Jihočeská univerzita v Českých Budějovicích

Ekonomická fakulta

Katedra aplikované matematiky a informatiky

Bakalářská práce

Zabezpečení důvěrnosti a integrity elektronických záznamů o činnostech (logů) pro potřeby soudního dokazování

Vypracoval: Pavel Duchan
Vedoucí práce: doc. Ing. Ladislav Beránek, CSc.
České Budějovice 2021

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH

Ekonomická fakulta

Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Pavel DUCHAN
Osobní číslo:	E18604
Studijní program:	B6209 Systémové inženýrství a informatika
Studijní obor:	Ekonomická informatika
Téma práce:	Zabezpečení důvěrnosti a integrity elektronických záznamů o činnostech (logů) pro potřeby soudního dokazování
Zadávající katedra:	Katedra aplikované matematiky a informatiky

Zásady pro vypracování

Cílem bakalářské práce je navrhnout v praxi použitelné řešení pro zajištění důvěrnosti a integrity logů, které by bylo možné použít při soudním řízení jako přípustný důkaz. Obsah práce bude mít dvě části. Teoretická část bude obsahovat následující problematiku: popis dokazování v trestním právu; integrita a nepopiratelnost, elektronický podpis, elektronické pečeti, časová razítka, certifikáty (PKI infrastruktura). Praktická část bude obsahovat návrh směrnice/politiky logování v souladu s požadavky vyhlášky č. 82/2012 Sb. s přihlédnutím k relevantním částem článku 12.4 (resp. 12.4.2) normy ISO 27002 a požadavkům platné legislativy (Zákoník práce, zpracování osobních údajů, Trestní zákoník, případně další).

Metodický postup:

1. Studium odborné literatury.
2. Teoretická část práce, popis hlavních metod a technologií.
3. Zpracování návrhu směrnice/politiky logování v souladu s požadavky příslušných směrnic a standardů pro tuto oblast.
4. Vypracování doporučení a závěrů.

Rozsah pracovní zprávy: 40 – 50 stran
Rozsah grafických prací:
Forma zpracování bakalářské práce: tištěná

Seznam doporučené literatury:

1. ANDERSON, R. (2020). *Security Engineering*. [online]. Cambridge. Dostupné z: <https://www.cl.cam.ac.uk/ rja14/book.html>.
2. KOLOUCH, J., & BAŠTA, P. (2019). *CyberSecurity*. Praha: CZ.NIC, z.s.p.o.
3. LANDOLL, D. J. (2016). *Information security policies, procedures, and standards: a practitioner's reference*. Boca Raton: CRC Press, Taylor & Francis Group.
4. VACCA, J. R. (2017). *Computer and information security handbook*. Cambridge, MA: Morgan Kaufmann Publishers, an imprint of Elsevier.
5. WILLIAMS, B. L. (2013). *Information security policy development for compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA standard, PCI DSS V2.0, and AUP V5.0*. Boca Raton, FL: CRC Press, Taylor & Francis Group.

Vedoucí bakalářské práce: **doc. Ing. Ladislav Beránek, CSc.**
Katedra aplikované matematiky a informatiky

Datum zadání bakalářské práce: **17. ledna 2020**
Termín odevzdání bakalářské práce: **16. dubna 2021**

JIHOČESKÁ UNIVERZITA
V ČESKÝCH BUDĚJOVICÍCH
EKONOMICKÁ FAKULTA
Studentská 13 (26)
370 05 České Budějovice

doc. Dr. Ing. Dagmar Škodová Parmová
děkanka

doc. RNDr. Tomáš Mrkvička, Ph.D.
vedoucí katedry

V Českých Budějovicích dne 26. března 2020

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47 zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské/diplomové práce, a to – v nezkrácené podobě/v úpravě vzniklé vypuštěním vyznačených částí archivovaných Ekonomickou fakultou – elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

Datum

Podpis studenta

Obsah

1 Úvod

Cílem práce je navrhnout postup pro zajištění elektronických logů způsobem, aby byly uznány v soudním sporu jako přípustný důkaz.

Práce zkoumá legislativní požadavky na důkazy a požadavky na ochranu informačních aktiv, aby z nich mohla vycházet při formulaci postupu. Zároveň přihlíží k relevantním částem mezinárodních bezpečnostních standardů a norem, které se vztahují k problematice ochrany informací, forenzní analýzy nebo ochraně elektronických dat.

Praktickým výstupem práce je popsaný postup správy elektronických logů, aby se minimalizovalo riziko spojené s odmítnutím přípustnosti logů pro jejich nedůvěryhodnost z důvodů nedostatečného zabezpečení integrity nebo důvěrnosti. Důvěrností rozumíme „*vlastnost, že informace není dostupná nebo není zpřístupněna neoprávněným jednotlivcům, entitám nebo procesům*.“ (ISO 27000, 2018, s.10) Integritou „*zajištění přesnosti a úplnosti*.“ (ISO 27000, 2018, s.12)

V práci jsou využívány pojmy „elektronické záznamy o činnostech“, „auditní záznamy“ „auditní stopy“ nebo „auditní informace“ které jsou synonymem pro logy. *Log je záznam události vyskytnuté v systémech a síti organizace*.“ (Kent & Souppaya, 2006, s.A-1). Práce se nezabývá jinou formou záznamů než elektronickou.

Logy zaznamenávají úspěšnou nebo neúspěšnou činnost uživatelů nebo systémů. „*Původně se logy používaly primárně pro řešení provozních problémů, ale logy dnes mají pro většinu organizací velké množství funkcí, jako je např. optimalizace výkonu systému nebo sítě, zaznamenávání činnosti uživatelů a poskytování dat užitečných pro vyšetřování škodlivých činností*.“ (Kent & Souppaya, 2006, s.2-1).

S rozvojem a využíváním informačních technologií v organizaci[1] vzrůstá také zákonná povinnost organizací chránit informace uložené v elektronické podobě[2]. S nově

[1] Pojem organizace v této práci reprezentuje právnickou osobu podle §118 - §488 zákona č. 89/2012 Sb. občanského zákoníku, živnostníky podle §2 zákona č. 455/1991 Sb. o živnostenském podnikání, organizační složky státu podle §3 odst. 1 zákona č. 219/2000 Sb. o majetku České republiky a jejím vystupování v právních vztazích, rozpočtové organizace a příspěvkové organizace podle příslušných zákonů.

