Rukověť kybernetické odolnosti

Honza Šípek

27. listopadu 2023

Model ohrožení

Počítačová bezpečnost je strašlivě podceňovaná.

Dosáhnout v ní dokonalosti je ale složité, ne-li nemožné, každopádně dost komplikované. Whistle-blower Edward Snowden měl prý na útěku čtyři notebooky: jeden na běžné surfování po webu, jeden na šifrovanou komunikaci, jeden jako „návnadu“ a jeden, který se nikdy nedotkl internetu. [1, s. 307] S vysokou mírou zabezpečení přichází i vysoká míra opruzu. Bezpečnostní odborníci tedy pracují s něčím, čemu říkají „threat-model“, model ohrožení. Proti všem teoretickým hrozbám se neubráníme, ale můžeme se bránit těm, se kterými počítáme a které odpovídají tomu, co chráníme.

Co je mým modelem ohrožení? Že mi ukradnou počítač? Že manžel objeví milence a bude mu vartovat pod oknem se slzákem? Že přijde povodeň? Že se konkurence dostane k seznamu zákazníků? Hraju proti blackoutu nebo proti tomu, že volby vyhraje extrémistická strana a to, co bylo dříve legální, se dostane za hranici zákona? (To ani nemusí být extrémní příklad politických poprav 50. let, to můžou být současné protipotratové zákony v Polsku nebo USA a následné vytěžování menstruačních kalendářů z telefonů, uložených v cloudu [2]. Nebo kriminalizace dříve legální substance).

Když odcházím, zamykám barák, protože mým modelem ohrožení je, že mne někdo vykrade. V odlehlých severských oblastech ve Finsku, kde je pravděpodobnější, že vám v mrazu chcípne auto, dojdete k nejbližší samotě, ale nedoboucháte se, a umrznete před dveřma, domy naopak nezamykají vůbec.

K modelům ohrožení je třeba přistupovat racionálně: jedna věc je, jaké riziko vnímáme a jaké nám skutečně hrozí. V potravinářství se zjistilo, že zatímco spotřebitelé mají největší strach z „éček“ (E300 je třeba vitamín C), nejčastějším zdrojem skutečných průšvihů jsou toxické produkty plísní při nevhodném skladování potravin.

Skoro každý ale hrajeme proti automatizované počítačové kriminalitě – virus z odkazu nebo přílohy poslané mailem (desetitisícům lidí současně) nakazí počítač a při nejbližší příležitosti vysaje elektronické bankovnictví, ovládne účty na sociálních sítích, které použije k šíření spamu, nebo si z našeho počítače udělá „zombie“ k DDoS útokům na Ukrajince nebo Rusy. Nebo vám zašifruje data v celém baráku a požaduje výkupné (což je smutné, když ten barák je fakultní nemocnice v Brně [3] nebo špitál

v Benešově [4] během epidemie covidu a ta data jsou ultracitlivé chorobopisy vašich pacientů. To, že se údaje o vašem zdravotním stavu dostanou do cizích rukou, je skandální, ale nejspíš vás to nezabije. To, že se k nim nedostane doktor, když je potřebuje, vás zabít může. [5])

Hackeři často mluví o ekonomice útoku: když nejste novinář, který rozkrývá korupční sítě nebo třeba operátor místní elektrárny (a co čert nechtěl, zrovna na Ukrajině, kde se schyluje k válce, jak se to stalo v letech 2015 [6, s. 10] a 2022 [7]), nebude si na vás nikdo plýtvat vzácné a drahé exploity na „zranitelnost nultého dne“. Ve svém počítači i tak máte spoustu děr, o kterých asi nevíte a které jsou útočníkům dávno známé a tedy „laciné“. Kašlali jste na updaty softwaru, heslo máte „123456“ (statisticky ho mají asi 3 procenta účtů, přičemž desetina lidí používá některé ze seznamu 25 nejčastějších hesel, takže útočník má slušnou pravděpodobnost, že se trefí během prvních pár pokusů [8]), instalujete si do počítače nebo telefonu každou blbost z neznámého zdroje, otvíráte bez rozmyslu přílohy mailů (a když jste vysoce zaměřený cíl, jako třeba důstojníci ukrajinské armády, vyplatí se takovou přílohu zfalšovat tak, že pro vás vypadá velice věrohodně, třeba rozpis služeb od nadřízeného). Smyslem obrany pak je zvýšit cenu útoku na takovou míru, že zaútočit na vás je dražší než to, co chráníte. To nemusí být jenom číslo na vašem účtu, ale i problémy, které vám způsobí, když se toto číslo sníží na nulu.

Zálohovat, zálohovat, zálohovat!

Ať je váš model ohrožení jakkoliv, dost pravděpodobně se vám stane, že ztratíte data.

„Lidé se dělí na dvě skupiny: na ty, kteří zálohují a ty, kteří ještě nepřišli o data,“ říká hacker Shaddack. Patřím do té první skupiny od té doby, co jsem v rozespalosti zakopl o šňůru k externímu disku s půlroční prací na rozdělaném filmu. Firmy specializované na obnovu dat si účtují nemalé poplatky a když vezmu v úvahu úsilí i nástroje, které jsou k tomu zapotřebí, peníze jsou to adekvátní. Ale ne vždycky se obnova podaří a málokdy úplně. Od té doby paranoidně zálohuju.

Jediné, na co se dá spoléhat je, že každý disk dříve či později chcípne. Když mi naposledy zdechl disk v pracovním počítači, vzdychl jsem, zašel do obchodu pro nový, data obnovil ze zálohy a pokračoval jsem v práci. „Zálohovat, zálohovat, zálohovat,“ říkám všem kamarádům, ale čas od času mi stejně někdo přinese disk, na kterém je něco strašlivě důležitého, co nejde přečíst. Jeden takový jsem obnovoval rychlostí 30kB/s celý jeden rok, a podařilo se zachránit půlku. Zálohování je levnější. Ale nějak hřešíme všichni.

