Soukromí a osobní data in internetu

Petr Maronek

27.10.2022

Vysoká škola finanční a správní
Fakulta právních a správních studií
Projektování Informačních Systémů 1
Zimní semestr 2022
Vedoucí práce: **Ing. Václav Řezníček, Ph.D.**

Abstrakt

Návrh zlepšení procesu pro správu Microsoft Office 365, která již vykazuje známky stárnutí technologie. to může vézt až ke výrazné ztrátě firemních finančních prostředků.

Klíčová slova

Office365, Microsoft, proces, automatizace, korporace, cloud

Úvod

Užívání moderních technologií není v současné době žádnou výsadou. Internet byl přiveden do České republiky před téměř 30 lety a výpočetní technika doznala za tu dobu neuvěřitelného pokroku. Pokud odhlédneme od problematiky politických režimů, které aktivně omezují nebo znemožňují svobodný přístup k informacím, která není tématem této práce, má dnes člověk bezprecedentní možnost vyhledat svobodně přístupné informace z celého světa.

S rozvojem chytrých mobilních telefonů, které mají dnes již výkon plnohodnotných stolních počítačů, naše prezence v on-line světě vzrostla takřka na celodenní trvání. V mnoha instancích si již ani neuvědomujeme, že konkrétní funkcionalita potřebuje pro své funkce on-line připojení a naopak, že některé aplikace nepotřebují být připojeny vůbec. A protože má dnes chytrý telefon bezmála každý, data z jeho funkcí [chytrého telefonu] začaly zpracovávat velké nadnárodní korporace v rámci zkvalitňování nabízených služeb. Pro uživatele tato praktika explicitně nic neznamená, ale implicitně tím uživatel dává těmto firmám souhlas se zpracováním jeho osobních dat. Proto, abychom ale mohli studovat problematiku osobních údajů v kybernetickém prostoru, si nejdříve musíme definovat, co vlastně osobní údaje jsou. Podle směrnice zákona o ochraně osobních údajů jsou to jakékoli informace o identifikovaném nebo identifikovatelném subjektu údajů. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby (GDPR, 2015).

Dále si také musíme definovat kybernetický prostor. Jedná se o amorfní, údajně "virtuální"svět vytvořený propojením mezi počítači, zařízeními připojenými k internetu, servery, routery a dalšími součástmi internetové infrastruktury (Bussel, 2013). Když tedy nahlížíme na osobní údaje jako na předmět našeho zkoumání, musíme si uvědomit, že se jedná o velice citlivá data, se kterými se nesmí nakládat lehkovážně. Předchozí věta může působit očividně, jsou ale v historii případy, kdy únik osobních dat proběhl v tak velkém měřítku, že na tuto situaci museli reagovat i správní úřady. V dnešním propojeném světě jsou osobní údaje součástí mnoha systémů a ve většině případů nám, uživatelům, usnadňují život natolik, že jsme ochotni je sdílet s naším blízkým, ale i vzdáleným okolím.

Cílem této práce bude pro průměrného uživatele elektronických služeb navrhnout sadu doporučení, která zajistí co nejmenší únik citlivých osobních údajů společně se zachováním si pohodlí při užívání zmíněných služeb. Průměrným uživatelem zde chápeme uživatele, který nemá hlubší technické znalosti ohledně informačních technologiích a využívá je pouze ke konzumaci obsahu a služeb.

Důvěrná data a internet

Důvěrná data, nebo-li osobní informace, jsme si již definovali v předchozí kapitole. Tato definice je však vysoce objektivní a každý uživatel bude chápat různé oblasti svých osobních informací jinak a s jinou váhou. Abych práci udržel v uchopitelném měřítku, v budoucí kapitole se budu zajímat o modelování hrozeb, který je už součástí řešení. Nyní se budu zabývat nástroji, které jsou běžně užívány ke sběru nejen osobních dat z našich zařízeních. Postupně zde proberu jak osobní počítače (Mac, Windows, GNU/Linux), tak mobilní zařízení (iOS, Android).