[2] Např. zákon č. 110/2019 Sb. o zpracování osobních údajů upravující nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES nebo zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů

přijímanými zákony je také spojena medializace problematiky ochrany firemních aktiv[3], kterou velmi dobře ilustruje mediální pokrytí vstoupení Obecného nařízení o ochraně osobních údajů[4] v účinnost v květnu roku 2018, kdy média o potřebě ochrany osobních údajů, a především sankcích spojených informovala prakticky na denní bázi po dobu tří měsíců. S o něco menším mediálním ohlasem vstoupila v účinnost aktualizace vyhlášky č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritérií, kdy v médiích rezonoval především odpor vůči této aktualizaci ze strany úřadů. V budoucnosti lze očekávat velké mediální pokrytí schválení nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (tzv. ePrivacy), ohledně které by měl být v dohledné době být vedený trialog. (Úřad k návrhu nařízení o soukromí a elektronických komunikacích, 2021)

Díky medializaci úspěšných a probíhajících kybernetických útoků a edukaci uživatelů (např. Týdeník Policie, Národní úřad pro kybernetickou a informační bezpečnost, Velitelství kybernetických sil a Informačních operací, ale také běžná média) věnují organizace problematice zabezpečení informačních a kybernetických aktiv větší pozornost a finanční prostředky. V praxi organizace řeší především ochranu dat před útoky zvnějšku organizace (ochrana koncových stanic, firewall) a vychází se z předpokladu loajality zaměstnanců. Právě zaměstnancům a dodavatelům je ve většině organizacích důvěřováno, ačkoliv zkušenosti z domova i ze zahraničí (kdy zaměstnanec předal databázi zákazníků konkurenci[5] nebo kdy přes přístup dodavatele získali útočníci přístup k datům organizace[6]) ukazují na takovou důvěru jako na důvěru neopodstatněnou.

Jsou to právě uživatelé, především privilegovaní uživatelé, kteří mohou způsobit úmyslně nebo neúmyslně největší škody, případně umožnit získání přístupu útočníkovi na základě tzv. sociálního inženýrství[7]. Zdroje uvádějí, že 90-95 %[8] [9] všech kybernetických útoků

---

[3] „*Cokoliv, co má hodnotu pro jednotlivce, organizaci nebo veřejnou správu*“. (Jirásek et al., 2013, s. 12)
[4] Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES nebo zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů
[5] Usnesení Nejvyššího soudu ze dne 23.8.2017 5 Tdo 781/2017-23
[6] https://tech.ihned.cz/internet/c1-66894460-pohled-do-tovarny-tesly-vezeni-i-nemocnic-hackeri-ziskali-pristup-k-tisicum-bezpecnostnim-kamer
[7] „*Způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace*.“ (Jirásek et al., 2013, s. 93)
[8] https://www.e-zu.co.uk/2020/06/16/95-of-cyber-security-breaches-are-due-to-human-error/
[9] https://www.entrepreneur.com/article/345638

v nějaké fázi využije (resp. zneužije) člověka. Tyto statistiky společně s rostoucí regulací a sankcemi za porušení informační bezpečnosti nutí organizace školit zaměstnance v oblasti informační bezpečnosti a tím mít možnost postihovat zaměstnance. Pro postihnutí je ale nutné mít dostatečné důkazy, a právě elektronické důkazy mohou být kamenem úrazu při dokazování. V praxi je při soudním řízení přihlíženo k důkazům, které byly připuštěny druhou stranou. Přípustnost důkazů tak obvykle posuzuje advokát na základě svých znalostí a vědomostí v oblasti informačních technologií. Soudní znalec pak hodnotí již připuštěné důkazy, což může znamenat například záznam činnosti (log) vytištěný na papíru.

Práce si záměrně vybírá návrh bezpečnostních opatření pro situaci, která je pro zaměstnavatele nejobtížnější, tedy využití vlastních logů při soudním řízení se zaměstnancem při dokazování jeho pochybení nebo záměrného způsobení škody spadající do oblasti kybernetické kriminality.[10] Taková bezpečnostní opatření budou dostatečná pro využití logů i v jiných případech, než je prokazování závadných činností zaměstnanců.

[10] Pojem kybernetická kriminalita není v trestním řádu České republiky definován. Dokonce není definován ani v základním dokumentu mezinárodního práva Úmluvě o počítačové kriminalitě 104/2013 sb.m.s. (ratifikována Českou republikou 22.8.2013) a tedy ani v navazující evropské směrnici 2013/40/EU ze dne 12. srpna 2013

2 Trestné činy zaměstnance využívající informační technologii

Předkládání důvěryhodných elektronických důkazů, mezi které se elektronické záznamy o činnostech řadí, může být velkým problémem při dokazování trestné činnosti zaměstnance, a to hned z několika důvodů:

1) v rámci pracovněprávních vztahů „*existuje zvláštní zákonná ochrana zaměstnance*“,[11]
2) „*nedotknutelnost osoby a jejího soukromí je zaručena a omezena může být jen v případech stanovených zákonem*“,[12]
3) „*elektronická data mohou být snadno změněna, přepsána, poškozena nebo zničena*“ (Interpol, 2019, s.13).

Z těchto důvodů je potřeba klást v organizacích velký důraz na zabezpečení důvěrnosti a integrity elektronických záznamů o činnostech, aby bylo možné je využít nejenom jako zdroj pro vyšetření časové souslednosti událostí, ale také jako důkazu při soudním řízení.