Na cloud doporučuji nespoléhat. Jednak dáváme provozovateli svoje osobní data na podnose – smluvní podmínky psané drobným písmem jsme nečetli a nemáme šanci jim rozumět. Data jsou často uložená v jiné jurisdikci, která se na pojem „soukromí“ může dívat dost jinak než ta evropská. Nechráníme jenom svoje data, ale i data, která nám byla svěřena (právníci, lékaři, učitelé, psychologové...). Provozovatelé podléhají pokušení i státnímu tlaku na to, aby vaše data strojově analyzovali a tak se může stát, že vaše fotky dětiček od bazénu budou označeny za dětskou porno-

grafii a smazány. [9, 10] A vy zařazeni do databáze pedofilů. Ale hlavně: v případě většího průšvihu se může stát, že se ke svým datům, uloženým v datacentru někde za polárním kruhem (kde je lacinější chlazení) [11], prostě nedostanete. Budujete si závislost na třetí straně. To ne každý chce.

Při cestách do zahraničí se mi ale osvědčilo mít důležité doklady (pas, pojištění, letenky...) naskenované a uložené online. To se pak musí dobře zašifrovat. Nebo na malinkém flash-disku, který má člověk s sebou a který vám neukradnou s počítačem.

Na flash-disky se ale při dlouhodobé úschově dat spoléhat nedá. Klasické rotační disky vydrží víc, ale i ty odcházejí. Proto máme vždy alespoň jednu úplnou zálohu všeho ještě jinde a disky čas od času vyzkoušíme, případně překopírujeme. Kamarád má ten systém, že jednou za půl roku kompletní zálohu roznese na třech discích ke třem kamarádům. I o fyzický nosič totiž můžeme přijít: povodeň, krádež, zalévání kytek na polici nad disky, nebo domovní prohlídka kvůli něčemu, z čeho nás podezírali, i když se později ukáže, že jsme nic neudělali – disky budou dlouho ležet na poličce mezi důkazy a nedostaneme se k nim.

Média stárnou, nejen fyzicky, ale i morálně. Kdo zažil dobu disket, nebo CD a DVD, jistě má doma ještě krabici záloh, které už nemá na čem přečíst. Některá DVD se zálohami jsou čitelná kupodivu i po deseti letech, jiná zkorodovala a možná záleželo na tom, jestli si člověk tehdy kupoval kvalitní média nebo šetřil pár korun na jednom a pořizoval „noname“ v supermarketu. Nemáme s nimi dlouhodobou zkušenost. Dobře ustálené fotografie vydrží i sto let (co zatím víme). Plíseň vezme kus fotky v rohu, ale zbytek obrázku zůstane zjevný. Malá chybka na disku může znamenat, že nemáme žádnou fotku za posledních patnáct let. Možná jsme pár generací, po kterých nezůstane vůbec nic.

Na zálohování si člověk musí najít vlastní systém. Já to dělám automaticky, pokaždé, když dodělám větší kus práce, o který by mne mrzelo přijít. Práci s porovnáváním souborů a sledováním změn můžete přenechat specializovanému programu. Zálohování se netýká jenom počítačů, ale i telefonů, tabletů, foťáků a dalších elektronických zařízení. Oblíbená a vyzkoušená metoda je 3–2–1: máme 3 kopie svých dat (originál a dvě zálohy), na dvou různých typech médií (třeba paměťová karta, externí disk, server nebo magnetická páska, které se používají v průmyslu) a jedna z nich by měla být fyzicky uložená na jiném místě, než se nachází zbytek.

I kdybyste nenašli morál na to, zálohovat pořádně, udělejte to jakkoliv: později budete rádi. Rutina a zvyk stejně přijde až potom, co s pláčem ztratíte fotoalba svých dětí, fotky ze svatby (ani fotograf nezálohoval, nebo to je už spoustu let), roky budovanou sbírku kuchařských receptů nebo hesla ke všem službám.

Hniloba internetu

Ještě generace před náma byla generací sběratelů: nejen známek, ale i gramofonových desek, videokazet, knih nebo časopisů. Naše generace si budovala rozsáhlé archivy hudby ve formátu mp3, filmů nebo elektronických knih. Soubory se pak vyměňovaly s kamarády podobně jako nahrané kazety na burze za socíku. Dostupnost všech těchhle médií na internetu nás uvádí

do pocitu, že k jakýmkoliv informacím se můžeme dostat kdykoliv. Když se film dá stáhnout na ulož.to za pár minut, písnička přehrát na jůťubu a informace kdykoliv najít na Googlu, podléháme iluzi, že data venku jsou nějak trvalá a neschováváme si nic.

V srpnu 2020 přišla česká literatura nenávratně o kus své historie, když majitel TV Nova koupil druhdy populární službu Blog.cz a rozhodl se ukončit její provoz. [12] Videa jsou terčem protipirátských organizací nebo majitelů práv. Online noviny a časopisy zanikají, inovují weby, nebo se ocitají za platební zdí („pay-wall“). Muziku jsme si zvykli poslouchat přes internet, ale po bezplatném období začnou provozovatelé kasírovat.

Ukládám si do prohlížeče záložky na stránky, které jsem našel, četl nebo mne zaujaly. Když je procházím po dvou třech letech, zhruba třetina z nich už z webu zmizela. Po pěti tak půlka, po deseti už je štěstím otevřít vůbec něco. Říká se tomu „link-rot“, odkazová hniloba. Existují institucionální archivy jako archive.org nebo Webarchiv Národní knihovny. Americká nadace ale české stránky uloží pouze s notnou dávkou štěstí či náhody a podobně selektivní „sklizně“ NK jsou přístupné z větší části jen prezenčně v knihovně.

