ČÁST PRVNÍ: PŘÍRUČKA CRYPTOPARTY

HISTORIE CRYPTOPARTY

Protože všechno zní lépe, když slíbíte, že tam bude pivo.

Co je CryptoParty?

Skupina či skupiny lidí, kteří se zajímají o počítače a další zařízení a jsou ochotni se učit, jak vyyužívat nejzákladnější šifrovací programy a fundamentální koncepty jejich operací! CryptoParty jsou vždy otevřené, veřejné a bez komerčního záměru.

CryptoParty je decentralizovaná globální iniciativa, která se snaží veřejnosti představit základní kryptografické nástroje – jakými jsou síť Tor, veřejný šifrovací klíč (PGP/GPG) a OTR (Off The Record messaging).

Nápad CryptoParty vznikl 22. srpna 2012 jako výsledek běžné konverzace na Twitteru mezi informačním aktivistou vystupujícím pod identitou Asher Wolf a počítačovými experty v oblasti bezpečnosti. Důvodem byly obavy z důsledků Cybercrime Legislation Amendment Bill 2011 (australská legislativa o kyberbezpečnosti – pozn. překl.).

"DIY, samoorganizační hnutí se okamžitě stalo virálem s tucty autonomních CryptoParty, které byly zorganizovány během pár hodin ve městech napříč Austrálií, Spojenými státy, Spojeným královstvím a Německem."

Šestnáct současných CryptoParty (údaj se vztahuje k datu psaní této příručky, tzn. začátek října 2012 – pozn. překl.) se odehrály v mnoha různých zemích po celém světě a mnohé další jsou plánovány. Užívání Toru v Australii se po čtyřech CryptoParty výrazně zvýšilo a londýnská CryptoParty se musela přesunout z londýnského Hackspace do kampusu Google, aby se přizpůsobila počtu zvědavých účastníků, který se vyšplhal na 120 se vstoupenkou a s 30 dalšími lidmi na čekacím seznamu. Obdobně probíhala i CryptoParty Melbourne – původně plánována pro 30 účastníků, ale nakonec se jich ukázalo 70.

CryptoParty obdržela dopisy podpory od Electronic Frontier Foundation, AnonyOps, whistleblowera z NSA Thomase Drakea, bývalé hlavní editorky Wikileaks Central Heather Marshové a reportéra Wired Quinna Nortona. Eric Hughes, autor Cypherpunkového manifestu zformulovaného před dvaceti lety, dodal CryptoParty v Amsterdamu základní myšlenky.

MANIFEST CRYPTOPARTY

"Muž je nejméně sám sebou, když hovoří sám za sebe. Dejte mu masku a on vám poví pravdu." – Oscar Wilde

V roce 1996 John Perry Barlow, spoluzakladatel Electronic Frontier Foundation, napsal Deklaraci nezávislosti kyberprostoru. Ta obsahuje i následující pasáž:

> *Kyberprostor se skládá z jednání, vztahů a myšlenek samotných, seskupuje se jako stálá vlna v síti naší komunikace. Náš svět je takový, který je zároveň všude i nikde, ale rozhodně není tím, kde žije tělesná schránka.*
>
> *Vytváříme svět, do kterého může vstoupit kdokoliv bez privilegia nebo předsudku kvůli rase, ekonomickému vlivu, vojenské síle nebo místě v životě.*
>
> *Vyváříme svět, kde může kdokoliv kdekoliv vyjádřit své přesvědčení, bez ohledu na to, jak je zvláštní, beze strachu z vynucování tichého souhlasu.*

O šestnáct let později změnil Internet způsob, jakým žijeme naše životy. Předal nám mnoho kombinovaných lidských znalostí. Můžeme utvářet nové vztahy a sdílet své myšlenky a životní příběhy s přáteli po celém světě. Můžeme organizovat, komunikovat a kolaborovat tak, jak by nikdo nečekal, že by bylo možné. Tohle je svět, který chceme předat svým dětem, svět se svobodným Internetem. Naneštěstí ne vše z vize Johna Perryho Barlowa se stalo skutečností. Bez možnosti online anonymity se nemůžeme osvobodit od privilegií či předsudků. Bez soukromí je svobodné vyjádření nemožné.

Problémy, kterým čelíme v 21. století vyžadují společnou práci celého lidstva. Tyto problémy jsou vážné: klimatické změny, energetická krize, státní cenzura, masový dohled a pokračující války. Musí nám být umožněno komunikovat a slučovat se beze strachu. Potřebujeme podpořit open source projekty, které chtějí zlepšit běžnou znalost technologií, na kterých my

všichni závisíme. (http://opensourceecology.org/wiki)

Abychom si uvědomili naše právo na soukromí a anonymitu online, potřebujeme odborně posuzovaná a hromadně založená řešení. CryptoParty nabízí příležitost k setkání a k přiučení se dovednostem s těmito řešeními, které nám všem mohou poskytnout prostředky k uplatňování našeho právo.

- Všichni jsme uživatelé, bojujeme za uživatele a usilujeme o posílení pozice uživatele. Jsme přesvědčeni, že 'uživatelské požadavky' jsou důvod, proč počítače existují. Věříme v kolektivní moudrost lidských bytostí, nikoliv prodejcům software, korporacím nebo vládám. Odmítáme okovy digitálních gulagů ovládaných vazaly ve službách zájmů vlád a korporací. Jsme cypherpunkoví revolucionáři.

- Právo na osobní anonymitu, pseudoanonymitu a soukromí patří mezi základní lidská práva. Tato práva obsahují právo na život, svobodu, důstojnost, bezpečnost, právo na rodinu a právo žít beze strachu či zastrašování. Žádná vláda, organizace ani individuum by neměly bránit lidem v přístupu k technologiím, které tato práva umožňují.

- Soukromí je absolutní nárok individua. Transparence je požadavek na korporace a vlády, které jednají ve jménu lidu.

- Pouze individuum vlastní právo na svou identitu. Pouze jedinec si vybírá, co bude sdílet. Vynucovací pokusy získat přístup k soukromým informacím bez předchozího souhlasu jsou narušením lidských práv.

- Všichni lidé jsou oprávněni věnovovat se kryptografii, bez ohledu na rasu, barvu, pohlaví, jazyk, náboženství, politický či jiný názor, národní či sociální původ, majetek, věk nebo statut země či teritoria, ve kterém daný člověk sídlí.

- Stejně jako mají vlády existovat jen pro to, aby sloužily občanům, kryptografie by měla patřit lidem. Technologie by neměla být uzamčena a schována mimo dosah lidí.

- Dohled nemůže být oddělen od cenzury a otroctví, které je jejím následkem. Žádný stroj by neměl být využíván pro sledování a cenzuru. Šifrování je klíč k naší společné svobodě.

- Kód je projev: kód je člověkem vytvořený jazyk. Zamezit, cenzorovat či odepřít kryptografii lidem je jako připravit člověka o svobodu projevu.

- Ti, kdo se snaží zastavit šíření kryptografie, jsou podobni kléru 15. století, který se pokoušel zarazit šíření knihtisku, neboť se obával ztráty monopolu na znalosti.

JAK NA CRYPTOPARTY

- Připrav party. Vše, co potřebuješ, je čas, datum a místo. Přidej se na wiki: https://cryptoparty.org/

- Ujisti se, že budeš mít dobré připojení k Internetu a dostatek zdrojů elektřiny pro všechna zařízení. Pokud nemáš místo, kde CryptoParty uspořádat, najdi hospodu nebo park, kde se mohou účastníci sejít a zmáčkni veřejný bandwidth. To vybrousí tvé dovednosti!

- Přines usb disky a vytištěné materiály pro ty, kteří je potřebují, a nastav staré počítače lidem, aby si s nimi mohli pohrát a vyzkoušet nové dovednosti.

- Mluv o Linuxu s každým, koho na CryptoParty potkáš. Pokud jsi v CryptoParty nový, zeptej se někoho, co Linux je.

- Umožni přístup zdarma, pokud to je možné. CryptoParty jsou neziskové a nekomerční, důležité jsou zejména pro ty bez prostředků.

- Uč hromadně zacházení se základními kryptografickými nástroji. Doporučujeme výuku zahájit s PGP, OTR a Torem.

- Přizvi experty i ne-experty ze všech oblastí. Každý je v něčem expertem.

- Pokud chceš, aby CryptoParty něco udělala, začni to na tom dělat. Organizuj organicky a chaoticky. Neměj jasné vedení. Přesvědčuj lidi, aby se ujali 'sudo role' – při přípravě výuky, opravení wifi, aktualizování wiki nebo organizování další

CryptoParty. Pokud někdo tvrdí, že ostatní to dělají špatně, přizvi ho, aby to zlepšil.

- Požaduj zpětnou vazbu. Asimiluj kritiky – požádej je o pomoc při vytváření lepší CryptoParty. Neměj strach z trollů, troll je nazpět, nebo je vykaž ze svého shromáždění. Sdílej zpětnou vazbu na wiki. Opakuj.

- Úspěšná CryptoParty může mít mnoho i málo účastníků. Velikost není důležitá, to, co chceš dělat, je důležité. Hlavním kritériem pro úspěch je, že se každý bavil, něco se přiučil a chce přijít na další party.

- Uvažuj o hnutí CryptoParty jako o velkém Twitter úlu připraveném se vyrojit v jakoukoliv chvíli. Tvoř smysluplné tweety. Retweetuj obsah ostatních CryptoParty.

- Ujisti se, že šifrování, které na party učíš, by zvládlo pochopit i desetileté dítě. Pak nechaj desetiletého předat své poznatky osmdesátiletému.

- Zvaž hostování soukromých CryptoParty pro aktivisty, žurnalisty a jedince pracující na rizikových místech.

- Neděs ne-technické lidi. Neuč o příkazové řádce předtím, než lidé vědí, jak zapnout své laptopy. Každý se učí vlastním tempem – ujisti se, že je dostatečná podpora pro ty, kdo to potřebují.

- Dělat na CryptoParty skvělé věci nevyžaduje žádné povolení nebo neoficiální konsenzus. Pokud si nejsi jistý zajímavostí toho, co děláš, zeptej se ostatních, co si o tom myslí.

- Zvaž potřebu vyhazovače, zejména pokud tvá CryptoParty čeká víc jak 50 lidí. Neboj

se nechat vyhodit někoho, kdo narušuje zásady proti obtěžování.

- CryptoParty má poskytnout příjemnou zkušenost pro každého, bez obtěžování kvůli pohlaví, sexuální orientaci, invaliditě, fyzickému vzhledu, rodokmenu nebo vyznání. Pokud se chováš jako pitomec, může to způsobit, že nebudeš zván na CryptoParty. Obtěžování obnáší:

    * urážlivé či ofenzivní komentáře
    * úmyslné zastrašování
    * přímé či nepřímé výhružky
    * stalking
    * nevhodný fyzický kontakt
    * nevítaný sexuální zájem

- Povzbuzuj kulturu sdílení. Povzbuzuj pokročilé uživatele, aby pomáhali těm méně pokročilým. Deleguj.

- Využívej pro online schůzky platformy jako mumble (např. místnost #cryptoparty na http://occupytalk.org/), pokud nejsou osobní setkání možná nebo praktická.

- Kopíruj z ostatních CryptoParty. Remixuj, používej znovu a sdílej. Vytvoř sklad starých zařízení, která jsou lidé ochotni věnovat těm, kdo je ocení.

- Rozšiřuj informace! Vytiskni plakáty a letáky a rozdávej je ve svém okolí, nahraj online verze na sociální sítě a pošli je svým přátelům.

- Nezaprodávej se sponzorům za pizzu a pivo. Vyzvi lidi, aby se pokusili přinést erární jídlo a pití. Hostuj CryptoPikniky tak často, jak je to možné. Spřátel se s knihovníky,

kteří drží klíče k lokálním veřejným místnostem, které mohou být k využití zdarma.

- Přizvi všechny možné lidi. Přiveď účastníky s širokým záběrem dovedností a zájmů – hudebníky, politické učence, aktivisty, hackery, programátory, novináře, umělce a filosofy. Šiř lásku.

- Přizvi grafické designéry a ilustrátory, kteří se mohou podílet na zhotovení materiálů, které lidem umožní lépe pochopit šifrování.

- Přizvi každého, aby sdílel své znalosti a zkušenosti. Jedinci s malými či žádnými kódovacími, programovacími, hackovacími či šifrovacími dovednostmi mohou změnit kulturu tím, že budou propagovat ideu soukromí jako základního práva.

- Bav se! Sdílej hudbu, pivo a chipsy. Spřízni se s ostatními přes instalaci GPG, Truecrypt, OTR a Tor, stejně jako skrze společný poslech hudby nebo sledování filmů. Doporučujeme filmy jako Hackers, The Matrix, Bladerunner, Tron, Wargames, Sneakers a The Net.

PROČ NA SOUKROMÍ ZÁLEŽÍ

Soukromí je fundamentáním lidským právem uznaným mnoha zeměmi jako zásadní součást individuální lidské důstojnosti a sociálních hodnot, obdobně jako svoboda sdružování a svoboda projevu. Jednoduše řečeno je soukromí hranice, kterou vyznačujeme, jak dalece může společnost zasahovat do našich osobních životů.

Jednotlivé státy se v definicích soukromí liší. Například ve Spojeném království mohou být zákony o soukromí dohledány až do 14. století, kdy anglický král vytvořil zákony na ochranu lidí před odposloucháváním a šmírováním. Tyto regulace odkazovaly na narušení osobního komfortu a ani král nesměl vstoupit do sedlákova příbytku bez jeho svolení. Z tohoto pohledu je soukromí definováno v podmínkách osobního prostoru a soukromého majetku. V roce 1880 američtí právníci Samuel Warren a Louis Brandeis popsali soukromí jako 'právo být sám'. V tomto případě je soukromí synonymem pojmů samoty a nároku na soukromý život. V roce 1948 Všeobecná deklarace lidských práv specifikovala ochranu teritoriálního a komunikačního soukromí, která se později stala součástí ústav po celém světě. Evropská komise pro lidská práva a Evropský soudní dvůr pro lidská práva v roce 1978 rovněž poznamenaly, že soukromí zahrnuje navazování mezilidských vztahů a rozvíjí emocionální zdraví.

Dnes jsou se vzrůstající tendencí jako další aspekt soukromí vnímána osobní data, která poskytujeme organizacím, ať už online nebo offline. Způsob, jakým jsou naše údaje používány tak rozvíjí debatu o zákonech, které řídí naše chování a společnost. To má za následek lavinový efekt na veřejné služby, které využíváme, a byznys, se kterým interagujeme. Má to dokonce efekt i na to, jak definujeme sami sebe. Pokud je soukromí o hranici, kterou řídíme povolení k našemu sledování a dohledávání, pak je množství a typ shromážděných, šířených a zpracovaných osobních informací tím nejpodstatnějším pro naše základní občanská práva.

Často slyšený argument v otázkách soukromí a anonymity přichází s větami jako "Dělám

pouze nudné věci. Nikdo by se o to stejně nezajímal." nebo "Nemám co skrývat.". Oba tyto výroky jsou však snadno zpochybnitelné.

