Nenechat se chytit

Černorudá příručka

★ Nenechat se chytit

Černorudá příručka

Web: https://www.cernorudaprirucka.noblogs.org
Mail: cernoruda-prirucka@riseup.net

OBSAH

1. VSTŘÍC BEZPEČNOSTNÍ KULTUŘE

Navzdory tomu, že jsou za mřížemi naši soudruzi s vykonstruovanými obviněnými, které se vůbec netýkají žhářských útoků Sítě revolučních buněk, můžou si fízlové tleskat. Operace Fénix mnohé paralyzovala. Klopýtáme po klaccích, které nám hodili pod nohy, a vystrašeně se ohlížíme i na ty, kterým jsme donedávna věřili a říkali jim příteli.

Jak jsme se vůbec do tohoto bodu dostali? Je to jednoduché – jednou k tomu muselo dojít. Anarchismus je ze samé své podstaty nelegální. Narušování status quo, zpochybňování existujícího nebo „prosté“ přebrání osudu do vlastních rukou, vzchopení se, vzdor – nic z toho se státu nelíbí. Proto dokud tady bude stát a jeho bezpečnostní složky, dokud tady budou obhájci stávajícího pořádku, vždy budeme v jejich hledáčku. Tu více, tu méně. Být anarchista proto znamená být v permanentním ohrožení a vystavovat se rizikům, která nemůžeme nechat zmizet magickou hůlkou nebo je prostě neřešit. Svět a obzvlášť pak doba, v níž žijeme, to zkrátka nedovoluje.

Tady ale celé představení nemusí skončit. Ano, naši nepřátelé nám vždy půjdou po krku. Ano, naši nepřátelé jsou mocní. To ale neznamená, že bychom měli shrbit záda! Z Fénixu bychom se neměli odnést, že „zlobit“ se nemá. To je přesně to, kde nás chtějí mít. Naopak. Zlobit se má, jen musíme být opatrní!

Často ale nevíme, jak se bezpečně pohybovat po městě; nevíme, co nám hrozí; nevíme, jak něco prakticky provést. Přemáhá nás strach a riziko dopadení se zvyšuje, pokud se vůbec k něčemu odhodláme. S dostatečnými znalostmi ale můžeme strach zmenšit a rizika kontrolovat. Když víme, kde je kamera, jak se ji vyhnout a nezanechat po sobě žádné stopy, máme napůl vyhráno. Jinými slovy čím více známe nepřítele, tím více moci si bereme zpět do vlastních rukou.

To je smyslem následujícího textu – podpořit v nás sebevědomí, zmenšit náš strach a zároveň přiložit další kámen do pevnosti s názvem bezpečnostní kultura. Nejde přitom jen o jednotlivce, důsledný musí být každý jeden z nás. Pokud všichni budeme pevní a důslední, pak se výrazně sníží riziko, že budeme chyceni a nakonec rozbiti jako celek.

Sebrali jsme všemožné návody, manuály, kuchařky a články, které jsme protřídili, aktualizovali a doplnili o vlastní zkušenosti a znalosti. První část podrobně shrnuje jak hlavní nebezpečí, která při akcích hrozí, tak konkrétní návody, jak

některé sabotáže provádět. Vycházeli jsme hlavně z těchto knih: *Ecodefense: A Field Guide to Monkeywrenching* (revidovaná verze 1993), *Ozymandias' Sabotage Handbook*, *The Black Cat Sabotage Handbook* (1996), *Settin Fires With Electrical Timers – ELF Guide* (2001), *Anarchist Cookbook Version 2000*, *Anarchist survival guide for understanding gestapo swine interrogation mind games*.

Druhou polovinu průvodce tvoří kompletní překlad anglické brožury *ANONYMITY/SECURITY*, která se věnuje speciálně počítačům a chování na internetu a kterou doporučujeme všem. I těm, kteří se do sabotáží pouštět nechtějí.

Při čtení měj na mysli, že původním zdrojem byly i staré knihy z 80. a 90. let. Díky rychlosti, s jakou se technologie vyvíjejí, následující informace zastarávají a možná se časem stanou nepoužitelné. Proto je klíčové, aby ses udržoval stále v obraze, rozuměl alespoň základním principům a vypěstoval si v sobě zdravou obezřetnost.

Všechny informace z této brožury by měly být přístupné i na internetu na adrese **https://www.cernorudaprirucka.noblogs.org**. Budu se je snažit aktualizovat nebo doplňovat. Pokud bys chtěl přispět svými zkušenostmi nebo tipem na oblast, kterou je dobré pokrýt, napiš na **cernoruda-prirucka@riseup.net**.

ANONYM

2. PŘÍPRAVA A PLÁN

Tvou alfou a omegou by se mělo stát pravidlo NENECHAT SE CHYTIT. A to nejen na místě činu, ale i po útoku. Informace v této kapitole pocházejí od lidí, kteří studovali policejní techniky a zabývali se metodami a postupy bezpečnostních složek. Neber ji na lehkou váhu. Ve skutečnosti může být tou nejdůležitější kapitolou z celé brožury.

Některé věci ti možná přijdou přehnané a zbytečně se opakující. Je to tak schválně. Smyslem je, aby sis je pomyslně vytesal do kamene, aby se staly běžnou součástí tvého běžného života. S přibývajícími útoky se bezpečností složky vždy pokoušejí sabotéry odhalit a roznést je na kopytech. Čím precizněji budeš, tím hůř se k tobě dostanou.

Hořkou skutečností je, že od publikace jednoho amerického manuálu, ze kterého jsme vycházeli, *Ecodefense: A Field Guide to Monkeywrenching*, bylo pozatýkáno několik známých ochránců přírody, kteří se na jeho tvorbě přímo podíleli. Například Howie Wolde dostal šest měsíců za ničení geodetických tyčí. Veřejně pak prohlásil, že byl neopatrný a z pohodlnosti ustoupil z několika bezpečnostních pravidel. Mezi další zatčené patří Dave Foreman, Peg Miller, Mark Davis… přestože se všichni podíleli na zpracování následujících návodů a tipů, mnohokrát je sami porušili. Nejdi v jejich stopách! Buď důsledný!

PLÁN? A K ČEMU?

Dobrý útok se nesnese jen tak z nebe, základem všeho je plán. Důkladné promyšlení každého kroku celé operace je to, co tě udrží na svobodě, a to proto, že:

- ➔ vybrané místo budeš znát jako své boty a dokážeš se na něj a z něj dostat bez větších potíží
- ➔ budeš vědět, na co útočíš, takže budeš vědět i jaké vybavení si vzít s sebou, takže se zbytečně nebudeš zpomalovat
- ➔ můžeš si zajistit alibi tak, abys nemohl být s činem později spojen.

S plánem jsi prostě efektivnější, rychlejší a tím i nebezpečnější. A pokud se něco pokazí – objeví se hlídač nebo fízlové, spustíš alarm nebo se zraníš a potřebuješ co nejrychleji zmizet, již dopředu víš, jak postupovat.

Proces plánování útoku se dá rozdělit na několik fází. Nejdříve si musíš najít terč útoku a zodpovědět základní otázky, které se ho týkají. Ty totiž ovlivňují vše, co následuje.

VÝBĚR CÍLE

Z pohledu ochránců přírody a bojovníků za práva zvířat (původních autorů velké části tohoto průvodce) jsou cíle, na které se zaměřit, evidentní – kožešinové farmy, masokombináty, firmy převážející živá zvířata, obchody s kožešinami, fabriky znečišťující životní prostředí, těžařské společnosti…

Pro anarchisty je nepřítel čitelný hůře, je všude a nikde. Obecně to jsou socioekonomické vztahy mezi lidmi a stát s represivními složkami, kteří celé soukolí udržují v chodu. To vše přiživují všichni členové společnosti, kteří systém legitimizují. Naneštěstí jak hlásala jedna brožura – sociální vztah do vzduchu nevyhodíš. Škoda. I tak existují lidé a jejich majetek, které můžeme identifikovat. Může být být prohnaný šéf, který soustavně vykořisťuje své zaměstnance, mohou to být konkrétní fízlové, soudci a politici, kteří podněcují nenávist a zatýkají a vraždí naše soudruhy, mohou to být banky soustavně doplňující mazivo do kapitalistického soukolí včetně jejich nejmenších poboček - bankomatů, mohou to být jakékoliv symboly moci, státní či nadnárodní firmy a jejich reklamní poutače, cedule a prosklené výlohy... Nepřítel je všude a nikde. Výběr cíle je na tobě.

Přesto si troufám tvrdit, že nevyvratitelným pravidlem každého anarchisty musí být to, že NIKDY BY NEMĚLI BÝT ZRANĚNI LIDÉ, KTEŘÍ NEMAJÍ S AKCÍ NIC SPOLEČNÉHO!

Pokud uvažuješ o tom, co sabotovat a nikdy jsi nic nedělal, snaž se ignorovat pocit, který tě možná navštíví, že musíš za každou cenu udělat něco velkého a viditelného. Vykrást banku a expropriované peníze poslat dál je úctyhodné, ale i posprejovat blbou stěnu dá zabrat. Abys udělal velký krok, musíš předtím udělat spoustu malých kroků. Chce to čas, trénink a zručnost. Chce to sebevědomí a jistotu, které nenabudeš jinak než tím, že to budeš zkoušet znova a znova. Že budeš testovat své hranice a pomalu je posouvat.

SÁM, NEBO S PARŤÁKEM?

Jedním z mnoha úkolů je rozhodnout se, jestli do akce půjdeš sám, nebo se ti bude hodit pomoc. Pokud se rozhodneš pro druhou možnost, vyvstanou další potíže, které je třeba rozřešit. Když pominu ten nejzásadnější, komu vůbec věřit, tak budete společně muset rozhodnout třeba to, kdo bude dělat rozhodnutí? Kdo se zhostí jakého úkolu? Pokud bude jeden chycen, co udělají ostatní? O tom všem se dozvíš na dalších stranách.

JEDNORÁZOVĚ, NEBO OPAKOVANĚ?

Zamyslet se taky musíš nad tím, co si od útoku slibuješ a jaký dopad bude mít na tvé budoucí možnosti. Jinými slovy kolik příležitostí budeš po prvním útoku mít, aby ses na místo dostal znovu? Na málo střežených místech se ti sice podaří jednou udělat pořádnou neplechu, ale další příležitost nemusíš dostat.

A chceš místo úplně uzavřít, zrušit, zničit, nebo pouze narušit? I to ovlivňuje míru tvého útoku. S tím souvisí i to, jestli je cílem udělat jeden zničující úder na velké ploše, nebo bude lepší škodit trochu tady a pak zase támhle.

VE DNE, NEBO V NOCI?

Pokud půjdeš na věc v noci, asi si na sebe natáhneš tmavé oblečení, zatmavíš si obličej a v ruce poneseš baterku s červeným filtrem. Pokud by ses ale takhle pohyboval ve městě ve dne, asi to nebude ideální volba. Denní doba i roční období mají velký vliv na výběr oblečení a metody útoku. Často je to intuitivní. Pochybuju, že by tě vůbec napadlo pobíhat po městě s kuklou. Abych ale zmínil jednu ne možná úplně zřejmou věc, tak třeba noční operace na venkově se dobře dělají před úplňkem, protože je vidět tak akorát. Za úplňku bývá světla až překvapivě hodně. Pokud ale bude zataženo, může to zhatit celý tvůj plán.

PRŮZKUM OBLASTI

Průzkum oblasti ti dovoluje dostat se na místo, pohybovat se v něm a pak z něj zase odejít, aniž by ses ztratil, zranil nebo se nechal chytit. Na jeho základě navíc nejlépe můžeš zvážit, co si s sebou vzít. Při průzkumu se snaž působit co nejméně nápadně, dávej bedlivý pozor, aby ses neprozradil. V případě, že tě během průzkumu někdo vyruší (např. hlídač nebo zvědavý kolemjdoucí), odlož akci o nějaký čas. Pokud tě po cestě zastaví fízl a bude tě legitimovat, zvaž změnu cíle.

MAPY

Mapy jsou užitečné v tom, že si snadno vytipuješ přístupové a únikové cesty. Cest, jak se dostat z místa, bys měl mít více pro případ, že bys jednu nemohl použít. Na mapách se také lépe všímá širšího okolí, například blízkých řek, lesů, kolejí, dálnic a cest, které mohou být využity pro bezpečný úkryt nebo které naopak představují překážku. Vytipovaná místa si zaznač do mapy a poté

je obhlídni v reálu. Nikdy se nespoléhej jen na mapu, ta ti totiž neřekne nic o kamerách, hlídačích nebo náročnosti terénu. Vždy si projdi cestu fyzicky.

DENNÍ RUTINA

Čím více lidí se na místě pohybuje, čím více lidí v okolí žije, tím spíše bys měl vysledovat, jakým rytmem místo žije. Když ho budeš sledovat týden až dva, dostaneš dobrý obrázek toho, jací lidé se na tam vyskytují, kdy přicházejí a odcházejí apod. Dokonce i na místech, na kterých někdo neustále je, mohou být mezery, kterých můžeš využít.

Pokud děláš průzkum, nikdy nechoď něco očumovat až k plotu nebo si u toho dokonce dělat fotky. K místu se přibližuj obezřetně. Zkontroluj přítomnost poplachových zařízení, kamer, sekuriťáků, hlídacích psů nebo pohybových čidel. Pokud objevíš jakákoli bezpečnostní opatření, budeš následně muset vymyslet, jak se skrze ně dostat. Těchto bezpečnostních zařízení si všímej průběžně i při cestě na místo.

PŘÍSTUPOVÁ A ÚNIKOVÁ CESTA

Neplánuj pouze to, jak se dostat na místo samotné – plánuj celou cestu od bodu, kdy opustíš svůj dům až do chvíle, kdy do něj opět vkročíš. Po cestě je nejlepší úplně se vyhnout takovým místům, která jsou snímané kamerami nebo jsou plošně osvětlené (kamery a světla bys měl zkontrolovat už při předběžném průzkumu). To může někdy znamenat, že půjdeš pěšky několik kilometrů nebo se budeš muset prostříhat několika ploty. Armádní příručky pro příslušníky speciálních jednotek uvádějí jednoduché pravidlo – snadná cesta znamená problém, proto nedbej pohodlnosti a raději si zajdi bezpečnější cestou.

Dovoluje-li to členění terénu, dávám přednost tomu mít odlišnou přístupovou a únikovou cestu – dává to smysl třeba proto, že i kdyby byla moje přístupová cesta, například díra v plotě, odhalena, neznamená to ještě můj konec a pořád můžu utéct. Dobrá přístupová cesta je důležitá obzvlášť tehdy, pohybují-li se okolo nějací lidé a ty bys ji chtěl přitom využít opakovaně. V takovém případě bys měl vymyslet způsob, který nepřiláká pozornost. Pro případ, že se něco pokazí, bys měl mít zajištěnou i alternativní únikovou trasu.

Pokud nepůjdeš na místo pěšky, ale budeš cestovat na kole, autem nebo na motorce, tvůj dopravní prostředek by měl vypadat co nejobyčejněji. Jakékoli zvláštnosti, neobvyklá barva, polepy, lehce zapamatovatelná SPZ jsou nežádoucí, protože přitahují pozornost a utkví snadno v paměti. Na autě by mělo

být vše od blinkrů a pneumatik až po čelní sklo v perfektním stavu, aby fízlové neměli důvod auto zastavovat.

Pokud máš parťáka, který ti dělá řidiče, vždy by tě měl vyhodit a vyzvednout někde úplně jinde, abyste nepřitahovali moc pozornosti. Někdy není žádoucí, abys bouchal dveřmi. Raději je proto jemně přivři tak, aby byly zavřené jen částečně. Řidič je může zavřít později na bezpečném místě.

Když tě řidič vyhodí, hned by měl místo opustit. Aby vyplnil čas čekání, je pravděpodobně nejlepší kroužit po hlavních ulicích nebo dálnicích. Můžete se ale rozhodnout, že řidič zaparkuje a zaparkuje. Ideální je parkovat mimo dosah kamer, což v dnešní době není snadné. Pokud se kamerám nedá vyhnout, je lepší parkovat na rušných místech poblíž restaurace nebo kina a jeho auto splynou s davem. Při používání auta byste se měli vyhnout brzkým ranním hodinám, kdy je dopravní ruch tak malý, že budete vyčnívat. Nejlepší čas pro operaci v městském prostředí je od setmění do půlnoci.

Pokud se spoléháš sám na sebe a své prostředky, zajisti, že tvé odstavené kolo nebo auto nejdou vidět. Na venkově se může vyplatit i investice do kamuflážní plachty, která je k sehnání v army shopech.

JAK SE DOSTAT PŘES PŘEKÁŽKY

Při cestě člověk narazí na spoustu překážek. Mám několik taktik, jak se přes ně dostat:

- ➔ **PLOTY:** Nepřelézej je, ale procházej skrze ně! Pokud máš pákové kleště, nezabere to o moc více času a snížíš riziko, že budeš spatřen. O plotech se dočteš ještě na další straně.

- ➔ **ZDI:** Moc možností nemáš. Mou radou je, že pokud se přes ně můžeš dostat jen s pomocí vybavení (žebřík, lano…), raději se na ně jako na únikové cesty nespoléhej pro případ, že ti třeba někdo odstaví žebřík.

- ➔ **SILNICE:** Snaž se jim vyhýbat a překračuj je výhradně kolmo. Pokud jsou okolo cest živé ploty a zdi , pohybuj se za nimi, dokud se nedostaneš, kam potřebuješ.

- ➔ **PŘÍKOPY A ŘEKY:** Poskytují dobré krytí a dobře se v nich pohybuje, jsou-li vyschlé. Protože se lépe pracuje v suchu, nech si případné překračování řeky, je-li to nutné, až na cestu zpátky.

➔ **BRÁNY:** Pokud nejsou zamknuté, je to v cajku. Pokud zamknuté jsou, budeš k odstranění zámku potřebovat pákové kleště. Nikdy nenechávej přeštípnuté zámky a řetězy na očích, protože je to jasná známka toho, že je někdo uvnitř. Pokud je to možné, dej na místo svůj vlastní, stejně vypadající zámek. Na cestě zpátky se přes něj alespoň dostaneš bez problémů.

➔ **OTEVŘENÁ PROSTRANSTVÍ:** Nejsou bezpečná (co taky je, že?). Otevřeným prostorům se vyhýbej, obzvlášť okolo továren nebo kancelářských budov bývá hodně kamer.

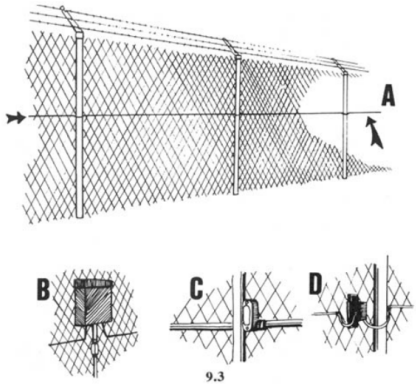
PLOTY

Jak už jsem řekl, ploty je lepší prostříhávat, než přelézat. Na jejich prostříhávání si nikdy nekupuj levné pákové kleště, protože tě vždy potopí, když to nejméně potřebuješ a v půlce cesty se prostě poserou.

Pokud ti záleží na tom, aby nikdo tvou díru nezmerčil, můžeš toto riziko minimalizovat tak, že přeštípneš jen spodní oka, abys mohl plot podlézt. A abys její odhalení ještě oddálil, můžeš s sebou nosit několik kousků drátu, kterým plot znovu přichytíš, aby nevypadal podezřele.

Když prostříháváš plot, používej malé pákové kleště a štípej vertikální drát opakovaně pokaždé, když jde šikmo doleva, nebo doprava (ne oboje) – vznikne ti elegantní díra. Možná budeš muset přestřihnout ještě dolní nebo horní drát.

Dávej si pozor na bezpečnostní ploty, na které je napojený alarm. Může rozsvítit světla, spustit sirénu nebo „nedělat nic“ a přesto potichu informovat vzdálenou bezpečnostní agenturu. Takový plot můžeš odhalit tak, že na místo vstoupíš násilím a pak se v bezpečné vzdálenosti schováš a počkáš. Pokud do půl hodiny až hodiny nikdo nepřijde, měl by být plot v suchu. Na některých plotech jde alarm vidět na první pohled. Jakýkoli tlustší drát připojený k plotu a vedený kousek nad zemí (jako na obrázku A vlevo) může indikovat bezpečnostní systém, který detekuje jak narušení plotu, tak jeho přelezení. Pokud budeš trpělivý, mělo by se ti podařit najít i senzory, které jsou na plotě v pravidelných rozestupech rozmístěné (B, C, D).



9.3

NOČNÍ OPERACE

Jít na věc pod rouškou noci je zpravidla bezpečnější. Pokud plánuješ noční operaci, seznam se s místem ve dne i v noci. Orientační body viditelné ve dne nemusí být vidět v noci, zatímco s některými zabezpečovacími prvky (osvětlení, hlídači…) se nemusíš setkat ve dne.

Předtím, než se vydáš do tmy, nech své oči, aby si na tmu zvykly. Pět minut je nezbytné minimum, půl hodina až hodina je optimální. Měj na paměti, že každý pozdější pohled do světla může tvé noční vidění narušit (vyhni se hlavně výrazným barevným poutačům, jejich vlnová délka je obzvlášť agresivní). Pokud se světlu vyhnout nemůžeš, vždy si jedno oko kryj. Pokud potřebuješ použít svítilnu, můžeš ji oblepit černou páskou a udělat do ni malou dírku. Nápomocný může být i červený filtr nasazený před světlo baterky – červené světlo tak nenarušuje noční vidění a je méně viditelné z dálky. Vždy se navíc snaž očima spíše kroužit po okolí, než zírat na jedno místo. Tvé oči zůstanou více přivyklé tmě.

Jdeš-li pěšky, pohybuj se normální rychlostí a vyhni se běhání. Když budeš zvedat kolena výš než je běžné, minimalizuješ šanci, že zakopneš o kameny, kořeny stromů nebo obrubníky. V lese se hodí mít jednu ruku nataženou před obličejem tak, aby tě nepraštila nějaká větev. Pokud musíš běžet, soustřeď se na zem jen několik kroků před sebou, dokážeš pak snáze zpozorovat výmoly a jiné překážky. Můžeš navíc běžet mírně v podřepu, sice je to docela nepohodlné, ale budeš dělat kratší kroky, které jsou bezpečnější a snáze se kontrolují.

Sluch ti v noci bude pravděpodobně lepším společníkem než oči. Předtím, než vstupuješ na nebezpečné území, vždy se na několik minut zastav a bedlivě naslouchej. Pokud máš kuklu, naneštěstí nebudeš mít sluch tak citlivý. Komunikace mezi členy týmu by měla probíhat gesty rukama. Pokud musíš mluvit, pošeptej to druhému z bezprostřední blízkosti přímo do ucha. V případě nebezpečí, nebo pokud jsou ostatní v nedohlednu, můžete jako signál použít houkání nočních ptáků nebo píšťalku. Všichni by navíc měli být označeni čísly pro případ, že budete na sebe muset křičet. Můžete si vymyslet i falešná jména, ale čísla jsou vhodnější, protože nejsou tak zmatečná.

ZAMĚSTNANCI A HLÍDAČI

Pokud se na místě pohybují lidé, je to samozřejmě problém. Většina hlídačů ale pracuje za minimální mzdu, a tak nemá zrovna velké nadšení pro svou náplň práce. Pokud hlídač pouze sedí ve své budce, nikdy nechodí na obchůzky

a nemá ani kamerový systém, můžeš se dostat dovnitř, nadělat neplechu a docela v klidu se zase dostat ven – musíš jen přizpůsobit své metody tomu, abys byl tichý. Plusem pro tebe je, že hlídání je nudná věc, která po dlouhých hodinách člověku otupuje smysly. Hlídači, kteří mají v plánu zůstat vzhůru celou směnu, proto často sledují televizi, brouzdají po internetu nebo si čtou, což opět znatelně snižuje jejich efektivitu, i když jsou vybavení kamerovým systémem.

Problém obvykle nastane, pokud si nejsi vědom toho, že na místě někdo je, dokud se s ním nesetkáš. Při předběžných průzkumech vždy dávej pozor kdo se kde a kdy vyskytuje. Buď trpělivý. Cigaretový nedopalek nebo šelest ti může napovědět. Pokud si nejsi jistý a nejsi schopný hlídače přesně určit, můžeš ho nalákat třeba na rámus. Vždy si buď ale jistý, že víš kudy utíkat. Pokud používáš k nalákání svítilnu, nezapomeň zavřít oči, abys nepřišel o schopnost vidět ve tmě.

To, že se na tebou vyhlídnutém místě někdo pohybuje, ještě neznamená, že to musíš vzdát. Způsobů je několik: jejich pozornost můžeš dočasně upoutat jinam, to ale nenaskýtá zrovna moc času na práci. V některých případech můžeš vyzkoušet přístup „otravného zvířete“. Ten spočívá v tom, že po dobu několika dnů či týdnů spouštíš alarmy, děláš do plotu díry, ale dovnitř nevkročíš. Hlídače to po určité době dozajista přestane bavit a pak jednou v noci nečekaně zaútočíš.

Počítej ale s tím, že i přes důkladný průzkum můžeš na někoho znenadání narazit. Pokud někoho naneštěstí potkáš, prostě odtamtud vypadni. Nesnaž se ho provokovat nebo konfrontovat. Naprosto nejlepším způsobem je běžet jako o život. Rozumný člověk se zřejmě nebude honit za někým, koho potkal v noci s kladivem nebo páčidlem v ruce. Kdyby se za tebou přesto pustil, snaž se běžet skrčený a s rukou nataženou před sebe. Abys ztížil svému nepříteli pronásledování, můžeš mu posvítit do očí svítilnou se stroboskopickým efektem, kterým ho oslepíš. Jen nezapomeň sám zavřít oči. Ne vždy ale na něco takového máš čas. Pokud nemůžeš utéct, raději to vzdej, protože odpor by ti akorát u soudu přitížil.

VYBAVENÍ

Součástí průzkumu by mělo být co nejpečlivější ohledání toho, co se na místě vyskytuje za vybavení, pokud ho hodláš sabotovat. Všímej si, jakou má konstrukci, jak je navržené, kde má zámky apod. Jedině tak můžeš určit, co si vzít na nářadí a jak ho použít.

OBLEČENÍ

V prvé řadě se vyhni tomu, abys vypadal podezřele. Město, nebo venkov? Noc, nebo den? Roční období? To všechno jsou faktory, které ovlivňují, jaké budeš mít oblečení a jak se budeš chovat. Během dne může být lepší obléct se tak, abys klamal tělem, abys nebyl považován za někoho abnormálního. Pokud se chystáš „pracovat" na staveništi, obleč se jako průměrný dělník do montérek, trička a žluté přilby. Pokud jdeš „pracovat" do kanceláří zmrdského šéfa, hoď na sebe košili a lepší kalhoty. Snaž se zkrátka splynout s okolím.

Během noci je důležité prostě nebýt (moc) vidět. Poblíž měst je i během bezměsíčné noci jen zřídkakdy úplná tma. Černé oblečení proto není vhodné, protože paradoxně proti „tmě" vystupuje. Vhodnější jsou tmavé odstíny modré nebo šedé. Pozornost ve tmě poutá i světlá pokožka – nejčastěji na tváři a pažích. Nevěřil bys, jak září v tlumeném osvětlení obličej. Pokud je pro to vhodná situace, hodí se vzít si kuklu nebo si začernit obličej. Paže zakryj dlouhými rukávy.

Nezapomeň před cestou zkontrolovat, jestli nemáš na oblečení a vybavení reflexní prvky. Pokud máš parťáka, můžete si pomoct navzájem. Obleč se do oblečení, které máš v plánu si na sebe vzít, a požádej kamaráda, aby na tebe za tmy posvítil. Pokud cokoli příliš vystupuje – od zmíněných reflexních prvků po obroučky brýlí a paže – měl by ti o tom říct.

Vyhni se příliš těsnému oblečení, které omezuje pohyb, ale také příliš volnému oblečení, které se zachytává do větví, ostnatého drátu apod. Pokud potřebuješ být opravdu tichý, vyhni se nylonu a umělým látkám, které vydávají šustivé zvuky (a snadno hoří, pozor na to!). Šusťákovky zahoď rovnou. Vlna je tišší než bavlna. Vlněné oblečení na druhou stranu za sebou rádo zanechává vlákna – hlavně když se zachytí do drátu, větví nebo se dokonce jen otře o hrubší stěnu.

TÝM

Jít do akce s dalšíma lidma má své pro i proti. Některé aktivity se dělají dobře o samotě – nekompromituješ sebe ani ostatní, zodpovídáš se jen sám sobě, nemusíš se spoléhat na druhé. Někdy ale může být skupinka dvou až pěti lidí efektivnější. Je mobilnější, protože jeden může dělat řidiče. Může být bezpečnější, protože více očí více vidí. Obvykle je příliš nebezpečné na něčem pracovat a zároveň se pořád ohlížet přes rameno. Někteří navíc uvítají přítomnost někoho, kdo jim dodá odvahu. Na druhou stranu více lidí může zanechat více důkazů a ne vždy se dá každému věřit. Zkušení sabotéři proto často radí pracovat o samotě.

Pokud chceš někoho do party, buď maximálně opatrný, s kým o tom budeš mluvit. Vybírat začni mezi svými přáteli, které znáš dlouho, osobně a víš něco o jejich hodnotách a názorech. I přes to není moudré na ně vybalit vše hned. Buď trpělivý. Pokud se od rozhovorů dostanete dál, začněte s něčím malým a jednoduchým, abyste se sehráli a poznali navzájem své reakce. Nikdy nikomu, ani příteli, v takové situaci neříkej, že už máš něco za sebou, že už máš nějaké zkušenosti! Pokud by na poslední chvíli vycouval, nebude na tebe nic mít.

Měj na mysli, že ne každý se může hodit na aktivity, o kterých uvažuješ. Je potřeba, aby byl schopný fungovat pod velkým stresem (což se zjišťuje bohužel dost těžko, nedojde-li přímo na věc). Vyhni se zbabělcům, nadměrným paranoikům, ne úplně oddaným lidem a těm, kteří si rádi pouští pusu na špacír (což platí mimo jiné pro ty, kteří pijí alkohol – nikdy nevíš, co druhý nebo dokonce ty sám při desátém panáku řeknete). Vyhni se taky povrchním známostem a lidem, kteří jsou hustí a vychloubají se, co všechno už udělali (jak nám ukázal Fénix). Žádný zaručený recept samozřejmě neexistuje, při výběru zkrátka musíš věřit svému úsudku.

Pokud ve svém okolí nemáš nikoho důvěryhodného, je lepší pracovat o samotě a s nikým o svých plánech nemluvit. Každý může být potenciální nepřítel.

MŮŽE TO BÝT AGENT V UTAJENÍ: Agenti provokatéři jsou nasazováni po staletí, aby zahnali do kouta jedince i celé skupiny. Podezřívej každého, koho znáš jen trochu, i když vypadá důvěryhodně a odhodlaně něco dělat. Agenti nejsou ze zákona postižitelní za nic, co udělají, včetně vraždy!

MŮŽE TO BÝT PROSTĚ JEN ČLOVĚK: Člověk, který pod tlakem okolností změní své postoje a udá tě. Jen málokdo je tak silný, aby odolal sofistikovaným výslechům fizlů, všichni navíc v průběhu života měníme své názory, stát se může leccos. Mysli na to. Někteří zkušení sabotéři jsou dokonce proti tomu, aby spolu pracovali partneři. V případě „romantického“ rozchodu se totiž tvůj protějšek může snadněji obrátit proti tobě. Pracovat s partnerem má ale zase velké výhody – komu jinému můžeš věřit tak moc jako jemu? Rozhodnutí je na tobě.

MŮŽE TO BÝT UDAVAČ: Ecodefence brožura tvrdila, že až 90 % zatčení bylo založeno na informacích od udavačů. Jedná se obvykle o jedince, kteří byli „obráceni“ po svém vlastním zatčení a kteří fízlům pomáhají výměnou za vlastní zmírnění trestu a jiné výhody (třeba na operaci THERMCOM, která vedla v Arizoně k zatčení pěti environmentálních aktivistů, se podílel naplno jeden profesionální agent FBI v utajení, několik dalších FBI agentů, kteří se účastnili demonstrací Earth First! a nejméně pět až deset tajných informátorů. Tito lidé byli aktivní mezi lety 1988 a 1989. Agent v utajení byl odhalen až v roce 1992, když mu na demonstraci v Tucsonu vypadla pistole – tzn. tři a půl roku po zatčení Arizonské pětky).

Nejlepší způsob, jak se vyhnout informátorům a udavačům, je spolupracovat v úzkém kruhu přátel, kteří se v ideálním případě znají roky. Ideální počet je čtyři až pět. Takto pevnou skupinu je takřka nemožné infiltrovat. Každý ve skupině by měl plně rozumět tomu, co je třeba udělat, měl by znát časový plán, kódy a posunky, přístupové a únikové cesty atd.

I přes vzájemnou důvěru není záhodno říkat si navzájem úplně vše. Pokud se v pětičlenné skupině dva rozhodnou pro sabotáž, na kterou si bohatě vystačí, je bezpečnější, když to zůstane jen mezi nimi. Pokud se v pětičlenné skupině domlouvá sabotáž a někteří ví, že se ji nezúčastní, měli by ze schůzky odejít. Zkrátka každý člen skupiny by měl vědět jen minimum nutné pro jeho roli. To neznamená, že bys neměl ostatní ani žádat o radu, sdílené zkušenosti jsou naopak velkou výhodou skupiny. Ostatní ale nemusí vědět čas, místo ani konkrétní cíl. Takto ochráníte jak sebe, tak ostatní, protože pokud o něčem nevíte, nemůžete o tom mluvit.

Není na škodu si v takové skupině otevřeně slíbit, že se budete vzájemně chránit a krýt, když se něco posere. Nemusí jít o žádný formální ceremoniál se skotačením kolem ohně za úplňku. Jasně řečený slib, že se neudáte, je totiž psychologicky hodnotnější než pouhý předpoklad, že to všichni máme stejně a nemusíme o tom ani mluvit. Takový moment pak může při výslechu člověku dodat odvahu a jistotu, obzvlášť pokud mu budou fízlové vykládat, jak ho jeho kamarádi vedle v místnosti zrovna udávají.