Důležité texty (videa, obrázky), které jsem našel, si stahuju a ukládám. Podle knihovnické pečlivosti jde najít i způsob pojmenovávání a organizace souborů, technicky zdatnější použijí i nějaký vyhledávací systém jako je například bezplatný software recoll. Podobně lze prohledávat i domácí knihovničku elektronických knih: vyhledávání často dává relevantnější výsledky než Google, protože knížky neobsahují... spam. A zůstanou vám i bez přístupu k Internetu.

Nejlepší záloha je podělit se s kamarády. A čím užitečnější data, tím spíš je někdo uchová.

Kolega dělí svá data na „černá“ a „červená“. Černá jsou veřejná, může je dát komukoliv a svobodně (v rámci zákonů) sdílet. Červená jsou soukromá a ty se mají zašifrovat a schovávat paranoidně, nejlíp aby se nikdy nedotkly internetu. Nechcete někomu s kolekcí hudby předat i svou milostnou korespondenci. To, že oba druhy dat systematicky držíme odděleně, nám usnadní a zrychlí manipulaci v budoucnosti, třeba i ve velkém stresu.

Jak se chovat bezpečně?

Počítačová bezpečnost je strašně dynamická, každý den se objevují nové zranitelnosti i metody útoku. Konkrétní rady by zastaraly dřív, než půjde kniha do tisku. Několik obecnějších rad ale snad bude mít delší platnost.

Neuděláte chybu, když budete používat bezpečný operační systém. Nechci se nekonečně hádat, ale Linux je na tom přecejenom v průměru líp, než Windows, a jednoduchost ovládání i dostupnost softwaru se už dostala do takové fáze, že je přístupný opravdu každému. Operační systémy často sbírají data pro své výrobce, a tak se vám dost snadno stane, že vaše soukromá data automaticky a bez vašeho vědomí putují na servery Microsoftu, Applu nebo Googlu, kterému patří mobilní operační systém Android. Každý software podle Murphyho zákona obsahuje alespoň jednu chybu: ty jsou často odhaleny a díry záplatovány výrobcem. Musíte si ale instalovat bezpečnostní aktualizace, jinak jste jako nazí v trní. Týká se to nejen

počítačů, ale i všech těch zařízení, na která jsme si zvykli a která nějaký počítač obsahují: modemy, IP kamery, chytré spotřebiče nebo telefony.

Dobrý zvyk je zamykat obrazovku, kdykoliv vstáváte od počítače. V počítačových firmách je oblíbeným vtípkem, když na to někdo zapomene, rozeslat jeho jménem sprosté zprávy nadřízeným. Příště si dá pozor. A co asi počítače nadřízených? Když budete obrazovku zamykat důsledně vždycky, stane se z toho zvyk, na který nezapomenete, ani když jste ve stresu, opilí nebo unavení. To platí i o jiných věcech.

Hesla si volíme dlouhá, neslovníková a unikátní. Dlouhá proto, že louskání hesla „hrubou silou“ – tedy, když stroj zkouší všechny kombinace jako „aa“, „ab“, „ac“... – je exponenciálně složitější s každým dalším znakem. Tuhle jsem zapomněl jedno z vlastních hesel a louskal ho na výkonné grafické kartě u kamaráda. Prvních pár znaků se prošlo za pár hodin. Pátý znak trval asi 14 dní. Odhad na šestý znak byl několik měsíců. Jak se znám, zvolil jsem si asi 20 znakové heslo a ke své kryptoměně se dostanu asi tak za dobu současného trvání vesmíru. Zkrátka délka hesla rozhoduje. Srandovní korporátní politiky, které nás nutí v heslu mít čísla a speciální znaky, nás přivádějí k nezapamatovatelným kombinacím (a má to logiku, další znaky stupňují obtížnost louskání, protože musíme zkoušet nejen všechna malá písmena, ale i čísla a znaky). Oblíbený citát, jednu větu z písničky, „BylaJednou1HolcickaATaSeJmenovalaKarkulka...“ obvykle nezapomenete a znaků mají habaděj.

Heslo musí být „neslovníkové“. Hackeři mají sestavené slovníky známých hesel a spojení, které hádání hesla zrychlují. Se zmíněnou Červenou Karkulkou jste asi v pohodě, s Paříží, Václavem Havlem nebo Punťou spíš ne. Heslo musí být unikátní. Vymyslíte si jedno geniální heslo a to používáte všude. Někde na internetu hacknou nějakou velkou službu a ukradnou seznamy uživatelských jmen a hesel, včetně adres a soukromých údajů (to se děje každý den). Vaše heslo se pak dostane do databází, navíc je identifikované i vašimi ostatními údaji. A stane se tím prvním, co někdo vyzkouší, klidně i automatizovaně, roboticky.

Nezanedbáváme ani dvoufaktorovou autentizaci, kdy kromě hesla používáme i další ověření. Když máme ale napadený počítač i telefon (můžou se nakazit navzájem), je nám k ničemu.

Software instalujeme jenom z prověřených zdrojů. To je teoretický problém i pro odborníky z oboru, základ ale je, neinstalovat si do počítače každou blbost. Čím méně, tím lépe. Zvlášť v chytrém telefonu by mělo platit, že instalujeme jenom to, co nezbytně potřebujeme a oprávnění aplikací osekáme na funkční minimum. Proč by aplikace, která rozsvěcí baterku měla potřebovat přístup k telefonnímu seznamu? Copak s ním asi dělá? Proč by Messenger měl mít přístup k poloze a mikrofonu? Tajné služby používají někdy princip „need-to-know“: tajné informace se sdělují jenom těm, kteří je nezbytně potřebují (a jenom v nutně nezbytném rozsahu), byť ostatní mají příslušnou bezpečnostní prověrku. Takhle bychom se měli chovat k aplikacím ve svém telefonu, protože případů jejich nevhodné „ukecanosti“ je víc než dost. A když analyzujeme síťový provoz běžného chytrého telefonu, stačí se připojit k internetu, nic nedělat, a telefon velmi čile komunikuje s kdekým a odesílá mu... bůhvíco.

