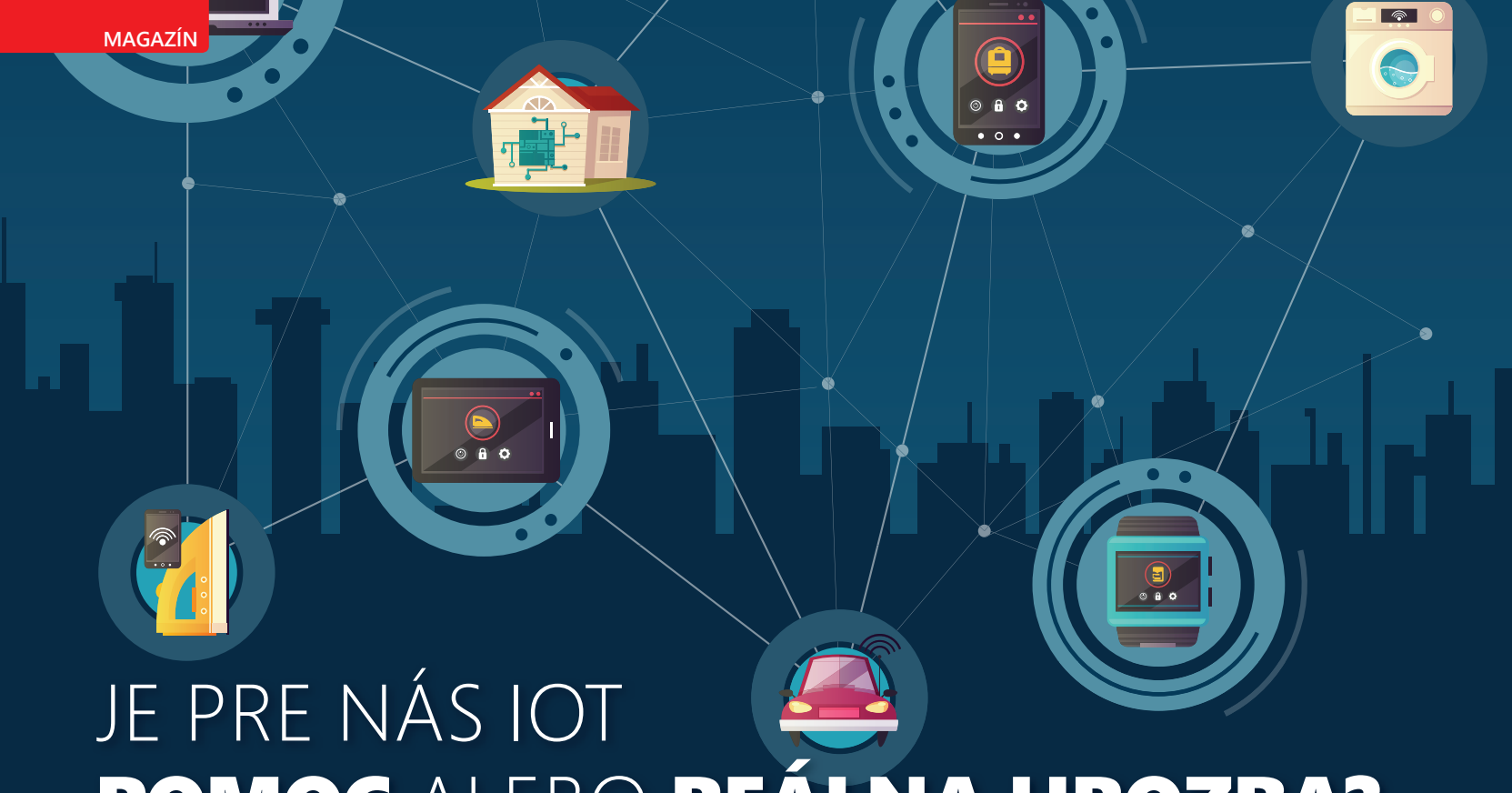

JE PRE NÁS IOT **POMOC** ALEBO **REÁLNA HROZBA?**

IoT je Internet of things alebo po našom Internet vecí. Čo si však za tým môžeme naozaj predstaviť, čo to vôbec znamená? Zložito povedané, je to novo vznikajúca internetovo založená technická architektúra zľahčujúca výmenu informácií a služieb v globálnom rozsahu. A jednoducho? Internet už dávno nie je vec vyhradená iba pre počítače. Dnes sú do siete pripojené inteligentné chladničky, osvetlenie, kúrenie, televízor, hlasoví asistenti v domácnostiach, automobily, tlačiarne, ba i domáci kávovar. A mohli by sme donekonečna pokračovať vo vymenovávaní. V roku 2020 bolo na svete takto pripojených odhadom 25 miliárd zariadení. A to reálny rozmach IoT ešte ani zďaleka nenastal. Takže do internetu vecí spadá každé obdobné zariadenie, ktoré je pripojené na internet vlastnou adresou.

