CYBER COVID ESEJ

Kybernetika je věda, zabývající se obecnými principy řízení a přenosu informací ve strojích, živých organismech a společenstvích. Kybernetický útok je úmyslné jednání v kyberprostoru, které má jakýmkoliv způsobem poškodit zájmy osoby, na kterou se útočník zaměří, nutno podotknout, že útok nemusí být zaměřen na jednotlivce, útočník si může vybrat firmu nebo počítače ve zdravotnictví. Tématem mé eseje je, jak by vypadal kybernetický útok, který by měl stejné dopady, jako pandemie nemoci Covid – 19. V této souvislosti bych si chtěla přiblížit dopady pandemie a zároveň si položit několik otázek ohledně kybernetických útoků. Jaké následky by musel mít takový útok, aby byl srovnatelný s následky pandemie Covid – 19? Jak by takový útok mohl vzniknout a na co by se zaměřil? V čem jsme, jako společnost zranitelná ohledně našich dat v systému počítače či na internetu? Měli bychom se bát a jak se bránit?

Co je nemoc Covid – 19? Je to infekční onemocnění, který má příznaky podobné chřipce, ale je vážnější. Co v tom našem malém světě způsobila pandemie? Řekla bych to velice stručně. V každé části světa je to jinak. Zasáhl naši ekonomiku, zkomplikoval situaci ve zdravotnictví, zavřel nás do karantény… Opatření probíhají různě a následky se také mění, někdo je na tom lépe, někdo hůře. Virus, který ze začátku vypadal nevinně, když napadl Čínu, se pak ale rozšířil skoro všude. Takhle pro mě může vypadat kybernetický útok, ze začátku vypadá nevinně, jako nenápadná příloha v emailu, ze které se stane velký problém. Na pandemii nikdo nebyl připraven, a i když říkáme, že jsme chráněni před kybernetickou hrozbou, tak na ni podle mě nejsme zcela připraveni.

Jak by takový útok mohl vzniknout a no co by se zaměřil? Na první část otázky není za mě úplně jasná odpověď. Kdybychom znali způsob vzniku, tak bychom se asi ani nebavili o rizikách, protože by se nikdo nebál. Zeptala bych se proč? Lidé pravděpodobně díky těmto útokům vydělají peníze, někomu takový zdařilý kyberútok vyvolá pocit radosti. Aby byl útok tak ničivý pro naší populaci, musel by se zaměřit na něco důležitého. Nebezpečné je, pokud se někdo naboural do systému nemocnice, lékaři mají v počítači data o lécích a informace o pacientech, jakmile data nejsou dostupná, může to ohrozit i lidský život. Aby útok byl na světové úrovni musel by napadnout nějaká opravdu citlivá data, která jsou před někým skrývána. Například armádní data. Pokud někdo ukradne citlivá data organizace NATO, může to vyvolat válečné konflikty, zvláště pokud jsou data proti někomu zaujatá. Následně by také mohly uniknout informace o zbroji a taktice, ty by mohly pomoci porazit zemi ve válce. Útok je také možné zaměřit na jednotlivce. Pokud útočník například někomu ukradne jeho cenná data, nebo ho okrade o peníze na jeho bankovním účtu, nemá to světový vliv. Jakmile útočník zaútočí na počítač jednotlivce, který je součástí firemní domény, může to být větší oříšek.

Kyberútok by mohl postihnout naši ekonomiku, můžou býti odcizena národní tajemství. Nebo zmizí údaje ve zdravotnictví. Naše osobní údaje a data, například naše adresa, fotky, data narození, rodina. Kdokoliv může napadnout naše bankovní konta a obrat nás doslova o miliony. Lidé se začnou bát nebo zlobit. Co kdyby po nehezké skutečnosti začaly opouštět sociální sítě a internet? Zkomplikuje se komunikace a internetové a počítačové firmy začnou

prodělávat. Lidé se můžou bát i reálného světa, takzvaný hacker – počítačový specialista může být kdekoliv kolem nich.

Co si myslím, že je naše zranitelnost? Veliká část populace vlastní chytré elektronické zařízení. Už malé děti si hrají s tabletem, samy se zvládnou obsloužit a na platformě YouTube si s lehkostí pustí různé oblíbené seriály z televize. Když dítě necháme bez dozoru, může se omylem dopustit chyby. Změní nastavení, nebo omylem přenastaví heslo na sociálních sítích. Stačí mu rozkliknout pochybnou stránku na internetu nebo stáhnout do zařízení hru společně s virem. Virus se v oblasti počítačové bezpečnosti označuje jako program, který se umí šířit bez vlivu uživatele. Nejen že virus napadá vaše soubory na disku, může také zpomalit výkon vašeho zařízení. Děti nízkého věku by podle mě neměli mít přístup k internetu, ale to je v dnešní době už nereálné, alespoň rodič by měl dohlédnout na jejich činnost na sociálních médiích.

Jak se můžeme bránit? Je potřeba dát si prostě pozor. Do počítače bychom si měli nainstalovat dobrý antivirus. Pozor je třeba dát si na internetu, neklikat na pochybné webové stránky, neotevírat neznámé emaily a nestahovat přílohy od cizích lidí. Důležité je vymyslet si bezpečné heslo, to by mělo obsahovat kombinaci velkých a malých písmen a číslic. Nejpoužívanějším heslem na světě je 123456, toto heslo může hacker prolomit za pár sekund. Pozor bychom si měli dávat, když se připojujeme k veřejné WiFi. Pokud se na ní nachází hacker může se pomocí ní dostat k nám. Doporučené je používat VPN. VPN je takzvaná virtuální privátní síť, která umožňuje uživateli prohlížet internet v soukromí, VPN zašifruje naše data a skryje nás za falešnou IP adresu. Používaný trik, jak dostat z lidí jejich heslo od úču je zaslání falešné adresy na přihlašovací webovou stránku, graficky totiž webovka vypadá, jako stránka vaší banky, ale není to ona, hacker z vás takto vytáhne úplně snadno přihlašovací údaje. Jedna ze zranitelností je určitě to, že lidé nejsou správně informováni o bezpečnosti na internetu. Myslím, že by měly informovat děti už základní školy v rámci přednášek.

Moje shrnutí. Myslím, že jako společnost nejsme plně chráněni. Už malé děti jsou na sociálních sítích a nejsou informovány o bezpečnosti na internetu. Technologie se neustále ženou kupředu, vymýšlíme lepší a lepší systémy. Proto se rozrůstají i kybernetické útoky. Většina aktualizací pořád zdokonaluje svoji „obranu proti hackerům“. Stejně, jako se zdokonalují hackeři, tak se zdokonalují antiviry. Nemůžu tedy říct, že bychom se útoku bát měli. Důležité je podotknout, že bát se něčeho, je zdravé, právě náš strach pomáhá vylepšovat naše systémy, hledat v nich chyby a dělat nás více chráněnými. Strach je naše prevence, když nastala pandemie činili jsme opatření, kdyby nastala taková kyber-pandemie budeme se chovat stejně. Nejvíce nás ochrání problémům předcházet, když se to nepovede poučit se a postupně elimininovat zranitelnosti dnešní společnosti.