CYBER COVID ESEJ

Tématem eseje je možnost kybernetického útoku srovnatelného se současnou pandemií COVID-19. V této době na počítače a jiné elektronické přístroje dost spoléháme a v budoucnosti na nich budeme pravděpodobně závislí ještě více. Covid 19 způsobil již 512 000 úmrtí a 10 512 383 nakažených osob (ke dni 1. 7. 2020). Lidé na něj nebyli připraveni, proto se tak rychle rozšířil po celém světě. Kdyby svět zažil stejný útok, ale z kybernetického světa, byl by stejně hrozný nebo dokonce horší? A jak by vlastně mohl vzniknout?

Může vzniknout ze spousty důvodů. Například ho může vyrobit nějaký programátor a potom ho omylem vypustí do internetu, kde už ho nebude mít pod kontrolou. Nebo ho může vyrobit nějaká země, která tím chce vyhlásit válku nějaké jiné zemi, rozšíří se následně po celém světě a vnikne z toho 1. světová kybernetická válka. Nebo se nějakému hackerovi vymkne z kontroly něco, co se nemělo vůbec dostat ven mimo jeho počítač.

Kybernetické útoky se dějí neustále, každý den, už mnoho let. Mohou mít různou podobu:

Virus je škodlivý program, který je nechtěnou součástí programu nebo dokumentu a negativně ovlivňuje výkon zařízení. Je nejběžnějším typem kybernetického útoku a stejně jako skutečný vir, i tento kybernetický by mohl poškodit celý svět.

Phishing jsou podvodné stránky vytvořené nejčastěji za účelem získaní citlivých informací od uživatelů (uživatelská jména, hesla nebo třeba přihlašovací údaje do internetového bankovnictví). Jde o velmi častou formu kybernetického útoku.

Malware je škodlivý kód, který se může šířit různými způsoby, například prostřednictvím přílohy v e-mailu, nakaženými webovými stránkami, chybou v programu apod.

Trojan (Trojský kůň) je škodlivý program, který se tváří jako užitečný/legitimní (např. hry nebo nejrůznější editační nástroje). Na rozdíl od virů a počítačových červů

se trojany samy nereplikují - nemohou tedy infikovat další počítače svou kopií. Trojany se odlišují typem akcí, které vykonávají. Mohou sledovat akce uživatele počítače, rozesílat z napadeného počítače spam nebo odposlouchávat uživatelská jména a hesla.

Probe znamená, že útočník skenuje celý IP rozsah přidělený určité instituci a hledá na jejích serverech nějakou přístupnou službu, kterou by se do sítě dostal a využil ji.

Botnet je síť nakažených strojů, tzv. botů. V současné době je termín nejvíce spojován s malwarem, kdy botnet označuje síť počítačů infikovaných speciálním softwarem, který je řízen z jednoho centra. Botnet pak provádí nežádoucí činnost, jako je rozesílání spamu, útoky DDoS a podobně.

Všechny uvedené možnosti by mohly být cestou, kterou by se cyber virus šířil a škodil po celém světě.

Virus Covid 19 se šíří vzduchem, kapénkami a kýcháním, uvažuje se, že na vzdálenost dvou metrů. To znamená, že se dva lidé musí fyzicky potkat, být spolu v jednom místě v určitý čas, určitou dobu. Přitom nejkratší let kolem země dopravním letadlem trval 31,5 hodin. Tedy k nejrychlejšímu přesunu viru po světě by byl potřeba více než jeden den, v reálu šlo o několik měsíců.

Kybernetový útok má rychlejší možnosti a cesty šíření. Mohl by se šířit nejen přes internet a pevnou síť, ale i přes Wi-Fi, ta je dostupná v kavárnách restauracích a dalších veřejných prostorech. Dále by se šířil třeba přes bluetooth, takže by se rozšířil do všech spotřebičů v domě a dokonce i do aut. Šíří se i na delší vzdálenost, než jen na 2 metry, takže se lidé nemusí ani fyzicky setkat. Pokus dokázal, že e-mail dokáže obletět svět za 17 sekund. To znamená, že by se mohl šířit mnohem rychleji, než covid 19.

Tedy proti šíření skutečného COVID 19 během měsíců, by kybernetickému viru stačila ani ne jedna minuta pro cestu kolem světa. Takže by se během chvilky mohl rozšířit do většiny elektronických přístrojů na světě. Ale jaké by to mělo následky pro nás lidi? Třeba i rovnou smrtelné - máme autonomní vozidla, která kdyby byla nakažená, mohla by se vybourat a způsobit smrt všem ve voze. Nebo by lednice mohla přestat mrazit,

takže by se nám mohlo zkazit všechno jídlo. Světla by zhasla, dveře by se zamkly, veškeré chytré zařízení by mohli přestat fungovat, topení by netopilo i když by venku mrzlo. Kdyby se virus dostal do nemocnic, mohl by zabít spousty lidí tím, že je odpojí z přístrojů, které je udržují při životě, nebo smaže zdravotní údaje o léčbě. Když by se dostal do bank, mohl by okrást spoustu lidí, ale i celá města a státy. Mohl by na internetu vyvolávat dezinformace. V našich počítačích a mobilech by mohl virus získat nebo změnit informace, nebo hesla k důležitým věcem.

Kybernetické útoky v počítačovém světě jsou časté, lidé i státy se jim snaží zabránit. V počítačích i mobilech máme antivirové programy. Existuje např. firewall neboli ochranná zeď, kterou máme v počítači a má nás před útoky zvenku chránit. Dále existují tzv. hlídači např. CSIRT (Computer Security Incident Response Team) neboli Skupina pro reakci na počítačové bezpečnostní události, ty máme i v České republice (CSIRT.CZ). Mají za úkol řešit bezpečnostní události (incidenty) v počítačových sítích provozovaných na celém území Česka. Sami bychom se před virem mohli chránit tím, že se budeme chovat zodpovědně.

Pokud už by kybernetický vir ovládl svět, zbavovali bychom se ho velmi špatně, zastavit útok by trvalo hodně dlouho. Covid 19 začal na konci roku 2019 a ještě v červenci ho nemáme polapeného. Zároveň hodně lidí tvrdí, že bude ještě druhá vlna. Stejně jako proti Covidu 19 se musí vyvinout vakcína, u počítačového viru by se musel vymyslet účinný počítačový antivirus. A do té doby by se s tím asi nedalo nic dělat a následky by mohly být hrozivé.

Pravděpodobnost útoku je docela veliká a je možné, že není ani v tak vzdálené budoucnosti. Hackerských útoků stále přibývá, a je dost možné, že někdo udělá třeba i malou chybu, nebo přijde útok úmyslný.

Kdyby na nás počítačový cyber virus doopravdy zaútočil, měli bychom tři možnosti: první možnost je bránit se různými ochrannými programy. Druhá možnost je útok, takže vyhledávat škodlivé viry a programy předem a ničit je. Třetí možnost je útěk, utekli bychom od elektroniky, takže bychom byli úplně off-line, mimo počítačovou i

mobilní síť, to by však asi hodně lidí nechtělo. A potom existuje ještě jedna možnost, čtvrtá, a to nedělat nic. Jen čekat a nechat se porazit, ale to by asi bylo to nejhorší, co bychom mohli udělat.

Zdroje

https://www.czechairliners.net

https://www.chip.cz/casopis-chip/earchiv/rubriky/komunikace-archiv/cesta-kolem-sveta-za-17-sekund/

https://www.ceskovdatech.cz/clanek/89-kyberneticka-ne-bezpecnost/

https://cs.wikipedia.org/wiki/CSIRT.CZ