Zařízení Sigfox jsou chráněna před kyberútoky. K internetu se připojí pouze v případě potřeby.

Praha, 1. října 2019 - Bezpečnost a zajištění ochrany citlivých dat představují pro další rozvoj internetu věcí (IoT) tu nejzásadnější výzvu. Globální síť Sigfoxu, pokrývající i celé Česko, je proto vybudována na sofistikované bezpečnostní infrastruktuře tvořené miliony chytrých zařízení, komunikujících bez stálého připojení k internetu.

Nástup chytrých technologií je nezastavitelný. Podle analytické firmy Gartner se už nyní na světě nachází víc IoT zařízení než lidských bytostí. Polovinu z 8,4 miliard přístrojů tvoří běžné spotřebiče jako chytré televizory, ledničky, dětské chůvičky či domácí termostaty. Podle odhadů analytické firmy IDC dosáhnou v roce 2019 výdaje na IoT rekordních 745 miliard amerických dolarů, tedy asi o 15,4 % více než 646 miliard utracených v roce 2018.

Navzájem propojená chytrá zařízení mezi sebou přenášejí ohromné množství citlivých osobních a firemních dat, čímž vznikají nová a složitá bezpečnostní rizika. Spotřebitelé i firmy je však často podceňují a nakupují nejlevnější zařízení od výrobců zanedbávajících kvalitu zabezpečení. Ty jsou pak skrze vlastní IP adresu připojena přímo k internetu a tvoří ideální terč pro útoky hackerů.

Chytré technologie se také stávají součástí kritické infrastruktury státu či soukromých firem. Jejich absolutní spolehlivost, bezpečnost a schopnost chránit uživatelská data před zcizením je proto nezbytná. *„Důvěra našich partnerů a zákazníků v absolutní spolehlivost a bezpečnost systému je pro nás zásadní. Jediný větší únik citlivých dat by ji přitom mohl nenávratně poškodit. Proto je celá infrastruktura sítě Sigfox od začátku projektována tak, aby byla proti případným kybernetickým útokům imunní“,* vysvětluje Jan Soukal, výkonný ředitel provozovatele sítě Sigfox v ČR.

Přestože jsou zařízení Sigfoxu součástí internetu věcí, nejsou k internetu připojeny přímo ani nekomunikují přes internetový protokol (TCP/IP). Bezpečnost sítě Sigfox je naopak založena tom, že pro komunikaci využívá vlastní uzavřenou infrastrukturu s unikátní radiovou modulací. Jednotlivá zařízení se k ní v případě potřeby připojují přes speciální protokol a pouze v rámci úzce limitovaného časového rámce.

Inteligence chytrých zařízení spočívá v tom, že fungují pouze tehdy, kdy je to relevantní. Chytré čidlo tak může klidně dlouhé měsíce spát a probudí se pouze tehdy, když zaznamená změnu stavu, např. havárii vody domácnosti. V tu chvíli pošle prostřednictvím radiového signálu zprávu, která je přes základnové stanice a cloud Sigfoxu doručena až do aplikace v telefonu uživatele. Každá zpráva má přitom vlastní autorizační kód vytvořený sofistikovaným kryptografickým algoritmem. Díky tomu dokáže systém lehce rozpoznat případnou podvrženou zprávu a včas tak detekovat a eliminovat kybernetický útok vedený velkým množstvím zpráv s cílem síť ochromit.

Pokrytí technologií Sigfox je postaveno na robustní infrastruktuře tvořené hustou sítí základnových stanic (BTS) jejichž signál se navzájem překrývá. V Česku je momentálně takových stanic 320. Každá zpráva je přijímána všemi stanicemi v dosahu, takže při možném výpadku některé z nich se automaticky doručí přes jinou. Systém je tak vysoce imunní proti výpadkům či rušení.

V případě dotazů se prosím obracejte na:

agenturu Marcus&Art

Marek Němčík

M: 725 900 705

E: nemcik@marcusandart.com