ROZVRH PRÁCE A NAČASOVÁNÍ

Vždy se řídím rozvrhem práce. Počítám, jak dlouho mi zabere dostat se na vybrané místo, sabotovat každý kus vybavení, odejít z místa a dostat se zpátky domů. I když to může znít až příliš přísně, je to velmi efektivní způsob jak se vycvičit, jak dělat, co jsem přišel dělat a jak rychle vypadnout. Když totiž vezmeme v úvahu policejní hlídky, výměnu hlídačů nebo zajištění vlastního alibi, načasování se stává o to důležitější.

Svůj rozvrh si utvoř několik dnů předem a vryj si jej do paměti. Jakmile pak přijdeš na místo, nebudeš muset ztrácet čas přemýšlením, co máš vlastně dělat. Zkrátka se sebereš a uděláš to, protože ses tak rozhodl předem.

Pokud nepracuješ sám a máš odvoz, je rozvrh práce důležitý mimo jiné kvůli člověku, který tě bude vyzvedávat. Pokud pracuju s někým dalším, vždy určím přesný čas, kdy potřebuju vyzvednout, a vše podřídím tomu, abych to stihl. Když se v průběhu ukáže, že mi cesta na místo zabrala o 10 minut déle, oželím raději jeden bagr, než abych přišel pozdě. Svůj odvoz nikdy nenechávej čekat

nebo nekonečně kroužit okolo, přitahuje to pozornost. Pokud je to možné, vždy si smluvte takové místo, kde můžeš na odvoz čekat, aniž by tě někdo viděl. I to, že někde postáváš, je totiž podezřelé.

CO JE TŘEBA JEŠTĚ ZVÁŽIT

Vždy existuje něco, na co jsi nemyslel. Proto se věnuj i takovým myšlenkám, jako například – co se stane, když ztratím šroubovák? Co udělám, pokud tam nebude to, co chci zničit?

Zvaž také situace, které mohou napomáhat, nebo zabraňovat úderu. Například hluk, který bys dělal, je problematický. Ale ne už tolik, pokud jej děláš uprostřed bouřky, kdy zvuk větru a padajícího deště dost ruchů schová. Podobně může úder vyžadovat dlouhé cestování, které jde nejlépe při svitu měsíce. Pokud je ale zataženo, budeš to asi muset vzdát. Nejlepší způsob, jak se s podobnými situacemi vypořádat, je vyhradit si ve svém plánu nějaký čas navíc.

3. CO TĚ MŮŽE DOSTAT ZA MŘÍŽE
(NEZBYTNÉ MINIMUM)

Pokud děláš prvotní průzkum řádně a sleduješ pozice bezpečnostních systémů, blízkého okolí a lidí, kteří se na místě vyskytují, měl bys být schopný snížit riziko, že tě někdo na místě potká nebo tě zpětně identifikuje, na minimum. Odstranit zcela je ale nemůžeš hlavně kvůli neočekávaným událostem.

Pokud se ti zadařilo a nechytili tě přímo na místě, pořád nemáš vyhráno. Nejsme nevystopovatelní duchové, ale zranitelní lidé z masa a kostí, kteří za sebou neustále zanechávají jen těžko smazatelnou stopu. Nepřítel má k dispozici neuvěřitelný arzenál techniky, která nás může usvědčit. Přemýšlej. Délka tvého kroku je důkaz. Tvá krev je důkaz. Výpověď svědka je důkaz. Kamerový záznam je důkaz… Obecná pravidla bezpečnosti proto jsou:

- ➔ Nic na místě činu nenechej
- ➔ Nic si z místa činu neber

Oboje tě totiž může později s útokem spojit. A nikdy nemluv s lidmi (jakkoli dlouho je znáš) o věcech, o kterých nemusí vědět.

OTISKY PRSTŮ

Otisky prstů jsou v klasických detektivkách hlavním důkazním materiálem. Je to proto, že jsou nesmírně přesné a v kombinaci s pokročilými technologiemi a přístupem k obrovským databázím dávají fízlům značnou moc. Proto by ses měl vyvarovat tomu dotýkat se jakýchkoli předmětů, aniž bys měl chráněné ruce.

Všechny své nástroje musíš před úderem zbavit jakýchkoli náhodných otisků, nejlépe je očisti lihem. Zaměř se i na takové části, jako je sklíčko svítilny, žárovka nebo baterie. Jakmile to uděláš, už se jich nesmíš dotknout jinak než s rukavicemi. Já si rukavice nasazuji zpravidla ve chvíli, kdy na místo vcházím a sundávám si je, když odcházím. Když jsi na místě, za žádných okolností si už rukavice nesundávej. Rukavice by proto měly být pohodlné, aby se ti v nich dobře pracovalo a mohl jsi je nosit dlouho.

Pokud pracuješ přes den a vypadalo by podezřele nosit rukavice, můžeš se vyhnout zanechání otisků tak, že přetřeš bříška prstů průhledným lakem na nehty. V takovém případě měj při sobě pro jistotu i odlakovač.

OTISKY BOT

Pamatuj, že tvé boty zanechávají otisky, které říkají víc než jen to, jakou máš velikost nohy. Dají se z nich vyčíst tvé fyzické proporce, jako je váha, výška nebo styl chůze. Nebezpečné nejsou jen očividné a na první pohled viditelné stopy v blátě, ale i latentní otisky, které se snímají podobně jako otisky prstů. Respektive většina bot je nějak pogumovaná a hlavně na hladkých površích, jako je linoleum, dlaždice, parkety apod. zanechává otisk, který se při malém množství vlhkosti může chovat podobně jako otisk prstu. Takové latentní otisky je ale snadné poničit a nevím, jak často se používají jako důkaz.

Levné boty, které hned po útoku můžeš zahodit, jsou ideální. Taky si můžeš koupit pár bot o několik čísel větší, než běžně nosíš, a prázdné místo vyplnit ponožkama. Zmateš tak trochu nepřítele. Dražší boty, které je ti líto vyhodit, můžeš překrýt velkýma ponožkama. Pro jistotu měj s sebou náhradní pár pro případ, že bys jedny prošoupal – to hrozí hlavně v náročném, kamenitém terénu. Pamatuj ale, že by tě nikdy takové opatření neměly omezovat v pohybu!

DNA

Stopy DNA je možné získat takřka z jakékoli části těla – z krve, vlasů, kůže… proto na sebe musíš být extrémně opatrný. Pokud se řízneš nebo šbrábneš, měl bys u sebe mít náplast, kterou krvácení okamžitě zastavíš a ránu překryješ, jakkoli se zdá být malá a nevýznamná. Měl by ses taky pokusit očistit to, co tě zranilo, protože na tom zůstanou stopy tvé kůže a krve, i když je nevidíš. Pokud se zraníš vážněji a krvácíš, měl bys místo okamžitě opustit.

Pokud máš dlouhé vlasy – jinými slovy pokud nejsi na skina – vždy by sis měl hlavu chránit šátkem nebo čepicí, abys za sebou vlasy nenechával nebo se nezachytával do plotů, částí strojů apod.

Oblečení, které máš na sobě, taktéž nese stopy tvého DNA z kůže a vlasů, případně se z něj dají dostat pachové stopy. Pokud tvoje oblečení najdou, identifikují tě. I proto je dobré skladovat nářadí a oblečení odděleně. I kdyby totiž našla tvou skrýš na oblečení, nebudou mít nářadí, které by tě spojovalo s konkrétní akcí. Nejlepší ovšem je oblečení co nejdříve po akci zničit.

FORENZNÍ VĚDA

Forenzní věda vpravdě nahání hrůzu. Například pokud přeřežeš hadici, zůstane na ni z tvého nože stopa toho konkrétního kovu, ze kterého byl vyrobený, nehledě na typ čepele apod. Z těchto malých stop je pak možné zhruba určit typ použitého nářadí a tím pádem zúžit hledané předměty. A stejně tak na tvém noži zůstane hydraulická kapalina, benzín, olej nebo cokoli dalšího, s čím se setkal během používání. Specifické složení těchto látek pak může zase spojit tvůj nůž s konkrétním místem a činem.

„Měkké“ materiály, jako je oblečení, z okolí snadno sbírají kontaminující látky. To funguje dvěma způsoby. Oblečení, které jsi měl na místě činu, může zachycovat stopy, špínu a další materiál, který zůstává v tkanině látky často i potom, co jsi ho vypral. To tě může spojit s místem činu. Například pokud tvé kroky vedly přes rozkvetlou louku, pravděpodobně si s sebou odneseš sadu pylu, která je specifická právě pro tuto konkrétní louku nedaleko místa činu. Také pokud máš své oblečení dlouho předtím, než se dostaneš na místo, může na sebe zachytit třeba specifickou špínu a prach z tvé domácí pracovny. Pak tě opět jakýkoli utržený kousek látky zanechaný na místě může s místem spojit.

Jinou možností je, že sis možná připravil některé vybavení doma – například že jsi přesypal brusný prach z původního obalu do náhradního. Pokud ti pak někdo doslova vyluxuje byt – a věř, že to udělají, pokud jsi hlavním podezřelým – pak s největší pravděpodobností najdou ve vysátém bordelu i brusný prach. Pozdější analýza prachu a jeho velikosti tě může spojit s tím, který byl nalezený ve zničeném bagru.

SVĚDCI

Jednou tě někdo někde a někdy určitě uvidí. To samo o sobě ještě nemusí být problém. Lidé tě mohou vidět, problém nastává až ve chvíli, kdy si tě všimnou, kdy tě zaznamenají jako něco zvláštního a utkvíš jim v paměti. S pečlivým plánem se ale toto riziko zmenšuje.

Problém nastává hlavně, chceš-li se někam dostat nepozorovaně. Pokud je to možné, nevydávej se na místo cestou, která je s ním přímo spojená. Pokud bych si měl vybrat mezi dlážděnou cestičkou nebo pětikilometrovou trekovou obchůzkou, vyberu si obchůzku. Na druhou stranu v počtech je síla – pokud děláš něco během dne nebo na místech, kde se pohybuje hodně lidí, pak tě dav může schovat. Velké množství lidí výrazně stěžuje schopnost jiných lidí nebo kamer jasně identifikovat jednotlivce.

Obecným pravidlem je, že se musíš vyhnout tomu, abys vypadal nevhodně, podivně nebo neočekávaně. Jak je to jen možné, snaž se působit normálně. Pokud s tím máš problém, zamaskuj se tak, že zakryješ své hlavní rysy – vlasy, barvu očí, jizvy a mateřská znaménka, tetování a především svůj hlas či akcent.

Další úkolem je zamaskovat odvoz. Osamělé auto projíždějící Horní Dolní a přilehlé polní cestičky určitě někdo zpozoruje. A pokud fízlové natrefí na osaměle stojící auto, pravděpodobně alespoň zkontrolují SPZ, jestli náhodou nebylo kradené – což je údaj, který zůstane v systému a může tě zpětně ohrozit.

ZÁZNAMY A POZNÁMKY

Zaprvé vše, co sis v posledních letech kupoval, půjčoval nebo vyhledával, se někde eviduje. Proto nikdy nekupuj nic kompromitujícího, jako je třeba nářadí, na internetu a nikdy neplať kartou. Vždy plať v hotovosti a všech účtenek a dokladů se ihned bezpečně zbavuj (to znamená nevyhazuj je doma do koše).

Další problém představuje získávání informací o zamýšleném útoku. V devadesátkách manuály radily, aby sis nikdy nepůjčoval v knihovně knihy spojené s konkrétním místem, metodou nebo strojem, který chceš zničit. Dnes se tato rada týká spíše vyhledávání na internetu, které je kapitolou sama o sobě a více se mu věnuje druhá polovina průvodce.

Poslední rada se týká map a poznámek – nejlepší je, pokud je k útoku nepotřebuješ. Pokud se bez nich neobejdeš, bezpodmínečně vše pečlivě znič ještě před započetím. Papír je nejlepší spálit – nejlépe každý papír zvlášť, a ne na hromádce, protože při větším množství se nemusí vnitřní listy spálit úplně. Pokud jsi venku, můžeš popel polít vodou, zaházet hlínou a rozmělnit. Pokud jsi doma, můžeš vše spálit v záchodové míse a popel spláchnout. Pokud poznámky potřebuješ při samotném útoku, měj je napsané tužkou na cigaretovém papírku. Ten se dá v případě nebezpečí snadno sníst nebo zabalit do kuličky a odhodit.

PACHOVÉ STOPY

Každý člověk vydává pach, který je natolik specifický, že je spjatý právě a jedině s ním. Vždy, když se něčeho dotkneš nebo když se někde zdržuješ, tak po sobě pachové stopy zanecháváš, protože na povrchu věcí ulpívá tvůj pot nebo „ztrácíš“ šupinky kůže. Ačkoli jsou pachové stopy považovány za nepřímý důkaz a fízlové potřebují přijít ještě s něčím jiným, co tě usvědčí, rozhodně bys měl na tento druh stop myslet.

Důležité je, že pachová stopa na místě vydrží hodiny, maximálně dny pokud jsou dobré podmínky, a nedá se nijak zakrýt nebo přebít jinými pachy. Voňavka možná funguje ve filmech, ale v reálném světě ti nepomůže. Co ti však pomůže, je mít stále nasazené rukavice a dbát na to, aby ses ničeho nedotýkal kůží. Proti šupinkám kůže a lupům zase pomůže čepice a oblečení s dlouhými rukávy. Pokud se pohybuješ v uzavřených prostorech, je lepší zkrátit tam pobyt na minimum, protože se tam pachové stopy udrží déle, než venku.

JAK SETŘÁST STOPOVACÍ PSY

Následující řádky jsou zde předně pro zajímavost a pro rozšíření představy o tom, s jakým nepřítelem máš tu čest. Nasazení policejních psů nelze nikdy vyloučit, proto je dobré zahrnout nějaké pasivní způsoby obrany do případného plánu akce. Nejdůležitějším faktorem však stále zůstává obezřetnost při manipulaci s jakýmikoliv předměty. Pokud necháš na zemi kleště nebo svůj svetr, policejní pes je nejmenší problém. I když i ten dovede celou situaci ještě zhoršit.

Dobře trénovaný pes je tuhý soupeř, má ale své limity. Jako při sledování lidmi, tak i v případě psů je nejlepší pohybovat se rychle a zvětšovat náskok. Sledovací psi mohou sledovat pach na zemi – jak čerstvý lidský pach (který vydrží prvních několik hodin), tak pach pošlapané vegetace a narušené půdy (která vydrží déle).

Mohou také sledovat pachové stopy ve vzduchu. Pach ve vzduchu se udržuje v klidném počasí a usazuje se v nízko položených místech jako jsou příkopy. Psi mohou rozlišovat pachy různých lidí. Proto i když se kladivo na místě činu dostalo do styku s několika lidmi, přesto může být zpětně spojeno s tebou, protože tě pes identifikuje. Proto na místě nikdy nic nenechávej!

Většina psů dokáže držet stopu, která není stará více než 24 hodin (rekord je přes 100 hodin). Tady je několik způsobů, které mohou psům stopování ztížit:

- ➔ Opouštěj místo činu skrze místo, které bude pravděpodobně „kontaminováno“ prvními lidmi, kteří ráno přijdou do práce. Když tvůj pach překrývají jiné pachy, pes většinou neví, po které z nich se vydat.

- ➔ Neztrať žádnou věc, jako je oblečení nebo nářadí. Pokud se musíš zbavit inkriminujících předmětů, odhoď je daleko od cesty, po které jdeš, preferovaně do hustého křoví, hluboké vody nebo z vysokého srázu.

- ➔ Jdi po silnici (je-li to bezpečné), kde pachy zanechané projíždějícími auty jednak rozptýlí tvůj pach a jednak ho zamaskují.

➔ Procházej nechráněnými, větrnými místy (je-li to bezpečné), kde vítr tvůj pach rozfouká.

➔ Procházej skrz místa, kam dopadá přímé slunečné světlo. To totiž zabíjí bakterie, které produkují pach.

➔ Jdi po suchém písku nebo štěrku (obsahují méně bakterií, které by umocnily stopu), spíše než po bohatém humusu nebo hustou vegetací, které skýtají pro sledovací psy ideální podmínky.

➔ Kontaminuj své stopy červeným pepřem nebo pepřovým sprejem a benzínem. Ty údajně nedělají psímu nosu dobře. To neznamená, že přebiješ svůj pach nebo ho dokonce odstraníš, akorát pes nebude tak efektivní, protože to naruší jeho čich.

➔ Procházej po tvrdých površích, které mohou psa zranit nebo zpomalit.

➔ Měň směr v ostrých úhlech, ideálně jdi chvíli po svých stopách zpátky. Měň také směr v místech, které například prudce sestupují a kde rychlost psa a jeho setrvačnost způsobí, že změnu směru přejde. I když se pes nakonec zřejmě znovu chytí, psovod může být poněkud překvapený. Pokud je to možné, měň směr chůzí s větrem. Tímto způsobem vítr nezanese tvůj pach ke starším stopám.

➔ Předtím, než změníš směr, choď sem a tam a křižuj stopy, které už jsi udělal, z ze strany na stranu. Představ si, jak bude pes zmatený a jak se bude psovod asi tvářit, kdy ho pes bude tahat sem a tam. Pes nakonec opět možná zachytí tvou stopu, ale psovod si může myslet, že pes ztratil stopu a vrhl se na novou. Tohle opakuj pokaždé, když měníš směr. Průměrný psovod může nakonec předpokládat, že pes ztratil stopu a ukončí hledání.

JAK SE ZBAVIT DŮKAZŮ

Důkazem může být kdeco – oblečení, které jsi měl na sobě a nářadí, které jsi použil. Tiskárna, na které jsi tisknul propagandistický leták nebo počítač, na kterém je zalogováno vše, co jsi na něm kdy dělal. Nejlepší je se všech nebezpečných věcí ihned po akcích zbavovat. V některých případech to neplatí. Pokud je nářadí, které jsi používal, těžko vystopovatelné a snadno nahraditelné, může být lepší nechat ho poblíž místa činu (ne však na očích přímo vedle zničeného auta – takový předmět může nést tvé pachové stopy, které mohou psům posloužit k stopování), než riskovat, že tě s ním někdo chytí.

Pokud proběhla razie ve tvém okolí nebo tě přímo sebrali k výslechu, ale neudělali domovní prohlídku, udělej doma pro jistotu velký úklid a všeho problematického se zbav. Nikdy nevíš, kdy si pro tebe můžou přijít, kdy se jim podaří získat dost důkazů, aby s četou navštívili i tebe. Buď připravený předem.

Je několik možností, jak se věcí zbavit:

- ➔ Můžeš je prostě vyhodit do popelnice. Samozřejmě by to neměla být popelnice před tvým domem, ani ve vedlejší ulici a všechny věci by měly být zbavené otisků prstů. Bezpečnější je věci rozdělit na části a rozházet je do různých od sebe vzdálených kontejnerů, ideálně těsně předtím, než je vyvezou popeláři.

- ➔ Pokud to okolnosti dovolují, je lepší papír a oblečení spálit. Okolnostma myslím to, že bys neměl táborákem přitahovat zbytečnou pozornost. Vše se snaž spálit pokud možno úplně a popel pak rozmělnit, polít vodou, zahrabat…

- ➔ Některé věci můžeš zahodit do vody. Ujistit se, že je voda dostatečně hluboká na to, aby za dne nebylo vidět na dno. Tma je matoucí. Nevyhazuj proto nic inkriminujícího v noci do vody, kterou neznáš.

- ➔ Něco zase můžeš zakopat. V takovém případě by mělo jít o místo, kde tě někdo může zpozorovat jedině, když přijde dostatečně blízko. V hlubokém lese uprostřed houští to nemusí být zlé. Taky mysli na to, že vystoupit z auta s lopatou přes rameno je podezřelé. Používej raději skládací náčiní, které se ti vleze do batohu. A nikdy věci nezakopávej u sebe na zahradě nebo u známého.

- ➔ Pokud jsi použil auto, většinou bys ho měl po akci pečlivě vyčistit. Špína, prach a kameny se můžou dostat takřka kamkoli, obzvlášť pokud jsi cestoval po lesních cestách. Vnitřek auta vysaj, zvláštní pozornost věnuj podlaze, kde se usazuje špína z bot. Vnějšek auta umyj, a to nejlépe vícekrát. Neměl bys vynechat žádné škvíry, spodek karoserie, pneumatiky a jiné místa, kde se rády usazují nečistoty. Zvaž, že vyměníš vzduchový filtr. To vše dělej nejlépe na nějakém komerčním místě, kde nemusíš řešit výměnu sáčků do vysavače a kde je k dispozici vysokotlaká vodní pistole. Neměl bys ale zase působit příliš podezřele.

- ➔ A poslední rada – pamatuj, že cena nového vybavení je daleko menší než jakékoli soudní výlohy, které bys musel v případě zadržení platit.

NEBEZPEČÍ RUTINY

Ze způsobu, jakým právě píšu (nebo překládám) tento text, jaká slova a slovní spojení používám, si o mě mohou bezpečnostní složky udělat docela dobrý „psychologický profil“. Pokud by navíc měli k dispozici jiné věci ode mě, křížovým porovnáním by mohli snadno odhalit mou identitu. Něčemu takovému se předchází těžko.

A stejné je to se samotným úderem – tvůj pracovní postup tě může odhalit. To, že něco ovládáš, je sice dobré v tom, že nemusíš dělat chyby a cítíš se jistěji. Nevýhodou je, že nepřítel může být pro příště obezřetnější a může ti, pokud tě chytí, přišít i další případy. Proto bys měl svůj postup a metody měnit. Neznamená to, že tě nechytí. Ale může tě to ochránit před tím, aby tě spojili s jinými útoky.

Můžeš měnit své cíle – auta fízlů, plánovaná stavba supermarketu, norková farma, mýtná brána, ambasáda, soukromá firma, znečišťující továrna… Měnit můžeš i techniky – zapalování, sabotáž pracovních strojů, osvobození zvířat, zkratování, Molotovy, ucpání odpadních trubek… Tím, že obměňuješ neustále svůj postup, místo činu, přístupové cesty, tím nepřítele mateš. Co je ale hlavní, nemusí být schopni tě spojit s každým útokem, který jsi kdy udělal.

4. NÁŘADÍ

NA CO JE NÁŘADÍ DOBRÉ?

Nářadí je prostředek, který nám pomáhá na cestě k cíli. Pokud bych chtěl zatlouct do prkna hřebík, použiju spíše kladivo než svou hlavu. Podobně pokud budu chtít prorazit palivovou nádrž, abych vyhodil bagr do povětří (což je snazší způsob, než se snažit zámek ze zamčené nádrže dostat kladivem), použiju důlčík. Pouze pekelné nástroje Babylonu mohou Babylon svrhnout!

Takže co potřebuješ? První otázku, kterou by sis měl klást, je, co se chystám udělat? Odpověď na ni určuje, jaké vybavení budeš potřebovat:

- ➔ Na lehké večerní potěšení si vystačíš s lepidlem, kladivem, dlátem a francouzským klíčem, které dokážou i tak napáchat velkou škodu.
- ➔ Pro významnější cíl si dopředu přichystej přesný plán, rozvrhni si práci na přesně načasované jednotky a s sebou nes jen to vybavení, které potřebuješ, abys dosáhl vytyčených cílů v určeném čase.

JAK NÁŘADÍ ORGANIZOVAT (JEŠTĚ TROCHA BEZPEČNOSTI)

Nářadí musí být takové, aby:

- ➔ kvalitou odpovídalo cílům
- ➔ bylo neidentifikovatelné v případě ztráty
- ➔ bylo jednorázové v případě, že bude odhaleno nebo bude nutné z místa ihned zmizet
- ➔ bylo výhradně určené pro sabotáže – nikdy své pracovní nářadí nepoužívej v běžném životě nebo si ho nenechávej doma

Poslední bod je, myslím, nejdůležitější. Dnešní forenzní věda dokáže obdivuhodné věci. Může srovnat hydraulickou kapalinu na tvých pákových kleštích s kapalinou poškozeného bagru. Dokáže srovnat chemické složení tvých imbusových klíčů se stopami kovu na odstraněném šroubu.

Proto si NIKDY – NIKDY – NIKDY nenechávej použité nářadí doma. Měl by sis pro ně najít bezpečný úkryt, nejlépe mimo dohled veřejnosti, ale zato

s přístupem, který bude snadný a nebude podezřelý (v praxi bohužel zjistíš, že je to takřka nemožné a mnohdy i nepraktické, protože máš naráz omezené možnosti, musíš všemu věnovat více času apod. I tak se snaž!). Stejně bys měl naložit s oblečením, obuví a rukavicemi. Cokoli, co by tě mohlo spojovat s místem činu – s výjimkou tvého vlastního těla, které si po každé akci řádně vydrhni – bys měl ukrýt.

Pokud je to možné a dovolují to tvé finance, zajisti si více úkrytů, každý s vlastní sadou nářadí. Poté, co nářadí použiješ, by ses k úkrytu neměl vracet dřív než za jeden až tři týdny, případně až šest týdnů v případě, že akce vyvolala rozruch.

Vybavení může být uchováváno několika způsoby:

- ➔ zahrabáno v plastovém pytli
- ➔ uloženo do vzducho a vodotěsného kontejneru a poté zahrabáno nebo ukryto „nad zemí“
- ➔ uzamčeno ve staré garáži, opuštěné budově nebo stodole
- ➔ uchováno způsobem „jehly v kupce sena“ – tzn. na místě, kde už je spousta jiného náčiní

Nářadí by mělo být uchováváno v suchu nebo v naolejovaných hadrech, které zabrání vzniku rzi. Chemikálie je potřeba skladovat v těsnících nádobách, které nebudou korodovat. Oblečení, pokud ho používáš opakovaně (což nedoporučuju), je zase potřeba mít ve vzducho a vodotěsných obalech.

Vsuvka: *„Neměj všechny vejce v jednom košíku“*, neboli pokud je to jen trochu možné, měj několik úkrytů v jedné malé oblasti, abys minimalizoval ztráty, pokud bude jeden z tvých úkrytů objeven.

V případě nářadí je klíčové zajistit, aby bylo nevystopovatelné. Pokud si musíš nářadí koupit, vždy plať hotově. Nikdy si ho neobjednávej před internet. Pokud je to možné, kupuj si ho co nejdále od místa, kde bydlíš, nejlépe v úplně jiném městě a pokud možno v nějakých výprodejích a akcích, ve kterých se tvůj nákup ztratí mezi ostatními. Nikdy nenakupuj vzorově jako bys chtěl vařit podle receptu – pokud si do košíku hodíš tři pytle hnojiva, pytel moučkového cukru a krabici uhlí a o pár dnů později chemický oheň pohltí šest JCB, tak bude docela očividné, kdo to asi udělal. Rozděl si proto své nákupy na různá místa, věci kupuj odděleně, a pokud je to možné, tak i s časovými odstupy. A tak jako v případě skladování nářadí, není-li to nevyhnutelné, nikdy si neber opravdu inkriminující důkazy s sebou domů (*„Promiňte pane, co ve vašich účtech dělá kapesní svařovací hořák a pár pákových kleští?“*).

ZÁKLADNÍ SOUBOR NÁSTROJŮ

Pokud chceš udělat jen pár nepříjemností, pak bych navrhoval následující:

- ➔ 1x dvoukilové kladivo
- ➔ 3 tuby vteřinového lepidla
- ➔ brusný prach nebo písek
- ➔ 1x stavitelný klíč
- ➔ 1x dláto (2,5 cm široké)
- ➔ 1x páčidlo
- ➔ 1x štípačky
- ➔ 3 různě velké ploché šroubováky
- ➔ 3 různě velké křížové šroubováky

Zde je seznam toho, s čím můžeš začít:

- ➔ **OBLEČENÍ:** Pokud je to možné, nevracej se domů v tom oblečení, ve kterém jsi pracoval. Forenzní testy dokážou zachytit například hydraulický olej i na oblečení, které bylo vyprané. Vezmi si náhradní oblečení a vodu a mýdlo na umytí, svleč se, smyj ze sebe všechen olej, mazivo nebo prach a pak použité oblečení ukryj. Čisté oblečení si oblíkni až na úplný konec, když odcházíš.

- ➔ **RUKAVICE:** Ne gumové jako ve filmech, ale pevné, které nepropíchneš. Pokud se pořežeš a zakrvácíš místo činu, může policie udělat testy DNA, přidat je do databáze a někdy v budoucnu tě zpětně spojit s konkrétním činem, což nechceš.

- ➔ **KRABIČKA PRVNÍ POMOCI:** Náplast, obinadlo, obvaz na popáleniny, dezinfekční utěrky a destilovaná voda a sluneční brýle pro případ, že se ti do očí dostanou nějaké úlomky nebo olej.

- ➔ **SVÍTILNA:** Hodí se menší svítilna zakrytá tmavým červeným filtrem nebo přelepená elektrikářskou páskou s malou dírkou, aby světlo nepoutalo tolik pozornosti a nenarušovali ti noční vidění.

- ➔ **PÍŠŤALKA:** Ta se hodí jen, když je vás více nebo když má někdo výhled na okolí. I ty nejlepší plány se mohou dostat do průšvihu, proto si určete houkání/pískání/křik, kterým spolu budete komunikovat.

- ➔ **OCHRANNÉ BRÝLE:** Pokud něco přeřezáváš, navrtáváš, vytloukáš, vždy bys měl mít na očích brýle.

➔ **POŘÁDNÉ PÁKOVÉ KLEŠTĚ:** Nejlepší jsou kleště z tvrzené oceli. Dají se použít na všelicos, třeba na ničení tenčích trubek, kabelů a pletiva.

➔ **FRANCOUZSKÝ KLÍČ:** Nosit s sebou několik klíčů je těžké a hlučné. Francouzský klíč, což jsou vlastně kleště s proměnnou velikostí úchopu, které se dají zaaretovat, řeší tento problém. Je-li to možné, ber si s sebou to nářadí, které je schopné chytnou třícentimetrový šroub (velikost mnoha šroubů na JCB strojích). Pokud se budeš pouštět do benzínových motorů, bude se ti hodit klíč na zapalovací svíčky.

➔ **MALÁ PILKA NA KOV:** Většinu práce zastanou pákové kleště, pokud se ale setkáš s tvrzenými tyčemi, mřížemi apod., je malá pilka na kov nezbytná.

➔ **ŠROUBOVÁKY:** S sebou si beru čtyři až šest šroubováků. Standardně malý (3 mm), střední (5 mm) a velký (10 mm), křížový a plochý. Alternativně je možné koupit multišroubovák, který má jedno tělo, do kterého nasazuješ různě velké bity. Nasadit se na něj dají i jiné nástroje jako imbusové a nástrčkové klíče. Ve tmě je ale výměna bitů zaolejovanýma rukama zdlouhavá.

➔ **MALÁ RUČNÍ VRTAČKA:** Většina hydraulického vedení na strojích Cat a JCB jsou vyztužené kovaným, flexibilním, spirálovým pouzdrem. To ztěžuje jejich narušení. Nicméně malý, ocelový vrták (ne s průměrem větším než 0,4 cm), dokáže prorazit obal docela rychle. S sebou si budeš muset vzít několik náhradních bitů, protože se otupí po pěti až šesti použitích.

➔ **SADA IMBUSOVÝCH KLÍČŮ:** Imbusové neboli šestihranné klíče se ve strojírenství používají často. Opět vybírej kvalitní kusy.

➔ **OSTRÉ A TUPÉ DLÁTO:** Dláta mají různorodé využití od rozsekávání hadic (ostré dláto) až po prorážení drátěných sít benzinových filtrů a kalových plnicích trubek (tupé dláto).

➔ **DVOUKILOVÉ KLADIVO:** Hodit se bude každé kladivo, ale zrovna dvoukilové skýtá dobrý poměr váhy a efektivní síly. V praxi kladivo zas tak často nepoužiješ, protože je moc hlučné.

➔ **PÁČIDLO:** Páčidlo je jedna z nejužitečnějších věcí. Krom páčení uzavřených věcí se díky své délce stává skvělým „dlouhým dlátem“, kterým můžeš udělat škodu i ve špatně přístupných místech. Navíc pokud ho budeš držet za špičatý konec, dostaneš docela dobré lehké kladivo.

➔ **VTEŘINOVÉ LEPIDLO:** Na malé nebo střední staveniště si vystačíš s třemi nebo čtyřmi pětigramovými tubami vteřinového (kyanoakrylátového)

lepidla. Vteřinové lepidlo nejlépe funguje v malých dutinách nebo mezi dvěma na těsno dosedajícími povrchy (např. zámky, vypínače, páky). Na větší dutiny (zásuvky, karburátor atd.) použij raději rychleschnoucí dvousložkové epoxidové lepidlo nebo lepidla a tmely ve větších tubách. K těm budeš potřebovat i pistoli.

➔ **SEŠÍVACÍ PISTOLE:** Elektrické kabely nepracují zrovna nejlépe, pokud v sobě mají deset až dvacet kovových skob. Nejlepší sešívací pistole jsou ty, které se používají v čalounictví.

➔ **TMEL A TĚSNICÍ PRYSKYŘICE:** Prodávají se v tubách a používají se k utěsňování škvír okolo okenních a dveřních rámů. Těsnící pěna nastříkaná do alarmů a sirén zajišťuje, že je nikdo neuslyší, pokud je spustíš. Tmel navíc dokáže udělat pěkný nepořádek v nasávání motoru a vzduchovém kompresoru.

➔ **DŮLČÍK ČI DŮLKOVAČ:** Vypadá jako dláto, ale má ve středu hrot. Je tak efektivnější v prorážení nádrží, oken, strojních panelů a desek s elektrickými obvody.

➔ **1,5 AŽ 2 METRY DLOUHÁ PLASTOVÁ TRUBIČKA:** Používají je hlavně milovníci vína, ty však nebudeš nasávat víno, ale benzín. Alternativně s jejich pomocí dostaneš zápalné nebo korozivní látky do těžko dostupných míst. Na jeden konec umísti trychtýř a druhý konec umísti tam, kam chceš látku dostat.

➔ **KVALITNÍ NŮŽ:** Budeš překvapen, s čím vším ti pomůže obyčejný nůž.

➔ **PÍSEK, BRUSNÉ A LEŠTICÍ PRÁŠKY:** Překvapivě jedny z nejničivějších látek, protože se sypou do mazacích systémů. Když pak motor běží, postupně se zadrhává a ničí, protože olej neplní funkci, jakou by měl.

Nejdůležitější ale je, brát s sebou obyčejný ZDRAVÝ ROZUM – nikdy nedělej něco, o jehož následcích si nejsi jistý nebo jsi je dostatečně nepromyslel!

NÁKUP A USKLADNĚNÍ

Jak jsem už zmínil na začátku, pokud to není nevyhnutelné, nikdy by sis neměl brát nářadí k sobě domů – ukládej si ho někde jinde. Pokud policie tvoje nářadí najde, rychlý forenzní test je přivede až k tobě a tvému poslednímu husarskému kousku.