Obzvláštní paranoici občas sahají ke starému tlačítkovému telefonu. Má to své výhody (velká výdrž baterie, nejdou na něj instalovat aplikace, takže

si nenainstalujete malware, který by vás sledoval, neocenitelný digitální detox) ale i slabiny (dávno známé a neopravené chyby, absence šifrování, závislost na GSM síti). S anonymní předplacenou SIM kartou se ale může hodit na jednorázový „burner–phone“, třeba když nechcete dávat podezřelému eshopu svoje telefonní číslo, nebo vás obtěžuje, když sociální síť vyžaduje k registraci ověření přes SMS.

Updatujeme. I tady může být skryté čertovo kopýtko, jeden z vektorů útoku proti ukrajinské státní správě před válkou bylo hacknutí výrobce účetního softwaru a následné infikování státních systémů při softwarovém updatu. [6] Ale takhle daleko si můžeme dovolit jít jenom, když bezpečnost opravdu řešíme vážně: a pak se dostaneme k dalším a dalším výzvám. Nezapomínáme na software (i hardware!), který už nemá bezpečnostní aktualizace. Výrobce přestane vyrábět, zkrachuje, nebo jenom produktu skončí podpora. Máme zařízení se spoustou známých chyb, které už nikdo nikdy neopraví. Zde občas pomáhá používat otevřený („open-source“) software a hardware, ale týkají se ho současně i stejné problémy.

Drtivá většina bezpečnostních průšvihů se stane díky neopatrnému používání internetového prohlížeče a emailu. Například podvržený mail, v němž nám banka píše, že něco změnila a máme se přihlásit „tímto odkazem“, vede na stránky, které vypadají jako elektronické bankovnictví, ale naše přihlašovací údaje posílají útočníkovi. Tohle se taky rychle mění, ale držíme krok s dobou, chováme se obezřetně a sledujeme aktuální doporučení odborníků. Ti si někdy povzdychnou, že nejvíc průšvihů vzniká mezi židlí a klávesnicí – a mají pravdu.

Skutečně senzitivní data (klíče, certifikáty, a obecně něco, co nikdy nesmí padnout do rukou někoho jiného) šifrujeme. Můžeme sice mít dobré heslo a používat dobrý šifrovací algoritmus, slabina ale může být v použitém softwaru. I ten může obsahovat chyby a jejich prolomení je snažším vektorem útoku než lámání hesla nebo klíče. Jsem v soukromém podezření (paranoidním, nepotvrzeném ale logickém), že výrobci operačních systémů, které umožňují šifrování samy o sobě, mají „záložní klíče“. Pak už jenom záleží, kdo je náš protivník: je-li to strana spolupracující s výrobcem softwaru (jak odhalil právě Snowden v případě Spojených států, nebo jak se Západ logicky obává v případě čínských aplikací jako TikTok), nebo někdo, komu je ochotna je předat či vyměnit za protislužbu, jsme v loji.

To už se ale týká spíš vysoce zaměřených cílů. Pokud jsme novinář, politik, voják, vědec ohrožený průmyslovou špionáží, disident, whistle–blower, cestujeme do Číny nebo máme cizí citlivá data, chováme se o to obezřetněji a zjistíme si o počítačové bezpečnosti co nejvíc (mění se v čase, nemá smysl psát do knížky). Nájemný špionážní software Pegasus izraelské firmy NSO Group, poprvé odhalený v roce 2016, měl pozoruhodné spektrum obětí od politiků, vládních i opozičních, přes diplomaty, novináře, lidskoprávní bojovníky až po lidi z neziskovek. Základní kyberškolení pro dokumentaristy působící v konfliktních oblastech jsme na FAMU zvládli za den. Když pak v roce 2022 unikly emaily některých pedagogů FAMU, kteří osnovali palácový převrat (jak je v Čechách dobrým zvykem, vznikla z nich divadelní hra [13]), neudělal autor leaku žádnou chybu, která by vedla k jeho odhalení. Nevím, jestli to souvisí, ale potěšilo.

Míra vaší osobní počítačové paranoii bude asi záviset od osobnosti. Jsou lidé, kteří se světu důvěřivě odevzdávají a nebojí se ho ani náznakem. To je

ve světě počítačové bezpečnosti bezbřehá naivita. Na druhé straně spektra jsou lidé skrývaví, kteří o nejosobnějších věcech nemluví ani s nejbližšími, na nich by se jistě psychologové vyřádili. Hodně jich nalezneme mezi hackery, protože domýšlení důsledků a potenciálních hrozeb vede k odhalování dalších slabin, až je z člověka... hacker. „Snowden mne vyléčil z paranoie. Nebyla to paranoia," připsal nám jeden z nich tužkou do pracovního výtisku Nebezpečné knihy. Vědomí všudypřítomného sledování (které se stalo průmyslovým odvětvím, jak popisuje Shoshana Zuboff ve své knize *Věk kapitalismu dohledu*) může vést u některých lidí k rezignaci: „Stejně mne sledují na každém kroku, není způsob, jak se bránit." I tady hledáme balanc, střední cestu. Úvahy o modelu ohrožení i ekonomice útoku mohou pomoct. A i zde platí, že „něco je lepší než nic". Ten malý krůček, který jsme udělali navíc, může být v případě průšvihu rozdíl mezi katastrofou a přežitím.

Decentralizace

Internet původně vznikl jako decentralizovaná síť, podle legend proto, aby přežil jadernou válku (není to úplně pravda, ale decentralizovaný by ji skutečně přežil). Redundance propojení jeho jednotlivých uzlů (tj. více propojek, než nezbytně potřebujeme) a eliminace hustě propojené „centrály" dává síti robustnost. Když přestane něco fungovat, data mohou téct jinudy, kolem, dokonce každý kousek jinou cestou a na konci se zase složí. Ekonomika komerčního provozu ale v průběhu času vedla k tomu, že se Síť vrátila k silnější centralizaci.