Kedy sa objavil pojem internet vecí? Ako by ste ho vysvetlili zjednodušene?

Výraz internet vecí prvýkrát použil v roku 1999 Kevin Ashton, ktorý pracoval v oblasti sieťovej RFID (radio frequency identification) a vznikajúcich snímacích technológií. IoT sa objavil približne v rokoch 2008 – 2009 a odvtedy trend pripájania vecí/zariadení každodenného použitia na internet stúpa. Hovoríme im „inteligentné“ zariadenia, obsahujú softvér, senzory, elektroniku a sieťové pripojenie na internet, aby mohli komunikovať s inými zariadeniami.

Od roku 2008 sa mnohé zmenilo, rozmach inteligentných zariadení je neudržateľný, IoT však priniesol so sebou množstvo nielen pozitívnych aspektov...

Dnešný **rozmach IoT** vedie k inteligentnejšiemu a prepojenejšiemu svetu. Neprichádza však bez **rizík**. Kybernetická bezpečnosť, keďže sa IoT významne dotýka, je jeden z najdôležitejších faktorov. Riešenia internetu vecí poskytujú zaujímavé a hodnotné údaje jednotlivcom aj firmám. Aj keď sú ich výhody nepopierateľné, sú **citlivé na kybernetické útoky** (zariadenia IoT sú „od prírody“ nie príliš dobre zabezpečené). Len v prvom polroku 2019 zistila spoločnosť Kaspersky 105 miliónov útokov na koncové body IoT. Aj keď bezpečnosť zostáva hlavným záujmom riešení IoT, nedávny výskum ukazuje, že až 90 percent spotrebiteľov nemá dôveru v bezpečnosť zariadení IoT.

Aké sú trendy vo vývoji IoT a čo prinesie budúcnosť?

Trendy IoT v roku 2021 sa budú zameriavať najmä na základné ľudské potreby, domácnosti, kancelárie, ako aj na zaistenie bezpečnosti a ochrany zdravia a jeho monitorovanie.

Pripojené **zariadenia IoT** sa stanú všadeprítomnými. Pre pandémiu a obmedzenú mobilitu obyvateľstva sa možnosti a prínos vzdialeného monitorovania stali oveľa rozšírenejšími a tí, ktorí nikdy predtým neaktivovali vzdialené pripojenia, teraz tieto možnosti intenzívne využívajú. Masívna vlna zavádzania zariadení IoT je v plnom prúde, ale úsilie o zabezpečenie týchto zariadení sa začalo len nedávno.

Podľa najnovších odhadov webu Omdia (tracker trhu so zariadeniami IoT) sa očakáva, že globálna nainštalovaná základňa IoT vzrastie z dnešných asi 25 miliárd na 45 miliárd v roku 2025. S takým počtom zariadení dôjde k úmernému zvýšeniu rozsahu kybernetických hrozieb. Mnoho spoločností horlivo napreduje v iniciatívach týkajúcich sa internetu vecí.

Zvládne vôbec súčasná podoba internetu taký enormný nárast pripojených zariadení?

Tak ako sa musel zaviesť nový protokol IP adries z historického IP4 na nový IP6 z dôvodu ich vyčerpania, menia sa aj technológie na pripojenie veľkého počtu zariadení prenášajúcich nepredstaviteľné množstvá dát – mali sme tu 2G, 3G, 4G a dnes všade rezonuje 5G sieť. **Zavedenie technológie 5G skutočne spôsobí revolúciu na trhu IoT** uvoľnením jeho potenciálu prostredníctvom väčšej šírky pásma, nižšej latencie, zvýšenej kapacity, znížených nákladov a množstva ďalších výhod. To síce rozšíri možnosti správy zariadení z tisícov na milióny, **no slabé bezpečnostné postupy exponenciálne zvýšia mieru ohrozenia.** Takže môžeme očakávať rastúcu frekvenciu, sofistikovanosť a zložitosť kybernetických útokov zameraných na IoT.