Objevuje se tak problém, jak ho skladovat. Mě se osvědčily voděodolné bedny s uzamykatelným poklopem silné natolik, aby snesly zakopání, vykopání nebo přehození přes nejbližší živý plot pro případ rychlého útěku. Pokud nejsou dostupné, měl by ses poohlédnout po nějakém jiném voděodolném kontejneru. Jinou možností je zabalit nářadí do mastných hadrů, ty ale korozi zcela nezabrání.

Pokud si pořizuješ nářadí, nikdy si nekupuj nic unikátního – to je totiž snadno vystopovatelné. Kupuj si běžné, masově produkované vybavení, ne lokálně vyráběné nářadí unikátní značky. Pokud používáš staré nářadí, odstraň z něj před použitím jakékoli identifikovatelné značky.

Nejdůležitější – nikdy si neobstarávej nářadí přes internet a nikdy neplať kartou – všechny „snadno objednatelné a snadno zaplatitelné“ metody jsou ty nejsnáze vystopovatelné, hotovost taková není.

PŘÍPRAVA NÁŘADÍ

Jen zřídka poberu svoje nářadí a jdu na věc – několik dní předem ho nejdříve zkontroluju, udělám nějaké přípravy (naolejování, naostření, je-li to potřeba), a nakonec vše dobře vyčistím lihem, abych se zbavil jakýchkoli náhodných otisků prstů – příště, až na ně budu sahat, už budu mít rukavice.

Jaké nástroje budeš potřebovat, ti napoví pečlivý průzkum a plán útoku. Není třeba nosit všechno. Pokud je to možné, je lepší brát si jednu věc, která zastane více úkonů. Jinými slovy proč si brát malé a velké kleště, když velké zvládnout práci obou?!

Zásadní je zvážit, v čem nářadí budeš přenášet. Já mám opasek na nástroje s malými poutky a kapsami na cvoky, do kterých všechno nacpu. Vyhovuje mi, když pracuju o samotě, pokud ale pracuješ ve skupině, bude se vám hodit spíše batoh nebo taška. Když je na místě více lidí, zvolte někoho, kdo bude mít batoh na starosti a zkontroluje a ujistí se, že jste na místě nic nezapomněli. Když jsi sám, je snazší to uhlídat - pokud mám na opasku nějakou kapsu prázdnou, hned vím, že něco chybí.

Lepidlo, barva, prášek apod., to vše bys měl předem zbavit původních obalů, abys zabránil jeho zpětnému vystopování (například pokud bys použitý tmel v původním obalu pohodil bez otisků prstů poblíž místa činu, budou mít fízlové alespoň jednu stopu, které se držet – půjdou po prodejnách, které tmel prodávají a možná se díky tomu dostanou až k tobě). Věc přesypej, přelij apod. do jiného obalu, který nemá žádné označení (to obecně neplatí pro lepidla,

proto se snažím kupovat takové lepidla, ze kterých můžu odlepit nebo odmočit papírové přelepky). Původní obaly si nikdy nenechávej doma, protože pokud policie udělá razii, projde si i tvoje odpadky. Alternativně můžeš výrobek zbavit jakéhokoli identifikovatelného značení.

Tak jako se vším ostatním, i tvůj batoh nebo opasek by měl být pořízený čistě pro jednu jedinou činnost – nikdy k akci nepoužívej svůj starý batoh, a to i tehdy, pokud ho chceš vyhodit. Hlavní nebezpečí spočívá v tom, že jsi s batohem spojený, tvoji přátelé ho znají a látka batohu bezpochyby nese tvé DNA.

5. ZDRAVÍ A BEZPEČNOST PRÁCE

Sabotérství je nebezpečná činnost. Například pokud budeš zároveň kouřit a přeřezávat palivové potrubí, pěkně se proletíš do vzduchu. Pokud budeš stát pod ramenem bagru, kterému přeřezáváš hydrauliku, pěkně tě to rozmázne nebo přinejmenším uvězní. A tohle byly jen dva nejmarkantnější příklady.

➔ **OČI:** Když je to možné, nos brýle. Hlavním nebezpečím je zanesení hydraulické kapaliny nebo benzínu do očí. Podobně když navrtáváš nebo tlučeš do něčeho, snadno se ti můžou do očí dostat úlomky a prach. Nejvhodnější jsou pracovní ochranné brýle, postačí ale i brýle obyčejné.

➔ **RUCE:** Nenos slabé rukavice – minimem by měly být robustní zahradnické rukavice. Rukama ti totiž budou procházet ostré předměty, které tě mohou pořezat nebo bodnout. Malé řezné rány nemusí sice vypadat vážně, ale i ta nejmenší ranka může zanechat stopy krve a tím pádem i tvůj genetický otisk. Dobré rukavice jsou průmyslové s hustě prošívaného materiálu, rukavice pro mechaniky nebo motorkářské rukavice, stojí okolo tří set korun. Jsou pohodlné a hlavně relativně přesné i na jemnější práce.

Pokud svařuješ, zapaluješ nebo používáš pájecí lampu, musí být tvé rukavice ohnivzdorné a nesmí se roztavit. Takže na plastové a PVC rukavice zapomeň.

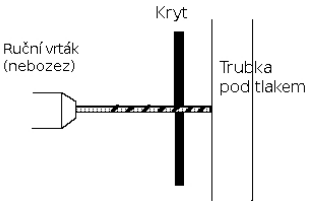
➔ **HLAVA:** Pokud tvoje kroky míří do míst, kde ti něco může spadnout na hlavu, nos přilbu. Ostatně vždycky je dobré mít něco na hlavě, abys po sobě nenechával vlasy (opět snadno vystopovatelné). Já preferuju trampový klobouk s širokým okrajem. Zakrývá moje hipísácké lokny a široký okraj zase dovoluje snadno sklonit hlavu a skrýt si obličej, pokud mě někdo zpozoruje.

➔ **OBUV:** Více v kapitole Otisky bot na straně 22.

➔ **OBLEČENÍ**: Více v kapitole Oblečení na straně 17.

➔ **VRTÁNÍ:** Při vrtání bys měl mít brýle, které jsem už zmínil. Hodí se hlavně pokud navrtáváš trubky pod tlakem, protože ve chvíli, kdy vrták projde skrz, rozprskne se tekutina všude kolem a může tě potřísnit. Pro takové případy se hodí mít na vrtáku nasazenou obrubu – obsah se pak ne-

rozstříkne všude kolem, ale od obruby se odrazí dolů. Jak taková věc vypadá můžeš vidět na obrázku vpravo. Při vrtání dávej pozor ještě na to, že pokud trubka obsahuje palivo nebo plyn, může je teplo nebo jiskry při vrtání zapálit.



➔ **HYDRAULIKA:** Vždy se ujisti, že hydraulika, kterou se chystáš porušit, nedrží něco, na čem nebo pod čím stojíš. Například na JCB strojích vedou hydraulické ohebné hadice z těla stroje do ramene. Pokud je ve vzduchu a ty takovou hadici porušíš, rameno se zřítí. Pokud si nejsi jistý, pokus se zrakem vystopovat, kterou část hydraulika drží a pokud toho nejsi schopni, raději si najdi jiný cíl.

➔ **OHEŇ A CHEMIKÁLIE:** Pokud používáš chemikálie, nos oblečení a brýle, aby sis jimi nepotřísnil kůži. Pokud se to přesto stane, opláchni ihned místo vodou a pokud se ti dostanou do očí, vypláchni je, opusť místo a vyhledej doktora.

Pokud věci zapaluješ, obzvlášť je-li poblíž benzín nebo plyn, dej si pozor, abys nebyl poblíž. Chytnout může jak benzín, tak jeho výpary a pokud stojíš třeba jen poblíž, může tě oheň ožehnout. Existují dva snadné způsoby, jak něco zapálit: hodit na to Molotov nebo použít zápalné zařízení s časovou prodlevou. O zapalování píšu na stranách 46-51.

➔ **ELEKTŘINA:** Elektřina představuje nejvážnější riziko. Pokud přestříháváš hlavní kabely pod napětím, je to 50 na 50, jestli se uzemní přes tebe, nebo ne. Pokud ano, zraní tě. 230 voltů, které jsou standardně doma v zásuvkách, docela kopnou. V průmyslových budovách se ale používá 415 voltů a výš. A pokud si začneš pohrávat s elektrickými rozvodnami nebo stožáry vysokého napětí, pak se bavíme o 11 000 voltech - ty tě na místě zabijou. Nejsem specialista na elektřinu, proto ti doporučuju něco si o bezpečnosti práce s elektřinou načíst.

➔ **TRUBKY A KABELY:** Běžná zařízení mají elektrické a palivové vedení poblíž sebe. Pokud obě vedení narušíš, vystavuješ se dost velkému riziku, protože se palivo může znenadání vznítit, pokud se ho dotkne elektrický kabel pod napětím. Proto nepřeřezávej palivové a elektrické vedení poblíž sebe. Jestli chceš izolovat elektřinu, odstraň pouze elektrickou energii odštípnutím bateriových kabelů.

Snadno vznětlivé jsou také chemikálie. Pokud odstraníš čepičky článků na olověné baterii, budou se chvíli vypařovat hořlavé páry. Pozor na ně! A podobné je to s výpary z rozpouštědel, barev nebo benzínu.

OBECNĚ PLATÍ:

- ➔ Dávej si pozor na všechny elektrické systémy. Před přestřižením drátu si musíš být jistý, že víš, co přestříháváš. V zájmu bezpečnosti nos vždy rukavice a štípací kleště určené pro práci s elektřinou – jsou odizolované a dokážou tě před základními hrozbami ochránit.
- ➔ Pokud to není nezbytně nutné, nenarušuj palivové trubky.
- ➔ Nenarušuj žádné „zabezpečovací" systémy, jako jsou brzdy, požární čidla apod.
- ➔ Nikdy nelez do míst, ze kterých můžeš snadno spadnout nebo na nich můžeš být snadno chycen nebo uvězněn – to platí hlavně pro vysoké jeřáby.
- ➔ POKUD SI NEJSI JISTÝ TÍM, CO TVOJE AKCE ZPŮSOBÍ, NEDĚLEJ JI!

Další důležité varování je, aby ses vždy ujistil, že svými aktivitami neznečisťuješ životní prostředí. Proražení palivové nádrže může způsobit masivní znečištění, stejně jako založení požáru ve farmářově stodole plné pesticidů. Není přece třeba naší zplundrované Zemi dávat další nakládačku, ne?

A pamatuj na to, že tvé akce mohou způsobit problémy později. Pokud jen narušíš elektrické kabely, protože tvé kleště nebyly dostatečně ostré, tak pokud se systém znovu zapne, může způsobit zkrat, který založí požár. V zájmu bezpečnosti není na škodu použít něco na způsob navštívenky, která lidem řekne, že jsi tam byl nebo přinejmenším označí poškozená místa a varuje tak majitele nebo obsluhu. Svými akcemi nesmíš ohrožovat a ubližovat nevinným lidem!

MENTÁLNÍ ZDRAVÍ

Sabotérství je bezesporu stresovější než hrát fotbal a číst knihy. Snižování stresu a zlepšování pracovních návyků je běžně používáno k zvyšování výkonu lidí pracujících ve vysoce stresových zaměstnáních. I tobě může duševní průprava výrazně zvýšit schopnosti a bezpečnost.

Stres je nepředvídatelný element. Americká armáda utratila miliardy na to, aby dokázala vytipovat jedince odolné vůči stresu. Byla ale neúspěšná, protože psychické procesy jsou natolik komplikované, že se nedá určit, co vše se na spouštění stresové reakce podílí. Jednoduše řečeno nikdy nemůžeš dopředu vědět, jak ty nebo tvůj parťák budete reagovat v okamžiku, kdy na vás přistane kužel světla nebo ti na dveře zaťuká kriminálka. Na druhou stranu nebezpečí plynoucí z nejistoty může být výrazně sníženo jednoduchými cvičeními. Následující rady nejsou prázdnou teorií, jejich autor má s nimi bohaté osobní zkušenosti nebo jich byl přinejmenším svědkem.

Stres je všudypřítomný. I ty nejobyčejnější úkony jsou pro sabotéra stresující. I když si toho nemusíš být vědom, přesto můžeš být pod stresem a tím pádem i v nebezpečí. Příklad: Vejdeš do obchodu s kožešinami na průzkumnou misi. I když neděláš nic nelegálního a nemáš u sebe nic inkriminujícího, tvé oči bloudí nervózně po okolí, vyděsíš se, když se za tebou nečekaně vynoří prodavač nebo se prostě nechováš jako běžný kupující. Protože je tvé chování trochu neobvyklé, prodavači si tě zapamatují a za dva týdny tě popíší policii, která bude vyšetřovat, kdo v obchodě rozlil červenou barvu.

Malá úroveň stresu tě dělá zranitelným vůči vysokým hladinám stresu. Díky nervozitě, kterou cítíš vždycky, když vyrážíš na misi, je snazší, aby tě přemohly nenadálé problémy. Příklad: Jsi velmi obezřetný, znáš perfektně okolní terén, průběžně se zastavuješ a naslouchášs, jestli v okolí neuslyšíš podezřelé zvuky. Máš sucho v puse a trochu se potíš. Najednou se ozve hlas: *„Zůstaň kde jsi! Jsi zatčen!“* Strneš a místo abys utekl, zmatený a nejistý stojíš jako přikovaný. A do téhle situace tě dostalo jen to, že sis nevšiml zcela očividných věcí, protože jsi je prostě vlivem stresu neviděl.

Existuje spousta reakcí na stres, následující jsou pro sabotéry ty nejnebezpečnější:

TUNELOVÉ VIDĚNÍ

Běžná reakce na silný stresový podnět. Tvé smysly se zkreslí natolik, že se začneš soustředit pouze na nejočividnější nebezpečí, ale vyloučíš vše okolo. Příklad: Sleduješ auto hlídače, které projíždí poblíž. Už si ale vůbec nevšimneš druhého hlídače, který prochází po tvé levici a má tě přímo na očích.

Zablokování okolních zvuků: Podobné jako tunelové vidění, v tomto případě zaměřuješ pozornost na očekávané zvuky, ale ignoruješ všechny ostatní. Příklad: Jsi přesvědčený, že jsi slyšel kroky Bedlivě naslouchášs a přitom si vůbec nevšimneš vzdáleného zvuku motoru, který se rychle přibližuje k místu, kde se skrýváš.

ZKRESLENÍ ČASU

Čas se pro tebe může zpomalit nebo zrychlit. Ať tak či tak dostáváš naráz nepřesné informace, které tě mohou dostat do problémů. Příklad: Padneš do trávy hned, když uvidíš siluetu člověka pohybujícího se kousek od tebe. Čekáš v relativním bezpečí, jsi potichu, zdá se to už jako věčnost a proto pomalu vstáváš... ve skutečnosti ale uběhlo pouhých patnáct sekund od doby, co jsi siluetu zahlédl.

ZTRÁTA JEMNÉ MOTORIKY

Stres automaticky připravuje tvé tělo na velkou hrubou reakci, jako je útěk nebo útok. Schopnost jemné motoriky se proto výrazně snižuje. Příklad: Jsi přesvědčený, že tě viděl hlídač. Běžíš proto k nedaleko zaparkovanému autu, šátráš po klíčích a nemůžeš je najít. Konečně je máš v ruce, hledáš ten správný klíč, ale nemůžeš se trefit do klíčové dírky, jak se ti třesou ruce. Klíče ti nakonec padají do trávy a hlídač se nebezpečně rychle přibližuje.

ZTRÁTA SCHOPNOSTI SPRÁVNĚ SE ROZHODOVAT

I když jsi se úspěšně vyrovnal se zmíněnými omezeními smyslů, vysoký neklid a nejistota může narušit i tvou schopnost dělat správná rozhodnutí. Příklad: Hlídači na tebe nastražili past, ty ale unikneš. Po chvíli běhu se zastavíš, abys chytil dech. Pak se znovu rozeběhneš, ale místo, aby běžel do hlubších lesů, míříš přímo na lesní cestu, kde už na tebe čekají fízlové.

JAK ZMÍRNIT STRESOVOU REAKCI

Protože jsi během akce stále pod stresem a v neustálém ohrožení, musíš se ho vždy snažit stres alespoň zmírnit, a ne čekat, až na to budeš mít čas. To už totiž možná bude pozdě. Existuje spousta knížek, kurzů a seminářů, které učí lidi vyrovnávat se se stresem. Zavřít oči nebo postupně uvolňovat sval po svalu může být ale pro tebe dost nepraktické ve chvíli, kdy ti na krk dýchá zákon a ty musíš být maximálně ostražitý vůči svému okolí. Proto je asi nejvhodnější metodou, jak se vyrovnat se stresem, jednoduché DECHOVÉ CVIČENÍ. Je to navíc něco, co můžeš dělat veřejně, aniž bys vzbuzoval pozornost.

Dechové cvičení jde proti rychlému a mělkému dýchání, které stres běžně doprovází. Uklidnění těla vysílá do mozku signál, že je vše v pořádku, což dále redukuje stres.

Klíčem je dýchat pomalu a hluboce. Hluboce se nadechni a počítej do pěti. Zadrž dech a opět počítej do pěti. Poté úplně vydechni a přitom počítej do pěti. Jakmile máš úplně prázdné plíce, znovu počítej do pěti a pak začni znovu. Opakuj tyhle kroky znovu a znovu... nádech, zadržení, výdech, pauza...

Zkoušej si toto cvičení doma a jinde. Jakmile se ho naučíš, tak předtím, než se vydáš na misi nebo hned potom, co tě vyhodil řidič, nebo těsně předtím, než začneš přestříhávat plot, se zastav a věnuj několik chvil tomu, aby ses uklidnil.

Poté vždy, když začneš zrychleně dýchat nebo jsi zrovna zalehl do trávy, protože jsi viděl hlídače, opakuj dechové cvičení zatímco kontroluješ okolí nebo si rozmýšlíš další kroky.

Jiný prostředek ke zmírnění stresu je VIZUALIZACE. Protože budeš reagovat tak, jak ses naučil reagovat, trénuj se opakovaně v tom, co budeš dělat, pokud...

...tě zleva oslepí záře světla.
...tě zprava oslepí záře světla.
...uslyšíš poblíž startující motor, zrovna když slézáš z buldozeru.
...se vrátíš k místu, kde tě má řidič vyzvednout, a uvidíš policejní majáky.
…stojí ti před domem policejní auto a někdo tluče na dveře.

Vizualizuj si přesně a úplně, jak na tyto nebezpečné scénáře budeš reagovat. Představuj si vše do veškerých detailů: budeš utíkat, nebo půjdeš pomalu? Zavřeš dveře do jiných místností, schováš pár věcí a pak otevřeš dveře, nebo rovnou utečeš zadním vchodem?

Z těchto vizualizací různých scénářů udělej rutinní součást sabotérství. Pokud se objeví problém, už budeš mít za sebou první krok správného rozhodování, protože ušetříš těch několik prvních vteřin, během kterých by ses normálně musel rozhodnout.

Nakonec tě trochu uklidním. Úspěšné zvládnutí jedné stresové situace vede k tomu, že s každou další se vyrovnáš daleko snadněji. Asi nikdy nebudeš tak klidný, jako když nakupuješ rohlíky v sámošce, ale postupné zlepšování na sobě určitě postřehneš.

6. KONKRÉTNÍ NÁVODY

Tato kapitola je nutně neúplná. Útočit můžeš mnoha způsoby: můžeš posprejovat billboard, zalepit bankomat, zkratovat vedení, prořezat autu pneumatiky nebo ho zapálit, nahlásit někam bombu nebo ji opravdu vyrobit a použít. Představivosti se meze nekladou. Tato kapitola pojednává jen o některých metodách – některé návody nemá smysl opakovat (jak udělat transparent...), jiné zase vyžadují pokročilé znalosti, kterými ani já sám neoplývám (jak vyrobit dynamit...). Proto se těmhle extrémům vyhýbám. Zvídavý čtenář si k nim ale jistě cestu najde.

AUTOMOBILY, NÁKLADĎÁKY A JEJICH KONSTRUKČNÍ ŘEŠENÍ

Vypořádat se s auty, nákladďáky a vším na kolečkách, co má motor, představuje specifický cíl. Obecně se důležité části takových strojů ukrývají za pevnými ocelovými uzávěry, víky a zámky, proto je těžké se k nim dostat. Ovládací systém je obvykle uvnitř kabiny za uzamčenými dveřmi a tvrdým sklem. A co je nejdůležitější, protože jsou to drahé hračky, mnohem spíše budou pod alarmem. Jejich sabotáž se tak stává o to těžší.

Automobily a dodávky je docela snadné nějakým způsobem imobilizovat, ale už není tak snadné je opravdu zásadně poničit až zničit. Vozidla dnes mají nejen pohybové a vibrační detektory, ale alarm hlídá i kapotu a víko palivové nádrže. Vydat se na lov aut tak vyžaduje nemálo přemýšlení a přípravy.

Velká nákladní auta jsou jiný oříšek. K jejich zranitelným částem je snazší se dostat – to se týká hlavně nádrže, elektrických obvodů a hnacího systému, ke kterému se dá dostat zespodu. Na rozdíl od automobilů, kde přeřezání brzd znamená, že auto nemůže zastavit, mají nákladďáky většinou systém vzduchových brzd – tzn. pokud v nich vzduch není, není vůbec možné odbrzdit – to z nich dělá jednoznačný cíl.

Vždy o situaci přemýšlej komplexněji – jaké jsou na vozidle přístupné části? Jaká možnost je efektivnější? Není lepší napadnou něco jiného poblíž?

Dobré je zvážit, jaké části jsou přístupné. Pokud můžeš nasypat písek do olejové vany bez ohledu na cokoli jiného, můžeš považovat svou práci za dokončenou. Pokud si chceš být opravdu jistý, můžeš se podívat i na jiné části

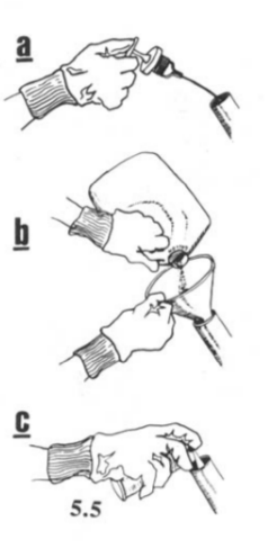
vozidla. Hydraulický systém je jasnou volbou v případě bagrů a elektrický/vzduchový systém zase v případě nákladáků. I v případě aut, pokud jsi dostatečně jemný, by ses měl být schopný dostat pod něj a zničit přívod paliva nebo se protáhnout zespodu do prostoru motoru a přestřihnout několik drátů.

Pokud by sis měl vybrat mezi autem a vedle stojícím nákladákem, je asi jasné, co čeho půjdeš – nákladák má více přístupnějších částí. Podobně – pokud máš uzavřené parkoviště plné aut pod dohledem kamer a alarmu, které je obehnáno plotem a bránou se silným zámkem, můžeš „jen" zalepit zámek. Ať už použiješ jakoukoli taktiku, měl bys vždy přemýšlet nad tím, na jakém systému vozidlo funguje a jak bude nejefektivnější jej poškodit.

JAK VYŘADIT Z PROVOZU VOZIDLA VŠEHO DRUHU
– OBECNÉ MOŽNOSTI SABOTÁŽE

➔ Obecně se tvrdí, že nejlepší a nejefektivnější způsob k zničení těžké techniky, je dostat do mazacího systému abrazivní materiál. To znamená nasypat do olejové nálevky třeba pomocí trychtýře písek nebo brusný prach.

Obrázek vpravo ukazuje, jak to nejlépe udělat: Odšroubovat uzávěr a vyndat měrku. Nasypat písek nebo prach. Pomocí oleje ve spreji spláchnout zbytky písku dolů, aby nebyly na první pohled vidět. Strčit měrku zpátky, vytáhnout ji a ještě jednou zkontrolovat, jestli na ni neulpívá žádný písek. Někteří dělníci totiž před započetím práce kontrolují hladinu oleje. Nakonec nasadit uzávěr zpátky a je to. Aby byla práce dokonána, musí se ještě stroj rozeběhnout, aby se měl šanci zadřít. Tvá sabotáž proto nesmí být objevena dřív, než dělník nastartuje motor.



5.5

➔ Jiný údajně podobně efektivní způsob je nasypat cukr nebo nalít sirup do palivové nádrže. Poté, co se motor rozběhne, cukr se rozpustí a dostane se přes potrubí do motoru, začne karamelizovat a měnit se na tuhou hmotu. Až motor zase zchladne, cukr by měl zatuhnout natolik, že už

se motor vůbec nerozběhne. Staré příručky tvrdí, že okolo pěti kilogramů moučkového cukru nasypaného do průměrné dieselové nádrže zalepí hlavy válců do několika hodin. Jeden kilogram údajně působí na 30-50 litrů paliva.

Tato metoda ale ve skutečnosti NEFUNGUJE! Cukr se totiž v automobilovém palivu nerozpouští, proto ani nekaramelizuje a neničí motor. Místo toho zůstane cukr neporušený a dříve než se dostane do motoru (kde by mohl udělat podobnou škodu jako písek, protože je abrazivní), zachytí ho filtr. Menší množství cukru tím pádem zastaví auto jen tak, že zacpe jeho palivový filtr, který pak stačí několikrát vyměnit. Každopádně větší množství cukru teoreticky může možná auto zacpat natolik, že bude lepší vyměnit celou nádrž.

➔ Nalij do palivové nádrže vodu. Benzín má menší hustotu než voda, proto plave nahoře a voda zůstává dole. Když se pak motor rozběhne, palivové čerpadlo naplní potrubí vodou, což může auto dost rozhodit.

➔ Zalep zámky a startování sekundovým lepidlem, silikonovým těsněním nebo něčím podobným.

➔ Nalij vodu nebo slanou vodu do palivové nádrže (slaná voda je účinnější, protože dál rozežírá kov).

➔ Nalij vodu do olejové vany. Množství záleží na velikosti motoru, ovšem čím víc, tím líp. Voda sice „jen“ rozředí olej, ten ale bude hůř fungovat jako mazadlo.

➔ Prořezej boční stěny pneumatik, ty se špatně záplatují. Na některých pneumatikách ale může být snazší odstranit ventilky. Buď však opatrný: pneumatiky těžkých strojů bývají naplněny vodou pod tlakem, proto může být jejich poškození nebezpečné.

➔ Znič palivovou nebo vodní pumpu, víka ventilů, karburátor nebo cokoli jiného krom baterie (pro tvou bezpečnost) a brzd (pro bezpečnost někoho řidiče).

➔ Nalij benzín nebo jiné palivo do olejové nádrže. Olej ztratí svoje schopnosti.

➔ Chlorid železitý a jiné leptavé sloučeniny používané v elektronice mají značnou schopnost rozrušovat měď. Pokud jsou přidány do vody topného tělesa, do několika dnů ho rozežerou na kousky.

➔ Nastříkej do výfuku montážní pěnu nebo natlač do výfuku syrovou bramboru. Abys ji dostal co nejhlouběji, pomož si tyčí. Jakmile řidič nastartuje, motor se zadusí a vypne.

MOTOR A PALIVOVÝ SYSTÉM

Palivová nádrž je na většině aut v zadní části pod kufrem. Pod podvozkem k němu vede kovová trubka, která je napojená na palivové čerpadlo. Narušení tohoto systému připraví motor o palivo.

Znát tyto části se hodí hlavně tehdy, když chceš auto podpálit. K podpálení totiž můžeš použít přímo palivo, které se nachází v autě. Můžeš ho vysát z nádrže pomocí hadičky, bezpečnější ale je přeřezat přívod paliva nebo prorazit nádrž, než se snažit odstranit uzávěr nádrže, který je pod alarmem. Ležet pod podvozkem ale i tak není zrovna bezpečné, proto je vhodnější podpalovat auto zvenčí pomocí přinesené zápalné směsi.

K motorům je těžké se dostat, protože jsou uzamčené pod kapotou nebo, v případě nákladďáků, je třeba vyvěsit celou kabinu. Možnosti jsou proto omezené. Je možné vypustit olej odstraněním uzávěru olejové vany, ale škoda se objeví až ve chvíli, kdy se nastartuje motor. Vypuštěný olej může obzvlášť v případě nákladďáků navíc způsobit značné znečištění.

Pokud je možné dostat se pod kapotu, nejdříve bys měl jít po zážehových svíčkách nebo, jde-li o dieselové motory, po vstřikovacím ventilu. Pokud chceš udělat opravdu dobrou práci, najdi plnicí hrdlo oleje nebo měřící tyčku a pokus se skrz něj dostat nějaký abrazivní materiál do motoru. Brusný prach je nejlepší (protože je tvrdý), ale může ho dobře nahradit i písek.

BRZDY A HYDRAULICKÝ SYSTÉM

Nikdy bys neměl přeřezávat brzdný systém na autech nebo dodávkách. Brzdná kapalina totiž vyteče a auto není možné zastavit. Vzduchové brzdy na velkých nákladďácích naopak přeřezat můžeš. Je to proto, že pracují díky tlaku vzduchu a pokud jsou přeřezány, znamená to, že v systému není žádný tlak a kola jsou permanentně zabrzděná.

Hydraulický systém je docela nebezpečný – stroj se totiž může pohnout nebo zřítit. Hydraulická kapalina opět není k životnímu prostředí zrovna přívětivá. Vybrat, jakou trubku či hadici přeřezat, je otázkou tvé vybavenosti. Pokud máš dobré pákové kleště, pak by ti hadice do 1,3 centimetru neměly dělat žádný problém. V případě větších trubek bys měl zvážit, že je spíše navrtáš malým (2 mm) vrtákem. Pokud jsou části přístupné, je efektivnější jít po rozdělovačích a ventilech – jsou dražší a trvá déle je nahradit.

ELEKTRICKÝ SYSTÉM

Pokud je vozidlo vypnuté, pak by kromě vedení z baterie do elektromagnetu, osvětlení a zabezpečení neměla dráty procházet žádná elektřina. Tím pádem krom kabelů akumulátoru způsobí poškození dalších kabelů minimální škodu, protože nastalý zkrat detekují pojistky a obvod přeruší.

Poznat konkrétní části elektrického systému může být náročné, kromě jednoduchých částí, jako jsou distributor cap/plug leads (rozvaděč/zásuvky a kabelů akumulátoru). Často je nejsnadnější prostě přestřihnout rychle všechno. Lepší je přestříhávat dráty ne na jednom místě, ale vystřihnout z nich nějakou třeba deseticentimetrovou část. Potom je bude nutné nahradit a ne jen spojit dohromady.

JAK ZAPÁLIT AUTO

Hlavním výhodou ohně je, že může úplně zničit auto, bagr, jeřáb a jiné vybavení bez ohledu na to, jak je velké. A i když má stroj veškeré zranitelné prvky chráněné, přesto může být zapálený. Nevýhodou je, že je těžké dosáhnout dostatečně horkého a rozsáhlého požáru, aby stroj úplně zničil. Plameny navíc rychle poutají pozornost. Od hořícího stroje může chytnout i něco v okolí a zakládání ohně je nebezpečné i pro samotného sabotéra. Oproti předešlým návodům může být ale zapálení auta minutová záležitost.

K zapálení velkého kovového objektu je potřeba polít ho hořlavou kapalinou. Každého asi hned napadne benzín. Ten je vysoce výbušný a velmi nebezpečný. Proto každý, kdo ho používá k podpalování, riskuje, že zapálí sám sebe. Samotný benzín je hodně tekutý a nezůstává tam, kde byl nalit, rychle se rozlévá do okolí.

Účinnější je použít ztužený benzín, který se tolik neroztéká, neodpařuje a ulpívá na povrchu, což koncentruje žár do jednoho místa. Ke ztužení se používá benzín buď 1) smíchaný s motorovým olejem, nebo 2) se benzín ztužuje rozpouštěním mýdla (stačí na struhadle nastrouhat mýdlo s jelenem, aby se dobře rozpustilo, měl by být benzín zahřátý, nejlepší způsob je naplnit velkou nádobu horkou vodou a ní vložit nádobu s benzínem, ohřívat benzín na přímém plameni je sebevražda!) nebo 3) rozpuštěním polystyrenu (do velké nádoby s benzinem postupně vkládej polystyren, až dostane sirupovitou konzistenci). Ztužením vznikne kapalina viskozitou připomínající med. Taková ztužená směs se nazývá napalm. Její nejznámější použití je v Molotovově koktejlu.

Pokud je molotov to jediné, co proti stroji máš, tak po dopadu může benzín vyhořet na povrchu a nezpůsobit v podstatě žádné škody. Pokud je ale stroj v předstihu politý dieselem nebo, což je nebezpečnější, ztuženým benzínem, kompletní zničení je pravděpodobnější.

Diesel na rozdíl od benzínu není výbušný. Je hustější a hoří delší dobu, ale při nižší teplotě. Jeho použití je mnohem bezpečnější, ale je také těžší ho zapálit – obzvlášť za chladného počasí. Někdy se nevznítí dokonce ani když je přímo u něj sirka. K podpálení může být použitý molotov, bezpečnější cestou je použít hadr namočený v rozpouštědle nebo denaturovaném lihu, které snadno hoří, ale nevybuchují (druhá edice Ecodefence mylně doporučovala použít hadr namočený v čistícím alkoholu, ten ale hoří velmi těžko).

JAK VYROBIT A POUŽÍT MOLOTOV

Jak už jsem řekl, molotov se dá typicky použít k zapálení auta, jeho použití je ale mnohem širší. Tvé představivosti se meze nekladou. Následuje jeden ze způsobů, jak takový molotov vyrobit a použít.

Obalem molotovu je skleněná nádoba. Měla by mít tvar vhodný k vrhání a měla by být dostatečně křehká, aby se při dopadu na cíl snadno rozbila. Vhodná je půllitrová láhev od vodky s plechovým uzávěrem. Větší typ láhve pojme více kapaliny. Je ale obtížnější ho vrhnout dostatečně daleko a trefit cíl. Dobré je otestovat si to.

Do láhve je potřeba nalít benzín a motorový olej (v poměru 1:1). Neplň láhev úplně po okraj, nech místo pro výpary. Benzín zajistí rychlou vznětlivost. Motorový olej zvyšuje dobu hoření a zajistí přilnutí k povrchu. Pokud by v nádobě byl pouze benzín, účinnost by se výrazně snížila. Po vznícení by benzín rychle shořel a odpařil se. Olej nebo jiný typ podpůrné látky je tedy potřebný.

Když je kapalná směs v láhvi, je potřeba ji dobře uzavřít plechovým víčkem. Kolem víčka je dobré ještě omotat elektrikářskou lepicí pásku, abys měl jistotu, že se kapalina nedostane ven ještě před vržením molotovu. A to ani její výpary.