Zaprvé spousta společností se velmi podrobně zajímá o všechny ty nudné věci, které děláš, protože pak mají příležitost ti nabídnout své produkty, které zapadají do tvých potřeb. Tímto způsobem se jejich nabídky stávají mnohem více efektivními – jsou schopny přesně se přizpůsobit tvým potřebám a touhám. Zadruhé máš hodně co skrývat. Možná to přesně nevyjadřuješ ve zprávách svým přátelům a kolegům, ale procházení Internetu – pokud není chráněno technikami popsanými v této knize – o tobě poví mnoho věcí, které by sis raději ponechal jen pro sebe: bývalý partner, kterého hledáš na Googlu, nemoci, které zkoumáš, nebo filmy, které sleduješ, jsou jen pár příkladů.

Další ke zvážení je možnost, že sice nemáš co skrývat teď, ale může se ti to snadno přihodit v budoucnu. Dát dohromady všechny nástroje a dovednosti, jak se vyhnout dozoru, vyžaduje praxi, důvěru a trochu úsilí. Toho nemusíš dosáhnout ve chvíli, kdy to nejvíce potřebuješ, a to nemusí jít o obdobu špionážního filmu. Například posedlý a odhodlaný stalker ti může snadno narušit tvůj život. Čím více následuješ doporučení v této knize, tím menší dopad na tebe takové útoky budou mít. Rozšiřování počítačové sítě umožňuje společnostem tě také sledovat a nacházet více a více možností, jak dosáhnout na tvůj každodenní život.

Koneckonců, nedostatek anonymity a soukromí neovlivňuje pouze tebe, ale i všechny okolo tebe. Pokud třetí strana, jako tvůj poskytovatel Internetu, čte tvé e-maily, je to narušení soukromí všech tvých kontaktů. Tento problém působí ještě dramatičtěji, když se podíváš na problémy spojené se sociálními sítěmi jako Facebook. Běžně se stává, že někdo nahraje a otaguje fotky bez vědomí nebo svolení těch, kteří se na nich nacházejí.

Protože podporujeme tvé právo být politicky aktivní, abys mohl hájit své právo na soukromí, sepsali jsme tuto knihu, abychom podpořili ty, kteří cítí, že udržování soukromí na Internetu je též osobní zodpovědností. Doufáme, že následující kapitoly ti pomohou získat kontrolu nad tím, kolik toho o tobě ostatní vědí. Každý z nás má právo na soukromý život, právo objevovat,

brouzdat a komunikovat s těmi, se kterými si přeje komunikovat, beze ze strachu z žití pod dohledem zvědavých očí.

O TÉTO KNIZE

Příručka CryptoParty se zrodila po návrhu Marty Peirano a Adama Hydea po první berlínské CryptoParty 29. srpna 2012. Julian Oliver a Danja Vasiliev, spolupořadatelé berlínské CryptoParty, byli touto myšlenkou nadchnuti, protože viděli potřebu praktické příručky s nízkou vstupní bariérou pro následující party. Asher Wolf, zakladatelka hnutí CryptoParty, byla přizvána k práci a projekt byl na světě.

Tato kniha byla napsána první tři říjnové dny ve studiu Weise7 v Berlíně, v obležení dobrého jídla, pochybného vína a malého oceánu kávy uprostřed ohromného kabelového hada. Přibližně dvacet lidí bylo zapojeno do tvorby tohoto díla, někteří více než jiní, někteří místní a někteří zdaleka.

Book Sprint ('knižní sprint' – pozn. překl.), systém práce využitý pro sepisování, zdůrazňuje minimalizování všech překážek k expertíze, psaní stránek a slouží k osobní diskuzi a dynamickému přidělování úkolů. Stejně jako samotná CryptoParty. Publikační platforma Booktype byla vybrána pro editaci zadání, relativně snadno umožňující tento chapadlovitý styl paralelní spolupráce. Asher také založila několik TitanPadů pro hromadnou tvorbu kapitol Manifest CryptoParty a Jak na CryptoParty. Vše zmíněné se 3. října stalo oficiální Příručkou CryptoParty.

Projekt CryptoParty Handbook můžeš najít i na githubu:

https://github.com/cryptoparty/handbook

Book Sprint trval tři dny, následuje úplný seznam přítomných tvůrců:

Adam Hyde (koordinátor), Marta Peirano, Julian Oliver, Danja Vasiliev, Asher Wolf, Jan Gerber, Malte Dik, Brian Newbold, Brandan Howell, AT, Carola Hesse, Chris Pinchen s

ilustracemi Emile Denichaud.

Titulky Příručky CryptoParty

Koordinace:

Adam Hyde

Tým:

Marta Peirano

Asher Wolf

Julian Oliver

Danja Vasiliev

Malte Dik

Jan Gerber

Brian Newbold

Asistence:

Brendan Howell

Teresa Dillon

AT

Carola Hesse

Chris Pinchen

'LiamO'

'13lackEyedAngels'

'Story89'

Travis Tueffel

Obálka:

Emile Denichaud

Další obsažený materiál:

https://en.flossmanuals.net/bypassing-censorship/

Návody použité v první polovině této knihy čerpají ze dvou knih sepsaných FLOSS Manuals:

How to Bypass Internet Censorship, 2008 & 2010

Adam Hyde (koordinátor), Alice Miller, Edward Cherlin, Freerk Ohling, Janet Swisher, Niels Elgaard Larsen, Sam Tennyson, Seth Schoen, Tomas Krag, Tom Boyle, Nart Villeneuve, Ronald Deibert, Zorrino Zorrinno, Austin Martin, Ben Weissmann, Ariel Viera, Niels Elgaard Larsen, Steven Murdoch, Ross Anderson, helen varley jamieson, Roberto Rastapopoulos, Karen Reilly, Erinn Clark, Samuel L. Tennyson, A Ravi

Basic Internet Security, 2011

Adam Hyde (koordinátor), Jan Gerber, Dan Hassan, Erik Stein, Sacha van Geffen, Mart van Santen, Lonneke van der Velden, Emile den Tex and Douwe Schmidt

ČÁST DRUHÁ: E-MAIL

TYPY MAILU

Typy mailu jsou v zásadě dva:

1. Mail čtený, psaný a odeslaný z prohlížeče (webmail)
2. Mail čtený, psaný a odeslaný v mailovém programu, jako např. Mozilla Thuderbird, Mail.App či Outlook Express.

E-MAIL HOSTOVANÝ NA VZDÁLENÉM SERVERU (WEBMAIL), UŽÍVANÝ PROSTŘEDNICTVÍM PROHLÍŽEČE

E-mail odeslaný a doručený přes prohlížeč, někdy nazývaný webmail, většinou předpokládá účet na vzdáleném serveru, jako je Google (Gmail), Microsoft (Hotmail) nebo Yahoo (Yahoo Mail). Hostování e-mailu otevírá mnoho možností pro obchod: propojení s jinými službami nabízenými tou kterou společností, vystavení značky a hlavně vytěžení tvého e-mailu pro vzorce, které mohou být užity pro zhodnocení tvých zájmů – velmi podstatná věc pro reklamní byznys (o vládě nemluvě).

Protože e-mail sídlí na serveru, je tu základní riziko jeho ztráty – útočník, který získal přístup k účtu, jej může smazat, či je útokem zrušena celá služba.

E-MAIL HOSTOVANÝ NA VZDÁLENÉM SERVERU, UŽIVANÝ PROSTŘEDNICTVÍM E-MAILOVÉHO KLIENTU NEBO PROHLÍŽEČE

Mail napsaný a odeslaný v programu je např. Outlook, Thunderbird, Mail.App může být také použit ve webmailové službě, jako je Gmail či e-mail tvého zaměstnavatele. V každém případě i ve chvíli, kdy si mail stáhneš do počítače, stále zůstává na serveru (např. Gmail). Tvůj e-mail tak nezávisí na prohlížeči, ovšem stále užíváš služeb, jako je Gmail nebo Hotmail.

Rozdíl mezi uložením mailu na tvém počítači v mailovém klientu a mezi uložením na vzdáleném mailovém serveru (Hotmail, Gmail či server vaší university) může být nejprve trochu matoucí, nicméně přináší s sebou jisté výhody.

Společné užívání webmailu a mailového klientu obvykle přináší svobodnou možnost přihlášení se z jakéhokoliv počítače připojeného k internetu (dobré pro cestovatele), ale také možnost zálohování na tvém vlastním stroji – přibližuje se to tzv. data redundancy. Mít uloženy maily u sebe i na vzdáleném serveru je rozhodně doporučováno pro maily s citlivým obsahem. A hlavně v mailovém klientu je možnost šifrování (více v části Šifrování e-mailu) a tím zamezení nepovolaným osobám ve čtení tvé pošty. Pokud užíváš pouze webmail, není šifrování zase tak snadné.

Pokud e-maily zároveň stahuješ klientem i čteš v prohlížeči, je důrazně doporučeno zašifrovat si disk (viz Šifrování disku). Pokud ti počítač někdo ukradne či zadrží, nikdo jej nebude moci číst.

E-MAIL UŽÍVANÝ V E-MAILOVÉM KLIENTU BEZ UKLÁDÁNÍ NA VZDÁLENÉM SERVERU

Mail může být odesílán serveru, ale neukládán na něm, toliko vypálen do místa určení jakmile e-mail dorazí na doručovací server. Google a Microsoft toto nastavení nepodporují, ale tvůj zaměstnavatel či tvá škola by to nabízet mohli. Měj na paměti, že v tomto případě stále existuje ještě nesporné riziko: systémový administrátor má stále přístup do tvého mailu ve chvíli, kdy dorazí na server či jej opouští.

KONTEXTOVÉ ÚVAHY

Můžeš být sám sobě serverovým administrátorem a mít vlastní mailovou službu. Můžeš mít e-mail ukládaný na serveru svého zaměstnavatele. Nebo můžeš používat služby korporací, jako je Google (Gmail) nebo Microsoft (Hotmail). Užívání všech vede k úvahám, které ústí v základní fakt – pokud není e-mail samotný zašifrovaný, admistrátor si stále může udělat tajně kopii ve chvíli, kdy mail dorazí na server. Nezáleží na tom, že používáš bezpečné přihlášení TLS/SSL ve chvíli, kdy se do mailu přihlašuješ a čteš ho, toto zabezpečuje pouze připojení mezi tvým strojem a samotným serverem. Proto nikdy nenechávej e-mail s citlivými informacemi nezašifrovaný, natož ve chvíli kdy užíváš službu, která nemá tvou plnou důvěru.

Zaměstnavatel/Organizace

Tvůj zaměstnavatel či organizace, se kterou spolupracuješ, se nacházejí ve velmi dobré pozici – ve chvíli, kdy mají tvou důvěru, mohou číst tvé maily uložené na jejich serveru, ve snaze zjistit o tobě co nejvíc – tvé motivace, zájmy, program. Případy špehování zaměstnanců zaměstnavatelem jsou tak běžné, že jsou považovány za takřka samozřejmost. Vaše jediná obrana spočívá v šifrování mailů, např. způsobem zvaným GPG (viz Šifrování e-mailu).

Vlastní e-mailový server

Ideální hosting, avšak vyžaduje vyšší úroveň technických znalostí. Zde už je pouze na tobě, jak si zabezpečíš mail proti útokům (špatná hesla, žádné SSL), vše jde na tvou odpovědnost a možné pokušení číst maily těm, kterým tuto službu sám poskytuješ.

'Freemailové' služby

Jak bylo zmíněno výše, nebezpečí v užívání mailu poskytovaném korporacemi bývá vyšší ve chvíli, kdy není občanským právem zabezpečeno tvé soukromí. U společností hostující tvé milostné dopisy či deníkové zápisy vždy hrozí, že podlehnou ekonomickému, politickému či právnímu tlaku státu, kterému právně podléhají. Například malajský uživatel Gmailu riskuje odhalení svých zájmů a záměrů vládě, kterou nevolil, nemluvě o obchodních partnerech Google, kteří vždy hledají možnost rozšíření jejich tržního záběru.

Neziskové organizace hostující e-mail

Různé neziskové weby nabízejí freemailové účty organizacím, které jsou také neziskové či filantropické. Některé z nich nabízejí i wiki, mailingové listy, chaty a sociální sítě. Ke zvážení pro organizace pracující na poli polilitickém mohou být rozdíly v zájmech států, kde je e-mail hostován, a v politické zainteresovanosti organizace užívající tuto službu. Tata rizika bývají v ideálním případě zmíněna ve Smluvním ujednání.

Přeposílání mailů

Služba přeposílání mailů poskytuje velké pohodlí pro 'napojení' jednoho e-mailového účtu na druhý. Nejčastěji v případě, kdy je majitel účtu na dovolené a je mu z pracovního mailu, který je jinde než v zaměstnání nedostupný, přeposílána pošta na účet jiný. Rizika přeposílání jsou stejná jako u mailů hostovaných na vzdálených serverech typu Gmail, například mohou být kopírovány a uloženy třetí stranou. Je zde možnost šifrování mailů jako např. GPG (část Šifrování mailů), která zajistí, že i když bude mail zkopírován a uložen, třetí strane si jej nepřečte.

ZÁKLADNÍ TIPY

Stejně jako u jiných způsobů webové komunikace i zde je dobré pro co nejlepší zabezpečení vzít v potaz jistá základní opatření.

VE ZKRATCE:

- Hesla by neměla obsahovat osobní informace a měla by se skládat ze směsi nejméně osmi písmen a dalších znaků.
- Čteš-li e-maily na počítači, který je k Internetu připojen přes wifi (zejména v internetových kavárnách), vždy se ujisti, že připojení je zabezpečeno.
- Dočasně uložené soubory soubory (např. 'cache' a historie) v počítači, na kterém čteš maily, představují jisté nebezpečí. Často je maž.
- Vytvoř si oddělené e-mailové účty, specifický mail pro specifický účel.
- Zašifruj všechno, co bys nechtěl napsat na pohlednici.
- Buď si vědom rizik, které přináší mail hostovaný u tvého zaměstnavatele či organizace.

HESLA

Hesla jsou primární bod zranitelnosti mailové komunikace. I silné heslo může být přečteno, není-li připojení zabezpečeno. Jen proto, že je heslo dlouhé, neznamená, že jej nemůže uhodnout člověk, který tě zná a je schopen uhodnout tvá oblíbená slova a čísla.

Hlavní pravidlo pro vytváření hesel je, že by měla být dlouhá (osm a více znaků) a obsahovat směs písmen a ostatních znaků (čísla a symboly, což znamená, že vám stačí vybrat krátkou sentenci). Kombinace tvých narozenin a příjmení je krásná ukázka toho, jak hesla netvořit. Tyto informace se dají snadno získat i ze zcela veřejných zdrojů. Populární trik je postavit

heslo na oblíbené frázi a pak do ní rozhodit pár čísel. Nejlepší je užít generátor hesel, ať už na tvém počítači či online.

Často je obtížné si hesla zapamatovat a tím se nám otevírá druhý slabý bod – fyzické přečtení. Není lepšího řešení, než ukládat hesla pouze ve vlastním mozku, avšak služby, jako je OnlinePasswordGenerator (http://www.onlinepasswordgenerator.com/), nabízejí kompromis v náhodně generovaných heslech, která nejasně připomínají slova a umožňují si z nich vybrat.

