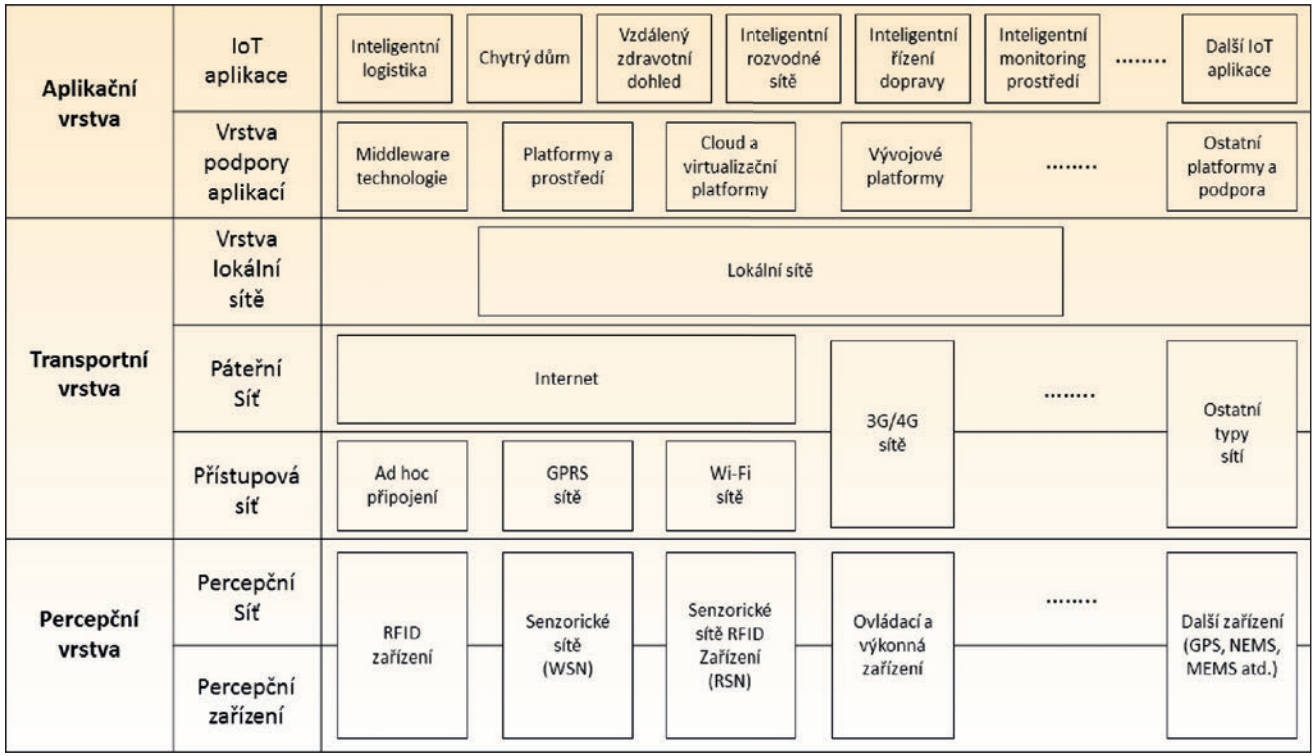
Komunikaci IoT lze popsat [1] třívrstvým komunikačním modelem (viz Obr. 1). Nejnižší percepční vrstva zahrnuje fyzická zařízení: snímače, senzory, čidla, ovládací a další obecně koncová zařízení a sítě, které je propojují nebo připojují k přístupové síti. Druhá vrstva je transportní a zajišťuje komunikaci mezi koncovými zařízeními a aplikacemi, které s nimi pracují nebo je ovládají. Transportní vrstvu tvoří celkem tři podvrstvy: přístupová síť, páteřní síť a lokální síť. Přístupová síť zprostředkuje komunikaci mezi percepční sítí koncových zařízení a páteřní sítí, která zajišťuje dálkový přenos dat mezi aplikacemi uživatele a vzdálenými koncovými zařízeními. Aplikace může, ale nemusí, být provozována i na systémech připojených do lokálních sítí. Nejvyšší aplikační vrstvu tvoří aplikace pro práci s koncovými zařízeními a technologie pro jejich provoz a podporu.

Obecně samozřejmě platí, že bezpečnost IoT systému je určena bezpečností každého prvku vyskytujícího se v komunikačním modelu. Zatímco aplikační a transportní vrstvy lze z hlediska bezpečnosti považovat za více či méně standardizované, bezpečnost koncových zařízení je velmi proměnlivá a nezřídka chabá. Není cílem tohoto článku podrobně analyzovat bezpečnost jednotlivých typů koncových zařízení. Metody aktivní bezpečnosti se obecně týkají zabezpečení komunikačního kanálu IoT jako celku.

