Kybernetické hrozby

Zbraně hromadného ničení, tak se poslední dobou hovoří o velmi závažném problému 21. století a to přesněji o kybernetických hrozbách. Tyto hrozby byly před nedávnem velkou neznámou, o které většinová společnost bohužel nevěděla. Naštěstí se poslední dobou čím dál více medializuje tento rozsáhlý problém, který by mohl do budoucna představovat ohromnou hrozbu pro lidstvo. Kupříkladu kybernetické útoky na nemocnice během koronavirové krize otřásly českou společností, dokonce je odsoudil i americký ministr zahraničí Mike Pompeo. Tyto hrozby se neustále vyvíjejí a zdokonalují, což by mohlo způsobit dalekosáhlé škody. Nádherný příklad je vznik ransomware. Tím, že na vzestupu je digitální doba i digitální měny, jsme najednou schopni převádět peněžní transakce v podstatě anonymně. Z pohledu útočníka je to lákavý cíl. Proč já bych si měl dokazovat, že jsem schopen ochromit počítače, když můžu od organizací požadovat anonymně peníze? Teď bych se však rád přesunul k něčemu vážnějšímu. Položil bych si takovou řečnickou otázku „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“?

Na začátek bych chtěl říci, že toto je velice složitý problém, na který je těžké odpovědět. V současné době, takto rozsáhlý útok doufejme, nehrozí, což ale neznamená, že by nebyl za určitých okolností proveditelný. V prvé řadě je asi dobré si říci, kdo je vlastně ten útočník? Protože za útokem nemusí stát pouze jednotlivec, organizace nebo státní útvar, ale útočníkem se může stát bezpochyby i umělá inteligence, která se rok co rok zdokonaluje a vylepšuje. Už dnes je umělá inteligence využívána ve většině odvětví například ve finanční sféře, zdravotnictví, akademickém světě nebo právních systémech. Počítače se učí na základě rozpoznávání vzorců uvnitř daných souborů dat. Problémy nastanou v momentě, kdy data nesou informace obsahující zaujaté společenské názory a předsudky, což by mohlo mít neblahý dopad na společnost. Teď bych se však rád přesunul k samotnému útoku, jak by hypoteticky útok mohl vypadat. Akce takto velkého měřítka by musela být precizně naplánována dopředu, musela by ochromit více

ekonomických sektorů najednou a také by musela zasáhnout do společenského života občanů. Z pohledu útočníků by si takový útok žádal velké kapacity, protože by se muselo „bojovat“ na více frontách. Jednotlivec by neměl s největší pravděpodobností šanci napáchat tak zdrcující škody. Hlavní výhodou útočníků jak sám tvrdí i armádní plukovník Miroslav Feix je moment překvapení.

Naštěstí v dnešní době nejsou útočníci o moc úrovní napřed, jak by se mohlo na první pohled zdát. Teď je nejvyšší čas posunout se k samotnému útoku. Pokud bych byl na pozici útočníka, tak bych se v prvé řadě zejména zaměřoval na distribuci elektrické energie a na energetické sítě jako celek. Jestliže by se povedlo přerušit dodávky energie nebo zastavit produkci elektrické energie na delší dobu v řádů týdnů či měsíců, znamenalo by to zastavení státu, který by nebyl schopen efektivně fungovat. Lidé by neměli přísun k informacím, tudíž by lidé nevěděli, co se děje. Začal by chaos a z největší pravděpodobností by to celé vyústilo v anarchii. Veškeré fungování veřejné infrastruktury by se zastavilo. Nefungovaly nemocnice, školy, průmysl, rekreační objekty, služby, mezinárodní obchod a tak dále. Dalo by se říci, že žádný ekonomický sektor by nebyl schopen normálního fungování. Lidé by neměli pocit bezpečí, jednu ze základních lidských potřeb, protože by vzrostla kriminalita a s tím spojené problémy. Vezměme si příklad z 13. července roku 1977 z New Yorku, kdy celou metropoli postihl blackout. Ve městě vzplálo na tisíc požárů a z chudých čtvrtí začalo mohutné rabování, lidé rozbíjeli výkladní skříně obchodů a brali úplně všechno na co přišli. Policie do akce povolala všechny dostupné posily a dohromady pozatýkala více než tři a půl tisíce lidí. Škody byly vyčísleny v řádů sta milionů dolarů, přičemž blackout, který uvalil New York do tmy, trval pouhých 25 hodin. Když si uvědomíme, že se tento incident stal před 43 lety, tak až mrazí, co by to mohlo napáchat v dnešní době, jestliže je naprostá většina zařízení závislá na elektřině. Ani bychom si nemohli zajít do obchodu pro potraviny nebo pro hygienické potřeby, protože by nefungovala pokladna, která je závislá na elektřině. Kazily by se potraviny v chladničkách, které by nebylo čím napájet. Kdyby se útočníci zaměřovali na strategická odvětví například na nemocnice, úřady, ministerstva, průmysl nebo dopravu, tak by to také napáchalo nemalé škody, možná i ztráty na životech. Pokud by taková nemocnice nebyla provozuschopná, kdyby se nedokázala postarat o své pacienty a v akutních případech operovat, tak by lidé dozajista umírali v důsledku

kybernetického útoku. Dalším velice důležitým sektorem jsou média, jak sociální sítě nebo internetové televize, tak standardní televevizní či rozhlasové. Kdyby se útoky zaměřovaly na rozšiřování fake news, vytváření deepfake a následné rozšiřování, narušování médií, nebo vydávání se za cizí osoby ve smyslu rozšiřování rasismu, nenávisti nebo lynčování menšin. Je smutné, že naprostá většina útočníků je nedohledatelných a nevymahatelných.I kdyby byli dopadeni, tak z velkou pravděpodobností by nebyli odsouzeni, protože by neexistovalo dostatečné množství důkazů na jejich usvědčení. Proto si myslím, že zabezpečení klíčových subjektů státu pro normální chod je důležitá a nezbytná věc, která funguje v České republice velmi dobře.

Na závěr bych rád podotknul, že si nikdo nepřeje kybernetický útok, který by napáchal podobné škody jako epidemiologická krize typu COVID-19. Bohužel určité riziko zde opravdu existuje a je naší povinností ho co nejvíce minimalizovat, aby tyto útoky byly pouze extrémně raritní záležitostí.Také bychom se měli zaměřit na edukaci, zejména na žáky základních škol a studenty středních nebo vysokých škol. Čímž bychom zamezili únikům dat nebo vydírání, což je v současnosti velmi častý problém, který může vyústit až k sebevraždě.