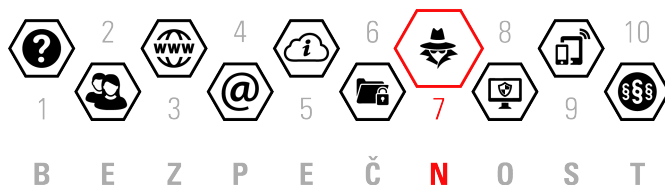


ŠKOLENÍ IT BEZPEČNOSTI UŽIVATELŮ SÍTĚ ZČU



Anonymita na Internetu

Materiály vznikly v rámci projektu Fondu rozvoje CESNET na Západočeské univerzitě v Plzni. Školení má celkem 10 kapitol a veškeré texty, prezentace a další podrobnosti naleznete na stránce <https://bezpecnost.zcu.cz>.

Licence: Creative Commons Attribution 4.0 International Public License

- 1 Když nevíš, zeptáš se.**

V případě podezření na kybernetický útok, když obdržím pochybný e-mail nebo se počítač chová divně, kontaktuji uživatelskou podporu a domluvím se na dalším postupu. Řídím se pokyny odborníků.
- 2 Budeš se autentizovat a autorizovat.**

Počítač mě sám nepozná, proto mu musím svou identitu prokázat například znalostí hesla k uživatelskému účtu (autentizace). V aplikacích, programech a informačních systémech často nemám oprávnění ke všem činnostem. Proto po autentizaci následuje autorizace, která stanoví, co smím a co ne.
- 3 Dáš si pozor, kam heslo zadáváš.**

Přihlašovací údaje vyplňuji pouze do webové stránky, která je šifrovaná, tedy její adresa začíná **https://** nebo je na jejím začátku ikona zámku. Je důležité, aby adresa stránky byla uvedena přesně; i podvodné stránky mohou používat šifrování.
- 4 K přichozí poště budeš zdravě podezřívý(á).**

Elektronická pošta je často zneužívána k rozesílání spamů, hoaxů, phishingových nebo hromadných zpráv. Dávám si pozor na podezřelé e-maily, zvláště na ty, které obsahují přílohu nebo odkazy na stránky. Příloha může obsahovat škodlivý kód a odkazovaná stránka může být podvodná.
- 5 Nebudeš věřit všemu, co se na Internetu píše.**

Na Internetu může zveřejňovat informace každý, i autor neznalý nebo záměrně manipulující. Proto si věrohodnost získávaných informací vždy ověřuji. V pracovním prostředí musím zacházet s informacemi uvážene; ne všechny údaje jsou určeny všem.
- 6 Důvěrné informace budeš šifrovat.**

Šifrování dat zajišťuje, že si informaci nemůže přečíst každý, kdo ji získá, ale jen ten, kdo zná navíc dešifrovací klíč. Elektronický podpis potvrzuje, že podepsaná osoba je autorem nebo že s obsahem souhlasí. Zároveň potvrzuje, že obsah elektronicky podepsaného dokumentu se po podepsání už nezměnil.
- 7 Na Internetu nejsi anonymní.**

Prohlížením stránek i používáním služeb na Internetu po sobě zanechávám množství stop. Další stopy vznikají dobrovolným zveřejňováním informací o sobě, zejména na sociálních sítích. Všechny tyto činnosti moji anonymitu snižují a je dobrým zvykem chovat se tak, jako by mě mohl kdokoli identifikovat.
- 8 Budeš chránit své počítače a data zálohovat.**

Nikdo nepovoláný by neměl používat cizí osobní věc, jakou je například počítač. Takové zařízení musím chránit zamykáním kanceláře a používáním zámku obrazovky. Dbám na aktuálnost jeho programového vybavení, případně svěřím správu zařízení odborníkům. Důležitá data pravidelně zálohuji.
- 9 Mobilní zařízení jsou také počítače.**

Mobilní zařízení, dnes nejčastěji chytrý mobilní telefon, je malý počítač a chovám se k němu a datům v něm stejně jako v případě počítače. Navíc si musím uvědomovat rizika, která přináší možnost zařízení přenášet nebo ho mít stále u sebe.
- 10 Budeš dodržovat pravidla a ctít právo.**

Na Internetu platí stejná legislativa jako v reálném světě, ale je rozšířená o některé další specifické právní normy. Mimo tuto státem vyžadovanou legislativu dodržuji také interní pravidla organizací nebo pravidla používání konkrétních služeb.

Anonymita na Internetu

7.1 Úvod

Mnoho uživatelů Internetu si myslí, že když sedí u svého počítače na své židli ve svém vlastním domově, nikdo o nich neví a jejich činnost na Internetu je zcela anonymní. Například pokud napíše komentář do diskusního fóra a nepodepíše se, nikdo nemůže zjistit autora komentáře. Opak je ale pravdou. Ve skutečnosti na Internetu je vše zaznamenáno a navíc s daleko větší trvanlivostí než v běžném světě. Zatímco v běžném životě se ledasco rychle zapomene a nedá se v paměti vyhledávat, to, co se dostane na Internet, zaindexují vyhledávače a v nich to může zůstat k dohledání skutečně dlouho. Pokud je tedy potřeba dohledat konkrétního autora na Internet napsaného textu, není to často až tak velký problém.