Holistický přístup k bezpečnosti IoT systému

Jak plyne z komunikačního modelu, IoT systém obsahuje značné množství míst potenciálně použitelných k útoku a průniku. Zabezpečení musí tedy zahrnovat zařízení, data, komunikační sítě i aplikace. Základní schéma bezpečnostního modelu IoT systému [2] znázorňuje (viz Obr. 2). V souladu s třívrstvým komunikačním modelem se bezpečnostní model dělí na dvě části: bezpečnost koncových zařízení, která rámcově odpovídá bezpečnosti na percepční vrstvě, a IT bezpečnost, které v zásadě odpovídá bezpečnosti na transportní a aplikační vrstvě. Z modelu lze odvodit několik důležitých skutečností. Především je zřejmé, že bezpečnostní charakteristiky koncových zařízení a percepčních sítí hrají klíčovou roli v bezpečnosti IoT systému. Vzhledem k jejich různorodosti jak z hlediska účelu, tak z pohledu interní inteligence, velikosti, možností napájení a dalších technologických faktorů, jsou však zajištění a standardizace jejich zabezpečení a komunikace velmi komplikované a půjde spíše o dlouhodobou záležitost. Lze se rovněž směle domnívat, že celkově budou pokulhávat za překotným rozvojem nejrozmanitějších nových zařízení. Z druhé strany oblast bezpečnosti jednotlivých IT komponent modelu, jak již bylo řečeno, je poměrně propracovaná i standardizovaná a při dodržování implementačních a realizačních požadavků lze na transportní a aplikační vrstvě zajistit relativně vysokou bezpečnost.

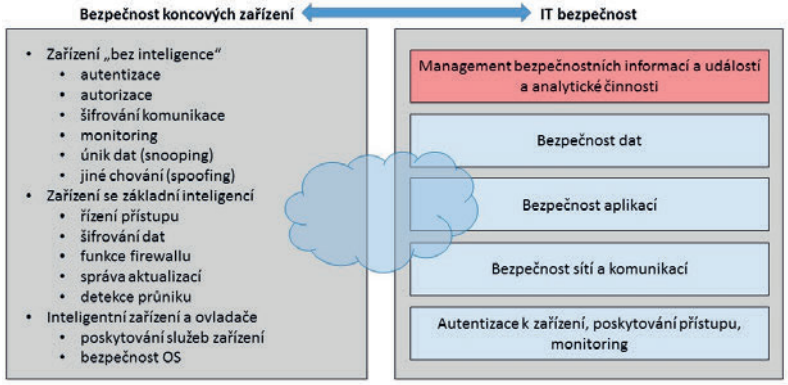
Důležitou, dosud ale poměrně opomíjenou roli v oblasti IT zabezpečení (a to nejen IoT) hraje management bezpečnostních informací a událostí (SIEM) a na něj navazující analytické činnosti poskytující globální pohled na chování systému a umožňující výrazně zvýšit jeho celkovou bezpečnost.



Obr. 1: IoT komunikační model

Role analýzy bezpečnostního chování pro zajištění bezpečnosti IoT systému

Management a analýza bezpečnostních informací a událostí umožňují na základě údajů o chování jednotlivých komponent získaných z jejich systémových záznamů, tzv. log management, vyhodnocovat bezpečnostní chování celého systému a na základě stanovených podmínek, tzv. korelací, detekovat jeho úzká místa a bezpečnostní slabiny, odhalovat