2.1 Důkazy trestné činnosti v české právní úpravě

Právní prostředí České republiky vychází z presumpce (předpokladu) neviny, která je zakotvena v Listině základních práv a svobod: „*Každý, proti němuž je vedeno trestní řízení, je považován za nevinného, pokud pravomocným odsuzujícím rozsudkem soudu nebyla jeho vina vyslovena.*“[13] Téměř identicky se vyjadřuje Trestní řád: „*Dokud pravomocným odsuzujícím rozsudkem soudu není vina vyslovena, nelze na toho, proti němuž se vede trestní řízení, hledět, jako by byl vinen.*“[14]

Trestnost činu je posuzována na základě zjištěného skutkového stavu věci, o němž nejsou důvodné pochybnosti.[15] Právě skutkový stav věci je zjišťován pomocí hodnocení důkazů.[16] Za důkaz „*může sloužit vše, co může přispět k objasnění věci, zejména výpovědi*

[11] §1a odst. 1 písm. a) zák. č. 282/2006 Sb.
[12] čl.7 odst. 1 písm. a) usn. č. 2/1993 Sb.
[13] čl. 40 odst. 2 usn. č. 2/1993 Sb.
[14] §2 odst. 2 zák. č. 141/1961 Sb.
[15] §2 odst. 5 zák. č. 141/1961 Sb.
[16] §2 odst. 6 zák. č. 141/1961 Sb.

obviněného a svědků, znalecké posudky, věci a listiny důležité pro trestní řízení a ohledání.“[17]

Cílem předložených důkazů je podle Trestního řádu dokázat v nezbytném rozsahu (pro rozhodnutí):

a) „zda se stal skutek, v němž je spatřován trestný čin,

b) zda tento skutek spáchal obviněný, případně z jakých pohnutek,

c) podstatné okolnosti mající vliv na posouzení povahy a závažnosti činu,

d) podstatné okolnosti k posouzení osobních poměrů pachatele,

e) podstatné okolnosti umožňující stanovení následku, výše škody způsobené trestným činem a bezdůvodného obohacení,

f) okolnosti, které vedly k trestné činnosti nebo umožnily její spáchání.“[18]

Z výše popsaného je zřejmé, že logy samotné nejsou dostatečným důkazem a jejichž základě by mohl být kdokoliv odsouzen za spáchání trestného činu. Logy nic nevypovídají o pohnutkách aktéra takového činu ani o podstatných okolnostech osobních poměrů pachatele. Podstatné okolnosti mající vliv na posouzení povahy a závažnosti činu z logů také nelze vyčíst. Logy nestanovují následky ani výše škody, jsou pouze dokladem o uskutečněných aktivitách. Logy mohou v trestním řízení prokázat, že se trestný čin (nebo souslednost událostí) stal. Nepřímo také ukazují, kdo trestný čin spáchal, protože součástí logu může být například síťový identifikátor zařízení (IP adresa), identifikátor zařízení přidělený výrobcem (MAC adresa) nebo přihlašovací údaj uživatele (login). Aby se jednalo o důkazy nade vši pochybnost, je nutné logy doplnit o další důkazy a svědectví (záznam o pracovní docházce, svědectví kolegů, záznam o přístupu do kanceláře, kamerový záznam[19], atp.).

[17] §89 odst. 2 zák. č. 141/1961 Sb.
[18] §89 odst. 1 zák. č. 141/1961 Sb.
[19] Kamerový záznam bude dostupný v případech vyšetřování počítačové kriminality pouze vzácně. Držení kamerového záznamu bývá přiměřeně dlouhé, obvykle v řádech dnů (45 dní držení kamerových záznamů v celních skladech je považováno za velmi dlouhé z pohledu ochrany osobních údajů. Je dlouhé také z hlediska velikosti potřebného úložiště pro uložení záznamů). Naproti tomu je průměrná doba identifikace ztráty dat v organizaci 197 dní (studie Ponemon institutu z roku 2019 na objednávku IBM), proto záznamy z doby, kdy incident nastal zřejmě již nebudou dostupné.

2.2 Trestní zákoník a kybernetická kriminalita

Zákon č. 40/2009 Sb. trestní zákoník obsahuje 49 paragrafů postihujících skutkovou podstatu trestných činů, jejichž znaky mohou být naplněny kybernetickým útokem. (Kolouch, 2016, s.339). Trestné činy zaměstnance vůči datům zaměstnavatele jsou řešeny v trestním zákoníku především paragrafy:

- §182 – porušení tajemství dopravovaných zpráv,
- §230 – neoprávněný přístup k počítačovému systému a nosiči informací,
- §231 – opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat a
- §232 - poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.

2.2.1 Porušení tajemství dopravovaných zpráv

Trestní zákoník §182 odst. 5 se týká správců počítačového systému, kteří mohou mít a velice často mají přístup k datům posílaným prostřednictvím sítě elektronické komunikace, především při správě e-mailových účtů ostatních zaměstnanců. Prozrazení nebo editace obsahu e-mailové komunikace je porušením článku 13 Listiny základních práv a svobod.[20]

Do této oblasti je možné zahrnout také sledování internetového provozu konkrétního zaměstnance na síťových zařízeních, které takové sledování umožňují (např. rozšifrováním obsahu komunikace pro jeho kontrolu jako ochrana před škodlivým kódem – malware).

[20] *„Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.“* (čl. 13 zákona 2/1993 Sb.)

2.2.2 Neoprávněný přístup k počítačovému systému a nosiči informací

Z detailně rozebíraných paragrafů v této práci je §230 ve svém rozsahu nejobsáhlejší a týká se všech zaměstnanců. Především odstavec 2 by měl být v organizacích zaměstnancům vhodným způsobem připomínán. Jeho úvodní textaci „kdo získá přístup“ vysvětluje usnesení Nejvyššího soudu České republiky takto:

> „*Získáním přístupu se rozumí takové jednání, které umožní pachateli volnou dispozici s počítačovým systémem nebo nosičem informací a využití jeho informačního obsahu. Získat přístup k počítačovému systému nebo nosiči informací lze neoprávněně, ale i oprávněně. Nezáleží na důvodu, který vedl k získání přístupu (může to být náhoda, plnění pracovních úkolů, využití počítače pro zábavu, odcizení nosiče informací atd.).*“ (Nejvyšší soud ČR, 2017)

Neoprávněné užití a smysl §230 popisuje v jednom ze svých rozsudků Nejvyšší soud České republiky takto:

> *„Za neoprávněné užití uložených dat lze považovat takové jejich užití, které je v rozporu s právní normou nebo je činěno v rozporu se stanoveným účelem, popř. bez vědomí či souhlasu oprávněné osoby. Předmětem ochrany tohoto přečinu je primárně integrita a dostupnost počítačových dat a systémů, ochrana je poskytována počítačovým datům a počítačovým programům před neoprávněnými zásahy, které mohou mít vliv na existenci, kvalitu, správnost dat, a ustanovení chrání i před neoprávněným užíváním uložených počítačových dat. Neoprávněným užitím dat (neboli počítačovou špionáží) je jakákoli nedovolená manipulace s daty uloženými v počítačovém systému nebo na nosiči informací. Neoprávněné bude takové užití, které je v rozporu s právní normou nebo je činěno v rozporu se stanoveným účelem, popř. bez vědomí či souhlasu oprávněné osoby.“* (Nejvyšší soud ČR, 2017)

