POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra kriminální policie

Využívání informací z otevřených zdrojů při sledování osob a věcí

Diplomová práce

Using Information from Open Sources during Surveilance of People and Things

VEDOUCÍ PRÁCE

Ing. Bc. Luděk Michálek, Ph.D.

AUTOR PRÁCE

Bc. Luboš Kubovec

PRAHA 2022

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci na téma „Využívání informací z otevřených zdrojů při sledování osob a věcí“ vypracoval samostatně a s použitím uvedené literatury a pramenů.

V Praze, dne 10. 3. 2022

Bc. Luboš Kubovec

ANOTACE

Tato diplomová práce je zaměřena na seznámení se s základními pojmy v oblasti využívání, získávání informací z otevřených zdrojů obecně a komplexní popis problematiky OSINT, nebo-li Open Source Intelligence. Také se budu věnovat možnostem zneužití těchto informaci se zvýšeným zřetelem na sociální sítě, jakožto jednomu ze zdrojů těchto „veřejně“ dostupných informací. Práce je zaměřena zejména na popis metod a nástrojů problematiky OSINT, na jejich možné využití v rámci sledování osob a věcí z pohledu odpovědných orgánů bezpečnostních složek státu. Součásti zaměření této diplomové práce, je také snaha přiblížit dotazníkovým šetřením případné rozdíly ve vnímání dané problematiky definovanými skupinami osob.

KLÍČOVÁ SLOVA

zpravodajství * právní úprava * otevřené zdroje * OSINT * informace * zpravodajský cyklus * dotazníkové šetření * bezpečnost na internetu * sociální sítě * SOCINT * metody a nástroje

ANNOTATION

This diploma thesis is focused on getting acquainted with the basic concepts in the use and acquisition of information from open sources in general and a comprehensive description of the issues of OSINT, or Open Source Intelligence. I will also address the possibilities of misusing this information with an increased focus on social networks, as one of the sources of this "publicly" available information. The work is focused mainly on the description of methods and tools of OSINT issues, their possible use in the monitoring of persons and things from the perspective of the responsible authorities of the security forces of the state. Part of the focus of this thesis is also an effort to approach the questionnaire survey of any differences in the perception of the issue defined by groups of people.

KEYWORDS

intelligence * law * open sources * OSINT * information * intelligence process * questionnaire survey * internet security * social networks * SOCINT * Tools and metods

Obsah

Úvod

Aktuálně se píše rok 2022. Internet a sociální sítě jsou dnes slova, bez kterých si většina lidí nedokáže představit existovat. Internetové prostředí se stalo, vedle mobilního telefonu, nejrychleji se rozvíjející technologií v historii lidstva. Každým rokem dochází nejen k dalšímu vylepšování možností, které nám v oblasti komunikace, rychlosti a způsobu šíření informací internet nabízí, ale i k nárůstu počtu jeho uživatelů. Aktuálně využívá internet přes 4,9 miliardy lidí na světě, z toho cca 4 miliardy lidí využívá sociální sítě. Průměrně globálně každý člověk stráví na internetu 2 a půl hodiny denně[1]. Toto obrovské číslo je ukazatelem závislosti lidí na technologiích, ale zejména relativně snadným přístupem k těmto službám, kdy drtivá většina lidí používá k připojení na internet mobilní telefon. Řekněme si narovinu, že na stolním PC má každý z nás nainstalovaný antivirový program, případně firewall, či jiné zabezpečení. Ale co v mobilním telefonu ? Jak jste na tom právě vy ? Ze statistik vyplívá, že mobilní telefon si chrání antivirem cca 60% uživatelů, zatímco stolní počítač cca 90% uživatelů. Absence nutnosti používat k připojení k internetu stolní počítač způsobuje dle mého názoru první z faktorů zranitelnosti uživatelů, které mu se budu věnovat v dalších bodech této diplomové práce. Druhý neméně zásadní faktor je obrovský počet dat a informací, které lidi sdílí ať už vědomě, či nevědomě a absolutně si neuvědomují, že v této záplavě a dalo by se říci nadbytku všudypřítomných dat by mohl někdo chtít tato data, nebo informace zneužít. Mnohdy ať už nevědomky, či z důvodu prosté nevědomosti, nedbalosti dává uživatel toliko informací veřejně, že by se z těchto informací mohl vytvořit kompletní psychologický profil dané osoby. Zjistíme kde daná osoba bydlí, s kým sdílí jednu domácnost, jaká vlastní vozidla, kam a v kolik hodin přesně chodí do práce, či do restaurace. Jak vypadají, jak se oblékají, kde utrácejí, s kým chodí.

Zjednodušeně řečeno lidé dle mého úsudku ztrácí obezřetnost nadbytkem dostupnosti všudypřítomných technologií a tím dávají možnost potencionálním útočníkům získat citlivá data. A právě tomuto tématu se budu dále věnovat. Na začátek se pokusím objasnit základní témata a principy vyhledávání, sběr dat a

[1] Data Mezinárodní telekomunikační unie (ITU) při OSN

informací. Dále přiblížím druhy sběru dat, dopodrobna vysvětlím problematiku práce s otevřenými zdroji. Přiblížíme si hlavní oblasti, kde dochází k využívání právě takto získaných dat z otevřených zdrojů, ať už ve sféře komerční v rámci například konkurenčního boje mezi institucemi, žurnalistiky, v oblasti kriminality jako čistý zdroj nelegálních aktivit, nebo jako nástroj v boji proti takové kriminalitě. V neposlední řadě také využití dostupných informací v rámci práce bezpečnostních složek státu v průběhu operativně pátracích činností atd.

Zaměřím se na konkrétní metody, nástroje a možné využívání otevřených zdrojů (OSINT) při sledování osob a věcí, jako nezanedbatelného podpůrného prostředku. Jelikož mám s touto problematikou již cca 10 let osobní zkušenost v rámci Bezpečnostní informační služby, uvedu pro účely této diplomové práce a snahu přiblížení tématu s důrazem na závažnost celé problematiky „otevřených zdrojů“ a jejího zabezpečení i názorné příklady z praxe.

Součástí této práce je i dotazníkové šetření, které jsem na dané téma s důrazem na porovnávané skupiny (příslušníci bezpečnostních sborů X civilisté) ještě nikde neviděl. Toto jsem zaměřil bez rozdílu pohlaví na obecnou povědomost lidí o bezpečnosti na internetu, technologiích a celkově řekl bych zdravé hygieně používání sociálních sítí a vědomí toho, že by mnohdy tyto sdílené informace mohly být zneužity. Důraz jsem kladl na to, zda budou rozdíly v odpovědích markantní jednak u osob v závislosti na věku, tak zejména hlavně v rámci této práce u osob, které jsou součástí nějaké bezpečnostní složky státu a u osob z civilní sféry. Zajímá mě hlavně to, zda osoba která pracuje v některé z bezpečnostních složek a mohla by se tedy zvýšenou měrou setkávat s danou problematikou buďto okrajově, nebo i přímo ve výkonu služby. Již při vytváření samotného dotazníku bych dle mého pohledu a zkušeností předpokládal, že rozdíly budou patrné.

Výsledek tohoto šetření samozřejmě shrnu v této diplomové práci. Budu se z něho snažit vyvodit závěr a případně bych se pokusil navrhnout řešení pro zlepšení tohoto „problematického“ povědomí. Slovo problematické používám záměrně, protože se domnívám, že neznalost v tomto případně je skutečně problém.

1 Vymezení základních pojmů dané problematiky

1.1 Zpravodajství obecně

Zpravodajství jako základní stavební kámen a pojítko všeho, o čem budu dále psát. Samotný pojem můžeme nejčastěji v literatuře i v médiích chápat ve dvou rovinách. Toto níže uvedené rozdělení na 2 základní typy zpravodajství je rozdělení čistě v rámci této diplomové práce a určitě neposkytuje absolutně konečný výčet možností realizace „zpravodajství“. Kromě níže uvedených typů se s zpravodajstvím můžeme setkávat na každém kroku jak v současnosti, tak ale také jako neoddělitelnou součást dávné historie. První zmínky jsou již v bibli. Ať se jedná o historii, současnost, nebo budoucnost, vždy bude jeden společný jmenovatel – INFORMACE.

To nejznámější spojení všeobecně mezi lidmi, se domnívám tvrdit je činnost novinářská, nebo také můžeme říct činnost žurnalistická. A to ať už seriózní, bulvární, investigativní, či jinou v závislosti na tom, jakou optikou na danou kategorizaci nahlížíme. Více se na toto téma zaměřím v části věnované oblastem využití informací z otevřených zdrojů.

Druhou možností pohledu na zpravodajství jsou činnosti zpravodajských služeb státu. Anglické označení v literatuře „Intelligence“. Současně na velmi podobném principu mohou pracovat i nejrůznější „soukromé agentury“ kterým se v této práci budu věnovat jen okrajově, ale je důležité, abychom si uvědomili, že tyto soukromé agentury mohou leckdy využívat stejné, či velmi obdobné nástroje pro vlastní sběr informací. Zpátky se zaměříme na státní zpravodajské služby. Zpravodajství ve smyslu činnosti zpravodajských služeb je soubor činností a procesů spočívající zejména v utajovaném získávání, sběru a vyhodnocování informací s cílem „výstup“ (zprávu pro adresáty, zadavatele v mezích právního rámce konkrétní zpravodajské organizace či její části). Tento výstup slouží jako podklad k učinění co možná nejadekvátnějších rozhodnutí.

Mohu uvést, že například výstupní zpráva Bezpečnostní informační služby, dále jen BIS, dle zákona č.153/1994 Sb. o zpravodajských službách

České republiky i zákona 154/1994 Sb. O bezpečnostní informační službě slouží „pouze“ jako „doporučení“.

Prezident republiky, předseda vlády a příslušní členové vlády jsou též adresáty výstupních zpráv, kterými je BIS informuje o zjištěních, která nesnesou odkladu. Adresáty informací BIS jsou též státní orgány a policejní orgány. Pokud poskytnutí takové informace neohrožuje zájem, který BIS v dané věci sleduje, předává jim BIS informace o svých zjištěních, která patří do jejich působnosti. Konkrétní reakce na výstupní informace je výhradně v kompetenci adresátů, kteří mají výkonné pravomoci.

Oproti tomu „výstup“ například Útvaru zvláštních činností služby kriminální policie a vyšetřování, který se zabývá zpravodajstvím jako jednou ze svých činností v rámci orgánu, který je ze své podstaty činný v trestním řízení může vést sám o sobě například k zahájení úkonů v trestním řízení, což BIS nemůže.

Jak jsem uvedl, zpravodajství nemůžeme chápat jako jednu konkrétní činnost, ale naopak jako celou řadu dílčích činností. Na samém začátku je zadání úkolu,

následuje sběr informací, jejich důkladná analýza až po výsledek, kterým nejčastěji bývá sestavení zprávy a její předání. Tím hlavním termínem zpravodajství, pod kterým si nemalá část veřejnosti představí hlavně i díky médiím „špionství", nebo špionáž a podobné výrazy“ je označována činnost, která směřuje k ochraně vlastních informací před zpravodajskou činností jiných států, nebo přinejmenším alespoň k odhalení těchto snah a zabránění jim. Tato činnost je pojmenována jako kontrarozvědné zpravodajství. V České republice výhradně v kompetenci Bezpečnostní informační služby.

Jak jsem naznačil výše, ať už komerční služby (média, žurnalistika, firmy, atd.), nebo bezpečnostní složky státu, které pracují se zpravodajstvím (v nejrůznějších podobách), se všichni zaměřují na získávání, sběr a vyhodnocování informací. Tento proces se nazývá „zpravodajský cyklus“ (intelligence process) a společný jmenovatel je informace.

1.2 Zpravodajský cyklus

Zpravodajský cyklus jako takový lze chápat spíše jako popis samotné zpravodajské činnosti, tudíž se může do jisté míry odchylovat v závislosti na konkrétní instituci, která ho aplikuje. Jedná se o teoretické popisování chodu, nikoliv právních aspektů. Považuji za důležité znát jak takový zpravodajský cyklus funguje i vzhledem k tématu a kdy pracujeme s otevřenými zdroji informací, které mají v tomto cyklu nezpochybnitelnou roli.

Samotný zpravodajský cyklus ve své nejobecnější formě se neobejde dle mého názoru o 4 nezbytné fáze. Na začátku řetězce je „řízení“, následuje fáze „sběru“, „analýzy“ a v konečné fázi „výstup“

Řízení

První fáze zpravodajského cyklu, kde dochází k prvotní formulaci informačních potřeb, proč a co chceme, nebo potřebujeme vědět a také jak se získanými informaci budeme dále chtít pracovat. V této fázi je nezbytná komunikaci mezi zadavatelem a „pracovníkem“, který bude mít na starosti ať už třeba jen následující fázi cyklu, nebo v nějakém méně složitém úkolu i zde popsaný cyklus. Tento pracovník by měl být plně seznámen s úkolem, aby nedocházelo k omylům. Měl by mýt veškeré nezbytně nutné informace potřebné pro další fáze. Proto nedochází k absolutnímu oddělování fáze řízení a sběru. U BIS se řídí veškerá činnost heslem „need to know“ (v praktickém překladu – „jsem seznamován jen s tím, co nezbytně potřebuji vědět ke své práci“)

Ve třech bodech můžeme shrnout základní pravidla co by měl každý řídící pracovník stanovit :

- pro jakého adresáta je výstupní zpráva určena, a s kým je zapotřebí komunikovat,

- co potřebujeme zjistit, jakou informaci hledáme,
- jakou má mít výstupní zpráva formu a k čemu bude použita.

Sběr

Po nezbytně důležité komunikaci mezi zadavatelem a pracovníkem by měla následovat analýza vhodných metod, prostředků a zdrojů informací tak, abychom se vyvarovali za prvé přílišnému nadbytku informací, které se stanou nepřehledné a zbytečně prodlouží naši následnou činnost analýzy a naopak při volbě špatných metod a prostředků se může stát, že se nedostaneme k žádné validní informaci.

Tato diplomová práce se primárně soustředí na otevřené zdroje informací, které níže popíši detailněji, nicméně obecně bez dalšího nutného dělení je musím zmínit i v tomto bodě. Otevřené zdroje informací jsou jednou několika možností k přístupu k informacím. Jako veřejný zdroj informací disponuje obrovskou škálou informací a dat. V tomto obrovském množství dat je potřeba volbou vhodných metod a prostředků vyhledávat. Vzhledem k tomuto obrovskému množství dnes dostupných zdrojů dat je třeba klást velký zřetel také na pravdivost a platnost, nebo také validnost těchto dat a informací. Z hlediska informační hodnoty můžeme informace nadále označovat jako informace primární nebo sekundární. Primární informace jsou ta autentická fakta přímo od zdroje, který je důkladně obeznámen s požadovanou problematikou. Za sekundární informace považujeme takové, které jsou určitým způsobem pozměněné, zprostředkované, nebo např. zkrácené, či subjektivně vnímané primární informace jinou osobou.

Dalším metodám sběru informací v rámci zpravodajských prostředků se budu věnovat v kapitole „metody sběru informací“

Analýza

Z již uvedeného nám plyne, že následující analýza je stěžejním a nejdůležitějším prvkem celého zpravodajského procesu. Opět zde platí stejné pravidlo jako mezi „zadáním x sběrem“ a to sice to, že ani analýza nemůže stát ve zpravodajském procesu jako samostatná kapitola řetězu. Kvalitní a kvalifikovaný analytik komunikuje, hodnotí a validuje získané informace od pracovníka, které dané informace a data získal. Společně kooperují na bázi zpětných vazeb a případně upravují další postup. V procesu analýzy dochází za pomoci rozličných analytických metod k takzvané transformaci získaných informací a dat na potřebné „poznání“ té, či oné problematiky. Na základě tohoto „poznání“ můžeme učinit následné kroky, které vedou až k závěrům a rozhodnutím. Výše uvedená fáze vyžaduje a měla by být vykonávána s využitím nejlepších dostupných metod a prostředků. Jako jeden ze zásadních prostředků je právě otázka personální. Na postu analytika by měla být osoba s vysokou úrovní intelektuální, profesní a psychické kvality. V tomto oboru jsou zkušenosti a „mozek“ k nezaplacení, a nelze je nahradit žádným jiným nástrojem.

Analytický proces by mohl vypadat následovně :

- Prvotní popis všech informací, jejich roztřídění podle, platnosti, důležitosti, aktuálnosti, ale i jiných priorit v rámci každého individuálního procesu. Tento proces je individuální, každý analytik je jiný, jeho mozek pracuje s daty jinou pro něj individuální formou. Nejčastěji se uvádí, že nejlepší takovou formou, je forma grafického znázornění. Příkladem budiž už v dobách „devadesátých“ nástěnka s fotkami a u toho fixou a nejrůznějšími pomůckami naznačeny vazby atd. (v dnešní době jsou na vazby mezi osobami, věcmi, adresami atd. již plně automatizované a sofistikované aplikace)

- Logická úvaha která spočívá, ve spojování jednotlivých dílů v určité celky. Můžeme si zase příkladně uvést jednotlivé dílky puzzle. Čím více

správných informací a dílků máme, tím více se nám rýsuje výsledný obraz a díky tomu jsme schopni vytvářet a sestavovat určitější hypotézy.

- Formulace hypotéz, ty jak je uvedeno výše vycházejí u jednotlivých nám známých „dílků“ informací, či indicií, které máme v danou chvíli k dispozici. V tento okamžik jsou opět důležité zkušenosti analytika, aby z těchto dostupných informaci sestavil co možná nejpravděpodobnější hypotézy. Všechny takto stanovené hypotézy se následně potvrzují a vyvracejí.

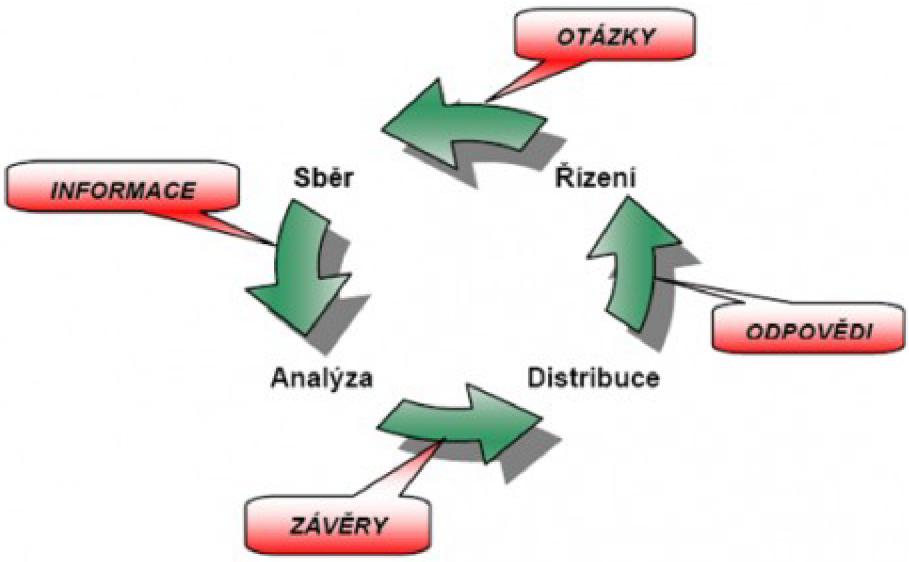
- Formulace závěrů, kde dochází k finální a konečné formulaci poznaného tak, že na základě zadání potvrzujeme, nebo vyvracíme stanovené prvotní domněnky a signály. Následně tyto informace předáváme vhodným a stanoveným způsobem dál pro další postupy.

Výstup

Výstup, nebo také distribuce zjištěných poznatků představuje pomyslnou závěrečnou fázi zpravodajského cyklu. V této fázi jsou závěry získané ve fázi analýzy zpracovány do potřebné výstupní zprávy a následně jsou předány koncovému adresátovi v takové formě a podobě, která umožní jejich další využití. Každá taková zpráva by měla splňovat určitá kritéria, my si pro účely této práce uvedeme 3 nejzásadnější a nejuniverzálnější :

- Obsahově musí být zpráva jasná, stručná a hlavně srozumitelná koncovému adresátovi tak, aby po jejím přečtení nedocházelo ke zmatečnosti a pochybnostech o jejím obsahu.
- Zpráva by měla být využitelná vzhledem ke vztahu k zadání.

- Zpráva by měla být hlavně aktuální a platná. Zásada raději neúplné, ale včas, než úplně, ale pozdě. Což si můžeme uvést tímto příkladem : nikdo nechce číst zprávu, že se chystá teroristický útok, který se již dávno stal.



Obrázek 1 - Zpravodajský cyklus

zdroj : https://wikisofia.cz/wiki/Competitive_intelligence

1.3 Metody sběru informací – zpravodajské prostředky

1.3.1 HUMINT

HUMINT je jako jedna ze základních metod sběru informací již od historie lidstva samého. Přeloženo z angličtiny se toto slovo skládá z **HUM**an**INT**eligence (doslovně lidské zpravodajství). Jak již samotný název napovídá využívá se při něm lidských zdrojů. Zdroj informace je tedy člověk. V tom nejužším smyslu slova jde o spolupracovníka jeho tajné úkolování, řízení a vytěžování a to jak pro potřeby špionáže, tak i kontrašpionáže.

HUMINT patří k nejúčinnějšímu (ale také nejrizikovějšímu) způsobu sběru informací. Jedná se o chráněný a utajovaný způsob sběru informací. Může být jediným zdrojem informací, může být primárním a bezprostředním zdrojem, který dokáže odhalit plány a záměry protivníka ještě ve fázi plánování. K nevýhodám patří zejména vysoké riziko odhalení spolupracovníka (s ohledem na vysoké tresty, které většina zemí za špionáž proti sobě uděluje) a výsledky se obvykle dostavují pomalu. Základním předpokladem pro získání relevantních informací je výběr osob, které budou do HUMINT sítě zařazeny[2]. HUMINT sítě si budují zpravidla všechny známe rozvědky i kontrarozvědky již od pradávna. A tomuto také věnují velké množství úsilí.

V zásadě můžeme rozdělit spolupracující osoby na osoby, které tuto činnost dělají dobrovolně, ale i nedobrovolně (výslechy, mučení atd.) A osoby „laické“ a „odborné“

Laik může být osobou využívanou pro získávání informací, ale hrozí bez nedostatku znalostí riziko, že v daném místě a čase nedokáže rozeznat jaká informace je a není důležitá. Zároveň z důvodu absence vycvičení hrozí dekonspirace jeho samotného i případného "zájmu".

Osoba „odborná“ již dokáže výše uvedené nedostatky eliminovat a dokáže rozeznat věci důležité a podstatné. Tyto osoby také bývají často vycvičeni v oblasti základů kontrasledování a konspirace tak, že je pro ně snazší utajit v daném místě a čase svůj skutečný zájem.

U Bezpečnostní informační služby je činnost HUMINT zakotvena v § 15 zákon 154/1994 Sb. O bezpečnostní informační službě následovně.

Využívání služeb osob jednajících ve prospěch Bezpečnostní informační služby

§ 15

(1) Bezpečnostní informační služba je oprávněna při plnění svých úkolů využívat služeb poskytovaných osobami jednajícími v její prospěch.

[2] https://cs.wikipedia.org/wiki/HUMINT

(2) Osobou jednající ve prospěch Bezpečnostní informační služby se pro účely tohoto zákona rozumí fyzická osoba starší 18 let, která dobrovolně a utajeným způsobem poskytuje služby Bezpečnostní informační službě při plnění jejích úkolů.

(3) Bezpečnostní informační služba je povinna ochraňovat osobu jednající ve prospěch Bezpečnostní informační služby před vyzrazením a způsobením újmy na cti, životě, zdraví nebo majetku, která by jí mohla vzniknout pro poskytování těchto služeb nebo v souvislosti s ním.[3]

1.3.2 OSINT

Jedná se o informace a data u již zmíněného zpravodajství z otevřených zdrojů (open source intelligence, OSINT), která lze získat z otevřených zdrojů, tedy laicky řečeno „volně“ dostupných informačních kanálů, databází atd. Slovo „volně“ je v uvozovkách záměrně z důvodu, že ač název inklinuje k pocitu, že otevřený zdroj je přístupný všem, ne vždy to tak je. Otevřené zdroje opravdu přístupny všem jsou, avšak jejich část pouze za poplatek, například (denní tisk, internet, databáze, katastrální úřad a jiné...). Otevřené zdroje tudíž nejsou, až na výjimky zdrojem utajovaných informací. Například při uniklých tajných dokumentech na internet, ať už chybou jednotlivce, nebo záměrnou špionážní činností. Získávání informací z otevřených zdrojů se v posledních letech a desetiletí i díky rozmachu technologií a výpočetní techniky stalo jedním z důležitých zdrojů informací pro zpravodajské služby.

Jak jsem psal v části věnované zpravodajskému cyklu, platí zde maximální možná opatrnost a důraz na ověřování a důvěryhodnost takovýchto informací. Zvláště v posledních letech, kdy se „válčí“ mezi světovými mocnosti na poli mediální války prostřednictvím dezinformací, neboli takzvaných „fakenews“. Přeloženo do češtiny jako záměrně pozměňované informace, dezinformace s cílem vyvolat v lidech paniku, strach averzi vůči menšinám atd.

---

[3] Zákon č. 154/1994 Sb. *Zákon o bezpečnostní informační službě*

Spolehlivé vyhodnocení informací pocházejících ze zdrojů OSINT v současnosti nedokážou ani ty nejvyspělejší informační technologie, je tedy potřeba vysoce odborného lidského faktoru a někdy i zdravého a selského rozumu.

Pokud bych měl OSINT ve dvou větách shrnout a říct výhody a nevýhody tak bych uvedl následující. Mezi obrovské výhody patří volná dostupnost těchto informací, rychlost a relativní finanční nenáročnost pořízení, jejich sběr nepředstavuje pro zpravodajskou službu žádné riziko.

Nevýhodou je potřeba dalšího podrobného zpracování a ověřování takto získaných informací, jsou nestabilní (některé zveřejněny pouze dočasně). Více podrobností popíši o problematice OSINT v hlavní části této diplomové práce.

1.3.3 SIGINT

SIGINT patří mezi utajované a chráněné zdroje informací před jakýmkoliv cizím přístupem. Jedná se z anglického překladu o zdroj informací na „signální“ bázi.

Jedná se například o :

- radiové vlny a jejich provoz, schopnost jejich zachycení, využití, pozměnění atd.
- datová komunikace (v současnosti nejsložitější komunikace na detekci)
- internet
- odposlechy telefonních hovoru, čtení sms zpráv
- síťové zachytávání IMSI, IMEI a detekce takového zachytávání.
- jiné vysílání, které je možno zachytit pomocí radiových vln a adekvátních přístrojů

Stejně jako je tomu v případě HUMINT, je i SIGINT částečně právně zakotven. U Bezpečnostní informační služby je část činnost SIGINT zakotvena v § 8 zák č. 154/1994 Sb. O bezpečnostní informační službě následovně. Zejména pak pod číslem b) a d)

§ 8 Zpravodajská technika

(1) Zpravodajskou technikou se pro účely tohoto zákona rozumějí technické prostředky a zařízení, zejména elektronické, fototechnické, chemické, fyzikálně-chemické, radiotechnické, optické, mechanické anebo jejich soubory, používané utajovaným způsobem, pokud je při něm zasahováno do základních práv a svobod občanů při

a) vyhledávání, otevírání, zkoumání nebo vyhodnocování dopravovaných zásilek,

b) odposlouchávání, popřípadě zaznamenávání telekomunikačního, radiokomunikačního a jiného obdobného provozu, popřípadě zjišťování údajů o tomto provozu,

c) pořizování obrazových, zvukových nebo jiných záznamů,

d) vyhledávání použití technických prostředků, které by mohly znemožnit nebo znesnadnit plnění úkolů v rámci Bezpečnostní informační služby,

e) identifikaci osob nebo předmětů, popřípadě při zjišťování jejich pohybu za použití zabezpečovací a nástrahové techniky. [4]

1.3.4 IMINT

IMINT můžeme přeložit do češtiny jako obrazové zpravodajství, vyslovovaná buď jako Im-Int nebo I-Mint. Jedná se o způsob získávání a shromažďování zpravodajských informací za využití analýzy snímků, fotografií za účelem zjištění zpravodajské hodnoty. Snímky používané pro účely obranného zpravodajství jsou obecně shromažďovány prostřednictvím

[4] Zdroj : Zákon č. 154/1994 Sb. *Zákon o bezpečnostní informační službě*

satelitních, nebo leteckých snímků. Ty se následně jak jsem uvedl výše analyzují a porovnávají (komparují), například se snímky staršího data pořízení .