Poslední krokem je pruh hadru přivázaný k hrdlu láhve. Není nutné aby hadr byl ponořen v kapalině uvnitř. Může být jen zauzlován kolem vnější části hrdla nebo připevněn drátem. Trčící část hadru je potřeba napustit petrolejem, aby z něj vznikl knot. Ten po zapálení a následném rozbití vržené láhve zapálí kapalnou směs.

Výroba molotovu je ještě ta snadnější část. Složitější je jeho použití. Každý, kdo si chce být jistý, že to zvládne, nesmí podcenit trénink. Opakovaným hodem

lahví na určený cíl se člověk brzy zdokonalí. Na trénování je možné používat lahve naplněné vodou.

PŘÍPRAVA STROJE PŘED ZAPÁLENÍM

Aby se dieselové palivo nerozšiřovalo do okolí, použij hadr (bavlna je lepší než syntetické materiály), kterým ho napustíš. Můžeš použít i jiné savé materiály – piliny nebo slámu. Hadr nacpi do motoru, pokud je přístupný, a pod přístupné elektrické vedení, hadice a měřidla, do podvozku nebo kolem pneumatik. Pět litrů paliva by měly být víc než dost. Nakonec vše podpal pomocí hadru nasáklého snadno hořlavou látkou nebo už zmíněným molotovem.

Ve městě může být tohle skotačení kolem auta nápadné. Podle jednoho prověřeného návodu však stačí polít kolo auta a to zapálit:

Potřebovat budeš PET láhev (1,5 l) naplněnou z poloviny benzínem a z poloviny motorovým olejem. Benzín zajistí rychlou vznětlivost. Motorový olej prodlužuje hoření a umožní, aby kapalina více přilnula k povrchu. Dále potřebuješ gumové rukavice, malý igelitový pytlík nebo nádobu, kus hadru, zapalovač (ten co se používá na plynový sporák) a trochu petroleje. Samozřejmostí je maskování obličeje a použití oblečení, které běžně nenosíš. Po akci se ho rozhodně zbav

Při plánování a provádění akce mysli na to, že na místě nesmí zůstat otisky, pachové stopy a stopy DNA. Úspěšná akce všechny důkazy spálí, ale může se stát, že tam zůstanou nedopalky láhve či hadru. Příprava materiálu tedy musí probíhat v rukavicích a to včetně veškeré manipulace z hadrem.

Hadr zmuchlej nebo poskládej aby bylo možné s ním lépe házet na určené místo. Spodní polovinu polij petrolejem. Pak hadr vlož do pytlíku nebo nádoby. Vlož si to do kapsy nebo někam připni, ať hadr můžeš snadno jednou rukou vytáhnout. Pytlík nebo nádoba zajistí, aby se tvé pachové stopy nedostaly z tvého oblečení na hadr.

Přistup k přednímu kolu auta u řidiče a přikrč se. Auto tě tak bude částečně krýt. Pak nalij zápalnou směs z PET láhve na kolo. Měla by se částečně dostat i za něj. Kolem mokrého kola ti vznikne louže. Do ní polož víčko a láhev se zbytkem kapaliny. Udělej krok či dva vzad. Zapal hadr a hoď ho do kapaliny u kola. Kapalina vzplane. Během chvíle shoří PET láhev s víčkem. Brzy chytne kolo a od něj se dostanou plameny pod kapotu. Plameny projdou dírou kolem tlumiče. Pokud akci provedeš šikovně, pak si nepřítel plamenů všimne až v době, kdy už dávno budeš pryč na bezpečném místě.

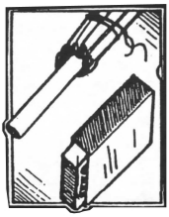
BEZPEČNOST

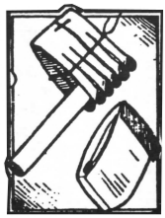
Pokud se potřísníš dieselem nebo benzínem, budeš po nich smrdět ještě dlouho. To tě může inkriminovat. Nos na sobě staré oblečení, které můžeš po akci ihned zlikvidovat. Zbavíš se tak i pachových stop.

Buď opatrný, abys neznečistil vodní zdroj nebo oblast v okolí unikajícím palivem. Také si ujisti, aby se požár nemohl nekontrolovatelně rozšířit na jiné budovy nebo les, pokud to nemáš v plánu. Jistější je zapalovat stroje na volném prostranství. Tresty za žhářství jsou vysoké, dávej velký pozor.

JAK ODDÁLIT ZALOŽENÍ OHNĚ

Když zapaluješ auto nebo cokoli jiného molotovem, jde to sice rychle, ale taky hlasitě a nápadně, protože plameny rychle poutají pozornost. Požár ale můžeš založit i ve chvíli, kdy už jsi v bezpečí. Je několik možností, jak toho dosáhnout. Zásadní je, aby následující metody neselhaly, proto je párkrát prověř, než půjdeš na věc.



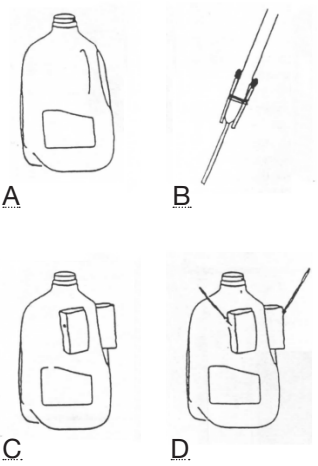


➔ **CIGARETA** (zpoždění 5-10 minut): Na konec cigarety, kde začíná filtr, umísti několik zápalek (buď kolem dokola nebo do dvou řad, jako na obrázcích vpravo) a pevně je oblep páskou dohromady. Vše pak zabal do hořlavého materiálu (novinový papír, lihem napuštěný hadr...) a to nakonec umísti mezi materiál, který chceš zapálit.

➔ **PLASTOVÝ KANYSTR A VONNÉ TYČINKY** (zpoždění 15-45 minut): Potřebuješ plastový kanystr s uchem (prodávají se v nich prací gely, velké množství sirupu, destilovaná voda apod.). Před použitím jej vypláchni, vysuš a očisti od všech otisků. Nalij do něj petrolej (v žádném případě nepoužívej benzín, je příliš prchavý a jeho výpary se snadno vznítí) takřka po okraj, nějaké místo ale ponechej pro výpary. Část petroleje si vezmi s sebou ve zvláštním kanystru, důvod se dozvíš za chvíli. Pak budeš potřebovat jednu houbičku na mytí nádobí. Pro zpoždění zapálení obluž dolní konec vonné tyčinky kolem dokola několika sirkami, nejlepší je oblepit je páskou. Pro každé zařízení vyrob minimálně dvě takové tyčinky. Doba zpoždění se liší na základě teploty, větru atd. a pohybuje se mezi 15

až 45 minutami. Některé tyčinky nehoří dobře a samy zhasínají, proto před akcí vyzkoušej několik značek.

Zařízení je složeno ze tří částí – kanystru (obr. A), tyčinek se sirkami (obr. B) a houbičky. Jednotlivé části přenášej odděleně. Jakmile dorazíš na místo, vtlač houbičku do ucha kanystru (obr. C). Tu pak pořádně polij petrolejem, polít můžeš i okolí a samotný kanystr. Zapal vonné tyčinky v bezpečné vzdálenosti od kanystru a pak je umísti do předem připravených dírek v houbičce (obr. D), jednu na každé straně.


A B C D

Ve chvíli, kdy dohoří tyčinka k sirkám, ty zapálí petrolejem nasáklou houbičku, která roztaví kanystr a zapálí se tím pádem i její obsah. Hlavičky sirek by měly být co nejblíže houbičce. Pokud je mezi nimi velká mezera, může sirka zhasnout a tvé úsilí přijde vniveč. Pokud se ti to hodí, můžeš vonné tyčinky vynechat a zapálit rovnou houbičku. Vždy s sebou nos náhradní zapalovač.

➔ **STŘELNÝ PRACH:** Vyprázdni střelný prach ze čtyř nebo pěti nábojnic a vysypej ho do krabičky od sirek. Do krabičky na jednom konci udělej dírku dostatečně velkou, aby se do ní vešla cigareta. Na druhém konci udělej větší díru. Pak dlouhý pruh látky polij dieselem, kerosinem nebo rozpouštědlem. Látka by měla být nasáklá jen trochu, aby nenavlhl prach. Na místě pak protáhni látku skrz otvor až do střelného prachu. Krabičku pak dej na místo, které má být zapáleno. Do menší dírky nakonec umísti cigaretu bez filtru tak, aby byl její konec opět přímo v prachu. Nyní máš až 15 minut, abys bezpečně odešel. Čas závisí na typu a délce cigarety, na větru a vlhkosti. Tato technika je mnohem snazší, než se na první pohled zdá a funguje ve většině případech. Nicméně na rozdíl od USA je v našich podmínkách poměrně obtížné si bez větších problémů a bezpečnostního rizika opatřit střelivo či přímo střelný prach!

➔ **MINUTKA A HODINKY**: Sofistikovanější a složitější metody jsou použití kuchyňské minutky, náramkových hodinek a přesného časovače. Návody jsou v *The Black Cat Sabotage Handbook* na stranách 109-113. a v Průvodci od Earth Liberation Front *Setting Fires With Electrical Timers*.

➔ **SVÍČKA A MÍČEK:** Nevyzkoušenou metodou je použití svíčky, která se používá na narozeninové dorty a která se nedá zfouknout, pokud je za-

pálena. Budeš k tomu potřebovat ještě pingpongový míček. Udělej do něj díru o průměru svíčky a tu do něj pak vlož tak, aby její velká část byla venku. Celé „zařízení“ dej na místo, které chceš podpálit. Zapal svíčku. Jakmile svíčka dohoří k míčku, měl by vzplanout a podpálit, co je v okolí.

STAVENIŠTĚ

S většinou stavebního vybavení si poradíš s pomocí informací výše. Na staveništích můžeš najít ale také hybridní stroje, které budeš možná muset předem prostudovat, protože jsou složitá a nestandardně zkonstruovaná. Sám bys už měl být schopný přijít na to, co dělat, pokud analyzuješ energetický tok ve stroji a zkopíruješ některé nápady aplikované na standardní systémy popsané výše.

Každopádně při sabotáži staveništ není klíčované uvažovat jen o tom, jak který stroj nejlépe zničit. Měl bys uvažovat o místě jako o funkčním celku. Některé stroje jsou pro chod staveniště nezbytné a jejich sabotáž může stavební práce značně pozastavit. Jiné jsou méně důležité. Na staveništi je většinou nejdůležitější materiální zásobování, v některých fázích ale mohou být stěžejní i míchačky nebo bagry.

Existuje celá řada věcí, které můžeš na staveništi udělat:

➔ V počátečních fázích můžeš jednoduše přemisťovat výměrné sloupky. Pouhé jejich přemístění o několik desítek centimetrů vedle je nenápadné a nepostřehnutelné. Pokud pak stavba bude probíhat podle „plánu“, nebudou do sebe nakonec předem smontované části zapadat. Tichý, ale zákeřný úder.

➔ Dobrým terčem jsou zásoby písku. Do písku totiž můžeš přimíchat cukr nebo sůl (sůl je lepší). Cement nebo beton potom bude křehký. Z důvodu bezpečnosti bys ale poté, co se materiál použije, měl dát stavbyvedoucímu vědět, co se stalo, jinak ohrozíš nevinné lidi. To můžeš ostatně udělat tak či onak, i když jsi cukr nebo sůl nikam nepřimíchával.

➔ Aby byly výkopy suché, pracují na mnoha staveništích po celý den čerpadla. To z nich dělá dobrý terč. Pokud je ale poblíž vodní tok nebo usazovací nádrž, je efektivnější způsob, jak napáchat pěknou škodu. Stačí hadice přemístit – tu, která vodu odčerpává, vyměnit za tu, která vodu vypouští. Výsledkem bude jáma plná vody.

➔ Dalším terčem je také kancelář, respektive unimobuňky. Můžeš zalepit jejich zámky, vylepšit uvnitř dekoraci nebo se je dokonce pokusit převrátit.

➔ Věžový jeřáb je riskantní cíl – pokud bys byl odhalen, není z něj jak utéct. A kdyby se něco nepodařilo, můžeš na něm uvíznout, ošklivě se zranit nebo umřít. Pokud to chceš riskovat, můžeš vyřadit z provozu ovládání v kabině nebo přerušit napájení. Nikdy by ses ale neměl pokoušet jeřáb svrhnout, pokud si nejsi naprosto jistý, že to dokážeš a že tam, kam dopadne, nikoho nezraní.

Ať už děláš cokoli, nezanechávej věci ve stavu, který může být následně nebezpečný pro stavbaře nebo obyvatele budov poté, co by byly dokončené.

POTRUBÍ A PŘENOSOVÉ VEDENÍ

Potrubí a elektrické přenosové systémy jsou neobyčejně snadnými terči, ale mohou být také značně nebezpečné. Pokud uvažuješ například o sabotáži vysokotlakého plynového potrubí nebo o nějakém elektrickém kabelu, který má v sobě víc než 415 voltů, tak ti rovnou říkám, zapomeň na to! Jsou lepší způsoby, jak umřít. I přesto existují terče, které stojí za zvážení…

Elektrické vedení vysokého napětí je náročné přerušit – dokonce i běžným 230 voltovým napětím v domě se můžeš zabít. Kabel ale můžeš „propálit“ – nejsnadnější způsob, jak to udělat, je umístit pájecí lampu na kabel nebo trubku a poté se rychle schovat do bezpečí.

Elektrické vedení nízkého napětí může být snadno přerušeno kleštěmi za předpokladu, že mají izolované rukojeti nebo máš na rukách silné gumové rukavice. Na věci typu vysokoproudé indukční motory nebo svařovací zařízení si dej pozor – těmi vede vysoké napětí, které tě může popálit nebo jinak zranit.

Potrubí bývají doplněny čerpadly, aby v nich látky mohly proudit. Čerpadla jsou snadným terčem. Můžeš jít po motoru, který čerpadlo pohání, nebo přímo po jeho potrubí. Existují dva typy čerpadel:

➔ **MEMBRÁNOVÁ ČERPADLA:** pracují na bázi oscilační membrány a dvou jednosměrných ventilů. Poznáš je podle pravidelného pulsování. Ventil čerpadla můžeš zablokovat například dlouhým tvrdým předmětem, který strčíš dovnitř. Můžeš jít taky po pohonu čerpadla.

➔ **ROTAČNÍ ČERPADLA:** mají disk, který se otáčí vysokou rychlostí (tzv. rotor), který neustále nasává a zároveň vypouští vodu – proto není slyšet žádné pravidelné pulsování. To, že mu chybí ventily, z nich dělá těžší terče, proto bys měl jít raději po pohonu čerpadla.

Oba typy čerpadel fungují tak, že vytváří nízký tlak na nasávací straně a vytvářejí vysoký tlak na straně druhé. Pokud uděláš otvor do trubek na straně s nízkým tlakem, tak díky přítomnosti vzduchu čerpadlo přestane sát. Pokud vytvoříš otvor na straně s vysokým tlakem, potrubí nebude těsnit.

Koaxiální kabely přenášejí radiové vlny a používají se na stožárech vysílačů, počítačových sítích a některých radiových vysílačích. Mohou být snadno přerušeny štípačkami nebo ještě lépe sešity sešívačkou (ta kabel zkratuje a potenciálně poškodí i vysílač). Dej si pozor na mikrovlnné vysílače – někdy je vlnovod hned za talířem vysílače, což může být pro tvoje zdraví nebezpečné.

Vysokotlaké potrubí nebo kabely vysokého napětí je možné poškodit i pomocí některých chemických zápalných směsí, ty jsou ale pořád velmi riskantní. Problém nastává i proto, že chemické podpalovače mohou shořet, aniž by narušily trubku nebo kabel, ale přitom způsobí vážné nebezpečí, které může někoho ohrozit později. Chemické podpalovače také mohou podpálit něco v okolí, vznítit se může obsah potrubí, nebo, pokud je v potrubí vysoký tlak, výbuch může odhodit hořící části do velké vzdálenosti, kde opět mohou něco podpálit.

SKLADY, KANCELÁŘE, OBCHODY...

Komerční prostory, jako jsou sklady, kanceláře a obchodní domy, jsou velkým soustem. I nevinná kancelář dnes může mít zabezpečení jako lokální banka, a tak je náročné pracovat skrytě. Nemám prostor vysvětlovat, jak se dostat před zabezpečovací systém, protože to vyžaduje vysoké technické a počítačové znalosti. Někdy to ale nemusí být ani potřeba. Někdy má cenu zorganizovat útok do třiceti sekund až jedné minuty a pak se prostě co nejrychleji zdejchnout, ačkoli při tom spustíš snad každé bezpečnostní zařízení, na které v areálu narazíš. Pokud máš ale jistotu, že personál nepřijede do pěti-šesti minut, můžeš uniknout.

V takových prostorech je řada možných terčů, na které se můžeš zaměřit. Ty často bývají specifické, proto stojí za to o nich něco vědět.

CHLADICÍ SYSTÉMY

Jinou běžnou věcí, kterou v komerčních prostorech najdeš, jsou chladicí systémy – používané buď jako chladničky nebo jako klimatizace. Pokud chladicí systém poškodíš, není zrovna levné ho vyměnit, ale levné není ani zboží, které se může zkazit.

Chladicí systémy obsahují hořlavé plyny jako je butan, vysoce dráždivé plyny jako je čpavek nebo dusivé plyny jako CFC a halony. Pokud narušíš jejich potrubí a uvolníš tyto plyny, měl bys z místa hned zmizet. V praxi je bezpečnější jít po elektrickém ovládání chladicího systému a úplně ho vyřadit z provozu.

Moderní chladicí systémy používají elektrické motory, které pohání speciálně navržené čerpadla nebo šroubové kompresory. Zničením nebo odpojením motoru nebo zdroje energie můžeš vyřadit z chodu celý chladicí systém. Problém nastává, když motor a čerpadlo tvoří jednu uzavřenou jednotku – v takových případech můžeš odpojit zdroj energie.

ZABLOKOVÁNÍ ZÁMKŮ

Protože jsou zámky a kladky levné, používají se dnes nejčastěji k zabezpečení čehokoli od vrat a dveří, přes skříně na nářadí až po kapoty strojů. I ty můžeš sabotovat tak, že je jednoduše zalepíš. Snadné je použití sekundového nebo jiného pevného lepidla, u kterého si akorát musíš spočítat, jestli stihne zatuhnout dřív než se bude zámek snažit někdo odemknout. Jakékoli lepidlo, které ztuhne během několika hodin, je pro zalepení zámku ideální. Můžeš použít lepidlo s aplikátorem, které si šikovné, ale je ho málo, a tak se celá akce dost prodraží. Nahradit ho můžeš větší a levnější tubou bez aplikátoru. Do jejího víčka akorát vyvrtáš dírku, kterou pak přelepíš páskou, aby lepidlo nevyschlo. Ať už použiješ lepidlo jakékoli, vtlač do klíčové dírky tolik lepidla, jak jen to jde, ale nezamazej jím vše okolo, aby na první pohled nevypadal podezřele. Přebytečné lepidlo otři nejlépe papírovým ubrouskem.

BEZPEČNOSTNÍ KAMERY

TYPY KAMER

➔ **FALEŠNÉ KAMERY:** Věrné kopie kamer – ty sofistikovanější mají čočku, dráty do zdi, držák... i tyto kamery by měly být ničeny, protože vyvolávají všeobecnou paranoiu a pocit dohledu.

➔ **SKRYTÉ KAMERY:** Většinou malých až titěrných rozměrů. Někdy se používají jako záložní pro dohled v místech, kde je primární tradiční kamera. Skryté kamery v těchto případech slouží jako zálohy, pokud jsou primární kamery vyřazeny z provozu. Nejčastěji jsou používány dočasně pro podchycení opakující se kriminální činnosti.

➔ **KAMERY PŘIPEVNĚNÉ NA ZDECH:** Běžně jsou připevněny mimo dosah jednotlivce, ale jsou přístupné dvěma lidem, kteří vzájemně spolupracují. Nejčastěji střeží soukromý majetek, ale často snímají i veřejný prostor.

➔ **KAMERY PŘIPEVNĚNÉ NA STŘECHÁCH:** Běžně se jedná o kamery dopravní policie, ale někdy to mohou být kamery soukromé nebo spadající pod velké úřady a instituce.

➔ **KAMERY UMÍSTĚNÉ V ULICÍCH:** Běžně jsou umísťovány a řízeny místními autoritami pro dohled nad nákupními centry nebo se jedná o kamery dopravní policie.

METODY ÚTOKU

➔ **IGELITOVÁ TAŠKA:** Igelitka naplněná lepidlem udělá svojí práci pěkně a dobře. Je to levná a téměř stejně tak efektivní metoda jako ostatní krátkodobé techniky. Pokud chceš zabalit do tašky kameru, ke které je snadné se dostat, neváhej ještě rozbít sklo, čočky a další komponenty. Potom ji už do tašky vlastně ani nebal. Lidé pak lépe vidí, že je kamera nefunkční.

➔ **NÁLEPKA A LEPICÍ PÁSKA:** Přelep čočku nálepkou nebo páskou. Dobrá aktivita na trénink, která jasně ukáže, že je kamera nepoužitelná.

➔ **BARVA V PISTOLI:** Používej dětskou pistoli a normální barvu na zdi. Je to jednoduchá, rychlá a zábavná metoda, kterou vřele doporučuji. Za hodinu totiž zvládneš jednoduše sundat na deset kamer a ještě se docela dobře zabavíš.

Připrav se na to, že budeš od barvy, takže si obleč něco na jedno použití. Nejprve začni s čočkou, pak obarvi zbytek kamery a okolí. Jasně tak bude vidět, že je kamera nepoužitelná. Barva se dá ale snadno očistit, proto je dopad této metody krátkodobý.

Já používám pro tyto účely super soaker SC 400 s kamufláží pro noční akce ve městě. Barvu míchám s vodou v poměru 1:1. S touto emulzí jsem schopný strefovat cíle ve výšce až 4,5 metru. Náhradní barvu s sebou nos v plastových nádobkách. Předem ji přeceď, aby v ní nebyly hrudky a neucpávaly tvoji zbraň.

➔ **LASEROVÉ UKAZOVÁTKO:** Silný laser dokáže teoreticky krátkodobě oslepit nebo dokonce zcela poškodit CCTV kameru. Hodí se k tomu

laserové ukazovátko. Ty se slušným výkonem vyjdou na 700 korun, ukazovátka s vyšším výkonem jsou dražší.

Pozor, v tomto případě nemáš žádný ukazatel, který by potvrdil, že jsi kameru vyřadil. Při špatném míření nebo při odrazu od krytu kamerové čočky navíc hrozí riziko poškození očí. Je také poměrně těžké udržet laserový paprsek stále v potřebné vzdálenosti. Pro lepší míření může být připevněn k dalekohledu. Tuto metodu raději nedoporučuju.

➔ **PŘESTŘIŽENÍ KABELŮ:** Kabely mohou být přeťaty buď ostrou sekerou nebo zahradními nůžkami. Ujisti se, že máš nářadí izolované, abys předešel elektrickému šoku. Oprava vyžaduje nákladnou výměnu kabelů. Pozor, jakmile přestřihneš dráty, vyšlehnou jiskry. Ty tě mohou sice potěšit, ale při neopatrné manipulaci možná i trochu zranit.

➔ **SHAZOVÁNÍ TVÁRNIC:** Rozhodě hardcorová metoda jen pro odvážné. Vyšplhej na střechu budovy, na které je kamera umístěna a vytáhni tam s sebou i nějaký těžký předmět, například stavební tvárnici. Tu pak shoď z vrchu na kameru. Správnou pozici zjistíš postupným shazováním malých kamenů. Naprosté zničení kamery doprovodí sprška jisker. Velký pozor při této metodě dávej na bezpečnost lidí pod tebou.

PLÁNOVÁNÍ A PROVEDENÍ AKCE

➔ Vytvoř si mapu umístění kamer ve tvém regionu a posléze polohu kamer ověř.

➔ Poznamenej si, které sloupy mají na sobě připevněné kamery (na některých sloupech je více kamer). Všimni si a zaznamenej, kterým směrem kamery míří. Porozhlédni se po okolí a hledej, jestli je k patě sloupu takový přístup, aniž bys byl vystaven jejich pohledu.

➔ Na sloupu bývá umístěn kryt. Je zhruba 30 cm nad zemí, měří zhruba 10x15cm a je vyroben z kovu či plastu. Za tímto krytem jsou kabely vedoucí ke kamerám. Kryt je obvykle připevněn šroubem. K odšroubování budeš potřebovat plochý nebo šestistranný šroubovák, případně jiné nářadí.

➔ Podívej se také na to, jak vypadají kabely, které vedou ke kamerám na vrchu sloupu. Tyto kabely budeš muset po otevření krytu najít. Jsou to obvykle dva černé kulaté kabely (nebo jsou spojeny v jeden). Po otevření totiž uvidíš změť kabelů různých barev (červený, zelený, bílý, atd), které vedou třeba k semaforům (ty mají často právě tyto barevné kabely).

➔ Obleč se tak, abys zakryl své charakteristické rysy (obličej, tetování, atp.) a abys zamezil zanechávání otisků prstů. Chladné počasí je pro takovou akci ideální. Halloween nebo karneval může být také dobrým načasováním.

➔ Vyčisti své nářadí. Budeš potřebovat kleště, hasák a šroubováky, abys byl připraven na různé druhy šroubů, které drží kryty na sloupech. Vybírej si takové kleště, které mají odizolovanou rukojeť a jsou certifikovány jako elektrikářské kleště, aby zamezil úrazu elektřinou. K očištění a odstranění otisků použij líh.

➔ Krom samostatných sabotáží se dá pracovat při různých příležitostech. Využít se dá například pouličních demonstrací: zkušená skupina lidí může využít této příležitosti a přestříhat dráty ke kamerám na křižovatkách a poté se zamíchat v davu.

➔ Ostatní metody – dopravní kamery, které se používají k ukládání pokut tím, že fotí poznávací značky, jakmile auto přejede na červenou, jsou často níže nad zemí. Mohou být třeba přesprejovány nebo nabarveny, pokud na ně dosáhneš ze země. Kabely u těchto kamer bývají často chráněny kovovým flexibilním obalem, takže k jeho odstranění potřebuješ více než pouhé kleště, aby ses prostříhal skrz.

DALŠÍ RADY

Jakmile budeš stříhat dráty, bude tam obvykle jeden černý, který zajiskří a druhý, který nikoliv. Ten, který bude jiskřit, je napájecí. Drát, který nejiskřil, slouží k přenosu obrazu optickým vláknem nebo koaxiálním kabelem. Pokud vím, tak optické vlákno nemůže být zpětně spojeno dohromady, ale musí být vyměněn celý kabel. Až dráty ustřihneš, může se stát, že se spojí kladný a záporný a dojde ke zkratu, což znamená další jiskry. Tento zkrat může občas způsobit přepětí a zničit celou řídící jednotku kamery.

Z třiceti kamer, které jsem přestřihával, jsem jen jednou dostal elektrický šok, jednou bylo slyšet hlasité BZZZ doprovázené velkým jiskřením a občas se z neznámého důvodu vypnuly na křižovatce všechny světla.

Protože tyto kamery nepotřebují velké napětí, náhodné zasažení proudem by nemělo způsobit vážná zranění. Pro jistotu si obleč odizolované rukavice a obuv. NIKDY NEPROVÁDĚJ TYTO AKTIVITY ZA DEŠTĚ!

SMRADLAVÉ BOMBY

Snad jen s výjimkou těch nejotrlejších nedělá pohled na hromádku exkrementů nikomu dobře. Není asi dostupnější a efektivnější metody, jak někomu zkazit den. Dá se říct, že pokud se vše povede, tak je možné udělat za málo peněz hodně muziky. Podívejme se na smradlavé bomby zblízka. Dají se použít jak za bílého dne, pokud je sabotér pronese na nějaké setkání či konferenci, nebo v noci, když sabotér zapáchající látku aplikuje skrz ventilaci do kanceláří.

Látky, které opravdu výrazně zapáchají, jsou:

- ➔ Sirouhlík (Carbon disulfide)
- ➔ Sirovodík (Hydrogen sulfide) – jako zkažená vejce
- ➔ Skatol (Skatole) – jako fekálie
- ➔ Etylamin (Ethyl amine) – jako ryby
- ➔ Kyselina propionová (Proprionic acid) – jako pot
- ➔ Kyselina máselná – jako zvratky

Kyselina máselná patří mezi neuvěřitelně efektivní látky. Je to slabá kyselina (není nebezpečná) s neuvěřitelně silným zápachem, který připomíná zvratky. Není ji potřeba mnoho – dvě kapky dokážou naplnit svou vůní celou místnost. Třicet mililitrů provoní celou budovu. Její zápach se těžko odstraňuje, na místě se drží i týdny.

Díky její síle může být její transport na místo problematický. Je možné použít kapátko, já ale používám injekční stříkačku. Kyselinu můžu díky ní dostat i na jinak těžko přístupná místa (skrze gumové těsnění okolo okna auta, pod dveřmi kanceláře apod.). Smrdutou látku si navíc můžeš držet od těla, což se hodí nejen proto, že by tě zápach inkriminoval, ale taky by mohl nemile zasáhnout do tvého společenského života. Nejlepším řešením politého oblečení je zničit ho.

Kyselinu máselnou by u nás neměl být problém sehnat. Není to kontrolovaná látka, proto o ní policie neuchovává záznamy. Běžně ji skladují chemické a některé vysokoškolské laboratoře a prodávají se například v prodejnách s rybářskými potřebami, protože se používá jako návnada.

Zahraniční návody doporučují také butylmerkaptan. Přidává se do zemního plynu, který sám o sobě nijak nezapáchá, aby bylo možné zjistit jeho úniky. Co je zásadní – ve vyšších koncentracích silně připomíná skunka. Butylmerkaptan není nijak škodlivý, ale brzy vyvane. Problém je, že u nás se, pokud vím, nedá legálně sehnat. Držel bych se proto kyseliny máselné.

Některé prodejny s potřebami pro zvířata nebo lovce nabízejí zvířecí pachy, které se používají k výcviku loveckých psů. Sehnat se dá také sprej s vůní skunka, který používají lovci, aby zakryli po sobě v terénu stopy. Něco podobného se dá získat i v obchodech s potřebami pro kouzelníky nebo v prodejnách s vtipnými potřebami.

7. ŠPIONÁŽ
– ANEB KDYŽ MÁŠ FÍZLY ZA ZADKEM

Nikdy nevíš, jestli jsi v hledáčku fízlů. Pokud bys byl opravdu v bezpečí a věděl bys, že se o tebe nemohou v žádném případě zajímat, pravděpodobně bys nikdy nečetl tyhle řádky (pokud ovšem nejsi zaměstnanec BIS, který o tomhle textu musí podat hlášení).

Určitá pravděpodobnost vždycky existuje a pokud jsi velká ryba nebo máš hodně kontaktů, šance, že budou sledovat každý tvůj krok, roste. Když jdeš do sámošky pro rohlíky a čteš si zprávy na internetu, asi o nic nejde. Když jdeš ale někoho navštívit, odesíláš komuniké nebo jdeš nedejbože přímo na věc, je to průser.

Tato kapitola shrnuje některé možnosti, jak mohou bezpečnostní složky pronikat do tvého soukromí. Její součástí je i kompletní překlad anglické brožury ANONYMITY/SECURITY, která se věnuje speciálně počítačům a internetu.

ŠTĚNICE A ODPOSLECHY

Štěnice jsou malá zařízení, která dokážou snímat zvuk či obraz, ukládat ho na disk nebo ho v reálném čase odesílat na jiný zdroj. Jedním typem jsou RF štěnice, které odposlechnutý zvuk rovnou vysílají pomocí radiového signálu. Jejich dosah je do stovek metrů a jeho obsluha musí sedět v dosahu signálu – nejčastěji před budovou v autě.

Jiný typ štěnic obsahuje GSM modul a pro přenos využívá mobilní síť, takže posluchač může být kdekoli na světě, na štěnici stačí jen zavolat.

Štěnice, které potřebují vyměňovat baterie nebo paměťové karty, se nejčastěji umisťují na spodní desky stolu do montážních otvorů, na zadní strany skříní, radiátory nebo do květináčů. Naopak štěnice, které potřebují být napojené na rozvod elektrické energie, se nejčastěji nachází v zásuvkách, vypínačích, elektroinstalačních krabicích, prodlužovačkách nebo uvnitř počítačových skříní. Alternativně také v lampách nebo ve stropních podhledech.

Aby ti někdo dal do bytu štěnici, musí se samozřejmě do bytu fyzicky dostat. Prevencí je mít byt zabezpečený a nenechávat žádné návštěvy bez dozoru. Někdo radí dávat si doma pozor na rozmístění nábytku. Technici po sobě údajně občas nechávají rozhozený nábytek a jiné stopy, kterých si můžeš všimnout. Podle mě je to ale nadlidský úkol.

Pokud máš podezření, že máš doma štěnici, můžeš se ji pokusit najít. Přeji ti hodně štěstí, protože může být kdekoli a pokročilé modely pravděpodobně ani neobjevíš (pro představu skrytým kamerám stačí průhled menší, než je díra po vpichu špendlíkem). Hledání pak vypadá tak, že projdeš celou místnost se šroubovákem a rozmontuješ všechna místa, kde by se mohla ukrývat. Existují sice firmy (u nás Probin) a přístroje (detektor vysokofrekvenčního pole, detektor nelineárních přechodů, termokamera...), které dokážou odposlechy identifikovat, ale jsou drahé a ne vždy spolehlivé.

Jistější je dávat si prostě pozor na to, co říkáš. Vyhni se jakýmkoli konkrétním a inkriminujícím slovům a neříkej víc, než je potřeba. Používej kódovanou a vágní řeč ve stylu „zítra jdu na nákup, pomůžeš mi?“ Vyšší úroveň je nikdy nemluvit doma, v autě nebo poblíž mobilů, počítačů a neznámých lidí. Pokud potřebuješ druhému něco sdělit a nemáte možnost jít na bezpečné místo, raději si napište vzkaz, který hned potom spálíte.

Dej si také pozor, abys neprobíral citlivé věci ve stejný čas na stejném místě. Jednou jdi na zahradu, příště na rušnou ulici, do parku, pak do přírody… pokud budeš odposlouchávaný štěnicí, vždy to bude tam, kde se očekává, že budeš mluvit.