2.2.3 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

Zpřístupnění přístupových prostředků do elektronických sítí (hesla, získání „dalších faktorů“ více faktorové autentizace) podle §231 je častým problémem a praxí v mnoha organizacích, často pro potřeby řešení zástupnosti nebo pohodlnosti zaměstnanců. Trestný čin požaduje kumulativní naplnění znaků. Zatímco na straně předávajícího lze najít znak nabídky[21] zřejmě bude nedokazatelné v rámci výše zmíněné praxe dokázat úmysl spáchat trestný čin Podle TrZ § 182 odst. 1 písm. b), c) (porušení tajemství dopravovaných zpráv) nebo § 230 odst. 1, 2 (překonání překážky a neoprávněný přístup k datům).

2.2.4 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

Uplatňuje se pouze při způsobení alespoň značné škody na majetku zaměstnavatele (tj. nejméně za 500.000 Kč) a to hrubou nedbalostí[22] §232 odst. 1 zák. č. 40/2009 Sb. říká, že *„porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté“*. Tyto povinnosti jsou obvykle stanoveny na základě zák. č. 262/2006 Sb., zákoník práce, §301 písm. d) (řádně hospodařit s prostředky svěřenými zaměstnavatelem) a §302 písm. g) (zabezpečovat přijetí opatření k ochraně majetku zaměstnavatele), nebo vyplývají z §316 (zákaz využívání výpočetní techniky zaměstnavatele pro svou osobní potřebu). O hrubou nedbalost se bude jednat „*zejména, jestliže byl pachatel opakovaně na riziko vyplývající z jeho činnosti upozorněn nebo byl o možném riziku řádně proškolen nebo už mu byl v minulosti nesprávný postup při zacházení s počítačem vytčen apod*.“ (Šámal, 2010, s. 2105)

---

[21] „*Nabídka je jakékoli předložení přístupového zařízení, které má za cíl, aby si jej jiný převzal. Proč má dojít k převzetí, není důležité (prodej, směna, darování, výpůjčka). Nezáleží na tom, zda jiná osoba nabídku přijme;*“ Komentář s trestnímu zákoníku, (Šámal, 2010, s. 2099)

[22] „Trestný čin je spáchán z hrubé nedbalosti, jestliže přístup pachatele k požadavku náležité opatrnosti svědčí o zřejmé bezohlednosti pachatele k zájmům chráněným trestním zákonem.“ zák. č. 40/2009 Sb. §16 odst. 2

2.3 Úskalí získávání elektronických záznamů o činnosti zaměstnance

Rozsudek Nejvyššího soudu ČR:

> „*Při hodnocení důkazů po stránce jejich zákonnosti zkoumá soud, zda důkazy byly získány/opatřeny a provedeny způsobem odpovídajícím zákonu nebo zda v tomto směru vykazují vady (zda jde o důkazy zákonné či nezákonné); k důkazům, které byly provedeny v rozporu s obecně závaznými předpisy, soud nepřihlédne.*“ (Nejvyšší soud ČR, 2007)

> *„Nejvyšší soud proto již dříve (za právní úpravy účinné před 1. 1. 2014) dospěl k závěru, že navrhne-li účastník občanského soudního řízení k prokázání svých tvrzení důkaz, který byl pořízen nebo účastníkem opatřen v rozporu s obecně závaznými právními předpisy a jehož pořízením nebo opatřením došlo k porušení práv jiné fyzické nebo právnické osoby, soud takový důkaz jako nepřípustný neprovede (srov. rozsudek Nejvyššího soudu ze dne 21. 10. 1998 sp. zn. 21 Cdo 1009/98 uveřejněný pod č. 39 ve Sbírce soudních rozhodnutí a stanovisek, roč. 1999).“*
> (Nejvyšší soud ČR, 2018)

Zaměstnavatel je při získávání elektronických důkazů o činnosti zaměstnance limitován dodržováním platných zákonů. Vztah zaměstnance a zaměstnavatele je upraven zákoníkem práce, který významným způsobem chrání zaměstnance v nerovnovážném závislém postavení vůči zaměstnavateli.[23] Zákoník práce nařizuje:

> „*Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.*“[24]

[23] „Zásady zvláštní zákonné ochrany postavení zaměstnance, uspokojivých a bezpečných pracovních podmínek pro výkon práce, spravedlivého odměňování zaměstnance, rovného zacházení se zaměstnanci a zákazu jejich diskriminace vyjadřují hodnoty, které chrání veřejný pořádek.“ (§1a odst. 2 zák. č. 262/2006 Sb).
[24] §316 odst. 2 zák. č. 282/2006 Sb.

Úřad pro ochranu osobních údajů vysvětluje pojem zvláštní povaha činnosti zaměstnavatele takto: „*Pod tím si lze představit například mezinárodní bankovní převody nebo dozor nad prací vězňů.*“ (ÚOOÚ, 2009) Takový popis by vedl k myšlence, že logování činnosti zaměstnanců v organizacích s jinou agendou je vyloučeno.

Tento odstavec umožňující narušení soukromí zaměstnance ze závažného důvodu spočívající ve zvláštní povaze činnosti zaměstnavatele je doplněn dalšíma dvěma odstavci. Odstavec první umožňuje přiměřeným způsobem kontrolovat dodržování zákonného požadavku nevyužívat pracovní prostředky výpočetní techniky pro svou osobní potřebu bez souhlasu zaměstnavatele. Třetí odstavec přidává povinnost „*přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění*“.[25]

Nezbytné je uvést, že log, který má být použitý jako důkaz o činnosti zaměstnance musí spojovat zařízení nebo konkrétní osobu s činností nebo řetězcem činností. Pokud bude log spojovat osobu s činností, bude tím naplňovat definici osobního údaje, kterým je informace o identifikované nebo identifikovatelné fyzické osobě.[26] Log tedy může být nebo je osobním údajem.