Český internet, tedy sítě jeho jednotlivých poskytovatelů, jsou v ČR propojeny v Praze, trošku i v Brně. Při průšvihu tam se bez internetu ocitá víceméně celá republika. Když procházím obřím klimatizovaným sálem datového centra, kde vedle sebe v policích hučí tisíce serverů, které obsluhují místní internet, představuju si, jakou paseku by udělal *jeden jediný* granát (a při běžných průšvizích není potřeba ani to, jako třeba když v roce 2022 v části Prahy, v níž stojí datacentrum Master, vypadla elektřina a vzápětí selhalo několik záložních systémů současně [14]).

Ukrajinský Internet při ruské invazi v roce 2022 přežil kupodivu docela dobře, protože vzhledem k rozloze země nebyla tamější síť tolik centralizovaná jako u nás. [15] Pomohla i pomoc zvenčí, dobročinné sbírky hardwaru, které do země vozily náklaďáky ze západu i pro bono satelitní připojení StarLink od milardáře Muska (které pak vypnul v okolí Krymu, během útoku ukrajinských podmořských dronů na ruskou černomořskou flotilu a efektivně tak přerušil jejich řízení [16]). V případě průšvihu se dá počítat s tím, že internet bude fungovat omezeně nebo vůbec. Jeden překopnutý podzemní kabel nebo podmořský, spojující Internet na kontinentech, může znamenat omezení, výrazné zpomalení připojení do některých oblastí i přetížení okolních tras. Když kolem podmořských internetových kabelů brousí ruské ponorky, oprávněně znejistíme [17].

Občas, když u nás vypadne třeba Google (lokální výpadky po světě jsou časté), vyjde najevo nečekaná závislost: kupříkladu sice máte svůj web hostovaný v ČR, ale na rozlišování živých návštěvníků a robotů používáte systém od Googlu – a celý váš web přestane fungovat. V Rusku už v roce 2019 podnikli velký test (pravděpodobně už to byla příprava na válku), zda jsou

zemi schopni odpojit od „vnějšího internetu“ a snažili se tak odhalit a odstranit podobné závislosti [18]. Dává to smysl. Že s tímto ostrovním provozem jde ruku v ruce ostražitá „pohraniční stráž“ státních cenzorů i sledovačů na síťových „hraničních přechodech“ (orgán Roskomnadzor a systém SORM), je druhá věc [19].

I v časech klidu a míru nám občas „nejde Internet“, protože průšvih má někdo z místních operátorů. Zatímco sousedovi ve vedlejším bytě, který má jiného operátora, „internet funguje“. Zůstáváte tak odříznuti od spojení a máte jenom data, která máte doma. V případě spoléhání na dostupnost Síťě se z vašeho počítače stává jenom chytřejší psací stroj. Nejjednodušším krokem je sdílení připojení se sousedy nebo domácí server třeba z vyřazeného počítače, který obsahuje data, k nimž má přístup celá rodina. Chce to trochu znalostí a péče, ale leckomu se to vyplatí i jenom kvůli sledování seriálů na chytré televizi. Nebo kvůli domácímu DNS serveru, který pomůže zpřístupnit weby zakázané státem nebo operátory.

Kolem roku 2002, kdy vysoké ceny operátorů a jejich nízká schopnost instalovat nové přípojky vedly k tomu, že v Praze z podobných „sousedských sítí“ vznikla decentralizovaná síť známá jako CZFree.Net. Připojení od kamoše ke kamošovi za pomoci wi-fi vysílačů, kabelů natažených světlíkem nebo po střeše, optická laserová pojítka, ubastlená z laserových ukazovátek, sdílení vlastního připojení k internetu těm, kdo na něj byli ochotni přispět, dala vzniknout síti, která byla sice občas pomalá, ale plně v rukou jejích uživatelů a odolná proti výpadkům centrál. Pozdější rozšíření lacinéh širokopásmového internetu sice v Praze vedlo k útlumu této sítě, v hradeckém nebo plzeňském kraji ji ale místní spolky provozují do dnešních dnů docela úspěšně (jenom čelí útokům berňáku, kterému se před soudem snaží vysvětlit, že negenerují zisk a že jejich členové nejsou de facto zákazníci [20]).

Když se z domácího serveru pro rodinu stane server pro celý dům, komunitu nebo vesnici, když se navzdory nefunkčnímu připojení ven jsme schopni spojit alespoň v rámci města nebo okresu, když v konkrétních spojích nespoléháme na techniky korporace, co přijedou z města, ale na zdatné sousedy, co jsou po ruce, je to v případě katastrofy víc než nic.

Hybridní model může obsahovat více druhů připojení (ideálně včetně satelitního), mezi nimiž se automaticky přepíná (to už chce technického ducha na zprovoznění), nebo jednodušší sdílení wi-fi se sousedy, kteří mají jiného operátora. Technicky založení jedinci můžou experimentovat s přenosem typu „packet radio“ na radioamatérských frekvencích, které se obejdou bez kabelů a mají násobně delší dosah než wi-fi. Sice jsou pomalé, ale těch pár kilobytů informací může být někdy lepší než informace žádné (zpráva: „Jsem živej, ve 3 u lípy,“ je jenom pár bytů). V případě potřeby přenosu větších dat možná dojdeme ke „kabelovému přenosu“: data nahrát na disk a v kabele odvézt někam jinam :-). A jak upozorňuje hacker Shaddack, i poštovní holub na microSD kartách unese nezanedbatelné množství dat. A vzhledem k objemu i nezanedbatelně rychle.

