BYDLENÍ
STAVBY REALITY

ORANGE controls

CHYTRÁ DOMÁCNOST KOMFORT I HROZBA

Moderní bydlení spolu s provozními úsporami a zabezpečením zajišťují nejnovější vyspělé technologie. Takové domácnosti můžeme říkat chytrá nebo digitální, ale vždy jde jen o jedno – vzájemné propojení techniky, kterou doma užíváme, její spolupráce a možná kontrola i ovládání prostřednictvím informačních technologií. Nejde o nic nového, takzvaná chytrá domácnost má už své dětské krůčky za sebou a nadneseně řečeno spěje k jakési své pubertě, v níž se teprve ukáže, zda ji dokážeme ovládat a využívat, nebo jestli ona z nás neudělá své služebníky. Dnes se už ukazuje, že obyvatel inteligentní domácnosti nemusí být odborníkem na informační technologie.

Z počátečních řešení se dostáváme k intuitivnímu ovládání, které pouze předpokládá, že alespoň jeden člen takové domácnosti si bude třeba jen minimálně rozumět s tabletem či smartphonem, i když i tato dnes téměř samozřejmá dovednost nebude v budoucnosti zřejmě nutná. Chytrá domácnost není o luxusu, stejně jako jím není dnes samozřejmé centrální vytápění, ale je to jen další krok ve vývoji komfortu bydlení. Zatímco dnes připadají na jednoho obyvatele dvě zařízení připojitelná k internetu, do pěti let jich už podle expertů bude přinejmenším pětadvacet, z toho pak bude právě na domácnost připadat více než dvacet.

Internet věcí

V souvislosti s termínem chytrá domácnost se stále více objevuje termín jiný – internet věcí, zkráceně IoT (Internet of Things). Není to jen o tom, že můžeme nosit takzvané chytré hodinky či fitness náramky, ale týká se to i zařízení pro inteligentní domácnost, například termostatů, IP kamer, chytrých žárovek a vůbec veškeré techniky, která je na základě vyhodnocení hodnot z okolí pomocí vlastních senzorů a jejich propojení na základě internetového protokolu (proto také IP – Internet Protocol) schopna patřičně reagovat. Samozřejmostí se už dávno staly přístroje, jako jsou teplotní čidla či detektory vody, různé stmívače, a je jen otázkou času, kdy se sníží ceny například bílé techniky s propojením přes IP, aby měla početnější zastoupení. Projekt a systémy chytré domácnosti se dají zařadit do několika okruhů. V první řadě se bude jednat o internetové připojení a počítačovou síť, na kterou už dnes často navazují multimediální i komunikační technologie a služby. O využití moderních technologií si vyloženě říká vytápění, klimatizace a osvětlení a rozhodně bychom neměli zapomínat na bezpečnost v domácnosti, jejíž řešení bude spočívat v dohledovém systému a v propojení s vnějškem v případě krizových situací. Pochopitelně, že mnohé může odradit prozatím vyšší cena takových systémů a někdy i nutnost stavebních úprav, ale je důležité si uvědomit, že vložené investice se z dlouhodobé perspektivy budou postupně vracet jak v úsporách třeba energie, času nebo na pojistném (v případě dobrého zabezpečení), tak i zvýšeným komfortem bydlení.

Hledá se konektivita

Dá se říci, že čím komplexnější řešení, tím lepší spolupráce různých zařízení a zároveň větší pohodlí pro uživatele. Tady je ale jeden problém – jsme na začátku, a to platí jak pro uživatele, tak pro výrobce chytrých zařízení. Pro nás se zvyšují nároky na znalosti i čas, potřebný k pochopení systémů, popřípadě údržby. To se dá řešit pomocí odborníků z oblasti informačních technologií, které by nám měl poskytnout většinou výrobce příslušných zařízení. U výrobců je to ale složitější. Tím největším problémem je neexistence jednotných standardů. Většina přístrojů jednotlivých značek kooperuje na vlastních platformách, jež ignorují ty konkurenční. Je to jednoduché a připomíná to historii záznamových zařízení, jejichž výrobci se snažili právě ten svůj systém prosadit, rozšířit a učinit z něj tak standard. Vypadá to tedy tak, že veškerá bílá technika, která by měla mezi sebou spolupracovat, musí pocházet od jedné značky, jinak jednotlivou techniku, která využívá různé komunikační systémy a protokoly, musíme řídit zvlášť. V praxi to pak znamená, že jediným propojovacím můstkem je právě náš chytrý telefon či tablet. U různých senzorů, IP kamer a detekčních zařízení to zatím není takový problém, protože je snadné si je od jednoho výrobce spolu s jejich systémem pořídit, horší je to třeba u bílé a černé techniky, kdy nám jednotlivé články výrobní řady jednoho výrobce nemusejí vyhovovat.

