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

Při koronavirové krizi jsme začali ve velkém používat on-line komunikaci. Začali jsme pracovat z domova, chodili na on-line vyučování a i s přáteli jsme komunikovali virtuálně. Během několika měsíců jsme si zkusili, jak vypadá práce nebo škola z domova. Technologie nám umožňují se navzájem propojit a vědět o všech událostech rychleji než dříve. Řekli bychom proto, že nemají žádnou chybu, ale mají, tou je hrozba kybernetického útoku.

Koronavirová krize měla hlavně ekonomické dopady, krachování živnostníků a velký schodek státního rozpočtu. Způsobila také mnoho úmrtí osob v celém světě a i v České republice.

Kybernetický útok by však kromě ekonomických dopadů mohl paradoxně přinést více obětí na životech, než pandemie COVID-19. Vzpomeňme na útok hackerů na nemocnici v Benešově. Nemocnice se musela z části zavřít a pacienti tak museli jít do jiné nemocnice. Takový útok na jednu nemocnici není až tak velký problém, jako třeba útok na nemocnice v celém kraji. Hlavní problém by měli senioři nebo vážně nemocní, kteří by se museli složitě dopravovat do jiných nemocnic. A největší problém ve zdravotnictví by nastal v momentě, kdy by útok postihl většinu nemocnic v České republice. Při útoku na nemocnice by pravděpodobně byly odcizeny citlivé údaje o zdraví pacientů. Jedním z důvodů vyřazení nemocnic z provozu by bylo napadení přístrojů, které zajišťují pacientům mimotělní oběh, nebo jiných zařízení na podobném principu. Dalším problémem by bylo přetížení nemocnic, které útok nepostihl. Pokud by bylo napadeno jenom několik nemocnic v republice, dal by se tento problém ještě zvládnout. Komplikace by ale nastaly při napadení velkého množství nemocnic v určité oblasti, například v

Praze. V našem hlavním městě žije velká část obyvatel České republiky, pacienti by museli být přesunuti do nemocnic například ve Středočeském kraji, ale každá nemocnice v naší zemi není vybavena přístroji, jako jsou v Motole, Na Bulovce, nebo v Ikemu. V hodně nemocnicích neprovádějí všechny zákroky nebo vyšetření, a to by mohl být další významný problém. Otázkou jsou i zaměstnanci, někteří, hlavně doktoři, by museli dojíždět do jiných nemocnic, aby nemocnice zvládly nápor pacientů z těch, které byly vyřazeny z provozu. A k tomu se vztahuje další problém – kapacita nemocnic. V každé nemocnici máme pouze určitý počet volných míst na lůžkových odděleních a hlavně omezený počet na specializovaných odděleních, jako je jednotka intenzivní péče (JIP). Armáda České republiky sice může poskytnout polní nemocnici, ale těch je také omezený počet a asi by nedoplnily požadovanou kapacitu. Došlo by tak k situaci, že by se řada akutních zákroků musela odkládat, vážně nemocným pacientům by nebyla poskytnuta už žádná zdravotní péče. V konečném důsledku by to vedlo k nárůstu úmrtí, který by mohl být vyšší, než je tomu dnes v souvislosti s onemocněním COVID-19.

Pokud by byl útok směřován na fyzické osoby, byli by ohroženou skupinou, stejně jako při koronaviru senioři. Další rizikovou skupinou by byli také menší děti. Děti, které vyrůstaly před 20 nebo 15 lety neměly možnost přijít do styku s počítačem v takové míře jako dnešní děti, kterým je 5 nebo 6 let. V některých případech už 6 leté děti už mají svůj telefon. Pokud si dítě hraje na společném počítači, který používá celá rodina, může se lehce stát, že dítě do počítače „natáhne“ nějaký virus. Malé děti rády experimentují a ani si nemusí uvědomit, že svým neopatrným jednáním vlastně napomohou hackerům.

Další problém mohou mít senioři. Pokud někdo vyrůstal před 60 nebo 70 lety, tak si ani neuměl představit, že něco takového, jako osobní počítač a online komunikace bude existovat, jako běžná věc v každé domácnosti. Jako malí byli zvyklí, že pokud si chtěli něco koupit, museli si vystát frontu. A dnes si mohou vše koupit přes internet. Jejich nižší zdatnost a schopnosti mohou být zneužity a tak se stávají mnohdy snadným terčem útočníků na síti.

Asi největší problém by nastal ve chvíli, kdy by byly odpojeny dodávky elektřiny. Pokud by byl nedostatek elektřiny, mohlo by se to projevit třeba v zásobování potravinami nebo vodou. Také v obchodech by nefungovala elektřina, proto by nešlo kupovat chlazené a ni mražené zboží. Lidé, kteří pracují v tomto sektoru, by přišli o práci. Když by o práci přišlo hodně lidí, a byla by tu velká nezaměstnanost, tak by se také mohla zvýšit kriminalita. Také by mohlo nastat rabování obchodů. Při výpadku elektřiny by lidé nemohli používat metro ani tramvaje nebo trolejbusy. Museli by se proto posílit autobusové linky. Dnes se podporují elektromobily, aby bylo čisté životní prostředí. Pokud by se ale používaly z velké části elektromobily, tak by při výpadku elektřiny lidé neměli kde elektromobil dobýt. Ale i automobily na benzinový pohon by měly problémy, protože by nefungovaly semafory, a tak, by vznikl chaos na silnicích. Také by se nemohlo platit kartou, takže bychom museli platit pouze hotově. Ale nefungovaly by ani bankomaty, tak bychom si neměli kde hotovost vybrat.

Další problém by byla zvýšená kriminalita. Pokud by nešla elektřina, nešlo by ani pouliční osvětlení, mohlo by tak dojít k nárůstu pouličních přepadení. Lidé by také nemuseli mít dost peněz, tak by narůstaly krádeže.

V této souvislosti by nepochybně mohla přijít finanční krize. Pokud by lidé přišli o práci, neměli by peníze na nákupy. S tímto důvodem by také mohla v některých

oblastech narůstat chudoba. Mohly by vznikat chudinské čtvrtě na okrajích měst – slumy, kde by právě mohla být vysoká kriminalita.

Stát by také ale nemohl vyvážet zboží z České republiky, protože z důvodu výpadku elektřiny, by se nevyrábělo, tím by měl ze zahraničního obchodu nulové příjmy. Pokud by lidé neměli práci, neměli by z čeho platit daně, a tak by stát přišel o potřebné peníze, z kterých pořizuje různé věci a služby pro Českou republiku. Když by ale kybernetický útok zasáhl celou Evropu, nemohl by se ani spolehnou na Evropskou unii a její případnou finanční pomoc. Úplně by se tím zastavila ekonomika a celý systém světového trhu. Trvalo by také ale mnohem déle šíření informací. Pokud by nebyla elektřina, nemohli bychom používat počítače mobily a jiné komunikační technologie.

Při sečtení všech těchto problémů, zjišťujeme, že kybernetický útok je mnohem nebezpečnější, než si hodně lidí myslí. A tyto krizové situace, které jsou tu vypsané, nejsou rozhodně všechny, neboť o některých „černých“ scénářích nemáme ani tušení.