Komunikace

Problém centralizace se netýká jenom internetu samotného, ale i služeb, které na něm používáme. Komunikačních, vyhledávacích a emailových služeb existovala původně bohatá diverzita, včetně množství sociálních sítí. Podle pravidla nabalující se sněhové koule ale některé služby přerostly do de-facto monopolu a používají je skorem všichni – ostatní pomalu vymírají. Bohatí bohatnou, chudí chudnou. Centralizované služby s sebou nesou i centralizovanou moc a o názorech drtivé většiny světové populace rozhoduje dnes to, co jim naservírují algoritmy Facebooku. Algoritmy, jejichž fungování je nejasné a tudíž nepodléhá veřejné kontrole. Stránka, kterou nenajde Google, pro svět neexistuje. Velcí hráči se ale taky snadněji regulují, stát se s nimi snadněji dohodne na cenzuře i předání osobních údajů uživatelů státním službám.

To, co potřebujeme, je komunikace decentralizovaná, nevlastněná jednou firmou či jednotlivcem. A pokud nám záleží na důvěrnosti přenášených zpráv, též i šifrovaná (end-to-end, tedy celou cestu od toho, kdo ji poslal, k tomu, kdo ji čte). Občas takové varianty vzniknou, problém ale je, s kým si popovídáte přes chat nebo sociální síť, které (skoro) nikdo jiný nepoužívá. Kromě vytrvalého přesvědčování blízkého kroužku přátel, se kterými chceme komunikovat, se občas objeví disruptivní událost, která přechodu k alternativě pomůže.

Když Elon Musk v roce 2022 koupil platformu Twitter a začal cenzurovat některé novináře [21], nastal masivní úprk miliónů uživatelů k decentralizované sociální síti Mastodon. [22, 23] Mastodon nemá ani vlastníka, ani centrální servery. Jeho server může provozovat každý, kdo je toho technicky schopen, a své služby nabízet každému, o koho bude stát. Instancí jeho serverů vzniklo mnoho, udržují je dobrovolníci, a zprávy si vyměňují mezi sebou, bez ohledu na hierarchii. Pokud chtějí omezit trolly zvenčí, uzavřou server lidem mimo svou vlastní komunitu.

Klastru podobných otevřených a decentralizovaných služeb se říká Fediverse. Najdeme v nich například i decentralizovanou variantu YouTube, webový přehrávač videí, křížený s torrentem. Osobně rád experimentuju s decentralizovaným fulltextovým vyhledáváním. Ve škatuli pod stolem mám zaindexovaných asi 30 milionů zpravodajských textů, o jejichž vyhledávání se dělím s dalšími dobrovolníky – a zkouším, jestli jsem schopen nahradit si vyhledávač Google. [24] Dře to. Je to bláznovství, kterému se kamarádi smějou. Ale prozkoumávat alternativy mne baví.

V panice se ale dá sáhnout i ke špatné variantě. Organizovat protivládní protesty v Bělorusku v roce 2020 umožnila aplikace Telegram [25], která nebyla pod kontrolou běloruského státu a tvrdilo se, že ani toho ruského. Typickým scénářem, kdy potřebujete komunikaci nezávislou na státu totiž je, když jste vůči němu v opozici. A není divu, že na Telegram přešly všechna místní opoziční média, která Lukašenkův režim postupně likvidoval [26, 27] (včetně jamesbondovské zápletky s nuceným přistáním letadla se zakladatelem kanálu NEXTA pod záminkou bomby na palubě a jeho následným uvězněním [28]). Když EU po ruské invazi na Ukrajinu v březnu 2022 zakázala některá státní ruská média s nejflagrantnější propagandou [29], začaly Telegram k šíření svých zpráv používat i ony [30]. Šifrování „z jednoho konce na druhý“ (end-to-end), na které Telegram láká,

je vypnuté ve standardní instalaci, dá chvíli práce ho zapnout a někdy to ani nejde. Skupinové chaty a kanály toto šifrování neumožňují vůbec. Reputace majitele pochybná. Útěkem k domněle bezpečné variantě si tedy můžeme i uškodit. Jako se to stalo drogovým dealerům po celé Evropě, kteří spoléhali na údajně dokonale bezpečnou komunikační aplikaci EncroChat a pak je v létě 2020 posbírali všechny v jednom celoevropském zátahu [31]. Nejsme drogoví dealeři, ale pokud chceme mít možnost někomu skutečně soukromě sdělit tajemství nejtajnější, zjistíme, že je to i v 21. století podivuhodně obtížné.

Modelovým příkladem decentralizovaného chatu snů může být například aplikace Briar. Nepotřebuje žádné centralizované servery, zprávy si dokáže vyměňovat i bez internetu, stačí, když jsou spolu telefony v kontaktu. Umí i předat zprávu pro někoho jiného, která se pak šifrovaná šíří telefon od telefonu, dokud nedoputuje k cíli. Podobá se to „mesh-sítím“, které nemají centralizované uzly, ale síť propojují ad-hoc podle toho, jak jsou v dosahu jednotliví účastníci. Telefon v kapse pak není pasivním příjemcem služeb, ale i jejich aktivním prostředníkem. K síti se tak dostaneme i bez přímé viditelnosti na „centrální anténu“, stačí, když je v okolí někdo jiný. Není divu, že mesh-sítě používá armáda v podmínkách, kde je udržet centralizovanou strukturu složité.

Kdo chce decentralizovat ještě šířeji, nevyhne se určitě zájmu o kryptoměny, protože finanční toky jsou snadným a logickým terčem (např. Visa a MasterCard přinutily ke spolupráci pornoserver PornHub prostě tím, že mu zrušily přijmání plateb za reklamu [32], podobně jako spolu s PayPalem odřízly od financování server WikiLeaks [33, 34]). S decentralizovanou měnou nám to nehrozí. Do problémů se dostaneme jenom, když ji chceme vyměňovat za *fiat* peníze.

Black-out

Pokud do vašeho modelu ohrožení patří i black-out (asi by měl), skončíte nejspíš u nějakého solárního panelu. Pokud se nebudete namáhat s připojením k okolní elektrické síti, není to zase taková věda, jak to líčí firmy, které se tím živí. Naši mají chatu v oblasti, kam není zavedena elektřina. Metrový solární panel pokryje pohodlně základní spotřebu domácnosti – na svícení, rádio, dobíjení akuvrtačky i provoz čerpadla stačí. Energožrout lednička je na plynovou bombu, kamna na dřevo.

