FACEBOOK, WHATSAPP A INSTRAGRAM UŽ CVIČNĚ VYPNULI – CHYSTÁ SE GLOBÁLNÍ ÚTOK NA INTERNET

- CZ24 News | 5. října 2021

Zřejmě ano, a bude to mnohem horší, než současná globální krize vyvolaná pseudopandemií koronaviru.

Obrátili se na mne někteří vlastenci, kterým není lhostejný osud naší země, zda něco nevím o chystaném mezinárodním kybernetickém „cvičení“ pod organizací Světového ekonomického fóra (WEF) s názvem „Cyber Polygon“ a zda je nutné mít z této akce vážné obavy. Sám jsem nevěděl takřka nic, proto jsem se obrátil na skutečného odborníka. Můj kamarád Petr se problematice počítačů věnuje od poloviny 80-tých let, oblasti kybernetické bezpečnosti se pak soustavně profesně věnuje posledních 15 let. Je aktivním členem mezinárodní komunity „kyberbezpečáků“, takže je plně v obraze, co se v tomto světě, pro většinu smrtelníků naprosto neznámém a nepochopitelném, reálně děje.

Bylo mi v sérii následných rozhovorů řečeno přibližně toto: “Co se týká Cyber Polygonu, netřeba se zrovna tohoto obávat. Je to jen cvičení na “efekt”, každoroční cirkus pro veřejnost, který ve skutečnosti nemůže tragickou situaci v oblasti kybernetické bezpečnosti zlepšit. V lepším případě si někteří účastníci uvědomí, že opravdu musí zálohovat svá data a chránit systémy lépe než doposud a pečlivěji aplikovat „záplaty na záplaty“ svého software v bláhové naději, že tím odstranili všechny chyby a zranitelnosti tohoto software. “

Realita je ve skutečnosti mnohem, mnohem horší. Petr již dlouhodobě upozorňuje na skutečnost, že velké počítačové společnosti v honbě za krátkodobými zisky produkují v podstatě „softwarové zmetky“ a to na úkor svých zákazníků, kde většina nově vytvořených SW produktů obsahuje systémové chyby, které umožňují docela jednoduchý průnik zvenčí, a tudíž přímo vybízejí ke kybernetickým útokům, vedeným buď z kriminálních, finančních, zpravodajských, vojenských nebo politických důvodů (často se tyto důvody překrývají a násobí). Ve světě software existuje pojem „zranitelnost“, což je závažný problém, který umožňuje výrazné zneužití použitého software. Zranitelnosti jsou klasifikovány podle jejich závažnosti („severity“) od 1 do 10, přičemž 10 je chyba nejhorší. V poslední době bylo několik významných softwarových a hardwarových produktů vypuštěno s „kritickou chybou“ 10/10! Jednalo se např. o nadnárodní společnost, jejíž produkty tvoří základ síťových a internetových komponent nebo software pro připojení VPN (Virtual Private Network – pro bezpečné soukromé připojení stanic do podnikové nebo státní sítě) a jiné významné IT firmy. V obou případech proběhl velký humbuk na sociálních sítích a v IT médiích, ale za týden už se o tom nemluvilo. Všichni se ale diví, jak kyberzločinci mohli do nějakého systému proniknout. Zranitelnost 10 z 10 přitom znamená, že nejen jste si dům nezamkli, o kvalitním zámku a bezpečnostních dveřích nemluvě, ale ještě jste nechali klíče pod rohožkou, protože žádného zloděje přece nenapadne se pod ní podívat.

Kamarád Petr to přirovnává k tomu, jako by automobilka dala do prodeje automobily, u kterých by zákazník záhy zjistil, že nemají funkční brzdy. A místo toho, aby výrobce vozu okamžitě svolal všechny vozy do servisu a na své náklady brzdy opravil, tak vyzve zákazníky s tím, že chyba se skutečně stala, brzdy nebrzdí, tak my jsme vyvinuli nové brzdy a vy si je můžete nechat do svého vozu namontovat za malý poplatek (tzv. údržba software)! Přesně tak se nyní chovají počítačoví giganti. Prodávají „zmetky“ – a nikomu to nevadí! Licence na počítačový software je totiž typu „AS-

IS“, což znamená, že software si kupujete a následně používáte tak, „jak je“ (včetně chyb a zranitelností). Zmetky kupují vlády, vládní instituce, armády, policie, podniky i jednotliví zákazníci. A následně se diví, že něco nefunguje, padá, nebo je jejich počítačový systém nabouráván zvenčí. Komické je přitom to, že kyberzločinci vlastně využijí těch chyb a zranitelností, tj. použijí software tak, „jak je“, podle licence.