Ochranu osobních údajů řeší také Obecné nařízení o ochraně osobních údajů, které umožňuje provádět logování činnosti zaměstnanců jako „*zpracování nezbytné pro účely oprávněných zájmů příslušného správce*“[27].

Oprávněné zájmy správce v praxi zahrnují zákoníkem práce zmíněnou kontrolu dodržování zákonného požadavku nevyužívat pracovní prostředky výpočetní techniky pro svou osobní potřebu bez souhlasu zaměstnavatele, ale také kontrola neporušování autorského práva neoprávněnou instalací softwarových licencí, které nejsou legitimně zakoupené, a především sbírání logů za účelem vyšetřování a předcházení bezpečnostním událostem[28] a incidentům[29].

Tento zákonný důvod ke zpracování rozvádí dokument Evropského sboru pro ochranu osobních údajů, který uvádí, že:

---

[25] §316 odst. 3 zák. č. 282/2006 Sb.
[26] Článek 4 odst. 1 Nařízení 2016/679
[27] Článek 6 odst. 1 písm. f) Nařízení 2016/679
[28] „Událost, která může způsobit nebo vést k narušení informačních systémů a technologií a pravidel definovaných k jeho ochraně (bezpečnostní politika).“ (Jirásek et al., 2013, s. 23)
[29] „Jednotlivá nežádoucí nebo neočekávaná událost bezpečnosti informací nebo série neočekávaných událostí bezpečnosti informací, které mohou s významnou pravděpodobností ovlivnit operace související s činností organizace a ohrožení bezpečnosti informací.“ (ISO 27000, 2020, s.10)

„*Pokud se zaměstnavatel hodlá opřít o zákonný důvod podle článku 7 písm. f) Směrnice o ochraně údajů*[30]*, pak účel zpracování musí být oprávněný a zvolená metoda nebo konkrétní technologie zpracování musí být nezbytná pro naplnění oprávněného zájmu zaměstnavatele. Zpracování také musí být proporcionální vzhledem k podnikatelským potřebám, tj. odpovídat danému účelu. Zpracování dat na pracovišti by mělo být prováděno co možná nejméně vtíravým způsobem a být zaměřeno na specifickou rizikovou oblast. Navíc při využití článku 7 písm. f) zůstává zaměstnanci právo na námitku vůči zpracování ze závažných a legitimních důvodů, jak je stanoveno v článku 14.*“ (Pracovní skupina podle článku 29, WP249, 2017, s.6)

Úřad pro ochranu osobních údajů označuje údaje z logů (zaznamenávající historii navštívených stránek, historii uskutečněných hovorů, údaje spojené s používáním elektronické pošty, údaje o zařízení používaných zaměstnancem) jako údaje vysoce osobní povahy (ÚOOÚ, 2020).

Z výše citovaného textu a metodiky Úřadu pro ochranu osobních údajů lze dovodit, že je pravděpodobné, že zpracování logů bude mít za následek vysoké riziko pro práva a svobody fyzických osob. Zaměstnavatel proto musí vypracovat posouzení vlivu na ochranu údajů a stanovit na základě metodiky[31], zda bude mít zpracování osobních údajů skutečně za následek vysoké riziko pro práva a svobody zaměstnanců (Pracovní skupina podle článku 29, WP248, 2017). Tento test proporcionality má za úkol posoudit nezbytnost přiměřenost takového zpracování z hlediska účelu (v tomto bodě se může opírat také o §1a odst. 1 písm. d) zákoníku práce[32], povinnost řádného hospodaření[33],

[30] Zde myšlena měrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, Úř. věst. L 281, 23.11.1995, s. 31–50, dostupná na: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:31995L0046

[31] Např. Metodika obecného posouzení vlivu na ochranu osobních údajů, dostupná na: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=46487

[32] „Smysl a účel ustanovení tohoto zákona vyjadřují i základní zásady pracovněprávních vztahů, jimiž jsou zejména řádný výkon práce zaměstnancem v souladu s oprávněnými zájmy zaměstnavatele.“ (§1a odst. 1 písm. d) zákona č. 262/2006 Sb.)

[33] „Kdo přijme funkci člena voleného orgánu, zavazuje se, že ji bude vykonávat s nezbytnou loajalitou i s potřebnými znalostmi a pečlivostí. Má se za to, že jedná nedbale, kdo není této péče řádného hospodáře schopen, ač to musel zjistit při přijetí funkce nebo při jejím výkonu, a nevyvodí z toho pro sebe důsledky.“ (§159 odst. 1 zákona č. 89/2012 Sb.)

odpovídající judikaturu[34], případně o zákony vyžadující sběr elektronické evidence) na straně jedné a riziky pro zaměstnance na straně druhé.[35]

[34] „*Pojem péče řádného hospodáře lze přitom chápat tak, že řádný hospodář činí právní úkony týkající se obchodní společnosti odpovědně a svědomitě a stejným způsobem rovněž pečuje o její majetek, jako kdyby šlo o jeho vlastní majetek. Taková péče tedy nepochybně zahrnuje péči o majetek akciové společnosti nejen v tom smyslu, aby nevznikla škoda na majetku jeho úbytkem či znehodnocením, ale také, aby byl majetek společnosti zhodnocován a rozmnožován v maximální možné míře, jaká je momentálně dosažitelná*." (Usnesení č. 5 Tdo 1412/2007)

[35] Článek 35 Nařízení 2016/679

3 Požadavky na ochranu logů

Opatření vedoucí k prokázání důvěrnosti a integrity logů jsou dvojího typu:

1. procesní, např. neslučitelnost rolí, řízení přístupu, povinnost outsourcovat správu zařízení schraňujícího logy) a
2. technická, např. logování/nahrávání činnosti administrátorů, případně opatřování logy některým z prvků zajištujícím důvěru (elektronický podpis, pečeť, časové razítko).

Kombinací těchto opatření (ideálně v certifikovaném prostředí – např. dle norem z oblasti bezpečnosti informací řady ISO/IEC 27000) organizace buduje úroveň bezpečnosti, která má odpovídat cílům a potřebám organizace.

Tyto požadavky jsou pro přehlednost rozděleny na legislativní (ve smyslu legislativy České republiky a Evropské Unie) a požadavky norem, mezinárodních úmluv, případně zákonů jiných zemí, které jsou v oblasti bezpečnosti informací standardem nebo se k nim přihlíží.