Apple v posledních letech své produkty označuje za ochránce osobního soukromí. Veškeré výpočty a funkce, které aplikace od společnosti Apple vykonávají, se odehrávají a zůstávají na uživatelském zařízení. Pokud je potřeba kontaktovat vzdálený server pro nějaká data (jako například pro zjištění stavu dopravy pro navigaci), aplikace data pouze přijme a neodešle žádná soukromá data, která by vedla k identifikování koncového uživatele. Navíc Apple přidal do AppStore (služba pro získávání aplikací) tzv. Privacy Labels nebo-li štítky pro soukromí. Tyto štítky uživateli signalizují, jaká data vývojář aplikace získává a jakým způsobem. Všechny tyto informace jsou stejně relevantní pro mobilní operační systém od společnosti Apple iOS.

V Apple ekosystému je více služeb, která chrání data uživatele, nicméně tento systém opatření padá ve chvíli, kdy si uživatel do svého zařízení nainstaluje aplikaci, která má za primární účel právě sběr dat. V

odborné komunitě, která se soukromím na internetu zabývá, existuje jedno pravidlo, které platí takřka v každém případě: Pokud je něco zdarma, vy jste produkt [2]. Toto pravidlo neplatí pouze pro Apple, ale pro veškeré dění v kyberprostoru.

Operační systém Windows a obecně produkty od společnosti Microsoft si z hlediska soukromí stojí někde uprostřed pomyslné škály. Windows 10 byl v době svého uvedení na trh distribuován všem uživatelům, kteří měli licenci na Windows 7, zdarma, pokud splňovali základní hardwarové požadavky na systém. Pravidlo, které je uvedené výše zde do jisté míry platí. Hned po uvedení Windows 10 na trh se začaly vyskytovat články z odborné komunity kybernetického bezpečí o možném úniku dat, které systém automaticky posílá na servery společnosti Microsoft. Odesílaná data například obsahovala hlasové příkazy virtuálnímu asistentovi Cortana, text psaný v kancelářském balíčku Microsoft Office nebo informace o poloze. Dále data o vlastním počítači, jako stav baterie, rozlišení obrazovky nebo seznam instalovaného software [1]. Ačkoli se na první pohled zdá, že uživatelé systému Windows jsou sledováni na každém kroku, většina funkcí, která se o kolekci těchto dat stará, může být vypnuta v nastavení systému.

Systém GNU/Linux a všechny operační systémy, které jsou postaveny na UNIX, jsou ve většině případů kompletně zabezpečené proti úniku soukromých dat uživatele. Opět zde platí, že pokud uživatel nainstaluje do svého systému aplikaci, která nectí nastavení nebo má přímo v podmínkách používání sběr dat, dochází k úniku těchto dat a nastalá premisa přestává platit. I ve světě Linux ale narazíme na okamžiky, které pověst soukromého a bezpečného operačního systému negativně ovlivňují. Operační systém Ubuntu od společnosti Canonical v roce 2015 přidal aplikaci Amazon pro rychlé on-line nákupy. Amazon je znám pro své praktiky v oblasti kolekce dat a tento krok od Canonical byl brán velice negativně. V současné době aplikace Amazon již v Ubuntu obsažena není, nicméně vývojářská firma Canonical úzce spolupracuje se společností Microsoft což opět vyvolává otázky, zda je systém Ubuntu bezpečný a privátní. Ostatní distribuce operačního systému Linux, jako například Arch Linux, CentOS nebo BSD systémy touto problematikou netrpí. Naopak jsou brané jako nejbezpečnější a nejvíce privátně orientované operační systémy.