Když se rozhodneš mít heslo uloženo i jinde, než ve své hlavě, můžeš si vybrat mezi prostým poznamenáním si na papír nebo do souboru, nebo užitím keychain software. Toto je poměrně rizikové rozhodnutí, zejména ve chvíli, kdy máš heslo uloženo na stejném zařízení, ze kterého se přihlašuješ do e-mailu (počítač, telefon).

Keaychain software, jako je třeba Keepass, slučuje různá hesla a passfráze na jedno místo a umožňuje k nim přístup přes hlavní heslo či passfrázi. Toto ovšem pokládá velký tlak na hlavní heslo. Když už se rozhodneš keychain software využívat, vyber si rozhodně bezpečné heslo.

Můžeš se též rozhodnout používat rozdílná hesla pro rozdílné účty. V takovém případě, je-li jeden z účtů napaden, ostatní jsou v bezpečí. Nikdy nepoužívej stejné heslo pro osobní a pracovní e-mail. Více v části Hesla, kde se naučíš, jak se lépe zabezpečit.

ČTENÍ MAILU NA VEŘEJNÝCH MÍSTECH

Jedna z velkých výhod bezdrátového připojení a 'cloud computingu' je možnost pracovat odkudkoliv. Často chceš prohlížet mail v internetové kavárně či na jiném veřejném místě. Špehové, zločinci a zlomyslní lidé to dobře vědí a navštěvují tato místa, aby kradli ID, slídili v mailech a prolamovali se do bankovních účtů.

Často se zde podceňuje nebezpečí, že někdo sleduje tvou komunikaci pomocí network packet sniffing. Nesejde na tom, jestli je síť otevřená nebo chráněná heslem, když se někdo připojí na tu stejnou šifrovanou síť, může snadno získat a přečíst všechna nezabezpečená (viz kapitola Zabezpečené připojení) spojení od všech ostatních uživatelů na stejné síti. Klíče k síti wifi se dá nabýt za cenu šálku kávy a dává tomu, kdo umí zachytit a číst síťové pakety, slušnou šanci na přečtení tvého hesla ve chvíli, kdy kontroluješ e-mail.

Vždy proto aplikuj toto jednoduché základní pravidlo: když kavárna nabízí kabelové připojení, využij ho! A stejně jako u bankomatu se ujisti, že ti nikdo nekouká pod prsty v momentě, kdy píšeš své heslo.

CHYTRÉ ZACHÁZENÍ S CACHE

Cesta do pekel je opět dlážděna dobrými úmysly. Rozčiluje-li tě neustálé psaní hesel, můžeš v prohlížeči či mailovém klientu nastavit možnost uložení hesla. Samo o sobě to není špatné, ale ve chvíli, kdy ti někdo odcizí laptop nebo mobil, umožňuje to zloději dostat se ke tvému e-mailovému účtu. Nejlepší je proto mazat cache pokaždé, když zavíráš prohlížeč. Všechny nejpoužívanější prohlížeče tuto možnostz nabízejí.

Jedno základní opatření ti však umožní užívat si pohodlí cache – šifrování disku. Když je ti laptop zcizen a zloděj ho spustí, setká se s zašifrovaným diskem. Také je moudré mít instalován na počítači nebo telefonu screen lock. I ve chvíli, kdy je ti stroj zcizen ve stavu zapnutí, není možné se do něj dostat.

ZABEZPEČENÍ KOMUNIKACE

Kdykoli píšeš a posíláš mail, ať už v prohlížeči nebo mailovém klientu, vždy se ujisti, že je celá relace zabezpečena. Dá se to snadno zajistit přes TLS/SSL (Secure Socket Layer)

připojení mailových serverů.

Užíváš-li pro přístup do mailu prohlížeč, zjisti jednoduše, zdali server podporuje SSL relace – odhalí to 'https://' na začátku URL adresy. Není-li tam, zapni si ho v nastavení svého mailu. Toto zajistí, že není zabezpečeno jen tvé připojování, ale i psaní a odesílání zpráv.

V tomto momentě Gmail používá TLS/SSL jako výchozí, kdežto např. Hotmail ne. Když tvůj účet neumožňuje TLS/SSL, je doporučeno jej opustit. I ve chvíli, kdy své maily pokládáš za nedůležité, jednoho dne se můžeš dočkat zamezení přístupu k nim, protože ti někdo změní heslo.

Když užíváš mailový klient, ujisti se, že je TLS/SSL zapnuto v jeho nastavení. Například v Mozilla Thunderbird to pro odesílané zprávy najdeš v Nástroje → Nastavení účt → Odchozí server (SMTP) a pro zprávy příchozí v Nástroje → Nastavení účtu → Nastavení serveru. Tak zajistíš, že odesílání i doručení mailu je šifrováno a každému, ať už je na tvé síti či na nějaké mezi tebou a serverem, velmi ztíží číst tvé přihlašovací údaje či tvou komunikaci.

ŠIFROVÁNÍ SAMOTNÉHO MAILU

I když máš přes SSL zabezpečeno samotné přípojení, stále má poskytovatel plný přístup do tvé schránky. Když chceš užívat webmail a být si jistý, že poskytoval nebude tvou poštu číst, potřebuješ něco jako GPG, což ti umožní maily šifrovat. V hlavičce mailu však stále zůstává tvá internetová IP adresa, která prozrazuje, odkud byl mail odeslán, stejně jako i jiné kompromitující informace.

Hodí se poznamenat, že užívání GPG ve webmailu je mnohem méně pohodlné než jeho užití v klientu jako Thunderbird nebo Outlook Express.

ODDĚLENÍ ÚČTŮ

Pro výhody služeb jako Gmail je čím dál častější, že lidé mají jen jediný mailový účet. To pochopitelně značně centralizuje potenciální škody způsobené zpronevěřeným účtem. Co víc, není nic, co by bránilo rozladěnému zaměstnanci Google smazat či ukrást tvou poštu, případně může být samotný Google hacknut, jak už se několikrát stalo.

Praktická strategie je mít svůj soukromý mail opravdu soukromý. Když máš pracovní e-mail, vytvoř si nový účet, neudělalal-li to pro tebe zaměstnavatel. Stejně tak učiň v případě organizací či klubů, kde jsi členem, a ke každému účtu měj zvláštní heslo. Nejenže to snižuje riziko zcizení identity, ale navíc to skvěle redukuje možnost, že se ti celá schránka zahltí spamem.

POZNÁMKA K MAILOVÉMU HOSTINGU

Ti, kteří ti poskytují schránku na svém serveru, kde čteš, posíláš a stahuješ zprávy, nejsou zatěžování TLS/SSL. Mohou číst tvůj e-mail i přihlašovací údaje jako prostý text. Je-li na nich právníky požadován přístup do vaší schránky, mohou ho vydat. Mohou studovat tvůj e-mail a hledat vzorce, klíčová slova či oblibu/neoblibu různých značek, ideologií či politických skupin. Je velmi důležité číst EULA (smluvní ujednání koncového uživatele) poskytovatele tvého e-mailu a trochu si je proklepnout ještě předtím, než si u nich založíš schránku. Toto by tě mělo zajímat i u poskytovatele příjemce tvých zpráv.

OBAVY

Kdo všechno může číst maily, které jsem poslal i dostal?

Kdo všechno může číst maily, když cestují přes Internet?

Mohou je lidé, kterým je posílám, sdílet s kýmkoliv?

Maily, které jsou posílány bez jakéhokoliv šifrování (což znamená většina mailů) mohou být čteny, protokolovány a indexovány na jakémkoliv serveru nebo routeru, kterým projdou při cestě od odesílatele k příjemci. I za předpokladu, že používáš šifrované připojení mezi svým strojem a e-mailovou službou, to prakticky znamená, že následující lidé stále mohou číst jakoukoliv zprávu, kterou jsi obrželi či poslali:

1. Ty
2. Tvůj e-mailový poskytovatel
3. Operátoři a vlastníci každého mezisíťového připojení (často nejednoznačné nadnárodní konglomeráty či suverénní státy)
4. Poskytovatel e-mailu příjemce
5. Předpokládaný příjemce

Mnoho poskytovatelů webmailu automaticky prověřuje všechny poslané a přijaté zprávy, aby mohli lépe cílit reklamu. Zatímco pro některé uživatele to může být rozumný kompromis (freemail), pro mnohé jiné je znepokující, že je jejich soukromá korespondence zkoumána a indexována jako část skrytého a potenciálně velmi odhalujícího profilu, drženého mocným korporátním obrem.

Někdo také může na osoby popsané výše zatlačit s následujícími žádostmi:

1. Protokolovat e-mailová metadata (seznam zpráv poslaných či doručených každému uživateli, předmět, příjemci), v některých jurisdikcích i bez povolení.

2. Zprávy odeslané a doručené jistým uživatelem či skupinou, v některých juridikcích s povolením či soudním příkazem.

3. Odčerpávat všechny zprávy a datové toky k mimostránkové analyzaci a indexaci v určeném připojení.

V případech, kdy má uživatel obchodní nebo služební vztah s e-mailovým poskytovatelem, některé vlády chrání právo na soukromí uživatele proti neautorizovanému a nevyžádanému čtení či sdílení zpráv, ale často sama vláda hledá informace a často uživatelé souhlasí se vzdáním se části svých práv v smluvním ujednání. Je-li poskytovatel mailu uživatelův zaměstnavatel či akademická instituce, často může na právo na soukromí zapomenout. Záleží na soudní praxi, firmy však často mají zákonné právo číst všechny doručené i odeslané zprávy svých zaměstnanců, pokud byly odeslány či čteny na jejich firemních účtech a počítačích, včetně soukromých zpráv odeslaných po pracovní době či během dovolené.

Možná je načase opustit textové maily, neboť cena a námaha uchovávání a indexování rostoucího počtu zpráv je příliš vysoká: už tak bylo dost těžké jen zprávy spolehlivě doručit. To je důvod, proč mnoho e-mailových systémů neobsahuje mechanismy k ochraně soukromí obsahu zpráv. Cena monitoringu klesá rychleji než velikost internetového spojení a je rozumné očekávat široce zaměřené sledování a indexování všech zpráv (ať už na straně odesílatele či příjemce), i těch nejvíce nevinných.

Více o právní ochraně mailových zpráv 'v odpočinku' (technický termín pro zprávy uložené na serveru poté, co byly doručeny), speciálně o přístupu vlády k vašim zprávám:

https://ssd.eff.org/3rdparties/govt/stronger-protection (USA)

http://en.wikipedia.org/wiki/Data_Protection_Directive (EU)

Samozřejmě je nutné dbát i na to, že existují jisté fotografie, dopisy a dokumenty, které bys nikdy neměl dávat jen tak bezstarostně na Internet, protože nechceš, aby byly náhodně zaindexovány a objevily se ve výsledcích vyhledávání, a nikdy bys neměl bezstarostně posílat mailové zprávy, když nechceš, aby k nim měl snadný přístup tvůj zaměstnavatel či nabručený úředník.

NAHODILÉ ZNEUŽITÍ A KRÁDEŽE PROVÁDĚNÉ HACKERY

Co když někdo získá úplnou kontrolu nad mým e-mailovým účtem?

Přihlásil jsem se z nezabezpečeného místa... jak poznám, že mi byl hacknut účet?

Nedělám nic špatného... proč bych se měl skrývat?

Proč by se o mě někdo zajímal?

Naneštěstí, je zde mnoho praktických, společenských a ekonomických pohnutek zákeřných hackerů, kteří se chtějí vloupat do náhodných účtů na Internetu. Nejobvyklejší je krádež peněz nebo identity – útočník se snaží dostat čísla kreditních karet, nakupovat site credentials nebo bankovní informace kvůli krádeži peněz. Hacker nemá možnost zjistit, který uživatel bude lepší cíl, tak se prostě snaží vlámat do všech účtů a to i v případě, že uživatel nemá nic k ukradení nebo je opatrný v informacích, které o sobě poskytuje.

Méně obvyklé jsou útoky sloužící k získání validních a důvěryhodných účtů k získání kontaktních e-mailových adres a následné masové distribuci spamu nebo k získání přístupu k důvěrným službám spjatým s e-mailovým účtem, nebo jej užít jako odrazový můstek v sofistikovaných, sociálně inženýrských útocích. Například ve chvíli, kdy hacker získá přístup ke tvému účtu, může okamžitě pod tvým jménem rozeslat zprávy tvým známým či spolupracovníkům a vyžadovat pohotovostní přístup k lépe zabezpečeným systémům.

Finální neočekávaný problém, vyvstávající špatně zabezpečným uživatelům, je masové hacknutí účtů velkých poskytovatelů, kdy hackeři získají přístup do hostingové infrastruktury,

extrahují hesla a soukromé informace ve velkém a posléze je prodají nebo zveřejní seznamy přihlašovacích informací na online černém trhu.

CÍLENÉ ZNEUŽITÍ, OBTĚŽOVÁNÍ A ŠPEHOVÁNÍ

Napsal jsem něco, co rozčílilo někoho mocného... jak se mám chránit?

Když zjistíš, že jsi cíl mocné organizace, vlády nebo soukromých, avšak odhodlaných osob, aplikuj stejné techniky a principy jak udržet svůj e-mail bezpečný a stále soukromý, ale speciální péči věnuj ochraně před hackery, kteří mohou užívat promyšlené techniky k narušení tvých přístrojů a účtů. Když hacker získá kontrolu nad tvým zařízením nebo přístup do jakéhokoliv tvého e-mailového účtu, velmi rychle se mu podaří dostat se do veškeré korespondence i externích služeb, které máš s e-mailem propojené.

Snaha ochránit se před útoky snadno vyeskaluje v pravou bitvu vůle a zdrojů, ale pár základních návodů pomůže k delšímu udržení pozic. Používej specifická zařízení pro specifickou komunikaci a užívej je pro ten jeden konkrétní účel. Odhlaš se a vypni svá zařízení ihned, jakmile na nich skončíš práci. Používejte open source šifrovací nástroje, prohlížeče a operační systémy a hlídej si updaty oprav děr v zabezpečení.

Neotevírej PDF soubory pomocí Adobe Readeru nebo jiných zákonem chráněných PDF readerů. Non-open source PDF readery bývají používány ke spuštění škodlivých kódů vložených do PDF souboru. Když obdržíš .pdf jako přílohu, nejdříve zvaž, jestli znáš případného odesílatele a zda od něj očekáváš nějaký dokument. Poté můžeš užít PDF readery, v nichž byly testovány známá slabá místa a nelze v nich spustit kódy java scriptem.

Linux: Evince, Sumatra PDF

OS X: Preview

Windows: Evince

Používej krátkodobé účty ve stylu 'použít a zahodit' s náhodně generovanými hesly všude, kde je to jen trochu možné.

POTÍŽE SE ŠIFROVÁNÍM

Co se stane, když ztratím své 'klíče'? Přijdu o svůj e-mail?

Pečlivé GPG šifrování mailů není bez potíží.

Když budeš mít uložené starší maily šifrované a přijdeš o všechny kopie soukromého klíče, bude dokonale nemožné, abys četl svůj archiv a když nebudeš mít kopii svého revokačního certifikátu pro soukromý klíč, bude též obtížné prokázat, že nově vygenerovaný klíč je validní, minimálně do doby, než původní soukromé klíče expirují.