Jako disciplína shromažďování informací závisí produkce IMINT do značné míry na robustním systému správy shromažďování informací. IMINT doplňují nezobrazovací elektrooptické a radarové senzory MASINT.

Z uvedeného vyplívá, že IMINIT jako zdroj informací spadá spíše do sekce "vojenství a obraného zpravodajství", který je závislý na dostupnosti techniky, která je schopna pořizovat snímky.

Největšího rozmachu se IMINT dočkal v dobách II. světové války u RAF, která pořizovala z průzkumných letadel fotografie nepřátelského území a byly následně vyhodnocovány pro další plánování operací. Zjištěné informace tedy mohly obsahovat pozice nepřátelských vojsk, obrněné techniky atd. Po II. světové válce nastala éra špionážních letounů a v dnešní době převládají bezesporu satelity.

1.3.5 MASINT

MASINT složeno ze slov measure (měřit), signature (popisovat) je technické odvětví shromažďování zpravodajských informací, které slouží k detekci, sledování, identifikaci nebo popisu charakteristických vlastností (signatur) pevných nebo dynamických cílových zdrojů. To často zahrnuje radarové metody, akustické metody, jaderné metody a chemické a biologické metody. MASINT je definován jako vědecká a technická metoda odvozená z analýzy dat získaných ze snímacích přístrojů za účelem identifikace jakýchkoli charakteristických znaků spojených se zdrojem, emitorem nebo odesílatelem, aby se usnadnilo jeho měření a identifikace.

Příkladem zdroje informací MASINTU nám může být, testování balistických raket dlouhého doletu Severní Koreou. Právě díky MASINTU, se v místech, které běžně sledují například seizmickou aktivitu shromažďují online data a informace, které jsou automaticky ihned analyzovány. Pokud dojde k

anomálii způsobené právě ať už odpalem, nebo dopadem takové balistické rakety, dokážou tyto měřící body relativně přesně například triangulační metodou, ve kterém konkrétním místě došlo k dopadu rakety. Tuto metodu může doplnit výše uvedená metoda IMINT, která může potvrdit, nebo vyvrátit případné hypotézy.

2 Otevřené zdroje informací OSINT obecně a jeho druhy

Na začátek je nejdůležitější pochopit, co OSINT, neboli open source intelligence je. OSINT vychází z veřejně dostupných informací. Je to shromažďování, analyzování a šíření informací včas a adekvátním adresátům.

Důležitá fráze, na kterou je třeba se zde zaměřit, je „veřejně dostupné“. Termín „open source“ se vztahuje konkrétně na informace, které jsou dostupné pro veřejnou spotřebu. Pokud jsou pro přístup k informacím vyžadovány speciální dovednosti, nástroje nebo techniky, nelze je rozumně považovat za open source.

Rozhodující také je, že informace z otevřeného zdroje se neomezují na to, co můžete najít pomocí nám veřejně známých velkých vyhledávačů. Webové stránky a další zdroje, které lze nalézt pomocí Google, jistě představují masivní zdroje informací s otevřeným zdrojovým kódem, ale musíme vědět, že to nejsou zdaleka jediné zdroje. Podle bývalého generálního ředitele Google Erica Schmidta, velkou část internetu (přes 99 procent), nelze najít pomocí velkých známých vyhledávačů [5]. Tato zbylá "anonymní" část, nebo takzvaně „deep web“ je množství webových stránek, databází, souborů a dalších, které z různých důvodů, včetně přítomnosti přihlašovacích stránek nebo platebních bran nemohou být indexovány Googlem, Bingem, Yahoo ani žádným jiným vyhledávačem, na který je většina veřejnosti zvyklá. Navzdory tomu lze velkou

[5] Zdroj : https://seon.io/resources/the-best-tools-for-osint/

část obsahu "deep webu" považovat za open source, protože je různými metodami snadno dostupný veřejnosti.

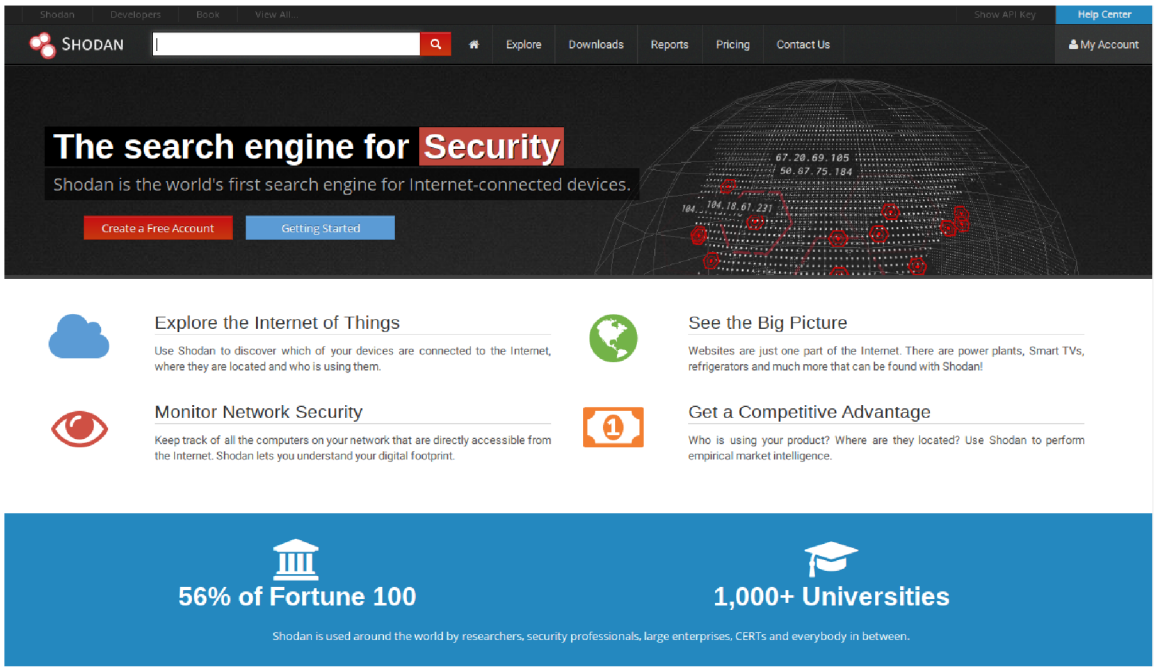
Důvody, proč nemohou vyhledávače a vyhledávací nástroje některé stránky "DEEP WEBU" indexovat:

- na stránku "deep webu" nesměřují žádné odkazy a zároveň stránka sama žádné neobsahuje
- dynamicky generovaný obsah stránek
- jsou to jen neindexované databáze
- obsah souborů některých formátů (např. doc, pdf, postscript, komprimované soubory apod.),
- stránky jsou téměř vždy s autorizovaným přístupem (chráněné loginem)
- stránky nepovolující indexaci
- omezení počtu indexovaných stránek v rámci jedné domény
- kontextuální web – stránky s obsahem lišícím se dle způsobu přístupu (např. dle IP adresy nebo dle předchozího pohybu na stránce),
- scriptový obsah – stránky přístupné pouze přes odkazy vytvořené Java skriptem, nebo obsah přístupný přes Flash nebo Ajax,
- alternativní webové služby jako Tor Hidden Service či Freenet apod.

Kromě toho existuje spousta volně dostupných informací online, které lze najít pomocí jiných online nástrojů, než tradičních internetových vyhledávačů. Jako jednoduchý příklad uvedu jeden z nich, a to nástroj Shodan.io. Ten lze použít k nalezení IP adres, sítí, otevřených portů, webových kamer, tiskáren a v podstatě čehokoli, co je připojeno k internetu.

Shodan.io - je někdy označován jako „nejnebezpečnější internetový vyhledávač“. Na rozdíl od Google vyhledavače neprohledává webová rozhraní, ale prochází internet jako celistvou síť zařízení. Co zde potká, to si zapamatuje a umožňuje to následně vyhledat. Projde otevřené TCP porty, "zaťuká" na ně

a prohlédne si odpověď. Pokud objeví známou službu (v paměti jich má aktuálně přes 300), rozebere si odpověď, vyhledá si známé zranitelnosti a "otaguje" (označkuje), případně udělá screenshot a všechno uloží do databáze, kterou pak nabídne k prohledání. Shodan umožňuje vyhledávat zařízení, která by rozhodně neměla být připojena do internetu. Najdete tu routery, kamery, volně přístupné webové kamery, IoT zařízení, rozhraní pro ovládání solárních elektráren a spoustu dalších zajímavostí, které se jen tak povalují na internetu. V dnešní '"chytré domácnosti" kdy je k síti připojena televize, herní konzole, ale i lednička nabízí velmi rozmanité portfolio možností. To ovšem není všechno, co Shodan umí. Nabízí například zobrazení výsledků vyhledávání v interaktivní mapě. To se hodí, pokud hledáte třeba otevřené web kamery ve svém okolí. Užitečné je také prohledávání obrázků, které Shodan na "své cestě potkal", nebo sám pořídil. Příjemné je, že jsou opatřeny tagy, takže si snadno můžete najít třeba otevřené plochy Windows nebo web kamery v Česku.[6]



Obrázek 2 - Shodan.io úvodní obrazovka

Zdroj : http://shodan.io

[6] Zdroj : https://www.root.cz/clanky/shodan-io-uzitecny-vyhledavac-internetovych-slabin/

Když už jsme psali o otevřených zdrojích informací, vysvětlíme si, kde můžeme hledat a provádět šetření. Nejedná se o kompletní výčet těchto zdrojů, ale pouze o jeho názorný příklad. Odborná praxe určitě není omezena pouze na tyto níže uvedené

2.1 Zdroje informací

- Internetové vyhledávače (nejpoužívanější vyhledávače: Google, Bing, Yahoo, DuckDuckGo, Ecosia, IxQuick, Ask, Lycos, Yandex, Dogpile, Startpage, Peekier, Webcrawler, Yippy, Exalead, Factibites, Wayback Machine, Gibiru, Siri, Alexa, atd.) pomocí logických operátorů, kterými jsou :

  Google Dorks a jeho operátory, symboly a příkazy lze použít pro explicitní a specifické vyhledávání, jak budu psát v kapitole věnované metodám vyhledávání v open source dále.

  - AND, OR, NOT, XOR: (příklad: hrozba AND džihád)
  - (): (příklad: (hrozba OR terorismus) AND (islám OR džíhád)
  - Operatory, nebo-li zkratky: *, #, ¿, $, €, “”, například
  - Symboly: <, >, =, <>, <=, >=
  - Příkazy: define: term; filetype: term; site: site/domain; link: url, atd..
  - A mnoho dalších příkazů
- Webové stránky, fóra a blogy z různých zemí a v různých jazykových mutacích na základě informací a dotazů, které hledáme, lidí, konkrétních informací, nebo témat.
- IP sítě a lokátory zařízení (sítě, otevřené porty, webové kamery, tiskárny a mnoho dalších síťových zařízení): Shodan.io, Myip.es, Ip-address.com, Iplocation.net, Httrack.com, Pastebin.com, Whois.com, Robtex.com, IANA, RIPE, atd.).

- socialní sítě (Facebook, Youtube, Vimeo, Instagram, Twitter, Pinterest, Reddit, Vkontakte, Tumblr, Linkedin, Infojobs, Snapchat, TikTok a mnoho dalších, které se soustředí například na seznamování : Meetic, eDarling, Badoo, Tinder, atd.).
- mapy (internet) a polohová data (maps.google.com, mapy.cz Iplocation.net, Coordenadas-gps.com, Mapsdirections.info, Mapscoordinates.net, atd.).
- časopisy (různé jazyky, země a konkrétní vyhledávače na základě informací a cílů, které sledujeme)
- noviny (stejně jako v předchozím bodě)
- konference, kterých se lidé mohli zúčastnit, a to i akademických, veřejných nebo soukromých, které jsou zveřejňovány na firemních webech
- radiové a televizní vysílání
- úřední věstníky a databáze (registr obyvatel, firem, evidence majetku, obchodní registrace atd.
- informace dostupné veřejnosti na vyžádání (například údaje ze sčítání lidu, údaje od orgánů veřejné moci v rámci práva na informace. Právně ukotveno jako zákon 106/1999 Sb. o svobodném přístupu k informacím),
- organizace (profesní asociace, profesní a vysoké školy, nevládní organizace atd.,
- mobilní aplikace (WhasApp, Skype, Telegram, Signal, Viber, Messenger atd.)
- e-mailové stránky, které můžeme použít pro generování dočasného e-mailu, nebo pro hledání v případě, že by účty mohly být hacknuty (Pastebin.com, Haveibeenpwned.com, Shodan.io, Verifyemailaddress.org , Mxtoolbox.com, Toolbox.googleapps.com, Mailnator.com, Guerrillamail.com, Temp-mail.org, Correotemporal.org, Throwawaymail.com, Maildrop.cc, Mailnator.com, etc.).
- Skenování obrázků (vyhledáním obrázků na internetu a kontrolou jeho metadat a umístění, nebo dokonce možného falešného obrázku profilu

(Google Images, Bing, Tineye, Yandex, Revimage.com, Pictriev.com, Exiftool, Fotoforensics.com, Photo-forensics, atd.).

Tyto zdroje informací lze ještě dále obecně rozdělit na:

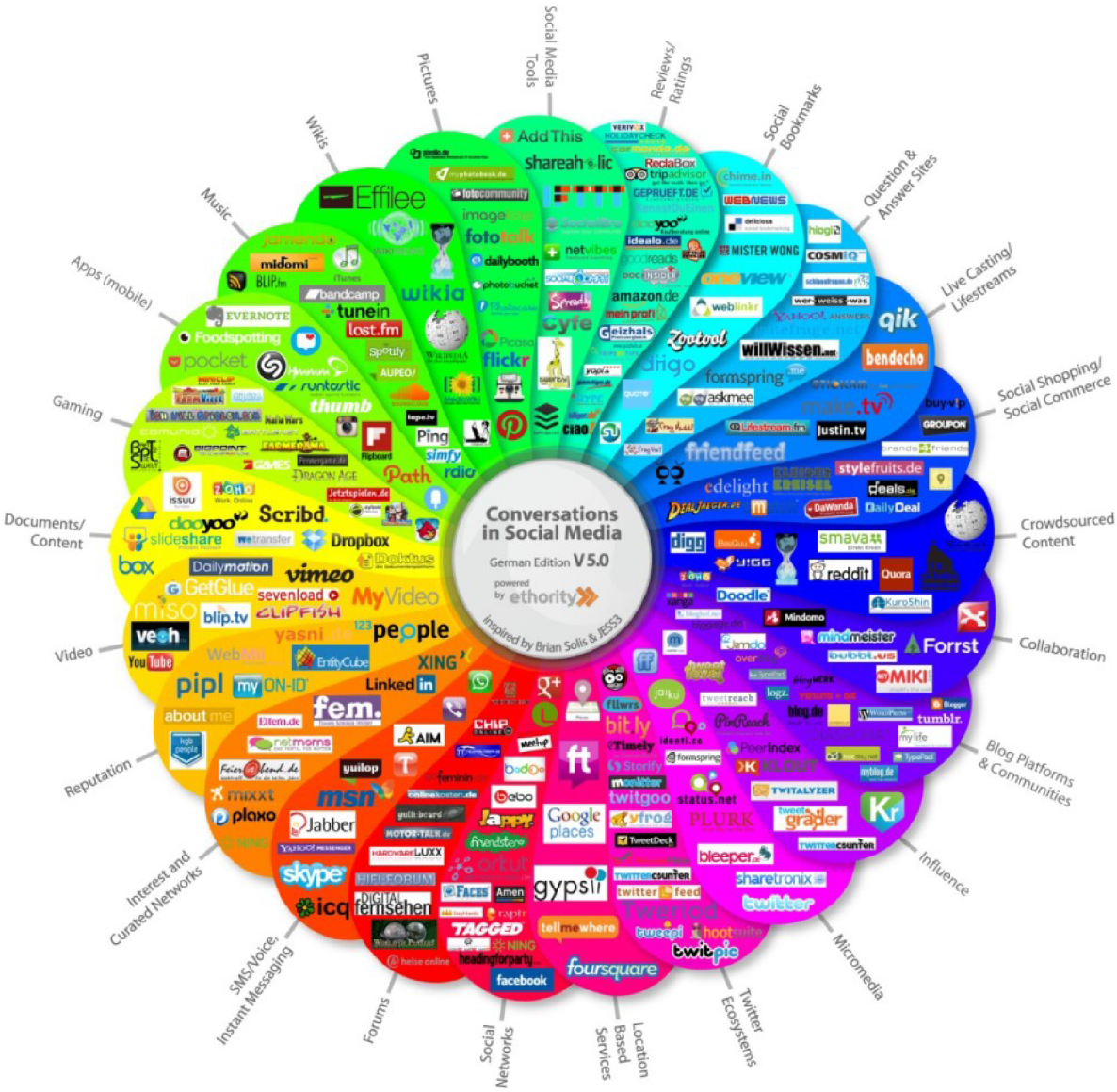
- bezplatné databáze a registry
- databáze zdarma, ale s požadavkem na založení profilu
- bezplatné databáze, ale s požadavkem na skutečný a ověřený profil a žádost (například úmrtní list)
- placené zdroje

Jako další názorný příklad může posloužit níže uvedený neúplný seznam otevřených databází domén .CZ :

- administrativní informace
  - www.justice.cz - katalog "životních" situací
  - wwwinfo.mfcr.cz - ares, registr ekonomických subjektů
  - www.czso.cz - český statistický úřad
  - www.edb.cz - evropská databanka
- kreditní informace
  - www.creditreform.cz - hospodářské informace, pohledávky
  - www.cekia.cz - kapitálová informační agentura
  - www.intercredit.cz - bankovní databáze
- marketingové informace
  - www.komora.cz - registr hospodářské komory
  - www.czso.cz - český statistický úřad
  - www.hn.cz - hospodářské noviny
  - marketingovedatabaze.cz - marketingové databáze
  - časopis Trend Marketing - marketingové databáze
- legislativa
  - www.sbirka.cz - sbírka vydaných legislativ

V tuto chvíli si pravděpodobně říkáte, že se jedná a nepřeberné množství informací....

A ano, máte pravdu. "Open source" je skutečně zdrojem nepředstavitelného množství informací, které díky technologickému rozmachu a hlavně dostupnosti technologií a internetu široké veřejnosti skrze mobilní telefony roste mnohem rychleji, než by kdokoli mohl doufat. I když zúžíme pole na jediný zdroj informací – například u sociální sítě Twitter jsme nuceni se každý den vypořádat se stovkami milionů nových dat a informací. O pravdivosti a validitě nemluvě. Toto je stinná stránka práce s otevřenými zdroji, absolutní nadbytek informací, které jsou mnohdy neověřené a zároveň neověřitelné. Ale jak jste pravděpodobně pochopili, je neodmyslitelným kompromisem práce s otevřeným zdrojovým kódem. Pro analytika je možnost mít k dispozici tak obrovské množství informací velkou zbraní a darem, ale zároveň i prokletím. Na jednu stranu máte přístup téměř ke všemu, co by jste mohli potřebovat, ale na druhou stranu to musíte být schopni najít v nekonečném proudu dat.



Obrázek 3 - OSINT paleta možností

Zdroj : https://z3r0trust.medium.com

2.2 Použití OSINT v oblasti bezpečnosti - vyhledávání rizik

Po představě obecných základů zpravodajství s otevřenými zdroji informací a toho co jsou to otevřené zdroje, se můžeme podívat na to, jak se OSINT běžně používá v oblasti bezpečnosti. V praxi se může setkat se dvěma úhly pohledu, podle toho na které straně "zákona" stojíme. První si nastíníme problematiku z pohledu bezpečnostních složek (útvary PČR a SKPV, útvary zpravodajských služeb, národní úřad pro kybernetickou a informační bezpečnost, ale i korporace a organizace které se zaměřují na bezpečnost na internetu a sítích, například ESET atd.) U této problematiky jsou nejčastěji uváděny dva základní případy použití:

2.2.1 "Etický hacking" a penetrační testování

Bezpečnostní profesionálové používají OSINT k identifikaci potenciálních slabin v přátelských sítích, aby je bylo možné napravit dříve, než je zneužijí aktéři hrozeb (hackeři). Mezi běžně zjištěné slabiny patří:

- Náhodný únik citlivých informací, například prostřednictvím sociálních sítí
- Otevřené porty nebo nezabezpečená zařízení připojená k internetu
- Neopravený software, jako jsou webové stránky se starými verzemi běžných produktů CMS (CMS jsou systémy pro správu obsahu internetových domén, jednoduše lze pomocí těchto systému založit a spravovat internetové prezentace, internetové obchody a jiný obsah, avšak tyto systémy jsou zranitelné proti útoku, kdy hacker může nezabezpečený a neaktualizovaný software napadnout a získat pro něj důležitá data, kterými jsou nejčastěji osobní údaje uživatelů, hesla, čísla platebních karet atd.) Pokud uživatel internetu používá v síti jedno univerzální heslo pro více svých účtů, může se snadno stát obětí dalšího hackerského útoku. Zkoumání tohoto jevu chování a neopatrnosti uživatelů se budu věnovat na konci této práce v dotazníkovém šetření.

- Uniklá nebo odhalená aktiva, jako je proprietární kód na pastebinech. Autor proprietárního softwaru vymezuje uživatelům přesné možnosti používání daného softwaru. Podmínky používání předem definuje například v licenci. Jedná se o software s uzavřeným kódem, zdrojový kód tedy není volně k dispozici. Uživatelé nejsou oprávněni volně šířit takový software ani v něm provádět jakékoliv úpravy. Z praktického pohledu se jedná například o možnost instalace softwaru na určitý počet pracovních stanic. Bývá dodáván s určitými bezpečnostními opatřeními, nejčastěji se jedná o přístupový klíč. Zatímco pastebin je server, kde se sdílí anonymně prosté texty, tyto servery jsou podezřelé ze sdílení nelegálních kódů a v mnoha zemích jsou tyto servery nelegální. Jako názorný příklad mohu uvést útok na internetové stránky České televize, dále jen ČT a zároveň stránky hydeparkct24.cz, ze dne 17. 3. 2012, ke kterému se přihlásil později uživatel s přezdívkou „p1r@t3z'sec“. [7] Z následného šetření bylo zjištěno, že dne 10. 3. 2012 byly na serveru pastebin.com zveřejněny přístupové údaje k celkem 189 uživatelských účtů ČT. Databáze obsahovala uživatelské ID, uživatelské jméno a heslo. Ke dni útoku na ČT (17. 3. 2012) bylo u této databáze umístěné na pastebin.com uvedeno pouze 60 zobrazení. Je tedy velmi pravděpodobné, že právě v tomto případě napadení ČT se nejednalo o žádný sofistikovaný útok, ale právě o využití a jakousi zkoušku údajů z výše zmíněné databáze.

2.2.2 Identifikace vnějších hrozeb

Jak jsem již mnohokrát uvedl v této práci, internet je vynikajícím a přehlceným zdrojem informací. To platí i o hrozbách nejrůznějších organizací. Od identifikace, jaké nové "zranitelnosti" jsou aktivně zneužívány, až po zachycení „komunikace“ aktérů hrozeb o nadcházejícím útoku. OSINT a jeho metody a techniky umožňují bezpečnostní reakci pro profesionály nejenom v oblasti IT, kteří tak mohou soustředit svůj čas síly a prostředky na řešení

[7] Zdroj : https://ct24.ceskatelevize.cz/domaci/1184279-hacker-napadl-stranky-ceske-televize

nejvýznamnějších současných hrozeb. Ve většině případů tento typ práce vyžaduje, aby analytik identifikoval a koreloval více datových bodů za účelem ověření hrozby, dříve než by měl přijít samotný útok. Například, zatímco jeden výhružný tweet na Twitteru nemusí být důvodem k obavám, na stejný tweet by bylo pohlíženo v jiném světle, pokud by byl spojen s osobou, nebo se skupinou osob, o které je známo, že působí v konkrétním rizikovém odvětví.

Jednou z nejdůležitějších věcí, které je zapotřebí o OSINT pochopit je, že se často používá v kombinaci s jinými podtypy zpravodajství. Zpravodajství z vlastních uzavřených zdrojů, jako jsou interní poznatky a informace, uzavřené webové komunity, externí komunity a nejrůznější mezinárodní organizace pro sdílení zpravodajských informací, se pravidelně používají k filtrování, validování a ověřování zpravodajství s otevřeným zdrojem. Existuje celá řada dostupných nástrojů, které analytikům pomáhají provádět tyto funkce. A právě ty si popíšeme v následující kapitole.

Po nastínění základních principů se můžeme soustředit na druhý hlavní problém s OSINT. Protože pokud je něco snadno dostupné pro analytiky, je to také snadno dostupné pro aktéry hrozeb, hackery. Aktéři hrozeb, nebo hackeři používají nástroje a techniky otevřeného zdroje k identifikaci potenciálních cílů a využívají slabiny v cílových sítích. Jakmile identifikují zranitelné, nebo citlivé místo se špatným zabezpečením, nebo jinou slabinu, je to následně často extrémně rychlý a jednoduchý proces, jak ji zneužít a dosáhnout různých škodlivých cílů. Tento proces je jedním z hlavních důvodů, proč je každý rok napadeno tolik malých a středních firem. Tyto firmy nejsou cílem útoku, protože by byli záměrně individuálně vybírány, ale proto, že byly vyhledány a analyzovány automatickými metodami pro svoji zranitelnost v síti, nebo nedostatečným zabezpečením architektury webových stránek. Takové stránky respektive firmy jsou snadným cílem. Výsledným produktem může být jakákoliv informace, kterou lze následně zneužít.

OSINT neumožňuje pouze technické útoky na IT systémy a sítě. Aktéři hrozeb mohou také vyhledávat informace o jednotlivcích a organizacích, které

lze použít k informování sofistikovaných kampaní sociálního inženýrství pomocí phishingu (e-mail), vishingu (telefon nebo hlasová schránka) a SMiShing (SMS). Zdánlivě neškodné informace sdílené prostřednictvím sociálních sítí a blogů lze často použít k vývoji vysoce přesvědčivých kampaní sociálního inženýrství, které se zase používají k přivedení uživatelů s dobrými úmysly, aby ohrozili síť nebo majetek jejich organizace. To je důvod, proč je použití OSINT pro bezpečnostní účely tak důležité. Poskytuje vám příležitost najít a opravit slabá místa v síti vaší organizace a odstranit citlivé informace dříve, než aktér hrozby použije stejné nástroje a techniky k jejich zneužití.

2.3 Metody a nástroje obecně

Nyní, když jsme si částečně vysvětlili využití OSINT (obě strany hranice), představím Vám zde zatím obecně některé z metod a nástrojů, které lze použít ke shromažďování a zpracování informací s otevřeným zdrojovým kódem. Nejdůležitějším faktorem úspěchu každé iniciativy OSINT je přítomnost jasné strategie – jakmile víte, čeho se snažíte dosáhnout, a odpovídajícím způsobem si stanovíte cíle, bude identifikace nejužitečnějších nástrojů a technik k dosažení stanovených cílů mnohem lépe dosažitelnější.

2.3.1 Metody

V první řadě a to se budu opakovat, musíme mít jasnou strategii a rámec pro získávání a používání informací s otevřeným zdrojovým kódem. Nedoporučuje se přistupovat k zpravodajství v otevřeném zdroji z pohledu hledání čehokoli, co by mohlo být zajímavé nebo užitečné – jak jsme uvedl již několikrát v této práci, internet je přesycený informacemi a je velmi obtížně se v tomto "zmatku" orientovat, obrovské množství informací, které jsou prostřednictvím otevřených zdrojů dostupné vás jednoduše zahltí.

- Musíme si zaprvé předem určit strategii co chceme vyhledávat. Zda vytyčujeme slabé místo v zabezpečení naší sítě, nebo máme jiné cíle. Vyhledáváme konkrétní dokumenty, osoby, věci, rizika, hrozby, atd.
- Za druhé, musíte vhodně zvolit sadu nástrojů, metod a technik pro vyhledání, shromažďování a zpracování informací z otevřeného zdroje. Ještě jednou, objem dostupných informací je příliš velký na to, aby manuální procesy byly byť jen trochu efektivní.

Obecně řečeno, shromažďování informací s otevřeným zdrojovým kódem spadá do dvou kategorií: pasivní shromažďování a aktivní shromažďování.