Mobilní operační systém Android má otevřený zdrojový kód a každý si může tento kód prostudovat. Sám o sobě je tento systém velice bezpečný a soukromý. Společnost Google, která Android aktivně vyvíjí však do své implementace přidává nadstavbu svého softwaru, který na jedné straně usnadňuje uživateli práci s ním, na straně druhé nicméně sbírá takřka všechna data, která mobilní zařízení generuje. Není to jen poloha a data o užívání zařízení, ale také data ze všech senzorů, data o hovorech a audio data z mikrofonu (Sumagaysay, 2018). Konkrétně data z mikrofonu jsou velice citlivá. Protože jsou všechny moderní telefony se systémem Android vybaveny virtuálním asistentem, mikrofon je stále zapnutý a čeká, až obdrží klíčová slova pro aktivaci právě tohoto asistenta (Johnson, 2021). Audio data jsou poté sbírána a používána v rámci reklamy. Zde jde například o situaci, kdy telefon rozpozná mluvené slovo, vybere z něj klíčová slova a poté vše odešle na server. Zde se tato data nadále zpracovávají do algoritmu pro nabízení reklamy. Google je za tyto praktiky penalizován státními institucemi, nicméně pokaždé upraví své obchodní podmínky tak, aby bylo vše v souladu se zákonem.

Nebezpečí či nikoliv?

Na základě výše zmíněného, do jaké míry jsou ohroženy naše informace? I když jsou všechny technologické i netechnologické společnosti vázány regulacemi, ne vždy jsou tato nařízení dodržována v jejich úplnosti. Elektronická data neznají hranice a každá společnost se řídí zákony své země a zemí kde působí. To ale bohužel nestačí. Je běžné, že data, která byla získána jednou společností, jsou posléze prodána společnosti jiné a díky takové praxi se již na tuto koncovou společnost nevztahují nařízení, které platili pro společnost předešlou (Gundersen, 2020). Moderní technologie se rozvíjí rychleji, než se dokáže adaptovat legislativa. To ale může pro, například českého, uživatele znamenat, že jeho data skončí v databázi data miningové společnosti ve Spojených Státech. Ze stejného článku, který je citován výše, také vyplývá, že podobné praktiky jsou opravdu nezákonné, ale jejich vymáhání je do jisté míry nereálné právě díky globální podstatě celé problematiky.

Stále platí pravidlo, že největší zodpovědnost za bezpečí a soukromí v kyberprostoru závisí v prvé řadě na samotném uživateli. Ten volí, kdy a jak bude sdílet své informace se světem, jaké používá nástroje a jaké je

jeho obecné chování. Zda dokáže myslet na důsledky svého chování a jaké to pro něj bude mít implikace do budoucna.

Modelování hrozeb

Jak si ale uživatel dokáže určit správnou polohu „svaté“ trojice internetu: soukromí, bezpečnost a pohodlí? Kde pro něj leží hranice mezi uchováním si soukromí, být zabezpečen a užívat moderních technologií bez větších překážek? Existuje způsob, jak docílit požadovaného nastavení pomocí tzv. modelování hrozeb. V angličtině také známé pod pojmem „Threat modeling“ je způsob, jak si uživatel může navrhnout svůj model ohrožení a reálně se jím řídit (Santarcangelo, 2017). Navíc nemusí mít ani odborné znalosti ohledně informačních technologií.

Začíná se analýzou útočného povrchu (attack surface). Tím se rozumí velikost naší digitální stopy. Ta se skládá z například počtu účtů, které máme u různých služeb, naše historie procházení apod. Dále nás zajímá, jak silná hesla máme k těmto účtům a zda se neopakují. Zde platí další pravidlo, že pokud všude používáme stejné heslo, případnému útočníkovi stačí pouze heslo k hlavnímu emailu. Odtud je poté možné takřka cokoliv. Email se stal středobodem naší digitální identity i když není paradoxně ve své podstatě vůbec bezpečný. Veškerá komunikace probíhá otevřeně, pokud není vyloženě aktivně šifrovaná a to až na pár výjimek není.

