Jak by asi vypadal útok na stát nebo celý svět v kybernetickém prostoru, aby ve svých důsledcích způsobil podobné dopady jako epidemiologická krize typu COVID-19

Atentáty a kyberterorismus za použití Internetu věcí

Úvod

Tzv. pátou dimenzí obrany se kybernetický prostor stal v roce 2016[1], kdy Severoatlantická aliance uznala vojenskou důležitost tohoto kosmopolitního a dynamicky se vyvíjejícího prostoru. Prostoru, který na poli bezpečnosti představuje nesčetné možnosti a vyžaduje velikou zodpovědnost. Prostoru, v němž budou dnešní obranné prostředky zítra zastaralé, ne-li překonané. A v neposlední řadě prostoru, o jehož hrozbách máme sice teoretické povědomí, ale doufáme, že nedojde k jejich praktickému naplnění.

Tak, jako neměli Němci v první světové válce jasnou představu o tom, jak změní budoucí válečnictví bojový plyn yperit a Američané ve světové válce druhé, jaké globální důsledky bude mít atomová puma Little Boy shozená na Hirošimu, nemají ani současní bezpečnostní experti jistotu v tom, co přesně by mohl úspěšný a dobře mířený kybernetický útok způsobit a odstartovat.

Přestože je možné ke kybernetickému prostoru vymyslet mnoho scénářů, zaměřuje se tento esej na konkrétní fenomén, který Vojenské zpravodajství ve své zprávě o činnosti za rok 2018 zařadilo mezi významné trendy kybernetické bezpečnosti – Internet věcí.

Mnoho definic a ještě více přístrojů

Internet věcí jsou autonomní chytrá zařízení, s nimiž přicházíme denně do styku; senzory, pohybová čidla, chytré měřící „krabičky“, chytrá sluchátka, webkamery, chytré hodinky, chytré hračky... Ostatně, někteří mezi tato zařízení řadí i chytrý mobil nebo tablet.

První v podstatě akademický problém u Internetu věcí, zkráceně IoT, nastává u hledání definice. Je jich mnoho a často se v základních rysech liší. Opakují se v nich však společné znaky, díky nimž můžeme IoT vytyčit. Těmi jsou přítomnost M2M[2] komunikace, připojení k sítí, schopnost sběru a výměny dat a z toho plynoucí schopnost samostatného rozhodování (vedoucí k vyvolání/nevyvolání další akce).

Obdobný problém nastává u určení toho, kolik funkčních připojených zařízení momentálně na světě je. Odhady se v závislosti na nevyjasněných definicích výrazně liší – v rozmezí 20 až 50 miliard.[3]

---

[1] Paganini, Perluigi. 2016. “NATO officially recognizes cyberspace a warfare domain.“ *Security Affairs*, June 18, 2016. https://securityaffairs.co/wordpress/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html#:~:text=The%20NATO%20has%20officially%20declared,of%20a%20powerful%20cyber%20attack..

[2] Machine-to-machine.

[3] Fazal, Khadija et al. 2017. “A Systematic Literature Review on the Security Challenges of Internet of Things and their Classification.“ *International Journal of Technology and Research*. https://www.semanticscholar.org/paper/A-Systematic-Literature-Review-on-the-Security-of-Fazal/4a379ef4722a6fb4c0d3018a24d4a24c6d184634.

Bezpečnost jako téma na vedlejší koleji

Z pohledu kybernetické bezpečnosti mají IoT zařízení dva základní technické nedostatky – malou paměť a nízký počítačový výkon.[4] Na ně se nabalují další, dělající z IoT ideální vstupní bránu do systémů, jež chce útočník napadnout. Bránu, která bývá mnohdy nedostatečně zabezpečená.

Výrobci těchto zařízení totiž obecně postrádají motivaci implementovat bezpečnostní opatření. Za prvé se jedná o finančně i časově náročný proces a za druhé není právně vynutitelné, aby bylo IoT zařízení adekvátně zabezpečeno.[5] To vede k přehlížení a zanedbávání bezpečnosti.[6]

Dalším specifikem IoT je, že vzhledem k různé povaze přístrojů nelze aplikovat jednotné bezpečnostní řešení.[7] Každý typ má svou specifickou potřebu a kapacitu. A to všechno vytváří bludný kruh, v němž se vracíme k tomu, že se výrobci bezpečnostními opatřeními raději nezabývají.

Atentáty a útoky zítřka

Nejen kvůli zmíněným důvodům si tak lze představit scénář, v němž bude Internet věcí představovat ono *něco*, co rozpoutá kybernetický útok s dalekosáhlými následky.

Zneužitý prvek IoT se dá využít k závažnějším útokům, než jsou ty typu DDoS,[8] jako tomu bylo v říjnu 2016 za pomoci Mirai malwaru, kdy armádu kompromitovaných zařízení tvořily Ipady, chytré měřiče, chytré hodinky nebo třeba webkamery.[9]

Autorky knihy *Cyberspace, Cybersecurity, and Cybercrime* zmiňují ideu budoucí podoby vraždy. Demonstrují ji na příkladu chytrého automobilu, kdy útočník nad vozem převezme kontrolu a nasměruje jej i s posádkou z mostu.[10] Přitom není těžké si představit další možnosti, kdy by IoT hrálo roli v převzetí kontroly nad jinými dopravními prostředky – třeba u letadel. Když teroristé naleznou bezpečnostní skulinu v IoT prvku, co je dělí od toho, aby letadlo unesli a zopakovali útoky z 11. září 2001, aniž by se sami nacházeli na palubě?