Pasivní shromažďování často zahrnuje použití platforem pro informace o hrozbách (TIP) ke spojení různých zdrojů hrozeb do jediného a snadno dostupného místa. I když jde o významný krok vpřed oproti ručnímu získávání informací, riziko přetížení informacemi je velmi vysoké. Pokročilejší řešení ve vyhledávání hrozeb, jako je Recorded Future (Recorded Future je soukromá společnost v oblasti kybernetické bezpečnosti založená v roce 2009 se sídlem v Somerville v Massachusetts. Společnost se specializuje na sběr, zpracování, analýzu a šíření zpravodajských informací o hrozbách)[8]. Tento problém řeší pomocí umělé inteligence, strojového učení a zpracování přirozeného jazyka k automatizaci procesu upřednostňování a odmítání výstrah na základě specifických potřeb organizace.

Velice obdobným způsobem využívají organizované skupiny zaměřené na shromažďování cenných informací pomocí technik, jako je sledování provozu a keylogging BOTNETY (Botnet je v informatice označení pro softwarové agenty nebo pro internetové roboty, kteří fungují autonomně nebo automaticky. V současné době je termín nejvíce spojován s malwarem).[9]

[8] Zdroj : https://www.recordedfuture.com/open-source-intelligence-definition/

[9] Zdroj : https://cs.wikipedia.org/wiki/Botnet

Oproti tomu aktivní sběr, je použití různých technik k vyhledávání konkrétních poznatků nebo informací. Pro bezpečnostní profesionály se tento typ sběru obvykle provádí ze dvou důvodů:

- Pasivně (automaticky) shromážděná výstraha detekovala a upozornila na potenciální riziko, nebo hrozbu a je zapotřebí získat další informace.
- Zaměření shromažďování zpravodajských informací je velmi specifické, jako je například cvičení penetračního testování.

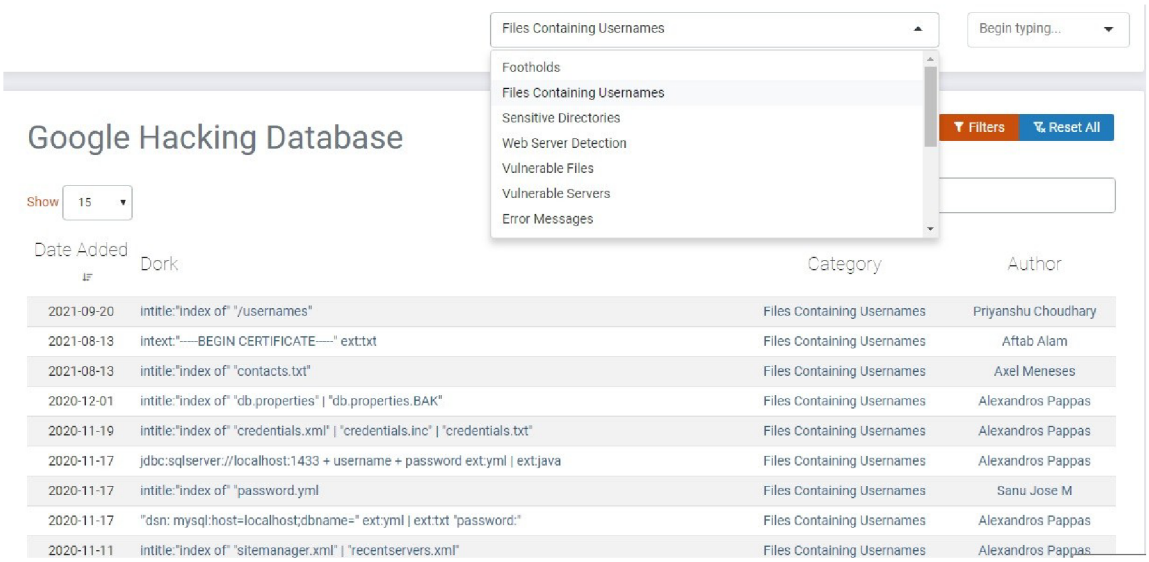
2.3.2 Nástroje

Abychom si udělali vlastní obrázek o dané problematice, podíváme se na některé z nejčastěji používaných nástrojů pro shromažďování a zpracování informací s otevřeným zdrojovým kódem.

Přes to, že existuje mnoho manuálních i automatických bezplatných a užitečných nástrojů dostupných pro bezpečnostní profesionály i aktéry hrozeb, některé z nejběžněji používaných (a zneužívaných) OSINT nástrojů jsou vyhledávače jako Google, avšak zdaleka ne tak, jak si většina z nás myslí. Jedním z největších problémů, kterým čelí bezpečnostní profesionálové, a ve finále i my sami jako "prostí" uživatelé, je pravidelnost, se kterou uživatelé s dobrými úmysly nechají citlivá data a informace vystavené internetu v domněnce, že jsou námi sdílená data a informace dostatečně zabezpečená a nemůže se nic stát. Existuje řada pokročilých vyhledávacích funkcí, nazývaných dotazy „Google dork“, které lze použít k identifikaci informací a dat, která dokáží bez problému vyhledat. Hacking Google, také nazývaný Google dorking, je hackerská technika, která využívá Vyhledávání Google a další aplikace Google k vyhledání bezpečnostních mezer v konfiguraci a počítačovém kódu, které webové stránky používají. Google dorking lze také použít pro OSINT. Dorkové dotazy Google jsou založeny na vyhledávacích operátorech, které denně používají IT profesionálové a hackeři k provádění své práce. Mezi běžné

příklady patří „filetype:“, který zužuje výsledky vyhledávání na konkrétní typ souboru, a „site:“, který vrací výsledky pouze z konkrétního webu nebo domény.

Internetová stránka Exploit - databáze nabízí "otevřeně a bezplatně" nepřeberné množství "dork" dotazů. Pro Vaši představu jsem přidal vlastní screenshot na kterém můžete vidět, že si lze dokonce přehledně vybírat z nejrůznějších kategorií vybraných příkazů. V mém případě jsem zvolil kategorii příkazů, po jejichž zadání do Google vyhledavače budou vyhledávány soubory, které obsahují uživatelská jména , loginy a případně hesla. Opět zopakuju varování, že používání duplicitních hesel je to nejsnadnější co můžeme útočníkům dát, respektive "naservírovat na zlatém podnose". Viz dotazníkové šetření v poslední části této diplomové práce.



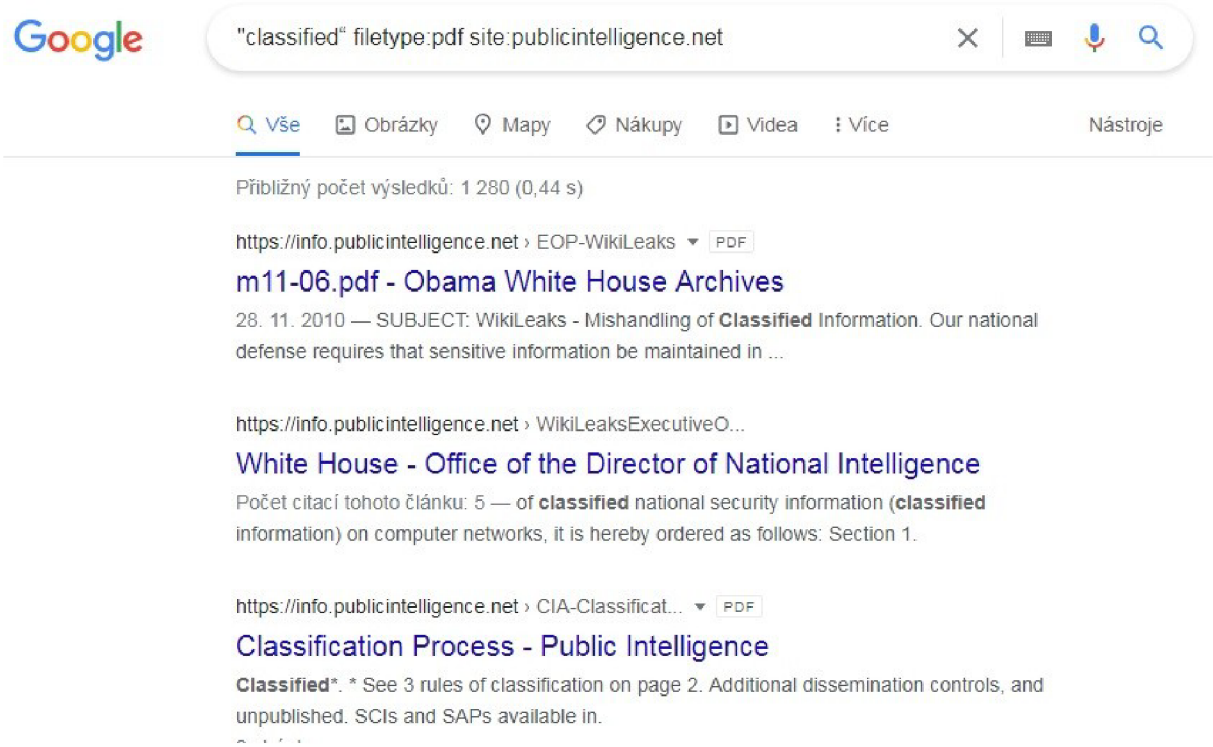
Obrázek 4 - Google hacking databáze

Zdroj : Exploit - databáze

Internetová stránka Public Intelligence nabízí důkladnější přehled dotazů "Google dork", ve kterých je uveden následující příklad vyhledávání:

„classified“ filetype:pdf site:publicintelligence.net

Pokud zadáte tento hledaný výraz do vyhledávače, jako výsledek se vrátí pouze dokumenty PDF z webu Public Intelligence, které někde v textu dokumentu obsahují slovo „classified“ (utajované). Jak si dokážete představit, se stovkami příkazů, které mají profesionálové k dispozici, mohou bezpečnostní experti a aktéři hrozeb použít podobné techniky k hledání téměř čehokoli. Konkrétním případům Google dork dotazům se budu věnovat v kapitole určené podrobnějšímu vyhledávání osob, e-mailových adres, telefonních čísel, atd. v další části diplomové práce.



Obrázek 5 - Snímek autora Google.com

Viz snímek autora : můžeme vidět po zadání uvedeného dotazu ve vyhledávači Google.com shodu pro cca 1280 dokumentů PDF ve kterých se vyskytuje slovo "tajné". Na prvních místech si můžeme všimnout "uniklých

a zveřejněných tajných" dokumentů ze serveru WikiLeaks, jeho zakladatele a aktivisti Juliana Assange.

Kromě vyhledávačů existují doslova stovky nástrojů, které lze použít k identifikaci slabin sítě nebo odhalených aktiv. Můžete například použít Wappalyzer k identifikaci, které technologie jsou na webu používány, a zkombinovat výsledky se Sploitus nebo National Vulnerability Database, abyste zjistili, zda existují nějaké relevantní zranitelnosti konkrétní webové stránky, nebo databáze. Pokud jdeme o krok dále, můžete použít pokročilejší řešení pro informace o hrozbách, jako je Recorded Future, k určení, zda je zranitelnost aktivně zneužívána, nebo je zahrnuta v jakékoli sadě aktivního zneužití.

Berme v potaz fakt, že zde uvedené příklady jsou samozřejmě jen nepatrným zlomkem toho, co je možné pomocí nástrojů open source zpravodajství vyhledávat, shromažďovat a v neposlední řadě analyzovat.

Existuje obrovské množství bezplatných a prémiových nástrojů, které lze použít k vyhledání a analýze informací s otevřeným zdrojovým kódem, přičemž běžné funkce zahrnují:

- vyhledávání metadat,
- hledání zdrojového kódu,
- vyhledávání osob a identity,
- vyhledávání telefonních čísel,
- vyhledávání a ověřování e-mailů,
- propojení účtů sociálních sítí,
- analýza obrazu,
- geoprostorový výzkum a mapování,
- detekce bezdrátové sítě a analýza paketů.

Obrázek 6 - OSINT nejčastější nástroje

Zdroj : http://www.hisutton.com/OSINT_Landscape.html

2.4 Problematika identit

V této kategorii bych se rád zaměřil na problematiku, která bezpochyby s otevřenými zdroji, internetem a sociálními sítěmi souvisí, je problematika identit osob, uživatelů. Obecně si pod identitou uživatele, nebo chcete-li osoby můžeme představit jakékoliv osobní údaje, nebo jiné údaje, které přímo vedou k jednoznačné totožnosti konkrétní osoby. Avšak mimo toto klasické pojetí uživatelské identity se v důsledku rozmachu technologií, internetu a sociálních sítí, čím dál více skloňují názvy jako internetová identita, virtuální identita, či technická identita uživatele. Tato se však od té "reálné", fyzické identity může v mnohém lišit. Internetové prostředí skýtá domnělou představu jisté anonymity, a proto v mnohých lidech vyvolává pocit, že se můžou vydávat za kohokoliv. To nemluvím o automatických "botech" které se vydávají za uživatele s různým cílem, ať už odcizení dat, zahlcení webové stránky a jiné. To ale není předmětem této "identity", jen bychom měli pro naší představu s touto možností také počítat.

Vyhledávání informací o uživatelích (osobách) na internetu je zaměřeno na vyhledávání veškerých dostupných informací o daném uživateli – tedy veškerých relevantních datech, a také o vyhledávání těch stop, které po sobě daný uživatel svou činností na internetu zanechává s cílem zjistit konkrétní osobu, autora článku atd.

Mezi takové údaje může patřit především následující:

- Relativně neměnné informací jako jsou jméno, příjmení, rok a místo narození, rodné číslo, bydliště.
- Časem proměnné informace jako jsou přezdívka, e-mailová adresa(y), telefonní číslo, používané IP adresy, digitalizované podpisové vzory, číslo bankovního účtu, číslo platební karty, SPZ používaného, nebo vlastněného vozidla, informace ze zápisů v databázích (katastr nemovitostí, rejstřík firem atd.).
- Méně či více trvalé profily na různých sociálních sítích, účty na aplikacích Messenger, Viber, ICQ, Skype atd. Na Facebooku například seznamy přátel a příbuzných.

2.4.1 Reálná identita

Reálná (či fyzická) identita osoby se skládá z takových osobních údajů, které umožňují danou osobu přímo či nepřímo identifikovat. V tomto smyslu se tedy fyzickou identitou rozumí souhrn osobních údajů. Pro přesnější představu by se reálná identita dala také označit přívlastkem fyzická.

Osobní údaje jsou definovány dle zákona č.101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, v § 4 písmeno a) následujícím způsobem:

„Osobním údajem (se rozumí) jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě

čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“ [10]

2.4.2 Virtuální identita

Hlavními specifickými znaky virtuální, online, nebo také internetové identity je to, že zahrnuje kromě údajů reálné identity i údaje jiné, doprovodné. Avšak i tyto doprovodné údaje jsme schopni zpětně přiřadit k identitě reálné, daného uživatele internetu. Do těchto doprovodných údajů virtuální identity spadají například jak jsem uvedl výše: přezdívky, uživatelská jména, unikátní i unifikované "avatary" užívané na diskusních fórech a webech, číslo ICQ nebo jiné chatovací služby, uživatelské jméno používané na Skype, YouTube, Twitteru a dalších aplikacích. Na rozdíl od reálné identity, u které lze poměrně jednoduše definovat údaje, které jednoznačně určují totožnost dané osoby, u virtuální identity je toto složitější, dalo by se říct při troše snahy skoro nemožné. Zatímco reálná identita se v čase přirozeně vyvíjí, a v zásadních bodech je neměnná, pokud nedojde například svatbou přirozeně ke změně jména, virtuální identita se v čase nepředvídatelně vyvíjí (s každým nově vzniklým uživatelským jménem, se změnou přezdívky, změnou hesla apod.). K jedné reálné fyzické identitě můžeme přiřadit jednu virtuální identita, ta se může časem vyvíjet. Kromě této jedné reálné virtuální identity však může být zároveň k reálné fyzické identitě přiřazen libovolný počet falešných virtuálních identit. Muž se může vydávat za ženu, dítě a naopak. V současnosti neexistuje žádná možnost kontroly nezletilých při přístupu například na stránky s pornografickým obsahem. Jediná nastavená ochrana je ta, že uživatel potvrdí, že je mu více jak 18 let a tím autorizace končí.

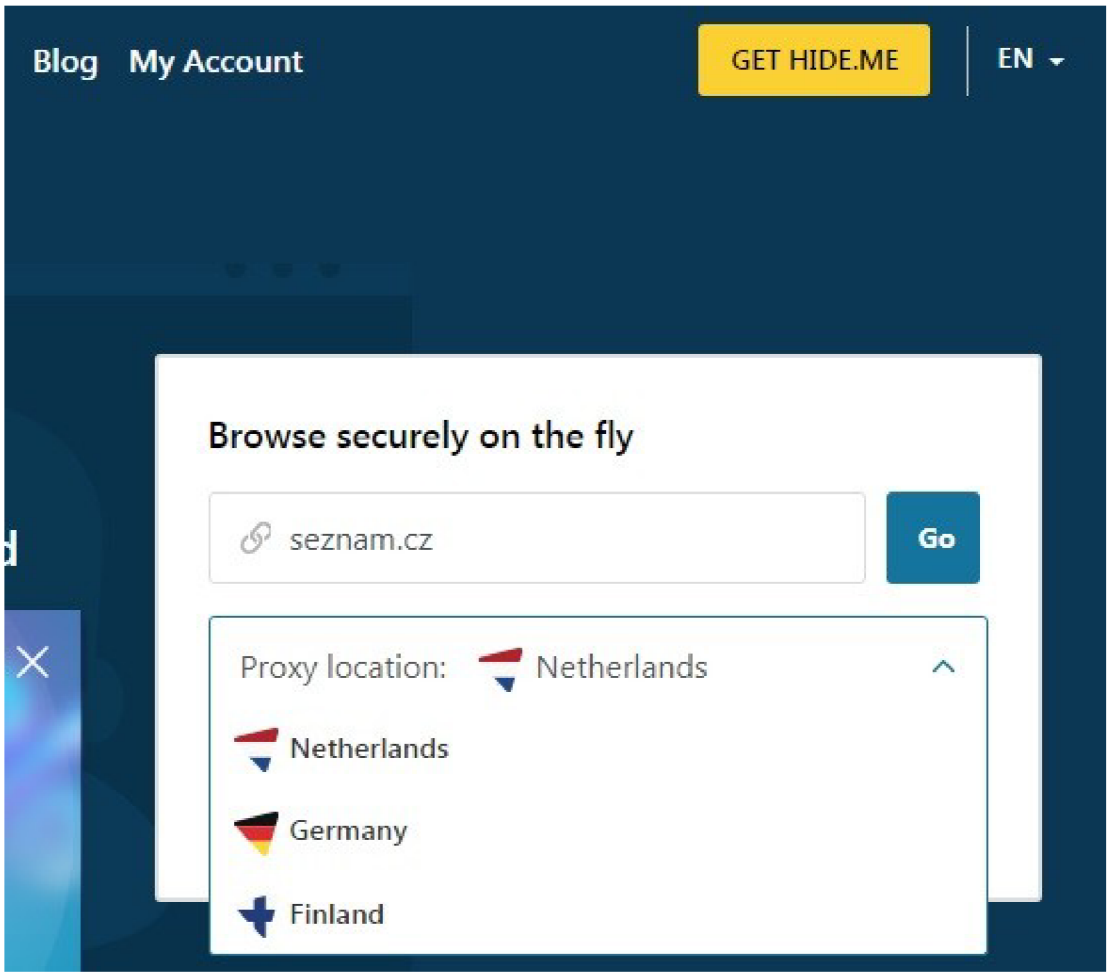
[10] Zdroj : Zákon č. 101/2000 Sb. Zákon o ochraně osobních údajů a o změně některých zákonů

2.4.3 Technická identita

Každý uživatel zanechá na internetu po své činnosti specifickou stopu. Ať už ve formě ukládání IP adres a některých dalších údajů o užitém počítači, operačním systému nebo verzi prohlížeče. V současné době při návštěvě 99% webových stránek potvrzujeme přijímání tzv. souboru cookies, které také nesou jistou část informací o uživateli. Tyto záznamy bývají logovány při návštěvě dnes již drtivé většiny webových stránek. Údaje technické identity se tedy většinou týkají dané osoby pouze nepřímo a nemusí ji jednoznačně identifikovat – mohou ale nasměrovat k dalším postupům. Nejcennějším údajem spadajícím do této problematiky z hlediska vyhledávání informací o osobách je bezesporu IP adresa.

Některá diskusní fóra nebo diskuze pod internetovými články také ukládají např. IP adresu diskutujících a v některých případech je tato adresa (nebo její část bez posledních několika znaků) zobrazena veřejně přímo u každého příspěvku. Dále je IP adresa součástí podrobné hlavičky e-mailů. IP adresa může být pevná, přidělená danému počítači na stálo ze strany poskytovatele internetových služeb (ISP) nebo dynamická, která se v čase mění. Ze získané IP adresy lze pomocí různých nástrojů zjistit některé údaje o jejím uživateli (resp. o jeho počítači). Z IP adresy lze dále zjistit DNS jméno, lokalitu (země, kraj, město, PSČ), časové pásmo, údaje o poskytovateli internetové služby (ISP) pro danou IP adresu. Dále je možno sledovat směrování, resp. trasu vedoucí od aktuálního počítače k počítači s danou IP adresou. Vyhledávání údajů o IP adrese lze provést pomocí k tomu určených nástrojů typu Whois.net, nebo prostřednictvím některých speciálních aplikací. Samozřejmě existují možnosti, jak každou IP adresu skrýt, ať už z důvodu prosté ochrany soukromí, nebo z důvodu zakrytí nevhodné či nelegální činnosti na internetu. Mezi nejběžnější metody patří využití služby TOR (The Onion Routing), anonymní šifrované VPN (Virtual Private Network), nebo připojení prostřednictvím anonymní proxy. To lze velmi jednoduše prostřednictvím některého z dostupných "anonymizérů" Tento způsob je navíc absolutně rychlý a spolehlivý.

Jako příklad uvedu server HIDE.ME , kde si dokonce můžeme vybrat přes kterou zemi nás bude server "anonymizovat". Tím pádem, pokud by na serveru seznam.cz dohledávali mojí aktivitu v daný čas připojení, zobrazila by se IP adresa připojená z Nizozemska a ne ta reálná.



Obrázek 7 - Internetový anonymizér HIDE.ME, snímek autora

Zdroj : HIDE.ME

2.5 Sociální sítě

Sociální sítě jako prostředek veřejné komunikace a jeden z nejvýznamnějších otevřených zdrojů informací zastávají stále významnější roli v oblasti získávání informací o osobách. Vytěžování sociálních sítí stojí v popředí zájmu mnoha firem, zejména z důvodu získávání údajů pro marketingové účely. Sociálních sítí existuje velké množství. V českých podmínkách jsou nejčastěji

využívány služby Facebook, Twitter, YouTube, Instagram atd. Cílené vytěžování údajů ze sociálních sítí je ve většině případů v rozporu s podmínkami provozovatelů těchto služeb. Současný trend je růst věkového průměru uživatelů sociálních sítí. S tím souvisí rostoucí význam sociálních sítí právě pro oblast vyhledávání informací o osobách, nebo věcech, neboť užívání těchto sítí již není výsadou mládeže.

2.5.1 Aktuální statistika využití sociálních médií

- 3,96 miliardy lidí v současné době používá sociální média po celém světě, což je téměř dvojnásobek oproti 2,07 miliardám v roce 2015.
- Průměrný člověk měl v roce 2020 8,8 účtů na sociálních médiích oproti 4,8 v roce 2014
- Míra růstu sociálních médií od roku 2015 je v průměru meziročně 12,5%. Růst je však na ústupu, přičemž údaje z let 2019–2020 ukazují míru růstu 9,2 %.
- Podle regionů je růst sociálních médií v letech 2019–2020 veden Asií: +16,98 %, Afrika +13,92 %, Jižní Amerika +8,00 %, Severní Amerika +6,96 %, Evropa +4,32 % a Australasie +4,9 %.
- 50,64 % z 7,77 miliardy lidí na světě používá sociální sítě.
- 83,36 % uživatelů internetu mají profily na sociálních platformách.
- Z 3,96 miliard uživatelů sociálních médií má 99 % přístup k webům nebo aplikacím prostřednictvím mobilního zařízení, přičemž pouze 1,32 % má přístup k platformám výhradně přes počítač.
- Globálně je průměrná doba, kterou člověk tráví denně na sociálních sítích, 2 hodiny 24 minuty. Kdyby se někdo přihlásil v 16 letech a dožil se 70 let, strávil by na nich 5,7 roku svého života.

- Facebook je nejnavštěvovanější sociální síť s 2,7 miliardami aktivních uživatelů měsíčně, následuje YouTube (2 miliardy), WhatsApp (2 miliardy), FB Messenger (1,3 miliardy) a WeChat (1,2 miliardy).[11]

Pokud se podíváme na top 8 sociálních platforem podle měsíčních aktivních uživatelů, YouTube, LinkedIn, Twitter a TikTok mají vyšší index mezi muži. Weby jako Facebook a Instagram jsou více zaměřeny na ženy. Pinterest také dominuje u ženského publika.

	Muži (% používání)	Ženy (% používání)
Facebook	63	75
Instagram	31	43
Twitter	24	21
LinkedIn	29	24
Pinterest	15	42
Snapchat	24	24
YouTube	78	68
TikTok	56	44
Reddit	15	8
WhatsApp	21	19

Obrázek 8 - Statistika využívání sociálních sítí dle pohlaví

Zdroj: https://lerstudio.cz/statistiky-vyuziti-socialnich-siti-kolik-lidi-pouziva-socialni-media-v-roce-2021

[11] Zdroj: https://lerstudio.cz/statistiky-vyuziti-socialnich-siti-kolik-lidi-pouziva-socialni-media-v-roce-2021

Facebook je v současnosti světově nejpoužívanější sociální sítí, na které je zaregistrováno přes 2,7 miliardy uživatelů .Jde o velmi cenný zdroj údajů o osobách, neboť lidé zde zcela dobrovolně poskytují své osobní údaje a mnoho informací ze svého soukromého života prostřednictvím profilových údajů, statusů, odkazů na zdi či sdílením fotografií, videa, nebo přesné polohy. Toto chování je taky součástí mého dotazníkového šetření.

Facebook umožňuje vyhledávání lidí, stránek, skupin, aplikací, událostí a příspěvků uživatelů. Uživatelské nastavení soukromí umožňuje určitou kontrolu nad sdílením zveřejňovaného obsahu, včetně možnosti znemožnit vyhledání profilu pomocí vyhledávačů či jakýmkoliv jiným způsobem. Pokud to však uživatel nezakázal, je možno ověřit, zda je k určité e-mailové adrese přiřazen některý profil jednoduchým zadáním e-mailové adresy do vyhledávacího pole Facebooku. V případě, že uživatel znemožnil vyhledání svého profilu prostřednictvím e-mailové adresy, lze alespoň ověřit, zda je e-mailová adresa na Facebooku použita (ale bez možnosti přiřazení ke konkrétnímu profilu). Toho lze docílit provedením neúplné registrace na Facebooku pod danou e-mailovou adresou, tedy zadáním zjišťované adresy do registračního formuláře – pokud je adresa již použita, objeví se chybová hláška: "Již existuje účet spojený s tímto e-mailem.“ V současné době není Facebook výsadou pouze mladší generace uživatelů internetu, ale naopak přibývá množství uživatelů střední či starší věkové kategorie. Cílené vytěžování údajů z této sítě je v rozporu s podmínkami užívání.