Pokud podepíšeš zprávu svým soukromým klíčem, budeš mít velký problém dokázat, že jsi nic nepodepsal ve chvíli, kdy příjemce zveřejní zprávu či jen podpis. Termín pro něco takového je ne-neuznání: každá zpráva, kterou jsi kdy poslal podepsanou, může být použita jako důkaz u soudu. To znamená, že když je tvůj soukromý klíč zkompromitován, může být užit ke čtení všech šifrovaných zpráv. Zprávy mohou být v bezpečí, když jsou na cestě, a ve chvíli, kdy jsou doručeny, ale všechny kopie jsou ohrožením a hazardem, zda bude nebo nebude soukromý klíč někdy odhalen. I když smažeš každou zprávu ihned po přečtení, každý, kdo vyslídil zprávu na síti si může pořídit kopii a pokusit se ji rozšifrovat později, když se dostane k soukromému klíči.

Řešením je užívat takový protokol zpráv, který poskytuje tzv. Perfect Forward Secrecy generováním nového unikátního kódu pro každou konverzaci nahodile, takže klíč pro žádnou relaci nemůže být znovu vygenerován poté, co byl jednou přečten. OTR chat protokol toto poskytuje (http://en.wikipedia.org/wiki/Perfect_forward_secrecy) v reálném čase instantního

posílání zpráv a SSH protokol jej poskytuje pro remote shell connections, ale zatím neexistuje ekvivalent pro e-mail.

Může být složité vybalancovat pohodlí mobilního přístupu k soukromým klíčům s faktem, že mobilní zařízení bývají mnohem častěji ztracena, ukradena, prozkoumána či zneužita než nepřenosné stroje. Pohotovost nebo nečekaný čas nejvyšší potřeby může být právě ta chvíle, kdy budeš nejvíc ze všeho chtít poslat tajnou zprávu nebo podepsanou zprávu k ověření tvé identity, ale jsou zde také momenty, kdy můžeš snadno skončit bez přístupu ke svým soukromým klíčům, bude-li tvé mobilní zařízení zabaveno či v něm nebudeš mít nahrány všechy své klíče.

ZABEZPEČENÁ PŘIPOJENÍ

KDYŽ ČTU SVŮJ E-MAIL, MOHOU TAK SE MNOU ČINIT I JINÍ LIDÉ?

Jak bylo zmiňováno v kapitole Základní tipy, kdykoliv používáš webmail nebo mailový klient, ujisti se, že používáš šifrování po celou dobu, od přihlášení do odhlášení. Tím zabráníš, aby ti přes poskytovatele někdo slídil v mailu. Naštěstí se tohle dá snadno zvládnout s populární TLS/SSL připojením na serveru.

Pokud tvůj webmail nepovoluje TLS/SSL, zvaž, zdali tento účet raději nezrušit. I kdyby nebyly tvé maily nijak zvlášť soukromé nebo důležité, tvůj účet může být snadno hacknut 'vyčmucháním' hesla! Pokud jen není TLS/SSL zapnuto, ujisti se, že jsi jej zapnul v uživatelském nastavení.

Používáš-li klienta jako Thunderbird, Maill.app nebo Outlook, zkontroluj, zda máš funkční TLS/SSL v nastavení programu.

POZNÁMKA

Je důležité poznamenat, že administrátoři poskytovatelů jako Hotmail nebo Google mohou číst tvůj e-mail i ve chvíli, kdy používáš zabezpečené připojení. To je také bezcenné ve chvíli, kdy Certifikační autority prodají soukromé klíče majitelům webových stránek - někdy mohou skončit v rukou vlády nebo hackerů vytvářejících tak lehčí prostředí pro 'Man In The Middle Attack' v připojení užívající TLS/SSL.

Také zde musíme poznamenat, že Virtual Private Network je také dobrá cesta zabezpečení připojení při odesílání a čtení e-mailu, leč vyžaduje pro připojení k serveru VPN klienta na tvém počítači (viz kapitola VPN v části Procházení Internetu).

ZABEZPEČENÉ E-MAILY

Je možné posílat a dostávat zabezpečné maily při používání standardních obvyklých e-mailových programů – stačí přidat několik add-onů či rozšíření. Esenciální funkce těchto add-onů je (ale už ne pole Komu: Od: CC: a Předmět) nečitelným pro třetí stranu, která zachytává komunikaci či se jinak snaží dostat do tvého mailu. Tomuto procesu se říká šifrování.

Zabezpečit si e-mail můžete užitím techniky nazvané Public-Key Cryptorography. Je to mazaný způsob, který užívá dvou kódovacích klíčů k posílání zpráv. Každý uživatel má veřejný klíč, který může být použit pouze k zašifrování zprávy, avšak již ne k dešifrování. Veřejné klíče můžeš užívat bez starosti, že je uvidí někdo nepovolaný, k ničemu mu totiž nebudou. Soukromé klíče jsou přísně střeženým tajemstvím příjemnce zprávy a jsou užívány k dekódování zprávy, která byla předtím zakódována veřejným klíčem.

V praxi to znamená, že chce-li Alice poslat Bobovi tajnou zprávu, potřebuje jen jeho veřejný klíč, kterým zakóduje text. Po obdržení zprávy Bob použije svůj soukromý klíč k dešifrování zprávy. Chce-li odpovědět, bude potřebovat Alicin veřejný klíč k zašifrování.

JAKÝ SOFTWARE POUŽÍT PRO ZAŠIFROVÁNÍ MAILU?

Nejpopulárnější systém public-key kryptorografie je Gnu Privacy Guard (GPG) k vytvoření a spravování klíčů. Jako add-on je možné ho integrovat do standardního mailového software. Užívání GPG ti dává možnosti zašifrovat citlivý mail a dekódovat příchozí zašifrované maily, ale nenutí tě užívat šifrovaní pokaždé. V minulých letech bylo dost obtížné instalovat a nastavit mailové šifrování, ale poslední vylepšení tento proces relativně zjednodušila.

Užíváš-li webmail a přeješ-li si mít jej zašifrovaný, je to poněkud složitější. Můžeš na svém

počítači pomocí GPG zašifrovat text pomocí svého veřejného klíče, nebo můžeš použít add-on, třeba Lock The Text (http://lockthetext.sourceforge.net/). Pokud však chceš udržet své zprávy v tajnosti, doporučujeme užívat mailového klienta jako například Thunderbird spíše než webmail.

ČÁST TŘETÍ: PROCHÁZENÍ INTERNETU

CO SE DĚJE PŘI PROHLÍŽENÍ?

Prohlížení webu je forma komunikace. Ani nemusíš odesílat moc textu co se týče počtu slov, ale prohlížeč vždy komunikaci iniciuje a udržuje odesíláním požadavků, které se posléze zobrazí jako výsledek na tvé obrazovce.

Prohlížeče jako Mozilla Firefox, Google Chrome, Opera, Safari i Internet Explorer se v tomto ohledu chovají podobně. Když napíšeme URL do adresního řádku, prohlížeč si od vzdáleného serveru vyžádá přístup na stránku (která je jen zvláštním druhem textu). Ta je pak zobrazena v okně prohlížeče v podobě vybarvených bloků, textu a obrázků. Aby sis prohlédl, co samotný prohlížeč vidí, stačí kliknout na záložku View (Zobrazení) a následně vybrat Page Source (Zdrojový kód stránky). Z toho ti vyleze ta samá stránka jen zobrazená v jazyce HTML, případně v kontextu s dalšími zdroji (CSS a JavaScript), které řídí způsob, jakým je obsah zobrazován a jak se chová.

Když se prohlížeč snaží otevřít nějakou stránku (předpokládejme, že v procesu nejsou využity proxy), první věc, kterou udělá, je kontrola vlastní cache. Pokud ve své paměti takovou stránku nenalezne, snaží se přeložit její název do adresy, kterou je schopen použít. Jelikož se jedná o internetový program, potřebuje adresu internetového protokolu (IP adresu). Aby tuto adresu získal, ptá se DNS serveru (něco jako Zlaté stránky pro internetové programy), který je nainstalován na routeru tvého internetového připojení. IP adresa je číselné označení přiřazené ke každému zařízení v (globální) síti, stejně jako adresa domu v poštovním systému. A stejně jako v případě tvé vlastní fyzické adresy bys měl být velmi opatrný, komu tuto adresu dáš při svém prohlížení webu (při výchozím nastavení to znamená komukoliv). Jakmile obdrží IP adresu, otevře prohlížeč TCP (komunikační protokol) spojení se svým cílem

a začne posílat balíčky na port dané adresy, obvykle na port číslo 80 (porty jsou jako serverové dveře, je jich mnoho, ale obvykle jen málo z nich je otevřených), pokud není stanovena jiná cesta. Tyto balíčky cestují na Internetu přes množství serverů, hodně záleží na tom, kde je cílová adresa umístěna. Poté server hledá žádanou stránku a když ji najde, doručí ji skrze HTTP protokol. Spojení lze zabezpečit pomocí TLS/SSL, čímž se zabrání čtení či upravování dat z třetí strany.

Když dorazí HTTP odpověď, prohlížeč může zavřít TCP spojení nebo ho použít pro další požadavky. Odpověď může vypadat různě, od přesměrování po běžný Internal Server Error (500, Vnitřní chyba serveru). Pokud odpověď dorazila dle očekávání a nalezla požadovanou stránku, prohlížeč si ji uloží do mezipaměti pro příští použití, dekóduje ji (rozbalí ji, pokud byla zabalená, renderuje video kodeky, atd.) a zobrazí/přehraje její obsah dle instrukcí.

Ceký proces může být ilustrován jako malý rozhovor mezi prohlížečem (P) a serverm (S):

P: "Ahoj."

S: "Čau!"

P: "Mohu dostat tu stránku s veselými králíčky, prosím?"

S: "Jistě, tady ji máš."

P: "Možná bys mi mohl dát ještě velkou verzi toho malého králíčka, který se mazlí s medvídkem."

S: "Jasně, proč ne."

[...]

P: "To by bylo pro teď vše, díky a měj se."

Měj na paměti, že během TCP/IP výměny dochází k množství paralelních činností. Podle konfigurace tvého nastavení pak může prohlížeč přidat stránku do historie, ukládat cookies, kontrolovat nové pluginy nebo RSS odběry a komunikovat s různými servery – to vše, zatímco ty děláš něco zcela odlišného.

Tvůj místopis: stopy

Je důležité si uvědomit, že po sobě zanecháš stopy. Některé budou přímo na tvém počítači jako souhrn dat z cache, historie prohlížeče a cookies se svou sloní pamětí. To vše může být velmi užitečné; pro zrychlení výkonu tvého prohlížeče, redukování objemu stažených dat nebo zapamatování si hesel a preferencí na sociálních sítí. Zároveň však slouží i pro špehování tvých návyku a sestavování záznamu o tom, kam jdeš a co tam děláš. To by tě mělo obtěžovat, zejména pokud používáš počítač v knihovně, pracuješ v internetové kavárně nebo bydlíš se zvědavým člověkem.

I když nastavíš prohlížeč tak, že si nepamatuje historii, odmítá cookies a promazává soubory v mezipaměti (nebo pro cache přiřadíš 0 MB volného místa), stále za sebou budeš na Internetu trousit drobky. Tvá IP adresa je všude a všemi zaznamenávána a odeslané pakety jsou monitorovány stále rostoucím počtem entit – komerčními, vládními či kriminálními, společně s potenciálními stalkery.

Demokratické vlády po celém světě se snaží předělat regulace tak, aby mohly po poskytovatelích Internetu vyžadovat kopii všeho, čímž by pak měly zpětně přístup k čemukoliv, co by je zajímalo. Sekce 215 American PATRIOTact říká, že 'je zakázáno sdělit jakémukoliv jedinci či organizaci, že jeho záznamy byly v rámci vyšetřování poskytnuty

federální vládě'. To znamená, že společnost, které každý měsíc jako zákazník platíš za přístup k Internetu, může dostat příkaz k vydání všech tvých záznamů o prohlížení včetně mailových služeb, aniž bys o tom byl zpraven.

Většinou však praktikovaný dohled nepůsobí jako v 1984. Google shromažďuje výsledky tvého vyhledávání, identifikátor tvého prohlížeče, tvou IP adresu a další hromadu dat, která mohou vést ke tvým dveřím, nicméně záměr bývá obvykle spíše tržní než politický. Inzerenti už nedělají povyk kvůli reklamním plochám, dnes o tobě chtějí všechno znát. Chtějí znát tvé stravovací a zdravotní návyky, počet tvých dětí a kam je bereš na prázdniny, jak si vyděláváš, kolik našetříš a kolik bys byl ochoten utratit. Co víc: chtějí znát, jaký vztah k věcem pociťuješ. Chtějí vědět, jestli tví přátele uznávají tyto pocity, takže bys je případně mohl přesvědčit ke změně jejich konzumních návyků. To není žádná konspirace, jedná se spíše o povahu kapitalismu v informačním věku. Abychom parafrázovali známé pozorování současné situace, dá se říct, že nejlepší mozky naší generace přemýšlí nad tím, jak přinutit ostatní kliknout na reklamu.

Někteří lidé si myslí, že reklamy mohou být ignorovány, nebo že inzeráty zaměřené přesně na jejich specifické potřeby jsou vlastně vítěznou situací, protože alespoň jsou spamováni něčím, o co by nakonec mohli mít zájem. I kdyby to byl náš případ, měli bychom důvěřovat Google a svěřovat mu tak intimní detaily o našich životech? I kdybychom Google věřili, že "nečiní zlo" (motto společnosti – pozn. překl.), může být koupen někým, komu už nedůvěřujeme. Benevolentní Larry Page a Sergey Brin mohou být přehlasováni představenstvem vlastní společnosti, nebo jejich datová centra mohou být zabavena fašistickou vládou. Nebo jeden z jejich 30 000 zaměstnanců opustí společnost, ale vezme si s sebou naše data. Jejich servery mohou být hacknuty. A v neposlední řadě, jako všichni ostatní se zajímají především o své zákazníky a společnosti za inzerování velmi dobře platí. Proto pro ně představujeme v první řadě prodaný produkt.

Sociální sítě navíc vytvářejí trvalý záznam, souhrn dat tak rozsáhlý, že pouze informace, které Facebook má o jednom jediném uživateli, mohou přesáhnout osm set stran. Nikoho nepřekvapí, že účel Facebooku není učinit nás šťastnými: pokud si za to neplatíš, nejsi

zákázník, jsi jen produkt. Ale i kdyby tě tyto komerční záměry nezajímaly, měl bys zvážit fakt, že Facebook sám denně potvrzuje průniky hackerů do uživatelských účtů.

Abys náhledl za oponu stránky, kterou navštěvuješ, nainstaluj si do svého prohlížeče plugin Ghostery. Ten funguje jako rentgenový paprsek, který na stránce odhaluje všechny vložené a většinu času skryté technologie určené ke sledování uživatele. Doplňky Do Not Track Plus a Trackerblock ti díky blokování cookies, nekompromisnímu opt-out cookies a jiným funkcím poskytnou další kontrolu nad online sledováním. Kapitola Sledování se tímto tématem zabývá hlouběji.