Skládací solární panel s větší powerbankou utáhne i při lehce zamračeném počasí bez problému i provoz laptopu. Pozor si ale musíte dát na to, že pokud chcete zůstat připojení k internetu, potřebujete napájet například i router (a stejně jste závislí na tom, zda běží nebo neběží síť operátora), stejně jako další přístroje a nabíječky. Utopíte se v množství rozličných konektorů, přestože přístroje většinou stejnak potřebují jenom 5 nebo 12 V stejnosměrných. Solární nabíječky se často dodávají s množstvím rozličných redukcí (pozor na napětí a polaritu), včetně krokodýlků na nabíjení autobaterky.

Není špatným řešením použít jako domácí napájecí standard USB a zohlednit jej při nákupu nových přístrojů. USBčkem jsou vybaveny powerbanky, které můžeme nabíjet ze soláru, nebo v nich donést energii odjinud.

USB nabíječku má v baťohu kdedko a patří k sortimentu i každé vesnické vietnamské sámošky. A když USBčkem napájíte světlo, nabíječky, telefon i počítač, je lhostejno, zda je krmíte z jiného počítače, zásuvky, powerbanky, zapalovače v autě nebo soláru. Jenom je potřeba si dát pozor na zásobu správných kabelů (je jich bambilión typů), které se s oblibou lámou a ztrácejí. Vyplatí se zvažovat i různou spotřebu přístrojů: zatímco smartphone vydrží v plném provozu nabitý jenom jednotky hodin, tlačítkový telefon několik dní a nepodsvícená čtečka elektronických knih na jedno nabití i celé měsíce.

Většinu z výše jmenovaného ale stejně nezařídíme v situaci, kdy průšvih už nastal. Budeme k tomu potřebovat internet, elektřinu, zboží i rady expertů. Počítá se jenom to, na co jsme se připravili dopředu. Nejlíp tak, že nám to k něčemu bylo i za klidějších časů.

Text je kapitolou z připravované knihy V. Cílka, A. Ibrahima a kol. „Nové ostrovy“ (Dokořán, 2024).

Reference

[1] Edward Snowden: *Nesmazatelné záznamy*. Alpress, Frýdek-Místek (2020).

[2] Richard Luscombe: *Virginia governor blocks bill banning police from seeking menstrual histories*. The Guardian, (2023). URL https://www.theguardian.com/us-news/2023/feb/16/virginia-governor-glenn-youngkin-extreme-bill-police-menstrual-histories. [Online; získáno 2023-09-29].

[3] gen Hana Novotná: *Před třemi roky zasáhl Fakultní nemocnici Brno kybernetický útok. Systém dodnes není plně obnovený*. iRozhlas.cz, (2023). URL https://www.irozhlas.cz/zpravy-domov/kyberneticky-utok-nemocnice-brno-obnova-dat_2303132201_gen. [Online; získáno 2023-09-29].

[4] Jana Magdoňová: *Na nemocnici v Benešově útočil ruský virus Ryuk. Jermanová odmítá, že by někdo požadoval výkupné*. iRozhlas.cz, (2020). URL https://www.irozhlas.cz/zpravy-domov/nemocnice-benesov-kyberneticky-utok-ransomware-vykupne-ochrana-osobnich-udaju_2001140615_cha. [Online; získáno 2023-09-29].

[5] *German hospital hacked, patient taken to another city dies*. Associated Press, (2021). URL https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94. [Online; získáno 2023-09-29].

[6] Scott W. Brady: *USA vs Yuriy Sergeyevich Andrienko et al. - Indictment* (10 2020). URL https://int.nyt.com/data/documenttools/russian-cyberattacks-indictments/144ea8fe6680730c/full.pdf. [Online; získáno 2023-09-29].

[7] Ilona Khmelova: *Cyber, Artillery, Propaganda. Comprehensive Analysis of Russian Warfare Dimensions* (2022). URL https://cip.gov.ua/services/cm/api/attachment/download?id=50923. [Online; získáno 2023-09-29].

[8] TeamsID: *Top 50 Worst Passwords of 2019*. TeamPassword blog, (2019). URL https://teampassword.com/blog/top-50-worst-passwords-of-2019. [Online; získáno 2023-09-29].

[9] Kashmir Hill: *A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal.* The New York Times, (2022). URL https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html. [Online; získáno 2023-09-29].

[10] Leo Kelion: *Microsoft tip leads to child porn arrest in Pennsylvania*. BBC, (2014). URL https://www.bbc.com/news/technology-28682686. [Online; získáno 2023-09-29].

[11] Danny Bradbury: *Super cool: Arctic data centres aren't just for Facebook*. The Register, (2016). URL https://www.theregister.com/2016/05/12/power_in_a_cold_climate/. [Online; získáno 2023-09-29].

[12] David Slížek: *Blogovací platforma Blog.cz po patnácti letech definitivně končí*. Lupa.cz, (2020). URL https://www.lupa.cz/aktuality/blogovaci-platforma-blog-cz-po-patnacti-letech-definitivne-konci/. [Online; získáno 2023-09-29].

[13] S. d. Ch.: *Filmařská trilogie*. Rubato, Praha (2023).

[14] Petr Krčmář: *Výpadek v datacentru Master Internet vyřadil spoustu služeb včetně Root.cz*. Root.cz, (2022). URL https://www.root.cz/zpravicky/vypadek-v-datacentru-master-internet-vyradil-spoustu-sluzeb-vcetne-root-cz/. [Online; získáno 2023-09-30].

[15] Petr Krčmář: *V jakém stavu je internet na Ukrajině? Většina sítě funguje díky decentralizaci*. Root.cz, (2022). URL https://www.root.cz/clanky/v-jakem-stavu-je-internet-na-ukrajine-vetsina-site-funguje-diky-decentralizaci/. [Online; získáno 2023-09-30].