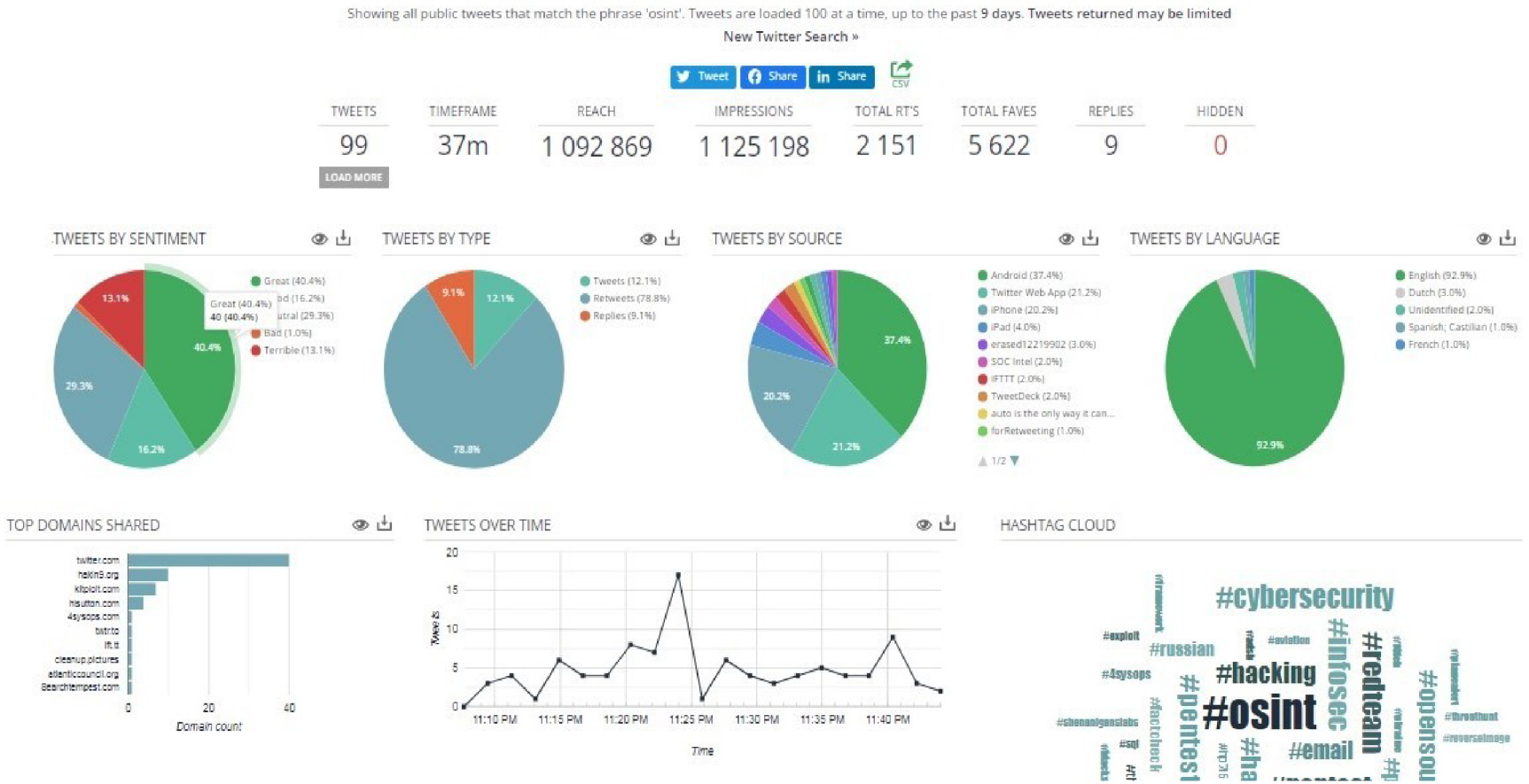
Jsou dvě možnosti, jak analyzovat sociální sítě – ručně, prohledáváním účtů a stránek anebo pomocí specializovaných nástrojů. Ty ve většině případů šetří hlavně čas.

Například nástroj fb-sleep-stats sleduje, ve které časy jsou uživatelovi přátelé na Facebooku online a vytváří graf podle kterého lze dlouhodobě monitorovat jejich denní rutinu nebo to, jak moc pravidelný spánek mají. Další užitečný nástroj sherlock podle uživatelského jména prohledá až 305 sociálních sítí a najde shody. Jiný nástroj, Social Bearing, analyzuje výskyt hledaného

výrazu na sociální síti Twitter, určí jeho typ, uvede zdroj, jazyk, čas, lokalizaci a nakonec uvede samotné tweety (viz obrázek č.9)

Já jsem zadal do analýzy slovo "OSINT". Viz moje snímky obrazovky níže, se můžeme podívat na analýzu využití tohoto slova a dále s "ním" nejčastěji související hashtagy.

Obrázek 9 - OSINT nejčastěji používané hashtagy, snímek autora



Obrázek 10 - OSINT Social Bearing analýza, snímek autora

Social Bearing nabízí také možnost vyhledávání z pohledu místa (např. zobrazí kdo během posledních 9 dní tweetoval z konkrétní oblasti, ulice, města, státu s možností volby rádiusu od 0,5 km do 2 000 km). S informacemi z Twitteru pracuje i nástroj Treeverse, který vizualizuje konverzace u sledovaných tweetů do hierarchické struktury stromu podle chronologické návaznosti, jednotlivé větve pak barevně odlišuje podle rychlosti uživatelovy odpovědi.

Social Searcher je nástroj pro real-time monitorování sociálních sítí založený na principu webového crawlingu. Vyhledávání třídí na web a konkrétní sociální sítě jako Twitter, Facebook, YouTube, Instagram, Reddit, Dailymotion, Tumblr, Vimeo, VKontakte, LinkedIn a Flickr. Uživatel se buď nepřihlašuje, ale využívá jen omezené nabídky vyhledávání za den, nebo si zaplatí měsíční paušál, který mu umožňuje více vyhledávání, uložení dat, zaslání upozornění na e-mail v případě nového příspěvku, a především úplný výsledek hledání. Samotný Social Searcher pod sebou sdružuje několik menších nástrojů, které se specializují na konkrétní případy užití. Social Buzz se zaměřuje na sociální sítě, Google Social Search prohledává web s možností filtrů sociálních sítí, Search Users podle jména či příjmení vyhledá profil uživatele a Social Trends, který k danému tématu najde nejoblíbenější, nejsdílenější či nejčtenější příspěvky na vybraných sociálních sítích, Facebook Search se zaměřuje na vyhledávání na této stránce. Vyhledávání je ulehčeno některými filtry, detailní statistikou a analýzou, kterou nástroj přehledně vizualizuje. Na výběr je omezení typu příspěvku (odkaz, fotografie, video, status), odhadovaný postoj přispěvatele (pozitivní, negativní, neutrální), zdroje (jednotlivé sociální sítě), jazyk (výběr ze 42) a řazení podle data nebo popularity. Při konkrétním hledání nástroj spočítá příspěvky, ve kterých byl výraz zmíněný, počet uživatelů, kteří výraz zmínili a poměr postojů. Podrobněji pak zobrazuje aktivitu po hodinách, dnech, týdnech a měsících až do chvíle, kdy byl hledaný výraz poprvé použit. Dále je tu poměr jednotlivých sociálních sítí, nejpoužívanější hashtagy a klíčová slova spojována s daným výrazem, postoje podle sítí, počet zobrazení, rozdělení na aktivní nebo populární uživatele, často otevírané odkazy a další přehled či řazení dostupných informací.

V praxi je nástroj možné využít pro jakékoliv monitorování osob, uživatelů, citací, hashtagů, hesel (sloganů) a jiných zmínek. Všechna větší sociální média v reálném čase, na jednom místě, s možností filtrování výsledků a detailní statistikou. Jedno z možných využití je například sledování reakcí zákazníků pro vypuštění kontroverzní reklamní kampaně nebo chování voličů ve volebním období.

2.6 Další oblasti využití informací z otevřených

2.6.1 Oblast konkurenčního „boje“ mezi obchodními společnostmi

OSINT se stále více stává populární i v komerčním sektoru. Používají se k usnadnění podnikových procesů v oblasti nákupu, HR, podnikové bezpečnosti a analýzy konkurence.

Použitím OSINT v podnikání za pomocí nejrůznějších technik založených na OSINT můžete zlepšit klíčové části obchodního procesu, včetně typování nových zákazníků, dodavatelů, konkurentů a třeba i obchodních značek. Komerční OSINT strategie můžeme rozdělit dle zaměření do následujících kategorii

- Zákazníci

V mnoha klíčových společnostech jsou metody OSINT používány v procesu takzvaného "know your customer" (KYC). Jedná se o shromažďování dat o obchodních příležitostech, zákaznících, konkurentech, dodavatelích a výběrových řízeních a zároveň objasňování jejich aktivit a korelací. Analýza takovéto digitální stopy nám navíc umožňuje identifikovat osoby s rozhodovací pravomocí a nalézt jedinečné prodejní a rozhodovací příležitosti. Výsledek takovéhoto dobře zaměřeného a cíleného zpravodajství může poskytnout pozoruhodnou konkurenční výhodu, což ve výsledku umožňuje vyhrávat mnoho jednání.

- Dodavatelé

Řešení OSINT jsou také velmi užitečná při zadávání veřejných zakázek, zejména při vyšetřování korupce, při kontrolách dodržování předpisů a při monitorování klíčových osob a organizací na sociálních sítích.

- Konkurence

Znát své konkurenty je zásadní. nejčastější problém je najít informace o jejich skutečných aktivitách: změny v organizační struktuře, personální operace, zpětná vazba od zákazníků, účast ve výběrových řízeních a tak dále. Dříve taková analýza zabrala nadměrné množství času a peněz. V dnešní době však nástroje OSINT využívající automatizovanou umělou inteligenci a zpřístupňují tyto informace v reálném čase a s naprostou legitimitou.

- Ochrana obchodní značky

Bezpečnostní složky států, vládní organizace a soukromí detektivové používají OSINT po desetiletí při identifikaci teroristických a zločineckých skupin prostřednictvím sociálních médií, "deep" webu a dalších online zdrojů. Dnes se stejné metody používají i v podnikání. Nástroje OSINT tím, že uživatelům na dosah ruky dávají nepřeberné množství vyhledávacích metod a otevřených zdrojů, umožňují společnostem hodnotit věrohodnost své značky, udržovat vysoce kvalitní správu svých domén a databází, zefektivňovat operace a vyšetřovat konkrétní případy, které by mohly poškodit pověst značky prostřednictvím nezákonných úniků softwaru a obchodování na deep webu. Zároveň lze tyto technologie také použít během marketingových kampaní k měření a porovnávání povědomí o dané značce v konkrétních lokalitách.

2.6.2 Žurnalistika

Práce s otevřenými zdroji je nedílnou a důležitou součástí žurnalistické zpravodajské činnosti. OSINT používaný pro žurnalistiku staví na široké škále digitálních zdrojů odvozených z nových technologií a internetových služeb. V této oblasti jsou často vyhledávány informace o osobách (např. politici, podnikatelé, vědci, celebrity, pachatelé trestné činnosti) nebo o společnostech či dalších subjektech a jejich vzájemných vztazích. V rámci žurnalistiky lze OSINT využívat k monitorování vývoje sociálních, hospodářských a jiných situací v některých zemích a k monitorování vývoje určitých specifických událostí. Důležitá je zde především práce s již existujícími zdroji informací. Výstupem je zveřejnění prostřednictvím tištěných či audiovizuálních médií. Jak se stále více novinářů seznamuje s technikami a nástroji, OSINT se bude rozšiřovat z velkých redakcí na menší a dokonce na individuální novináře. Open source techniky mohou být stejně cenné pro jednotlivé novináře a malé redakce jako pro mediální giganty.

2.6.3 Soukromé bezpečnostní agentury

Jednou z oblastí, které se věnují soukromé bezpečnostní agentury, je pátrání po osobách, či vyhledávání informací o osobách a firmách nebo vyhledávání vazeb mezi těmito subjekty, nebo naopak zajišťování bezpečí takových osob. Dále může jít o monitorování vazeb mezi osobami či jinými subjekty. Dále si může soukromá bezpečnostní agentura vyhledat veřejně dostupné informace například o majetku, životní situaci atd. Také společnosti pro vymáhání pohledávek využívají internet pro získání informací o dlužnících. Soukromé bezpečnostní agentury obecně používají velké placené databáze, aby určili pravděpodobnou aktuální adresu, telefonní číslo, historii adres a změť dalších irelevantních dat. Jako další varianta zdroje informací pro soukromé agentury, může být bezesporu v rámci propletení se s veřejnými orgány státní moci, využíváním těchto orgánů a jím podřízených útvarů, agend a dalších míst s přístupem k "omezeným" informacím. Například lustrace, osob, vozidel atd., a

to ať už "ze známosti", díky dobrým vztahům, nebo i korupci. V krajním případě by připadala i možnost "nabouraní" se do takové nepřístupné databáze.

2.7 Právní ukotvení sledování osob a věcí

Pro účely této diplomové práce a názornému příkladu jsem vybral právní ukotvení dle Zákona č. 141/1961 Sb. Trestní řád, o sledování osob a věcí

§ 158d

Ale aby to nebylo pouze okopírované znění uvedeného paragrafu Trestního řádu, pokusím se na některých odstavcích tohoto paragrafu poukázat na praktické možnosti použití OSINT.

(1) Sledováním osob a věcí (dále jen "sledování") se rozumí získávání poznatků o osobách a věcech prováděné utajovaným způsobem technickými, nebo jinými prostředky. Pokud policejní orgán při sledování zjistí, že obviněný komunikuje se svým obhájcem, je povinen záznam s obsahem této komunikace zničit a poznatky, které se v této souvislosti dozvěděl, nijak nepoužít.

Technickými, nebo jinými způsoby se rozumí právě prostředky, které sice nejsou přístupné široké veřejnosti, ale po splnění "podmínky" v podobě písemného povolení např. státního zástupce k nim má policejní orgán přístup. Příkladem jsou telefonní odposlechy, monitorování provozu konkrétních počítačů internetové sítě, skryté pořizování zvukových nebo obrazových záznamů v různém prostředí, identifikaci a zjišťování pohybu osob

(2) Sledování, při kterém mají být pořizovány zvukové, obrazové nebo jiné záznamy, lze uskutečnit pouze na základě písemného povolení státního zástupce.

Veškeré postupy policejního orgánu jsou protokolovány a zadávány do složek, systémů a databází jak v písemné formě, tak i elektronické

formě. Mezinárodní spoluprácí se dané protokoly dostávají i do mezinárodního "oběhu" informací. Tím se opět plní zdroje informací.

(3) Pokud má být sledováním zasahováno do nedotknutelnosti obydlí, do listovního tajemství nebo zjišťován obsah jiných písemností a záznamů uchovávaných v soukromí za použití technických prostředků, lze je uskutečnit jen na základě předchozího povolení soudce. Při vstupu do obydlí nesmějí být provedeny žádné jiné úkony než takové, které směřují k umístění technických prostředků.

Zde bych uvedl jako příklad takzvanou obhlídku místa zájmu. Ta může probíhat za využití otevřených zdrojů informací, jako jsou mapové podklady místa, výpisy z katastru nemovitosti, lustrace dané adresy a osob s vazbou na zájmovou osobu. To jsou kroky, které předcházejí samotnému vstupu do obydlí.

(4) Povolení podle odstavců 2 a 3 lze vydat jen na základě písemné žádosti. Žádost musí být odůvodněna podezřením na konkrétní trestnou činnost a, jsou-li známy, též údaji o osobách či věcech, které mají být sledovány. V povolení musí být stanovena doba, po kterou bude sledování prováděno a která nesmí být delší než šest měsíců. Tuto dobu může ten, kdo sledování povolil, na základě nové žádosti písemně prodloužit vždy na dobu nejvýše šesti měsíců.

V písemné žádosti o povolení, jak je uvedené výše by měli být uvedeny všechny známé údaje o osobách a věcech tak, aby nemohli být zaměněny. Toto opět probíhá pomocí dotazů do dostupných veřejných i neveřejných databází, lustrací osob, vozidel, ale například i v registru zbraní atd.

(5) Nesnese-li věc odkladu a nejde-li o případy uvedené v odstavci 3, lze sledování zahájit i bez povolení. Policejní orgán je však povinen o povolení bezodkladně dodatečně požádat, a pokud je do 48 hodin neobdrží, je povinen sledování ukončit, případný záznam zničit a informace, které se v této souvislosti dozvěděl, nijak nepoužít.

Jeden z případů, kdy po neobdržení dodatečného písemného povolení musí policejní orgán všechny zjištěné záznamy zničit a nijak je do databází neprotokolovat. Tudíž pak nejsou součástí dostupných zdrojů.

(6) Bez splnění podmínek podle odstavců 2 a 3 lze sledování provést, pokud s tím výslovně souhlasí ten, do jehož práv a svobod má být sledováním zasahováno. Je-li takový souhlas dodatečně odvolán, sledování se neprodleně zastaví.

(7) Má-li být záznam pořízený při sledování použit jako důkaz, je třeba k němu připojit protokol s náležitostmi uvedenými v § 55 a 55a.

Protokol je opět součástí vyšetřovacího spisu, tudíž součástí konkrétní databáze.

(8) Pokud nebyly při sledování zjištěny skutečnosti důležité pro trestní řízení, je nutno záznamy předepsaným způsobem zničit.

O zničení takových záznamů se vyhotovuje protokol, který je opět součástí vyšetřovacího spisu, tudíž součástí konkrétní databáze.

(9) Provozovatelé telekomunikační činnosti, jejich zaměstnanci a jiné osoby, které se na provozování telekomunikační činnosti podílejí, jakož i pošta nebo osoba provádějící dopravu zásilek jsou povinny bezúplatně poskytovat policejnímu orgánu provádějícímu sledování podle jeho pokynů nezbytnou součinnost. Přitom se nelze dovolávat povinnosti mlčenlivosti stanovené zvláštními zákony.

Zde je hezký příklad zákonné spolupráce provozovatelů telekomunikací a České pošty, kteří jsou povinni poskytnout nezbytnou součinnost na písemnou žádost policejního orgánu. Ten může dožadovat informace z jinak neveřejných "databází" těchto provozovatelů. Tím se policejní orgán dostane ke zdroji informací například o majitelích telefonních čísel a naopak, IMSI a IMEI zakoupených mobilních přístrojů, souvisejících službách, k online i offline hovorové komunikaci, sms

komunikaci, poloha telefonního zařízení, buď aktuální dle nejbližší BTS, nebo poslední známá před vypnutím zařízení.

(10) V jiné trestní věci, než je ta, v níž bylo sledování za podmínek uvedených v odstavci 2provedeno, lze záznam pořízený při sledování a připojený protokol použít jako důkaz jen tehdy, je-li i v této věci vedeno řízení o úmyslném trestném činu nebo souhlasí-li s tím osoba, do jejíž práv a svobod bylo sledováním zasahováno.[12]

3 Využití OSINT z při sledování osob a věcí

Vaše data a informace jsou vystavena více, než sami čekáte

V tomto článku vysvětlím, jak odhalit digitální stopu člověka, provádět digitální vyšetřování a shromažďovat informace pro konkurenční zpravodajství, penetrační testování, nebo vyhledávání bezpečnostních rizik a závadových osob.

V současné době je k dispozici mnoho nástrojů OSINT, takže je nebudu pokrývat všechny, pouze ty nejoblíbenější a užitečné v popsaných případech použití. V této práci ukazuji obecný přístup a různé nástroje a metody, které můžete použít v závislosti na požadavcích a počátečních datech, která máte.

Potřebuji najít, nebo sledovat osobu, uživatele, nebo identitu online. Kde začít?

Existují desítky webových stránek, kde můžeme najít informace o lidech nebo organizacích. Toto je samozřejmě závislé na dané zemi ve které hledáme, protože informační "otevřenost" může být různá. V současné době je k dispozici mnoho nástrojů OSINT, v možnostech této diplomové práce není je popsat všechny, a to nejen díky aktuálnímu množství těchto nástrojů, ale i z důvodu neustálému vývoji, kdy nové nástroje vznikají a jiné zanikají. Věnovat se budu

[12] Zdroj: Zákon č. 141/1961 Sb. Zákon o trestním řízení soudním (trestní řád)

pouze těm nejoblíbenějším a užitečným v následně popsaných případech použití. představuji pouze obecný přístup a různé nástroje a metody, které můžete použít v závislosti na požadavcích a počátečních datech, která máte.

Koncept úplné online anonymity je extrémně obtížné dosáhnout, stát se zcela anonymní online vyžaduje použití sady nástrojů a taktik ke skrytí jakékoli stopy, která může odhalit vaši identitu nebo dokonce typ hardwaru a připojení, které používáte pro přístup k internetu, a to vyžaduje určité technické dovednosti. Případy související s národní bezpečností nebo zahraniční špionáží vyžadují tuto úroveň anonymity a obvykle je vedou bezpečnostní agentury, které dobře vědí, jak své shromažďovací aktivity utajit.

OSINT základní kroky:

- Začněte tím, co znáte (e-mail, uživatelské jméno, reálné jméno, telefonní číslo atd.),
- definujte požadavky (co chcete získat),
- shromážděte data,
- analyzujte shromážděná data.

3.1 Základní principy využívání a metodiky z pohledu bezpečnostních složek

Využití OSINT při zkoumání nebo vyšetřování subjektu umožňuje orgánům činným v trestním řízení, zpravodajským službám (dále jen odpovědným orgánům) shromažďovat a analyzovat relevantní a včasné informace ze široké škály zdrojů, které pomáhají s řízením rizik a předcházením trestné činnosti. Vyšetřování vedené na rozkrývání rizik, hrozeb a osob za touto problematikou stojících, založené na zpravodajských informacích se spoléhají na spolehlivé, relevantní, včasné a použitelné zpravodajské informace. OSINT umožňuje odpovědným orgánům shromažďovat a analyzovat informace z

internetu týkající se jejich vyšetřování, identifikace osob, aktérů hrozeb, kriminality a svědků. OSINT umožňuje odpovědným orgánům shromažďovat informace ze široké škály zdrojů, vytvářet detailní obraz o zločincích, sítích organizovaného zločinu, obchodování s lidmi, nelegálním obchodu s různými kategoriemi nelegálních komodit a mnohem více.

Zpravodajští analytici shromažďují, shromažďují a analyzují informace z internetu pomocí Kiplingovy metody Šest otázek (Six Questions). Ta je jednou z nejobecnějších a přitom nejúčinnějších analytických technik. Používá se také název šestislovný graf nebo šest sluhů (six servants). V anglickém jazyce je někdy označována jako 5W + 1H (who, what, where, when, why, how). v českém jazyce kdo?, co?, kdy?, kde?, proč? a jak?, což určuje předpoklad pro úspěšné řešení kriminálních otázek a stanoví doporučení pro narušení kriminality.

Konkrétní taktiky a řešení používané při vyšetřování na internetu ze strany odpovědných orgánů obvykle nejsou plně zveřejněny, aby bylo zajištěno, že zločinci a zločinné organizace nebudou moci tyto informace využít k tomu, aby se vyhnuli odhalení, což by veřejnost ohrozilo. Vyšetřovatelé odpovědných orgánů mají vysoký standard při určování, zda může internetové vyšetřování získat takzvaně zelenou, přičemž schválení je dáno případ od případu. Souvisí to individuálně na objektu zájmu.

- Příklad z praxe : osoby ve služebním poměru mají například ze zákona možnost na evidenční ochranu. To znamená, že na jakýkoliv lustrační dotaz na jeho osobu, bydliště a další libovolné údaje které si chce nechat chránit (manželka, děti vozidlo) mu přijde lustrační upozornění, kde zjistí kdo, kde, kdy a proč ho lustroval. To může vzbudit v případě zájmu podezření a proto je důležité veškeré takové kroky konzultovat.

Profesionálové v oblasti zpravodajství, vyšetřování a vyhledávání pracující jménem odpovědných orgánů mohou OSINT využívat k několika účelům:

3.1.1 Odhad rizika a vyhledávání rizik

Pracovníci zpravodajského výzkumného týmu (speciální analytický tým) poskytují 24 hodin / 7 dní v týdnu zpravodajskou schopnost v reálném čase, provádějí výzkum pomocí otevřených a uzavřených zdrojů, aby uspokojili operační požadavky a poskytovali pro odpovědné orgány informace o možných rizicích v reálném čase. OSINT umožňuje zpravodajským analytikům a pracovníkům provádět kontroly, obhlídky na předmětu operativního zájmu činnosti, například s cílem určit, kdo v daném místě žije, vstupní body do jejich majetku, vazby na další možné závadové osoby a zda existují nějaká rizika, jako jsou zveřejněné obrázky zbraní, nástrahové techniky, zabezpečení, nebo například psů. V tomto ohledu lidé nevědomky zveřejňují toliko informací, že na první pohled z kusých střípku dokáže profesionál sestavit detailní pohled a doporučení pro další postup.

Internetový průzkum v reálném čase také může informovat o předběžném vývoji zpravodajských informací na podporu závažných nebo kritických incidentů. Bezprostředně po vážných incidentech mohou odpovědné orgány sledovat příspěvky na sociálních sítích související s daným incidentem, aby určily rozsah dopadu a míru bezpečnostních rizik. Tento výzkum umožňuje příslušníkům přijíždějícím na místo lépe interpretovat situaci a efektivně reagovat na situaci, která se v čase vyvíjí. Další možností je sledování příspěvků na sociálních sítích například po nějakém teroristickém útoku, kde lze využít získané poznatky pro možný předpoklad vývoje dalších sekundárních rizik jako jsou nezákonná podpora a schvalování takového jednání, popírání a rozdmýchávání negativních nálad ve společnosti atd.

3.1.2 Pozadí k objektu zájmu (subjektu)

Profesionálové v oblasti zpravodajství využívají informace z otevřených zdrojů informací k vytvoření profilu o objektu zájmu (subjektu) tím může být jakákoliv osoba, podezřelý, obviněný, ale i obchodní společnost atd.. Profily takových subjektů pomáhají při stanovování dalších priorit, pomáhají identifikovat mezery ve zpravodajství a zdůrazňují třeba i možnosti prevence, psychické narušení subjektu a možnost prosazování práva. OSINT umožňuje analytikům a vyšetřovatelům objevovat informace, které subjekty zveřejnily online, nebo se shromažďováním souhlasily, což poskytuje pohled na ně a jejich životní styl. Při procesu prosazování práva může relevantní OSINT zahrnovat jméno, místo, kontaktní údaje, fotografie, soudní záznamy, záznamy o vozidle, finanční údaje a zvyky osoby

3.1.3 Sledování aktivit na povrchovém internetu

OSINT poskytuje odpovědným orgánům možnost zjevně či skrytě vyšetřovat, zkoumat, vyhledávat a sledovat osoby přes internet. Tyto orgány mají přístup k profilům osob na sociálních sítích, aby mohli sledovat jejich online aktivitu, identifikovat položky k prodeji a komentáře, které například dokazují kriminalitu. K tomuto účelu založené "falešné" osobní účty mohou být použity k zajištění toho, že nebude vytvořena digitální stopa, jako je zobrazení na seznamu lidí, kteří si prohlédli stránku. Přístup k informacím z internetu, jako jsou tweety, může odpovědným orgánům poskytnout přístup k informacím, které by jinak nemohly být nikdy odhaleny. Například svědci trestných činů mohou zveřejňovat informace o tom, co viděli, ale nehlásili to přímo orgánu činnému v trestním řízení. OSINT pomáhá rozšířit zpravodajský obraz a umožňuje orgánům činným v trestním řízení mít co nejjasnější přehled o trestné činnosti.

3.1.4 Sledování aktivit na temném webu - "dark webu", "deep webu"

Kromě provádění činnosti OSINT na povrchovém webu jak jsem popisoval výše, mohou odpovědné orgány také provádět průzkum na temném webu s cílem odhalit trestnou činnost. Činnost na temném webu provádějí odpovědné orgány pouze tehdy, když je to nezbytné a přiměřené ke splnění cílů konkrétního případu. Nástroje OSINT prohledávají temná webová fóra a trhy za účelem zjištění nezákonné činnosti, která může zahrnovat obchodování s nelegálním zbožím a službami, jako jsou nelegální drogy, zbraně a školící materiály, jako jsou například příručky o hackerství, příručky na výrobu výbušnin atd..OSINT na temném webu zkoumá a usnadňuje vyšetřování zločinů včetně kybernetické kriminality, kybernetické války a kyberterorismu, které by tradiční policejní metody nebyly schopny detekovat a narušit..

3.1.5 Utajená vyšetřování

Většina vyšetřovacích internetových aktivit prováděných odpovědnými orgány je pasivní, což znamená, že nezahrnuje přímý kontakt s předmětem vyšetřování. Je-li to nutné a přiměřené, mohou příslušníci donucovacích orgánů využívat skryté účty ke kontaktování subjektů během činnosti OSINT. Příslušníci mohou působit pod skrytou legendou a získávat informace o zločincích a jejich činnosti tím, že navazují kontakt a používají právě vhodně zvolenou legendu, smyšlené jméno atd.. Utajené internetové vyšetřování může umožnit komunikaci s jedním subjektem, nebo se skupinami vyšetřovaných osob, aby bylo možné zjistit, zda vůbec dochází ke kriminalitě. Utajovaná činnost může příslušníkům pomoci získat důvěru zločinců a usnadnit vyšetřování organizované sítě a obchodů s nelegálním zbožím.

