EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

LEGISLATIVA

Legislativní rámec DR řešení

Metodický list

Autor: Ing. Marek Kocan, Metodik: Mgr. Hana Hrádková

Recenzent: Mgr. Jiří Činčura

Rok vydání: 2023

Obsah

Cíle

Studenti se seznámí s legislativním rámcem pro sběr provozních a lokalizačních údajů, tzv. data retention (DR), zejména pak s ohledem na komunikaci v rámci internetu. Studenti tak získají základní představu o ne-anonymitě v internetovém prostředí, přehled o legislativních otázkách i rámcových způsobech naplnění požadavků legislativy.

Student bude schopen vlastními slovy diskutovat problematiku anonymity v internetovém prostředí, uvést základní informace o platné legislativě související s data retention problematikou a popsat proces zavádění řešení umožňující naplnit legislativní požadavky. V dlouhodobém horizontu bude student schopen samostatně využít nové znalosti pro lepší orientaci v internetovém prostředí a celkovému pochopení problematiky anonymity.

Dovednosti

Student bude schopen věcně diskutovat o problematice anonymity v internetovém prostředí s ohledem na možnosti státních orgánů odhalovat trestnou činnost související s kybernetickou kriminalitou, a to s ohledem na sběr a provoz lokalizačních údajů.

Pracovní prostředí

Tradiční třída s projekční technikou.

1 Legislativní rámec DR řešení

Požadavky na sběr provozních a lokalizačních údajů – tedy tzv. data retention, DR – vycházejí ze směrnice Evropské unie 2006/24/EC. Tato směrnice byla v souladu s pravidly reflektována ve většině členských států do místní legislativy, v České republice jde zejména o *Zákon o elektronických komunikacích* (127/2005 Sb.), *Vyhlášku o uchovávání, předávání a likvidaci provozních a lokalizačních údajů* (357/2012 Sb.) a *Vyhlášku o stanovení výše a způsobu úhrady efektivně vynaložených nákladů na odposlech a záznam zpráv, na uchovávání a poskytování provozních a lokalizačních údajů a na poskytování informací z databáze účastníků veřejně dostupné telefonní služby* (462/2013 Sb.).

1.1 Anonymita na internetu

Představa, že jsou uživatelé v internetovém prostředí anonymní je ve své podstatě zcela iluzorní. Bez ohledu na použité komunikační prostředí má stát dostatek prostředků zpětně identifikovat původce problematické komunikace (u následných kroků pak včetně odposlechů komunikace). Z technického pohledu nejde o příliš obtížná řešení, zejména pak s ohledem na fakt, že drtivá většina účastníků nevyužívá žádné prostředky pro zastření pravé identity.

V případě komunikace prostřednictvím internetu je základní digitální stopou IP adresa původce komunikace, která se nemění ani v případě často používaného anonymního režimu v internetovém prohlížeči – je ironií osudu, že právě tento režim uživatelé často považují za prostředek dokonalé anonymizace. Zjednodušeně řečeno, bez ohledu na použité softwarové prostředky neměnící síťovou komunikaci (otázkou může být využití VPN, což je ale nad rámec tohoto scénáře), existuje vždy jednoznačná identifikace *od koho komunikace probíhala*.

Vyučující v případě potřeby rozvede diskusi se studenty na téma Kdo usiluje o anonymní jednání? (individuální pohled na to, že bychom měli mít svobodu vs. zakrytí skutečné identity s cílem páchání nekalé činnosti – nemusí jít nezbytně o trestnou činnost).

Kontrolní bod

Studenti vysvětlí, proč není anonymní režim prohlížečů dostatečný pro zajištění skutečné anonymity.

1.2 Pohled poskytovatele připojení

Jak bude ukázáno v dalších částech, legislativa stanovuje pro poskytovatele internetové konektivity určité povinnosti, které vedou k následné identifikaci původce komunikace. Poskytovatel připojení tak musí na žádost oprávněných orgánů:

- identifikovat původce komunikace, a to nejméně v rozsahu smluvní osoby
- poskytnout informace o tom kdy, kdo, s kým a jak dlouho původce komunikace komunikoval
- poskytnout technické informace o komunikace

Poskytovatel nemůže dodat obsah komunikace – toto legislativa neukládá, jde pak o předem schvalované odposlechy podléhající speciálnímu režimu.

1.3 Pohled oprávněných orgánů

Oprávněné orgány – nejčastěji policie – pro naplnění svého poslání v případě trestné činnosti související s internetovou komunikací může potřebovat:

- co nejpřesněji identifikovat konkrétního uživatele na základě vstupu IP adresa, port a čas (příjemce komunikace)
- zajistit odposlech (viz výše)

Kontrolní bod

Studenti diskutují pohled poskytovatele konektivity a pohled oprávněných orgánů.

