CYBER COVID ESEJ

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

Rozhodnutí tohoto problému vyžaduje mimo jiné detailnější analýzu aktuálního fungování online světa a chování lidí. Většina možností by však pro úspěšný útok vyžadovala víc než čistý kyberútok, a je tedy třeba vnímat i ostatní faktory, například fyzické zabezpečení objektů, na které by byl útok veden. Seriózní analýza tohoto problému samozřejmě vyžaduje odborníky i z jiných oblastí než IT bezpečnost, pokusme se však rozebrat několik myšlenek...

Díky snadnému a rychlému přístupu k informacím se můžeme domyslet, že podobnou situaci (lockdown na úrovni států, zákazy vycházení, nasazení armády) by musel vyvolat "neviditelný nepřítel", tedy podobně jako nyní – virus, superbakterie či radiace. Dále si můžeme představit několik možností, které životy přímo neohrožují, ale přesto mohou způsobit vážné problémy (dopady ekonomického rázu). Útok zaměřený na celý svět bude vždy řádově obtížnější, než pokus o "vyřazení" jednoho státu z provozu.

1 Kyberútok na laboratoř

Cílený útok s cílem "vypustit biologickou zbraň" by jednoduše neměl být možný – laboratoře uchovávající nebezpečný biologický materiál jsou (snad) dobře zabezpečené – kontrola prostředí není připojená k Internetu, je zavedeno digitální podepisování atp. Daný postup tedy **nevede k opatřením z doby COVID-19**.

Kybernetický útok stylu "pošleme satelitu na orbitě povel k sestupu do atmosféry a padající trosky zasáhnou vozidlo převážející vzorky biologických zbraní" je snad pouze úsměvný a statisticky nemožný.

Pokud by však došlo k využití více útočných vektorů ("hack" mailů, dálkové ovládání některých systémů, zápis příkazu práce pro zaměstnance a údržbu) spolu s neznalostí zaměstnanců IT bezpečnosti (sociálního inženýrství), mohlo by teoreticky dojít k postupu drobných chyb, které by opravdu mohly vést k úniku nebezpečné a nakažlivé látky – třeba pravých neštovic. Pravděpodobnost úspěchu tohoto útoku by samozřejmě museli posoudit odborníci na zabezpečení laboratoří a skladovacích prostor biologických látek. Avšak v **případě úspěchu by mohlo dojít ke stejným opatřením jako v době COVID-19**, jelikož by svět byl v podobné situaci jako s COVID-19, ne-li horší.

2 Falešná zpráva o katastrofě

Pokud by došlo k masovému šíření mylné informace, že nastala jaderná válka či jiná katastrofa velkého rozsahu, právě přístup k informacím by rychle vedl k vyvrácení této informace. Falešná informace o úniku viru či superbakterie by způsobila různé množství škod, dle rozsahu a sofistikovanosti útoku. Při pouhém rozšíření dezinformace o úniku viru v nějaké oblasti by největším rizikem byla panika obyvatel, následné přetížení nouzových linek a v horším případě rabování. Vše by ale pravděpodobně mělo pouze lokální a krátkodobý účinek.

Za předpokladu velmi sofistikovaného útoku, zahrnujícího i fyzické vypuštění méně škodlivého viru či bakterie, by situace byla již složitější. Představa, že by došlo k vypuštění dezinformace "ve městě X unikl virus, který způsobuje těžké průjmy a následně smrt" spolu s nakažením části potravin v daném městě třeba salmonelózou, není až tak nereálná. Zde by již musela být tvrdší opatření – karanténa, ozbrojené složky v ulicích a podobně. Jistě by došlo k panice vedoucí k rabování a případným ztrátám na životech.

Přes způsobené potíže by však **takové útoky nevedly k opatřením z doby COVID-19**, a to z důvodu rychlého lokálního prošetření a karantény.

3 Útok na kritickou infrastrukturu

Podobný útok, nehledě na sofistikovanost a velikost útočící skupiny, by pravděpodobně nevedl k rozsáhlým škodám ani omezením. Vzhledem k faktu, že stěžejní části kritické infrastruktury nejsou přístupné z Internetu, zůstává pravděpodobnější útok fyzický, případně sociální inženýrství. Obojí by však muselo být provedeno v tak masivním rozsahu, že by jistě došlo k brzkému prozrazení celé akce (zvlášť v případě plánování fyzického útoku by jistě došlo k zachycení informací tajnými službami).

Kontrola provozu a bezpečnostní protokoly tedy snad způsobí, **že nedojde k opatřením z doby COVID-19**.

4 Útok na "ekonomickou infrastrukturu"

Narušení, nebo ještě lépe likvidaci infrastruktury obsahující data o stavu bankovních účtů, sociálního pojištění (a dalších kritických dat) spolu se zveřejněním tajných vládních dokumentů zatím považuji za nejnadějnější formu útoku (vyjma zmíněného vypuštění biologické zbraně). Po masivním útoku, při kterém by došlo ke zničení tohoto typu dat, by muselo dojít k zastavení podniků, pozastavení výplat a zmrazení akcií (včetně množství dalších věcí), a to do doby, než by došlo k obnovení dat ze záloh. To by jistě nenastalo přes noc a situace by vedla k masivnímu rabování, poklesu ekonomiky, omezení zdravotní péče. Stačí si vzpomenout, jaké škody napáchala v USA roku 2013 krize spojená se státním dluhem[1].

Tento útok by musel být velmi rozsáhlý a muselo by být zapojeno velké množství lidí. Pokud by byl vůbec proveditelný, pravděpodobně by stejně selhal díky nedostatečnému utajení, odchycení tajnou službou či jinou bezpečnostní agenturou nebo by hackerské skupině jednoduše došly finanční prostředky. Proti útočníkům také stojí fakt, že bankovní a státní systémy jsou velmi staré, psané v praktický mrtvých jazycích jako COBOL nebo Fortran a také jsou částečně offline. Pokud by přesto došlo k souhře mnoha náhod a útok by byl proveden, **došlo by v dlouhodobém hledisku k podobným dopadům COVID-19 krize** – a to k dopadům ekonomickým.

O kompletním zničení těchto kritických dat snad nemusíme ani uvažovat díky masivní redundanci, geograficky oddělenému zálohování a přísnému utajení. Zde můžeme pouze doufat, že tato data opravdu není možné zničit jinak, než fyzickým zničením minimálně části kontinentu. Pokud by to možné bylo, došlo by prakticky ihned ke zhroucení celé společnosti a krizi, která nelze přirovnat k zatím ničemu v historii Země – lidé by sice měli k dispozici veškeré technologie, ale nikdo by nemohl dokázat, co komu patří.

Budoucnost, decentralizace a větší důraz na bezpečnost

V analýze výše jsem se pokusil představit několik cílů a metod útoků, a to od nemožných po velmi lehce pravděpodobné. Aktuálně vidím největší hrozby pro kritické systémy v jejich špatném zabezpečení a přílišné centralizaci. Přesto však zastávám názor, že je nepravděpodobné, aby čistý kyberútok vyvolal dopady podobné těm při COVID-19 krizi.

V blízké budoucnosti nás čeká přesun většiny "papírování" do virtuálního světa a snad také modernizace zastaralých systémů. Naším úkolem bude je dobře zabezpečit a zavést decentralizaci kritických systémů takovou, aby úspěšný útok na jednu část způsobil pouze malé nebo žádné škody.

[1] https://en.wikipedia.org/wiki/United_States_debt-ceiling_crisis_of_2013