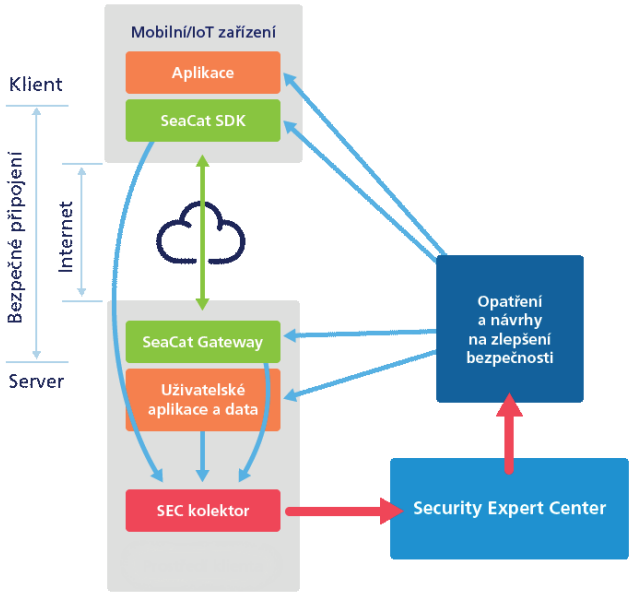
Obr. 2: Bezpečnostní model IoT

bezpečnostní incidenty, útoky a porušení bezpečnosti, identifikovat, zda v průběhu využívání nedošlo k narušení zabezpečeného kanálu např. podvržením podvodného certifikátu nebo zda provoz na něm nemonitoruje či dokonce nemodifikuje někdo nepovolaný třeba v důsledku kompromitace komunikujícího zařízení. Zdánlivě bezchybně pracující, leč kompromitovaný systém se totiž většinou stává časovanou bombou, kterou útočník může kdykoli spustit. Na základě následné analýzy zjištěných faktů lze přijímat operativní i dlouhodobá bezpečnostní opatření. Značnou výhodou uvedeného přístupu je mimo jiné vysoká úroveň automatizace procesu managementu, která umožňuje zpracovávat rozsáhlé objemy dat postupujících od velkého množství prvků současně a sledovat nejen jednotlivé komponenty IoT sítě, ale i chování celého systému. Je důležité zmínit, že výše uvedené principy lze prakticky beze změn přenést na nejrůznější aplikační systémy provozované v mobilních zařízeních, jako jsou pokladní nebo bankovní aplikace, formuláře, objednávky a mnoho dalších, které spolupracují např. s centrálními serverovými systémy a databázemi.

Aktivní zabezpečení komunikace koncových zařízení

Aktivní zabezpečení je inovativním způsobem ochrany IoT a mobilních systémů. Kombinuje použití zabezpečeného komunikačního kanálu s analýzou bezpečnostního chování celého komunikujícího systému.

Princip aktivního zabezpečení komunikace znázorňuje (viz Obr. 3). Aplikace v mobilním nebo IoT koncovém zařízení komunikuje přes internet s uživatelskou aplikací na serveru. Pro zabezpečení kanálu je zde použita bezpečnostní platforma SeaCat [3] firmy TeskaLabs, která díky pojetí bezpečnostní knihovny SeaCat SDK (viz Box 1), umožňuje jednoduše navázat zabezpečený



Obr. 3: Princip aktivního zabezpečení komunikace

šifrovaný komunikační kanál na libovolnou aplikaci. Přenášená data zprostředkuje serverovým aplikacím SeaCat Gateway. Analýza bezpečnostního chování je v tomto případě založena na službách Security Expert Center (SEC) od společnosti O2 IT Services [4]. Důležitým prvkem pro jejich využití je variabilní SEC kolektor, který lze přizpůsobit jakékoli mobilní nebo IoT platformě. SEC sleduje, zaznamenává, analyzuje a hodnotí bezpečnostní chování IT infrastruktury klienta. Na definované IT infrastruktuře realizuje bezpečnostní dohled, který umožní identifikovat její zranitelnosti, odhalit útoky a identifikovat bezpečnostní incidenty. Na základě výsledků hodnocení poskytuje podklady pro realizaci bezpečnostních opatření, popřípadě je pomůže uskutečnit. SEC kolektor, který shromažďuje systémové záznamy o průběhu a provozu komunikace i stavu prostředí a získané údaje předává do SEC ke zpracování a vyhodnocování, je umístěn v serverové části. SEC kolektor je možné navázat i na aplikační prostředí klientů, samozřejmě poskytuje-li systémové záznamy. Na základě výsledků analýz se poté identifikují bezpečnostní incidenty, hrozby, zranitelná místa a detekuje se případné narušení bezpečnosti komunikace, koncového zařízení i prostředí serveru. Operativně lze přijmout nezbytná opatření, např. zastavit komunikaci, dezaktivovat koncové zařízení nebo v případě zjištění potenciálních úzkých míst v zabezpečení alespoň zkvalitnit ochranu. Významným přínosem využití aktivní bezpečnosti je možnost sledovat, vyhodnocovat, statisticky zpracovávat a proaktivně zlepšovat bezpečnost rozsáhlých IoT sítí tvořených velkým počtem dílčích komunikačních kanálů.

Prověřeno v praxi

Důkazem, že výše uvedené řešení je funkční, může být připojení pokladního řešení O2 eKasa, které kromě odesílání povinných účetních informací do centrálního systému elektronické evidence tržeb poskytuje rovněž možnost bezpečně ukládat účetní informace do vzdáleného zabezpečeného úložiště. Rozšířená funkčnost je velice užitečná, ale přenášené informace jsou velmi citlivé a je potřeba je při přenosu z pokladen velice dobře chránit. Prostřednictvím webového portálu pak může uživatel s uloženými informacemi bezpečně pracovat např. z běžného kancelářského počítače. Aktivní zabezpečení založené na službě Security Expert Center, které eKasa využívá, zajišťuje, že veškeré předávané informace zůstanou nedotčeny, skryty potenciálním útočníkům, a současně odhalí případné útoky či narušení bezpečnosti přenášených dat pokladního systému.