3.1.6 Boj proti terorismu

Internet hraje klíčovou roli v radikalizaci, náboru, výcviku, financování a podněcování teroristických aktivit. Odpovědné orgány provádějí činnost OSINT na internetu s cílem pronásledovat teroristické aktéry a předcházet teroristickým aktivitám, chránit je před nimi a připravovat se na ně. Odpovědné orgány provádějí obranná opatření a praktikují techniky kontrarozvědky "red-teaming". To je skupina, která hraje roli nepřítele nebo konkurenta a poskytuje bezpečnostní zpětnou vazbu z této perspektivy. Tyto teamy se používají v mnoha oblastech, zejména v kybernetické bezpečnosti, letištní bezpečnosti, armádě a zpravodajských agenturách, aby zvýšily své situační povědomí. Potencionální vysoce rizikové cíle, lokace i jednotlivci, lze prozkoumat, aby odhalilo veřejné riziko, které může ohrozit jejich bezpečnost, což umožní toto riziko snížit. Kromě toho orgány činné v trestním řízení provádějí ofensivní internetová šetření tím, že vyhledávají, monitorují a nahlašují jakékoliv podezřelé teroristické zdroje a jednotlivce. Zpravodajští analytici a výzkumní pracovníci lokalizují teroristická místa, materiály, buňky, sítě, vazby zájmových osob a využívají je pro zpravodajské účely, což orgánům činným v trestním řízení umožní provádět fyzické operace k zatčení radikalizovaných jedinců plánujících trestné činy související s terorismem a zabránit tomu, aby k těmto zločinům došlo.

3.1.7 Analýza velkých dat

Odpovědné orgány mohou využívat OSINT pro analýzu "velkých dat" k analýze příspěvků na sociálních sítích k rozvoji situačního povědomí, pomocí zpravodajských analytiků a datových vědců k interpretaci kvantitativních dat ve velkém měřítku. Clustering je technika používaná k analýze souboru silných a slabých „signálů“/„indikátorů“ v datech za účelem předvídání většího obrazu, což umožňuje orgánům činným v trestním řízení detekovat signály z neurčitého "šumu". Pomocí analýzy slabých ukazatelů mohou slabé ukazatele pomoci při

řešení trestných činů, jako je obchodování s lidmi, zbraněmi a financování terorismu. Analýza slabého ukazatele bere v úvahu složky hrozeb, jako je nárůst obchodu se slonovinou, nebo celní zabavení zbraní. Jednotlivé indikátory nemusí přitahovat pozornost, ale pokud jsou seskupeny, mohou tyto indikátory naznačovat širší zájem a problém. Úspěšná OSINT analýza pro analýzu "dolovaných" dat využívá prvek mozku analytika vedle objektivních strojově vedených velkých dat a analýzy slabého signálu.

3.2 Konkrétní metody a nástroje pro vyhledávání osob a věcí

3.2.1 Reálné jméno

Jak jsem již uvedl, v roce 2002 začal Johnny Long shromažďovat vyhledávací dotazy Google, které odhalily zranitelné systémy, nebo citlivé informace. Označil je jako Google Dorks. V následujících řádcích Vám ukážu příklad postupu při vyhledávání osob u které se domníváme, že známe reálné jméno s metodou právě umíněného Google Dorkingu. Níže uvedené dotazy nám mohou poskytnout informace, které je obtížné najít pomocí jednoduchého vyhledávání tak, jak jsme všichni zvyklý.

V tomto případě nechám použité "jméno" JOHN DOE jako nejčastěji uváděné "příkladové jméno". Samozřejmě si můžete dosadit pro zajímavost jakékoliv jiné, či Vaše jméno a uvidíte markantní rozdíly. Například u jména autora "Luboš Kubovec" po zadání do Google.com se zobrazí spousta výsledků, ale tím, že se sám znám vím, že ani jeden z nich není relevantní mé osobě. Naopak při specifickém zadání toho samého jména s příkazy Google dorks, Google nabízí výsledky, které jsou již konkrétní a platné.

Příklady pro Vás : jména a servery lze pro zajímavost libovolně zaměňovat.

• „john doe“ site:instagram.com – uvozovky nutí vyhledávač Google provádět naprosto přesnou shodu, zatímco vyhledávání probíhá na serveru instagram.com.

• „john doe“ -“site:instagram.com/johndoe“ site:instagram.com – skryje příspěvky z vlastního účtu cíle, ale zobrazí komentáře u příspěvků ostatních na Instagramu.

• „john“ „doe“ -site:instagram.com - zobrazí výsledky, které přesně odpovídají křestnímu jménu a příjmení, ale v různých kombinacích. Z výsledků tentoktát vylučuje Instagram.

• „CV“ OR „Životopis“: PDF „john“ „doe“ – vyhledejte životopisy osoby, které obsahují slova „CV“ nebo „Životopis“ v názvu a mají příponu PDF.

Pokud jste si pravopisem 100% jisti, dejte jednotlivá slova do "uvozovek", protože ve výchozím nastavení se Google vždy pokusí upravit vaše klíčové slovo podle toho, co chce a vyhledává většina uživatelů. Mimochodem, na Instagramu je zajímavé to, že se správným Google Dorkem můžete vidět komentáře a lajky i soukromých účtů, do kterých nemáme absolutně žádný přístup.

Existují webové stránky, které se specializují na vyhledávání osob. Toto vyhledávání lze provést zadáním informací, které máme dostupné (skutečné jméno, uživatelské jméno, e-mail nebo telefonní číslo).

https://www.spokeo.com

https://thatsthem.com

https://www.beenverified.com

https://www.fastpeoplesearch.com

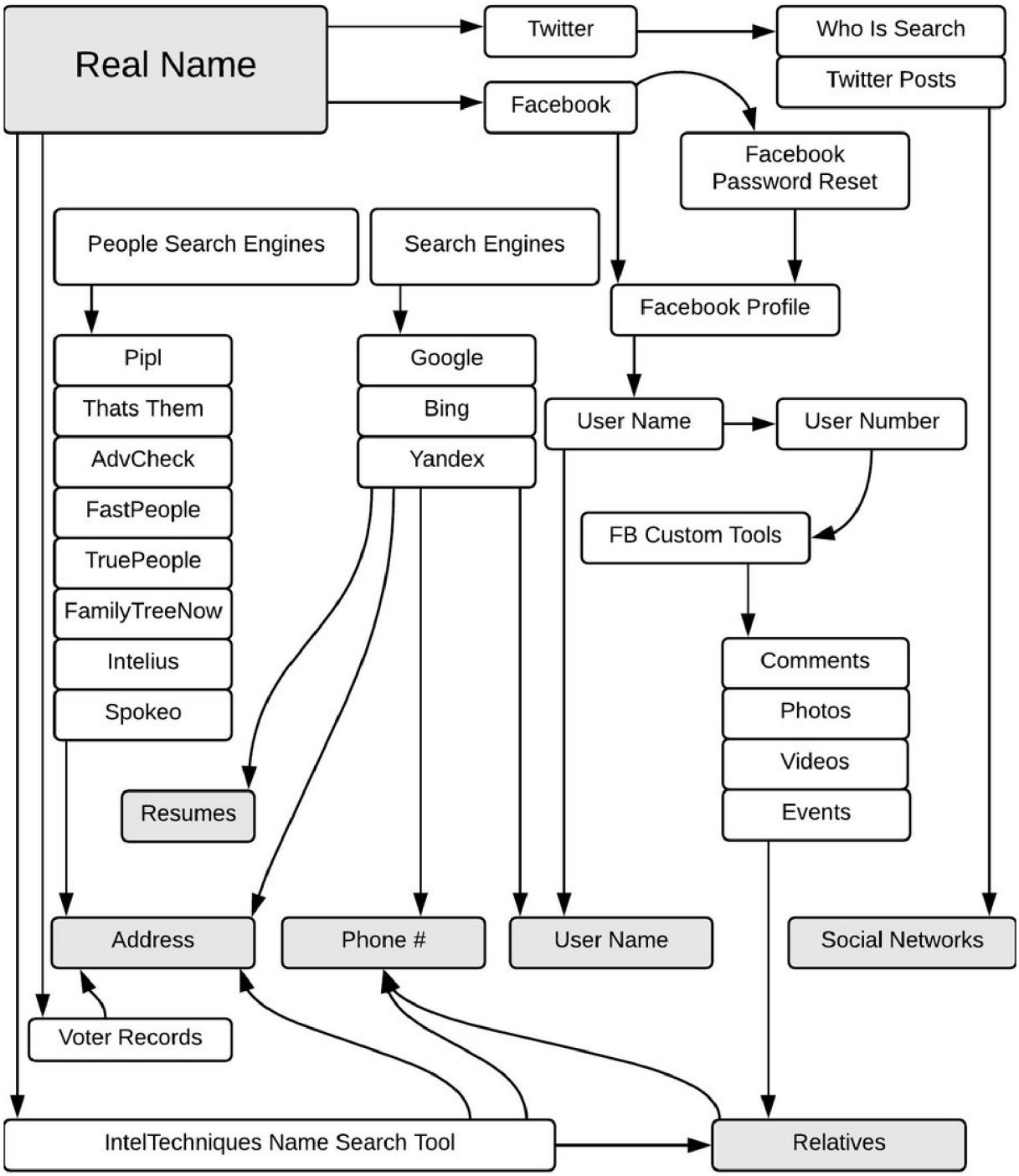
https://www.truepeoplesearch.com

https://www.familytreenow.com

https://people.yandex.ru

Většina z těchto uvedených webů je zabezpečena speciálními protokoly a nastavením, tudíž standardní prohlížeče s "defaultním" nastavením Vás nepustí dál do vyhledavače. Aktualizované prohlížeče Google Chrome, Internet Explorer, Firefox atd. uveřejňují informace, že webová stránka je nedůvěryhodná a nelze na ní pokračovat. Nicméně musím potvrdit, že aktuálně fungují všechny zde vypsané.

Na schématu níže si můžete udělat představu o tom, jaké metody a principy se využívají při vyhledávání informaci z otevřených zdrojů při znalosti "reálného jména"



Obrázek 11 - Princip vyhledávání a ověřování skutečných jmén

Zdroj: https://medium.com/the-first-digit/osint-how-to-find-information-on-anyone-5029a3c7fd56

3.2.2 Uživatelské jméno

V této části se pokusím přiblížit jak je teoreticky možné najít uživatelské jméno. Nejčastěji je to kombinace jména a příjmení, nebo kombinace odvozená z e-mailu, názvu domény webové stránky, kterou osoba používá, nebo vlastní. Začneme s daty, které máme, a provedeme zpětné vyhledání toho, co potřebujeme. Nejjednodušší způsob je samozřejmě vyhledat na Google vyhledavači jakákoli relevantní data, která v tuto chvíli známe, a pokusit se najít stránky s uživatelským jménem. K uživatelskému jménu se můžeme dostat skrze jméno reálné, které podrobíme metodě viz obrázek výše. Protože jedním z výstupů může být právě e-mailová adresa nebo uživatelské jméno. Můžeme ale také použít speciální webové stránky, které provádějí zpětné vyhledávání uživatelských jmen, jako je socialcatfish.com, usersearch.org nebo peekyou.com.

Stejný Google dorking, který jsem Vám ukázal pro hledání skutečného jména, je užitečný i při hledání odpovědí na uživatelské jméno. Kromě toho vám vyhledávání adres URL může poskytnout dobré výsledky, protože adresy URL obvykle obsahují uživatelská jména.

•inurl:johndoe site:instagram.com - vyhledejte na Instagramu adresy URL, které obsahují „johndoe“.

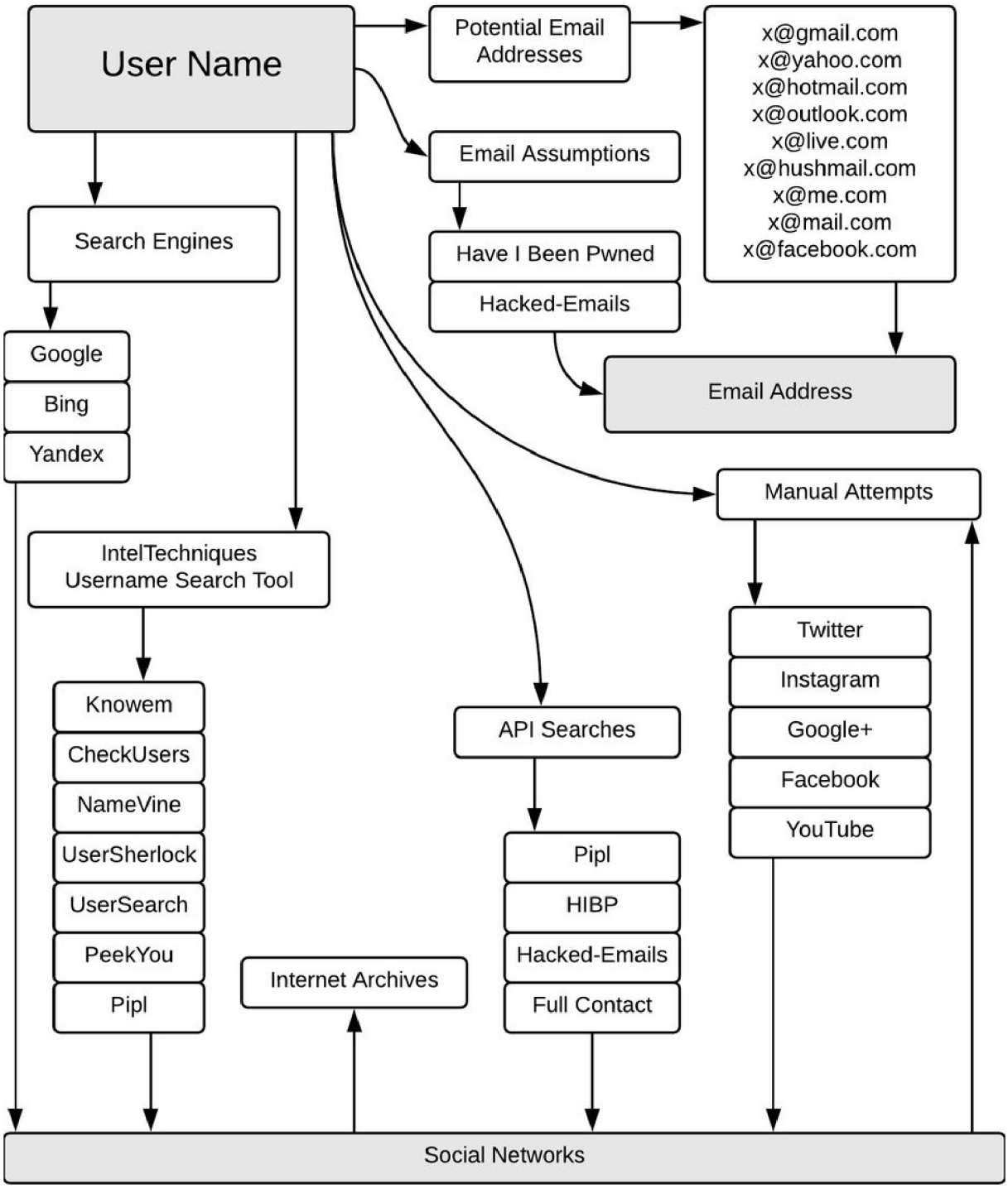
•allinurl:john doe any site:instagram.com - vyhledejte stránky se slovy „john“, „doe“ v URL Instagramu. Podobné jako "inurl", ale podporuje více slov.

Existuje opět mnoho webových stránek s vyhledáváním uživatelských jmen. Zde vybrané 2, jsou uváděny za jedny z nejlepších:

instantusername.com a namechk.com

Obvykle jedna služba najde ty účty, které ta druhá ne, takže je lepší používat obě webové stránky.

Na schématu níže si můžete udělat představu o tom, jaké metody a principy se využívají při vyhledávání informaci z otevřených zdrojů při znalosti "uživatelského jména"



Obrázek 12 - Princip vyhledávání a ověřování uživatelských jmén

Zdroj: https://medium.com/the-first-digit/osint-how-to-find-information-on-anyone-5029a3c7fd56

3.2.3 E-mailová adresa

V této části se pokusím přiblížit, jak je teoreticky možné najít e-mailovou adresu. Stejný Google dorking, který jsem Vám ukázal pro hledání skutečného a uživatelského jména, je užitečný i při hledání odpovědí na e-mailovou adresu.

•„@example.com“ site:example.com - vyhledá všechny e-maily v dané doméně.

•HR „e-mail“ site:example.com filetype:csv | filetype:xls | filetype:xlsx - vyhledejte seznamy kontaktů HR v dané doméně.

•site:example.com intext:@gmail.com filetype:xls - extrahuje e-mailovou ID z Google v dané doméně.

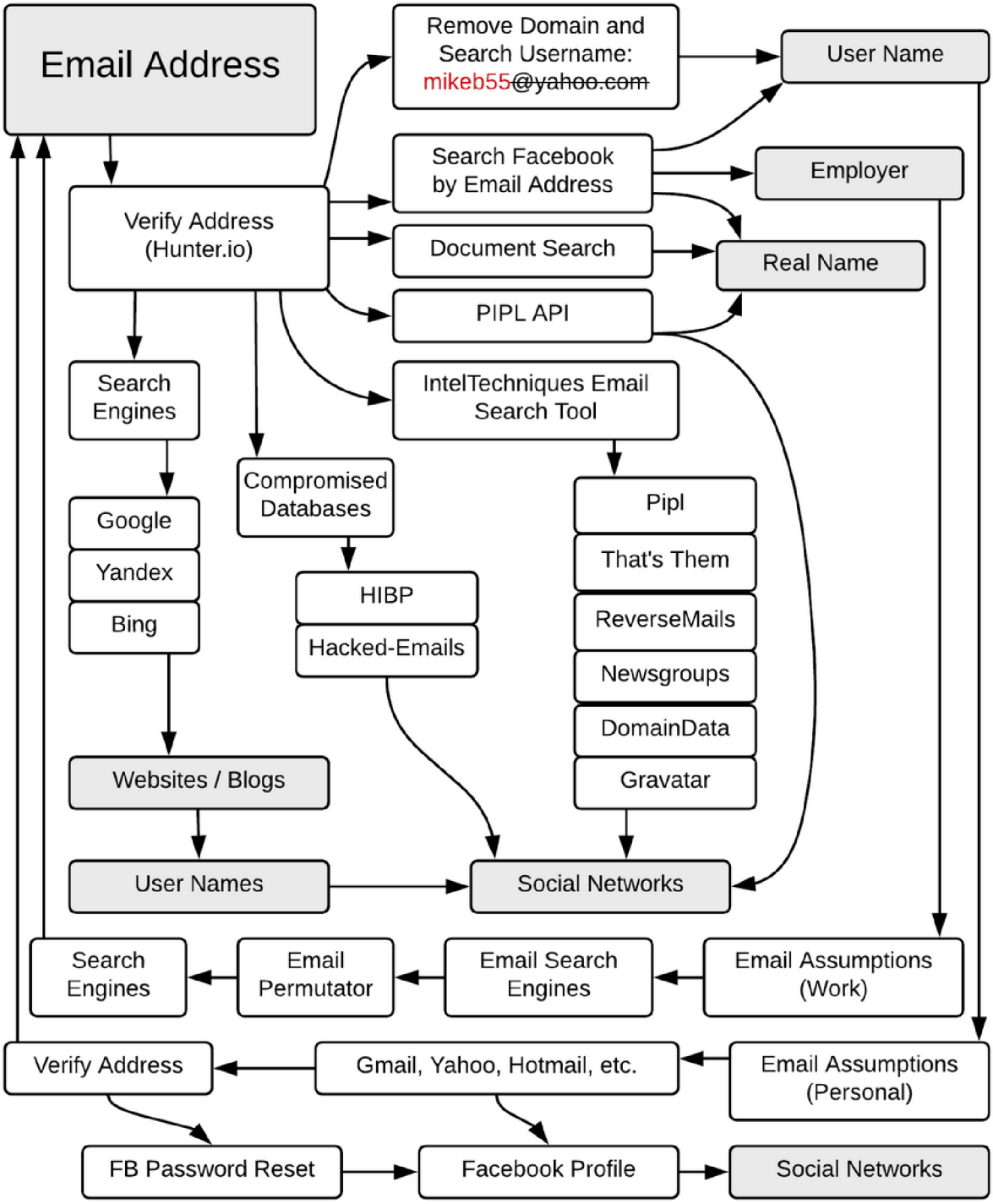
Užitečné e-mailové nástroje

- Hunter - provádí rychlé skenování názvu domény pro e-mailové adresy a odhaluje jeho společný vzor.
- E-mailový permutátor - generuje permutace až tří domén, u kterých bude mít za cíl pravděpodobnou e-mailovou adresu. Podporuje vstup více proměnných pro generování vlastních výsledků.
- Proofy - umožňuje hromadné ověřování e-mailů, což je užitečné, když jste vygenerovali seznam e-mailů pomocí permutačního nástroje a chcete je zkontrolovat všechny najednou.
- Verifalia - ověřuje jednotlivé e-mailové adresy zdarma a bez registrace. Chcete-li použít hromadné ověření, musíte se zaregistrovat.

Zásuvné moduly (pluginy) prohlížeče

- Prophet - odhaluje více informací o lidech. Využívá pokročilý engine k předpovídání nejpravděpodobnější e-mailové kombinace pro danou osobu na základě jména, společnosti a dalších sociálních dat. Poté Prophet ověří vygenerovaný e-mail, aby se ujistil, že je správný a doručitelný.
- OSINT rozšíření prohlížeče - obsahuje mnoho užitečných odkazů, včetně odkazů pro vyhledávání a ověřování e-mailů je kompatibilní s Firefoxem a Chromem.
- LinkedIn Sales Navigator - plugin pro Chrome, který zobrazuje přidružený účet Twitter a bohatá data profilu LinkedIn přímo v Gmailu.

Na schématu níže si můžete udělat představu o tom, jaké metody a principy se využívají při vyhledávání informaci z otevřených zdrojů při znalosti "e-mailové adresy"



Obrázek 13 - Princip vyhledávání a ověřování e-mailových adres

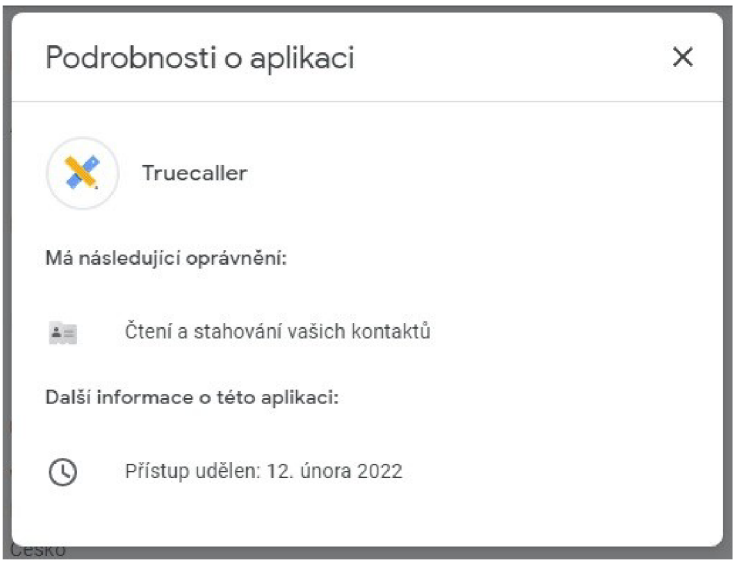
Zdroj: https://medium.com/the-first-digit/osint-how-to-find-information-on-anyone-5029a3c7fd56

3.2.4 Telefonní číslo

Nejčastěji si lidé spojují telefonní číslo a e-mail se svým profilem na sociálních sítích, zejména na Facebooku, aniž by přemýšleli nad tím, jaká z toho hrozí teoretická rizika. Takže když tyto údaje zadáte do vyhledávání na Facebooku, profil se kterým jsou tyto údaje spojené se Vám zobrazí. Tato funkce spojování a párování telefonních čísel právě na zmíněném Facebooku se tváří jako prvek zabezpečení a skutečně tak i funguje v rámci jakéhosi zabezpečení pro případ, kdy zapomenete uživatelské jméno, nebo heslo. Tento nástroj nicméně funguje skvěle i opačně, dává nám možnost verifikace námi zjištěných údajů.

Další možností je vyhledání telefonních čísel je v uživatelsky dodaných databází telefonních čísel, jako je whocallme.com , truecaller.com atd. Tyto databáze nejsou omezeny pouze na oblast Spojených státu amerických, ale lze kontrolovat i telefonní čísla z Evropy a zbytku světa. Tyto databáze jsou samozřejmě v dnešní moderní době dostupné i jako aplikace v mobilních zařízeních , díky tomu je potencionální využitelnost velmi vysoká.

Jelikož jsem veškeré informace, které zde uvádím sám zkoušel testovat, musím upozornit, že tyto informace ač se leckdy tak tváří nejsou "zadarmo" a to už jak ve smyslu peněžním (jednorázové poplatky, předplatné, license atd.) Tak hlavně ve smyslu, že instalací takových aplikací a registrací na těchto stránkách, musíte dát souhlas s poskytnutím "Vašich" údajů o kontaktech. Tím rozumějte, že pokud chcete skutečně vyhledávat, musíte souhlasit. Co si například server Truecaller od Vás vezme ? Vaším dobrovolným souhlasem se na server Truecaller.com a do jeho databáze stáhnou veškeré e-mailové adresy, se kterými jste byli kdy v kontaktu, k těmto údajům si "automatický skript" dohledává i spárované telefonní čísla, jména, adresy atd. Zkrátka veškeré údaje, které máte ve své e-mailové schránce.



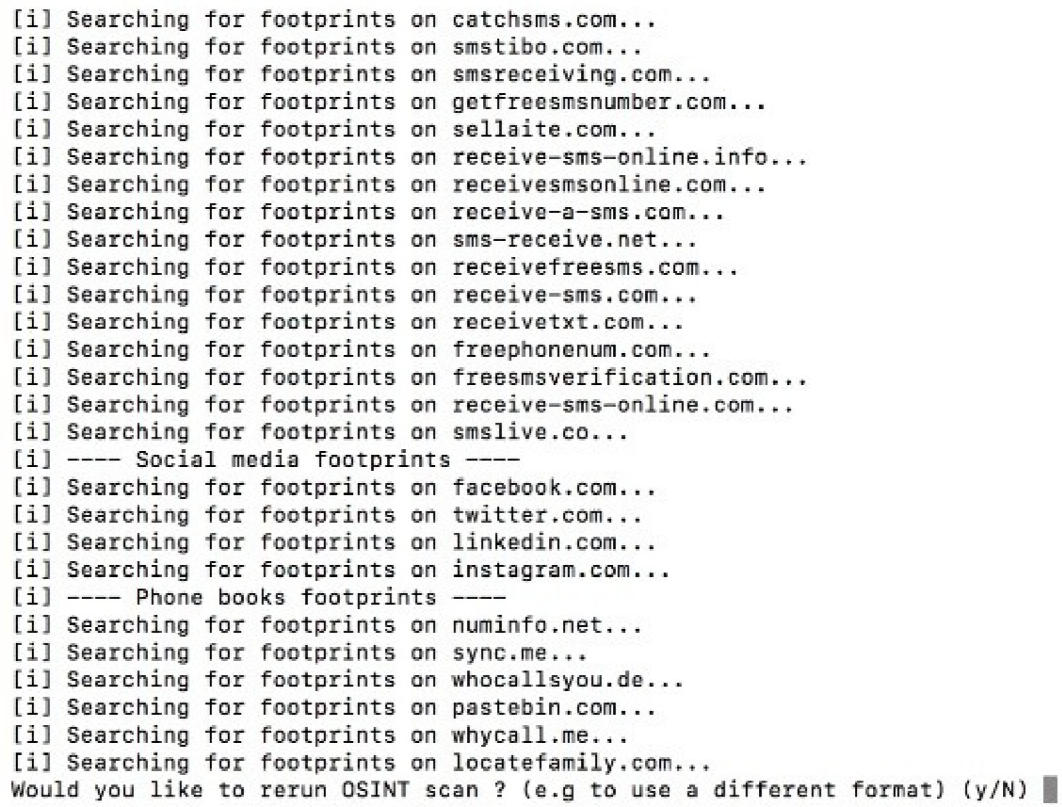
Obrázek 14 - Truecaller vyžadované oprávnění, snímek autora

Dalším vhodným nástrojem pro zjišťování telefonních čísel je PhoneInfoga. PhoneInfoga je jedním z nejpokročilejších nástrojů pro skenování telefonních čísel pouze pomocí bezplatných zdrojů. Cílem je nejprve s velmi dobrou přesností shromáždit základní informace, jako je země, oblast, operátor a typ linky na jakýchkoli mezinárodních telefonních číslech. Poté zkusí určit poskytovatele VoIP (Dnes jde již o poměrně zastaralou službu, která využívá pro volání prostředí internetu). Veškeré zjištěné poznatky automaticky vyhledává v nastavených vyhledávačích tak, aby se pokusila identifikovat vlastníka.