[16] Julian Borger: *Elon Musk ordered Starlink to be turned off during Ukraine offensive, book says*. The Guardian, (2023). URL https://www.theguardian.com/technology/2023/sep/07/elon-musk-ordered-starlink-turned-off-ukraine-offensive-biography. [Online; získáno 2023-10-05].

[17] H. I. Sutton: *How Russian Spy Submarines Can Interfere With Undersea Internet Cables*. Forbes, (2020). URL https://www.forbes.com/sites/hisutton/2020/08/19/how-russian-spy-submarines-can-interfere-with-undersea-internet-cables/. [Online; získáno 2023-09-30].

[18] David Slížek: *Úspěšně jsme otestovali odpojení od světového internetu, hlásí Rusko*. Lupa.cz, (2019). URL https://www.lupa.cz/aktuality/uspesne-jsme-otestovali-odpojeni-od-svetoveho-internetu-hlasi-rusko/. [Online; získáno 2023-09-30].

[19] Agáta Lukášková: *Listopadová revoluce. Odstřihne Putin Rusko od internetu?* Finmag, (2019). URL https://finmag.penize.cz/spolecnost/410506-listopadova-revoluce-odstrihne-putin-rusko-od-internetu. [Online; získáno 2023-09-30].

[20] Martin Drtina: *Spolky provozující komunitní internet založily sdružení na obranu před finančními úřady*. Lupa.cz, (2023). URL https://www.lupa.cz/aktuality/spolky-provozujici-komunitni-internet-zalozily-sdruzeni-na-obranu-pred-financnimi-urady/. [Online; získáno 2023-09-30].

[21] David Slížek: *Twitter začal blokovat odkazy na Mastodon, účty pozastavil i některým americkým novinářům*. Lupa.cz, (2022). URL https://www.lupa.cz/aktuality/twitter-zacal-blokovat-odkazy-na-mastodon-ucty-zrusil-i-nekterym-americkym-novinarum/. [Online; získáno 2023-10-02].

[22] Alex Hern: *Joining the herd: what's it like moving from Twitter to Mastodon?* The Observer, (2022). URL https://www.theguardian.com/technology/2022/nov/12/joining-the-herd-whats-it-like-moving-from-twitter-to-mastodon. [Online; získáno 2023-10-02].

[23] Wilfred Chan: *Thousands fled to Mastodon after Musk bought Twitter. Are they still 'tooting'?* The Guardian, (2023). URL https://www.theguardian.com/technology/2023/apr/18/mastodon-users-twitter-elon-musk-social-media. [Online; získáno 2023-10-02].

[24] Jan Šípek: *Decentralizovaný vyhledávač YaCy: indexujte a vyhledávejte si po svém*. Root.cz, (2020). URL https://www.root.cz/clanky/decentralizovany-vyhledavac-yacy-indexujte-a-vyhledavejte-si-po-svem/. [Online; získáno 2023-10-02].

[25] Daria Litvinova: *'Telegram revolution': App helps drive Belarus protests*. Associated Press, (2020). URL https://apnews.com/article/international-news-technology-business-ap-top-news-europe-823180da2b402f6a1dc9fbd76a6f476b. [Online; získáno 2023-10-01].

[26] Lucie Sýkorová: *Nezávislí novináři v Bělorusku živoří, většina chce ale zůstat a vidět padnout Lukašenka*. Hlídací pes, (2020). URL https://hlidacipes.org/nezavisli-novinari-v-belorusku-zivori-vetsina-chce-ale-zustat-a-videt-padnout-lukasenka/. [Online; získáno 2023-10-02].

[27] Lucie Sýkorová: *Bělorusko rok po volbách opouštějí stovky novinářů. Kdo neodejde, skončí za mřížemi*. Hlídací pes, (2021). URL https://hlidacipes.org/belorusko-rok-po-volbach-opoustej

i-stovky-novinaru-kdo-neodejde-skonci-za-mrizemi/. [Online; získáno 2023-10-02].

[28] Ivan Nechepurenko Anton Troianovski: *Belarus Forces Down Plane to Seize Dissident; Europe Sees 'State Hijacking'*. The New York Times, (2021). URL https://www.nytimes.com/2021/05/23/world/europe/ryanair-belarus.html. [Online; získáno 2023-10-01].

[29] *NAŘÍZENÍ RADY (EU) 2022/350 ze dne 1. března 2022, kterým se mění nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině* (03 2022). URL https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=OJ:L:2022:065:FULL. [Online; získáno 2023-10-01].

[30] Josef Šlerka: *Český Telegram jako ruský tlampač*. Investigace.cz, (2023). URL https://www.investigace.cz/cesky-telegram-rusky-tlampac/. [Online; získáno 2023-10-02].

[31] Swati Khandelwal: *Police Arrested Hundreds of Criminals After Hacking Into Encrypted Chat Network*. The Hacker News, (2020). URL https://thehackernews.com/2020/07/encrochat-encrypted-phone.html. [Online; získáno 2023-10-02].

[32] Michelle Price: *Mastercard, Visa suspend ties with ad arm of Pornhub owner MindGeek*. Reuters, (2022). URL https://www.reuters.com/business/finance/mastercard-visa-suspend-ties-with-ad-arm-pornhub-owner-mindgeek-2022-08-04/. [Online; získáno 2023-10-02].

[33] Andy Greenberg: *Visa, MasterCard Move To Choke WikiLeaks*. Forbes, (2010). URL https://www.forbes.com/sites/andygreenberg/2010/12/07/visa-mastercard-move-to-choke-wikileaks/. [Online; získáno 2023-10-02].

[34] Kevin Poulsen: *PayPal Freezes WikiLeaks Account*. Wired, (2010). URL https://www.wired.com/2010/12/paypal-wikileaks/. [Online; získáno 2020-07-28].