7.2 Anonymita

Anonymita je *schopnost být nepoznán*, což je prakticky schopnost nebýt odlišitelný od ostatních. Při pohybu na Internetu zanecháváme postupně množství stop, které nás činí méně odlišitelnými, a tedy čím déle se na Internetu pohybujeme, tím méně jsme anonymní.

S anonymitou na Internetu je to navíc komplikovanější než v reálném světě. *Elektronické stopy* přetrvávají na Internetu dlouho, jsou dostupnější více lidem a jelikož jsou v elektronické formě, lze je snadno vyhledávat a spojovat.

7.3 Používání Internetu

Pojďme se nejprve podívat na to, jak to na tom Internetu vlastně celé funguje.

Připojení k Internetu

Proto, aby mohly počítače spolu komunikovat, musí mít jedinečné identifikátory. Obdobně jako máme poštovní adresy nebo rodná čísla v reálném světě. Ve světě Internetu a počítačových sítí obecně se jim říká IP adresy (zkratka IP znamená Internet Protocol). Aby bylo možno zajistit unikátnost IP adres, jsou přidělovány hierarchickým způsobem. Nejvýše stojí celosvětová organizace IANA, která přiděluje rozsahy adres jednotlivým regionálním registrátorům (RIR), ti pak lokálním registrátorům (LIR) a ti nakonec jednotlivým organizacím nebo poskytovatelům internetového připojení (ISP).



Rozdělení světa podle oblastí regionálních registrátorů

- RIPE NCC (Réseaux IP Européens Network Coordination Centre) – Evropa, Rusko, severní Afrika.
- ARIN (American Registry for Internet Numbers) – Amerika, jižní Afrika.
- APNIC (Asia Pacific Network Information Centre) – Asie, Austrálie a Oceánie.
- LACNIC (Latin American and Caribbean Network Information Centre) – Latinská Amerika, Karibik.
- AfriNIC (African Network Information Centre) – Afrika.

Jednotlivé organizace pak přidělují konkrétní IP adresy jednotlivým zařízením nebo domácnostem a vedou si záznamy o tom, komu a kdy danou IP adresu přidělily. Jednak je to pro zajištění výše zmiňované unikátnosti a jednak chtějí mít přehled, kdo se v jejich síti pohybuje.

Prakticky to znamená, že už jen samotným *připojením k Internetu ztrácíme mnoho ze své anonymity* – z veřejně dostupné databáze registrátorů lze zjistit, které organizaci byla IP adresa přidělena, a současně správci sítě dané organizace ví, komu byla jaká IP adresa v jakém čase přidělena.

Jak vypadá IP adresa?

IPv4 (Internetový Protokol verze 4) je čtyřbytový identifikátor zapisovaný v desítkové soustavě, například **192.168.100.10**. Celkem existuje cca 4 miliardy IPv4 adres.

IPv6 (Internetový Protokol verze 6) vznikl jako náhrada IPv4, protože kupodivu jsou 4 miliardy adres málo. Proto jde o šestnáctibytový identifikátor a je zapisovaný hexadecimálně pro zkrácení délky zápisu, například **2001:db8:bee:b00:10ab**. Celkem tedy existuje 3.4×10^{38} IPv6 adres, což by mohlo na pár následujících století stačit.

Komunikace na Internetu

Správci počítačových sítí potřebují také vědět, co se v jejich síti vlastně děje, aby mohli včas *detekovat a odstraňovat technické problémy*. A v případě potřeby také *vyšetřovat kybernetické útoky* a nahlášené *bezpečnostní incidenty*. Proto jsou data o provozu na síti sbírána a ukládána – konkrétně tedy jaká IP adresa s jakou IP adresou komunikovala, kolik dat a kdy si přenesly apod. Vlastní přenesená data však ukládána nejsou, protože jich je ohromné množství. Je to tedy podobné, jako kdyby někdo sbíral informace o tom, s kým jste si telefonovali, ale neukládal si obsah hovoru. Tato data o provozu ukládá každý správce sítě – veřejný poskytovatel připojení (ISP) to má přikázáno zákonem a ostatní to dělají také, protože to je v jejich vlastním zájmu.

Nesmíme zapomínat, že Internet je vlastně tvořen mnoha vzájemně propojenými sítěmi a naše komunikace – například při návštěvě webové stránky na serveru v zámoří – jde přes několik různých sítí různých organizací. A každá z nich sbírá a ukládá data o provozu ve své síti. Po každé komunikaci tedy zůstávají stopy, díky kterým lze teoreticky ke každé přiřadit IP adresu jejího původce. A jak jsme si ukázali výše, používání IP adresy není zcela anonymní, takže ani *komunikace nemůže být z principu zcela anonymní*.