MOBILNÍ TELEFONY

Mobilní telefony rozhodně nejsou sabotérovým dobrým kamarádem, protože o tobě mnohé prozrazují a dokážou tě odposlouchávat a sledovat. Proto k mobilu přistupuj, jako by to byl fízl. S fízlem bys auto nezapaloval, ne? A zcela určitě bys o tom s fízlem ani nemluvil. Následující stránky popisují, jak fungují mobilní telefony, proč ohrožují tvou bezpečnost a jak se proti tomu bránit.

KDYŽ MOBIL SLEDUJE, KDE SE NACHÁZÍŠ

Zaprvé je možné prostřednictvím telefonu zjistit, kde se nacházíš nebo kde ses nacházel v minulosti. Existují nejméně čtyři způsoby, jak může být vystopována poloha telefonu:

1. SLEDOVÁNÍ MOBILNÍHO SIGNÁLU – VYSÍLAČE

V moderních mobilních sítích operátor může vypočítávat, kde se konkrétní uživatel nachází, kdykoli je mobil zapnutý a připojený do sítě. Tato schopnost vyplývá ze způsobu, kterým je síť postavení a kterému se jí říká triangulace.

Jeden ze způsobů, jak to operátor může udělat, je sledovat a porovnávat sílu signálů které vysílače z uživatelova telefonu dostávají, a následně vypočítat, kde se zhruba nachází. Přesnost závisí na několika faktorech, hlavně na použité technologii a počtu vysílačů. Obecně se dá říct, že jsou přesné na jeden městský blok, některé systémy ale mohou být přesnější.

Pokud je mobil zapnutý a vysílá signál do sítě operátora, neexistuje způsob, jak se tomuto způsobu sledování vyhnout. Ačkoli pouze mobilní operátor dokáže provádět tento způsob sledování, bezpečnostní složky mohou přimět operátora, aby jim tyto data o uživatelovi poskytl (ať už z minulosti, nebo v reálném čase).

Bezpečnostní složky mohou také požádat o výpis z vysílače, tedy o seznam mobilních zařízení, které byly v určitou dobu v dosahu konkrétního vysílače. To jim může posloužit při vyšetřování trestného řinu nebo k zjištění toho, kdo se v konkrétní dobu účastnil nějakého protestu (tento způsob využila v roce 2014 ukrajinská vláda k vytvoření seznamu účastníků protivládních demonstrací).

Taková data se následně dají využít pro analýzu tvého chování. Abys měl představu, jak to může fungovat, podívej se na případ Malta Spitze, který se rozhodl získat a zveřejnit data, která o něm jeho operátor nastřádal od srpna 2009 do února 2010. Někdo jiný z toho pak udělal interaktivní mapu (http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten), která velmi názorně ukazuje, kde se Spitz rád zdržoval, kam chodil na oběd, do práce, na výlety, kde obvykle spal a kde se bavil...

2. SLEDOVÁNÍ MOBILNÍHO SIGNÁLU – IMSI CATCHER

Bezpečnostní složky nebo jiné organizace s obstojnou technikou dokážou sbírat data o poloze i sami bez pomoci operátora, pomocí IMSI catcher (falešný přenosný telefonní vysílač, který předstírá, že je pravý, aby “chytal” signál uživatelů v okolí, detekoval jejich fyzickou přítomnost aodposlouchával jejich komunikaci, v Česku se mu kdoví proč říká Agáta). IMSI znamená International Mobile Subscriber Identity - je to číslo, které identifikuje konkrétního uživatelovu SIM kartu.

IMSI catcher musí být fyzicky umístěný v dosahu zařízení, které má být monitorováno. V současné době neexistuje účinný způsob, jak se proti IMSI catcheru bránit. Některé aplikace tvrdí, že dokážou jejich přítomnost detekovat, ale jejich účinnost je sporná (příkladem je Android IMSI-Catcher Detector). Na zařízeních, které to umožňují, může být nápomocné zakázat 2G podporu (takže se zařízení může připojit pouze do 3G a 4G sítí) a zablokovat roaming. Tato opatření ale platí pouze na některé typy IMSI catchers.

3. WI-FI A BLUETOOTH SLEDOVÁNÍ

Moderní chytré telefony mají většinou i jiné síťové rozhraní - obvykle mají WIFI a podporují Bluetooth. Tyto signály mají menší dosah než mobilní signál a mohou být přijímány pouze na krátké vzdálenosti, ačkoliv některé přídavné antény dokážou dosah signálu výrazně zvýšit. Oba tyto bezdrátové signály mají vlastní unikátní sériové číslo, které se nazývá MAC adresa a které může vidět kdokoli, kdo signál přijme. Toto číslo je spjato s konkrétním zařízením a nemůže být změněno softwarem, který současné telefony mají.

MAC adresa může být naneštěstí zjištěna i tehdy, pokud zařízení není aktivně připojené ke konkrétní bezdrátové síti nebo dokonce, i když aktivně nepřenáší data. Kdykoli je na typickém smartphonu WIFI zapnutá, tak jsou přenášeny občasné signály, které zahrnují MAC adresu a dávají tak okolí vědět, že je v dosahu právě toto konkrétní zařízení (tyto informace využívají některé komerční sledovací aplikace například k tomu, aby zaznamenávaly, jak často zákazníci nakupují a kolik času v obchodě stráví).

V porovnání s GMS monitoringem není tento způsob sledování pro bezpečnostní složky tak užitečný, protože funguje nejlépe jen na krátké vzdálenosti a je potřeba předem znát, jakou MAC adresu má zařízení konkrétního člověka. Tyto metody dokážou být nicméně velmi přesné při určování toho, kdy například člověk vstoupil do budovy. Navíc mohou být vyžádány zpětně. Vypnutím WIFI a Bluetooth můžeš tomuto typu sledování zabránit.

MAC adresu je možné na některých zařízeních změnit. Správný software a nastavení může například měnit MAC adresu každý den. Tato možnost ale není pro většinu modelů dostupná.

4. ÚNIKY INFORMACÍ O POLOZE SKRZ PROHLÍŽEČ

I samy mobilní telefony dokážou určovat svou vlastní polohu, často použitím GPS. Aplikace pak mohou mobilní telefon požádat o tyto informace a využít

je při poskytování služeb, které jsou založené na poloze, například mapy, programy kin ve tvém okolí...

Některé z těchto aplikací následně odesílají tvou polohu přes síť poskytovali služeb, což následně umožňuje jiným lidem, aby tě sledovali. Některé smartphony umožňují částečně kontrolovat, jestli aplikace mohou určovat tvou polohu. Doporučujeme zakázat aplikacím, aby tyto informace mohly získat, nebo povolit jen ty aplikace, kterým důvěřuješ a mají dobrý důvod vědět, kde se zrovna nacházíš.

V každém případě sledování polohy není pouze o zjišťování, kde se zrovna někdo nachází. Tato data dokážou odpovědět i na otázky o minulosti člověka, o jeho aktivitách, názorech, jakých akcí se účastnil a osobních vztahů, jak jsme zmínili na začátku.

POZNÁMKA O GPS

Global Positioning System (GPS) pomáhá jakýmkoli zařízením na světě rychle a přesně určit, kde se zrovna nacházejí. GPS funguje na základě analýzy signálů ze satelitů, které spravuje Americká vláda jako veřejnou službu pro každého. Je obecnou mýlkou, že tyto satelity pozorují každého GPS uživatele nebo vědí, kde se nachází. GPS ve skutečnosti pouze přenáší signály, satelity ani operátoři této sítě nepřijímají ani nesledují tvůj telefon, nemohou vědět, kde se konkrétní zařízení nachází a nevědí ani, kolik lidí tento systém zrovna využívá.

Je to proto, že každý GPS přijímač (jako ty uvnitř smartphonů) vypočítávají svou vlastní pozici pomocí toho, jak dlouho zabere rádiovému signálu, aby se vrátil z různě vzdálených satelitů. Proto jedině tvůj telefon ví, jaká je jeho poloha.

Proč tím pádem vůbec mluvíme o “GPS sledování”? Obvykle tento typ sledování provádějí aplikace běžící na telefonech. Žádají totiž operační systém telefonu, aby jim informace o poloze sdělil. Tyto aplikace je poté mohou předávat přes internet dál. Existují také miniaturní GPS přijímače, které mohou být ukryty ve věcech nebo na autě, které dokážou určovat svou polohu a pak ji opět předávat přes internet dál.

KDYŽ TĚ MOBIL ODPOSLOUCHÁVÁ

Mobilní síť nebyla původně navržena k tomu, aby chránila své uživatele před odposlouchávání. To znamená, že kdokoli se správným typem rádiového přijímače může hovory odposlouchávat.

Dnes je situace o trochu lepší. Šifrovací technologie jsou již součástí standardů mobilní komunikace. Řada z těchto technologií byla ale navržena opravdu bídně (někdy dokonce vědomě, protože vláda tlačila na to, aby šifrování nebylo silné). Někteří operátoři je používali, jiní nikoli. V jedné zemi byly dovolené, v jiné ne (aby šifrování fungovalo, musí ho používat oba komunikující). Jindy zase byly používány nesprávně. Proto je stále možné, že je někdo venku schopný se správným vybavením zachytávat hovory a SMS přenášené vzduchem.

I přes nejsilnější standarty mohou stále někteří lidé komunikaci odposlouchávat. Minimálně mobilní operátor má možnost zachytávat a nahrávat všechna data o tom, komu jsi volal, psal, kdy to bylo a co jsi říkal. Tyto informace mohou být dostupné tuzemské i cizí vládě na základě mezinárodních dohod. V některých případech jsou vlády cizích státu schopné nabourat se do sítě jiného operátora a získávat odtamtud data tajně.

Nejbezpečnějším opatřením je předpokládat, že tradiční hovory a SMS zprávy nejsou zabezpečeny proti odposlechu a nahrávání a chovat se podle toho. Je také možné používat některé šifrovací aplikace, opět ale záleží na jejich kvalitě a na tom, jestli jejich výrobce není schopný šifrování prolomit.

NAKAŽENÍ TELEFONU MALWAREM

Telefony stejně jako počítače mohou nachytat různé viry a malware ať už proto, že si je uživatel sám omylem nainstaloval, nebo se mu někdo do mobilu nabourал a udělal to za něj.

Malware na mobilních telefonech dokáže například číst soukromá data (uložené zprávy, fotografie, videa, telefonní seznamy...). Může také aktivovat senzory mobilu (mikrofon, foťák, GPS...) aby zjistil, kde se mobil nachází nebo aby monitoroval okolí a stal se tak regulérní štěnicí. Proto je namístě nechávat telefon v jiné místnosti nebo si ho vůbec nebrat s sebou, pokud je v plánu řešit citlivé věci.

VYPÍNÁNÍ TELEFONŮ

Jako opatření proti zmíněnému se často uvádí vypínat mobilní telefon nebo dokonce odstraňovat baterii. Doporučení vyjímat baterku je zaměřené hlavně proti malwaru, které dokáže předstírat, že je telefon vypnutý, i když zůstává zapnutý (ukazuje akorát černý displej) a schopný monitorovat okolní konverzaci nebo přijímat hovory. Takový malware opravdu existuje, není ale známo, jak je účinný a rozšířený.

Vypnutí telefonu má i svou nevýhodu - pokud několik lidí v jednom místě udělá to samé, je to určité znamení, že se děje něco nekalého (nebo zrovna začal v kině film). Řešením této situace je nechat telefony zapnuté v jiné místnosti, aby jejich mikrofony nebyly schopné váš hovor odposlouchávat.

JEDNORÁZOVÉ TELEFONY
NEBOLI „BURNER PHONES“

Telefonům, které se používají jen dočasně a poté jsou vyhozeny, se často říká burner phones nebo burners. Lidé, kteří se snaží předcházet sledování, mění často telefony (a telefonní čísla), aby bylo těžší je identifikovat. Používají předplacené telefony, které nejsou spojené s osobním bankovním účtem a které nejsou vázané na konkrétní osoby například smlouvou.

Tato metoda má ale některá omezení. Zaprvé pouhá výměna SIM karty nebo přenesení SIM karty z jednoho zařízení to jiného poskytuje jen minimální ochranu, protože mobilní síť eviduje jak SIM kartu, tak zařízení. Jinými slovy operátor zná historii toho, která SIM karta byla použita a ve kterém zařízení to bylo, takže si je dokáže zpětně spojit.

Zadruhé bezpečnostní složky vyvíjejí techniky analyzující polohu mobilních telefonů tak, aby bylo možné určovat, která zařízení náležejí konkrétní osobě. Existují různé způsoby, jak toho docílit. Analytik například může kontrolovat, jestli dvě zařízení mají tendenci pohybovat se pospolu nebo zda se pohybovaly v určité oblasti, i když byly použity v odlišné časy.

Další problém anonymního používání telefonu je, že lidé mají tendenci vytvářet specifické vzorce chování. Můžeš například obvykle volat své rodině a kolegům z práce. Ačkoli tito lidé přijímají hovory od celé řady jiných lidí, jsi pravděpodobně jediný na světě, kdo jim oběma volá ze stejného čísla. Takže i když náhodou změníš své číslo, ale budeš stále pokračovat ve stejných návycích, bude snadné zjistit, jaké je tvé nové číslo. Pamatuj, že tato dedukce není založena pouze na faktu, že voláš jednomu konkrétnímu číslu, ale spíše na unikátní kombinaci všech čísel, se kterými komunikuješ.

Z toho vyplývá, že efektivní používání burner phones vyžaduje minimálně: nepoužívat stejnou SIM kartu a telefon, nenosit pospolu různé telefony, nevolat na stejná čísla a zajistit, aby mi tyto čísla také nevolaly, pokud používám nové “čisté” zařízení. To není nutně vše, například existuje ještě riziko fyzického sledování na místě, kde byl telefon koupen (tzn. pozor na kamery v obchodech) nebo možnost použití softwaru, který dokáže rozpoznat konkrétní lidský hlas a tím identifikovat člověka.

RADY NA ZÁVĚR:

- ➔ Přistupuj k telefonu, jako by to byl fízl. Obezřetně. Proto před ním nemluv o žádných citlivých věcech. Raději ho nech doma, nebo ho zahrabej na dno batohu a ten pohoď někde opodál.

- ➔ Pokud děláš něco citlivého, nechej mobil doma, aby nebylo možné vystopovat tvůj pohyb.

- ➔ Pokud máš chytrý telefon a brouzdáš s ním po internetu, platí pro tebe většina věcí zmíněných v kapitolách o počítačích.

- ➔ Nečekej, že až tě začnou odposlouchávat, uslyšíš na druhém konci šumění a podezřelé zvuky. Tak už to nechodí. Údajně bys měl být na pozoru spíše tehdy, když je tvé spojení až příliš dobré. Ani na to ale nespoléhej – pořád platí, že bys do telefonu neměl říkat nic konkrétního. Pokud je to potřeba, používej vágní a kódovanou řeč k domluvě osobního setkání.

KDYŽ TĚ FYZICKY SLEDUJÍ FÍZLOVÉ

Obzvlášť v rušném městě není snadné všimnout si, že se za tebou už dobrou hodinu někdo táhne. Pokud chceš mít jistotu, vydej se do méně rušných částí města, kde máš lépe pod kontrolou lidi ve svém okolí. Všímej si kohokoli podezřelého a snaž se zapamatovat nějaký jeho specifický znak. Barva trička není nejlepší orientační prvek, protože ho mohou měnit. Lepší jsou kalhoty, boty, někdy batoh nebo specifický účes… Pak se můžeš začít proplétat všemožnými uličkami sem a tam a všímat si, jestli na nějakou tvář náhodou nenarazíš víckrát než je zdrávo.

Aby sis své podezření potvrdil, dělej nesmyslné věci. Obejdi blok několikrát po sobě. Přecházej křižovatku přes tři zebry. Jdi nějakou dobu na levé straně ulice, pak přejdi na pravou a po čase se zase vrať zpátky. Čekej na zastávce, nech si ujet několik autobusů, hraj, že na někoho čekáš a pak prostě odejdi. Nastup do tramvaje, popojeď jednu zastávku, vystup a zase se vrať zpátky. Nebo nastup na jinou tramvaj jedoucí opačným směrem. Pokud máš dojem, že je těsně za tebou, prudce se otoč, jdi zpátky a sleduj reakce. Fantazii se meze nekladou.

Většinou ale fízlové chodí v partách, a pokud si všimnout, že o nich víš, pohotově se vystřídají. Navíc mají auta, proto se můžou přesouvat rychle a relativně nepozorovaně. Ani oni ale nemají neomezené zdroje, takže máš-li dost času a jsi obezřetný, můžeš na ně vyzrát.

Neočekávej, že ti budou dýchat na krk a upřeně tě pozorovat. Mnohem pravděpodobnější je, že si budou udržovat značný odstup a někdy si tě nechají i zmizet z dohledu. Často se snaží vypadat nenápadně, proto si hrajou s telefonem nebo dělají, že někomu volají.

Pokud se přesouváš po městě v MHD, snaž se sedět úplně vzadu, abys měl přehled. Pro jistotu. Pravděpodobnější ale je, že si povezou zadky v autě a pověsí se na vůz, kterou cestuješ.

Některé manuály upozorňovaly na to, že i nevinně vypadající prázdné auta zaparkované na ulici před domem nemusí být tak úplně nevinné, protože v nich může být nastražená kamera, která tě snímá, kdykoli odcházíš nebo přicházíš včetně všech dalších lidí, kteří tě navštěvují. Opatřením proti takto nastraženým autům je být si vědom toho, jaké auta patří do tvé ulice. Zatímco na předměstích Ameriky to možná funguje, v našich podmínkách je takřka nemožné mít dokonalý přehled o tom, které auto je čí. I tak by sis měl všímat čehokoli podezřelého a nového. Můžeš si psát poznámky o autech, které se před tvým domem opakují, nebo si je můžeš dennodenně fotografovat a pak fotografie srovnávat. Na SPZ se nespoléhej, protože je fízlové mohou snadno měnit a navíc se podle nich neorientuje zrovna snadno. Pokud na něco nezvyklého natrefíš, všímej si veškeré aktivity, která se kolem auta odehraje.

Základem tedy je BÝT VNÍMAVÝ KE SVÉMU OKOLÍ.

KDYŽ SI TĚ FÍZLOVÉ POZVOU NA PODÁNÍ VYSVĚTLENÍ A VÝSLECH

K výslechu se dostaneš buď tak, že jsi chycen přímo při činu nebo razii, nebo ti do schránky přijde *Výzva k podání vysvětlení*. V prvním případě výslech začíná v podstatě ihned, ve druhém případě se musíš dostavit na policii, kde si tě odvedou do místnosti a teprve tam s tebou začnou svou parádu.

I když se to zdá přehnané, nepodceňuj možnost, že ti ráno zazvoní u dveří. To, o co fízlové opřeli domovní prohlídky během Fénixu, byly jen domněnky založené na starých záznamech, anonymních informacích z internetu a několikaměsíčním sledování. V případě Tomáše Z. se jednalo dokonce o evidentní lži – podezřívali ho z něčeho, co nemohl udělat, protože byl v té době v zahraničí. I přes tyto vybájené záminky k domovním prohlídkám soudce celou razii posvětil. Zbytek příběhu známe. Právě proto se hodí být na výslech připravený dopředu – je to první věc, která tě čeká, když si pro tebe přijdou.

Měj v každé chvíli na mysli, že fízlové nejsou a nikdy nebudou tvoji přátelé. Je nebezpečné podléhat sympatiím nebo se je snažit přechytračit. Jsou roky trénováni, aby z lidí dostali to, co potřebují slyšet. Poznají, když člověk lže. Umí člověka nalomit a ví, kde zatlačit. Učili se, jak v lidech zasít semínka viny a pochybností. Učili se, jak druhého vystrašit a přimět ho mluvit. Proto jim nevěř, ať ti říkají a ukazují cokoli. Zůstaň silný a drž jazyk za zuby!

Když jsi u výslechu v roli svědka, máš podle § 100 trestního řádu právo odepřít výpověď, pokud *1) jsi s obviněným v přímém pokolení, je to tvůj sourozenec, osvojitel, osvojenec, manžel, partner a druh; 2) pokud bys výpovědí způsobil trestní stíhání sobě, svému příbuznému v pokolení přímém, svému sourozenci, osvojiteli, osvojenci, manželu, partneru nebo druhu anebo jiným osobám v poměru rodinném nebo obdobném, jejichž újmu bys právem pociťoval jako újmu vlastní.* V žádném případě NEMUSÍŠ a ani bys neměl uvádět konkrétní osobu nebo konkrétní důvod, proč odmítáš vypovídat. Stačí prostě říct *„odmítám vypovídat podle paragrafu 100“.*

Odepřít výpověď nemůžeš u trestných činů, které mají oznamovací povinnost *(trestní řád, § 368 Neoznámení trestného činu)*. V anarchistických kruzích se typicky jedná o teroristický útok a rozvrácení republiky. Fízlové ti můžou tvrdit, že vypovídat prostě musíš, protože se na jejich případ vztahuje oznamovací povinnost. Budou se tě snažit zahnat do úzkých a zastrašovat tě tím, že jestli nebudeš mluvit, půjdeš na tři roky do vězení. Třeba takhle: *„Takže vy odmítáte vypovídat. Víte ale, že tady se jedná o terorismus, že jo? A víte, že v případě terorismu nemůžete odepřít výpověď, jinak půjdete na tři roky do vězení? Kopete si hrob, chlape. Úplně to na mě svítí, že když nám nic neřeknete, porušujete paragraf 368 a my pak budeme muset zahájit proti vám trestní řízení, takže tady příště budete sedět jako obviněný, to opravdu chcete?“*

Fízlové ti ale už neřeknou, že se v tom samém paragrafu píše, že za něho nemůžeš být trestaný, pokud bys oznámením přivodil trestní stíhání (nebo smrt, ublížení na zdraví apod.) sobě nebo osobě blízké. V praxi to tím pádem znamená, že kdybys lhal, kdybys opravdu o něčem věděl a přesto to neoznámil, fízlové ti to musí zaprvé dokázat a zadruhé bys musel lhát o takovém činu, jehož oznámení by tebe a tvé blízké nemohlo ohrozit. Za zmínku stojí, že fízlové se často dozvědí, že jsi lhal, protože je na to přivede jiný člověk, který u výslechu mluvil. Kdyby všichni odmítali vypovídat, fízlové by se většinou neměli čeho chytit.

Zatímco svědek musí říkat pravdu (pokud by lhal, mohl by být stíhaný za křivou výpověď – další důvod, proč je lepší mlčet), člověk v roli podezřelého nebo obviněného může lhát a fantazírovat. Bezpečnější, než se je snažit přeblafnout, je ale prostě mlčet.

Následují některé myšlenkové hrátky, které s tebou dozajista budou chtít hrát. Tvá schopnost zůstat na svobodě může jednou záviset nejen na okolnostech a síle tvého charakteru, ale také na znalosti těchto gestapáckých psychologických technik:

„VYPADÁŠ INTELIGENTNĚ A MÁŠ PŘED SEBOU SLIBNOU BUDOUCNOST. NECHCEŠ SI PŘECE TAKOVOUHLE PRKOTINOU ZKAZIT CELÝ ŽIVOT, NE?“

Oblíbená taktika – nejdříve polechtat ego a pak zasít pochybnosti. Snaží se vypadat, že jim na tobě záleží, že o tebe mají starost, že v tobě vidí nějaký potenciál. Z nějakého důvodu ti ale chtějí pomoct jen pod podmínkou, že budeš mluvit. No není to zákeřné? Pravdou je, že jsi jim u prdele, je to jen další způsob, jak s tebou manipulovat.

„VÍME O VŠEM, CO JSI UDĚLAL A MÁME VŠECHNY DŮKAZY K TOMU, ABYCHOM TĚ USVĚDČILI.“

Pokud by to byla pravda, rovnou by tě obvinili, poslali vše k soudu a neztráceli by s tebou čas. Opět je to lež. Někdy se může stát, že ti začnou ony důkazy jmenovat nebo ukazovat. Fotky, záznamy, odposlechy... mohou být dokonce skutečné, snaž se ale nepanikařit! Je pravděpodobné, že byly získány nelegálně, což znamená, že je nemohou u soudu použít a potřebují tvé doznání, což je důkaz, který už u soudu použít mohou.

Někdy zase budou důkazy pouze hádat. Například *„našli jsme tvé otisky na skle“, „tvá IP adresa se shoduje s IP adresou, která zveřejnila tohle komuniké“.* Budou ti je ukazovat a vyprávět ti o nich v naději, že se sesypeš a přiznáš se.

Jindy ti můžou předkládat falešné důkazy a čekat, jak zareaguješ. Když je člověk z něčeho neprávem obviněný, má tendenci obhajovat se a uvádět věci na pravou míru. Když se ale budeš ohrazovat a vysvětlovat, že *„to nemohli najít“*, že *„to bylo jinak“*, mají tě přesně tam, kde chtěli.

„TVOJI PŘÁTELÉ UŽ NÁM VŠECHNO ŘEKLI, PROČ SI NENALEJEME ČISTÉHO VÍNA?“

Pokud většina taktik selhala, budou se ti pokoušet namluvit, že tě tvoji soudruzi zradili (možná ti dokonce ukážou podepsaný protokol člověka, který vypovídal proti tobě, opět ale může jít o podvrh). Budou tě poštvávat buď proti tvým

přátelům nebo abstraktnímu hnutí, se kterým jsi údajně spolčený. Budou říkat *„Tvoji kamarádíčkové tě pěkně využili a zmanipulovali, víš to? To se ti líbí? Mě by se to teda nelíbilo“*. Načež se tě zeptají, jestli opravdu chceš chránit takové lidi, kteří tě jen využívají a nezajímá je, že ti hrozí vězení.

Nevěř jim. Snaží se v tobě zasít semínko pochybností o dalších členech tvé afinitní skupiny. Většinou je to čistá manipulace. A pokud by to byla pravda, k čemu by ti bylo, že budeš svědčit proti sobě?

„POKUD NÁM TEĎ NIC NEŘEKNEŠ, PŘÍŠTĚ SE VRÁTÍME S POZVÁNKOU K SOUDU.“

I toto jsou časté výhrůžky, které se nikdy nesplní. Soudní obsílka ti nemůže přijít dřív, než budou mít dost důkazů, aby vůbec případ soudu předali. Takže pokud budeš mluvit, naopak možná tyhle důkazy získají a obsílka ti opravdu přijde.

„POKUD BUDEŠ MLUVIT, BUDEME NA TEBE HODNÍ. POKUD ALE MLUVIT NEBUDEŠ, MŮŽOU PO NÁS PŘIJÍT OSTŘÍ HOŠI, KTEŘÍ SI NEBUDOU BRÁT TAKOVÉ SERVÍTKY JAKO MY. MĚJ ROZUM.“

Taková slova tě mají vystrašit. Z praxe se ví, že ke stupňování agresivity spíš nedochází. Je pravděpodobné, že pokud o tebe mají zájem, navštíví tě brzy jiné tváře, ty ale nebudou jenom agresivní. Budou používat opět a zase ty samé psychologické taktiky jako ti před nimi – cukr a bič. Je to logické. Sami by se ochudili, kdyby se spolehli jen na agresivitu.

„TIHLE EXTREMISTÉ UBLIŽUJÍ VAŠEMU HNUTÍ. KAZÍ JEHO OBRAZ NA VEŘEJNOSTI A VEŘEJNOST VÁS PAK VIDÍ JAKO NÁSILNÍKY. BUDE LEPŠÍ, KDYŽ NÁM ŘEKNEŠ, CO JE TO ZA LIDI. JEDINĚ TAK POMŮŽEŠ SVÉ VĚCI.“

Tihle extremisté jim leží v žaludku tak hluboko, že se snaží hnutí rozložit dokonce tím, že se odvolávají na jeho myšlenky! *„Ty si opravdu myslíš, že tihle radikálové prospívají zvířatům ve velkochovech?“* Tento trik většinou mezi zkušenými sabotéry nefunguje, protože jsou si moc dobře vědomi toho, jaký vliv mají. Naneštěstí některé méně zkušené a teoreticky zdatné jedince dokážou taková slova zviklat.

Můžou se tvářit oddaně, chápavě, přátelsky... můžou ti říkat jakákoli sladká slova, ale věř, že za rohem se budou s kolegy poplácávat po ramenou a smát se tomu, jak jsi byl naivní, že jsi jim na to skočil.

„MOJE DCERA JE TAKY VEGETARIÁNKA, TAKŽE TI ÚPLNĚ ROZUMÍM.“

Podobná situace. Budou s tebou sympatizovat. Uslyšíš od nich třeba *„Asi bych udělal to samé“* nebo *„Každý by za takových okolností jednal stejně jako ty.“* Snahou opět je vykreslit se jako spojenec a přítel, kterému můžeš v tomto nepřátelském prostředí věřit a který se ti snaží pomoct. Tahle taktika funguje jen tehdy, když přijmeš jejich nabídku a skočíš jim na jejich přátelské řeči.

„CO POSLOUCHÁŠ ZA HUDBU?“ – „PUNK“ – „TEN JSEM MĚL DŘÍV TAKY RÁD. A KAM CHODÍŠ NA KONCERTY?“

Když nebudeš spolupracovat, budou to zkoušet nenápadně a neformálně – budou se tě ptát, jak se dneska máš, jak se ti líbí ve škole nebo v práci, jestli sportuješ... zdá se to jako triviální informace, kterou bys jim mohl dát, že? Alespoň si ukrátíš tu dlouhou chvíli, co tam trčíš a čekáš, až tě pustí. Jejich otázky jsou ale sofistikované, brzy tě zavedou na půdu, která se jim hodí a kde z tebe můžou tahat potřebné informace. Takže po otázce, kam chodíš na koncerty, se většinou zeptají, co za lidi tam chodí. *„A viděl jsi tam někdy Marka?“* A už to jede... Jak už bylo řečeno – je trestné lhát. Pokud Marka znáš, měl bys říct *„ano“*, nebo *„odmítám vypovídat“*. Čímž jim pomáháš mapovat terén témat, které považuješ za citlivé.

Ať se tě budou ptát na to, jak se máš nebo co jsi včera dělal, neodpovídej jim. A to ani v případě, že tam sedíš několik hodin a oni do tebe pořád hučí. Neposkytuj jim ŽÁDNÉ informace, bez ohledu na to, jak nedůležité a triviální se zdají být, protože nikdy nevíš, kam tím směřují. I kdyby se tě nesnažili dostat, snaží se tě minimálně poznat, dostat se ti pod kůži, pochopit tě, aby na tebe mohli příště ušít ještě těsnější košili.

„NEBUDE TO TRVAT DLOUHO, MÁME JEN PÁR OTÁZEK.“

Ha, ha, ha. Lež jako věž. Čím víc jim dáš, tím více si vezmou a příště si přijdou ještě přidat. V okamžiku, kdy se byť jen trochu rozmluvíš udělají všechno pro to, abys mluvit dál. Z praxe víme, že ti, kteří u výslechu trochu spolupracovali, byli u výslechu vícekrát než ti, kteří neřekli vůbec nic.

„TAKŽE VY ODMÍTÁTE VYPOVÍDAT. ZÁKON ALE ŘÍKÁ, ŽE TO MŮŽETE UDĚLAT, JEN POKUD BYSTE OHROZIL SEBE NEBO BLÍZKÉ, ROZUMÍTE TOMU?“ – „ANO“ – „JAK SE NA TO TAK KOUKÁM, TAK Z TOHO VYPLÝVÁ, ŽE JSTE NĚCO UDĚLAL, JINAK BYSTE MLUVIL.“

Domnívat se mohou cokoli, pravda může být jakákoli. Ty jim nemusíš a ani bys neměl vysvětlovat, jak to chápeš a jak to myslíš a proč odmítáš vypovídat. Nemusíš dokonce ani uvádět, koho bys mohl stíháním ohrozit, i když se ti dozajista budou snažit tvrdit opak, budou na tebe zkoušet právní kličky, slovíčkaření... Stůj si za svým! Jediná věta, kterou bys za celý výslech měl pronést, je *„odmítám vypovídat“*. V protokolu by pak mělo být uvedeno něco ve smyslu *„odmítá vypovídat podle § 100“.*

„CO BY NA TO ŘEKLI DOMA?“

„CO KDYBYCHOM SE ŠLI NA TEBE ZEPTAT DO PRÁCE?“

Další ze způsobů, jak tě vystrašit. Ne každý chce, aby o jeho radikální stránce věděli jeho kolegové nebo rodina. Skutečností ale je, že zadržení policií není něco, za co bys měl mít problémy ve škole nebo v práci (s výjimkou toho, že je problém, že jsi do práce nepřišel). Fízlové dokonce nemohou nikde šířit, v jaké věci tě vyšetřují. Na druhou stranu policie si o tobě může získávat informace od různých subjektů, pro takový případ měj připravenou historku.

DALŠÍ RADY:

- ➔ Drž jazyk za zuby i ve chvíli, kdy na demonstraci klečíš spoutaný na zemi s dalšími lidmi. Mohou mít kolem tebe nasazené tajné, kteří využijí situace, kdy jsi zranitelný. A stejné je to v cele. Každý vězeň, který se vyptává na tvůj příběh, může být potenciální nepřítel, který, jen co se mu svěříš, už už u soudu svědčí proti tobě, protože doufá, že ho pustí za dobré chování. Není to nic neobvyklého.

- ➔ Všechny podmínky během výslechu jsou směřovány k tomu, aby ses necítil příjemně a sebejistě. Proto tě usadí do nepohodlné židle, zády ke dveřím, díky čemuž se většina lidí cítí zranitelně, obstoupí tě ze všech stran, takže mají všechny tvé reakce na očích... Aby tě nemohli tak dobře číst, sedni si do neutrální pozice – s ničím si nehraj, ovládej své pohyby,

měj pevný pohled a hlas. I když to samo o sobě může být nepohodlné, čím pevnější budeš uvnitř i zvenku, tím dříve pochopí, že z tebe nic nedostanou a tím dříve tě (snad) nechají jít.

➔ Buď ve střehu obzvlášť ve chvílích, kdy to vypadá, že zdánlivě o nic nejde. Třeba když zrovna listuje papíry a znenadání se na něco zeptá, jako by snad šlo o nějakou okrajovou otázku. Vždy se pečlivě zamysli nad tím, proč se asi ptá zrovna na toto a nejlépe – neodpovídej. Někdy se zeptá na něco, co se zdá být obecně známou skutečností, třeba proto že byla v novinách, ani na to neodpovídej. Potřebují tvoje přiznání a tvoje slova. Mohou mít sebepřesnější a sebeskutečnější domněnky, nepotvrzuj jim je.