Funkce:

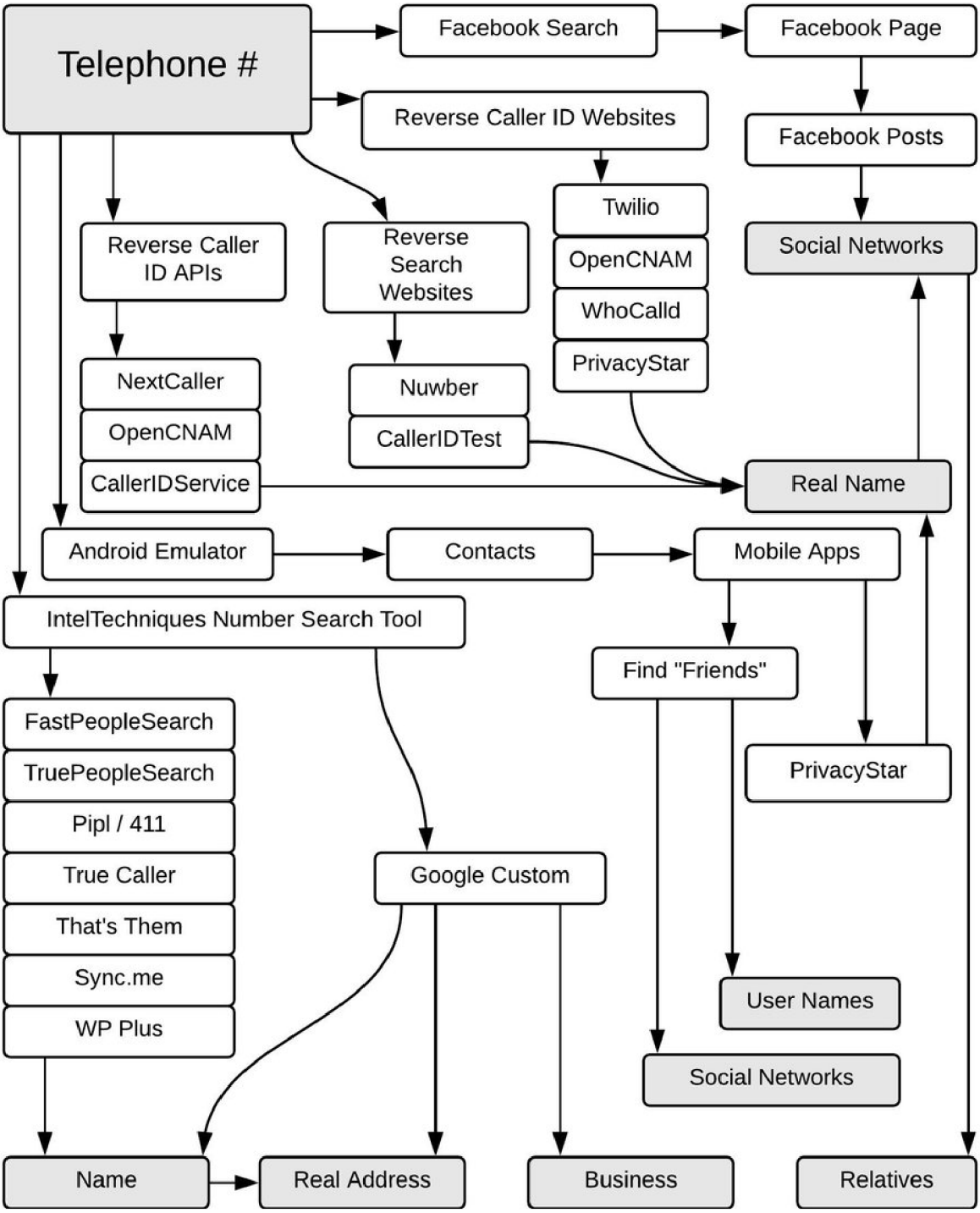
- Zkontroluje, zda telefonní číslo vůbec existuje.
- Shromáždí standardní informace, jako je země, typ linky, provozovatel atd.
- Zkontroluje několik čísel najednou
- Prozkoumává OSINT pomocí externích API, Google Hacking telefonních seznamů a vyhledávačů.
- Použije vlastní formátování pro efektivnější OSINT průzkum.

Na snímku obrazovky autora níže se můžete podívat na část vyhledávacího protokolu PhoneInfoga. Můžeme zde vidět předem definované vyhledávání digitálních stop konkrétního telefonního čísla na různých serverech. Proces vyhledávání funguje automaticky.



Obrázek 15 - Automatické vyhledávání PhoneInfoga, snímek autora

Na schématu níže si můžete opět udělat představu o tom, jaké metody a principy se využívají při vyhledávání informaci z otevřených zdrojů při znalosti "telefonního čísla"



Obrázek 16 - Princip vyhledávání a ověřování telefonních čísel

Zdroj: https://medium.com/the-first-digit/osint-how-to-find-information-on-anyone-5029a3c7fd56

3.2.5 Data na sociálních sítích

Sociální sítě, jako je Facebook , Twitter, nebo Instagram, ale i další nás mohou sledovat online aktivitu uživatelů i na jiných webových stránkách (ve skutečnosti dokonce mohou sledovat historii prohlíženého obsahu většiny uživatelů internetu). A to i v době, kdy tito uživatelé nejsou aktuálně přihlášeni ke svým přidruženým účtům !

Jako příklad uvedu situaci kterou všichni známe a setkáváme se s ní při procházení většiny internetových stránek, fór, aplikací atd.. Drtivá většina takových internetových stránek, aniž by nám to připadalo jakkoliv divné a pozastavovali jsme se nad touto funkcí, má v sobě implementována tlačítka (Facebooku) „To se mi líbí“ a „Sdílet“, která usnadňují sdílení obsahu na Facebookových novinkách uživatele. Doposud je tato akce zcela normální a užitečná, měli bychom avšak vědět, že kdykoli navštívíte webovou stránku, která má implementováno zmíněné tlačítko „To se mi líbí“ nebo „Sdílet“, Facebook tuto návštěvu zaznamená, a to i když jste na tlačítko neklikli ! Sledování Facebooku se v tomto bodě nezastaví, protože mohou sledovat uživatele mimo Facebook na různých webových stránkách pomocí skrytého kódu vloženého do jejich tlačítek „To se mi líbí“ a „Sdílet“, aniž by o tom uživatelé věděli.

U sociální sítě Twitter má "tlačítko" „Sledovat“ také stejnou výše zmíněnou roli při sledování online uživatelů, stejně jako tlačítka „To se mi líbí“ a „Sdílet“ na Facebooku.

V této části se zaměříme na pojem "SOCMINT", který je podmnožinou OSINT. SOCMINT se zaměřuje na shromažďování a monitorování dat na platformách sociálních sítí a médií. Některé techniky zpravodajství z sociálních sítí jsem již popsal. Ale pro dokreslení problematiky zde doplním uvedením dalších nástrojů, které jsou čistě spojené se sociálními sítěmi a jejich vytěžováním.

3.2.5.1 Facebook

- ExractFace - získává data z Facebooku a zpřístupňuje je pro offline použití jako důkaz, nebo k provádění pokročilé offline analýzy.
- Facebook Sleep Stats - odhaduje vzorce spánku na základě stavu uživatelů online/offline.
- lookup-id.com - pomůže najít Facebook ID profilu nebo skupiny.

3.2.5.2 Twitter

- Twitter advance search - no, to je docela samozřejmé :)
- TweetDeck - poskytuje řídicí panel, který zobrazuje samostatné sloupce aktivity z vašeho účtů na Twitteru. Můžete například vidět samostatné sloupce pro domovský kanál, oznámení, přímé zprávy a aktivitu – to vše na jednom místě a na jedné obrazovce.
- Trendsmap - zobrazuje nejoblíbenější trendy, hashtagy a klíčová slova na Twitteru z celého světa.
- Foller - poskytuje bohaté informace o jakémkoli veřejném profilu Twitteru (veřejné informace o profilu, počet tweetů a sledujících, témata, hashtagy, zmínky).
- Socialbearing - bezplatná analytika Twitteru a vyhledávání tweetů, časových os a twitterových map. Vyhledá, filtruje a třídí tweety nebo lidi podle zapojení, vlivu, umístění, sentimentu a dalších. (příklad "Socialbearingu" jsem uvedl výše v kapitole - Sociální sítě)
- Sleepingtime - zobrazuje plán spánku veřejných účtů Twitter.
- Tinfoleak - zobrazuje zařízení, operační systémy, aplikace a sociální sítě používané uživatelem Twitteru. Také zobrazuje místa a geolokační souřadnice pro generování sledovací mapy navštívených míst. Tweety uživatelů Map v aplikaci Google Earth a další.

3.2.5.3 Instagram

- www.picodash.com - exportuje statistiky sledujících vybraného uživatele, nebo statistiky podle vybraného hashtagu do tabulky (CSV - excel). Také exportuje lajky a komentáře.
- https://web.stagram.com - online prohlížeč a zároveň stahovač obrázků a videí.
- https://codeofaninja.com/tools/find-instagram-user-id - získá unikátní ID uživatele. Uživatelská jména se mohou totiž měnit, takže je užitečné znát ID profilu, abyste stránku neztratili
- http://instadp.com - zobrazuje profilové obrázky v plné kvalitě.
- https://sometag.org - vyhledává populární hashtagy, místa a účty. Kromě toho porovnává účty a exportuje sledující a statistiky hashtagů.

3.2.5.4 LinkedIn

- InSpy - výpočetní nástroj, který je napsán v systému Python. Lze použít k vyhledávání zaměstnanců konkrétní organizace. Kromě toho může zjistit, jaké technologie organizace používá, což se provádí pomocí seznamu úloh procházení pro konkrétní klíčová slova.
- LinkedInt - extrahuje e-mailové adresy zaměstnanců ve vybrané organizaci. Podporuje automatickou detekci prefixu e-mailu pro daný název domény společnosti.
- ScrapedIn - skript v Pythonu, který extrahuje data profilu a importuje je do souboru XLSX (pro další použití s tabulkami Google).

3.3 Plně automatizované nástroje OSINT

Internet jak jsem uvedl v této práci již vícekrát, je nepřeberné, přesycené množství dat a ruční hledání informací může být v některých případech časově náročné a neefektivní. Automatické OSINT nástroje mohou navíc vytvářet korelace (to znamená vzájemné vztahy mezi dvěma procesy nebo veličinami. Pokud se jedna z nich mění, mění se korelativně i druhá a naopak), které byste jinak ani nepostřehli. Vše závisí na specifickém případě, zda tyto nástroje potřebujeme použít nebo ne. Jelikož většina z těchto nástrojů má strmou křivku učení a jsou vyžadovány hlavně k řešení složitých problémů.

Pokud tedy potřebujeme provést, nebo vyřešit jen několik jednoduchých úkolů, hledání atd. – postačí použít online služby a samostatné skripty, které jsem popsal v této práci výše. Pokud si ovšem chceme ušetřit čas, námahu a máme vhodně vytvořené podmínky pro přípravu "vyhledávacího prostředí", Zaměříme se právě na tyto níže popsané automatické nástroje, které jsou vytvořeny a přednastavený pro automatickou práci s OSINT. Upozorňuji, že všechny tyto nástroje nefungují na platformách Windows, ale je potřeba používat virtuální prostředí operačního systému BUSCADOR - Linux Virtual Machine, který je navržen právě pro práci s OSINT

Obrázek 17 - Pracovní plocha Buscador, snímek autora

3.3.1 SpiderFoot

SpiderFoot je uváděn jako jeden z nejlepších vyhledávacích automatických nástrojů pro OSINT. Lze ho použít k dotazování do více než 100 veřejných datových zdrojů současně a jeho vysoká modularita (nebo možnost nastavení a přizpůsobení) umožňuje vyladit specifikovat dotazované zdroje. Může sloužit nejen pro vyhledávání a sledovaní zájmových osob, ale i k detekování nejrůznějších hrozeb. Jeho speciální vlastností je možnost vyhledávání podle případů použití. Na výběr máme čtyři různé okruhy:

- získej všechna data o osobě (o cíli),
- porozuměj tomu, co vámi dotazovaná osoba vystavuje internetu, procházení webu a použití vyhledávače. Zde máme příklad toho, že tyto moderní automatizované nástroje pro vyhledávání obsahu mají možnost "učení se a porozumění" v závislosti na tom, jak s daným nástrojem každý uživatel pracuje.
- Dotazuj se na černé listiny (deep web) a další zdroje pro kontrolu škodlivosti osoby,
- shromažďuj informace prostřednictvím různých otevřených zdrojů. Poslední z nich je ideální pro pasivní průzkum.

3.3.2 theHarvester

theHarvester je velmi jednoduchý, ale účinný nástroj používaný k získávání cenných informací o zájmových osobách, hrozbách, ale i věcí ve fázi shromažďování informací. Je nepostradatelný pro skenování a vyhledávání informací souvisejících s doménami DNS a sběrem e-mailů. Pro pasivní průzkum využívá theHarvester mnoho zdrojů k načtení dat, jako jsou vyhledávače Bing, Baidu, Yahoo a Google a také sociální sítě jako LinkedIn, Twitter a Google Plus. Pro aktivní průzkum provádí zpětné vyhledávání DNS, rozšíření DNS TDL a hrubou sílu DNS.

(DNS je zkratkou anglického slovního spojení Domain Name System a představuje protokol, který zajišťuje překlad názvů domén webových stránek z nepřehledné (číselné) podoby využívané stroji na tzv. „doménové jméno“ – tedy název, který vidíte v prohlížeči a který zadáváte, když chcete na stránku vstoupit. Jako příklad o tom, jak celý tento proces funguje, můžeme ho přirovnat k telefonnímu seznamu v mobilním telefonu. Zapamatovat si telefonní čísla je jistě složitější než si pamatovat jména lidí, kterým chcete volat. Proto můžete v seznamu vyhledávat podle jmen. Telefon pak ale vytočí konkrétní číslo).[13]

3.3.3 Recon-ng

Recon-ng je další ze skvělých nástrojů typu příkazového řádku používaný k důkladnému a rychlému shromažďování informací. Tento plnohodnotný rámec průzkumu webového prostředí obsahuje široký výběr modulů pro pasivní průzkum, pohodlné funkce a interaktivní nápovědu, která vás provede správným používáním. Recon-ng je výborný nástroj, pokud hledáme něco výkonného co dokáže rychle zkontrolovat viditelnost naší společnosti a našich dat na internetu.

3.3.4 Maltego

Maltego je pokročilá platforma vyvinutá pro analýzu složitých internetových prostředí. Kromě data "miningu" (dolování, shromažďování dat) provádí korelaci dat a navíc je vizuálně prezentuje. Maltego pracuje s informacemi o osobách, společnostnech, s webovými stránkami, dokumenty a dalšími, které propojuje tak, abychom o nich získali další informace z širokého spektra různých zdrojů. Výsledky jsou pak smysluplné, validní a platné. Charakteristickým rysem tohoto nástroje je „transforms“ , nebo-li knihovna

[13] zdroj : https://www.airwaynet.cz/co-je-to-dns-a-jak-funguje/

doplňkových pluginů, které pomáhají spouštět různé druhy testů a integraci dat s externími aplikacemi.

3.3.5 FOCA

FOCA (Fingerprinting Organizations with Collected Archives) se zaměřuje na vyhledávání, webových stránek, serverů, domén a dokumentů zveřejněných na určitém místě. Dále umožňuje extrahování skrytých informací a metadat z různých takto vyhledaných analyzovaných dokumentů. Když jsou všechny zkoumané dokumenty tímto nástrojem analyzovány a extrahovány metadata, provádí se automatická analýza těchto metadat. Tato analýza se provádí, aby se zjistilo, které dokumenty byly vytvořeny stejným uživatelem. Je to jakýsi princip "otisku stejného psaní" (opakující se chyby, slova, nářečí, slovosled atd.) Jak již z názvu nástroje vyplívá o každém individuálním jedinci. FOCA také provádí korelaci podle serveru a tiskárny. Je to velmi užitečný a efektivní nástroj pokud potřebujeme zjistit zda jedna a tatáž osoba může být autorem více vytipovaných zpráv, nebo dokumentů. Z hlediska OSINT je nejvýznamnější funkcí možnost extrakce metadata ze všech dokumentů na určité doméně.

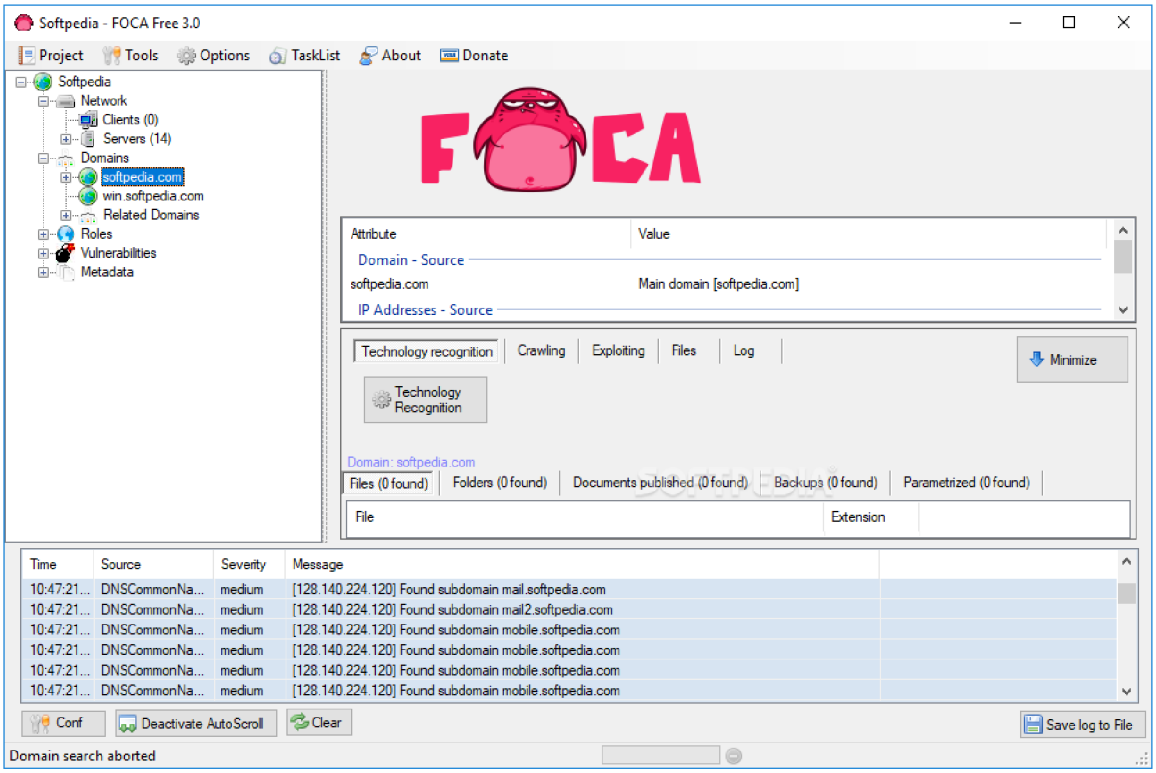
3.3.6 Metagoofil

Metagoofil je nástroj resp. skript v jazyce Python v podobě příkazového řádku, který se používá ke stahování veřejných dokumentů z webových stránek, doplněný o následující analýzou a extrakci metadat. Pracuje s pdf, doc, xls, ppt a dalšími formáty. Dokumenty jsou poté uloženy na disk a z nich extrahována metadata. Dále je vygenerován výstup obsahující uživatelská jména, e-mailové adresy, verze SW, názvy serverů a dalších PC.

Hlavními funkcemi nástrojů FOCA a Metagoofil je automatizované nalezení dokumentů na vybraných webových stránkách, jejich následné stažení,

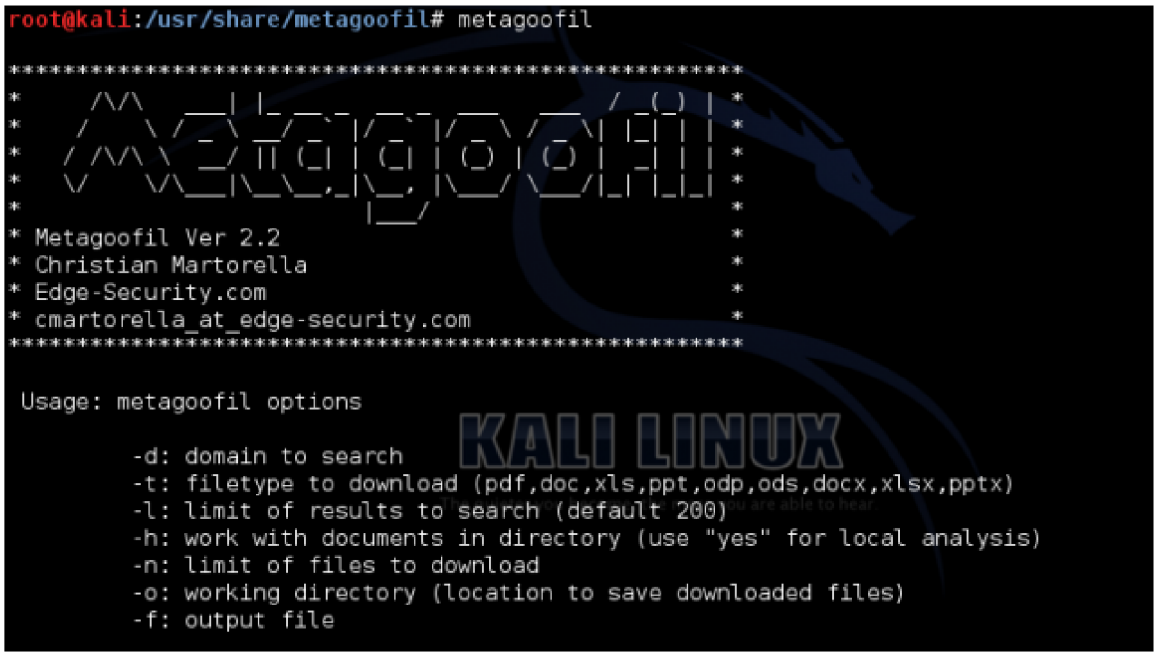
extrakce a analýza metadat z těchto dokumentů. Výhodou nástroje FOCA je přívětivé grafické uživatelské rozhraní a možnosti využití rozšiřujících pluginů.

Porovnání uživatelských rozhraních viz obrázky níže.



Obrázek 18 - Uživatelské prostředí nástroje Foca

Zdroj: https://www.elevenpaths.com/labstools/foca/index.html



Obrázek 19 - Uživatelské prostředí nástroje Metagoofil

Zdroj: http://www.edge-security.com/metagoofil.php

3.4 Případová studie využití sociálních sítí a otevřených zdrojů informací jako podpora v praxi při sledování osob

Já sám sloužím již cca 10 let u Bezpečnostní informační služby. Zde jsem začínal na pozici člena operativního oddělení. V tomto samém týmu jsem i v dnešní době, ovšem dnes již na pozici vedoucího tohoto oddělení. Z tohoto kontextu si myslím, že mám již alespoň malé a základní povědomí minimálně o tom, jaké metody vytěžování otevřených zdrojů na podporu sledování jsme měli a používali právě před cca 10 lety a jaké metody nám usnadňují práci teď v roce 2022.

Jelikož má Bezpečnostní informační služba celostátní působnost a my jsme měli "základnu" v Praze. Neobešli jsme se na začátku roku 2013 nikdo z nás bez papírové mapy. Což byl v té době náš otevřený zdroj informaci. První

verze mobilní aplikace mapy.cz pro mobilní telefony byla vydána 18. prosince 2013 a byla pro nás jako dar z nebes. Rychle jsme jí začali využívat jako skutečný mobilní veřejný zdroj informací. Ostatní v té době využívané otevřené zdroje bylo možné využívat pouze na stolních PC a byly to zejména katastry nemovitostí a program Tovek, který byl a stále je špičkou v oblasti analytického vyhledávání a zpracování informací z různorodých nestrukturovaných i strukturovaných zdrojů dat. Jelikož jsem psal, že sloužím u "výkonové" složky, tak jsme sami do styku s jinými otevřenými zdroji nepřišli. Jediný další podpůrný zdroj informací byly podklady od operativních složek vždy ke konkrétním případům a šetřením. Ty obsahovali právě informace z databází, lustrací, majetkové výpisy, vlastněná vozidla, fotografie, osobní vazby atd.

V porovnání s dnešní, řekl bych moderní a technologicky vyspělou dobou, se možnosti rozšířili o další možné a využitelné otevřené zdroje informací. Tyto informace nicméně u našeho oddělení slouží pouze jako jakási podpora a je velmi závislá na šikovnosti a zájmu o obor každého jednotlivce. To hlavně tím, že se nespecializujeme na tento sektor, protože práce s otevřenými zdroji spadá do působnosti sekce analytické.

Nicméně i přes tato fakta představím příklad právě takové podpory využití otevřených zdrojů informací, které jsem sám zažil.

3.4.1 Problém doby "covidové" - příklad č.1

Byl začátek roku 2020, v ČR se začali objevovat první případy nákazy nemocí COVID-19 a postupem času přišli první restrikce a nařízení. První příklad se týká právě nařízení o povinném nošení roušek a respirátorů i na veřejnosti. Nastal první problém se kterým jsme se nikdy nesetkali, a to ten, že jsme nebyli schopni spolehlivě identifikovat osoby podle vzhledu obličeje. Samozřejmě u osob, které jsou dlouhodobě rozpracovány a mají své návyky, již obličej vidět nemusíme a jsme si i tak jisti, že to je ta, či ona osoba. Nicméně v té době se měla konat extrémně důležitá schůzka s předávkou mezi dvěma osobami. Jedna z těchto osob byla operativě známá, ale my jsme měli za úkol vyfotit a následně

ustanovit osobu druhou, neznámou. Schůzka opravdu proběhla podle předpokladu, vše jsme zadokumentovali, ale i přesto, že schůzka proběhla v venku na nejmenovaném místě, nesundala si zájmová osoba ochranu úst ani kšiltovku. Výsledkem teda byla pouze detailní fotografie postavy, jeho oblečení, a rysů očí a obočí. Dle dalších indiciích zúžila operativa totožnost neznámého na 2 konkrétní jména, 2 exponované osoby mediálního zájmu. V tomto případě jsem akci sám vedl, a proto mi to nedalo a znovu jsem se zaměřil na pořízené fotografie. V jednom okamžiku jsem si řekl větu "že tak děsný a nápadný kalhoty s žokejem jsem na nikom v životě neviděl" a zeptal jsem se sám sebe kolik lidi asi tak může přesně takový kalhoty nosit. Otevřel jsem aplikaci Facebook s tím, že se podívám, zda ty 2 možné osoby mají vlastní profil. První osoba ho neměla vůbec, tím zbyla možnost poslední. Ta druhá tipovaná osoba, říkejme jí třeba Aleš skutečně profil na Facebooku měl. Problém byl ten, že profil byl uzavřen pro osoby které nebyli v seznamu jeho přátel. Tím pádem jsem neviděl jedinou fotografii. Jelikož my žádnými analytickými nástroji, ani falešnými profily nedisponujeme, zkusil jsem štěstí vyhledal si Aleše manželku. Ta už byla "sdílnější" a bez dalšího sdílela absolutně všechny informace a fotografie s každým. Dokonce i fotografie s celou rodinou společně i s Alešem. Trvalo mi projít asi 200 fotografií a cca jeden rok "života manželky" než jsem mohl říct "mám tě". Skutečně jsem našel co jsem potřeboval. Fotku Aleše s manželkou a hlavně se stejně "blbými" kalhotami. Obrázky žokeje přesně seděli i v místech střihu na kapsách. Takže ve výsledku, i když byl Aleš opatrný a sám dbal na ochranu svého soukromí, které nesdílel s někým koho nezná. Jeho manželka žila o dost sdílnější život a ráda ukazovala světu všechno možné, včetně Aleše.

Na závěr tohoto případu chci říct, že se samozřejmě nejedná o ztotožnění, které by mohlo sloužit jako 100% důkaz, ale jelikož operativa Aleše jako tip měla, posloužilo toto hledání jako platný závěr.

(poznámka : rysy očí a obočí souhlasily taktéž) .

Obecně z praxe je Facebook.com a Instagram.com mocný zdroj informací. Je na každém z nás, kolik úsilí věnujeme ochraně informacím, které na ně vkládáme.