Balíčky dat, se kterými pracuješ, mohou být snadno narušeny i mezi počítačem a routerem, například v prostředí kavárny. Tam venku je džungle, přesto si stále vybíráme hesla jako 'heslo' nebo '123456', provádíme transakce a nakupujeme lístky na bezdrátových sítích a klikáme na odkazy z nevyžádaných e-mailů. Nejenže je naším právem chránit si své soukromí, je rovněž i naší zodpovědností tak činit navzdory pokusům vlád, korporací nebo kohokoliv jiného. Pokud si svá práva nehájíme, plně si zasloužíme to, co může přijít v budoucnu.

ZÁKLADNÍ TIPY

VE ZKRATCE:

- Při návštěve libovolné webové stránky o sobě dáváš vědět vlastníkovi stránky, pokud neučiníš opatření, která tomu mohou zabránit.
- Tvé procházení Internetu může být sledováno stránkami, které navštěvuješ a jejich partnery. Používej software proti sledování.
- Návštěva webové stránky nikdy není přímým spojením. Počítače vlastněné mnoha lidmi jsou zapojeny do tohoto procesu. Používej bezpečené připojení, abys měl jistotu, že tvé aktivity nejsou zaznamenávány.
- To, co hledáš, představuje zájem pro poskytovatele vyhledávačů. Používej anonymní vyhledávací software, abys chránil své soukromí.
- Je lepší věřit open source prohlížečům jako Mozilla Firefox, protože mohou být uživateli snadno kontrolovány v otázkách bezpečnosti.

TVŮJ PROHLÍŽEČ O TOBĚ ZA TVÝMI ZÁDY MLUVÍ

Všechny prohlížeče předávají webovému serveru informace. Tyto informace obsahují jméno a verzi prohlížeče, odkazující informace (například odkaz na další stránku) a informace o operečním systému, který používáš.

Webové stránky tyto informace často využívají k přizpůsobení tvého prohlížení, nabízejí ti downloady pro tvůj operační systém a formátují stránku, aby lépe seděla do tvého prohlížeče. Nicméně tato skutečnost představuje určitý problém, neboť poskytnuté informace jsou součástí většího celku dat, která mohou být použita k identifikování tvé osoby.

Zarazit klábosení prohlížeče není snadné. Můžeš ale podvrhnout některé z informací zasílaných na web servery upravením dat obsažených v User Agentovi, čili identitě svého

prohlížeče. Například pro Firefox existuje užitečný plugin zvaný User Agent Switcher, který ti umožňuje přiřadit k prohlížeči jiný profil vybraný ze seznamů možností.

WEBOVÉ STRÁNKY TĚ PŘI BROUZDÁNÍ SLEDUJÍ

Malé soubory zvané 'cookies' jsou často webovými stránkami zapsány do tvého počítače. Cookies umožňují jisté výhody, jako cache tvých loginů, údaje o relaci a další data, která usnadňují procházení Internetu. Tyto malé kusy dat však představují významný risk pro anonymitu na webu: mohou sloužit ke tvé identifikaci, pokud se na stránku vrátíš, a také tě sledují při pohybu ze stránky na stránku. Společně s User Agentem jsou mocným a přitom skrytým prostředkem jak tě vzdáleně identifikovat.

Ideální řešení tohoto problému je zamítnutí všech pokusů webových stránek zapsat cookies na tvůj systém, to ale může výrazně zhoršit kvalitu tvého užívání webu.

Viz kapitola Sledování, kde nalezneš rady, jak webovým serverům sledování zakázat.

ONLINE VYHLEDÁVÁNÍ O TOBĚ PODÁVÁ INFORMACE

Když něco hledáme online pomocí služeb jako Bing nebo Google, naše právo na soukromí je v sázce mnohem více, než kdybychom se například šli zeptat zaměstnance na Informacích na letišti.

Kombinace cookies a User Agenta může být celou dobu používána k vytvoření pozvolna se doplňujícího profilu o tvé osobě. Inzerenti považují tuto informaci za velmi hodnotnou, vyvozují z toho závěry o tvých zájmech a mohou ti pak cíleně nabízet své produkty.

Zatímco někteří zákaznící pějí na cílenou reklamu chválu a jiní se o ni možná nestarají, rizika

často nebývají pochopena. Zaprvé shromažďované informace mohou být požadovány vládou, dokonce i vládou, kterou jsi nevolil (například Google je americkou společností a musí se tedy podřídit americkým soudním procesům a politickým zájmům). Zadruhé hrozí nebezpečí, že pouhé vyhledávání informací může být pochopeno jako záměr nebo politické stanovisko. Například umělec studující estetiku různých forem náboženského extrémismu může být asociován, či přímo nařčen z podpory organizace, kterou se zabývá. Zároveň existuje i možnost, že tvůj skrytý profil může být prodán pojišťovacím agentům nebo poskytnut zaměstnancům či jiným klientům té společnosti, jejíž vyhledávací služby používáš.

I když se ujistíš, že tvé cookies byly pročištěny, tvůj User Agent byl pozměněn (viz výše a dále v kapitole Sledování), stále o sobě podáváš podstatnou informaci: internetovou adresu, ze které se připojuješ (viz kapitola Co se děje při prohlížení?). Můžeš využít anonymizační službu jako Tor (viz kapitola Anonymita), aby ses tomuto vyhnul. Pokud jsi uživatel Firefoxu (doporučeno), nainstaluj si užitečný add-on Google Sharing, což je anonymizér pro vyhledávání přes Google. Pamatuj, že i když Google vědomě nepoužíváš, velké množství stránek využívá přizpůsobené Google Search lišty coby prostředek pro prozkoumávání vlastního obsahu.

Jak už bylo zmíněno, nemáš žádný důvod věřit Googlu, Yahoo nebo Bingu. Doporučujeme přejít na vyhledávací služby, které tvé právo na soukromí berou vážně, například DuckDuckGo (https://duckduckgo.com/).

VÍCE OČÍ, NEŽ MŮŽEŠ VIDĚT

Internet je velké místo a není jednou jedinou sítí, nýbrž obrovskou sítí složenou z mnoha menších mezi sebou propojených sítí. Takže když vyšleš požadavek na přístup na stránku, musí tvůj požadavek projít přes mnoho strojů, než se konečně dostane na serverový hosting dané stránky. Tato cesta je známá jako 'route' a obvykle obsahuje alespoň 10 různých strojů. Při pohybu ze stroje na stroj jsou pakety zkopírovány do paměti, přepsány a poslány dál.

Všechny stroje použité při pohybu na síti někomu patří, obyčejně společnosti nebo organizaci, a mohou být umístěny v různých zemích. Přestože jsou pokusy o standardizaci komunikačních zákonů mezi jednotlivými zeměmi, současná situace se projevuje jurisdikčními odlišnostmi. Takže zatímco ve tvé zemi nemusí být v platnosti zákony vyžadující logy tvého procházení webu, mohou být takové zákony zavedené kdekoliv po cestě tvých paketů.

Jedinými prostředky, jak ochránit route před zaznamenáváním nebo násilným vniknutím, je využívání šifrování bez mezifází, které je umožněno díky TLS/SSL (více v jednotlivých částech o šifrování) nebo soukromé virtuální sítě (viz kapitola VPN).

PRÁVO BÝT NEPOZNÁN

Kromě zájmu minimalizovat unikání soukromých údajů ke konkrétním poskytovatelům služeb bys měl zvážit i zakrývání své internetové adresy (viz kapitola Co se děje při prohlížení?). Touha dosáhnout takové anonymity podnítila vznik Tor Projektu.

Tor využívá rozrůstající se síť uzlů ke spojení se stránkou takovým způsobem, který k tobě nemůže být zpětně vystopován. Je to robustní prostředek zajišťující, že tvá internetová adresa nebude logována vzdáleným serverem. V kapitole Anonymita nalezneš více informací o tom, jak to funguje a jak můžeš začít Tor používat.

OBAVY

SOCIÁLNÍ SÍTĚ – JAKÁ HROZÍ NEBEZPEČÍ?

Fenomén sociálních sítí nezměnil pouze způsob, jakým lidé Internet používají, změnil samotnou podobu Internetu. Po celém světě, zejména pak ve Spojených státech, byla zavedena ohromná datacentra pro náhlou a širokou potřebu lidí nahrávat obsah o jejich zájmech a životech ve snaze se podílet na budování sociálních sítí.

Sociální sítí jako Facebook nebo Twitter (a dříve Myspace) jsou ovšem velmi vzdáleny pojmu 'svoboda'. Spíše se jedná o byznys, který se vyvíjí a následně těží z jedné z nejzákladnějších úzkostí: ze strachu ze sociální bezvýznamnosti a izolace. Jako sociální tvorové nejsme schopni unést myšlenku, že bychom byli ponecháni stranou. Pak mnoho z nás dobrovolně umístí svá citlivá a intimní vyjádření přímo na hard disky byznysmanů, které jsou uschovány hluboko v datacentru v nějakém vzdáleném státě – tedy někde, kam se uživatel dost možná nikdy nepodívá.

Mnoho lidí namítá, že sociální sounáležitost a ověřování osob sociálními sítěmi vyvažují potenciální ztrátu soukromí. Takový výrok je však možný pouze ve chvíli, kdy si je uživatel vědom všech možných rizik.

Rizika sociálních sítí ohledně osobního soukromí jsou definovány:

- Rozsahem a intimitou uživatelových vlastních kontribucí.
    * Uživatel přispívá často a jeho příspěvky obsahují mnoho osobních detailů, které jsou použity pro cílený marketing.

- Připraveností uživatele přijmout sociální hrozby.

* Uživatel, který přistupuje nekriticky k vytváření sociálních vazeb, je ohrožen aktivitami internetových predátorů a sociálních inženýrů.

- Ekonomickými zájmy a partnery organizace poskytující danou službu.

* Studie zadané klienty, získávání dat a analýza chování.

- Politické/zákonné požadavky provedené státem vůči organizaci dle jurisdikce, pod kterou organizace spadá.

* Soudní příkazy vyžadující data určitého uživatele (lhostejno jestli místního či zahraničního).

* Agendy dozoru nad obsahem vyžadované ochránci zákona nebo partnery organizace.

* Analýza chování a uvažování: projektování politického záměru.

Když zohledníme vypsané body, můžeme snadno srovnat projekty jako Diaspora a Facebook: první projekt nabízí určitou úroveň organizační transparence, závazek k udržení soukromí a obecnou otevřenost, zatímco Facebook dokazuje, že je neprůhlednou společností přístupnou k ekonomickému hazardu se soukromím svých uživatelů a staví se do čela občanských žalob v zájmech svých vlastních klientů. Pravděpodnost, že tvé interakce se sociální sítí ovlivní nahlížení pojišťovací společnosti nebo možného zaměstnavatele na tvou osobu, je tedy daleko nižší u menších a více transparentních organizací než u velkých sociálních sítí.

KDO MŮŽE UKRÁST MOU IDENTITU?

Tato otázka souvisí s tím, jak při procházení webu postupuješ. Slabé univerzální heslo představuje pro mnoho služeb včetně sociálních sítí, internetového bankovnictví a mailové schránky nebezpečí, že tvé účty na nich budou zneužity. I silné univerzální heslo, které je na bezdrátové síti sdíleno s ostatními (ať už otevřené nebo šifrované), je stejně tak zranitelné.

Obecným pravidlem je používat dostatečně silné heslo (viz část Hesla).

Bezdrátové sítě

V případě bezdrátových sítí se ocitáme uprostřed často podceňovaného rizika, že někdo může odposlouchávat naši komunikaci skrze zachytávání síťových paketů. Potom málo záleží na tom, zdali je síť otevřená nebo zabezpečená heslem. Pokud někdo využívá stejnou šifrovanou síť, může snadno zachytit a číst veškerý nezabezpečený provoz ostatních uživatelů uvnitř stejné sítě. Klíč k bezdrátové síti se dá sehnat relativně snadno a těm, kdo ví, jak zachytit a číst síťové pakety, dává šanci získat tvé heslo, zatímco kontroluješ svůj e-mail.

Vždy platí jednoduché pravidlo: pokud internetová kavárna nabízí kabelové připojení, použij ho! A stejně jako u bankomatu si dávej pozor, jestli ti při psaní hesla někdo nekouká přes rameno.

Cache v prohlížeči

Kvůli neustálému vyplňování hesla častokrát necháváme prohlížeč či mailového klienta, aby naše heslo pro budoucí přihlášení ukládal. To samo o sobě není vůbec špatné, ale když je náš laptop nebo telefon odcizen, umožňuje to zloději přístup k vlastníkově účtům. Doporučená praxe je promazávat cache pokaždé, když zavřeš svůj prohlížeč. Populární prohlížeče mají v sobě tuto možnost zabudovanou.

Šifrování disku je opatření, kterým můžeš zajistit bezpečné zachování svého cache. Pokud je tvůj laptop ukraden a zloděj počítač restartuje, narazí na šifrovaný disk. Také je rozumné mít nastavené zamykání obrazovky, protože i když je ti stroj odebrán při stále běžící relaci, není možné ho odemknout bez znalosti hesla.

Zabezpečení linky

Kdykoliv se přihlásíš k jakékoliv službě, měl bys pro celou svou relaci využívat šifrování. Toho lze snadno dosáhnout díky použití TLS/SSL (Secure Socket Layer).

Zjisti, zdali služba, kterou využíváš (ať je to e-mail, sociální síť nebo online bankovnictví) podporuje TLS/SSL relaci. Zjistit se to dá snadno napsáním 'https://' na začátku dané URL. Pokud se ti to nedaří, ujisti se, jestli je možné toto ve službě nastavit.

MOHU SE DOSTAT DO PROBLÉMŮ KVŮLI GOOGLENÍ DIVNÝCH VĚCÍ?

Google a další společnosti zaměřené na vyhledávání na Internetu mohou být skrze soudní příkazy přinuceny sledovat konkrétní jedince. I webová stránka využívající uzpůsobeného vyhledávacího pole od Google může být nucena zachovávat logy a dotazy na vyhledávání v rámci jurisdikce, do které organizace provozující stránky spadá. Akademici, umělci a výzkumní pracovníci tak podstupují riziko, že budou špatně pochopeni a může u nich být shledána chybná motivace jen na základě jejich projeveného zájmu o téma.

KDO ZACHOVÁVÁ ZÁZNAMY O MÉM PROCHÁZENÍ A JE MI UMOŽNĚNO SE PŘED NÍM SKRÝT?

Anonymní přístup na webovou stránku zcela určitě patří mezi základní lidská práva. Stejně jako je ti umožněno navštívit veřejnou knihovnu, prolistovat knížky a vrátit je zpět na polici bez toho, aby si někdo poznamenával, co sis četl, máš nárok po Internetu brouzdat anonymně.

JAK NEODHALIT MOU IDENTITU?

Viz kapitola Anonymita.

JAK SE VYHNOUT SLEDOVÁNÍ?

Viz kapitola Sledování.

ÚČTY A BEZPEČNOST

Při procházení Internetu můžeš být v jednu chvíli přihlášen na více různých službách. Může to být webová stránka společnosti, tvůj e-mail nebo sociální síť. Naše účty jsou pro nás důležité, protože naše velmi citlivé údaje jsou uloženy na strojích kdesi na Internetu.