➔ Někdy záměrně překrucují fakta a snaží se tě zlákat k tomu, abys je opravil a doplnil, třeba ve smyslu: *„Po demonstraci jste s Viktorem a Mirkou šel do parku a tam jste...“* (i když jsi tam šel jen s Mirkou).

➔ V určitých intervalech se budou ptát na lidi otázkami, které naznačují, že už něco vědí. Takovou otázkou třeba je, *„Jak dlouho znáš Janu Vzpurnou?“* Spíše než aby se zeptali *„Znáš Janu Vzpurnou?“*

➔ Pokud tě mají dobře přečteného a znají tvé soukromí, budou na tebe tahat kdejakou špínu. I kdyby na tebe vytahovali, že ti tvůj partner zahýbá, nenech se zviklat.

➔ Možná ti budou slibovat imunitu nebo ti navrhnou, abyste sepsali dvě verze protokolu: jednu, kde bude uvedeno, že jsi nic neřekl, a druhou, kde bude tvá výpověď. Ty si domů odneseš tu první (abys soudruhům dokázal svou mlčenlivost) a oni soudu poskytnou tu druhou. Může to být pravda, ale taky nemusí. Není žádný zákon, které by fízlům umožňoval s tebou vyjednávat. Mohou ti slibovat nižší trest, imunitu, ochranu nebo jiné výhody výměnou za tvou spolupráci. Neskoč jim na to.

➔ Hodný a zlý fízl – Je to jeden z jejich nejstarších triků. Zatímco jeden ti vyhrožuje vězením a říká ti, že už jsi jednou nohou v cele, druhý si hraje na tvého spojence, který se tě prý z té cely snaží dostat. Někdy to zajde tak daleko, až to skoro vypadá, že tě ten zlý napadne. V tu chvíli ho hodnej fízl utne, pošle ho vedle, aby vychladl, a pak se tě pokusí uklidnit

➔ Nevzdávej se! Jsou případy, kdy obžalovaný neřekl ani slovo a oni jej pustili.

VÝŇATKY ZE SKUTEČNÝCH VÝSLECHŮ:

Pro představu následují skutečné věty, které fízlové při výsleších řekli. Je zcela jisté, že pokud se k výslechu někdy dostaneš, řeknou ti je, aby tě zviklali. Když je ale budeš znát předem, nemusí tě tak vyvést z míry. Je totiž patrné, že je používají úplně na každého.

- ➔ *Zamyslel ses někdy nad lidmi, kterým ubližuješ? Co takhle dělníci, kteří s tím nemají nic společného a kteří dokonce s tebou sdílejí stejné myšlenky?*
- ➔ *Nechceme tě vidět za mřížemi, chceme ti dát šanci.*
- ➔ *Jsi mladý. Přece si nechceš pokazit celý život, ne?*
- ➔ *Mám syna ve stejné věku jako jsi ty a nechci ho vidět v takových trablech, v jakých jsi ty, proto ti chci pomoct.*
- ➔ *Pokud nám něco řekneš, můžeš hned odejít a všechno skončí.*
- ➔ *Jen tak ze zvědavosti, kolik lidí je v té skupině?*
- ➔ *Napadlo tě někdy, že mohl zranit děti a nevinné lidi? Co kdyby se ten oheň dostal na vedlejší dům? Takové lidi chceš chránit?*
- ➔ *Vždycky mě zajímalo, jestli tomu, co říkáte, opravdu věříte?*
- ➔ *Nejsi podezřelý jen z tady toho útoku, je tady spousta jiných incidentů, které na tebe můžeme přišít. Jsou tady další útoky, které se odehrály v oblasti, kde jsme tě sebrali* (háže přede mě spoustu složek). *A další máme z jiných oblastí.*
- ➔ *Nejsme tady proto, abychom tě dostali za mříže, ale abychom ti pomohli.*
- ➔ *Co na to řeknou tvoji rodiče?*
- ➔ *Co na to řekne tvůj šéf v práci?*
- ➔ *Tohle je jediná možnost, jak si můžeš pomoct.*
- ➔ *Co to je, to „odmítám vypovídat“? Zníš jako nějaký robot. Kdo tě naprogramoval?*

JAK ODHALIT TAJNÉHO FÍZLA

Neexistuje samozřejmě žádný návod, jak poznat tajného agenta. Když se ale zamyslíš nad Fénixem a dvěma agenty, kteří v kauze figurovali, určitě si všimneš toho, že nejsou zrovna mladí. Je nepravděpodobné, že by práci agenta dělal dvacetiletý student. Očekávej spíše starší jedince.

Dalším významným faktem na našich dvou agentech je, že měli prostředky a čas, který ani běžný člověk nemá. Měli dodávku, měli peníze a byli ochotni udělat první poslední. Je to logické – jedině tak se dostali do kontaktu se spoustou lidí, kteří jim na základě výpomoci začali důvěřovat. I před takovými lidmi se měj na pozoru. Okaté mohlo být i jejich vychloubání a provokace.

Pokud někoho podezříváš z toho, že je tajný fízl, buď trpělivý. Operace v utajení jsou drahé a pokud nepřinášejí výsledky, mohou být zrušeny nebo přesunuty jinam. Pokud agent v utajení nezíská žádné užitečné informace ani po dlouhé době, může být převelen jinam. Proto se měj na pozoru před jedinci, kteří se přesouvají z jednoho místa na jiné, protože se může jednat o tajné fízly, kteří vychytávají vhodné příležitosti.

Americké návody uváděly jako jeden ze způsobů, jak odhalit tajného fízla, štvanici. Podezřelému je jakoby mimoděk poskytnuta nějaká cenná informace, která je tak lákavá, že po ni autority prostě musí skočit. Může se jednak o určitý čas, datum nebo místo budoucí akce, případně umístění inkriminujících předmětů. Akce samozřejmě nakonec nedopadne tak, jak byla plánovaná, nebo se ony „inkriminující předměty" ukážou být naprosto neškodné. Pokud je podezřelý jediný, kdo o téhle informaci věděl, a policie opravdu nějak zareagovala, máš zřejmý důkaz, že jde o agenta.

Tato metoda může být ve stejný čas použita i proti více lidem naráz. Každému je předhozena mírně odlišná informace. Odpověď opět ukáže, od které osoby unikají informace dál. Štvanici ber ale s rezervou – fízlové nemusí reagovat okamžitě nebo viditelně.

Cennější je podle mě následující seznam chování, které může naznačovat, že je někdo fízl:

- ➔ Když se snaží získat informace, které nepotřebuje pro svou roli znát.
- ➔ Když se pokouší donutit lidi k tomu, aby zopakovali inkriminující prohlášení, které řekli dříve (protože si je potřebuje nahrát).
- ➔ Když opakovaně podezřívá ostatní, aniž by měl patřičný důvod. Často se snaží mlžit, aby sám nebyl podezřelý.
- ➔ Když neustále řídí rozhovor a snaží se ho směřovat směrem, který se mu hodí.
- ➔ Když přímo a zbytečně zmiňuje jména lidí, o kterých se mluví nepřímo (opět se může snažit získat dobrou nahrávku).
- ➔ Když zapracovává do rozhovoru čas, datum nebo lokaci a explicitně říká inkriminující věci.
- ➔ Když se snaží od druhých získat ujištění a potvrzení inkriminujících prohlášení.
- ➔ Když se neustále ptá na konkrétní jedince (obzvlášť jedná-li se o zjevné tahouny hnutí).
- ➔ Když iniciuje rozhovory o sabotážích a snaží se neustále vracet na ilegální témata, když se od nich rozhovor náhodou stáčí pryč.
- ➔ Když tvrdí, že je vyléčený alkoholik, čímž omlouvá, že nepije a zároveň se chrání, aby se v opilosti neprokecnul.

8. ANONYMITA A BEZPEČNOST

Žijeme v panoptikonu – i když na nás na všechny stát nemůže v jednom okamžiku upírat svůj zrak, nemůžeme si být nikdy jisti, že se zrovna nedívá. Tato psychická všudypřítomnost podpořená hmatatelnými důkazy o sledovacím aparátu bezpečnostních složek je paralyzující. Hrozba zadržení, soudního procesu a cely nám poutá ruce.

Je nemožné dosáhnout spolehlivé bezpečnosti nebo úplné anonymity. Struktura tohoto světa zabraňuje, aby náš pohyb byl neviditelný a naše akce bez rizika. I když se nemůžeme zneviditelnit, můžeme se některým očím vyhnout, když je to potřeba.

Smysl tohoto průvodce je poskytnou základní informace o následujícím: specifických způsobech, jak můžeš být digitálně identifikován a jak anonymizovat svůj přítomnost na internetu; jak zabezpečit počítač a skrýt svá data před chtěnýma očima; jak kontrolovat a zbavovat se záznamů, které o tobě počítač uchovává; jak ochránit počítač před viry a sledovacími programy; jak bezpečněji používat email; a další témata s tímto spojená.

Přiznáváme se, že nejsme experti. Je možné, že jsme něco nepochopili nebo nevysvětlili správně, proto ke každému tématu, programu nebo aktivitě přidáváme také doplňující seznam zdrojů pro další vzdělávání.

ANONYMITA

Vše, co na internetu děláš, může být vystopováno zpětně k tvému počítači nebo místu, kde se k internetu připojuješ, pokud neskrýváš nebo neanonymizuješ ty aspekty počítače či připojení, které o tobě podávají informace a dokážou tě identifikovat. Mezi takové identifikátory patří software a hardware. Pokud by ses soustředil jen na jeden z aspektů, nemohl bys plně zakrýt svou identitu. Musíš se věnovat oběma. Obecně čím více identifikátorů zkreslíš a skryješ, tím těžší bude vystopovat konkrétní aktivitu až k tvé osobě. Nic bys ale neměl považovat za všespásné, hlavně kvůli nepředvídatelným chybám, které tvé úsilí dokážou zhatit. Vše na cestě mezi tebou a tím, co děláš a hledáš (informace, komuniké...), zvyšuje šanci odposlechu. Komunikace face-to-face je vždy bezpečnější.

Množství úsilí, které věnuješ snaze skrýt svou aktivitu, závisí na její povaze. Nevinné brouzdání internetem, přístup k anarchistickým webům, odesílání komuniké – každá činnost vyžaduje jinou úroveň zabezpečení. Je zbytečné zabývat se všemi za chvíli zmíněnými metodami jen aby ses podíval na počasí. Ovšem nechat prosáknout citlivé informace ve chvíli, kdy odesíláš komuniké, tě může stát svobodu. Rozhodnutí je subjektivní a závislé na strategii, situaci a cílech. Nikdy však nedovol, aby tě tvá snaha o „úplnou anonymitu“ odrazovala od akce. Nic takového totiž neexistuje.

První čtyři aspekty anonymity, na které se podíváme (provider, IP adresa, MAC adresa a session data), jsou nejdůležitější. Jedná se totiž o nejjednodušší způsoby, jak vysledovat aktivitu zpětně až ke konkrétní osobě. Vším, co následuje, také mohou unikat informace, první čtyři jsou ale nejnebezpečnější a pokud v nich selžeš, vše ostatní postrádá smysl. Proto by ses jimi měl zabývat přednostně.

POSKYTOVATEL INTERNETOVÉ PŘIPOJENÍ (ISP, PROVIDER)

CO TO JE?

Poskytovatel internetového připojení (Internet service provider) je společnost, která zajišťuje přístup k internetu. Obstarává to, k čemu se připojuješ, když se přihlašuješ na mail a prohlížíš si stránky. Příkladem je kabelový modem, dial-up, DSL nebo wifi. Nejdůležitější je vědět něco o wifi, protože je to nejjednodušší rozhraní, pomocí kterého dosahovat anonymizace. Wifi je buď otevřená, nebo uzavřená a buď veřejná nebo zašifrovaná vyžadující k přístupu heslo. Příkladem otevřené sítě jsou veřejná místa jako kavárny, knihovny nebo nezabezpečené domácí sítě. Příkladem uzavřené sítě je domácí nebo pracovní síť používající nějakou formu šifrování.

PROČ SE TÍM ZABÝVAT?

Když někdo zkoumá internetovou aktivitu, je jeho cílem dopídit se umístění tvého internetového připojení. Pokud to, co jsi dělal, se dá vysledovat zpátky k poskytovali, pak je snaha o anonymitu ohrožena, jestliže jsi to dělal na internetu doma. Bez ohledu na to, kolik úsilí věnuješ svému skrytí, tvé informace stále mohou být zachyceny na úrovni poskytovatele nebo mohou být vysledovány k tvému připojení. Pokud se stane, že je tvá anonymizace z jakéhokoli důvodu oslabená, mohou si přijít až pro tebe, používal-li jsi připojení, které je tvoje nebo někoho, kdo je s tebou spojený.

JAK NA TO?

Na tomto místě je příhodné hackerské moudro *„nehackuj na svém vlastním připojení“*. Pokud by ses připojoval k internetu, které není spojené s tebou ani s nikým z tvých známých, tak i kdyby tvé další pokusy o anonymizaci selhaly, bezpečnostní složky dojdou do mrtvého bodu (například internetová kavárna). Takže v krátkosti: NA SVÉM DOMÁCÍM PŘIPOJENÍ NEDĚLEJ NIC, CO NECHCEŠ, ABY FÍZLI VĚDĚLI.

Nejsnazším způsobem, jak anonymizovat své připojení, je používat veřejné wifi v kavárnách a knihovnách. Většinou jsou otevřené a snadno přístupné. Pokud to okolnosti vyžadují, vyber si místo, které není pod dohledem kamer. Když se k něčemu připojuješ na veřejnosti, zužitkuješ také metody šifrování (viz šifrování připojení str. 92), protože na takové wifi může kdokoli se správným softwarem získat tvé přístupové údaje nebo monitorovat tvou aktivitu. Důležité také je změnit si MAC adresu (viz MAC adresa str. 82), abys předešel tomu, že budou tvé hardwarové informace zalogovány v routeru.

Jinou možností je dostat se na cizí domácí síť. I když je to nelegální, pokud správně anonymizuješ svůj hardware, je nepravděpodobné, že by tě chytili. Abys volnou wifi našel, můžeš třeba jezdit městem sem a tam a zkoušet to (této metodě se říká wardriving).

Další možností je použít software k prolomení zabezpečené wifi. Může to být snadné, záleží na typu připojení a použitém heslu. Některé programy monitorují wifi připojení dokud nemají dostatek informací k tomu, aby šifrování prolomily, jiné zase používají databáze slov a pokoušejí se heslo tipnout. I když to vyžaduje o něco více technických znalostí, mohou vyhledání wifi hodně usnadnit.

Volné wifi raději hledej dál od svého domu. Můžeš použít také wifi anténu, která zvětšuje dosah síťové karty, takže se můžeš připojovat k internetu i skrze vzdálenější místa, na která bys bez antény nedosáhl. Anténa se dá buď koupit nebo vyrobit z několika speciálních kabelů a věcí, které má člověk běžně doma.

Pokud se k internetu připojuješ prostřednictvím poskytovatele, který s tebou není spojený (nemáš s ním smlouvu, není to internet u tvé sestry ani kamaráda...), postavil jsi mezi sebe a bezpečnostní složky silnou zeď. Pokud také správně změníš sofwarové informace a s použitím anonymizérů skryješ svou aktivitu, je nepravděpodobné, že by se činnost dala vysledovat až k tobě, pokud zrovna neběží nějaké velké vyšetřování a fízlové tě nesledují.

ODKAZY:

- ➔ *http://cs.wikihow.com/Jak-b%C3%BDt-online-anonymn%C4%9B* (Podrobněji o problémech spojených s poskytovateli připojení i konkrétní návod, jak dosáhnout silné anonymity)
- ➔ *https://cs.wikipedia.org/wiki/Data_retention* (O identifikačních a lokalizačních údajích, které poskytovatelé služeb o svých zákaznících ukládají a o které můžou fízlové zažádat)

IP ADRESA

CO TO JE?

Tvá IP (Internal protocol) adresa je řada čísel, která umožňuje odesílat a přijímat data skrz internetové připojení. Sestává ze čtyř číselných kombinací oddělených tečkou, z nichž každá je složená z jedné až tří číslic. Rozpětí kombinace je od 0 do 255. Příkladem IP adresy je například 78.125.1.209. Tato číselná kombinace identifikuje lokaci, poskytovatele a technické detaily tvého připojení a je srovnatelná s popisným číslem domu.

PROČ SE TÍM ZABÝVAT?

Nijak neskrývaná IP přivede vyšetřovatele přímo k tvému připojení. Pokud jsi nepoužil cizí internetové připojení (tzn. s jinou IP), pak to bude přímo k tvé osobě. I když využíváš jiného poskytovatele (jsi například v knihovně), doplňujícím skrytím IP ještě více zkomplikuješ vyšetřování a, v závislosti na typu skrytí a nasazení fízlů, pravděpodobně předejdeš tomu, aby vůbec zjistili připojení, které jsi použil (tedy v jaké knihovně jsi byl). Anonymizací své IP adresy stavíš mezi sebe a vyšetřovatele další zeď.

JAK NA TO?

Existují různé způsoby, jak skrýt svou IP adresu. Pro účely tohoto návodu se blíže podíváme na proxy a TOR – dva volné a relativně snadné způsoby jak zvýšit anonymitu. Přikládáme také odkazy na VPN služby a SSH tunely, pokud bys chtěl znát i jiné alternativy.

A) PROXY

Proxy jsou systémy nebo stránky, které nabízejí přístup k internetu prostřednictvím jejich připojení. Místo aby ses připojil ke stránce přímo, připojíš se nejdříve k proxy serveru, který tě až pak připojí ke stránce. Logy této stránky

pak budou ukazovat IP adresu proxy serveru, ne tvoji. Proxy mohou mít podobu stránek nebo seznamů.

Ty první fungují tak, že přijdeš na stránku, do jejich kolonky napíšeš URL a ona se následně načte přes jejich server. Anonymita je na takových stránkách ale sporná. Mohou totiž uchovávat rozsáhlé logy o tom, co jsi navštěvoval, což může být velký problém, pokud je používáš často.

Ty druhé můžeš získat z různých seznamů a zadat je poté do nastavení svého prohlížeče (většinou v Nástrojích - Nastavení připojení). Obecně jsou pomalejší a často nefungují, některé ale nabízejí mezinárodní připojení, které může zkomplikovat vyšetřování.

Nedoporučujeme používat tyto proxy, pokud si přeješ chránit soukromí. Kdokoli, kdo spravuje proxy server, bude mít přístup k čemukoli, co uvidíš. To je nebezpečné hlavně, pokud proxy běží jako návnada (státem řízená proxy určená k vychytávání zločinců a hackerů) nebo pokud uchovává logy (které si mohou zpětně vyšetřovatelé vyžádat).

Dále pokud používáš své domácí připojení, aby ses připojil k proxy, tvůj poskytovatel bude mít záznam ukazující, že se tvá IP k proxy serveru připojila v konkrétní čas. Pokud pak budou porovnány logy poskytovatele a proxy serveru, je možné zjistit, co jsi dělal. Tyto typy proxy ti doporučujeme používat jen, nemáš-li jinou možnost a připojuješ se odněkud jinud než z domu.

Vždy kontroluj, jestli proxy funguje. Stačí jít přes proxy na stránku zobrazující IP (https://www.iplocation.net/find-ip-address). Měla by ukazovat jinou IP, než když na ni přijdeš bez využití proxy.

B) TOR

Pro anonymizaci je vhodnější TOR. TOR je síť proxy, která funguje díky dobrovolníkům a jejímž deklarovaným cílem je zajišťování anonymity. Když používáš TOR, prochází tvé spojení skrz tři proxy. Každý z těchto tzv. nodů šifruje tvá data a nemůže přitom vědět, k čemu jsi připojený a kdo jsi. Třetí nod data dešifruje, připojí se k webu a pošle informace zpátky skrze proxy opět zašifrované. Nic není neprůstřelné, TOR ale nabízí svým uživatelům opravdu silnou anonymitu.

Stinnou stránkou TORu zaprvé je, že je pomalý. Získaná anonymita ale za ten čas navíc stojí. Zadruhé – poslední nod je zranitelný. Pokud své spojení nešifruješ (viz šifrování připojení str. 92), může správce posledního nodu tvá data vidět (přístupová data, informace o webech, na kterých jsi...). I když nemůže osobně zjistit tvé připojení, může zneužít jakýkoli účet, do kterého se loguješ,

proto šifruj! TOR mimo jiné nabízí portable verzi prohlížeče, kterou můžeš mít uloženou na flash disku. TOR tak nemusíš instalovat přímo do počítače a můžeš ho otevírat na jakémkoli počítači.

Varování: Nepřihlašuj se ke svému osobnímu emailu a nezadávej nikam své osobní údaje s použitím TÉ SAMÉ proxy nebo TOR identity, pokud jsi zároveň dělal něco kompromitujícího. Takhle už pár lidí chytli, nebuď tak hloupý.

ODKAZY:

- ➔ http://browserspy.dk (Stránka pro kontrolu IP adresy a celé řady dalších věcí, o kterých ještě bude řeč)
- ➔ https://www.iplocation.net/find-ip-address (Stránka pro kontrolu IP)
- ➔ http://www.cogipas.com/whats-my-ip/ (Rozcestník na stránky, kde je možné zkontrolovat IP adresu a další informace)
- ➔ *https://www.soom.cz/clanky/1035--Anonymita-a-proxy* (Více o proxy včetně návodu na proxychaining)
- ➔ https://www.bestvpn.com/blog/4085/proxies-vs-vpn-whats-the-difference (Rozdíl mezi proxy a VPN)
- ➔ https://cs.wikipedia.org/wiki/S%C3%AD%C5%A5ov%C3%A9_tunelov%C3%A1n%C3%AD (Obecně o síťovém tunelování)
- ➔ www.root.cz/serialy/tuneluji-tuAnelujes-tunelujeme (Návod na síťové tunelování)
- ➔ https://www.torproject.org (stránky pro stažení TORu)

MAC ADRESA

CO TO JE?

MAC adresa (Media access control), známá také jako hardwarová nebo fyzická adresa, je číslo, které unikátně identifikuje kus hardwaru, který se připojuje k síti. Příklad hardwaru s Mac adresou může být síťová karta tvého notebooku.

MAC adresy sestávají z dvanácti znaků (1-9, a-f) sdružených do dvojic oddělených dvojtečkami (např. 01:23:45:67:89:ab). První polovina adresy identifikuje výrobce adaptéru, druhá je sériovým číslem, který mu přiřadil výrobce.

PROČ SE TÍM ZABÝVAT?

MAC adresa slouží k rozpoznání tvého počítače. Když se připojuješ k internetu, router může tvou MAC adresu logovat a záznam uchovávat. Pokud bezpečnostní složky takový log projdou (dejme tomu log veřejné wifi, z níž

bylo odesláno komuniké) a poté ho srovnají s MAC adresou tvého počítače (který řekněme zabavili při razii), budeš s tím, co je zalogováno na routeru, přímo spojený. Pokud nezměníš svou MAC adresu předtím, než se připojíš k internetu, existuje možnost, že tvé aktivity budou vystopovány až k tobě, budou-li fízli dost trpěliví nebo budou mít štěstí.

JAK NA TO?

Aby ses tomu vyhnul, musíš svou MAC adresu změnit ještě předtím, než se vůbec k síti připojíš (některá zařízení nedovolují MAC adresu měnit, v takovém případě uvažuj buď o změně zařízení nebo o použití wifi adaptéru, přes který se budeš připojovat). Pokud by ses připojil k internetu v knihovně běžným způsobem, aby sis prohlédnul maily, a pak bys změnil MAC adresu, abys odeslal komuniké, je to už špatně. Router totiž bude mít těsně za sebou dva záznamy. Sice budou mít odlišné MAC adresy, ale dá se dokázat, že jsi tam v době odesílání komuniké byl.

Složitost změny MAC adresy závisí na tvém operačním systému. Pokud se nechceš tyto způsoby učit, můžeš použít software, který mění MAC adresu automaticky. Ať už na to půjdeš manuálně nebo automaticky, vždy dvakrát zkontroluj, jestli tvá MAC adresa byla skutečně změněna, než se k internetu definitivně připojíš! Níže popisujeme i způsoby, jak MAC adresu ověřit.

A) ZMĚNA MAC ADRESY V LINUXU

Jednou z výhod Linuxu je, že změna MAC adresy je snadná. Je to jen otázka několika příkazů v terminálu. Pro Linux existují i programy, které generují a mění MAC adresu automaticky.

1. Otevři Terminál (standardně stiskem kláves ctrl + alt + T)
2. Zadej příkaz: „ifconfig „název zařízení“ down” (na místo „název zařízení“ vlož hardware, který chceš měnit, například eth0 pro připojení síťovým kabelem, wlan0 pro použití wifi sítě, wlan1 standartně při připojení přes wifi adaptér)
3. Zadej příkaz: ifconfig „název zařízení“ hw ether 00:11:22:33:44:55 (tato čísla budou novou MAC adresou. Musí to být přesně šest párů znaků. První tři označují výrobce zařízení a zbylé tři páry jsou unikátní adresou toho kusu zařízení, který máš v počítači. Pro ještě větší věrohodnost můžeš do prvních tří párů napsat kombinaci přidělenou známému výrobci, například Intelu (seznam najdeš v odkazech)
4. Zadej příkaz “ifconfig „název zařízení“ up”
5. Nyní si ověř novou MAC adresu zadáním příkazu ifconfig -a (ve výpisu pak najdi kus hardwaru, který jsi měnil)

B) ZMĚNA MAC ADRESY VE WINDOWS

Ve Windows je možné MAC adresu měnit v registrech nebo upravením hardwarového nastavení. Tento postup dá trochu práce, ale měl by tvou MAC adresu změnit, pokud vše provedeš správně. Buď však opatrný, když budeš měnit registry nebo hardwarové nastavení, protože na nich šlape systém. Rozhodně doporučujeme, aby sis o měnění MAC adresy ve Windows ještě něco přečetl. Samozřejmě je možné využít i programů, které by měly MAC adresu měnit automaticky.

ZJIŠTĚNÍ MAC ADRESY VE WINDOWS

1. Start >> Spustit >> Do pole napiš cmd a potvrď, otevře se ti terminál
2. Do něj napiš: ipconfig/all
3. Najdi požadovaný adaptér (ethernet – eth0, wireless – wlan0, wlan1). Tvá MAC adresa bude popsána jako Physical Address a její název bude vedle Description.

ZMĚNA PŘES NASTAVENÍ SÍŤOVÉ KARTY

Toto bude záležet na verzi Windows, kterou používáš. Konkrétně v umístění jednotlivých možností:

1. Start >> Ovládací panely (Control Panel)
2. Dále pokračuj do možnosti Síť a Internet (Network and Internet)
3. Potom klikni na Síť a centrum sdílení (Network and Sharing Center)
4. V postranním panelu tohoto okna vyber Změnit nastavení adaptéru (Change adapter settings)
5. Vyber adaptér, kterému chceš změnit MAC adresu, klikni na něj pravým tlačítkem a vyber Možnosti (Properties)
6. Běž do Rozšířené nabídky (Advanced) NEBO klikni na tlačítko Konfigurovat a teprve poté budeš mít možnost jít do Rozšířené nabídky
7. Hledej možnosti jako Network Address, MAC Address nebo Physical Address
8. Do volného pole vepiš novou MAC adresu bez dvojteček (např. 00112233445566).
9. Restartuj PC a ověř MAC adresu v terminálu podle návodu výše.

ZMĚNA PŘES REGISTRY

1. Start >> Spustit >> Do pole napiš regedit, otevře se editor registrů
2. Postupně se proklikej následujícím:
   HKEY_LOCAL_MACHINE >> SYSTEM >> CurrentControlSet >>
   Control >> Class >> {4D36E972-E325-11CE-BFC1-08002BE10318} >>
   Uvidíš spoustu složek jako: 0000, 0001, atd. Ty postupně projdi a v jedné

z nich se bude nacházet položka DriverDecs, u které bude vyplněný název tvé síťové karty, kterou jsi zjistil v předchozím kroku.
3. Klikni do volného prostoru a dej Nový >> Řetězová hodnota (String value), kterou pojmenuješ NetworkAdress a do hodnoty vepíšeš novou MAC adresu bez dvojteček (např. 00112233445566).
4. Nyní restartuj počítač a MAC adresu ověř v terminálu. Měla by být změněna.

ODKAZY:

- ➔ *https://wiki.archlinux.org/index.php/MAC_address_spoofing* (Několik dalších návodů, jak na Linuxu změnit MAC adresu – jednorázově, permanentně, při bootování...)
- ➔ *http://www.netuj.cz/bezpecnost-sprava-pc/jak-zmenit-mac-adresu* (Český obrázkový návod na změnu MAC adresy ve Windows)
- ➔ *standards.ieee.org/regauth/oui/oui.txt* (Seznam MAC adres přidělených konkrétním výrobcům)
- ➔ *http://technitium.com/tmac/index.html* (Utilita pro úpravu MAC adresy)

SESSION DATA Z PROHLÍŽEČE

CO TO JE?

Do session dat (známé taky jako relace nebo sezení) se řadí jakékoli data, které se ukládají do počítače, když brouzdáš po internetu. Patří mezi ně cookies, Flasg cookies cache, historie, uložené formuláře a hesla a historie vyhledávání. Dále DOMstorage a geolokace.

COOKIES jsou malé soubory, které jednotlivé stránky ukládají do počítače, aby mohly být načteny později (při každé další návštěvě téhož serveru prohlížeč tato data posílá zpět serveru; cookies běžně slouží k rozlišování jednotlivých uživatelů, ukládají se do nich uživatelské předvolby apod.). Existují dva typy cookies – cookies pro jednu session a trvalé cookies. Session cookies jsou vymazány, když se prohlížeč zavře. Jsou uchovávány v dočasné paměti a nedá se k nim poté dostat. Oproti nim trvalé cookies se uchovávají na uživatelově počítači dokud nevyprší jejich platnost nebo nejsou smazány. Tyto cookies se používají k tomu, aby sbíraly informace, jako je třeba to, na co se díváš nebo jaké stránky preferuješ.

Existují taky **FLASH COOKIES** (známé taky jako Local shared object nebo Supercookies), které se od prohlížečových cookies odlišují. Flash cookies jsou kousky dat, které ukládají do počítače stránky používající Adobe Flash.

Flash cookies tak mají základ v Adobe Flash a ukládají se jinam než prohlížečové cookies. Uložiště je přitom sdílené všemi prohlížeči, takže data uložená Firefoxem může načíst například Explorer a obráceně.

HISTORIE je seznam navštívených stránek seřazený podle data.

CACHE, známé také jako mezipaměť, je zásobník souborů z navštívených stránek. Smyslem mezipaměti je zrychlit načítání stránek, protože se některé soubory při další návštěvě načítají z cache, a ne stahují se znovu ze serveru.

FORMULÁŘE A HISTORIE VYHLEDÁVÁNÍ jsou ukládané logy o informacích, které byly zadány do webových formulářů a vyhledávacích lišt.

ULOŽENÁ HESLA jsou jakákoli hesla, která jsi při přihlašování k účtům povolil uložit pro pozdější snadnější přístup.

DOMSTORAGE je uložiště prohlížeče určené k organizaci dlouhodobých dat. Je zabudováno do prohlížeče a defaultně je povolené.

GEOLOKACE je nastavení prohlížeče, které umožňuje přednostně ukazovat ve vyhledávačích i jinde ta data, která se vztahují k tvému umístění. Při zadání „program kin“ ti Google vyhledávač primárně ukáže divadla a kina, která jsou poblíž místa, kde bydlíš.

PROČ SE TÍM ZABÝVAT?

Většina těchto věcí ukládá data o tom, co jsi viděl, kdy jsi to vidět a co jsi do prohlížeče zadával. Skladuje tak informace (neboli velké množství důkazů) o tvé aktivitě. Dokonce i když jsi maximálně anonymní, ale nepročistíš uložiště těchto dat, zůstane tvůj počítač plný logů o tvé online aktivitě. Pokud se angažuješ v subverzích aktivitách, mohou tě takové data dostat za mříže.

JAK NA TO?

Není náročné nastavit prohlížeč tak, aby nezadržoval tolik dat. Několik kliknutí v nastavení a jeden nebo dva addony dokážou zajistit, že určitá data nebudou vůbec ukládána nebo, pokud ukládána budou, tak budou po ukončení prohlížeče vymazána. Krom tohoto nabízeného řešení je možné spouštět prohlížeč přes LiveSystem, který nedovoluje datům, aby se ukládaly na pevný disk, protože běží pouze v RAM paměti (viz Livesystem str. 105).

Většina návodů, které následují, je přizpůsobena prohlížečům založeným na Firefoxu. Doporučujeme na nějaký takový prohlížeč přejít, protože kladou důraz

na bezpečnost a dají se snadno konfigurovat. Tvé první kroky by v prohlížeči měly mířit ke změně nastavení zabezpečení (standartně Možnosti/Options >> Soukromí/Privacy). Zruš zaškrtnutí u každé možnosti, která by uchovávala nějaké informace. Patří zde historie formulářů, historie stahování, historie prohlížení... Vypni cookies (většina stránek ale nebude fungovat správně) nebo je nastav tak, aby expirovaly, jakmile zavřeš prohlížeč. Spolehlivé je nastavit historii prohlížení, cache, cookies, nastavení stránek, historii stahování, offline data a uložená hesla tak, aby se vymazaly, když zavřeš prohlížeč.

Můžeš je zablokovat i ručně. Napiš to adresního řádku “about:config” a do načteného vyhledávání napiš, co chceš editovat, například cache nebo cookies. Změň nastavení, například “browser.cache.disk.enable”, na False a hodnotu možnosti, například “browser.cache.disk.capacity”, na nulu.

I když doporučujeme udělat obě z nabízených možností, nejsnadnější cestou k tomu, aby si prohlížeč nic nepamatoval, je používat ho v privátním módu. Většina prohlížečů nabízí tuto možnost, která zajišťuje, že počítač neukládá žádné záznamy o tvém prohlížení. Vždy používej privátní mód.

Provedením zmíněného bys měl předejít dobře známým hrozbám, ale jsou i jiné specifičtější věci, které bys měl také pozměnit, jako jsou Flash cookies, geolokace a DOMstarage.

K zablokování DOMstage napiš do adresního řádku „about:config“. Do vyhledávací lišty napiš „dom.storage“. Změň “dom.storage.enabled” na „false“ a “dom.storage.default_quota” změň na „0“. Toto DOMstorage zablokuje.

K zablokování geolokace napiš do vyhledávací lišty opět „about:config“ a pak do vyhledávání napiš “geo.enabled“. Tento řádek opět změn na false. Tak geolokaci zablokuješ.