3.4.2 Neznalost politiky neomlouvá - příklad č.2

V tomto příkladu budu stručný, ale jistý pohled na otevřené zdroje určitě poskytne. Opět jsme měli zadokumentovat a identifikovat neznámou osobu, říkejme jí Radek. Informace, které jsme měli k dispozici byly pouze ty, že Radka má v daný den vyzvednout někde v oblasti Smíchovského nádraží v 10:00 řidič černého Mercedesu typu S a měli jsme uvedenou známou SPZ. Ten ho pak dále vezl na exponovanou schůzku. V první části jsme v internetových mapách (zdroj č.1) naplánovali a vytipovali možné příjezdové směry do oblasti Smíchovského nádraží. Následně jsme dané vozidlo skutečně zachytili. Vozidlo zaparkovalo asi 2 metry od vchodových dveří činžovního domu a vyčkávalo. Věděli jsme, že budeme mít jen pár vteřin na to, pořídit fotografii. Tak se skutečně stalo, fotografie se pořídila, ale záběr byl rozmazaný a Radek odjel. Po sdílení rozmazané fotografie ve společné konverzaci všech členů týmu, se ozval jeden z členů s tím, že Radka už někde viděl, že si myslí že to je politik a řekl i jméno. Využili jsme (zdroj č.2) a to vyhledavač Google a stránky PS.cz, kde jsou uvedení všichni poslanci, včetně fotografií. Bohužel ani po dlouhém dívání se, na fotografii z internetu a rozmazanou fotografii ze Smíchovského nádraží jsme nebyli schopni říct, že to je 100% shoda. V tu chvíli mě napadlo využít další užitečnou službu aplikace mapy.cz v mobilním zařízení, která po označení konkrétního domu nabízí možnost náhledu do katastru nemovitostí (zdroj č.3). A opět jsem si mohl říct, "mám tě". V listu vlastníků byl mezi dalšími 3 majiteli právě Radek.

Zde musím říct, že aplikace mapy.cz a mapy.google.cz jsou výborný nástroj. A to nejen pro zobrazení přesné polohy, plánování tras, ale i propracovanému systému "Streetview" pomocí kterého jde provést i obhlídka místa zájmu, aniž by tam člověk musel fyzicky jet a ztrácet drahocenný čas, ale i díky právě zmíněné přidružené funkci vyhledávání v katastru nemovitostí.

3.4.3 Univerzální příklad zjišťování - příklad č.3

V tomto posledním příkladě uvedu několik případů, které jsou unifikované a můžeme je využít jako zdroj informací relativně často. Ke všem informacím tak, jak je budete číst níže, může mít přístup každý a je ve výsledku chybou každého jednotlivce, že sdílí citlivá data relativně s každým, aniž by si uvědomil možnosti zneužití všech těchto informací.

- **Facebook.com** - zdroj aktuálních fotografií oproti starým fotografiím z rejstříku osob, nebo matrik.
- **Facebook.com** - zdroj informací o aktuálních polohách uživatelů. Uživatelé sdílí, že jsou na dovolené, kde přesně jsou a jak dlouho tam budou. Nebo informace o tom, v jaké jsou zrovna restauraci, kavárně atd. Myslím že jako příklad pro zamyšlení nad sdílením své polohy to stačí.
- **Facebook.com** - zdroj informací o tom, že si uživatel pořídil nové auto, motorku, k tomu ještě přiloží fotografii s čitelnou SPZ a riziko je na světě. Nejednou se nám podařilo zjistit nově používané vozidlo (ať už koupené a napsané na někoho jiného, nebo půjčené do dlouhodobého užívání), o kterém neměla z veřejných rejstříků operativa ani ponětí.
- **Facebook.com** - nekonečný zdroj vazeb, chraňte si seznamy vašich přátel, i takové údaje lze zneužít. Opět lze zjistit, s kým osoba žije v jedné domácnosti, s kým chodí do práce, do hospody, do kina, atd.

Pokud v tomto ohledu selže, Facebook, vím že existuje velká šance, že všechny tyto údaje mohu najít na Instagram.com. Na Instagram jsou specialisti hlavně mladší ročníky, takže když potřebuju cokoliv zkusit vyhledat, obracím se na ně a téměř vždy dostanu odpověď ve smyslu shody a informací navíc. Jen díky Instagramu, jsme například ještě předtím, než jsme vůbec začali jednu osobu, které říkejme například Abdul rozpracovávat, měli následující informace. Věděli jsme kam a v jaké dny chodí Abdul pravidelně jíst, kdy a kde se modlí, jaké má oblíbené noční podniky, jaký má nejužší okruh přátel, kam chodí do práce, jaké má koníčky, v jakém se vozí autě atd. Během následujících akcí jsme si všechny informace potvrdili.

Dalším využívaným zdrojem mohou být například veřejné fotografie z koncertů, kulturních akcí, tanečních a jiných klubů, kde je opět v dnešní době moderní činnost focení návštěvníků a následné zveřejňování na svých "fans" stránkách, aniž by se jakýkoliv účastník těchto akcí měl nad smyslem a účelem více zamýšlet. Z pohledu práce při sledování osob a věcí, naskýtá tato činnost důležitý zdroj informací. Příkladem můžou být i schůzky Abdula v jednom oblíbeném nejmenovaném klubu v pozdních nočních až brzkých ranních hodinách, přičemž v tomto klubu se Abdul zná skoro se všemi, včetně majitele, provozních, zaměstnanců a je tudíž obtížné příslušníky tyto osoby zadokumentovat. Ačkoliv s několikadenním zpožděním, ale přeci jen, samotný klub uveřejní fotografie části přítomných osob daného klubu v daný večer a zde již není obtížně poznat příslušníky osoby, které byli zahlédnuty například u jednoho stolu s Abdulem atd.. Ovšem i zde jsme se setkali s poznatkem, že pokud mají zájmové osoby povědomost o práci bezpečnostních složek, jsou často domluveni právě s fotografy na tom, aby je nefotili a nesdíleli na svých stránkách.

4 Dotazníkové šetření na povědomí o možnosti zneužití volně dostupných sdílených dat

V následujícím dotazníkovém šetření jsem se zaměřil na porovnání teoretického rozdílu mezi 2 skupinami lidí. První skupinu tvoří lidé, kteří slouží u některé z bezpečnostních složek státu a tudíž by jsme u nich mohli předpokládat alespoň základní znalosti a povědomosti o bezpečnosti na internetu a o možném využití, či zneužití sdílených dat s lidmi. Naopak druhou skupiny dotazovaných tvoří lidé, kteří nemají s bezpečnostními složkami spojitost ani osobní, ani v rodině. Cílem tedy je zjistit, zda jsou mezi těmito skupinami rozdíly, a pokud ano, tak jaké.

Dotazník a otázky byly konstruovány tak, aby byly jasné, stručné a bylo možno na ně odpovědět rychle, bez dlouhého přemýšlení nad danou otázkou tak, aby co nejméně zkreslovaly výsledky odpovědí hlubší úvahou respondentů. Tím pádem by výsledky měli být autentické, tak jak to respondenti cítili v danou chvíli a nesnažili se odpovědi zkreslovat.

Vzhledem k rozsahu této diplomové práce budu uveřejňovat pouze vybrané druhy otázek a daných odpovědí, které považuji za naprosto názorné. U obou dotazovaných skupin se zaměřím na problematiku sdílení citlivých informací na sociálních sítích, o povědomosti možného zneužití těchto dat a na problematiku hesel. Výsledky dotazníku jako celku budou součástí přílohy.

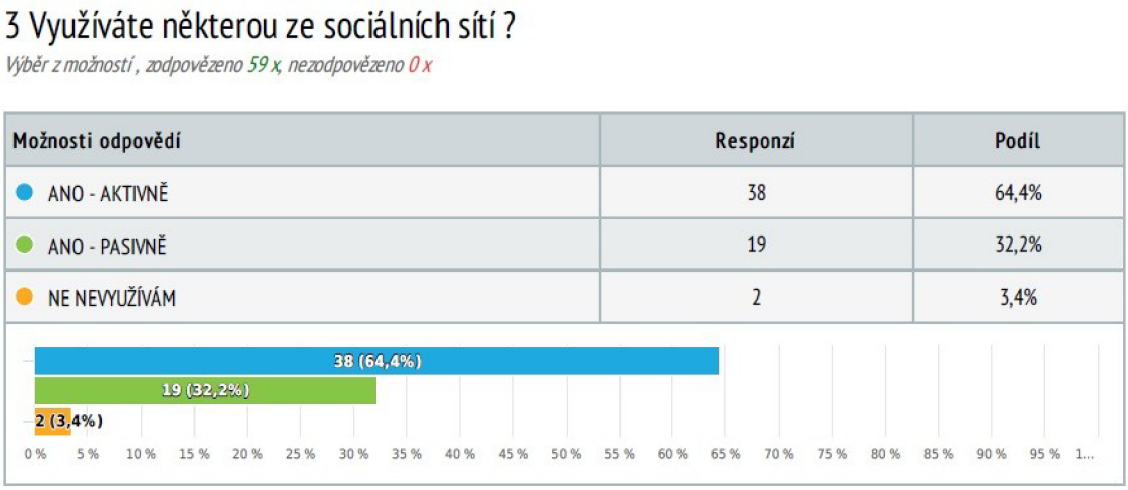
Celkově bylo zadáno 13 otázek a bylo obdrženo 180 odpovědí.

- Sloužíte, nebo pracujete v oblasti bezpečnostních složek ?
- Uveďte prosím Váš věk.
- Využíváte některou ze sociálních sítí ?
- Pokud využíváte viz. výše napište JAKOU.
- Sdíleli jste někdy u fotografií "vaši polohu" ?
- A myslíte si, že lze toto chování (označování) zneužít ?

- Označujete u míst a fotografií sebe, případně Vaše kamarády, nebo známé ?
- A myslíte si, že lze toto chování (označování) zneužít ?
- Jak často si měníte hesla k pro Vás "důležitým" účtům ?
- Používáte "stejné" heslo k více účtům ?
- Máte osobní zkušenost se zneužitím Vašeho volně dostupného sdíleného obsahu ?
- Jaké si myslíte, že máte povědomí o bezpečnosti na internetu ?

4.1 Výsledky šetření u osob, které JSOU součástí oblasti bezpečnostních složek

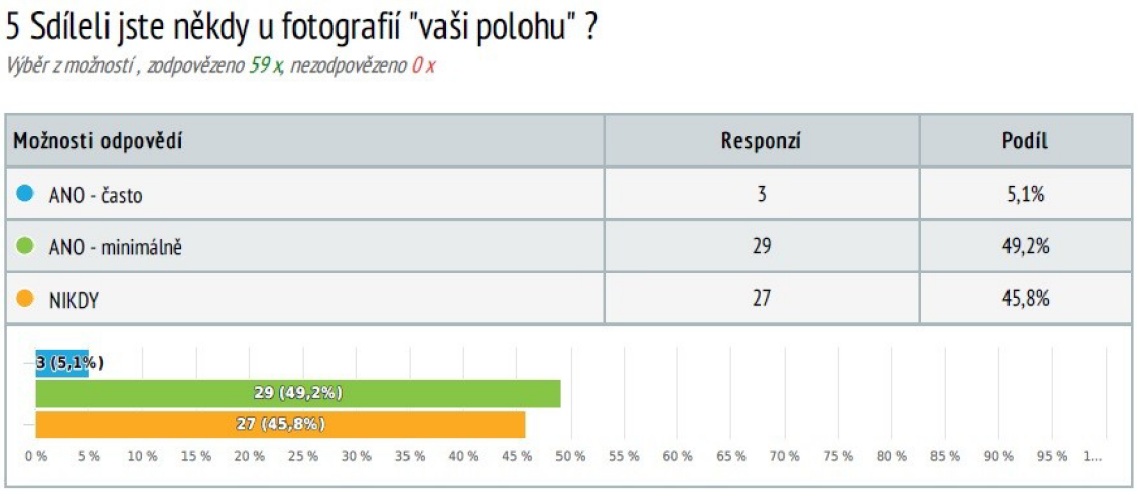
Celkově od této skupiny respondentů přišlo 59 odpovědí od osob přímo sloužících u některé z bezpečnostních složek..



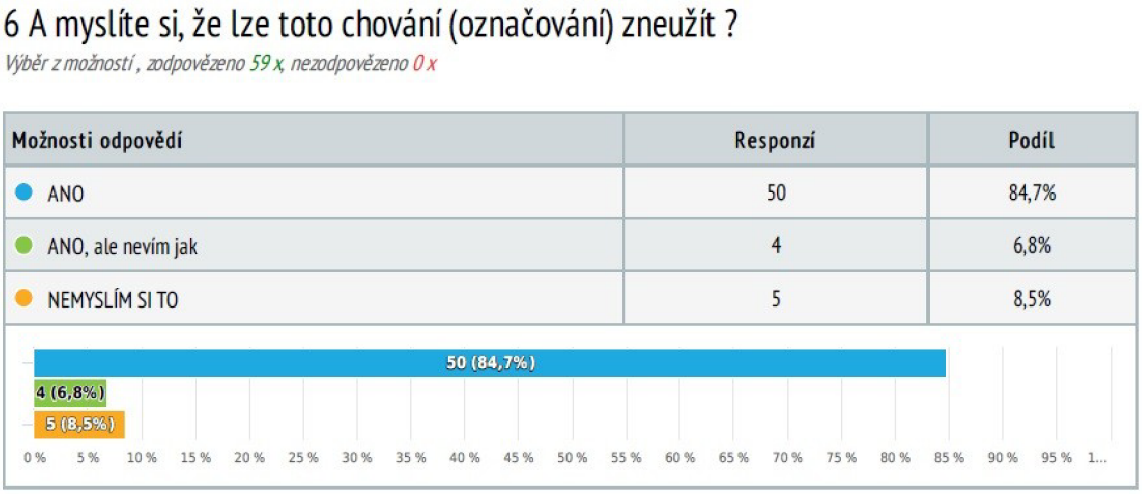
Obrázek 20 - Dotazník využívání sociálních sítí

Z další otázky vyplývá, že nejvyužívanější sociální sítí je Facebook a Instagram. Například Twitter označilo pouze 5 respondentů. Za mě nejdůležitější bod na který bychom se měli zaměřit, je podíl aktivního a pasivního využití těchto sítí. Kdy pod aktivním přístup chápeme přidávání fotek, textu, komentářů atd. , a naopak pasivním využíváním pak jen čtení a sledování těchto

sítí, aniž by daná osoba sdílela jakýkoliv data. U této skupiny respondentů je podíl cca 64% aktivních uživatelů oproti cca 36% pasivních.



Obrázek 21 - Dotazník sdílení polohy



Obrázek 22 - Dotazník povědomí

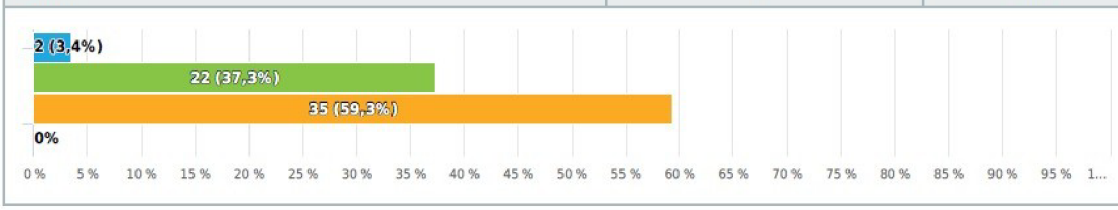
Co se týče problematiky sdílení polohy u vkládaných fotografií na internet, pouze 5% respondentů uvedlo, že často sdílí polohu sdílených fotografií. Zbytek respondentů cca 50% na 50% uvedlo, že ANO - minimálně, nebo NIKDY.

Povědomí o možnosti zneužití takovéhoto chování má celých 92% respondentů.

7 Označujete u míst a fotografií sebe, případně Vaše kamarády, nebo známé ?

Výběr z možností , zodpovězeno 59 x, nezodpovězeno 0 x

Možnosti odpovědí	Responzí	Podíl
ANO - často	2	3,4%
ANO - minimálně	22	37,3%
NIKDY	35	59,3%
Jiná...	0	0,0%

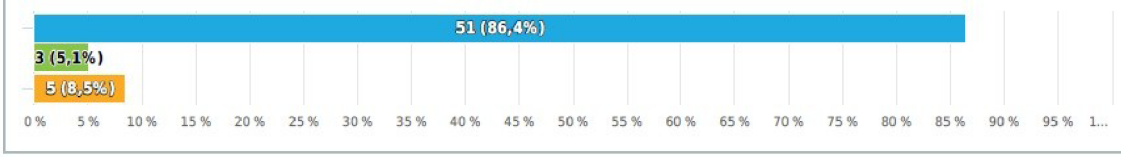


Obrázek 23 - Dotazník sdílení

8 A myslíte si, že lze toto chování (označování) zneužít ?

Výběr z možností , zodpovězeno 59 x, nezodpovězeno 0 x

Možnosti odpovědí	Responzí	Podíl
ANO	51	86,4%
ANO, ale nevím jak	3	5,1%
NEMYSLÍM SI TO	5	8,5%



Obrázek 24 - Dotazník povědomí

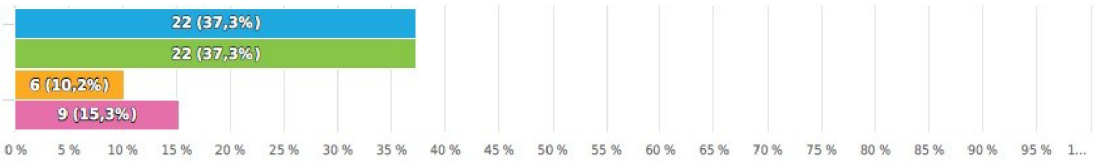
Co se týče problematiky sdílení identit uživatelů a jejich přátel na internet, pouze 3% respondentů uvedlo, že často sdílí identity své, nebo svých přátel. Největší díl respondentů cca 60% uvedlo, že nikdy nesdílí identity a cca 37% uvedlo, že ANO - ale minimálně.

Povědomí o možnosti zneužití takovéhoto chování má celých 92% respondentů.

9 Jak často si měníte hesla k pro Vás "důležitým" účtům ?

Výběr z možností , zodpovězeno 59 x, nezodpovězeno 0 x

Možnosti odpovědí	Responzí	Podíl
NEMĚNÍM	22	37,3%
1X za 1-3 roky	22	37,3%
1X za 3-5 let	6	10,2%
ČASTO	9	15,3%

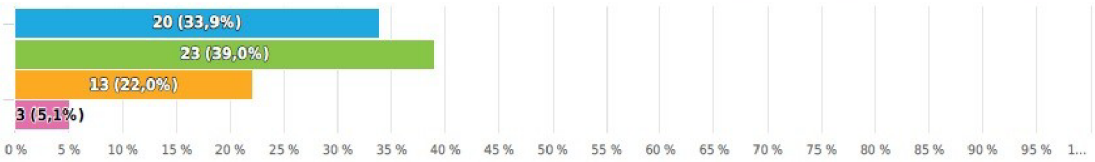


Obrázek 25 - Dotazník změna hesla

10 Používáte "stejné" heslo k více účtům ?

Výběr z možností , zodpovězeno 59 x, nezodpovězeno 0 x

Možnosti odpovědí	Responzí	Podíl
NE - každý účet jiné heslo	20	33,9%
ANO - ale minimálně (2 až 3 účty)	23	39,0%
ANO - většina (4 a více účtů)	13	22,0%
ANO - mám univerzální heslo na VŠE	3	5,1%

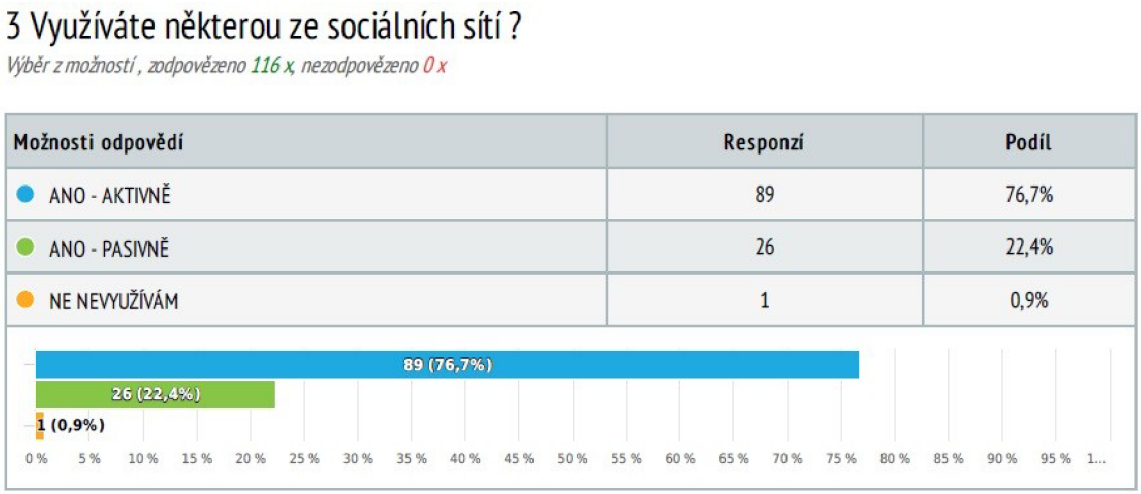


Obrázek 26 - Dotazník stejné heslo

Co se týče problematiky vytváření slabých a opakujících se hesel, cca 37% respondentů uvedlo, že si NIKDY nemění již jednou vytvořené heslo ke svým hlavních účtům. Stejný počet respondentů naopak uvedl, že si heslo mění minimálně 1x za rok. A naštěstí jen 5% respondentů uvedlo, že používají jedno univerzální heslo ke všem svým účtům.

4.2 Výsledky šetření u skupiny osob, které NEJSOU součástí oblasti bezpečnostních složek a jsou z civilní sféry

Celkově od této skupiny respondentů přišlo 116 odpovědí od osob z civilní sféry.



Obrázek 27 - Dotazník využívání sociálních sítí

Z odpovědí od skupiny civilní sféry vyplývá, že nejvyužívanější sociální sítí je stále Facebook a Instagram. Objevují se zde ale četně další sociální sítě jako, TikTok, Snapchat, YouTube, Reddit, Twitter a další. Za mě nejdůležitější bod na který bychom se měli zaměřit je podíl aktivního a pasivního využití těchto sítí. U této skupiny respondentů je podíl cca 80% aktivních uživatelů oproti cca 20% pasivních.

5 Sdíleli jste někdy u fotografií "vaši polohu" ?

Výběr z možností , zodpovězeno 116 x, nezodpovězeno 0 x

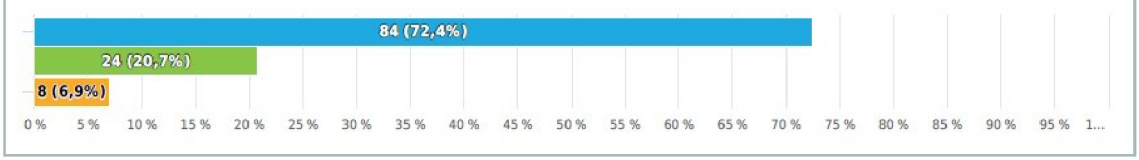
Možnosti odpovědí	Responzí	Podíl
ANO - často	29	25,0%
ANO - minimálně	56	48,3%
NIKDY	31	26,7%

Obrázek 28 - Dotazník sdílení polohy

6 A myslíte si, že lze toto chování (označování) zneužít ?

Výběr z možností , zodpovězeno 116 x, nezodpovězeno 0 x

Možnosti odpovědí	Responzí	Podíl
ANO	84	72,4%
ANO, ale nevím jak	24	20,7%
NEMYSLÍM SI TO	8	6,9%



Obrázek 29 - Dotazník povědomí

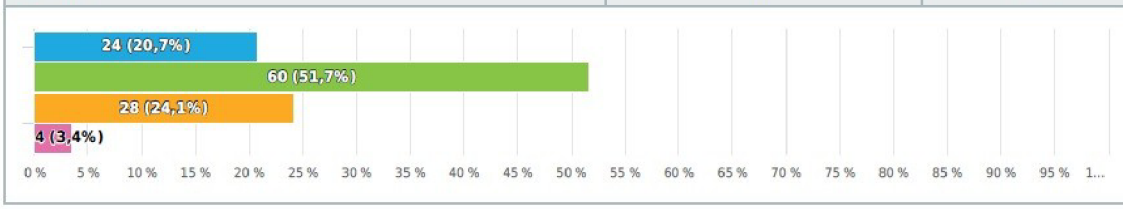
Co se týče problematiky sdílení polohy u vkládaných fotografií na internet, 29 respondentů uvedlo, že často sdílí polohu sdílených fotografií. Zbytek respondentů cca 50% uvedlo, že ANO - minimálně a pouze cca 26% uvedlo, že NIKDY.

Povědomí o možnosti zneužití takovéhoto chování má celých 93% respondentů, bohužel z toho cca 21% respondentů netuší jakým způsobem.

7 Označujete u míst a fotografií sebe, případně Vaše kamarády, nebo známé ?

Výběr z možností , zodpovězeno 116 x, nezodpovězeno 0 x

Možnosti odpovědí	Responzí	Podíl
ANO - často	24	20,7%
ANO - minimálně	60	51,7%
NIKDY	28	24,1%
Jiná...	4	3,4%

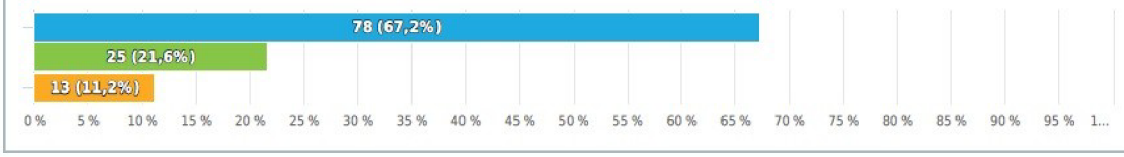


Obrázek 30 - Dotazník sdílení

8 A myslíte si, že lze toto chování (označování) zneužít ?

Výběr z možností , zodpovězeno 116 x, nezodpovězeno 0 x

Možnosti odpovědí	Responzí	Podíl
ANO	78	67,2%
ANO, ale nevím jak	25	21,6%
NEMYSLÍM SI TO	13	11,2%



Obrázek 31 - Dotazník povědomí

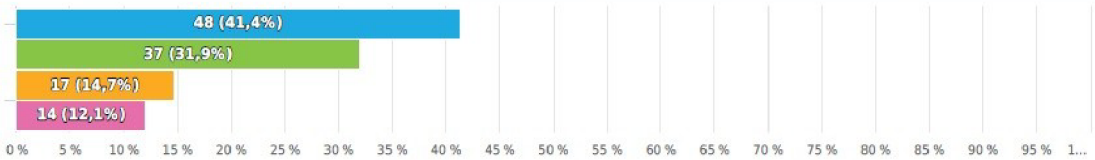
Co se týče problematiky sdílení identit uživatelů a jejich přátel na internet, pouze cca 27% respondentů uvedlo, že nesdílí identity své, nebo svých přátel. Největší díl respondentů cca 52% uvedlo, že ANO - minimálně a cca 21% uvedlo, že ANO - často.

Povědomí o možnosti zneužití takovéhoto chování má celých 89% respondentů, bohužel i zde ca 22% neví jakým způsobem lze toto chování zneužít a dokonce cca 11% respondentů si myslí, že toto chování zneužít nelze.