Anonymizační síť

Zkušený uživatelé mohou pro anonymizaci své činnosti použít anonymizační síť, například TOR nebo I2P. Komunikace je zde vedena přes mnoho prostředníků, takže dochází k zamlžení informace, kdo s kým vlastně komunikuje.

Jak ukazují případy vystopování několika zkušených kyberkriminálků, nelze se ani zde spoléhat na 100% anonymitu. Většina uživatelů anonymizačních sítí spoléhá na to, že informace o provozu jsou v jednotlivých sítích ukládány pouze omezenou dobu, takže po sobě sice stopy zanechají, ale než se k nim vyšetřovatelé dostanou, jsou přepsány novějšími záznamy.

Používání Internetových služeb

Lidé používají Internet kvůli mnoha nabízeným službám, například webovým stránkám. Každá takováto služba má svého provozovatele, který si ze stejných důvodů jako správce sítě ukládá provozní informace. Typicky se jedná o čas návštěvy/přihlášení a IP adresu zařízení, ze kterého uživatel přistupuje. Zaznamenává také čas provedení různých akcí uživatele, jako je registrace, zveřejnění příspěvku, editace profilu apod.

Většinou je také prováděno profilování uživatele, tj. kdy se obvykle přihlašuje, jak dlouho je přítomen, na jaké odkazy kliká, co ho zajímá. Tyto informace, které může provozovatel služby sbírat, jsou cenné pro prodejce reklamy a další firmy, takže mohou být předmětem obchodu. Abychom věděli, jak s těmito daty smí provozovatel naložit, je třeba si přečíst Podmínky používání/Licenční podmínky dané služby.

Co o vás prozradí váš prohlížeč?

Při návštěvě webové stránky jí webový prohlížeč o sobě posílá řadu informací, aby mohla být správně naformátována (rozlišení obrazovky, nastavený jazyk), ale i mnoho dalších, které lze použít ke snížení anonymity návštěvníka (například z jaké stránky přicházíme, geolokační údaje apod.).

Chcete vědět, co váš prohlížeč o sobě prozradí? Podívejte se například na <https://amiunique.org>.

Používáním Internetových služeb jsou zanechávány digitální stopy, které snižují anonymitu uživatele. Čím více služeb používá nebo čím déle je používá, tím méně je anonymní a ve spojení s informacemi od provozovatele sítě a v podstatě neanonymním přidělováním IP adres *na anonymitu na Internetu nelze spoléhat*.

Pseudonymita

V souvislosti s poskytovateli služeb se často používá také pojem pseudonymita. Informace, které má provozovatel dostupné, často nestačí k plné identifikaci fyzického uživatele, ale lze z nich určit, že jde o stejného uživatele (resp. prohlížeč) jako minule. E-shopy tak například mohou nabízet stejný druh zboží, které si uživatel prohlížel při minulé návštěvě.

7.4 Zveřejňování informací

Digitální stopy, které po nás zůstávají díky používání Internetu a které nemůžeme nijak ovlivnit, však nejsou jediné vodítko k naší identifikaci. Někteří uživatelé mají sklony se chovat jako neuvážliví exhibicionisté a sociální sítě jim poskytují prostor a příležitost. Často se rádi chlubí a dobrovolně zveřejňují informace, čímž postupně odhalují své soukromí. Je třeba si dát pozor, co o sobě zveřejňujeme a kdo to může vidět, a uvědomit si, že jednotlivé nevinné střípky lze seskládat tak, že mohou dohromady poskytnout zcela nepředpokládané informace. Například zkušený psycholog dokáže podle informací, které o sobě zveřejňujete, dobře popsát vaši osobnost. Využít těchto informací mohou také personalisté při prověřování uchazeče o zaměstnání.

7.5 Kdo mne může identifikovat?

K informacím, které nás plně identifikují, nemá naštěstí přístup úplně každý. Je třeba ale pamatovat na to, že bude-li identifikace potřeba, například při vyšetřování Orgány činnými v trestném řízení, je identifikace možná a je tedy nutné své chování na Internetu přizpůsobit tomuto faktu.

7.6 Shrnutí

Anonymitou rozumíme schopnost nebýt odlišitelný od ostatních. Používáním Internetu je anonymita jednotlivých uživatelů postupně snižována, protože po sobě zanechávají digitální stopy.



7. ANONYMITA NA INTERNETU

Z principu fungování Internetu tomu nelze zabránit, protože každý počítač pro komunikaci musí používat hierarchicky přidělované IP adresy a lze zpětně zjistit, komu byly v konkrétním okamžiku přiděleny. Další informace o používání Internetu získávají poskytovatelé používaných služeb, například webových stránek. Kromě těchto automaticky a technicky vytvářených digitálních stop o sobě uživatelé zveřejňují další informace sami dobrovolně na sociálních sítích, v komentářích, v diskusích nebo na vlastních webech. Případně některé informace zveřejní také zaměstnavatel o svých zaměstnancích. Je tedy dobrým zvykem se na Internetu na anonymitu nespoléhat a chovat se tak, jako bychom byli vždy plně identifikovatelní.