3.1 Legislativní požadavky na ochranu logů

„*Oblast kybernetické bezpečnosti je a bude jedním z určujících aspektů bezpečnostního prostředí České republiky. Všechny vyspělé země, mezi něž se Česká republika bezesporu patří, jsou již zcela závislé na správném fungování informačních a komunikačních systémů.“* (Kolouch & Bašta, 2019, s.131)

Česká legislativa není v problematice ochrany logů příliš konkrétní, zákony neupravují ani konkrétní požadavky na elektronické důkazy. Přesto je zde několik opěrných bodů pro návrh opatření.

3.1.1 Zákon o elektronických komunikacích

Obvyklé jsou logy využívány jako důkazní materiál na základě zákona č. 127/2005 Sb. o elektronických komunikacích. Požadavek „*uchovávat po dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb*

elektronických komunikací“[36] je doplněn povinností, aby provozní a lokalizační údaje „*měly stejnou kvalitu a podléhaly stejnému zabezpečení a ochraně před neoprávněným přístupem, změnou, zničením, ztrátou anebo odcizením nebo jiným neoprávněným zpracováním nebo využitím*“[37] jako je chráněna poskytovaná služba. Proto musí organizace vytvořit „*vnitřní technicko-organizační předpis; ochranu údajů zajistí s ohledem na stávající technické možnosti a na náklady potřebné k zajištění ochrany na úrovni odpovídající existujícímu riziku porušení ochrany*“.[38]

V prováděcích předpisech[39] konkrétně vyhl. č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, je v §2 popsána požadovaná struktura (obsah) provozních údajů včetně jmenné konvence, nejsou zde ale popsány konkrétní technické parametry (požadavky) na důvěryhodnost předložených údajů. V praxi se pak na takto poskytnuté údaje pohlíží jako na důvěryhodné.

3.1.2 Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti určuje jako technické opatření „*nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů*“[40]. Jeho prováděcí vyhláška o kybernetické bezpečnosti definuje požadavky na obsah jednotlivých logů a také seznam činností, které mají být (v informačním systému) logovány[41]. Ani zde není konkrétní popis opatření na zabezpečení důvěrnosti a integrity logů na rámec vyhodnocení v rámci analýzy rizik a přijetí opatření na snížení rizika na přijatelnou úroveň, což je postup zcela v souladu s kapitolami 8.2 a 8.3 mezinárodního standardu ISO 27001.

3.1.3 Zákon o ochraně utajovaných informací

---

[36] §97 odst. 3 zák. č. 127/2005 Sb.,
[37] §88a odst. 1 zák. č. 127/2005 Sb.
[38] §88a odst. 2 zák. č. 127/2005 Sb.
[39] Seznam prováděcích předpisů dostupný zde: https://www.mpo.cz/cz/e-komunikace-a-posta/elektronicke- komunikace/narodni-legislativa-a-predpisy/provadeci-pravni-predpisy-k-zakonu-o-elektronickych- komunikacich--37748/
[40] §5 odst. 3 písm. f) zák. č. 181/2014 Sb.
[41] §22 vyhl. č. 82/2018 Sb.

Více konkrétní jsou požadavky prováděcího předpisu vyhl. č. 523/2005 Sb. o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi zákona č. 412/2005 Sb. o ochraně utajovaných informací, který požaduje:

> „*nepřetržité zaznamenávání událostí, které mohou ovlivnit bezpečnost informačního systému do auditních záznamů a zabezpečení auditních záznamů před neautorizovaným přístupem, zejména modifikací nebo zničením. Zaznamenává se zejména použití identifikačních a autentizačních informací, pokusy o zkoumání přístupových práv, vytváření nebo rušení objektu informačního systému nebo činnost autorizovaných subjektů informačního systému ovlivňující bezpečnost informačního systému*“.[42]

Ochrana auditních záznamů před modifikací nebo zničením je ve vyhlášce zmíněna celkově 3x[43].

3.1.4 Občanský zákoník

I zákon č. 89/2012 Sb. občanský zákoník se drží uvedené dikce, když v souvislosti se záznamy údajů o právním jednání v elektronickém systému říká, “*že záznamy údajů o právních jednáních v elektronickém systému jsou spolehlivé, provádějí-li se systematicky a posloupně a jsou-li chráněny proti změnám*“[44], ale bez upřesnění, jakým způsobem mají být proti změnám záznamy chráněny.

3.1.5 Zákon o informačních systémech veřejné správy

Zákon č. 365/2000 Sb. o informačních systémech veřejné správy vznáší požadavek na vytvoření informační koncepce, potažmo skrze prováděcí vyhl. č. 529/2006 Sb. dokonce i provozní dokumentace, nicméně žádné detaily k logování nebo správě logů zde nejsou uvedeny, požadavky jsou obecného charakteru a vztažené k provozu informačních systémů provozovaných subjekty státní správy. Vyhl. č. 530/2006 Sb. tuto obecnost

---

[42] §7 odst. 1 písm. c) vyhl. č. 523/2005 Sb.
[43] §7 odst. 1 písm. c), §10 odst. 4, §23 odst. 8 vyhl. č. 523/2005 Sb.
[44] §562 odst. 2 zák. č. 89/2012 Sb.

potvrzuje v §4 písm. d) když říká, že „*bezpečnostní opatření uvedená provozní dokumentaci jsou v souladu s běžně užívanými postupy a opatřeními*“ bez uvedení potenciálních zdrojů těchto postupů a opatření.