9 Jak často si měníte hesla k pro Vás "důležitým" účtům ?

Výběr z možností , zodpovězeno 116 x, nezodpovězeno 0 x

Možnosti odpovědí	Responzí	Podíl
NEMĚNÍM	48	41,4%
1X za 1-3 roky	37	31,9%
1X za 3-5 let	17	14,7%
ČASTO	14	12,1%

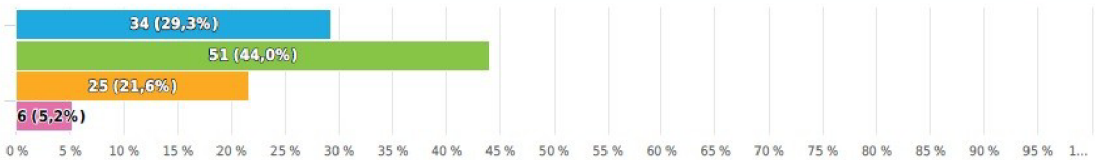


Obrázek 32 - Dotazník změna hesla

10 Používáte "stejné" heslo k více účtům ?

Výběr z možností , zodpovězeno 116 x, nezodpovězeno 0 x

Možnosti odpovědí	Responzí	Podíl
NE - každý účet jiné heslo	34	29,3%
ANO - ale minimálně (2 až 3 účty)	51	44,0%
ANO - většina (4 a více účtů)	25	21,6%
ANO - mám univerzální heslo na VŠE	6	5,2%



Obrázek 33 - Dotazník stejné heslo

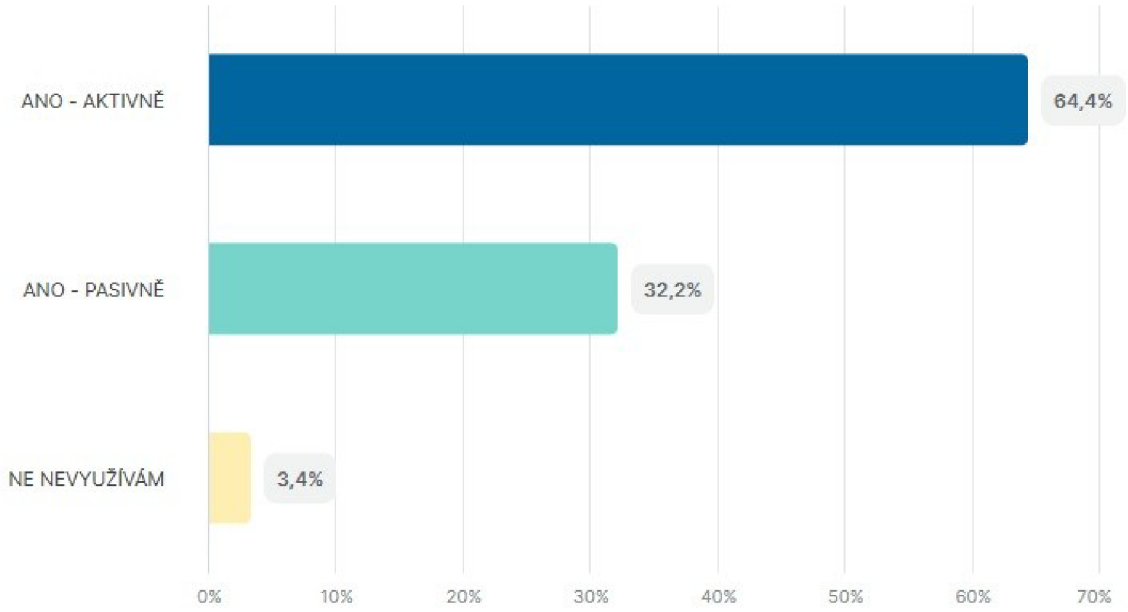
Co se týče problematiky vytváření slabých a opakujících se hesel, cca 42%, což je nejvíce zastoupená část respondentů uvedlo, že si NIKDY nemění již jednou vytvořené heslo ke svým hlavních účtům. Cca 32% respondentů naopak uvedlo, že si heslo mění minimálně 1x za rok. A naštěstí jen cca 5% respondentů uvedlo, že používají jedno univerzální heslo ke všem svým účtům.

4.3 Porovnání dotazníkového šetření mezi osobami z civilní a bezpečnostní sféry

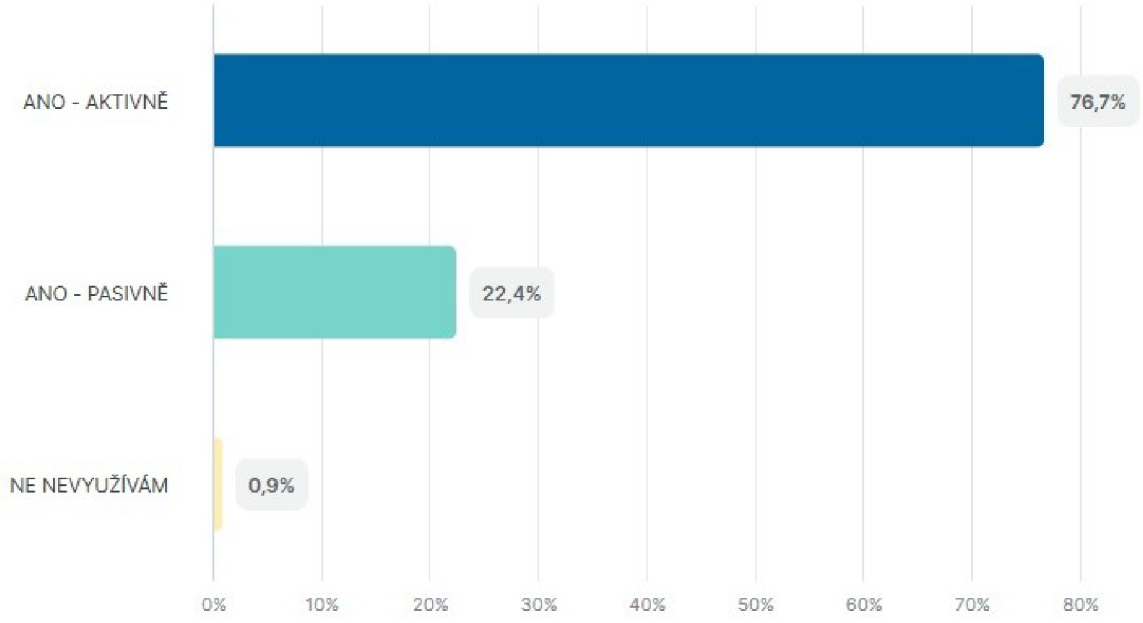
Hlavním cílem tohoto dotazníkového šetření bylo zmapovat rozdíly v povědomí o bezpečnosti sdílených dat na internetu, respektive sociálních sítích. Jako objektivní výsledky porovnáme zkoumané otázky , které jsem uvedl výše v každé z kapitol věnované výsledkům obou zkoumaných skupin.

4.3.1 Rozdíly v aktivním a pasivním využíváním sociálních sítí

Základní rozdíly, které můžeme vyčíst z grafů viz níže jsou následující. Z vyplněných dotazníků od 180 respondentů bylo zjištěno, že v současné době jsou sociální sítě fenomén. Tím pádem v tomto ohledu neshledávám rozdíl mezi tím, zda je osoba součástí té či oné skupiny, či jakékoliv jiné sociální skupiny. Sociální sítě skutečně využívá přes 97% uživatelů internetu. Možná drobný rozdíl v hodnotě cca 10% respondentů v rámci zkoumaných skupin je v počtu aktivních, oproti pasivních uživatelů, kde v civilní sféře dominuje v cca 80% aktivní využívání.



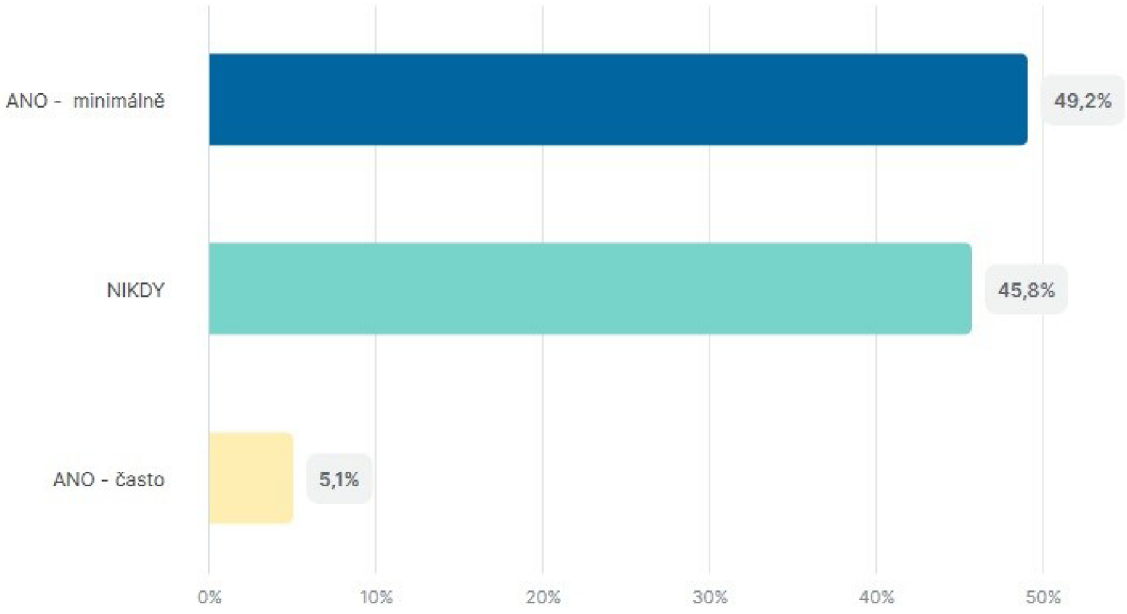
Obrázek 34 - Bezpečnostní složky, využívání sociálních sítí



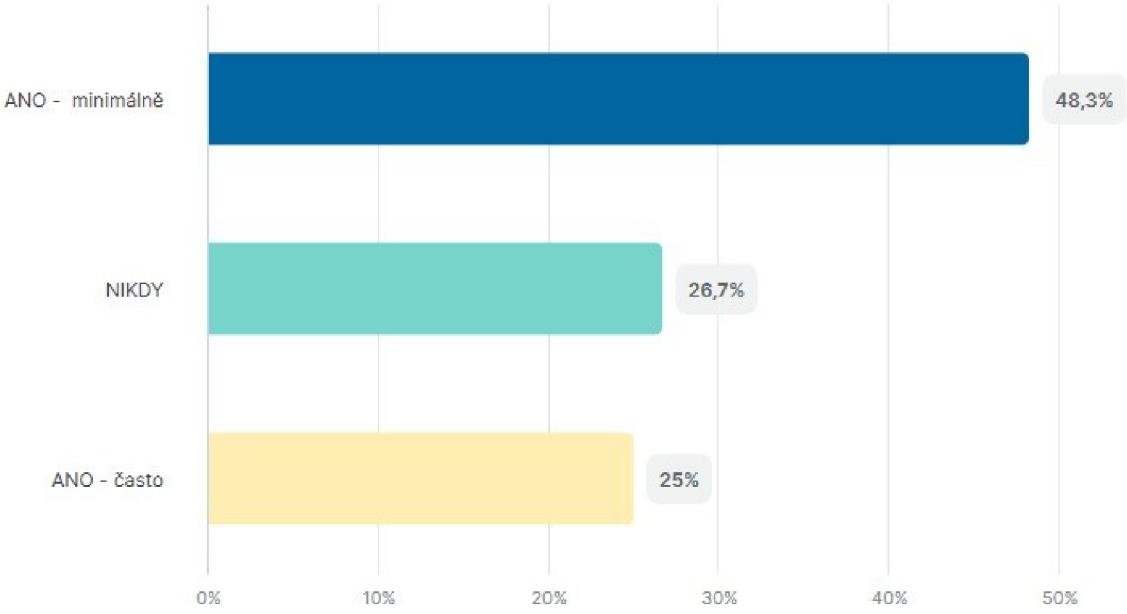
Obrázek 35 - Civilní sféra, využívání sociálních sítí

4.3.2 Rozdíly ve sdílení poloh u uživatelem sdílených fotografií na sociálních sítí.

Co se týká problematiky u sdílení údajů o poloze u uživatelem vkládaných fotografií na sociální sítě, ukazují se první rozdílné vnímání toho chování u obou sledovaných skupin. Téměř shodně, cca 49% respondentů uvedlo odpověď ANO - minimálně. Avšak ten zásadní rozdíl uvádějí respondenti v odpovědi NIKDY. U skupiny osob z bezpečnostních složek se odpověď NIKDY téměř shoduje s ANO - minimálně a to v počtu cca 46% a pouze cca 5% respondentů sdílí svoji polohu často. Oproti tomu respondenti z civilní sféry odpověděli NIKDY jen z cca 26% a dokonce 25% respondentů uvedlo, že polohu u sdílených fotografií zveřejňují často. Toto je zásadní rozdíl v pohledu vnímání možného nebezpečí a uvědomění si rizika mezi těmito skupinami. Nárůst 21% v častém sdílení informací o poloze u osob z civilní sféry je oproti skupině bezpečnostních složek markatní.



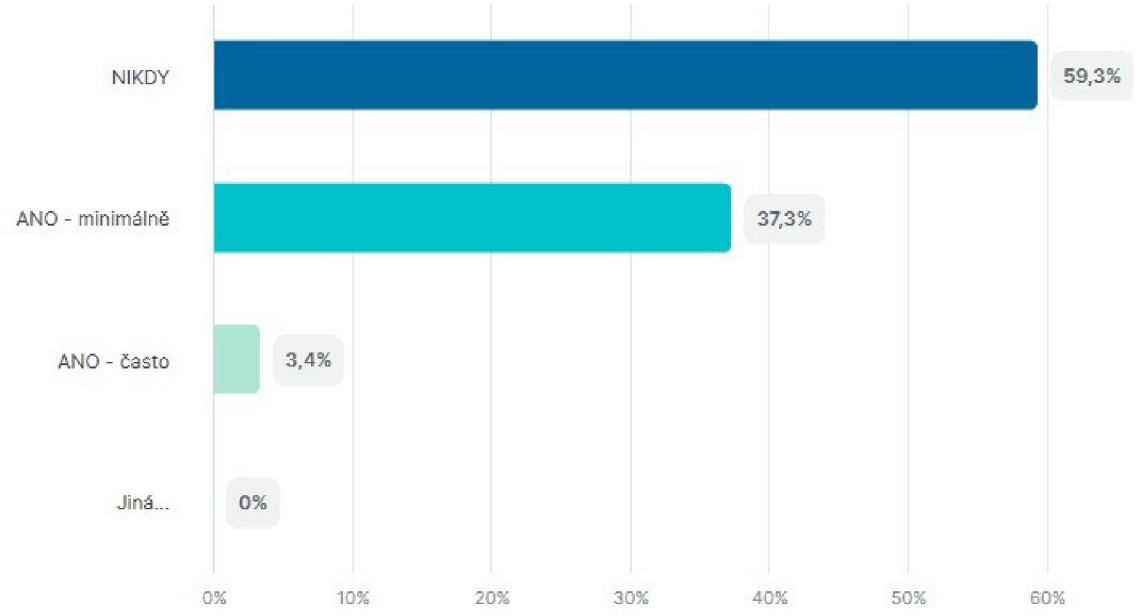
Obrázek 36 - Bezpečnostní složky, sdílení údajů o poloze



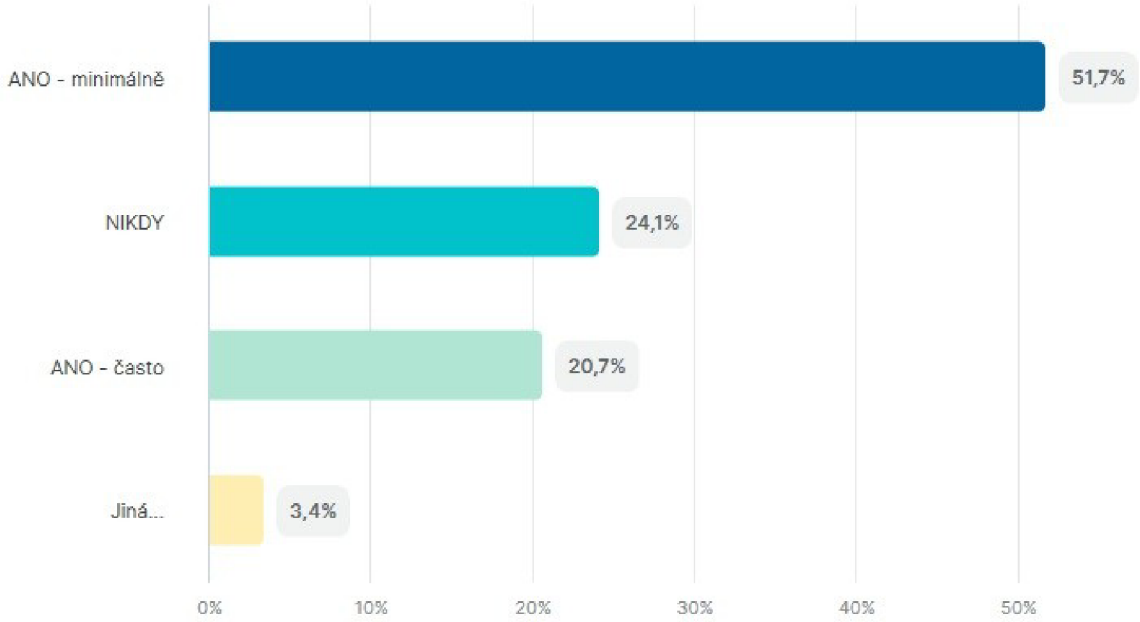
Obrázek 37 - Civilní sféra, sdílení údajů o poloze

4.3.3 Rozdíly ve sdílení identit uživatele a jeho přátel na sociálních sítí.

Co se týká problematiky u sdílení identity uživatele, nebo jeho přátel, známých rodiny u vkládaných příspěvků, nebo fotografií na sociální sítě. I v tomto případě se ukazuje rozdílné vnímání tohoto chování u obou sledovaných skupin. U skupiny osob z bezpečnostních složek dominuje na tuto problematiku odpověď NIKDY, a to u cca 60% respondentů. U cca 37% respondentů byla odpověď ANO- minimálně. Pouze zanedbatelné cca 3% respondentů uvedlo, že sdílí často identity, ať už své, či přátel. Oproti tomu se markantně otočili odpovědi u sledované skupiny osob z civilní sféry. 52% respondentů uvedlo odpověď ANO - minimálně, což je nárůst cca 15% oproti druhé skupině, ale oproti zanedbatelnému počtu 3% respondentů z bezpečnostních složek uvedlo cca 21% osob z civilní sféry, že často sdílí identitu svou, či svých přátel. Druhý zásadní rozdíl je, že ve skupině bezpečnostních složek jsme měli odpověď NIKDY zastoupenou v cca 60% odpovědích, zatímco u civilní sféry to je pouze cca 24%. To je rozdíl 36% !



Obrázek 38 - Bezpečnostní složky, sdílení identit



Obrázek 39 - Civilní sféra, sdílení identit

4.4 Shrnutí dotazníkového šetření

Před samotným započetím dotazníkového šetření jsem si stanovil hypotézu, že přeci musí existovat markantní rozdíly ve vnímání nebezpečí na internetu obecně ve skupině lidí, kteří se každý den setkávají s nejrůznějšími zločiny, přečiny a jinými delikty a skupinami lidí absolutně nezaujatými, neznalými, jinou osobou nepoškozenými a celkově lidmi kteří nepřicházejí téměř denně do kontaktu s jakýmikoliv riziky. Vím, že někteří jsme až pracovně posedlí a hledáme rizika i tam, kde nejsou, ale internet a sociální sítě, tím tak jak jsou v dnešní době rozšířené zkrátka představují riziko. Tento dotazník jen dokazuje, že se člověk internetu a sociálním sítím a médiím nevyhne a opravdu více než 97% respondentů uvedlo, že sociální sítě nějakým způsobem využívají.

Jak jsem si ve své hypotéze stanovil, že rozdíly ve vnímání internetu a sociálních sítí může být rozdílné, tak se tak i ukázalo. Zanedbatelné rozdíly co se týče využívání sociálních sítí jsou v porovnávání skrze parametry věku, příslušnosti do sociální, či jiné skupiny. Dokonce povědomost o teoretickém nebezpečí na internetu je u obou sledovaných skupin téměř shodná. Jako zásadní výstup je ale fakt, že lidé ze skupiny bezpečnostních složek se snaží lépe chránit osobní data, nesdílejí své identity, fotografie, statusy a fotografie tak často jako osoby z civilního prostředí.

Z dotazníkového šetření vyplívá také informace, že značná část osob ze skupiny civilní sféry má sice nějaké povědomí o plynoucích rizicích ve sdílení četných údajů. Nicméně si nedokážou představit jakým způsobem by mohli tyto údaje být zneužity, nebo jinak využity. Největší neznalost této problematiky jsem zaznamenal obecně u skupiny osob ve věkovém rozmezí 15 - 20 let. Zde si troufám říct, že stále chybí vhodně zvolená forma osvěty. A to taková forma, která by byla pro tuto skupinu zajímavá a hlavně příkladná. S důrazem na zveřejňování kauz a příkladů jednotlivých zneužití právě těchto údajů. Protože jen správně zacílená osvěta na internetovou bezpečnost a hygienu již třeba na základních školách by mohla prospět v rozšíření povědomí alespoň o části rizik, které plynou po přečtení této diplomové práce pro každého z nás.

Rady na závěr dotazníkové šetření:

- Dávejte si pozor na to, co zveřejňujete,
- nesdílejte fotografie svých dětí,
- dbejte na své soukromí,
- mějte pod kontrolou své účty,
- nepřidávejte si osoby, které neznáte,
- nevěřte všemu, co uvidíte na sociálních sítích,
- braňte se kyberšikaně,
- pokud to lze, hlídejte co sledují Vaše děti v online světě,
- vzdělávejte se v oblasti bezpečnosti na internetu.

5 Závěr

Závěrem této diplomové práce bych chtěl především zdůraznit důležitost tohoto tématu. Otevřené zdroje informací jsou téměř nekonečný prostor a zdroj dat, které lze využít / zneužít v dnešní době téměř na cokoliv. Sledování osob, jejich digitálních identit, nebo věcí nevyjímaje. Záleží na každém člověku jak nakládá s informacemi o sobě, svých blízkých a přátelích, ale i o sdílení svého volného času, svých zájmu, majetků a práci s nimi. Nedávno mě v Praze v místě kde je nejvyšší povolená rychlost stanovena na 50km/ předjelo vozidlo s unikátní SPZ na přání rychlostí převyšující 100km/h. Ze zvědavosti jsem zmíněnou SPZ zadal do vyhledavače Google. Výsledek ? Během pár minut jsem ze svého mobilního telefonu zjistil bez použití specializovaných nástrojů díky Instagramu, Facebooku, a dalších zájmových stránek jméno řidiče, jeho fotografii v uvedeném vozidle + další jeho používaná vozidla. Na profilu Facebooku z jedné fotografie a uvedených "tagů" skutečné zaměstnání, z další fotografie před domem, kde bylo vidět č.p. domu a označení polohy této fotografie a následné kontroly katastru nemovitostí v aplikaci mapy.cz i místo jeho bydliště. Následně ze zájmových sdílených stránek touto osobou i to, ve který den na kterém místě se bude účastnit toho, či onoho setkání. Práce na 5 minut ve veřejných všem

dostupných zdrojích a o dané osobě jsem měl informace, se kterými bych dotyčného mohl i sledovat, případně jiným způsobem naložit s těmito informacemi. Závěr je takový, přestože existuje celá řada absolutně vyspělých analytických nástrojů, nejrůznějších hackovacích kódů a jiných nástrojů, bohužel díky neopatrnosti, naivnosti a troufám si říci i absolutnímu nezájmu a ochranu svých dat, zpřístupňuje mnoho lidí nepřeberné množství dat ostatním "zadarmo" bez jediného důvodu.

Cílem této práce bylo poukázat právě na tuto problematiku otevřených zdrojů a přiblížit základní metody, nástroje a vůbec smysl využití informací, které lze v tomto prostoru získat, protože jak technologie každým dnem narůstají, vyvstává potřeba rychlého a specifického shromažďování informací a zvyšuje se potřeba OSINT. V současnosti se OSINT stal základní potřebou každé organizace, ať už je to organizace soukromá, nebo státní. Pomocí OSINT jsme schopni získat důležité informace během několika málo okamžiků v závislosti na metodě, prostředcích a hlavně tím, jak je požadovaná informace "chráněna".

Úplným závěrem lze říci, že je těžké zůstat v dnešním "moderním a sdíleném" světě v soukromí a mít pod kontrolou, jaké informace a kde všude o nás kolují. I za předpokladu, že nemůžete ovládat všechny informace, které o nás v digitálním světě kolují, je důležité si tento fakt alespoň uvědomovat. Je samozřejmé, že v digitální době hrají informace klíčovou roli, takže kdo je umí najít, bude vždy o krok napřed. K tomu slouží právě tato diplomová práce, která ukazuje a dává příklad, jak OSINT pomáhá řešit širokou škálu problematik: od marketingu přes vyšetřování a vyhledávání informací až po kybernetickou bezpečnost. Vše co jsem v této práci popsal, je ovšem jen názorným slovem popsáno jako "špička ledovce". Většina technik které jsou v této práci popsány jsou jednoduché, ale přesto účinné. A proto mohou i tyto jednoduché techniky při použití se zlým úmyslem způsobit škodu, nebo vyvolat nějaké riziko, proto pokud je budete zkoušet, používejte je vždy s rozumem.

Seznam použité literatury

Monografie

1. METĚNKO, Jozef. *Sledovanie I.* Bratislava: Akadémia PZ v Bratislave, Katedra kriminálnej polície, 2002.
   ISBN: 80-8054-219-8.
2. METĚNKO, Jozef. *Sledovanie v bezpečnostných činnostiach.* Bratislava: Akadémia PZ v Bratislave, Katedra kriminálnej polície, 2002.
   ISBN: 80-8054-237-6.
3. AKHBAR, Babak, BAYERL, Saskia, SAMPSON, Fraser (Eds.). Open Source Intelligence Investigation. From Strategy to Implementation. Springer, 2016.
   ISBN: 978-3-319-47671-1.
4. BAZZELL, Michael. Open Source Intelligence Techniques. Resources for Searching and Analyzing Online Information. 2018.
   ISBN-13: 978-1984201577.
5. JENKINS, Peter. *Surveillance tradecraft: the professional's guide to surveillance training.* 2nd ed. Harrogate, U.K: Intel Publishing, 2010.
   ISBN: 9780953537822.
6. Pokorný, Ladislav. 2012. Zpravodajské služby
   ISBN: 978-80-87284-21-6 - Auditorium - Česká republika
7. Michálek, L., Pokorný, L., Stieranka, J., Marko, M. 2013. Zpravodajství a zpravodajské služby.
   ISBN: 978-80-7380-428-2 - Aleš Čeněk - Česká republika

Legislativní prameny

1. ČESKO, 1994b. Zákon č. 154 ze dne 7. července 1994 o bezpečnostní informační službě. In: *Sbírka zákonů České republiky*. Částka 49. Dostupné také z: https://www.zakonyprolidi.cz/cs/1994-154
2. ČESKO, 1961. Zákon č. 141 ze dne 9. prosince 1961 o trestním řízení soudním (trestní řád). In: *Sbírka zákonů České republiky*. Částka 66. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141

3. ČESKO, 2000. Zákon č. 101 ze dne 25. dubna 2000 o ochraně osobních údajů a o změně některých zákonů. In: *Sbírka zákonů České republiky*. Částka 32. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-101

Online zdroje

1. Petro CHERKASETS, 2019. OSINT how to find information on anyone. http://medium.com [online] rešerše
2. Pompeu CASANOVAS, Juan ARRAIZA, Felipe MELERO, Jorge GONZÁLEZ-CONEJERO, Gila MOLCHO, Montse CUADROS. Fighting Organized Crime Through Open Source Intelligence: Regulatory Strategies of the CAPER Project [online]. [8. 3. 2022]. Dostupné z: https://core.ac.uk/download/pdf/78532664.pdf
3. BIELSKA, Aleksandra. Open Source Intelliegence Tools and Resources Handbook. I-INTELLIGENCE, 2018. https://www.i-intelligence.eu/wp-content/uploads/2018/06/OSINT_Handbook_June-2018_Final.pdf
4. Recorded future TEAM, 2019, What is open source, and it work it https://recordedfuture.com [online] rešerše
5. Tomas KADAR, 2020, The best OSINT software and tools https://seon.io [online] rešerše
6. Exploit database, 2022, Google hacking database exploit-db.com [online] rešerše
7. Fraser SAMPSON, 2016, Inttelligent evidence: Using OSINT http://researchgate.net [online] rešerše
8. NETBOX, 2019, Rizika sociálních sítí https://netbox.cz [online] rešerše
9. Petr Krčmář, 2018, Shodan.io: Užitečný vyhledavač internetových slabin. Root.cz [online] 2018 [cit. 1.3.2022]. Dostupné z : https://root.cz/clanky/shodan-io-uzitecny-vyhledavac-internetovych-slabin

10. ČT24, 2012, Hacker napadl stránky České televize. [online]. 17. 03. 2012 [cit. 1.3.2022]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/1184279-hacker-napadl-stranky-ceske-televize
11. BIS, 2022, Jak pracujeme. [online]. [cit. 1.3.2022]. Dostupné z: http://www.bis.cz/jakpracujeme.html
12. NATO, 2001, NATO Open Source Intelligence Handbook. [online] 2001 [cit. 18.2.2022]. Dostupné z : https://fdocuments.in/document/nato-osint-handbook-v12-jan-2002pdf.html
13. Ler.studio, 2021, Statistiky využívání sociálních sítí. [online]. [cit. 8.3.2022]. Dostupné z : https://lerstudio.cz/statistiky-vyuziti-socialnich-siti-kolik-lidi-pouziva-socialni-media-v-roce-2021

Seznam obrázků

Seznam příloh

Příloha č.1 - survey_report_skupina_bezpecnostni_slozky.pdf

Příloha č.2 - survey_report_skupina_civilní_sfera.pdf

Přílohy

Příloha č.1 - survey_report_skupina_bezpecnostni_slozky.pdf

Příloha č.2 - survey_report_skupina_civilní_sfera.pdf