Udržovat své účty v bezpečí vyžaduje více než jen silné heslo (viz část Hesla) a zabezpečený komunikační link se serverem skrze TLS/SSL. Pokud není určeno jinak, většina prohlížečů tvá přihlašovací data ukládá jako cookies, čímž ruší povinnost se na každé stránce opětovně přihlašovat. To znamená, že pokud má někdo přístup ke tvému počítači nebo telefonu, může mít i přístup ke tvým účtům, aniž by musel zjišťovat tvé heslo nebo používat různé sofistikované metody.

S vzestupem popularity smartphonů vzrostlo také zcizování přístupů k účtům z ukradených telefonů. Krádež laptopu též představuje určité riziko. Pokud necháváš svůj prohlížeč pamatovat si tvá hesla, zde je několik možností, jak si je chránit:

- Používej zamčení obrazovky. Pokud máš telefon a upřednostňuješ odemykací vzorec, zvykni si otírat obrazovku, aby útočník neuhodl vzorec podle tahů od prstu. U laptopu bys měl nastavit svůj spořič obrazovky tak, aby po tobě vyžadoval heslo.
- Zašifruj svůj hard disk. TrueCrypt je otevřený a bezpečný systém šifrování disku pro Windows, Mac OS a Linux. Většina Linuxových distribucí a OS X umožňují možnost šifrovat disk při instalaci systému.
- Pro vývojáře Androidu: Nepovolujte USB debuggování na svém telefonu jako výchozí. To umožní útočníkovi využít adb shell Androidu, aby se dostal k vašemu hard

disku bez odemykání telefonu.

MOHOU NEBEZPEČNÉ STRÁNKY PŘEVZÍT KONTROLU NAD MÝMI ÚČTY?

Cookies obsahující tvá přístupová data jsou primárním bodem zranitelnosti. Jedna z populárních technik pro získání přístupových dat se nazývá 'click-jacking' – v té je uživatel nalákán na zdánlivě neškodný link, který však spustí skript, který využívá toho, že je uživatel přihlášen. Tak mohou být přístupová data ukradena útočníkem, který tím získá vzdálený přístup k uživatelovým účtům. Přestože se jedná o komplikovanou techniku, ukázalo se, že je velice efektivní. Twitter i Facebook už zažily případy odcizení loginů tímto způsobem.

Je důležité si vybudovat zvyk vždy uvažovat, na který odkaz je vhodné kliknout, když jsme přihlášeni i na jiných službách. Jedna z možností je využívat jiný prohlížeč, kde nikde přihlášeni nejsme, coby nástroj pro testování bezpečnosti odkazů. Vždy si ověř, že adresa (URL) v odkaze je správně napsaná. Může to být stránka s velice podobným názvem jako ta, které věříš. Pamatuj, že zkrácené linky představují také určité riziko, protože nevíš, kam odkazují.

Pokud používáš Firefox, přidej si add-on NoScript, který omezí mnohé techniky, které se dají použít k získání tvých cookies. Na druhou stranu může na některých stránkách narušit některé funkce.

SLEDOVÁNÍ

Během procházení Internetu za sebou zanecháváš digitální stopy. Mnoho stránek využívá tato data jen k shromažďování statistik, ale některé stránky jdou do hloubky a využívají různé techniky ke sledování jednotlivých uživatelů, někdy až takové, které jim umožní uživatele přímo osobně identifikovat. To ale není všechno. Některé firmy ukládají data z prohlížečů ke sledování pohybu uživatele na webu. Tato informace může být kdykoliv předána libovolné organizaci, aniž by o tom uživatel věděl nebo by k tomu musel dát svolení.

To vše zní dost zlověstně, ale kdo se vážně stará o to, zdali nějaká velká společnost neví o webových stránkách, které navštěvujeme? Velké webové portály využívají tato data pro 'behaviorální propagaci', ve které jsou inzeráty upraveny tak, aby přesně vyhovovaly možnému zákazníkovi. Takže například po přečtení hesla 'Majorca' na Wikipedii můžeš být bombardován mnoha reklamami, které ti budou nabízet zájezdy a klobouky. To se zdá jako neškodné, ale když budeš vyhledávat věci jako 'léčba oparů' nebo 'fetiš komunity' a následně budeš při procházení Internetu vídat výpis relevantních produktů, možná ti familiárnost webu už nepřijde tak přívětivá.

Všechny tyto informace vzbuzují zájem u třetích stran, například u tvé pojišťovny. Pokud bude vědět, že ses díval na stránky o skydivingu nebo pročítal fóra o vrozených chorobách, může se to projevit na tvých sazbách. Zaměstnavatelé nebo domácí tě mohou vyhodit kvůli tvým zájmům na webu, v extrémních případech tě policie může podezírat ze spáchání trestného činu jen na základě tvého podezřelého surfování.

JAK NÁS SLEDUJÍ?

Při každém načtení stránky vygeneruje software na serveru dané stránky záznam o zhlédnutí, který je možné si prohlédnout v log file. Takový postup nemusí být vždy špatný. Když se totiž přihlásíš na webovou stránku, je nutné potvrdit tvou identitu a stránka si musí pamatovat, kdo

jsi, aby mohla uložit tvé preference nebo jinak vyjít vstříc tvému osobnímu nastavení. Právě k tomu slouží soubor nazvaný cookie. Tento soubor zůstává na tvém počítači i poté, co zavřeš webovou stránku. Cookie o tobě pak může vydat informace, třeba i o tom, jaké jiné stránky jsi navštívil. Některé velké služby, například Facebook nebo Google, využívají této metody, aby znaly tvé prohlížecí návyky.

JAK SE MOHU VYHNOUT SLEDOVÁNÍ?

Nejjednodušší a nejpřímější způsob je smazání souborů cookie ve tvém prohlížeči. Problém tohoto přístupu je v tom, že v okamžiku, kdy se na dané stránky vrátíš, obdržíš od nich nové cookies. Dalším nedostatkem je, že ztratíš veškeré údaje o aktuálním prohlížení, takže se například budeš muset u jednotlivých služeb přihlašovat znovu.

Vhodnější možnost podporovaná moderními prohlížeč je Private browsing nebo Incognito mode. To otevírá dočasné okno prohlížeče, které neukládá historii, heslo, stažené soubory ani cookies. Při zavření okna jsou všechny tyto informace smazány. I to má ovšem svá úskalí. Nemůžeme ukládat hesla, pamatovat si záložky nebo využívat jiné z užitečných výhod, které moderní prohlížeče nabízejí.

Naštěstí existuje dostatek pluginů, které jsou navrženy tak, aby se vypořádaly s problémy sledování. Jedním z nejrozšířenějších je Ghostery. Tento plugin ti umožňuje blokovat kategorie nebo jednotlivé služby, které uživatele sledují.

Další možností je instalace blokovacího pluginu jako je AdBlockPlus. Ten automaticky blokuje velké množství sledovacích cookies, které na uživatele posílají reklamní agentury.

JAK ZJISTÍM, KDO MĚ SLEDUJE?

Nejsnazší je používat plugin Ghostery, který do rohu tvého prohlížeče přidá malou ikonku,

která ti sdělí, jaké služby tě na jakých stránkách sledují. Rovněž je doporučen add-on Do Not Track s podobnými funkcemi. Oba doplňky je vhodné kombinovat, protože někdy odhalí konkrétní cookie jen jeden z nich.

VAROVÁNÍ

Když blokuješ sledovací cookies, získáváš vyšší úroveň soukromí při pohybu na síti. Nicméně vládní agentury, nadřízení, hackeři a síťoví administrátoři i tak mohou narušit tvé spojení a zjistit, co jsi vyhledával. Pokud chceš zabezpečit své připojení, rady nalezneš v kapitole o šifrování. Stejně tak tvá identita bude viditelná pro jiné lidi na Internetu. Pokud chceš chránit svou identitu, musíš učinit kroky potřebné k zachování online anonymity.

ANONYMITA

INTRO

Článek 2 Všeobecné deklarace lidských práv říká:

> *"Každý smí užívat veškerých práv a svobod, která jsou v Deklaraci obsažena, bez ohledu na rasu, barvu kůže, pohlaví, jazyk, náboženské vyznání, politický či jiný názor, národní či sociální původ, majetek, věk nebo jakýkoliv jiný status.*
>
> *Žádné rozdíly by neměly být činěny ani na bázi politického, jurisdikčního nebo mezinárodního statutu země či teritoria, ke kterému osoba náleží, ať už se jedná o teritorium nezávislé, svěřenské, bez vlády nebo podléhající jakýmkoliv dalším limitům suverenity."*

Jeden ze způsobů, jak toto základní právo prosadit v nepříznivém prostředí, je anonymita, která znemožňuje propojení aktivního agenta se specifickou osobou.

Anonymní aktivita je též skvělý způsob jak pomoci ostatním, kteří potřebují ochranu většího stáda. Toho lze snadno docílit využíváním Toru, techniky, která vede internetový provoz mezi uživateli přes speciální software, který činí jakoukoliv využívanou IP adresu nevystopovatelnou (pokud by potenciální narušitel nekontroloval celou síť a to se prozatím nikomu nepodařilo). Vysoce funkční prostředek pro ochranu vlastní identity jsou také anonymní proxy servery a Virtual Private Networks (VPN).

PROXY

"Anonymizér nebo anonymní proxy je nástroj, který se snaží zamezit sledování aktvit na Internetu. Proxy server v něm funguje jako prostředník a štít soukromí mezi počítačem klienta a zbytkem Internetu. Přistupuje k Internetu namísto uživatele, čímž chrání jeho osobní informace skrytím identifikačních údajů o klientově počítači."

(http://en.wikipedia.org/wiki/Anonymizer)

Hlavním účelem proxy je skrýt nebo změnit IP adresu přiřazenou k uživatelově počítači. Existuje několik důvodů, proč by o něco takového měl uživatel usilovat:

- Kvůli anonymizování přístupu k určitému serveru a zametení stop ponechaných v log file na web-serveru. Uživatel může například chtít nebo potřebovat přístup k citlivým materiálům online (zvláštní dokumenty, výzkumná témata nebo jiné) bez toho, aby k sobě přitáhl pozornost autorit.

- Kvůli snaze prolomit firewally korporací nebo represivních režimů. Korporace/vláda může limitovat nebo úplně zrušit přístup k Internetu pro konkrétní IP adresu nebo rozsah IP adres. Skrýt se za proxy umožní obelstít tyto filtry a zpřístupnit tak zakázané stránky.

- Kvůli sledování online videí nebo streamů, které jsou v dané zemi znepřístupněny.

- Kvůli přístupu k webovým stránkám nebo materiálům, které je možné prohlížet jen v určité zemi. Uživatel například chce sledovat video BBC ze streamu pouze ve Spojeném království, zatímco fyzicky je v jiném státě.

- Kvůli přístupu na Internet z blokované či banované IP adresy. Veřejné IP adresy mívají často 'špatnou reputaci' a mohou být z různých důvodů některými webovými stránkami blokovány.

Při přístupu na web proxy umožní vyslat požadavek přes vzdálený server. Oproti routeru, proxy server nepředává přímo uživatelovy požadavky, ale spíše tyto požadavky tlumočí a odpovědi posílá zpět do uživatelova počítače.

Proxy (pokud není nastavena jako 'transparentní') neumožňuje přímou komunikaci s

Internetem, z čehož vyplývá, že aplikace jako prohlížeče, chatoví klienti nebo download aplikace musí být nastaveny tak, aby o připojení přes proxy věděly (viz kapitola Nastavení proxy).

TOR

"- Tor zabraňuje ve zjištění vaší lokace nebo prohlížecích návyků.

- Tor je pro prohlížeče, klienty instantního posílání zpráv, vzdálené loginy a další.

- Tor je svobodný a otevřený software pro Windows, Mac, Linux/Unix a Android."

(https://www.torproject.org)

Tor je systém, který má zajišťovat anonymitu online. Je složen z klientského software a sítě serverů, které skrývají informace o uživatelově lokaci a o dalších faktorech, které by mohly vést k jeho identifikaci. Princip Toru si představ jako zprávu zabalenou do mnoha ochranných vrstev: každý server musí odstranit jednu vrstu, čímž okamžitě maže informace o odesilateli z předchozího serveru.

Používání tohoto systému činí sledování uživatelovy činnosti na Internetu daleko obtížnějším. Tor byl vytvořen za účelem ochrany uživatelových osobních svobod, soukromí a možnosti provozovat důvěrný byznys. Toho dosahuje schováním provozovaných aktivit před případným monitorováním. Software je open source a síť Toru je zdarma přístupná k využívání.

Tor nemůže zajistit ochranu proti monitorování vstupního a výstupního provozu sítě. Přestože Tor zajišťuje ochranu vůči analýze provozu, nemůže zabránit takzvané 'end-to-end' korelaci, která patří mezi způsoby propojení online a fyzické identity.

Jako příklad může posloužit nedávná kauza Jeremyho Hammonda, který se ocitl v hledáčku FBI kvůli jeho aktivitám spojeným s hnutím Anonymous. FBI Jeremyho sledovala jednak

fyzicky, dále skrze monitorování jeho bezdrátového připojení a zároveň byla na chatovém kanálu, kam Jeremy pod svým aliasem chodíval. Když Jeremy dorazil do svého domu, inspekce paketů z jeho připojení odhalila, že spustil Tor a ve stejný moment se na daný kanál připojil pod svou přezdívkou. To stačilo na Jeremyho kompromitování a FBI jej zadržela.

Více v kapitole Užívání Toru.

VPN

Cesta, kterou musí tvá data urazit na požadovaný server a zpět do tvého zařízení, není tak přímočará, jak by se mohlo zdát. Řekněme, že jsi doma připojen na bezdrátovou síť a otevřeš si Wikipedii. Tvůj požadavek (čili tvá data) musí projít přes mnoho bodů neboli 'hopů', jak se jim říká v terminologii síťové architektury. Na každém z těchto 'hopů' mohou být tvá data získána, zkopírována a případně i upravena. Několik příkladů, kde může dojít k zachycení dat vztahujících se ke zmíněnému případu:

- Tvá bezdrátová síť (tvá data mohou být zachycena ve vzduchu)
- Tvůj ISP (ve většině zemí je po ISP požadováno zachovávání detailních logů)
- IXP (Internet Exchange Point) na jiném kontinentě
- ISP společnosti, která stránku hostuje
- Interní síť, ke které je server připojen

Kdokoliv, kdo má fyzický přístup k počítačům nebo sítím, které jsou na cestě mezi tebou a vzdáleným serverem, může sbírat data, která pošleš na vzdálený server a která ti server pošle zpět. To se týká zejména takzvané 'poslední míle', což je název pro propojení mezi koncovým bodem komunikační sítě a účastníkem spojení. Svého ISP také nemůžeš považovat za důvěryhodného nebo 'datově neutrálního' – státní agentury mnoha zemí ani nepotřebují povolení k tomu, aby mohly ke tvým datům přistupovat bez omezení.

VPN neboli Virtual Private Network (Soukromá virtuální síť – pozn. překl.) je řešením pro problémy spojené s 'poslední mílí'. VPN je technologie, která umožňuje vytvoření virtuální sítě nad již existující infrastrukturou. VPN síť operuje se stejnými protokoly a standardy jako síť fyzická. Programy a operační systémy ji používají jako oddělené síťové připojení, ačkoliv její topologie neboli propojení jejích uzlů ve vztahu k fyzickému prostoru je zcela předefinována.