Stejný zákon na druhé straně ukládá v rámci výkonu působnosti kontaktního místa veřejné správy způsobem umožňujícím vzdálený přístup (poskytovatelé CZECH POINT) podmínky uveřejněné ve Věstníku Ministerstva vnitra[45]. Mezi těmito podmínkami je v bodě 3.4 Bezpečnostních podmínek uvedeno: „*Žadatel má zaveden systém řízení bezpečnosti informací vybudovaný na základě standardu ISO/IEC 27001, nebo jiný systém vyhovující požadavkům informačního managementu bezpečnosti.*“ (Ministerstvo vnitra. 2020)

3.1.6 Vyhláška o uchovávání, předávání a likvidaci provozních a lokalizačních údajů

Požadavek na ochranu ve vyhlášce č. 357/2012 Sb. se netýká logů, ale provozních a lokalizačních údajů. Přesto je důležitý, protože se zabývá prokázáním autentičností. Autentičnost důkazu je velmi důležitá. Odst. 4 písm. a) §3 „*K prokázání autentičnosti žádosti a předávaných údajů se použije uznávaný elektronický podpis, nebo uznávaná elektronická značka.*“

3.1.7 Vyhláška o výkonu znalecké činnosti

Náhled na zákonné požadavky na složitou problematiku exspirace používaných certifikátů, která není v současné době uspokojivě vyřešena, dává vyhláška č. 503/2020 Sb. v druhém odstavci §49:

> „*Pokud certifikát, na kterém je založeno kvalifikované elektronické časové razítko, pozbyde platnosti před uplynutím doby, po kterou má znalec povinnost uchovat se všemi náležitostmi znalecký posudek podaný v elektronické podobě, opatří se znalecký posudek kvalifikovaným elektronickým časovým razítkem opakovaně.*“

[45] VMV čá. 107/2020 (část II)

3.1.8 Zákon o službách vytvářející důvěru pro elektronické transakce

Zákon č. 297/2016 Sb. vychází z přímo aplikovatelného Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

Zde článek 24 odst. 2 písm. f) a g) hovoří o používání důvěryhodných systémů k uchování dat, kde by „*záznamy a změny v uložených datech mohly provádět pouze oprávněné osoby*“, také „*bylo možnost ověřit pravost dat*“, proto také musí přijmout „*vhodná opatření proti padělání a odcizení dat*.“

Právní účinek elektronických časových razítek je pospán v článku 41 odst. 2 jako „*u kvalifikovaného elektronického časového razítka platí domněnka správnosti data a času, které udává, a integrity dat, s nimiž jsou toto datum a tento čas spojeny*.“ Článek 42 v odstavci 1 doplňuje, že kvalifikované časové razítko:

„*a) spojuje datum a čas s daty takovým způsobem, že aby byla přiměřeně zamezena možnost nezjistitelné změny dat;*

b) je založeno na zdroji přesného času, který je spojen s koordinovaným světovým časem; a

c) je podepsáno s použitím zaručeného elektronického podpisu, opatřeno zaručenou elektronickou pečetí kvalifikovaného poskytovatele služeb vytvářejících důvěru nebo označeno jinou rovnocennou metodou.“

Přílohy I a III pak obsahují popis kvalifikovaného certifikátu pro elektronické podpisy a elektronické pečetě.

3.2 Požadavky bezpečnostních standardů na ochranu logů

Mezinárodně používané a uznávané standardy (též normy, anglicky „standard“) bezpečnosti nebo bezpečnostní požadavky (anglicky „compliance“) dané odvětvím (bankovnictví, zdravotnictví) nebo jako zákonné požadavky slouží jako zdroj inspirace bezpečnostním manažerům po celém světě. Tyto požadavky jsou považovány za „best practice“ a přihlížejí k nim všechny organizace. Výhodou standardů a požadavků je jejich nezávislost na velikosti organizace nebo odvětví.

Všechna opatření spojená s informační bezpečností by měla vycházet ze tří hlavních pilířů:

1) cílů organizace,
2) rizik[46] organizace,
3) zákonných, smluvních a dalších požadavků na organizaci.

Na neplnění zákonných a smluvních požadavků lze v praxi pohlížet také jako na jedno z rizik, kdy náklady na splnění požadavků mohou převyšovat smluvní nebo zákonnou pokutu, a tudíž může být pro organizaci výhodnější tyto požadavky neplnit. Obecně pak organizace přijímá taková opatření, která jsou levnější než následky, kdyby opatření přijatá nebyla.

> „*Výběr opatření je závislý na organizačních rozhodnutích na základě kritérií pro přijetí rizika, možnosti ošetření rizika a obecného přístupu k řízení rizik platících pro organizaci, a měl by také podléhat veškeré příslušné národní a mezinárodní legislativě a nařízením. Výběr opatření závisí také na způsobu, jakým na sebe opatření vzájemně působí, aby poskytovala hloubkovou ochranu.“* (ISO 27002, 2014, s.8)

V následujících kapitolách budou popsány požadavky na logování jednotlivých standardů a požadavků.

3.2.1 ISO/IEC 27001

Jako cíl opatření je stanoveno zaznamenávání událostí a vytváření záznamů. V Příloze A je uvedeno 114 kontrol, se kterými se organizace musí při implementaci tohoto standardu vypořádat (buď je aplikovat nebo jejich neplnění zdůvodnit). Z těchto 114 kontrol se logování a monitorování týkají čtyři opatření v bodu 12.4.

Tabulka 1: Přehled požadavků normy ISO27001 na logování

A.12.4. Zaznamenávání formou logů a monitorování
Cíl: Zaznamenávat události a vytvářet záznamy

[46] Rizikem zde rozumíme „*účinek nejistoty na dosažení cílů*“ (Jirásek et al., 2013, s. 99) přičemž tento „*účinek je odchylka od očekávaného. Může být pozitivní, negativní nebo obojí a může řešit, vytvářet nebo vyústit v příležitosti nebo hrozby.“* (ISO 31000, 2018, s.9)

A.12.4.1	Zaznamenávání událostí formou logů	*Opatření* Musí být pořizovány, uchovávány a pravidelně přezkoumávány logy událostí zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací.
A.12.4.2	Ochrana logů	*Opatření* Prostředky pro zaznamenávání formou logů a logy musí být chráněny proti zfalšování a neoprávněnému přístupu.
A.12.4.3	Logy o činnosti administrátorů a operátorů	*Opatření* Aktivity systémového administrátora a systémového operátora musí být logovány a logy chráněny a pravidelně přezkoumávány.
A.12.4.4	Synchronizace hodin	*Opatření* Hodiny všech důležitých systémů pro zpracování informací musí být v rámci organizace nebo bezpečnostních domén synchronizovány s jediným referenčním zdrojem času.

Zdroj: ISO 27001, 2014, s.19

Z těchto opatření lze za relevantní pro potřeby práce považovat body A.12.4.2 a A.12.4.4, nicméně norma ISO/IEC 27001 způsob naplnění nechává na organizacích. Organizace pak mohou inspiraci čerpat v normě ISO/IEC 27002.