Zrádné televizory

Tyto problémy ale určitě jednou zmizí, co však bude hrozit – a dnes už opravdu hrozí – je možnost napadení zařízení, která jsou připojena k internetu. Zmínili jsme se, že na každého obyvatele Země dnes připadají dvě taková zařízení, ve vyspělých zemích je to mnohonásobně víc. Zatímco do počítačů si můžeme nainstalovat bezpečnostní software a mít je zabezpečeny těžko prolomitelným heslem, jinou techniku takto opatřit zatím nemůžeme. Doposud na to nemyslí řada výrobců, a tak „chytré“ přístroje nevyžadují přístupové heslo, a když, tak je to heslo univerzální, nastavené právě výrobcem, o dalším zabezpečení nemluvě. Co to znamená? Třeba hrubé narušení soukromí. Nejen odborníci určitě zaznamenali skandál, který znamenalo například skenování obsahu připojených pevných disků u televizorů LG a zároveň monitoring toho, co s přístrojem dělá uživatel. Jiné prolomení soukromí představovaly také trvale aktivované mikrofony televizorů Samsung s hlasovým ovládáním; to vše v souvislosti se síťovým propojením na servery výrobců. Zatímco v těchto případech se v zásadě jednalo jen o možnost úniku soukromých informací na veřejné sítě, u IP kamer už je situace horší. Přes nezabezpečenou kameru unikají záběry určené výhradně jejímu uživateli. Obraz dětského pokoje i s jeho obyvatelem, který nechávají monitorovat pečliví rodiče, nebo snímky dalších obytných prostorů či okolí domu, které kamery hlídají v nepřítomnosti majitele, určitě mohou zajímat potenciálního zloděje, který si svůj postup podle nich může naplánovat. Zvlášť kamera v televizi znamená nebezpečí, když se k jejímu ovládání dostane nepovolaný – diváci před obrazovkou si mnohdy její existenci totiž neuvědomí a chovají se, jak to říci, přirozeně či nenuceně.

Útok domácí techniky

Nedostatečné či vlastně zcela chybějící zabezpečení síťového rozhraní u moderních domácích spotřebičů je hrozbou. Programy mohou obsahovat malware (škodící software) či virus, čekající jen na aktivaci zvenčí. Tento postup není ničím novým. Už v osmdesátých letech minulého století umožnili Američané nenápadně ruským špionům ukrást elektronické systémy, které v sobě měly chybu, na kterou sovětská, po moderních technologiích žíznící ekonomika nemohla přijít. Kdo bude dnes čekat, že něco takového bude obsahovat chladnička komunikující s okolím na dálku prostřednictvím tabletu? Ano, řekneme si, co ale může malware v chladničce udělat? Začneme tím jednodušším a dobře rozeznatelným – bude sabotovat její chod, zvýší teplotu, začne ji vypínat. Co když ale cracker neboli průnikář využije její systémové prostředky a zařízení začne předávat na zadané adresy nezvladatelné množství různých požadavků? Ne u jednoho, ale u tisícovek podobných přístrojů. Pak dojde k tomu, že se zahltí servery a síť přetížením spadne. To není vize daleké budoucnosti, ale stručný popis toho, co se stalo letos v říjnu, kdy se domácí spotřebiče nedobrovolně staly součástí botnetu, tedy sítě řízené škodícím kódem. Problém je v tom, že se pak chyba může nekontrolovatelně šířit dál, kód ozkouší další zařízení a je-li i to špatně zabezpečené, nastává domino efekt. Lze proti tomu něco dělat? Část úkolu je na výrobcích, část na uživatelích. Je potřeba zabezpečit zařízení, které zabezpečit jde, např. datová úložiště nebo routery. Dále je nutné změnit základní přihlašovací údaje od výrobce u další techniky tak, aby je šlo jen obtížně prolomit, tedy žádné vstupní heslo „heslo9876“. Nejsme-li si zcela jisti, není problém se podívat třeba na stránky neziskovky Národní centrum bezpečnějšího internetu (NCBI).

Propojení bez problémů

Společnost Orange controls s. r. o., působící na českém trhu od roku 2004, produkuje systémy pro chytrou domácnost (řídicí systémy AMX, CUE, Crestron), které jsou plně programovatelné a otevřené produktům jiných výrobců. Tím se od naprosté většiny ostatních výrobců a jejich systémů liší. Pro zákazníka se řešení programuje a navrhuje na míru a není ničím limitované. Managing director společnosti Jakub Němec uvádí, že u většiny ostatních systémů se naráží na nějaké limity, například na uzavřenost systému pouze pro produkty dodávané výrobcem, pevné grafické prostředí, které nelze měnit, omezené možnosti ovládání a nedostatečný počet vstupních/ výstupních portů či nemožnost integrovat technologie přes lokální síť.