K odstranění Flash cookies je nejlepší stáhnout addon nazývaný BetterPrivacy. Jeho nastavení umožňuje odstraňovat Flash cookies i jiné uložiště rozličnými způsoby.

ODKAZY:

- ➔ *http://www.allaboutcookies.org/privacy-concerns* (Podrobněji o cookies a jejich bezpečnostních rizicích)
- ➔ *https://www.mozilla.org/en-US/firefox/geolocation* (Podrobněji o geolokaci včetně návodů na jeho blokaci)
- ➔ Programy pro mazání session dat z prohlížeče: Click&Clean, BetterPrivacy

REFERER

CO TO JE?

Referer, nazývaná také jako referring page, je URL adresa stránky, ze které návštěvník na stránku přišel. Pokud klikneš na nějaký odkaz, stránka, na kterou se dostaneš, bude vědět, z jaké stránky ses na ni dostat. Referer je totiž část http požadavku, který prohlížeč posílá serveru.

PROČ SE TÍM ZABÝVAT?

Referer může stránce poskytnout informace o tvé aktivitě, protože dokáže říct, na jaké stránce jsi byl, když jsi na link klikal. Tato informace může být následně spjata s tvou IP k získání dalších informací o tvém prohlížení.

JAK NA TO?

Existuje několik programů nebo addonů, které pomáhají kontrolovat referery. Ve Firefoxu se jeden takový addon nazývá RefControl. Ten dovoluje nastavit, jakého referera stránka uvidí. Každé stránce můžeš přiřadit specifického referera nebo můžeš zvolit jedno nastavení pro všechny stránky. RefControl umí odesílat žádného referera, poslat jako referera stránku, na kterou přistupuješ a umí vytvořit specifického referera, který bude, jaký určíš. Doporučujeme ti změnit referera na kořenovou stránku nebo ho úplně zakázat.

Jinou možností je používat Privoxy, který je často zabalen spolu s TORem. V Privoxy můžeš měnit řadu aspektů tvého prohlížení. Tak jako RefControl i Privoxy umí skrýt referer, nastavit ho na kořenovou stránku nebo změnit na libovolnou možnost.

USER AGENT

CO TO JE?

User Agent (uživatelský agent) je soubor informací, které webový prohlížeč odesílá navštíveným stránkám, aby se identifikoval. Stránky následně mohou upravit svůj obsah tak, aby odpovídal patřičnému prohlížeči a operačnímu systému. User Agent se skládá ze šesti částí: název aplikace, její verze, kompatibilita, název prohlížeče, jeho verzi, nainstalovaná rozšíření a operační systém. Všechny tyto data se odvíjejí od toho, co na svém počítači používáš (jestli máš Linux nebo Windows, Internet Explorer nebo Firefox, atd.)

Příkladem informace, která se na webu zobrazuje, může být:
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)

PROČ SE TÍM ZABÝVAT?

Zakrytí informací poskytovaných User Agentem je důležité, pokud si přeješ předcházet tomu, aby webové stránky sbíraly informace o tvém operačním systému a prohlížeči. Pokud se tyto informace dostanou do rukou vyšetřovatelů, mohou napomoci tomu, aby si vytipovali podezřelé. Pokud totiž tvůj User Agent odpovídá tomu, který byl zaznamenán při ilegálních aktivitách, můžeš s nimi být rázem spojován.

JAK NA TO?

K zjištění tvého User Agenta napiš do adresního řádku prohlížeče „about:“ (dvojtečka je nutná). Následují způsoby, jak tyto informace měnit. Vždycky se opakovanou kontorlou User Agenta přesvědč, že změny fungují.

Mozilla Firefox podporuje addon, který se jmenuje User Agent Switcher, který by měl automaticky měnit tato data za tebe. Tato možnost se řadí mezi ty jednoduché a pohodlné, vždycky si ale ověř, že na aktivity, se kterými nechceš být spojován, používáš jiný, byť falešný User Agent.

Další možností je addon Privoxy, které dovoluje měnit data User agenta. Když nastavíš Privoxy jako své lokální proxy, které vyfiltruje tvé připojení, můžeš zároveň změnit User agenta na cokoli, co budeš chtít.

Pokud chceš User Agenta změnit manuálně, napiš do adresového řádku: „about:config“. Poté klikni na libovolný řádek pravým tlačítkem a v menu, které se ti objeví, vyber Nový >> Řetězec (String). Objeví se ti další okno, do kterého napiš: „general.useragent.override“. Následně se objeví další okno, do kterého napíšeš hodnotu řetězce (tzn. data jako z příkladu výše). Napiš sem takový User Agent, který budeš chtít, aby tvůj prohlížeč používal. Seznam možných User Agentů najdeš online. Některé stránky se nemusí zobrazovat správně nebo vůbec, kvůli nesprávné kompatibilitě, kterou bude uvádět tvůj změněný User Agent. Proto je dobré vybrat takový, který odpovídá nejběžnějším prohlížečům a operačním systémům. Navíc tím zvýšíš míru své vlastní nenápadnosti.

ODKAZY:

- ➔ *http://whatsmyuseragent.com* (Stránka pro zjištění User agenta)
- ➔ *http://www.yac.mx/cs/pc-tech-tips/internet/How_to_Change_the_User_Agents_in_Firefox_Chrome_and_IE.html* (Návod, jak změnit User agenta ve Firefoxu, Chormu a IE)

802.11 NICKNAME / HOSTNAME

CO TO JE?

802.11 nickname je funkce wifi připojení, které posílá tvou hostname (jméno tvého počítače) poskytovateli internetu.

PROČ SE TÍM ZABÝVAT?

Pokud se připojuješ na internet dejme tomu z veřejné wifi, která je později prošetřována, a jméno tvého počítače je tam zalogované, může to být s tebou (nebo s někým s totožnou hostname) spojené. Log bude ukazovat, že ses připojoval k této specifické wifi v konkrétní čas a dokáže tě tak spojit s aktivitami, které se na něm v tu chvíli děly.

JAK NA TO?

Nejlepší obranou proti tomuto je vybrat si běžný název počítače. Například default, počítač, PC, home, uživatel... Bude pak náročné dokázat, že jsi zrovna ty dělal něco na veřejné wifi, pokud je jediným důkazem to, že log a tvůj počítač se jmenují stejně, tedy například „počítač“.

ZMĚNA HOSTNAME VE WINDOWS

Ve Windowsu neexistuje snadný způsob, jak hostname změnit. Pokud už nějaké běžné jméno nemáš, doporučujeme ti, abys přeinstalovat systém a vybral si běžnější jméno nebo, ještě lépe, rovnou přešel na Linux.

ZMĚNA HOSTNAME V LINUXU

V Linuxu otevři terminál a zadej příkaz: [root@machine ~/dir]# iwconfig ath0 nickname “nový název”.

ODKAZY:

➔ *www.howtogeek.com/197934/hot-to-change-your-hostname* (Obrázkový návod, jak změnit hostname na Linuxu)

SKRIPTY

CO TO JE?

Skripty jsou atributy stránek, které dovolují určitým prvkům stránek fungovat a plnit své úkoly. Video, audio nebo dokonce základní prvky některých stránek vyžadují skripty.

PROČ SE TÍM ZABÝVAT?

Zatímco řada skriptů ti dovoluje dívat se na obsah stránek, ne všechny jsou tak prospěšné. Některé skripty se používají k reklamním účelům, k trackování tvého chování nebo k přístupu do tvého počítače, což je závažné ohrožení tvé bezpečnosti a anonymity.

JAK NA TO?

Hlavní problém je, že pokud některé skripty zakážeš, může to výrazně omezit schopnosti tvého prohlížeče. Obsah, ke kterému se chceš dostat, totiž bez některých skriptů vůbec nepůjde spustit (například videa na youtube, přihlašování do mailu...). Nicméně existují způsoby, které umožňují, abys povolil jen některé skripty.

První možností je manuálně skripty zakázat. Ty se tím pádem nebudou vůbec moci spouštět.

- ➔ K zablokování JavaScriptu ve Firefoxi: Nástroje >> Nastavení >> Obsah >> odtrhni „Povolit JavaScript“.
- ➔ K zablokování dalších skriptů ve Firefoxu: Nástroje >> Addons >> V záložkách Pluginy a Rozšíření vypnout Javu, JavaScript, Flash, Silverlight.

Existují také addony, které ti umožňují konkrétní skripty povolat, nebo zakazovat. Ghostery addon pro Firefox ti ukáže seznam skriptů, které na stránce běží, a dovolí ti vybrat, které z nich zablokovat. To však automaticky neznamená, že skriptům zabrání, aby běžely, což může být problém, pokud už tyto nechtěné skripty nemáš zablokované z dřívějška.

NoScript je jiný cenný addon pro Firefox. Defaultně blokuje veškerý aktivní obsah včetně Flash, Silverlight, JavaScriptu a Javy. Můžeš pomocí něj povolit určité skripty dočasně nebo permanentně a také přidat skripty na seznam vždy blokovaných. Pokud je NoScript používaný správně, znatelně snižuje riziko zneužití zákeřnými skripty. Pokud je zablokováno něco, co chceš vidět, tak to

naneštěstí vyžaduje několik kliknutí navíc a omezuje to tím pádem plynulost prohlížení. To se však zdá jako malá cena za výhody, které to přináší.

AdBlock, addon blokující reklamy (bannery, spoty ve videích apod.), je podobně užitečný Pokud mu dovolíš blokovat „basic list“, většina reklama bude od tohoto okamžiku blokována, nebude se načítat a neuvidíš ji.

Jedny z hlavních trackerů a analyzátorů chování uživatelů pohází od Googlu a Facebooku. Obrovské množství stránek používá některé jejich skripty (například tlačítka „To se mi líbí“, „Google plus“, facebookové komentáře...). Pokud na takové stránky vstoupíš a tyto skripty se načtou, Google a Facebook budou vědět, že jsi na těchto stránkách byl. Záznam si o tom navíc uchovávají na dobu neurčitou, proto je vhodné se těmto trackerům úplně vyhnout. Ochrání tě před nimi jak už zmíněné nástroje, tak třeba addon s názvem GoogleSharing. Ten filtruje tvé požadavky na většinu Google služeb skrze proxy a anonymizuje tak výsledky a brání Google, aby trackoval tvé online chování anonymizací tvé IP, HTTP hlaviček a User Agenta. Služba neuchovává žádné logy, šifruje komunikaci a byla vyvinutí anarchisty. (Poznámka: Tohle ti poskytna pouze základní anonymitu, proto je nejlepší pro každodenní brouzdání po internetu – pokud dělat něco nebezpečného, používej jedině TOR!). Můžeš také používat Scroogle, stránku, která dovoluje anonymizovat Google vyhledávání.

ŠIFROVÁNÍ PŘIPOJENÍ

CO TO JE?

V této kapitole se zabýváme šifrováním prohlížení pomocí HTTPS/SSL. Existují i jiné formy šifrování. Některé z nich nabízejí větší zabezpečení, jsou ale složitější. Více si o nich můžeš přečíst v odkazech.

Šifrování je způsob zabezpečení informací odesílaných nebo přijímaných skrze internet. Když přistupuješ na stránku, odesílané a přijímané informace putují jako obyčejný text z tvého počítače přes sít až k serveru, ke kterému se připojuješ. Kdokoli uprostřed tohoto připojení (tvůj poskytovatel, server, ke kterému jsi připojený, kdejaký slídil a fízl) může tyto informace vidět. Šifrování tomu zabraňuje tak, že text zakóduje – překlopí ho na (obecně) nerozluštitelný kód. HTTPS šifrování indikuje „https://“ na začátku URL adresy nebo malý zámek umístěný (většinou) na konci URL řádku. Můžeš ho nejčastěji vidět, když se přihlašuješ k emailu nebo k internetovému bankovnictví.

PROČ SE TÍM ZABÝVAT?

Šifrování je pro bezpečnost zásadní, protože nezašifrovaná data jsou jako pohlednice: kdokoli mezi odesilatelem a příjemcem je může vidět. Ačkoli SSL šifrování nezajišťuje perfektní bezpečnost, výrazně a jednoduše zvyšuje zabezpečení připojení proti možným slídilům.

Pokud používáš veřejné wifi připojení, je šifrování ještě důležitější, protože nemůžeš vědět, kdo toto připojení v danou chvíli používá spolu s tebou. Existují přitom různé nástroje i pro úplné laiky, které umožňují krást přihlašovací údaje z nezašifrované komunikace.

JAK NA TO?

SSL šifrování je snadné. Místo abys napsal „http://“, napiš do adresního řádku „https://“. Ne všechny stránky SSL šifrování umožňují, ale spousta z nich ano.

Pro ulehčení existuje firefoxový addon HTTPS Everywhere, který se automaticky připojuje pomocí HTTPS, je-li dostupné.

BEZPEČNOST

Počítačová bezpečnost má dvě hlavní složky: zabezpečení systému proti útokům a zabezpečení dat. První zahrnuje ochranu tvého počítače před viry, malwarem, keyloggery, rootkity a celou řadou dalších hrozeb. Druhá se zaměřuje na ochranu dat před kýmkoli, kdo o ně usiluje, a to pomocí šifrování dat, spravování logů a bezpečného mazání souborů. Následující bezpečnostní opatření staví mezi tebe a bezpečnostní složky nebo infiltrátory další ochranný val. Množství informací, které budou bezpečností složky schopné z tvého počítače získat v případě hackerského útoku nebo zátahu závisí jedině a pouze na času a námaze, kterou věnuješ zabezpečení svého systému. Důrazně doporučujeme věnovat se tomuto úsilí jak jen to jde, protože jde často o jediný způsob, který chrání tvůj počítač proč žádostivým zrakem státu.

BEZPEČNÉ MAZÁNÍ

CO TO JE?

Když odstraňuješ nějaký soubor tak, že prostě vysypeš koš, tak tyto soubory ve skutečnosti smazány nejsou. Počítač pouze udělá to, že označí místo, které tyto soubory zabírají, jako „prázdné“ a dovolí tak novým souborům, aby se na toto místo v případě potřeby zapsaly. Soubor tím pádem zůstane nedotčený až do chvíle, kdy je přepsán jiným souborem (Podobná situace se děje i ve chvíli, kdy soubor vyjímáš [ctrl+x]. Když ho totiž vkládáš na nové místo, ve skutečnosti se původní soubor „smaže“ a na nové místo se vloží jeho kopie. Příkaz ctrl+x slouží zkrátka jen k tomu, abys nemusel dělat dva kroky a vyjímaný soubor mazat ručně.). Bezpečné mazání naopak zapisuje několikrát po sobě na místo originálního souboru náhodná data, takže ho opravdu odstraní.

PROČ SE TÍM ZABÝVAT?

Soubory, které jsi smazal běžnou cestou, na počítači zůstávají, i když je nevidíš. Pokud se jedná o nějaká citlivá data a tvůj počítač ti zabaví fízlové, může to být problém, protože jejich technici dokážou tato data obnovit. Někdy jsou dokonce schopni obnovit i taková data, která už byla přepsána. Aby soubory, která jsi smazal, nemohly být takto odhaleny, je nezbytné je mazat bezpečně.

JAK NA TO?

Bezpečné mazání se provádí pomocí speciálních programů a příkazů. Ty většinou umožňují mazat konkrétní položky, obsahy složek i volný diskový prostor.

Jak efektivní skartování souborů je, záleží na použitém algoritmu. Obecně se má za to, že čím více průchodů (přepsání) algoritmus provede, tím větší je šance, že zakryl všechny stopy. Čím více průchodů, tím déle však mazání trvá. Často se doporučuje používat algoritmus Gutmann, který má 35 průchodů. Jeho tvůrce ale sám říká, že byl navržený pro disky z 90. let, které fungovaly na jiném principu než dnešní disky. Proto je podle něj naprosto zbytečné používat 35průchodové mazání a údajně postačí několik přepsání náhodnými daty. Na základě toho doporučujeme místo algoritmu Gutmann používat algoritmus Schneider, který má 7 průchodů (nejdříve zapisuje jedničky, podruhé nuly a pak 5x náhodná data).

V Linuxu potřebuješ mít nainstalovaný například program Shred, který je součástí některých distribucí. Tento program pracuje pouze v terminálu, ale nejedná se o nic složitého. Jeho výhodou je, že můžeš sám určit, kolikrát se má daný soubor přemazat a jakým způsobem. Pro bezpečné smazání fotky umístěné například ve složce Obrázky stačí tento příkaz: shred -zvn 10 /home/uživatel/Obrázky/nazev_fotky.jpg (písmeno Z znamená, že se soubor na závěr přemaže nulami, V znamená, že uvidíš jak mazání probíhá a N 10 znamená, že se soubor přepíše desetkrát, číslo samozřejmě můžeš změnit). Existuje také program Secure-delete, u něj ale nemůžeš určit počet přepisů (defaultně maže 35x).

Ve Windowsu budeš potřebovat skartační program. Typicky jej nainstaluješ, v nastavení vybereš žádaný algoritmus mazání a následně již vybíráš, co přesně chceš smazat. Doporučujeme si takový program pořídit a nedjříve promazat volné místo. Pokud jsi totiž nikdy bezpečné mazání nepoužíval, máš na volném prostoru disku bezpochyby spoustu zbytků souborů, které na něm byly uloženy už dávno. Promazání volného místa tě jich zbaví. Volné místo na disku doporučujeme mazat každý týden. V kombinaci s bezpečným mazáním inkriminujících souborů bys měl zabránit bezpečnostním složkám, aby se k nějakému citlivým informacích dostali, pokud nepoužijí nějaký hodně drahý mikroskop, což je možné, ale zároveň vysoce nepravděpodobné.

ODKAZY

- ➔ *https://en.wikipedia.org/wiki/Data_remanence* (Popis toho, jak funguje zapisování dat)
- ➔ *https://www.cs.auckland.an.nz/~pgut001/secure_del.html* (text od tvůrce algoritmu Gutmann o bezpečném mazání, kde stojí za přečtení hlavně epilogy, ve kterých vysvětluje, proč je dnes 35 přepsání zbytečných)
- ➔ *http://www.ubuntugeek.com/tools-to-delete-files-securely-in-ubuntu--linux.html* (Návod na bezpečné mazání v Linuxu)
- ➔ *https://ssd.eff.org/en/module/how-delete-your-data-securely-linux* (Další návod, jak bezpečně mazat na Linuxu)

- ➔ *https://ssd.eff.org/en/module/how-delete-your-data-securely-mac-os-x* (Návod na bezpečné mazání v MACu)
- ➔ *https://ssd.eff.org/en/module/how-delete-your-data-securely-windows* (Návod, jak mazat ve Windows pomocí Bleach Bit a další informace)
- ➔ Programy pro bezpečné mazání: Ccleaner (komplexní mazání všeho možného – cookies, volný prostor, soubory, cache...), Blechbit, Eraser (mazání souborů a volného místa)
- ➔ Nástroje určené pro Linux: Shred, Wipe, Secure-Delete

VIRY A MALWARE

CO TO JE?

Virus je program, který, pokud je uložený v počítači, replikuje sám sebe a šíří se dál. Často poškozuje nebo zasahuje do operačního systému a pracuje bez vědomí uživatele – například spouští programy nebo je mění.

VIRY se na jiné počítače přenášejí prostřednictvím jakéhokoli infikovaného souboru, který si předaly například flashkou nebo přes internet.

MALWARE je zákeřný software navržený k tajnému infiltrování systému bez souhlasu uživatele. Často je dotěrný a zasahuje do operačního systému nebo napadá uživatelovo soukromí. Příkladem malwaru je spyware, adware, červi nebo trojští koně.

PROČ SE TÍM ZABÝVAT?

Viry a malware mohou narušit správné fungování počítače, poškodit nebo zničit soubory a vymazat celý disk. Krom toho, že mít zničený počítač je pěkná otrava, je ohrožena také tvá anonymita a bezpečnost.

Vše, co na počítači děláš, je ohrožené, pokud se do toho vměšují viry nebo malware, protože destabilizují systém a dělají si, co chtějí. Státní agentury bažící po informacích navíc dokážou vytvářet viry a malware na míru konkrétním uživatelům.

JAK NA TO?

Antivirové a antimalwarové programy dokážou snížit hrozbu virů a malware. Jejich bezpečnost nicméně odvisí od jejich kvality, uživatelského nastavení a aktualizacích. Do odkazů jsme dali několik freewarových programů, můžeš používat ale i kradené placené programy.

Důležité je, že antiviry a anti-malware pouze reagují na existující hrozby. Software se umí s virem vypořádat až poté, co je taková hrozba identifikována a program je aktualizovaný (proto se tak často aktualizují virové databáze). Pokud ale takový vir nebo malware už v počítači máš, může být pro tebe pozdě.

Firewall je další pomocník, který dokáže zabránit útokům malware, virů a celé řady jiných hrozeb. Zabraňuje totiž neautorizovaným vnějším zdrojům, aby přistupovaly do tvého počítače, pokud nesplňují určitá bezpečnostní kritéria. Podobně jako antiviry a anti-malware software je i síla firewallu závislá na uživatelském nastavení a pravidelných aktualizacích.

Některé obecné tipy k ochraně před viry:

- ➔ Stahuj pouze takové soubory a otevírej pouze takové emailové přílohy, jejichž obsah znáš.
- ➔ Měj svůj antivirus a firewall plně aktualizovaný.
- ➔ Nastav programy na silné nebo nejsilnější zabezpečení.
- ➔ Ujisti se, že tyto programy běží po celou dobu.
- ➔ Každý týden počítač těmito programy skenuj.

Jinou možností je používat linuxový operační systém. Linux je ze své podstaty bezpečnější, protože většina virů a malware je navrhována pro Windows a Max a Linuxové bezpečnostní aktualizace jsou mnohem komplexnější, protože se jedná o open source. Zatímco editace firewallu v Linuxu může být pro většinu lidí těžký oříšek (včetně nás samotných), existují programy, jako je Firestarter, které celý proces zjednodušují. Linux také nabízí antivirový program KlamAV, který doporučujeme používat ke skenování všech souborů, které jsou posílány na počítače s Windows, protože Linux může windowsowské viry přenášet, aniž by sám byl infikován.

ODKAZY:

- ➔ *https://ubuntuforums.org/showthread.php?t=51081* (Podrobněji o virech a Linuxu)
- ➔ https://en.wikipedia.org/wiki/Comparison_of_antivirus_software (seznam a srovnání antivirů seřazených podle kompatibility se systémem)
- ➔ Freeware antiviry: AVG, Avira, Avast, Bitdefender, ClamXav, Panda
- ➔ Placené antiviry: Eset NOD32, Kaspersky (považovaný spolu s NO-Dem za nejlepší), Norton, rozšířené verze free antivirů
- ➔ Firewally: Comodo (Windows, Android), Kaspersky (Windows, OSX), TinyWall (Windows), Norton Internet Security (Windows), Agnitum, Firestarter, ZoneAlarm

KEYLOGGERY

CO TO JE?

Keylogger je program nebo část hardwaru, která ukládá každé stisknutí klávesy a vytváří log, který poté může odeslat konkrétnímu příjemci.

Hardwarový keylogger je malý, baterií napájený plug, která připojuje klávesnici k počítači; často se podobá klávesnicovému plugu. Hardwarový keylogger musí být fyzicky v počítači, aby získával logy. Softwarový keylogger oproti tomu dovoluje dálkový monitoring bez nutnosti fyzicky do počítače zasáhnout. Často je instalován pomocí spyware.

PROČ SE TÍM ZABÝVAT?

Keyloggery jsou zcela očividnou hrozbou. Mohou zachytit hesla, přihlašovací údaje, historii prohlížení a cokoli jiného psaného. Je tak možné obejít šifrování, narušit anonymní prohlížení, bezpečné emailové účty a navíc dát bezpečnostním složkám pěkný obrázek o veškeré tvé aktivitě.

JAK NA TO?

Informace z předešlé kapitoly platí i pro keyloggery. Firewall, antiviry a antimalware programy, programy detekující cizí vniknutí a obezřetnost při stahování – to vše snižuje šanci, že si na počítač nevědomky keylogger nainstaluješ. Livesystem, který zmíníme za chvíli, také obchází keyloggery, protože používá pouze RAMku. Útoky keyloggerů může zmařit i používání virtuální klávesnice. Místo, abys mačkal klávesy, vybíráš jednotlivá písmena na klávesnici přímo na obrazovce. Opět ale záleží na kvalitě virutální klávesnice, více v odkazech. Bezpečnost zvyšují i manažery hesel (viz Hesla na další straně).

ODKAZY:

- ➔ *http://www.symantec.com/connect/articles/introduction-spyware-keyloggers* (Podrobněji o keyloggerech)
- ➔ *https://securelist.com/analysis/publications/36138/keyloggers-how--they-work-and-how-to-detect-them-part-1/* (Podrobněji o keyloggerech podruhé)
- ➔ *https://www.raymond.cc/blog/how-to-beat-keyloggers-to-protect--your-identity/* (Souhrnný test antikeyloggerů a virtuálních klávesnic)
- ➔ Anti-keyloggery: KeyScrambler, KL-Detector, SpyShelter

ROOTKITY

CO TO JE?

Rootkit je software, který umožňuje privilegovaný přístup k počítači, aniž by byl známý jeho oprávněný uživatel. Rootkity jsou často navrženy právě tak, aby aktivně maskovaly svou přítomnost ovládáním chodu operačního systému. Rootkity umožňují opakovaný přístup a obcházení přístupového ověřování (hesla).

PROČ SE TÍM ZABÝVAT?

I rootkity narušují tvou anonymitu a bezpečnost. Umožňují totiž vzdálený přístup k tvému počítači, manipulaci s tvým operačním systémem a obcházení většiny bezpečnostních prvků vyřazením patřičného softwaru. V praxi to znamená prozrazení veškerých tvých aktivit, které na počítači děláš.

JAK NA TO?

Nejlepší ochranou je prevence. Správné bezpečné chování na internetu a obezřetnost při stahování znamená mnoho. Rootkit obecně potřebuje dostat přístup do tvé počítačové administrace, aby mohl přistupovat, kam potřebuje. Tomu můžeš zabránit tím, že zakážeš přístup k rootu (Linux) nebo omezíš administrativní práva (Windows) – platí to mimo jiné právě pro dialogová okna, která se zobrazují před instalací softwaru. Nikdy neposkytuj administrační přístup k tvému počítači nebo heslo nikomu, kdo jej nepotřebuje, nebo nikomu, komu plně nedůvěřuješ. Šifrování části nebo celého disku a použití silného hesla rozhodně není na škodu.

Vzhledem ke skryté povaze rootkitů je jejich odhalení obtížné. Obzvláště pro uživatele, kteří nedisponují rozsáhlými znalostmi o počítačích. Některé programy, jako například antimalwarové ochrany, mají schopnost detekovat rootkity. Linux disponuje programem chkrootkt, který je navržen ke stejnému účelu. Podobné program existují i pro Windows. Vedle těchto možností je možné ještě analyzovat uložiště paměti počítače, to však vyžaduje zkušenosti a znalosti.

Pokud se domníváš, že je tvůj počítač napadený rootkitem, tak nejjednodušší nebo také jedinou možností může být přeinstalování celého operačního systému. Ještě předtím se ale můžeš zkusit poohlédnout po nějaké pomoci online.

ODKAZY:

➔ Detekce a odstranění rootkitů: Kaspersky TDSSKiller, Sophos Rootkit Removal, AVG Anti-Rootkit, Rootkit Hunter, GMER

HESLA

PROČ SE JIMI ZABÝVAT?

Síla hesla, tvůj přístup k heslům a k jejich používání jsou klíčové pro bezpečnost tvého počítače, šifrování a uživatelských účtů. Jednoduchá hesla, pusa na špacíru a neobezřetné zadávání přihlašovacích údajů na neznámém počítači může prozradit tvé šifrování a další činnosti.

JAK NA TO?

Zde jsou nějaké tipy k heslům:

- ➔ NIKDY nikomu neříkej své heslo.
- ➔ Měj heslo dlouhé alespoň 15 znaků. Čím je heslo delší, tím je obtížnější jej prolomit útokem zvenčí (například tzv. slovníkovými útoky, které v krátkých a rychlých cyklech procházejí známá a slovníková slova a zkouší potvrdit přístup dokud heslo neuhádnou).
- ➔ Nikdy nepoužívej jako heslo své uživatelské nebo vlastní jméno a cokoli dalšího spojeného s tvým životem.
- ➔ Nikdy nepoužívej slova, která by mohla být v jakémkoliv slovníku. Tato hesla je nejsnazší prolomit (samozřejmě se nespoléhej ani na nespisovné výrazy).
- ➔ Ke každému účtu měj odlišné heslo. Nikdy nepoužívej jedno heslo pro více účelů.
- ➔ Při vymýšlení hesla používej malá a velká písmena, čísla a specifické symboly (@%`;#^&\!). Takto ztížené heslo odolá pokusům o prolomení déle.
- ➔ Pro snazší zapamatování složitého hesla ti může pomoci například použití prvních písmen nějaké básně či písničky.
- ➔ Čas od času všechna hesla změň. Frekvence změny záleží na požadované úrovni bezpečnosti.
- ➔ Pokud se přihlašuješ na počítači, kterému stoprocentně nedůvěřuješ, můžeš použít virtuální klávesnici nebo LiveSystem, abys předešel tomu, že své heslo vyzradíš.
- ➔ Existují programy, které umožňují vytvářet, ukládat a zašifrovat databáze hesel pod jedno hlavní heslo – tzv manažery hesel (obstojně fungující program s vícero bezpečnostními prvky je například KeePass; rozhodně v žádném případě neukládej svá citlivá hesla do databáze internetového prohlížeče). Podobně může fungovat i obyčejný textový dokument, který uložíš na zašifrovaný disk. Pro zvýšení bezpečnosti můžeš okolí hesla vyplnit náhodnými znaky či informacemi tak, abys zmátl případného čmuchala, který by se k takovému souboru dostal.

ODKAZY:

- ➔ *http://www.antimalware.cz/blog/jak-vytvorit-bezpecne-heslo* (Rady a tipy na silné hesla – česky)
- ➔ h*ttp://www.cnews.cz/navody/bez-silneho-hesla-neprezijete-rady-tipy--k-bezpecnosti-na-internetu* (Další rady a tipy na silné hesla – česky)
- ➔ *http://www.pcmag.com/article2/0,2817,2407168,00.asp* (Srovnání několika manažerů hesel)
- ➔ *http://www.wikihow.com/Create-a-Secure-Password* (Tipy na vytvoření silného hesla – anglicky)
- ➔ *http://www.makeuseof.com/tag/how-to-create-strong-password-that--you-can-remember-easily* (Rady a tipy na práci s hesly – anglicky)
- ➔ Manažery hesel: KeePass, LastPass, DashLane, 1Password, Master Password

ŠIFROVÁNÍ DAT

CO TO JE?

Šifrování znamená kódování dat. Nešifrovaná data jsou přístupná jako prostý text, ale šifrovaná data jsou plná čísel a nečitelných kódů, které není možné přečíst – tedy pouze v případě, že není šifrování nebo heslo prolomeno.

Šifrovat se dá buď celý disk, oddíl na disku nebo jen konkrétní soubor. Šifrování celého disku zašifruje na hardwarové úrovni celý tvůj disk. To znamená, že se k jeho obsahu nikdo bez klíče nedostane, a to i v případě, že ti disk fyzicky někdo sebere. Data se zašifrují ve chvíli, kdy šifrovaný disk vytváříš, a dešifrují se ve chvíli, kdy k nim přistupuješ. Šifrování souborů a oddílů umí zašifrovat konkrétní soubor nebo oddíl, který má v sobě více souborů.

PROČ SE TÍM ZABÝVAT?

Šifrování je rozhodující zeď mezi tvými soubory a těmi, kdo si je přejí získat. Jejich šifrování tedy zabraňuje, aby je někdo získal dokud neprolomí šifrování nebo hlavní heslo. Při každé razii na anarchisty slýcháme o denících, diářích a počítačích, které byly zabavené a použité k podepření případu. Zabavený počítač a všechny soubory na jeho disku se stávají automaticky důkazy. Deníky a diáře na nich uložené zase podávají docela přesný profil o aktivitách člověka a jeho společenské síti. Tomu je možné zabránit, pokud fízlové zabaví počítač, který je zašifrovaný nebo jeho vlastník zašifroval alespoň důležité soubory - telefonní čísla, klíče k dalším šifrovaným oddílům, osobní poznámky,

rozpracované texty... Vyšetřovatelé v takovém případě narazí, protože nejsou schopni se k těmto souborům dostat. Šifrování je důležité, proto šifruj!

JAK NA TO?

A) ŠIFROVÁNÍ CELÉHO DISKU

Šifrování celého disku může být provedeno již při instalaci operačního systému (některé linuxové distribuce nabízejí tuto možnost), nebo tak může být učiněno posléze s využitím určitého softwaru. Vyvarujeme se návodu, který by popisoval celé šifrování krok za krokem, k tomu jsou lepší již existující návody, které uvádíme v odkazech.

Navzdory všem výhodám má šifrování celého disku jednu velkou nevýhodu, kterou může počítačový expert zneužít k tomu, aby dostal přístup k datům na tvému disku. Při šifrování celého disku musí být malá část disku ponechána nezašifrována, aby mohla rozšifrovat zbytek. Právě tato část může být zneužita k získání přístupu k tvému disku, a to pomocí tzv. cold-boot útoku. Jedním z možných způsobů, jak se tomuto problému vyhnout, je umístit nezašifrovanou část na flash disk a skrýt jej. V odkazech uvádíme návody, které popisují, jak to provést.

B) ŠIFROVÁNÍ ODDÍLU

Šifrované oddíly vytvářejí pro vaše složky a soubory malé „pokojíčky“. Celý obsah šifrovaného oddílu nelze přečíst, dokud jej nedešifrujete. Velmi oblíbený program pro vytváření a otevírání šifrovaných oddílu je TrueCrypt, který považujeme za základ této kapitoly. Zašifrováním oddílu vlastně vytvoříš samostatnou část disku, kterou poté můžeš pomocí TrueCryptu načíst a dešifrovat, aby ses dostal k datům, které obsahuje. Fyzicky se samozřejmě tato data nachází na tvém harddisku, nedají se přečíst jako nezašifrovaná data.

Existuje také možnost vytvořit tzv. skrytý oddíl. Při vytváření uvedeš dvě odlišná hesla. Jedno bude pro vnější „fiktivní“ oddíl, druhý bude pro vnitřní skrytý oddíl. Pokud budeš (ne)legálně donucen vydat své heslo k šifrovanému oddílu, můžeš vydat heslo k vnějšímu oddílu a nikdo nebude vědět, že se zde nachází i oddíl vnitřní. Takto můžeš udržet své soubory v tajnosti.

