CYBER COVID ESEJ:

Společnost si přes svou závislost na moderních technologiích nepřipouštíme závažnost příští nevyhnutelné hrozby

Každý měsíc slyšíme zprávy o vládách, mezinárodních institucích nebo velkých konglomerátech, které se staly obětí kybernetického útoku nebo kybernetické špionáže. Vůči této skutečnosti jsme se stali necitliví, a je to riziko, kterého se obáváme, ale které přijímáme, protože jsme jako společnost na internetu a dalších moderních technologiích vysoce závislí. Nejenom lidé, ale také životně důležitá (někdy i život zachraňující) infrastruktura se tolik spoléhá na nové technologie, že se stává snadnou kořistí útoků které nejen narušují jejich činnost, ale mohou také ohrozit lidské životy.

S vědomím toho, že kybernetický útok vekého rozsahu je velmi pravděpodobně nevyhnutelný, je legitimní ptát se jak by mohl takový útok vypadat a jaké by mohly být jeho následky. Mnohé napadá srovnání s pandemií onemocnění covid-19, která zasáhla celý svět a s kterou se dosud potýkáme a jejichž následky budeme pociťovat ještě v následujících letech. K tomuto srovnání nakonec směřuje i tato esej.

Covid-19 odhalil nedostatky v krizovém managementu

Na celé situaci s pandemií covid-19 je znepokojující zejména nepřipravenost s jakou se vlády se situací vypořádávaly a vypořádávají. Až na některé výjimky jsme byli svědky improvizovaných opatření, která byla doprovázena kritickým nedostatkem zdravotnického materiálu, ale bohužel také již tradičního, o to více alarmujícího nezvládání krizové komunikace. Nejenže se veřejnost dozvídala informace kusovitě a různými kanály, ale docházelo k případům, kdy si informace od oficiálních představitelů protiřečily, či se měnily náhle bez dostatečného předstihu, nebo informace chyběly úplně.

I přes příznivější výchozí pozici, kdy se o rychle se šířícím virovém onemocnění vědělo nejpozději od listopadu 2019, první případy onemocnění covid-19 se v Evropě objevily na konci ledna 2020 a první potvrzený případ v ČR 1. března 2020, se Česká republika nedokázala vyhnout zmatku a celkově selhávajícímu krizovému managementu.

S virálně se šířícími malwary již máme zkušenost

Pokud bychom hledali paralelu k současné pandemii onemocnění covid-19 mezi kybernetickými útoky, mohli bychom ji částečně nalézt v malwaru NotPetya. NotPetya je škodlivý kód, který v červnu 2017 využila skupina hackerů ruské zpravodajské služby GRU, známá také jako Sandworm, pro svůj kybernetický útok proti Ukrajině. Útok byl součástí kybernetických aktivit, které mezi oběma státy probíhají v rámci neukončeného rusko-ukrajinského konfliktu.

Přestože byl útok primárně cílený proti Ukrajině, během hodin se malware rozšířil za hranice země a šířil se ze sítě do sítě, z počítače do počítače. Zasahoval zejména firmy, jež měly s Ukrajinou byznysové vazby. Každé zařízení a server do kterého pronikl, nenávratně zašifroval. Celková škoda se odhaduje na 10 miliard amerických dolarů.

Kromě rozsáhlých finančních ztrát malware NotPetya významně poškodil ukrajinský zdravotnický systém a přímo ovlivnil a dokonce i ohrozil zdraví a život tisíců lidí. V důsledku útoku byly zařízení v ukrajinských nemocnicích pracující na operačním systému Windows vyřazeny z provozu. Všechna vyšetření musela být zrušena, stejně jako lékařské zákroky. Nefungoval dokonce ani systém pro lokalizaci záchranných vozů. Výsledkem byla frustrace a chaos.

Obzvláště znepokojující a poučné ovšem je, že ukrajinské nemocnice nebyly jedinými zdravotnickými zařízeními postiženými tímto kybernetickým útokem. Virus pronikl i do několika nemocnic v USA. Stalo se tak pravděpodobně přes server jedné ze soukromých firem, která poskytovala služby postiženým ukrajinským a americkým nemocnicím.