Závěrem

Různorodost koncových zařízení, jejich omezené funkční schopnosti, diversita sítí, pokrytí mnohdy rozsáhlých

území a těžko dostupných míst spolu s velkými objemy dat, které nezřídka produkují, však činí IoT systémy velmi zranitelnými. Jejich ochrana se dnes opírá především o zabezpečování jednotlivých komponent a prvků, které se na struktuře IoT systémů podílejí: koncových zařízení, komunikačních kanálů a jejich součástí, aplikací a prostředí, v nichž jsou provozovány.

Podobný přístup umožňuje výrazně zvýšit bezpečnost IoT řešení, nemusí však být zdaleka dostačující. IoT systémy mohou tvořit stovky či tisíce dílčích komunikujících prvků a pro dosažení maximální bezpečnosti je proto třeba monitorovat a analyzovat bezpečnostní chování IoT systému jako celku. Může k tomu sloužit např. aktivní zabezpečení komunikace IoT a mobilních systémů založené na využití služeb Security Expert Center [4], které umožňuje jednoduše sledovat a vyhodnocovat chování systému, detekovat bezpečnostní incidenty, odhalovat útoky, pokusy o narušení bezpečnosti nebo identifikovat bezpečnostní slabiny a na základě získaných poznatků operativně přijímat příslušná opatření.

Jiří Sedlák
jiri.sedlak@o2its.cz

Ing. Jiří Sedlák

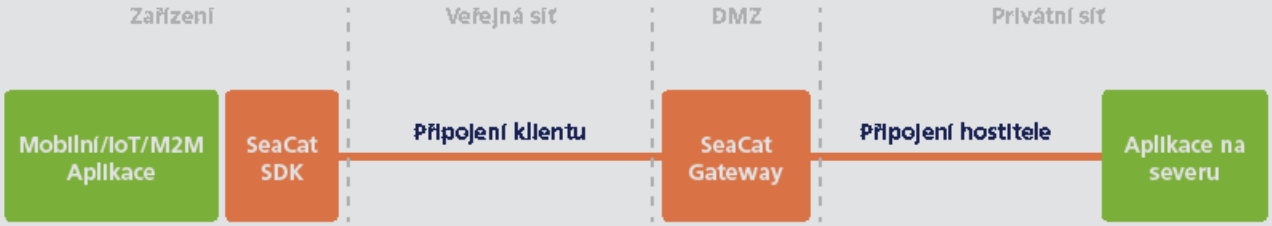
Jako krizový manažer má více než 15 let zkušeností z transformací společností a optimalizací modelů a systémů jejich řízení. Prošel významnými manažerskými pozicemi v prostředí telekomunikačních operátorů a energetických korporací, např. jako ředitel odboru Bezpečnosti ICT ve společnosti ČEZ ICT Services nebo bezpečnostní ředitel Telco Pro Services. V současné době je ředitelem Security Expert Center ve společnosti O2 IT Services.

Aplikační bezpečnostní platforma SeaCat BOX 1

SeaCat poskytuje zabezpečení pro komunikaci aplikací provozovaných na různých typech koncových zařízení, jako jsou chytré mobilní telefony, tablety, IoT nebo M2M zařízení či počítače, prostřednictvím veřejných datových sítí a internetu a chrání serverové aplikace před kybernetickými útoky. Integraci s mobilními, IoT a M2M aplikacemi zajišťuje klientská část, knihovna SeaCat SDK, která umožňuje vytvořit zabezpečené propojení aplikace v koncovém zařízení s odpovídající serverovou aplikací.

Základní komponenty: SeaCat SDK a SeaCat Gateway

Struktura:



Základní vlastnosti:

- jednoduchá implementace
- vysoká ochrana proti kybernetickým útokům na aplikační úrovni
- transparence pro vývojáře aplikací (nevyžaduje modifikaci vlastností aplikací)
- úspěšné využití v aplikacích, kde ostatní řešení nelze nasadit
- vysoká datová propustnost
- absence bodu selhání (SPoF)
- snadná administrace veřejných klíčů
- absence narušení bezpečnosti koncových zařízení se zastaralými bezpečnostními knihovnami
- podpora napojení na bezpečnostní monitoringy SIEM (podle RFC 5424, CEF)

POUŽITÉ ZDROJE

[1] QI JING, ANASTASIOS VASILAKOS, JIAFU WAN, JINGWEI LU, DECHAO QIU: Security of the Internet of Things: Perspectives and challenges, Wireless Networks 20(8):2481-2501, 11/2014
[2] PATRICK KEHOE, BRANDT HEATHERINGTON: Is the Internet of Things Too Big to Protect? Not if IoT Applications Are Protected!, Security Intelligence, 8/2015
[3] TeskaLabs: Introduction to SeaCat
[4] JIŘÍ SEDLÁK: Bezpečnost jako služba, nová dimenze vnímání informační bezpečnosti, DSM 1/2016, str. 15