U dopravních prostředků to ale nekončí, jelikož IoT je možné potkat prakticky ve všech odvětvích; třeba ve zdravotnictví jako měřidla glukózy a chytrá inzulinová pera pro diabetiky.[11] Co když takové zdravotnické zařízení ovládne útočník a jeho majitele předávkuje, nebo deaktivuje upozornění na nedostatek glukózy, což povede k hypoglykemickému šoku? Zneužitelná zařízení IoT by se snadno mohla změnit v nástroje moderních atentátů na politické představitele nebo jiné významné osoby.

---

[4] Kim, Jung Tae. 2017. "Requirement of Secure IoT devices for Smart Home Network Based on Internet of Things." *Information*, 20(8B): 6171-6178.
[5] Kolouch, Jan. *Cybercrime.* Praha: CZ.NIC, 2016.
[6] Ministerstvo obrany. 2019. „Výroční zpráva o činnosti Vojenského zpravodajství za rok 2018." https://vzcr.cz/uploads/41-Vyrocni-zprava-2018.pdf.
[7] Rehman, Aqeel Ur et al. 2016. "Security and Privacy Issues in IoT." *International Journal of Communication Networks and Information Security*, *8(3):* 147-157. https://www.ijcnis.org/index.php/ijcnis/article/view/2074/193.
[8] Distributed Denial of Service.
[9] Kremling, Janine and Amanda M. Parker Sharp. *Cyberspace, Cybersecurity, and Cybercrime.* New York: SAGE Publications, 2017.
[10] Ibidem.
[11] Econsultancy. 2019. "10 examples of the Internet of Things in healthcare." *Econsultancy.com*, February 1, 2019. https://econsultancy.com/internet-of-things-healthcare/.

Dopad takových útoků – které je navíc zpravidla obtížné či přímo nemožné atribuovat – by mohl mít na poli státní i globální bezpečnosti nedozírné následky. Jelikož ve chvíli, kdy nepřítel zůstává v kybernetickém prostoru ukrytý, stávají se potenciálními nepřáteli všichni.

Naprosté ohrožení národní – i mezinárodní – bezpečnosti by mohl představovat útok na kritickou či kritickou informační infrastrukturu – ať už českou či evropskou – provedený skrze IoT prvky v systémech subjektů, jež ji tvoří. V takovém případě si lze představit důsledky, jakými jsou nefunkčnost zdravotnictví, kolaps energetického průmyslu nebo pád komunikačních kanálů státu ke svým občanům.

Možná podoba kyberterorismu?

V nadsazeném scénáři by se z IoT prvků mohl stát elegantní nástroj kyberterorismu. Ten označuje Kenney (2015) jako počítačem generované útoky, cílící na jiná počítačová zařízení v kybernetickém prostoru, s přesahem do fyzického světa. Tedy s konkrétním hmatatelným výsledkem, který překročí hranice kybernetického prostoru.

Rozdíl oproti konvenčním teroristickým útokům (z nichž mnohé využívají v nějaké fázi kybernetický prostor) podle tohoto autora je, že se celý incident odehrává ve virtuálním prostoru – a pouze výsledek je hmatatelný. Takovým výsledkem pak může být smrt osoby (či více osob) nebo fyzické zničení.

Samozřejmostí v debatě o jakémkoli druhu terorismu je snaha vyvolat činem psychologický efekt, nejčastěji strach.[12] A není představa, že něčí webkamera nebo chytré hodinky mohou nevědomky stát za kolapsem některého z životně důležitých systémů státu, dostatečně děsivá?

Závěr

Přestože nastíněné úspěšné útoky za použití IoT zatím *nejspíš* neproběhly, nelze se utěšovat představou, že situace nenastane. Své o tom ví Izrael, který v posledních měsících několikrát čelil kybernetickým útokům na vodní infrastrukturu.[13]

Internet věcí je ukázkovým příkladem, jak dokáže chytrá technologie zjednodušit (nejen každodenní) život. Pokud však není zabezpečená či je zabezpečená nedostatečně, může i malý přístroj nadělat velké problémy. V krajním případě vést k ohrožení lidských životů nebo národní bezpečnosti. A v případě nejzazším až ke globálnímu chaosu, který by dokázal překonat i to, čeho jsme jako civilizace byli svědky v souvislosti s první světovou vlnou nemoci COVID-19.

Přitom by velkou část současných i budoucích kybernetických útoků dokázala eliminovat důsledná bezpečnostní opatření. Ta opatření, na něž výrobci často na počátku zanevřou, protože z nich nemají profit a nikdo je do implementace nenutí.

---

[12] Kenney, Michael. 2015. "Cyber-Terrorism in a Post-Stuxnet World." *Orbis,* 59(1), 111-128. https://www.researchgate.net/publication/270914520_Cyber-Terrorism_in_a_Post-Stuxnet_World.

[13] Cimpanu, Catalin. 2020. "Two more cyber-attacks hit Israel's water system." *ZDNet.com*, July 20, 2020. https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/.