Dále se pokračuje v analýze používaných technologií. Jaký používáme operační systém, internetový prohlížeč, aplikace na počítači, aplikace v telefonu nebo zda máme stále zapnutou GPS. Všechny tyto aspekty mohou hrát určující roli v otázce soukromí, bezpečnosti a pohodlí. Podle výše zmíněného je nastavení si svého modelu velice subjektivní. Nicméně zde nyní zmíním set obecných doporučení, které mohou soukromí a bezpečnost standardnímu uživateli zlepšit.

Revize účtů. Doporučuji projít všechny účty, které má uživatel zřízené u různých služeb. Podle práv GDPR (GDPR, 2015) má uživatel právo na to být zapomenut a to i u společností sídlících mimo Evropskou Unii. Pokud není možné dohledat, kde všude má uživatel účty, stačí si projít hlavní email, kam se všechny registrační zprávy posílají. Dále doporučuji revizi hesel. Kde všude uživatel používá stejná nebo slabá hesla a změnit je na unikátní a silná hesla. K tomuto kroku se nejlépe hodí používat správce hesel. Nejlépe nezávislou aplikaci, která je přenositelná mezi operačními systémy. Pokud by tím utrpělo pohodlí, může uživatel využít správce hesel svého hlavního internetového prohlížeče, které už z větší míry všechny mají on-line synchronizaci a aplikace na mobilních zařízeních. S tím úzce souvisí i zapnutí si dvou faktorového ověření, kdy kromě hesla uživatel ještě potřebuje jednorázový kód vygenerovaný aplikací, například v mobilním telefonu nebo pomocí SMS. Nainstalování rozšíření pro blokování reklamy je poslední doporučení. Protože reklamy potřebují pro svůj běh komplexní kód, mohou v sobě ukrývat i nebezpečné skripty. Z tohoto důvodu je lepší reklamy blokovat, nebo alespoň povolovat výjimky na důvěryhodných webech.

Tato doporučení jsou pouze okrajová a jsou namířena na uživatele, kteří si chtějí uchovat i pohodlnost moderních technologií. Pokud by chtěl uživatel jít ještě dál, může používat operační systém založený na Unixu spolu s privátním prohlížečem (například Firefox) a používat minimum aplikací.

Závěr

Moderní technologie nám v každodenním životě nesmírně ulehčují naše povinnosti. Zpřístupňují nám dříve nemyslitelné zdroje informací a dovolují nám vykonávat činnosti na dálku. Udržují nás v kontaktu se našimi blízkými a přinášejí neuvěřitelnou pohodlnost. Na druhé straně však stojí naše zodpovědnost, jak s těmito technologiemi zacházíme. Mnozí si již začínají uvědomovat, že ne vše potřebuje mít svou aplikaci a ne pořád musí být připojeny k internetu. Světová ekonomika je poháněná daty a datovými toky. Ty ve velké míře generují právě běžní uživatelé. Je ale v pořádku, abychom svá data takto dobrovolně odevzdávali? Na tuto otázku tato práce neodpoví, nicméně přinesla stručný vhled do praktik, jak velké nadnárodní společnosti nakládají s daty svých uživatelů a popsala set doporučení, která mohou vrátit uživatelům alespoň část svého soukromí. Těmito doporučeními je pravidelná revize on-line účtů, ke kterým je uživatel přihlášen, zodpovědnost v používání a uchování hesel, dvou faktorová autentizace, etické blokování reklam a pro více technicky orientované uživatele

také využívání software, který nabízí větší soukromí. Veškerá tato doporučení jsou navržena s ohledem na pohodlí v užívání moderních technologií a v konečném důsledku vše začíná a končí právě u uživatele samotného.

Bibliografie

[1] Fahmida Rashid. *How Windows 10 data collection trades privacy for security*. English. online. article. InfoWorld.com [online], 2016. URL: https://www.proquest.com/trade-journals/how-windows-10-data-collection-trades-privacy/docview/1845402393/se-2?accountid=37662.

[2] Kara Swisher. „You Know the Saying: You Are the Product“. English. In: (2021). URL: https://www.proquest.com/blogs-podcasts-websites/you-know-saying-are-product/docview/2596091357/se-2?accountid=37662.