Představ si to tak, že namísto toho, abys svěřoval svá data každému možnému

prostředníkovi (lokální síť, ISP, stát), máš možnost je vypustit přes server takového provozovatele VPN, kterému věříš. Od chvíle, kdy tvá data opustí tvůj počítač a dostanou se do VPN sítě, jsou plně zebezpečena TLS/SSL typem šifrování. Jako taková budou pro každý uzel, který by mohl být nastaven ke sledování tvé osoby, působit jen jako náhodný šum. Je samozřejmě možné namítnout, že v okamžiku, kdy data opustí bezpečí VPN, stanou se stejně zranitelnými jako předtím – to ale není pravda. V okamžiku, kdy data vystupují z VPN serveru, jsou od tebe už velmi vzdálená a nemohou s tebou být propojena. Seriózní poskytovatelé VPN budou mít své servery instalovány na vysoce zabezpečených místech internetové výměny a jakýkoliv fyzický přístup k datům, jejich odposlech nebo logování na serverech VPN by představovaly velmi náročný úkol.

Další zajímavá a často podceňovaná funkce VPN se skrývá přímo v jejím názvu – kromě 'virtuální' a 'soukromé' je rovněž samostatnou 'sítí'. VPN umožňuje nejen spojení se světem pomocí VPN serveru, ale zároveň i komunikaci s dalšími členy stejné VPN sítě, aniž by bylo nutné opustit bezpečí šifrovaného prostoru. Díky této funkci se VPN vlastně stává Darknetem, čili sítí izolovanou od Internetu. Protože připojení k VPN serveru vyžaduje klíč nebo certifikát, je zajištěno, že se do soukromé sítě dostanou skutečně jen pozvaní uživatelé. Není tedy možné, aby se náhodný vetřelec z Internetu mohl dostat k obsahu VPN, aniž by se musel přihlásit jako některý z již existujících uživatelů sítě.

ČÁST ČTVRTÁ: PUBLIKACE A DISTRIBUCE

ANONYMNÍ PUBLIKACE

Ať už jsi aktivista operující v totalitním režimu, zaměstnanec rozhodnutý odhalit veřejnosti křivárny ve firmě či mstivý spisovatel tvořící hanebný profil své exmanželky, potřebuješ chránit svou identitu. Pokud s nikým nespolupracuješ, je nutné se zaměřit na anonymitu, nikoliv šifrování či soukromí.

V případě nejvyšší nutnosti je nejjednodušší zajít do nepříliš frekventované internetové kavárny, vytvořit účty čistě pro onen konkrétní úkol, doručit data a ihned poté smazat použité účty. Pokud hodně spěcháš, zvaž užití MintEmail (http://www.mintemail.com/) nebo FilzMail (http://www.filzmail.com/), kde tvá adresa sama expiruje během 3 až 24 hodin. V kavárně při odesílání nedělej nic jiného, žádné kontrolování Gmailu či rychlé nakouknutí na Facebook, a než odejdeš, nezapomeň vymazat historii, cookies i cache a zavřít prohlížeč.

Pokud zachováš tato základní pravidla, nejhorší – a velmi nepravděpodobná – věc, která se ti může stát, je, že tobě přidělený počítač bude prolezlý nějaký svinstvem a nahrává úhozy kláves, odhaluje hesla nebo dokonce i tvou tvář v případě, že má webkameru, která je ovládána zdálky. Nedělej nic kompromitujícího v práci nebo v místě, kde jsi registrovaným členem nebo občasným návštěvníkem, například knihovna nebo oblíbený klub opravdu nejsou vhodná místa.

Potřebuješ-li komunikaci v reálném čase, třeba pro domluvení schůzky, je tato metoda poněkud nešikovná a brzy ti mohou dojít nenavštívené internetové kavárny. V takovém případě můžeš použít vlastní počítač, ovšem nemáš-li stroj vyhrazený právě pro tyto případy, nabootuj počítač v jiném operačním systému. Můžeš to snadno provést s bootovací USB

flashkou, která obsahuje operační systém, například TAILS, který má defaultně nastavený Tor a obsahuje nejlepší možné kryptografické nástroje. V každém případě použij Tor pro zakrytí své IP adresy.

Vypni v nastavení ukládání cookies, historie a cache a nikdy nepoužívej stejný profil nebo stejný prohlížeč pro stejné aktivity. Nejenže každým připojením přidáváš na Internet údaje o své činnosti, ale toto také otevírá velké příležitosti pro různé omyly. Chceš-li další ochranu, instaluj do prohlížeče rozšíření Do Not Track Plus, Trackerblock nebo Ghostery.

Užívej různá hesla pro různé účty a obměňuj je, případně měň i passfráze. Chraň celý systém pomocí hlavního hesla, často jej měň a nikomu neprozrazuj, zejména ne svému partnerovi. Všude si nastav odhlášení od všech služeb i programů po pěti minutách neaktivity. Svou 'superhrdinskou identitu' si nech pro sebe.

Pokud jsi schopen dodržet určitou úroveň disciplíny, můžeš používat i své vlastní internetové připojení, ale zvaž toto: při nepoužívání jednoúčelového systému vyvstává neuvěřitelný problém udržet všechny identity bezpečně oddělené a pocit bezpečí často vede k lehkomyslnosti. Udržuj si zdravou hladinu paranoie.

V současnosti existuje spousta možností internetové publikace, od blogů zdarma (Blogspot, Tumblr, Wordpress, Identi.ca) přes pastebiny až po systémy speciálně koncipované pro anonymní uživatele, jako je BlogACause. Global Voices Advocacy doporučuje užívat Wordpress přes síť Tor. Buď zdravě cynický: všichni poskytovatelé podobných služeb fungují z komerčních pohnutek a nedá se jim věřit, zejména ve chvíli, kdy mohou být vázáni v právním systému. Když na to přijde, všichni poskytovatelé jsou zrádci.

Pokud registrace v těchto službách vyžaduje funkční emailovou adresu, vytvoř si jednu věnovanou toliko tomuto účelu. Vyhni se Gmailu, Yahoo, Hotmailu a jiným velkým komerčním platformám, které jsou známy vydáváním dat svých uživatelů a vyberte si specializovanou službu, jako je Hushmail (https://www.hushmail.com/).

CO NEDĚLAT

Neregistruj si vlastní doménu. Existují služby, které ochrání tvou identitu dle jednoduché otázky 'Kdo je to', jako je například Anonymous Speech či Silent Register, ale kvůli platebním datům budou vědět, kdo skutečně jsi. Není-li možnost zaplatit Bitcoiny, omez se na jednu doménu nabízenou tvou blogovou plaformou, jako je například tvujblog.blogspot.com, a nastav si jiný stát, než je ten, ve kterém skutečně žiješ. Je též důležité vybrat si název, který tě snadno neodhalí. Pokud máš s výběrem jména problém, použij onlinový generátor blogových jmen.

Neotevírej si účet v sociální síti asociovaný s tvým blogem. Když už musíš, buď stejně opatrný jako v případě blogování a nikdy se nepřihlašuj ze stejného prohlížeče. Máš-li veřejný život na sociální síti, zbav se všech účtů s ním spjatých. Nakonec bys udělal chybu.

Nenahrávej videa, fotky nebo zvukové záznamy bez užití editoru, který upraví či vymaže veškerá metadata (fotografie obsahují GPS souřadnice z míst, kde byly pořízeny), jež automaticky přidávají standardní digitální fotoaparáty, chytré telefony a jiná nahrávací zařízení. S tím ti může pomoci Metadata Anonymisation Toolkit.

Nezanechávej žádnou historii. Umísti do svých http headerů X-Robot-Tag, jenž ti umožní zbavit se searching spiders indexujících tvou stránku. Též tě ochrání od webových úložišť jako je Wayback Machine na archive.org. Nevíš-li jak to provést, vyhledej si 'Robot Text File Generator'.

Nekomentuj. Když už tak činíš, zachovávej stejný stupeň ochrany, jaký užíváš při blogování, po zanechání komentáře se vždy odhlaš a netroll. Ani samo peklo nezuří tak, jako vytrollený bloger.

Nečekej, že ti anonymita vydrží. Stane-li se z tebe blogová senzace (jako třeba Belle de Jour, britská doktorka, která se stala senzací, vydala knihu a stála za dvěma TV seriály, odhalujícími její dvojí život luxusní prostitutky), budou legie novinářů, výběrčích daní a obsesivních fanoušků sledovat každý tvůj pohyb. Jsi jen člověk: dostanou tě.

Neváhej. Pokud zjistíš, že jsi udělal nějaké chyby a zatím tě nenachytal, zruš všechny své účty, odkryj stopy a začni znovu pod úplně novou identitou. Internet má nekonečnou paměť: jeden úder a jsi odhalen.

ANONYMNÍ EMAIL

Každý datový balík cestující po internetu obsahuje informace, odkud a kam byl poslán, ať už je to e-mail nebo jiný typ internetové komunikace. Je zde několik způsobů jak zredukovat informace vedocí ke tvé identifikaci, avšek není možné je odstranit úplně.

ODESÍLÁNÍ Z MAILOVÝCH ÚČTŮ NA JEDNO POUŽITÍ

Jedna z možností je používat e-mail na jedno použití. Je to účet třeba na Gmailu nebo Hotmailu použitý pouze jednou či dvakrát pro anonymní výměnu dat. Když se registruješ, nezapomeň zadat falešné osobní údaje (jméno, lokace). Po krátkém užití účtu, řekněme 24 hodin, se už nikdy nepřihlašuj. Potřebuješ-li komunikovat i nadále, vytvořte si nový účet.

Mysli na to, že tyto služby uchovávají IP adresu a odesíláš-li velmi citlivé informace, použij spolu s tímto mailem i Tor, aby nedošlo k odhalení tvé IP.

Ve chvíli, kdy neočekáváš na svůj mail žádnou odpověď, naskýtá se zde řešení v podobě remailerů, jako jsou AnonEmail a Silentsender. Remailer je server, který obdrží zprávu s místem, na které ji má poslat a přeposílá zprávu z generické adresy, bez odhalení totožnosti skutečného odesílatele. Tyto služby nejlépe fungují s e-mailovými poskytovateli typu Hushmail nebo RiseUp, které mají speciální nastavení pro zabezpečné připojení.

Obě tyto metody jsou funkční, avšak jen v případě kdy si uvědomuješ, že poskytovatel vždy ví, odkud byla původní zpráva odeslána a může číst doručenou poštu. Bez ohledu na proklamace o ochraně uživatelovy totožnosti, používají tyto služby často uživatelská ujednání, která vyžadují právo 'poskytnout třetí straně registrační údaje', či mohou být podezřelé ze spolupráce s tajnými službami. Jediná cesta jak bezpečně používat tuto techniku je zásadně nedůvěřovat poskytovatelům a aplikovat zvláštní bezpečnostní opatření: vždy jít přes Tor a

používat e-mail jen na jedno použití.

Pokud potřebuješ e-mail pouze k přijetí zprávy, jsou zde služby jako Mailinator a MintEmail, které vygenerují adresu, jež po pár hodinách sama zanikne. Pokaždé, když se někde registruješ, zadávej falešné osobní údaje a chraň své připojení Torem.

BUĎ OPATRNÝ NA SVÁ SLOVA!

Obsah zprávy může snadno odhalit tvou identitu. Když zmíníš detaily o svém životě, místě pobytu, společenské vazby nebo svůj vzhled, lidé mohou uhodnout, kdo zprávu odeslal. Už jen výběr slov a styl psaní může být použit k odhalení, kdo stojí za anonymními maily.

Neužívej stejné uživatelské jméno pro různé účty ani jméno, pod kterým jsi snadno vystopovatelný jako třeba přezdívka z dětství nebo oblíbená knižní postava. Nikdy nepoužívej svůj tajný e-mail k normální komunikaci. Když někdo zná tvé tajemství, nebav se s ním přes tuto adresu. Když na tom závisí tvůj život, měň často svou tajnou e-mailovou adresu i poskytovatele služby.

Když už máš e-mail nastavený tak, aby chránil tvou identitu, je marnivost tvým nejhorším nepřítelem. Vyvaruj se nápadnosti, nezkoušej být mazaný, okázalý nebo příliš jedinečný. Už jen způsob, jakým zalamuješ odstavce, je hodnotná informace ke tvé identifikaci, zejména dnes, kdy každá školní esej či blogpost, které jsi kdy napsal, jsou dostupné na Internetu. Mocné organizace mohou užít tento text k sestavení databáze, kde bude styl psaní obdobou otisků prstů.

SDÍLENÍ DAT (FILE SHARING)

Termín 'File Sharing' označuje sdílení dat na síti, často nejširší možnou formou. Naneštěstí byl v minulých letech populárně spojován s distribucí dat, která jsou pod ochranou autorských práv, která zakazují distribuci kopií (předpoklad kriminální aktivity). Bez ohledu na tuto asociaci zůstává sdílení dat živelným nástrojem pro mnoho webů: od akademiků, přes vědecké sítě až po open source komunity.

Tato kniha ti má pomoci naučit se sdílet data s ostatními uživatali v co největším soukromí, bez rizika, že bude jejich obsah znám komukoliv neautorizovénému či bude přenos zastaven někým z vnějšku. Zaručuje to tvé právo na anonymitu. Podezření, že ona data mohou být kradená a nepatří ti neznamená, že by se mělo podrývat tvé právo na soukromí.

Historie internetu je psána útoky na různé publikační a distribuční uzly, prováděnými různými způsoby (rozhodnutí soudu, DDoS). Takové události demonstrují, že když chce někdo neustálý přístup k dobře chráněným informacím, je nemysl spoléhat se na jediný uzel, který může být snadno neutralizován.

Toto bylo naposledy demonstrováno při likvidaci služby Megaupload, jež vedla k masivní ztrátě uložených dat uživatelů. Mnoho těchto dat vůbec nesouviselo s porušováním autorských práv, která byla záminkou k ukončení Megauploadu. Podobným způsobem poskytovatelé internetového připojení odstřihují weby obsahující sporný materiál, protože je to vyjde levněji než soud. Tato taktika dává prostor bezdůvodnému šikanování společnostmi, organizacemi a jedinci, kteří agresivně trvají na dodržování práv. Jak služby typu Megaupload (tedy direct download), tak poskytovatelé připojení jsou příkladem centralizovaných struktur, které nemohou záviset jedna na druhé, neboť je to slabé místo pro útok a jejich obchodní zájmy se neslučují se zájmy jejich uživatelů.

Decentralizovat data je nejlepší způsob jak se bránit takovým útokům. V následující kapitole

vám představíme dvě sdílecí služby. První je standardní P2P technologie, jejíž design je determinován efektivitou sítě, poskytující rychlost přenosu a průzkumu obsahu skrze asociované vyhledávací mechanismy. Druhé cílí na I2P jako příklad takzvaného Darknetu, staví nad jiné priority bezpečnost a anonymitu a nabízí cestu neustálé dostupnosti.