Nesmieme zabudnúť ani na využitie automatizácie, umelej inteligencie (AI) a strojového učenia. Systémy AI sú v uskutočňovaní mnohých prvkov hrozieb internetu vecí lepšie ako ľudia, napríklad na opakujúce sa úlohy, interaktívne reakcie a spracovanie veľmi veľkých súborov údajov. Veľké globálne organizácie v roku 2020 zaznamenali zvýšený počet kybernetických útokov založených práve na IoT, a to vrátane veľkých útokov DDoS (Distributed Denial of Service). Rastúce zavádzanie IoT rozšírilo možnosti útoku a takmer každý priemyselný sektor je zraniteľný rôznymi kybernetickými hrozbami.

Je zaistenie bezpečnosti zariadení IoT taký problém?

Pri nasadzovaní systémov v akomkoľvek prostredí majú spoločnosti tradične tri alternatívy. Systémy môžu byť buď rýchle, alebo bezpečné, alebo lacné. A každá z týchto troch vlastností ide proti zvyšným dvom. Takže realita často núti organizácie, aby si vybrali iba dve. Čierny Peter väčšinou padne na **bezpečnosť**, zatiaľ čo náklady a pohodlie zostávajú.

Ale máme tu aj druhú stranu mince – bežného používateľa, ktorý denne v práci využíva niekoľko pripojených zariadení a doma desiatky ďalších, postačuje iba jedna slabina, aby útočník napadol všetky. V roku 2020 identifikoval Open Web Application Security Project (OWASP) desať najdôležitejších zraniteľností zabezpečenia IoT a prvou v zozname boli slabé, ľahko uhádnuteľné heslá. Na ďalšom mieste bola nedostatočná aktualizácia, čo môže viesť k tomu, že zariadenia budú pracovať na starom zraniteľnom firmvéri, aj keď sú k dispozícii nové zabezpečené aktualizácie.

Čo také sa môže stať, keď mi niekto „hackne“ kávovar alebo chladničku? Prečo je okolo bezpečnosti IoT taký rozruch?

Dôležité je si uvedomiť to, čo som už spomenul, že zariadenia ako kávovar alebo chladnička nikdy nie sú vo firemnej alebo domácej sieti osamote. Môžu slúžiť ako vstupná brána k iným zariadeniam, do celej siete. Preto je ideálne svoju sieť zónovať, teda do jednotlivých zón pripájať veci podľa dôležitosti alebo zraniteľnosti. Laicky povedané, tieto zóny alebo podsiete sa správajú ako samostatné celky a navzájom sa nevidia, t. j. ak príde k útoku napr. na spomenutý kávovar v jednej zóne, v inej zóne, kde máme citlivé údaje alebo pracovné stanice, je relatívne bezpečne.

Ale aj „hacknutie“ jednotlivých zariadení môže byť nepríjemné a priniesť nám finančnú ujmu alebo únik informácií. Spomeniem pár – tlačiareň môže začať nekontrolovane plnofarebne tlačiť a zastaví sa, až keď dôjde papier, kávovar môže celú noc v kancelárii pripravovať dookola cappuccino, inteligentná nabíjačka pustí viac voltov a ampérov do pripojeného zariadenia, ktoré dokonale zničí, hlasový asistent bude odpočúvať celú našu konverzáciu, kamera na televízore sa stane skrytým oknom do našej domácnosti, automobil nás prestane poslúchať v tej najhoršej dopravnej situácii a ohlási chybu motora, počas našej dovolenky sa doma vypne alarm a kamery poslúžia zlodejom na kontrolu situácie. A možno na zasmiatie je možnosť, že náš trávnik bude polievaný nonstop.

No už menej úsmevné sú „hacky“ zariadení, ktoré monitorujú zdravotný stav našich blízkych, dávkujú lieky, zachraňujú životy v hraničných situáciách.

A veta na záver?

Musíme si uvedomiť, že čím prepojenejšia je kritická infraštruktúra, tým zaujímavejšia je pre zločincov. Zatiaľ čo sa aj bezpečnosť stáva „inteligentnejšou“, využíva umelú inteligenciu vrátane nových technológií, ktoré sľubujú priniesť bezpečnejšie IoT, stále zostáva dôležitý ľudský rozmer a zdravý rozum.

» VLADIMÍR **PALEČKA,**
špecialista na kybernetickú bezpečnosť, Aliter Technologies, a. s.