Nejprve se vytváří vnější oddíl. Doporučujeme použít silný šifrovací algoritmus, nejlépe AES-Twofish-Serpent a jako hash algoritmus vybrat Whirlpool. Čím silnější algoritmus, tím je těžší ho prolomit. V dalším kroku budeš vybídnutý k náhodnému kroužení kurzorem myši. Toto kroužení bude náhodně generovat čísla, které poslouží k vytvoření šifry. Čím chaotičtěji budeš kroužit kurzorem, tím obtížnější bude prolomit tvou šifru. V dalším kroku budeš vyzván k nahrání

nějakých dat do vnějšího falešného oddílu. Tento krok podporuje iluzi, že se jedná o opravdový oddíl, pakliže jsi donucen vydat své heslo. V dalších krocích se celý proces opakuje, tentokrát však již pro vytvoření opravdového vnitřního oddílu. Heslo k těmto oddílům je nejlepší se naučit nazpaměť.

C) DALŠÍ TIPY K ŠIFROVÁNÍ

- ➔ Vždy používej silné heslo (1234 nebo ASDF to opravdu není). Tvé šifrování je jen tak silné, jak silné je heslo, které jsi k jeho ochraně použil.
- ➔ Dávej si pozor na keyloggery. Používej raději virtuální klávesnici, Live-System nebo manažer hesel.
- ➔ Při šifrování používej nejsilnější možný algoritmus. Za nejsilnější je považován AES-Twofish-Serpent.
- ➔ Vytvoř si šifrovaný oddíl na flashce. Tu je snadné ukrýt před zraky fízlů nebo zlodějů, je snadné a méně bolestné ji zničit, kdyby ses dostal do průseru a dá se snadno přenášet, pakliže budeš mít u sebe i portable verzi TrueCryptu. Na počítači tím pádem nemusíš mít nic inkriminujícího, to si budeš nosit na flashce. Ve chvíli, kdy s tím budeš potřebovat nakládat, prostě připojít flashku k počítači a pomocí TrueCryptu ji otevřeš.
- ➔ Používej šifrovaný oddíl společně s LiveSystemem, abys předešel zaznamenávání údajů o uložených datech.
- ➔ Cítíš-li pochybnosti, šifruj. Čím méně toho proti nám budou vyšetřovatelé mít, tím lépe. Přemýšlej nad tím, co chceš, aby bylo použito před soudem... Pokud nechceš, aby se některé data objevily v rukou nepřítele, zašifruj je!

D) POZNÁMKA K NEJISTÉ BEZPEČNOSTI TRUECRYPTU:

V květnu 2014 dali od TrueCryptu jeho vývojáři ruce pryč, když vydali neočekávanou zprávu, že jeho používání již není bezpečné a lidé by měli přejít na jiný nástroj, například BitLocker od Microsoftu. To vyvolalo celou řadu domněnek, konspiračních teorií a obav, zda je vůbec TrueCrypt bezpečné používat.

Dnes je všeobecně přijímané, že poslední důvěryhodná verze je 7.1a, která prošla také auditem a kontrolou kódu, který je volně přístupný. Poslední audit z května 2015 došel k závěru, že nenašel žádné důkazy o zadních vrátkách nebo bezpečnostních chybách, které by TrueCrypt dělaly nepoužitelným. To ale neznamená, že je TrueCrypt perfektní. Auditoři našli několik menších závad (popsané na http://blog.cryptographyengineering.com/2015/04/truecrypt-report.html), které bude do budoucna potřeba opravit. Pokud chceš nadále TrueCrypt používat, používej tuto ověřenou verzi 7.1a.

Do budoucna se nepředpokládá, že by vyšla nová verze TrueCryptu, spíše se bude jednat o nástroj založený na stejném kódu, který ponese jiný název.

Nyní jsou vyvíjeny tyto náhrady: CipherShed, VeraCrypt, Command line, se kterými nemáme zkušenosti.

ODKAZY:

- ➔ *https://uzivatel.wordpress.com/2010/04/06/truecrypt-ako-sifrovat-systemovy-disk* (Slovenský návod jak šifrovat systémový disk v TrueCryptu)
- ➔ *magazin.stahuj.centrum.cz/sifrovani-2-dil-jak-pouzivat-truecrypt* (Šifrování oddílu v TrueCryptu – česky a s obrázky)
- ➔ https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software (Srovnání šifrovacích programů)
- ➔ www.abclinuxu.cz/clanky/cold-boot-utok-popis-obrana (Český popis cold-boot útoku a obrana proti němu)
- ➔ mizu.sk/bezpecnost-informacnych-systemov/cold-boot-utok-na-kryptovacie-kluce (Podrobnější popis cold-boot útoku, opět česky)
- ➔ www.pepak.net/bezpecnost/utoky-na-operacni-pamet/ (Obecně o cold-boot útocích)

LINUX

PROČ SE JÍM ZABÝVAT?

Linux je v zásadě mnohem bezpečnější než Windows už ve svém základním nastavení. Je to jednoduše proto, že je to open source, to znamená, že jeho kód je volně přístupný. Na rozdíl od něj je Windows patentovaný operační systém a jeho úpravy a aktualizace vydávají pouze vývojáři Microsoftu. Linux, tím že je open source, může být udržován takřka kýmkoliv. To znamená, že jakékoliv bezpečnostní trhliny jsou opraveny mnohem rychleji a systém je proto bezpečnější. Windows a Mac jsou navíc mnohem častějšími terči útoků. V praxi to znamená, že je Linux imunní vůči většině virů a dalšímu nebezpečnému softwaru.

Linux dále nabízí širokou nabídku svobodných programů, které poskytují velkou pomoc při zajišťování soukromí a anonymity. Jak bylo naznačeno výše, některé bezpečnostní úkony jsou na Linuxu snazší.

Podoba Linuxu se liší podle distribuce (Ubuntu, Fedora, OpenUse, Redhat, Knoppix, Debian). Každá distribuce se liší podle vnitřního jádra. Pro běžného koncového uživatele bude klíčový rozdíl ve vzhledu uživatelského rozhraní a v obtížnosti ovládání. Například současné verze Ubuntu jsou vizuálně přehledné a uživatelsky nenáročné jako Windows.

JAKÉ MÁ NEVÝHODY?

Hlavní nevýhodou Linuxu může být nekompatibilita. Některé programy jednoduše v Linuxu nefungují. Existuje však několik řešení. Prvním je program Wine, který umí pracovat se soubory určenými pro Windows. Není to ale zcela elegantní a stoprocentně funkční metoda zejména u náročnějších programů. Druhá možnost, Linux nabízí programy podobné těm, které jsou dostupné pouze pro Windows nebo Mac. Například GIMP je svobodným ekvivalentem Photoshopu apod. Nevýhodou samozřejmě je, že tyto programy nejsou vždy tak uživatelsky přívětivé nebo obsáhlé svými funkcemi jako jejich protějšky od Adobe. Třetí možností je použití LiveSystemu s Windows, který bude používat pouze RAM tvého počítače, zatímco na běžnou činnost budeš používat Linux.

ZÁVĚR

Linux je cesta k větší bezpečnosti a anonymitě. Mnohé bezpečnostní opatření jsou velice snadné oproti Windows a nabízejí v základu více bezpečnosti. Nevýhodou je určitá odlišnost od Windows, což platí zejména pro začínající uživatele, a některé omezené funkce.

LIVESYSTEM

CO TO JE?

LiveSystem je přenosný operační systém, který se může bootovat z CD (LiveCD) nebo flash disku (LiveUSB). LiveUSB na rozdíl od CD umožňuje v některých verzích distribuce operačního systému ukládat data, která byla během spuštění uložena. Podstata těchto systémů je, že využívají pouze RAM paměť daného počítače.

PROČ SE TÍM ZABÝVAT?

LiveSystémy zvyšují bezpečnost a anonymitu. Tím, že využívají RAM počítače, zabraňují, aby na počítači zůstaly po jejich aktivitě stopy. A protože nepotřebují harddisk počítače, neumožňují instalovat nejrůznější zákeřné sledovací programy.

LiveSystem je vhodný hlavně, když používáš veřejně přístupný počítač nebo jakýkoli jiný, který nespravuješ ty sám. Takové počítače mohou obsahovat zmíněné keyloggery, viry a jiné programy, které ohrožují tvoji bezpečnost. Protože LiveSystem nezanechává na počítači žádné stopy o své činnosti, zabraňuje, aby v počítači po tobě zbyly logy a snippety. Některé LiveSystemy

jsou specificky navrženy tak, aby poskytovaly anonymitu a bezpečnost a zároveň obsahovaly služby, jako je TOR prohlížeč, anonymní a šifrovaný mail a komunikátor, virtuální klávesnice a software k hackování bezdrátových sítí.

JAK NA TO?

Vytvoření LiveSystemu záleží na tom, jakou službu si vybereš. Nejčastěji to znamená stáhnout LiveSystem z internetu a nainstalovat ho na flash disk nebo vypálit na CD. Užitečné rady najdeš v odkazech.

Když vybíráš operační systém, poohlížej se po následujících věcech:

- ➔ Šifrovací program (abys mohl přistupovat k šifrovaným souborům, aniž bys zanechával na harddisku stopy).
- ➔ Anonymizační programy, jako jsou TOR, MAC changer a další.
- ➔ Emailový klient, který podporuje šifrování.
- ➔ Virtuální klávesnici

Obecně je moudré vyžívat LiveSystem, když:

- ➔ Přistupuješ k šifrovaným datům (tím zabráníš logování názvů šifrovaných souborů, jejich obsahu atp. Zároveň tím můžeš obejít další bezpečnostní hrozby, jako je Keylogger).
- ➔ Pracuješ s citlivými daty (stejný důvod jako výše).
- ➔ Používáš cizí počítač (tyto počítače nemusí být dostatečně zabezpečené nebo již obsahují nebezpečný software).
- ➔ Provádíš citlivý průzkum (opět zamezuješ zaznamenávání tvé aktivity. Společně s anonymizačními programy ti LiveSystem pomůže skrýt tvou přítomnost na internetu).

ODKAZY:

- ➔ *https://cs.wikipedia.org/wiki/Live_CD* (Více o Livesystemech)
- ➔ *https://en.wikipedia.org/wiki/Live_USB* (Více o Livesystemech – tentokrát česky)
- ➔ *https://en.wikipedia.org/wiki/Comparison_of_Linux_distributions#Live_media* (Srovnání Livesystemových linuxových distribucí)
- ➔ *https://tails.boum.org* (Vysoce doporučovaný Livesystem – TOR, GireGPG a Claws Mail, HTTPS Everywehre, Aircrack-ng, Pidgin s OTR, virtuální klávesnice a spousta dalšího open-source)
- ➔ *https://www.privacy-cd.org* (Livesystem určený pro procházení zašifrovaných dokumentů, není možné přistupovat na internet)
- ➔ *http://www.sabayon.org* (Livesystem se zabudovaným TORem)

EMAIL

CO TO JE?

Zdá se, že s rozšířením mobilních telefonů a sociálních sítí používají lidé emailovou komunikaci méně a méně. Emaily ale stále poskytují rychlý a snadný způsob, jak komunikovat s okolím. Vývoj bezpečnostních prvků emailové komunikace navíc dává našim komunikačním kanálům velké výhody.

PROČ SE TÍM ZABÝVAT?

Stejně jako jakákoliv jiná komunikace, i emaily mohou být zachyceny. Přihlédneme-li k tomu, že emaily putují přes mnoho sítí, jak přes ty zabezpečené, tak nezabezpečené, neměli bychom je považovat za bezpečnou formu komunikace. To, co autority zjistí ze zadrženého emailu, samozřejmě závisí na jeho obsahu a formě. Pokud zpráva obsahuje citlivé informace, může to vést k raziím, zatýkání nebo vyšetřování. Mail je zároveň velmi snadný způsob, jak zmapovat komunikační síť, a to jednoduše na základě toho, kdo si s kým píše, jak často a o čem. Bezpečnostní a/nebo anonymizační opatření mohou snížit nebezpečí, které emailová komunikace skýtá.

JAK NA TO?

Jak přistupovat k emailové komunikaci se odvíjí od tvých potřeb. Můžeš hledat bezpečnost, anonymitu a pokud je to možné, tak obojí. Anonymity dosáhneš nejlépe anonymním prohlížením internetu, anonymními remailery nebo používáním rozepsané (draft) pošty. Bezpečnost zvýší šifrování emailu a/nebo použití kódovaného jazyka. Je možné dosáhnout obojího – například odesláním zprávy v kódovém jazyce prostřednictvím anonymního mailu.

A) REMAILERY

Anonymní remailery (např. QuickSilver, paranoia remailer, Mixmaster, noreply) vezmou zprávu a předají ji adresátovi, aniž by zobrazily její původ. Různé druhy remailerů poskytují různé strategie anonymity a soukromí. Záleží tudíž na konkrétním remaileru. Než si nějaký Remailer vybereš a použiješ, důrazně doporučujeme ho nejdříve prověřit. Remailery fungují podobně jako proxy servery. Vezmou původní zprávu, odejmou z ní tvou IP adresu a hlavičku a poté ji odešlou adresátovi. Některé využívají více stupňů a přeposílají zprávy do vícero bodů, než ji odešlou konečnému adresátovi.

Exituje několik základních typů remailerů:

- ➔ PSEUDONYMNÍ REMAILERY, které prostě zamění jméno odesilatele za jiné. Příjemci umožňují odpovědět.
- ➔ CYBERPUNKOVÉ REMAILERY odstraňují odesilatelovu adresu, odešlou zašifrovanou zprávu remaileru, který ji dešifruje a následně odešle adresátovi. Tento způsob umožňuje přidávat další a další remailery a vytvářet tak řetěz, přes který zprávy putují, což zvyšuje tvou anonymitu a obvykle nezanechává log. Na druhou stranu adresát nemůže na tuto zprávu odpovědět.
- ➔ MIXMINIONOVÉ REMAILERY, které používají programy k tomu, aby anonymizovaly mailovou komunikaci. Navíc umožňují na zprávu odpovědět.
- ➔ WEBOVÉ REMAILERY jsou v podstatě webovými stránkami, které ti umožní odeslat zprávy anonymně. Je velmi snadné je používat, ale zároveň neposkytují takové bezpečí, jako regulérní remailery.

B) SLOŽKA ROZEPSANÉ (DRAFTS)

Jinou možností je používat ve skupině jeden email se složkou rozepsané pošty. Zamezíte skenování odchozí pošty, jak to provádí NSA v Americe, protože zprávy, které si vyměníte, nebudou nikdy odeslány, ale budou pouze uloženy ve složce rozepsané. Pozitivní na této možnosti je, že na rozdíl od remailerů nevyžaduje speciální programy. Je však nezbytné dbát zvýšené opatrnosti při zakládání a přihlašování do takové emailové schránky. Nevýhodou je, že k dosažení naprosté anonymity schránky je nezbytné, aby všichni, kdo do ni přistupují, dbali bezpečnostních pravidel.

Pokud nedůvěřuješ schopnostem ostatních zachovat anonymizační praxi při přístupu do schránky, je tato možnost nevhodná. Když bude schránka kompromitována, může být kompromitována všechna vaše konverzace.

Bez ohledu na to, zda ke komunikaci používáte remailery nebo draft složky je dobré řídit se následujícími pravidly:

- ➔ Přes email (ani jiné digitální zařízení) nikdy nic neplánujte. To provádějte výhradně tváří v tvář. Komunikační kanály využívejte nanejvýš k plánování takových setkání.
- ➔ Používejte nekonkrétní, zavádějící či kódovaný jazyk. Nikdy anonymními maily neodesílejte jména nebo jakékoliv osobní informace.
- ➔ Nikdy neuvádějte datum, čas ani místo vašeho setkání. Určete si pro takové informace kódované názvy.
- ➔ Bezpodmínečně přistupujte k mailu anonymně (tzn. přes Tor, se změněnou MAC adresou...).

- ➔ Nenechávejte si ve schránce maily, pokud nejsou nezbytně nutné. Mažte je průběžně.
- ➔ Jakmile vaše schránka posloužila svému účelu, smažte veškerý její obsah a účet zrušte.

C) PGP ŠIFROVÁNÍ

Emaily jsou odesílány v prostém textu. To znamená, že každý, kdo má přístup k serveru, přes který prochází tvůj email (nebo tyto servery monitoruje za použití sniffing packets), může obsah tvého mailu číst. PGP může zmírnit škody a ochránit obsah tvému emailu před zvídavými zraky. Základem PGP šifrování jsou dva klíče. Veřejný a soukromý. Ty zveřejníš nebo pošleš konkrétní osobě svůj veřejný klíč, což je v podstatě série číslic a písmen. Tím tento klíč učiníš přístupný komukoli, kdo by od tebe chtěl přijmout zašifrovanou zprávu. Soukromý klíč si uschováš, nejlépe v nějakém šifrovaném oddíle.

Když ti někdo bude chtít odeslat šifrovanou zprávu, použije tvůj veřejný klíč k tomu, aby ji zašifroval. Tuto zprávu pak může dešifrovat pouze tvůj soukromý, bezpečně uložený, klíč. Pro kohokoliv jiného (servery, fízly a jiné čmuchaly) bude zpráva vypadat jako změť nesmyslných číslic a písmen.

NASTAVENÍ PGP V THUNDERBIRDU

Nejprve budeš potřebovat emailový klient Thunderbird. Dále nainstalovaný plugin Enigmail a GNUGP software. Poté, co budeš tyto programy mít, otevři Thunderbird. V menu otevři možnost OpenPGP a klikni na Možnosti (Preferences). Zde by mělo být propojení s binárním GNUPG, vyber možnost Procházet (Browse) a najdi GNUPG program, který sis nainstaloval v prvním kroku. Nyní si můžeš vygenerovat veřejný a soukromý klíč. V menu OpenPGP vyber možnost Správa klíčů (Key Management). Následně v generovacím menu vyber Nový pár klíčů (New Key Pair). Vyber emailovou adresu, ke které budeš chtít klíč vygenerovat a klikni na Generovat klíč (Generate Key). Po několika minutách bude tvůj klíč vytvořený. Budeš také moci vytvořit certifikát o ukončení platnosti klíče, který zruší veřejný klíč v případě, že by byl soukromý klíč kompromitován. Tuto možnost doporučujeme.

Až budeš chtít odeslat email, napiš ho v Thunderbirdu běžným způsobem. Klíč v pravém dolním rohu okna ti umožní zprávu zašifrovat a označit PGP klíčem. Jestliže svítí zeleně, znamená to, že je PGP aktivované. K tomu, abys vyhledal něčí veřejný PGP klíč, vyber možnost Správce klíčů (Key Management) v menu OpenPGP. V nabídce Keyserver klikni na tlačítko Hledat. Vyhledávat můžeš podle jména nebo mailové adresy. Poté si můžeš přidat adresátův veřejný klíč do svého správce klíčů. Tento postup ti umožní zašifrovat zprávu pro dotyčnou osobu.

JAK JE PGP BEZPEČNÉ?

Šifrování je typicky velmi obtížné prolomit. Existují důkazy o tom, že FBI (a podobné bezpečnostní složky) nejsou momentálně schopné dešifrovat moderní PGP. Je zde ale určitá možnost, že počítače, kterými disponuje například NSA, mohou PGP prolomit. O tom ale zatím neexistují žádné důkazy (je však pravděpodobné, že kdyby se jim to podařilo, tajily by to, aby zabránily tomu, že by lidé PGP rázem přestali důvěřovat a používat ho, takže kdo ví). V zákoně není uvedeno, že bys byl povinný vydat svá hesla vyšetřovatelům, to ale neznamená, že to po tobě nebudou chtít. Proto se na tuto možnost připrav například vytvořením skrytého šifrovaného oddílu. A nejlépe za všech okolností drž jazyk za zuby!

Na druhou stranu prolamování šifry nebo donucování podezřelých k vydání hesla není mnohdy potřeba. Bezpečnostní složky používají keyloggery a další software k tomu, aby získali šifrovací klíče a hesla jiným způsobem. Jediným preventivním opatřením proti těmto útokům je dobře opevnit svůj systém a dbát správného bezpečnostního chování. Čím více budeme používat PGP, tím neviditelnější naše komunikace bude. Takže vstříc PGP.

Poznámka: Jsou mezi námi skupiny i jednotlivci, kteří používají Gmail. Ten důrazně nedoporučujeme. Gmail skenuje veškerou mailovou komunikaci, aby mohl poskytovat uživatelům reklamní sdělení přesně na míru. Tohle v kombinaci s množstvím informací, které o tobě Google nashromáždí při běžném brouzdání internetem pomocí trackerů pouze zvyšuje bezpečnostní rizika. Gmail svá data vyšetřovatelům předal například v případě soudu se skupinou Mt. Hope Infinity, čímž ukázal svou pravou tvář. Google je vždy ochoten pomáhat státnímu represivnímu aparátu. Proto se mu vyhýbej obloukem. Používej mailové servery jako například Riseup.net který je spravován antiautoritáři, kteří kladou důraz na bezpečnost a aktivně vzdorují policii tam, kde Google spolupracuje.

ODKAZY

- ➔ *https://cs.wikipedia.org/wikia/Asymetrická_kryptografie* (Jak funguje šifrování - česky)
- ➔ *https://cs.wikipedia.org/wiki/Pretty_Good_Privacy* (Česky o tom, jak funguje PGP)
- ➔ *https://en.wikipedia.org/wiki/Anonymous_remailer* (Podrobněji o remailerech)
- ➔ *http://www.zvedavec.org/techpor2003/04/568-jak-na-to-pgp.htm* (Český návod na PGP šifrování)
- ➔ *https://freedom.press/encryption-works* (Podrobněji o různých způsobech šifrování – OTR, PGP...)

SESSION DATA Z PROHLÍŽEČE

CO TO JE?

Záznam sezení se skládá z rozličných stop, které zanecháváš po své aktivitě na počítači. Příkladem jsou systémové logy, spuštěné programy, nedávno otevřené dokumenty, dočasné soubory, miniatury (thumbnails), vyhledávání a samozřejmě data z prohlížeče jako historie, cookies, cache atp.

PROČ SE TÍM ZABÝVAT?

I přesto, že dbáš správných zásad bezpečného a anonymního chování, tak tě tyto stopy na počítači mohou prozradit. Logy obsahují důkazy o tvé činnosti, které mohou kompromitovat tvá bezpečnostní opatření. Miniatury a seznam nedávných dokumentů ukazují, jaké soubory jsi vytvářel, ukládal nebo otevíral. Stejně tak data z prohlížeče poskytují mapu toho, co děláš online. Tyto data musíš mít pod kontrolou a měl bys je zredukovat na minumun, chceš-li své počínání udržet v tajnosti.

JAK NA TO?

Je několik způsobů, jak se zbavit těchto záznamů. Bezpečné mazání a pravidelné skartování volného místa na disku pomáhá eliminovat stopy po smazaných souborech. Mazání dat z prohlížeče (nebo jejich neukládání) snižuje nebo zamezuje ukládání stop o tvé internetové aktivitě. Stejně tak můžeš používat LiveSystem, obzvlášť když pracuješ s daty, které by neměly zanechat žádné stopy. Šifrování celého disku ti dále umožní zabezpečit i tyto záznamy.

I přesto existují místa, které je potřeba vytřídit a vymazat. Linux má opět nad Windowsem navrch. Ve většině Linuxových distribucí se /tmp složka (složka dočasných souborů) vyčistí při bootování. Linux navíc nemá žádné registry a má konkrétní místa, kam se logy ukládají. Většina dočasných souborů je uložena ve složkách /tmp a /var/log. V Linuxu můžeš s logy zatočit pomocí nástroje logrotate tool. Některé mazací programy, jako například BleachBit, je také možné na Linuxu nainstalovat a používat (nezapomínej je spouštět jako root).

Ve Windows mohou být některé logy vymazány manuálně:

1. Proklikej se přes Start >> Ovládací panely (Control Panel) >> Systém a zabezpečení (System and Maintenance/Security) >> Nástroje pro správu (Administrative Tools) >> Zobrazit protokoly událostí (View Event Logs)
2. Zde můžeš pravým tlačítkem označit rozličné logy a vymazat je.

Jinou možností je použít k mazání speciální programy. Jejich možnosti se liší program od programu, obecně by ale měly prohlédnout počítač a nabídnout ti možnost smazat specifické programy a logy. Je to užitečné hlavně k mazání nedávno otevřených dokumentů, dočasných souborů, miniatur, cache, záznamů z Office a jiných programů, systémových obnovovacích bodů (System restore points), dat z prohlížeče včetně historie, systémových logů apod.

Tyto programy vždy nastavuj tak, aby k mazání používaly silný algoritmus s několikanásobným přepisem (např. Schneider). Doporučujeme používat vícero prostředků k mazání, protože každý program detekuje trochu odlišné věci, které je potřeba smazat.

Rady k session datům můžeme shrnout následovně:

- ➔ K pravidelnému pročištění používej mazací programy
- ➔ Pravidelně skartuj volné místo na disku
- ➔ Šifruj disk
- ➔ Neukládej si historii prohlížeče

ODKAZY:

- ➔ *http://linuxcommand.org/man_pages/logrotate8.html* (Logrotate – nástroj pro mazání session dat v Linuxu)
- ➔ *http://www.thegeekstuff.com/2010/07/logrotate-examples* (Návod, jak Logrotate používat)
- ➔ *http://www.wikihow.com/Delete-your-Usage-History-Tracks-in-Windows* (Návod, jak mazat session ve Windows)
- ➔ Programy na mazání session dat: BleachBit, Ccleaner

METADATA

CO TO JE?

Metadata jsou identifikační prvky připojené k souboru. Například Microsoft Office vkládá metadata do jakéhokoli dokumentu, který vytváří. Do metadat patří jméno počítače, jméno společnosti apod. Jakožto anarchisté považujeme za vhodné zabývat se hlavně soubory z Office a obrázky.

PROČ SE TÍM ZABÝVAT?

Metadata dokážou prozradit tvou identitu. V případě Office dokumentů je prozrazeno jméno tvého počítače a jiné citlivé informace. V případě obrázků

se jedná o informace o foťáku, čase a v některých případech dokonce o tom, kde byl snímek pořízený. Pokud chceš tyto dokumenty a obrázky zachovat anonymní (třeba v případě fotek z akcí nebo riotů, příspěvků do anarchistických plátků, komuniké), musíš metadata odstranit.

JAK NA TO?

A) MICROSOFT OFFICE

Office ukládá jméno, jméno počítače, iniciály, jméno společnosti a informace o revizích do všech svých dokumentů. Doporučujeme používat pro hardware a software obecné, neidentifikovatelné názvy (viz 802.11 nickname str.90), všechny ostatní data tě ale přesto mohou se souborem spojit.

K odstranění metadat z dokumentů Office, proveď následující:

1. Klikni pravým na dokument a klikni na Vlastnosti (Properties)
2. Jdi do záložky Detaily (Details) a klikni na Odstranit nastavení a osobní informace (Remove Properties and Personal Information).
3. Vyber vše a data odstraň.

Informace můžeš vymazat také předtím, než soubor uložíš, a to následovně:

1. Klikni na Nástroje a poté na Nastavení
2. Jdi do záložky Bezpečnost (Security) a zaškrtni Odstranit osobní údaje z tohoto dokumentu při uložení (Remove personal information from this file on save)

B) OPENOFFICE

1. Klikni na Soubor
2. Klikni na Vlastnosti
3. Odškrtni Použít uživatelské údaje a volbu potvrď

C) PDF

1. Otevřit PDF v Adobe Acrobat (musíš použít Acrobat, Adobe Reader neumí editovat PDF soubory)
2. Zobraz Nastavení dokumentu kliknutím na Soubor a pak Nastavení dokumentu. Přesuň se do záložky Popis.
3. Odstraň jakýkoli nežádoucí údaj, který se nachází v kolonkách Autor, Subjekt nebo klíčová slova.
4. Přesuň se do záložky Custom a udělej to samé.
5. Soubor a Uložit jako.

1. Použitíš můžeš i automatickou funkci Adobe Acrobat Pro. Otevři v něm PDF a klikni vpravo na Nástroje (Tools)
2. Vyber záložku Ochrana (Protection) a v ní Odstranit skryté informace (Remove hidden information). Poté, co program najde různá metadata, smazání potvrď (Remove).

D) FOTKY

Digitální foťáky a foto editory metadata ukládají automaticky. Nejjednodušší způsob, jak je smazat, je stáhnout si skartační program. Níže odkazujeme na několik takových pro Linux, Mac a Windows.

ODKAZY:

- ➔ *https://lawyerist.com/2477/how-to-quickly-and-easily-remove-meta--data* (Návod na mazání metadat Wordu a OpenOffice)
- ➔ *http://www.coniseal.com/jak-odstranit-metadata-v-openoffice* (Snadný český návod na odstranění metadat z OpenOffice dokumentů)
- ➔ *http://www.coniseal.com/jak-odstranit-metadata-ve-formatu-pdf* (Návod na odstranění metadat z PDF)
- ➔ Programy na mazání metadat z fotek: GeoSetter, Exif eraser, Exif data changer

ZNIČENÍ PEVNÉHO DISKU

PROČ SE TÍM ZABÝVAT?

Pokud máš na svém pevném disku informace, které musí být bezpodmínečně zničeny, můžeš se rozhodnout disk fyzicky zničit. Není to nezbytné, pokud se řídíš bezpečnostními pravidly, které jsme popsali. I přesto může existovat situace, kdy budeš disk potřebovat zničit. Přikládáme několik tipů, jak na to.

JAK NA TO?

1. Spusť skartační program a bezpečně vymaž celý harddisk. Tento krok data přepíše a zničí většinu stop. Čím vícekrát to uděláš, tím menší šance, že na disku něco zůstane.
2. Přejeď párkrát silným magnetem přes disk. Tím data ještě více poškodíš.
3. Disk spal nebo ho rozbij na kousky.
4. Jednotlivé části vyhoď na několika různých místech. Dej si pozor na to, abys nebyl sledován.

Je možné, že pokud bude nalezena část disku, dokážou z ní bezpečnostní složky pomocí kvalitních mikroskopů některá data dostat (i když i o tom se vedou spory). Disk by ale v prvé řadě nemělo být snadné ani najít, a pokud se to stane, tak by mělo být díky opatřením, které jsi udělal, náročné, ne-li nemožné, dostat z něj něco kloudného.

POČÍTAČ BEZ DOZORU

PROČ?

Při jakékoli choulostivé práci na počítači bys měl brát v potaz jednoduchou věc. Ani sebelepší bezpečnostní chování tě neochrání, když necháš počítač bez dozoru. Hesla, šifrování a tajné diskové oddíly chrání tvůj počítač a data poměrně dobře, představ si ale situaci, kdy máš rozdělanou citlivou práci a musíš si odskočit. Může se tak snadno stát, že se určité informace dostanou k očím, pro které nejsou určeny. Samozřejmě tím není myšleno, že ti zásahovka vyrazí dveře a sebere počítač zrovna když budeš na záchodě. Mluvím spíš o očích nepovolaných přátel, spolubydlících nebo kolegů. K čemu je ti nedobytný trezor, když ho necháváš otevřený dokořán?

Pokud jsi v hledáčku policie, nebezpečí hrozí i z jejich strany, protože mohou tvůj počítač infikovat sledovacím softwarem během několika málo chvil, necháš-li ho bez dozoru. Většinou jim stačí k počítači připojit infikovanou flashku.

JAK?

Zde stačí opravdu málo. Pokud nemůžeš být při práci na počítači sám, posaď se pokud možno zády ke zdi tak, abys na obrazovku viděl jen ty. Sedět zády k oknu taky není to pravé – nejenže je to nepraktické, ale i přes okno tě může kdokoli sledovat.

Další a ještě podstatnější věcí je nenechávat počítač otevřený a přihlášený, když musíš odejít z jeho dohledu. Nikdy nevíš, kdy se třeba přijde podívat tvůj kamarád v rychlosti na předpověď počasí a místo toho uvidí inkriminující informace, o kterých nechceš, aby věděl. Vypínat stroj při každé cestě na záchod je nepraktické. Existuje však elegantnější řešení. Uzamykání obrazovky. Opět platí, že uživatelé Linuxu mají snadnější práci. V novějších distribucích odvozenin Debianu stačí pouze stisknout kombinaci kláves Ctrl+Alt+L. Obrazovka se zatmaví a pro její odemknutí musíš vložit přihlašovací heslo. Obdobnou funkci umožňuje i samostatný software, který existuje i pro Windows. Rozhodně nečekej na spuštění spořiče. Ukazovat obrazovku cizím očím je nejen nepříjemné, ale zároveň potencionálně velmi nebezpečné.

DALŠÍ VZDĚLÁVÁNÍ

Pokud chceš o internetové bezpečnosti a anonymizační praxi vědět víc, doporučujeme ti projít si následující stránky a články. Nejenže jsou přátelštější než než náš suchý text (bohužel je většina v angličtině), ale jsou komplexnější a plné odkazů na konkrétní nástroje:

- ➔ *http://www.cogipas.com/privacy-protection* (Souhrnný článek a rozcestník pro základní pravidla bezpečnostní anonymizační praxe)
- ➔ *https://www.epic.org/privacy/tools.html* (Seznam užitečných nástrojů i s odkazy na jejich stažení)
- ➔ *https://prism-break.org/en/all* (Ohromný seznam nástrojů a doplňků)
- ➔ *https://ssd.eff.org* (Přehledné návody na všelicos: jak používat Keepass, jak používat PGP na Linuxu, jak na OTR...)
- ➔ *http://billstclair.com/matrix/ar01s03.html*
- ➔ *stalluminati.neocities.org/matrix* (nenech se odradit oldschoolovým a konspiračním hávem stránky, protože ve skutečnosti pokrývá ještě víc témat, než o jakých jsme sami psali)

9. ZÁVĚR

Po všech těch informacích můžeš nabýt dojmu, že nemůžeš udělat už ani jeden krok bez toho, abys nebyl sledován nebo ohrožen. Tak tomu ale není. Zaprvé zrak státu nemůže nikdy spočívat v jednu chvíli na každém z nás. Zadruhé i fízlové jsou lidi, kteří dělají chyby, zanechávají stopy a jsou vidět. Pokud jsi obezřetný, můžeš popsaná bezpečnostní rizika snížit na minimum.

Udržuj své znalosti aktuální a měj na paměti, že bezpečnostní složky budou tento manuál číst a vyvíjet na něm svá protiopatření.

Proto experimentujme, improvizujme a trénujme. Buďme inovativní a vždy o krok napřed. Držím ti palce.

Se soudružskými pozdravy
ANONYM

https://www.cernorudaprirucka.noblogs.org
cernoruda-prirucka@riseup.net