Tyto způsoby sdílení jsou jen dva příklady z mnoha různých P2P technologií, které se vyvíjejí od roku 1999. BitTorrent a Soulseek mají velmi rozdílné způsoby, oba však byly postaveany na snadné dostupnosti široké veřejnosti a mají významné uživatelské komunity. I2P je novější, má tedy menší uživatelskou základnu.

BitTorrent je nejpopulárnější P2P systém sdílení. Je ironií, že kontroverze, která tyto služby v současnosti obklopuje, pomohla v růstu komunity ve chvíli, kdy policie v žoldu mocných držitelů práv zabavila torrentům servery a pronásledovala jejich provozovatele, což v některých případech vedlo až k uvěznění (Pirate Bay).

Soulseek není zrovna nejslavnější platforma pro sdílení dat, ovšem nikdy se o to ani nesnažil. Soulseek je zaměřen na výměnu hudby mezi nadšenci, undergroundovými producenty a badateli. Systém i komunita jsou dokonale izolovány od sítě: data ze Soulseeku se nedají linkovat, jsou exkluzivně uložená na hard discích uživatelů. Obsah sítě závisí výlučně na tom, kolik uživatelů je připojeno a co sdílejí, data jsou přenášena pouze mezi dvěma uživateli, nikdo jiný už není připojen. Díky tomuto 'introvertnímu' charakteru a specifičnosti obsahu zůstává Soulseek mimo hlavní zájem legislativy i advokátů, kteří obhajují správce autorských práv.

I2P je jeden z mnoha systémů vyvinutých k ochraně před cenuzurou (jiné jsou např. FreeNet a Tor), má velmi malou uživatelskou koumunitu a je zde zmiňován proto, že jej můžete nainstalovat spolu s BitTorrentem.

BITTORRENT

BitTorrent je peer-to-peer (P2P) protokol, který pomáhá přenášet data mezi více uzly/účastníky sítě. Nemá žádné centrální servery nebo rozbočovače (huby), každý uzel dokáže vyměnit data s jakýmkoliv jiným uzlem, klidně mezi stovkami zároveň. Data jsou vyměňována po částech mezi bezpočetnými uzly, umožňují tedy stahovat opravdu rychle (v případě populárního obsahu = velkého množství připojení).

Když užíváš BitTorrent k výměně materiálů, u kterých není jasné, jsou-li na síti legálně či ne, měl bys vědět, že agenti sbírají informace o uživatelích údajně porušujících právo připojením se do torrent swarmu a sledováním a dokumentací chování ostatních peerů. Díky velkému počtu uživatelů je pro orgány činné v trestním řízení složité postihovat každého jednotlivého uživatele – jednoduše nemají zdroje. Každý soudní případ vyžaduje platný důkaz o přenosu dat mezi tvým a jiným klientem (a obvykle důkaz i o uploadu) a stačí, když prokážeš, že se od tebe přenesla pouze část, nikoliv celý soubor, a případ se potáhne velmi dlouho. Pokud se přikláníš k větší opatrnosti, můžeš použít VPN k směrování BitTorrent trafficu.

Leeching (stahování) dat z BitTorrentu začíná s torrent file nebo magnet link. Torrent file je malý datový soubor, který obsahuje informaci o větším souboru, který chceš stáhnout. Torrent file řekne tvému torrent klientovi jména sdílených dat, URL pro tracker a hash kód, což je unikátní kód reprezentující a vytvořený ze základových dat – něco jako katalogové číslo nebo číslo občanského průkazu. Klient použije tento hash k nalezení seederů (uploaderů) souboru, který si chceš stáhnout, a pak můžeš stahovat z jejich počítačů a ověřit pravost dat ve chvíli, kdy dorazí.

Magnet Link se obejde bez torrent souboru, v podstatě je to hyperlink obsahující popis torrentu, který může torrent klient okamžitě začít vyhledávat mezi lidmi jej sdílejícími. Magnet link nevyžaduej tracker, namísto toho závisí na Distributed Hash Table (DHT) a Peer Exchange. Magnet linky nevedou k datům přes místo jejich uložení (například k IP adresám lidí, kteří sdílejí ta která data nebo k URL adresám), ale spíše definuje parametry, dle kterých je hledá. Když je magnet link nahrán, torrent klient vyhledá, zda je dostupný, v podstatě jako by křičel 'má někdo tenhle hash?!'. Torrent klient si pak připojí k uzlu, který odpověděl a

začne stahovat.

BitTorrent používá šifrování pro obranu před poskytovateli a jinými mezičlánky, co by mohli blokovat připojení či slídit v tom, co si právě vyměňujete. Nicméně BitTorrent swarmy (shluky seederů a leecherů) jsou dostupné všem, každý se může připojit a získat informace o všech připojených peerech. Používání magnet linků tě neochrání od toho, abys nebyl vidět ve swarmu; všechny uzly sdílející ta stejná data musí komunikovat mezi sebou a pokud je jeden z uzlů ve swarmu šmírák, může vidět tvou IP adresu. Také může tvému uzlu poslat download request a zjistit tak, zda seeduješ.

Jeden důležitý aspekt užívání BitTorrentu si zaslouží zvláštní zmínku. Každý kus dat, který obdržíš (leech), je okamžitě sdílen (seed) s ostatním uživateli BitTorretu. Tudíž se tak z procesu downloadu stává proces (nedobrovolného) sdílení, je tedy umožněn přístup k datům ještě předtím, než je download kompletní. Zatímco je BitTorrent často užíván ke sdílení volně dostupného a legálního software, filmů, hudby a jiných materiálů, ono 'umožnění přístupu' je velmi kontroverzní a vede k nekonečným bitvám mezi držiteli autorských práv a provozovateli BitTorrentových platforem. Kvůli těmto sporům byl například na základě mezinárodního zatykače vydaného švédskou policií zadržen spoluzakladatel The Pirate Bay, Gottfrid Svartholm.

Z těchto důvodů, vydatně podpořených mediálním tažením kolektivních správců autorských práv, se z užívání BitTorrentu stala prakticky analogie k pirátění. A ačkoliv význam slov jako pirátství, copyright a vlastnictví není v digitálním kontextu ještě úplně jasný, mnoho obyčejných uživatelů BitTorrentu již bylo soudně stíháno za porušování autorských práv.

Mnoho torrentů umožňuje pomocí blacklistů blokovat IP adresu známých copyrightových trollům. Při užívání veřejných torrentů je však lepší připojovat se do uzavřených trackerů nebo se do BitTorrentu připojit přes VPN nebo Tor.

Ve chvíli, kdy máš dojem, že by ses měl obávat o svůj traffic a jeho anonymitu, učiň

následující opatření:

- Zkontroluj, zda torrent klient podporuje peer-blacklisty.
- Zkontroluj, zda je peer-blacklist denně aktualizován.
- Ujisti se, že tvůj klient podporuje všechny nejnovější protokoly – DHT, PEX a Magnet link.
- Vyber si klienta, který podporuje šifrování peerů, a zapni si ho.
- Upgraduj nebo změň klienta ve chvíli, kdy neumožňuje některou z možností výše.
- Používej VPN na skrytí svého BitTorrent trafficu před poskytovatelem připojení. Ujisti se, že poskytovatel VPN umožňuje P2P traffic. Více tipů a doporučení v části Používání VPN.
- Neseeduj ani nestahuj data, o kterých vůbec nic nevíš.
- Buď podezřívavý k vysokým hodnocením a přehnaně pozitivním komentářům u torrent linků.

SOULSEEK

Jako u všech peer-to-peer (P2P) sítí, i zde je obsah vytvářen uživateli klientu Soulseek a tím, co se rozhodnou sdílet. Soulseek obsahuje rozličnou hudbu, od undergroundových a nezávislých umělců, přes nevydané věci – dema, mixy, bootlegy a další. Je plně financován z darů, bez reklam a bez uživatelských poplatků.

"Soulseek neschvaluje ani nepřehlíží sdílení materiálů chráněných autorskými právy. Můžete sdílet a stahovat pouze ta data, kterých jste nabyli legálně, nebo máte souhlas s jejich použitím."

(http://www.soulseekqt.net)

Síť Soulseek závisí na dvou centrálních serverech. Jeden server podporuje původního klienta a síť a další podporuje novější síť. I když jsou tyto servery klíčové pro koordinaci hledání a hostují chaty, v přenosu dat mezi uživateli nehrají žádnou roli, výměna probíhá přímo mezi uživateli.

Uživatel zde může vyhledávat: výsledky se zobrazí jako seznam dat, která odpovídají zadaným názvům. Může se zde vyhledávat konkrétní slovo nebo použít značky pro výběr souborů. Zvláštní funkcí Soulseeku je zahrnutí názvů složek a cest k datům do vyhledávacího listu, to umožňuje uživatelům hledat dle názvů složek.

Seznam výsledků vyhledávání ukazuje plný název a cestu k souboru, velikost, uživatele, který soubor hostuje a jeho průměrnou rychlost přenosu, a v případě mp3 souborů detaily o tracku samotném – bitrate, délka a tak dále. Seznam výsledků vyhledávání může být seřazen mnoha různými způsoby a jednotlivá data (nebo složky) vybrány ke stažení.

Na rozdíl od BitTorrentu, Soulseek nepodporuje vícezdrojové stahování nebo 'swarming' jako jiní post-Napsteroví klienti, soubor se přenáší jen z jednoho zdroje.

Ačkoliv je Soulseek software bezplatný, existuje schéma darů k podpoře jeho programátorů a údržbě serverů. Dárce pak získává jako ocenění privilegium přeskočit ve frontě na stažení ne-dárce (ale jen tehdy, nejsou-li data sdílena přes místní síť). Vyhledávací algoritmus Soulseek protokolu nebyl nikdy zveřejněn a běží pouze na Soulseek serverech. Existují však open source implementace serveru i klienta, jak pro Linux, OS X i Windows.

S ohledem na neveřejný charakter služby i nakladání s autorskými právy je Soulseek poměrně odlišný od BitTorrentu. Jen jednou byl předvolán k soudu (v roce 2008) ale bez jakéhokoliv výsledku. Nejsou zde žádné známky toho, že by uživatelé Soulseeku byli obviňováni z nelegální distribuce materiálů pod copyrightem či jiných zločinů 'digitálního milénia'.

Chceš-li anonymně používat Soulseek, čiň tak přes VPN.

I2P

I2P vznikl z projektu Freenet, původně zamýšleného jako platforma pro necenzurovanou publikaci a distribuci. Z webu I2P:

"I2P vznikl v roce 2003 k podpoře těch, kteří se snažili vybudovat více svobodnou společnost – chce jim nabídnout necenzurovatelný a anonymní systém se zabezpečenou komunikací. I2P je vývojářský nástroj vytvářející low latency, plně rozloženou, autonomní, odstupňovanou, anonymní, pružnou a odolnou a bezpečnou síť. Cíl: úspěšně operovat v nepřátelském prostředí – i ve chvíli, kdy zaútočí nepřítel s velkými finančními rezervami či politickým vlivem. Všechny části sítě jsou open source a dostupné bezplatně, aby se uživatelé mohli ujistit, že software dělá to, co prohlašuje, že dělá, a stejně tak proto, aby každému bylo v zájmu porážky těch, co se snaží umlčet svobodu slova, umožněno podílet se na jeho vylepšování."

(http://www.i2p2.de/)

Pro návod k instalaci a konfiguraci prohlížeče viz kapitola Instalace I2P v části Bezpečné sdílení. Po dokončení instalace se spustí stránka s konzolí obsahující linky na populární stránky a služby. K těmto stránkám (odkazovaným jako eePsites) dostaneš navíc různé aplikace, od blogového nástroje Syndie po build do BitTorrent klientu.

ČÁST PÁTÁ: BEZPEČNÉ HOVORY A SMS

BEZPEČNÉ HOVORY

Telefonní hovory v mobilní síti GSM jsou šifrovány a v běžné telekomunikační síti obsahují jistou formu ochrany před narušením třetí stranou. Nejsou ale zašifrovány úplně a telefonní operátoři navíc mnohdy podléhají nátlaku bezpečnostních složek či vlád, které se čím dál častěji dožadují přístupu k záznamům hovorů. Dodejme ještě, že šifrování používané v technologii GSM již bylo prolomeno a nyní se tedy do hovorů může nabourat kdokoli, kdo má dostatek zájmu a kapitálu k nakoupení nezbytného vybavení. Například GSM Interceptor (http://en.intercept.ws/catalog/2087.html) je volně dostupné zařízení, pomocí kterého lze na krátkou vzdálenost zachytit právě probíhající mobilní hovor. Centralizované služby soukromých společností, jako je Skype, sice též šifrují hovory, ale zároveň v sobě mají zabudovaná zadní vrátka pro případný zájem tajných služeb či vlád. Samozřejmostí pak je fakt, že podléhají příkazům svého vlastníka (v případě Skype je to Microsoft).

Řešení tohoto problému nabízí Internet, který umožňuje hlasový přenos přes IP (VoIP). Pro připojení lze použít jak WiFi, tak mobilní datový přenos: prolomení GSM či hesla tvé bezdrátové sítě v tomto případě neznamená, že bude zachycen také tvůj hovor.

Pokud jde o jednotlivé platformy, širokou škálu open source VoIP software nabízí Android. Důvodem je zejména společnost Apple, respektive podmínky jejího obchodu AppStore, který zakazuje distribuci software vydaného pod General Public License. Pod touto licencí vychází přibližně 60% veškerého open source software a je velmi populární především v komunitách zaměřených na bezpečnost a počítačové sítě (security and networking community).

V době vzniku této příručky měli majitelé iPhonů možnost zakoupit si pouze uzavřený

software jako například Groundwire (http://www.acrobits.cz/11/acrobits-groundwire-for-iphone). Varování: Protože Groundwire není otevřený software, nelze při jeho užívání zaručit bezpečnost!

Uživatelé Androidu se nyní mohou přesunout do části Šifrování hovorů, kde se naučí jak bezpečně volat přes VoIP.

BEZPEČNÉ TEXTOVÉ ZPRÁVY

SMS je služba, pomocí které se mezi mobilními telefony přenáší krátké textové zprávy. Text je odeslán bez šifrování a může být přečten a uložen jak mobilním operátorem, tak i dalšími subjekty, které mají přístup ke tvé síti. Proto pro ochranu svých zpráv před narušením používej v rámci datového přenosu chatový protokol. To naštěstí není příliš složité. Mnoho poskytovatelů dnes používá Extensible Messaging and Presence Protocol (XMPP), díky kterému uživatelé mohou komunikovat i s uživateli jiných programů.

Přestože XMPP pro ochranu před nežádoucím vstupem třetích stran používá šifrování TLS/SSL, poskytovatel stále může zprávu přečíst a předat dalším subjektům. Na druhou stranu, odesílání zpráv mimo záznam (Off-the-Record, OTR) ti umožní své zprávy zašifrovat. Takto odeslané zprávy neobsahují digitální podpis, jehož autentičnost by si pak třetí strana mohla případně ověřit. Díky tomu je identita odesílatele následně nenapadnutelná – upravit zprávu tak, aby vypadala, že pochází od tebe, může po ukončení komunikace v podstatě kdokoli. Naopak, v průběhu komunikace je pravost zprávy zaručena a to, co příjemce zprávy vidí, je tvá autentická a neupravená zpráva.

Více v části Šifrování zpráv.