Problém může nastat – a zřejmě již brzy nastane – když dojde k opravdu masivnímu globálnímu útoku na počítačové systémy a uzly sítě, což se může uskutečnit již ve velice krátkém časovém horizontu, třeba na podzim tohoto roku. Když jsou vrata do významných SW programů díky mamonářské politice jejich výrobců otevřena dokořán, jen těžko se odolává pokušení toho nevyužít. Není se tedy čemu divit, že v oblasti počítačových sítí zuří kybernetická válka, která je dnes mnohem efektivnější, než jakékoliv klasické zbraně.

Problém může samozřejmě nastat, když třeba takový Západ bude chtít odvést pozornost od zmetkovité práce svých expertů a místo přiznání vlastních chyb (za které by musel třeba i nemálo zaplatit) svede vzniklý velký problém na útok „vládních hackerů“, samozřejmě z Ruska, Číny nebo KLDR, jak se již mnohokrát vyjádřil americký lžiprezident Biden (naposledy 9. července 2021, informace
zde: https://www.hlavnespravy.sk/biden-vyzval-putina-aby-zasiahol-proti-pocitacovym-zlocincom-v-rusku/2602616) „Spojené státy podniknou všechny potřebné kroky na ochranu svých obyvatel a své kritické infrastruktury před pokračováním kybernetických útoků, které podle něho pocházejí z Ruska“.

Což může samozřejmě znamenat opravdu „všechny kroky“ včetně války nebo kybernetických útoků na infrastrukturu Ruské federace.

NATO se již několikrát slovy svého generálního tajemníka Jense Stoltenberga nechalo slyšet, že i kybernetický útok může být považován za důvod pro uplatnění článku 5 Washingtonské smlouvy a tedy i pro vyhlášení války.

https://www.natoaktual.cz/v-mediich/kybervalka-kyberutoky-varovani-nato-aliancni-summit.A210620_114721_na_media_m02

Příprava na kyberpandemii, která bude horší než současná globální „pandemická“ krize.

Bude Cyber Polygon 2021 při simulaci pandemické reakce stejně prorocký jako Event 201? Připomeňme si, že v říjnu 2019 Nadace Billa a Melindy Gatesových, Johns Hopkins Center for Health Security a Světové ekonomické fórum, které spojuje zájem o zavedení Nového světového ekonomického pořádku, společně uspořádali „pandemickou simulaci“ nazvanou „Event 201“ specificky zaměřenou na koronavirus. Mezi účastníky byli čelní představitelé farmaceutického průmyslu, armády a vlivní politici. O několik měsíců později byla spuštěna operace „Pandemie COVID-19“, která zcela změnila podobu života lidí a států takřka na celém světě!!

Světové ekonomické fórum (WEF) uspořádalo dne 9. července 2021 další cvičení kybernetických útoků „Cyber Polygon 2021“. Pokračuje tak v přípravě na možnou kybernetickou pandemii, která podle slov zakladatele WEF Klause Schwaba bude horší než současná globální krize: „Kybernetický útok s charakteristikami podobnými COVID by se šířil rychleji a dál než jakýkoli biologický virus“.

V letošním roce cvičení Cyber Polygon 2021 (bližší informace o této akci jsou
zde: https://cyberpolygon.com) simulovalo fiktivní kybernetický útok s účastníky z desítek zemí (zaregistrovalo se 200 týmů ze 48 států), kteří měli reagovat na „cílený útok na dodavatelské řetězce

a podnikové systémy v reálném čase“.

Podle WEF byl COVID-19 očekávané riziko, stejně jako jeho digitální ekvivalent, o to více, kybernetický útok s charakteristikami podobnými COVID by se rozšířil rychleji a dál než jakýkoli biologický virus. Jeho reprodukční rychlost by byla asi 10x až 1000x vyšší než to, co jsme zažili u koronaviru. Jinými slovy – jdete spát a vše je v pořádku, ráno se probudíte a nefunguje nic z infrastruktury – voda, elektřina, plyn, telefony, internet, zásobování palivy, potravinami a léky apod. Proti tomu jsou tzv. mutace delta a lambda dětskou hrou.

Očekávaná kybernetická pandemie

Zakladatel WEF Klaus Schwab ve svých uvítacích projevech na Cyber Polygon 2020 varoval před nadcházející „kybernetickou pandemií“, která by byla horší než současná globální krize: “Všichni o riziku víme, ale stále věnujeme nedostatečnou pozornost děsivému scénáři komplexního kybernetického útoku, který by zcela zastavil dodávky energie, dopravu, nemocniční služby, naši společnost jako celek,” řekl.

Krize COVID-19 by byla v tomto ohledu vnímána jako malé narušení ve srovnání s velkým kybernetickým útokem. Podle WEF je „jediným způsobem, jak zastavit exponenciální šíření hrozby kybernetického útoku, úplné odpojení milionů zranitelných zařízení od sebe navzájem a od internetu“.