2 Legislativní povinnosti a práva

2.1 Služba přístupu k internetu z pevného připojení (§ 2, odst. 3, písm. a) vyhlášky)

Legislativa (*Vyhláška o uchovávání, předávání a likvidaci provozních a lokalizačních údajů* (357/2012 Sb.)) poskytovatelům internetové konektivity v případě pevného připojení (o komunikaci s přepojováním paketů jako celek jde konkrétně o odst. 3 – *U sítí elektronických komunikací s přepojováním paketů*) ukládá povinnost shromažďovat následující informace:

1. typ připojení
2. telefonní číslo nebo označení uživatele
3. identifikátor uživatelského účtu
4. adresa MAC zařízení uživatele služby
5. datum a čas zahájení a ukončení připojení k internetu
6. označení přístupového bodu u bezdrátového připojení k internetu
7. adresa IP a číslo portu, ze kterých bylo připojení uskutečněno

U služby přístupu k internetu s překladem IP adres (tedy NAT) jde (písm. f) o:

1. privátní adresa IP
2. veřejná adresa IP a číslo portu, nebo přidělený rozsah portů
3. datum a čas zahájení překladu adres
4. datum a čas ukončení překladu adres

Další písmena odstavce 3 pokrývají:

1. služby přístupu k internetu z mobilního připojení
2. služby přístupu ke schránce elektronické pošty
3. služby přenosu zpráv elektronické pošty
4. služby IP telefonie

Vyučující upozorní na to, že v případě jiných způsobů komunikace – například u veřejných telefonních sítí či veřejných mobilních telefonních sítí – jsou povinnosti definovány mírně odlišně a odkáže na diskutovanou vyhlášku.

2.2 Další povinnosti

Poskytovatel internetové konektivity musí provozní a lokalizační údaje uchovávat po dobu přesně 6 měsíců, po této době by šlo o porušení zákonných povinností – je důležité si to uvědomit zejména z pohledu vytvářených záloh/archivů, které mohou být tímto pravidlem ovlivněny a je nutné na ně v reálném prostředí pamatovat.

Vyučující dle potřeby uskuteční se studenty diskusi na objem uchovávaných dat (u velkých poskytovatelů může půlroční období znamenat i stovky terabajtů dat).

U sítí uvedených v odstavcích 1 až 3 vyhlášky (tedy i v případě internetové komunikace) se dále uchovává jméno, popřípadě jména a příjmení a adresa účastníka nebo registrovaného uživatele uvedená ve smlouvě nebo adresa umístění telekomunikačního koncového zařízení.

Poskytovatel má dále povinnost předem nahlašovat výpadky či nefunkčnost jím používaného DR řešení a včas reagovat na výzvy oprávněných orgánů (poskytnout odpovídající součinnost).

Za zmínku s ohledem na technologické zajištění stojí povinnost *Údaje o času se uchovávají v místním čase. V případě, že místní čas neodpovídá času v České republice, jsou údaje o času udávány spolu s označením časového pásma.* Naprostý soulad v čase jednotlivých záznamů je elementárním předpokladem pro úspěšnou identifikaci. Vyučující dle potřeby a dosavadních znalostí třídy zmíní problematiku NTP.

2.3 Ekonomická stránka

Poskytovatel internetové konektivity má nárok na proplácení nákladů, a to jak z pohledu použitých technologií, tak i služeb. Celá problematika je nicméně příliš komplexní a za základ lze považovat fakt, že mohou být implementovány i speciální DR projekty schvalované příslušnými orgány (v tomto kontextu *Útvarem zvláštních činností služby kriminální policie a vyšetřování*, ÚZČ) – náklady na pořízení DR řešení (často formou leasingu) jsou pak propláceny zpětně v pravidelných splátkách. ÚZČ má metodiky a specialisty na vyhodnocování, zda podané projekty odpovídají průměrným limitům a využití, nejčastěji jsou limity odvozovány od počtu přípojek s orientační platbou cca vyšší počet jednotek stokorun na přípojku v celkových nákladech na dobu životnosti projektu. Dále ÚZČ zpravidla v takovéto situaci vyžaduje záruku včetně hardwarové.

Proces v případě projektové žádosti se zpravidla skládá z následujících kroků:

1. Příprava projektové žádosti zohledňující počet klientů, rychlost linek, nutnost využití NAT, předpokládaný nárůst v období 3 let (projekty se často schvalují na tři roky s možností prodloužení celkem na 5 let).
2. Domluva dodavatele (případně podmínek výběrového řízení)
3. Domluva financování (často forma leasingu)
4. Podání projektové žádosti
5. Proces schvalování ze strany ÚZČ, může vést k řadě dotazů
6. Realizace

Kontrolní bod

Studenti diskutují technický rozsah povinností a ekonomickou stránku DR řešení.

3 Ukázka DR řešení

Pro naplnění legislativních požadavků může poskytovatel internetového připojení využít jak své prostředky, tak i specializovaná DR řešení či nadstavby nad systémy pro monitoring síťové konektivity. Neexistuje nic jako schválený seznam řešení, nicméně ÚZČ má zkušenosti s možnými systémy a tyto své zkušenosti zohledňuje při schvalování projektových žádostí.

Vyučující v rámci prezentace komentuje základní snímky s řešením od společnosti Progress/Flowmon.

Kontrolní bod

Studenti diskutují problematiku anonymity na internetu a možnosti identifikace původce komunikace.

Shrnutí a závěr

Studenti se seznámili se základy legislativního rámce pro tzv. data retention – tedy sběru provozních a lokalizačních údajů – v případě poskytování internetové konektivity. Studenti byli dále seznámení s problematikou anonymity v rámci internetového prostředí.

Seznam použitých zdrojů

Zákon o elektronických komunikacích (127/2005 Sb.)

Vyhláška o uchovávání, předávání a likvidaci provozních a lokalizačních údajů (357/2012 Sb.)

Vyhláška o stanovení výše a způsobu úhrady efektivně vynaložených nákladů na odposlech a záznam zpráv, na uchovávání a poskytování provozních a lokalizačních údajů a na poskytování informací z databáze účastníků veřejně dostupné telefonní služby (462/2013 Sb.).