Budoucí útok velkého rozsahu by mohl využít zranitelností v zařízení IoT

Podobné důsledky jako onemocnění covid-19 by mohl způsobit kybernetický útok cílený na tzv. internet věcí (z anglického termínu *Internet of Things,* IoT). K němu obvykle dochází tak, že se v sérii zařízení IoT nachází zero-day zranitelnost, o které nikdo z uživatelů ani správců neví, pachateli se jí ale podaří nalézt. Útočník následně použije škodlivý kód, který tuto zranitelnost, chybu v zabezpečení, zneužije a například změní zařízení IoT na botnety a provede hromadný útok. Nemůžeme zcela vyloučit možnost, že správně vedený DDoS útok by mohl ochromit národní hospodářství, komunikace, služby a další prvky kritické infrastruktury.

Takto vedený útok na sérii zařízení IoT je samozřejmě zbraň schopná jediného výstřelu v tom smyslu, že po zjištění zranitelnosti v zařízení může být zranitelnost opravena a zařízení již nebude možné znovu zneužít (jednoduše proto, že chyba v zabezpečení, již nebude existovat).

Tento scénář se však dívá do budoucnosti a počet zařízení IoT, která budeme využívat v našem každodenním životě se zavedením sítí páté generace dramaticky zvýší. V určitém okamžiku bude existovat mnoho zařízení, které budou stále připojeny k síti, a které již nebudou výrobci z důvodu zastarání podporovány. K dispozici nebudou potřebné aktualizace a „záplaty“, které by případné zranitelnosti odstranily. To znamená, že bude existovat větší počet zařízení, na které bude jednodušší zaútočit a případně je zneužít k dalšímu masivnějšímu útoku.

Způsoby jak s tímto problémem bojovat jsou velmi nákladné a komplikované, v některých případech pravděpodobně (zatím) ani neexistují, jelikož víme, že v kyberprostoru není nic plně chráněno, stejně jako neexistuje ani perfektní imunita vůči onemocnění covid-19.

Hrozbou jsou státní aktéři a tomu by měla odpovídat i naše politika

Největší hrozbou do budoucnosti i nadále zůstávají kybernetické útoky sponzorované státními aktéry. Státy totiž disponují rozsáhlými zdroji, mají nejlepší kybernetické specialisty a mají především zájmy, které mohou pomocí kybernetických operací prosazovat. V této oblastni vynikají zejména Rusko a Čína, ale i Írán či Severní Korea.

Navíc, státy budou v budoucnu v kyberprotoru pravděpodobně ještě aktivnější než je tomu dnes. Problémy „skutečného světa“ se přenesou do světa kybernetického a odtamtud zase zpět. Vojenské kapacity jednotlivých států v kyberprostoru navíc ještě posílí rozvoj 5G sítí a technologií spadající pod zastřešující termín tzv. umělé inteligence.

K potlačení tohoto trendu potřebujeme budovat odolnost, ale také se snažit, aby případná rizika vůbec nevznikala. Nové bezdrátové technologie jako je 5G, jsou úžasným pokrokem, který ale zároveň přináší další rizika. V rámci vývoje a pokroku bychom tento technologický skok měli přijmout, ale přesto být obezřetní ohledně toho, jak jej využíváme, koho si vybereme ke zprostředkování této technologie a za jakou cenu, a také jakým způsobem bychom měli zabezpečit naši infrastrukturu (a to nejen tu kritickou). Měli bychom zajistit, aby se tyto nové technologie používaly ku prospěchu obyvatelstva a ne proti obyvatelstvu.

Jak bylo popsáno výše na příkladu malwaru NotPetya, kybernetické útoky mohou mít rozsáhlé důsledky na kritickou infrastrukturu, hospodářství i konkrétní lidské životy. Je žádoucí budovat robustní opatření pro zajištění kybernetické bezpečnosti. Nelze se však domnívat, že jsme vůči kybernetickému útoku zcela imuní, byť bychom zajištění

kybernetické bezpečnosti přisuzovali sebevětší prioritu. V případě že ke kybernetickému útoku dojde, musíme se snažit abychom nastalou situaci krizovým managemetem řešili a nikoli ji nejednotným a netrasparentním přístupem ještě více zhoršovali.