Více informací
zde: https://sociable.co/technology/prepping-cyber-pandemic-cyber-polygon-stage-supply-chain-attack-simulation/

Pozoruhodný je mimořádně vysoký počet účastníků z Ruské federace. Jedná se např. o ruskou státní tiskovou agenturu TASS, největší soukromou televizní společnost v Rusku NTV, bankovní gigant Sberbank, třetí největší finanční instituci v Rusku Tinkoff, nebo největší internetový obchod v Rusku Mail.ru. Z ruských politiků se akce zúčastnil Michail Mišustin, předseda vlády Ruské federace. Kamarád Petr přiznal, že si neumí vysvětlit, tak vysokou (počtem i obsazením) účast právě z Ruska, které je Západem obviňováno z většiny velkých kybernetických útoků.

Řada velkých kyberútoků přitom byla vedena před několika týdny a ukázala skutečně nebývalou zranitelnost infrastruktury USA. Takže to zavání myšlenkou, zda se skutečně nejednalo o varování a ukázku schopností nezápadních států významně narušit komplexní systém fungování západních států, které jsou již nyní z velké části plně závislé na fungování počítačových sítí.

Velmi početná účast vysoce postavených zástupců Ruské federace připomíná, že by mohlo jít o skryté mírové rozhovory navazující na Ženevu v IT oblasti potom, co Západ zjistil, že díky svým IT zmetkům dovedl sám sebe přímo před hlavně digitálních pušek a děl svých globálních protivníků. Pokud vám to připomíná rok 476 n.l., kdy barbaři (tehdy Germáni) finálně porazili antický Řím (v tu dobu tato říše existovala již tisíc let), tak podobnost není čistě náhodná.

Nějaké další informace v češtině aktuálně vyšly na Aeronetu (https://aeronet.cz/news/mamuti-hackersky-utok-na-usa-je-predehrou-simulace-kybernetickeho-utoku-cyber-polygon-2021-pod-zastitou-svetoveho-ekonomicke-fora-organizace-klause-schwaba-varuje/). Podle mého kamaráda – experta na kyberbezpečnost Petra – je otázka, nakolik má smysl kybernetické cvičení Západu přirovnávat k „pandemii Covid19“, neboť se jedná o kvalitativně odlišnou záležitost, navíc se schopností udeřit mnohem rychleji a plošněji než Covid19. Každopádně článek stojí za přečtení.

Jaký může mít dopad realizace masivního kybernetického útoku na nás?

V následné diskusi s vlastenci padla tato myšlenka: „neškodí popřemýšlet o tom, co by se stalo, kdyby se mezi lidmi rozneslo, že v důsledku výpadku počítačových sítí např. v Tescu v celé ČR nefunguje vůbec nic, nikdo si tam nic nenakoupí, apod. Toto bz se dále lavinově přeneslo na další super a hyper markety, nemluvě o situaci, kdy by výpadek informačních systémů zachvátil banky, bankomaty apod. Je lepší o tom alespoň popřemýšlet a uvědomit si, co by se pak dělo s naší společností, než to úplně pustit z hlavy“.

Samozřejmě máme docela reálnou představu o tom, co by se dělo, kdyby se rozneslo, že díky problémům se sítěmi nebo obecně s ICT nefungují obchody (nejen ty velké, ale skoro všechny, protože než si i malé obchody uvědomí, že v této krizové situaci není důležité nemarkovat na elektronické pokladně, ale za hotové peníze prodávat, dokud je co, protože stejně dříve či později při dlouhodobém výpadku dojde k vyrabování jejich prodejny hladovými davy), ale i čerpací stanice, nemocnice, banky a bankomaty – no, v podstatě všechno, včetně třeba i internetu a mobilních sítí. Ovšem mnohem fatálnější důsledky budou mít kybernetické útoky na řídící systémy elektráren, plynáren nebo vodáren a a distribučních sítí.

Spousta lidí věří, že i v případě nějakých útoků na sítě budou mít nadále k dispozici elektrickou energii, protože na elektrárnu nespadne bomba, ale zapomínají, že na elektrárnu a rozvodnou síť může být proveden kybernetický útok – a výsledek bude stejný.

Pro lidi kalkulující ve svých úvahách s takovýmito krizemi, by to neznamenalo nic, jen potvrzení jejich správného směrování a aktivaci již připravených krizových opatření. Pro velkou část našich spoluobčanů by to bylo naprosto fatální, protože na podobné situace nejsou připraveni ni mentálně, ani materiálně a stát, který se na podobné krize nepřipravuje, je v tom prostě nechá….

Autor: Aleš Přichystal