3.2.2 ISO/IEC 27002

„*Tato mezinárodní norma je určena pro organizace k použití jako doporučení pro výběr opatření v rámci procesu zavádění systému řízení bezpečnosti informací (ISMS), založeného na normě ISO/IEC 27001*“ (ISO 27002, 2014, s.7)

Tato norma obsahuje pokyny k implementaci, které nemusí být za všech okolností zcela vhodné nebo dostačující, také nemusí splňovat cíle a požadavky organizace a neberou ohledy na právní aspekty nebo jiné normy, přesto je užitečné k těmto pokynům přihlížet, aby při návrhu bezpečnostních směrnic nebo pracovních postupů nebyly opomenuty důležité body nebo aspekty.

Kapitoly této normy respektují řazení opatření uvedených v Příloze A normy ISO 27001, tedy relevantní budou kapitoly 12.4.2 a 12.4.4. (kapitola 12.4.1 popisuje události, které by měly být logovány a kapitola 12.4.3 připomíná, že by měly být logovány všechny aktivity privilegovaných uživatelů).

Zatímco cíl opatření v kapitole 12.4 normy ISO/IEC 27001 je definován jako „*zaznamenávat události a vytvářet záznamy*“ (ISO 27001, 2014, s.19), norma ISO/IEC

27002 cíl definuje jako „*zaznamenávat události a generovat důkazy*“ (ISO 27001, 2014, s.44), z čehož je zjevný kvalitativní posun.

Kapitola 12.4.2 popisuje opatření v souladu s popisem v normě ISO/IEC 27001, pokyny k implementaci nepřekračují obecný popis ochrany proti:

a) *„změny typů zpráv, které jsou zaznamenány;*
b) *úpravy nebo vymazání souborů se záznamy;*
c) *překročení kapacity média, obsahující soubor se záznamy formou logů.“* (ISO 27002, 2014, s.44)

V této kapitole je nicméně odkaz na kapitolu 16.1.7 normy o shromažďování důkazů.

Kapitola 16.1.7 doporučuje stanovit postupy, které budou dodržovány při zacházení s důkazy a při jejichž tvorbě je potřeba brát v úvahu také bezpečnost důkazů. Uchování je zde definováno jako „*proces k udržení a zajištění integrity a původního stavu potenciálních důkazů*“ (ISO 27002, 2014, s.66), přičemž je nezbytné „*zvážit požadavky různých jurisdikcí s cílem maximalizovat šanci na přijetí* (důkazů – pozn. autora)“ (tamtéž) a dodává, že je „*vhodné zapojit právníka či policii hned na začátku jakéhokoliv zamýšleného právního řízení a poradit se o potřebných důkazech*.“ (tamtéž) Kapitola je zakončena odkazem na normu ISO/IEC 27037 Směrnice pro identifikaci, sběr, získávání a uchovávání digitálních důkazů.

Kapitola 12.4.4 uvádí, že je potřeba řádně dokumentovat přesnost času (ať již z interního nebo externího zdrojů) a dodává:

> „*Správné nastavení počítačových hodin je důležité pro zajištění přesnosti auditních záznamů, které mohou být vyžadovány pro vyšetřování nebo jako důkazy v soudním nebo disciplinárním řízení. Nepřesné auditní záznamy mohou bránit takovému vyšetřování a poškodit důvěryhodnost takového důkazu. Jako hlavní zdroj času pro systémy záznamů formou logu mohou být použity hodiny napojené na radiový signálů z národních atomových hodin. Síťový protokol pro synchronizaci času může být použit pro udržení synchronizace všech serverů s hlavními hodinami.*“ (ISO 27002, 2014, s.45)

3.2.3 ISO/IEC 27037

Norma je zaměřena na aktivity při správě potenciálních důkazů. Je určena organizacím, které chtějí chránit, zkoumat a využít potenciální digitální důkazy. „*Digitální důkazy jsou křehké ze své podstaty. Mohou být změněny, přepsány, nebo zničeni při nevhodné manipulaci nebo jejich zkoumání.*“ (ISO 27037, 2012, s.8) Proto je nezbytné zajistit integritu a jejich hodnověrnost. Norma doporučuje přihlížet ke specifickým požadavkům národních zákonných požadavků v této oblasti.

Norma zmiňuje tři základní principy spojené s digitálními důkazy:

1) Relevance – mělo by být možné prokázat, že předložené důkazy souvisí s vyšetřováním konkrétního incidentu.
2) Spolehlivost – všechny činnosti provedené s digitálními důkazy by měly být auditovatelné.
3) Dostatečnost – tyto důkazy by měly dostatečné, alespoň jako podklad, že se čin stal.

Norma klade velký důraz na ochranu integrity důkazů, tedy ochranu proti změně nebo přepsání a důvěrnost dat a zmiňuje nutnost zaznamenávat řetězec zpracování (chain of custody), který by měl obsahovat přinejmenším:

- „*identifikátor důkazu,*
- *kdo, kdy a kde měl přístup k důkazu,*
- *kdo a kdy vložil/vyjmul důkazy do/ze zařízení pro ukládání důkazů,*
- *jaké důkazy a proč (za jakým účelem) byly vyjmuté a kdo to schválil,*
- *u nevyhnutelných změn zaznamenat kdo změnu provedl, schválil a zdůvodnění této změny.*“ (ISO 27037, 2012, s.10)

V kapitole 7.1.4 zmiňuje požadavky na zachování sesbíraných důkazů. Doporučuje se využití různých funkcí digitálního podpisu pro určení, že digitální kopie jsou stejné jako originály. Dále je nezbytné aplikovat další bezpečnostní opatření pro zachovávání důvěrnosti, dostupnosti a integrity potenciálních digitálních důkazů.

V Příloze A je pak uveden souhrn znalostí a schopností osoby odpovědné za zpracování důkazů:

Tabulka 2: Příklady požadavků na odbornou roli pracovníka s důkazy

#			**Popis kompetence**

	Klíčové dovednosti	Popis klíčových dovedností	Povědomí	Znalosti	Dovednosti
4	Uchování digitálních důkazů	Aplikovat a hodnotit požadavky na uchování potenciálních digitálních důkazů, porozumět faktorům a parametrům ovlivňující jejich přesnost. Pokryté oblasti: metodologie, dodržení řetězce zpracování, manipulace s počítačovým zařízením, manipulace s digitálními paměťovými médii.	Rozumět požadavkům a procesům řetězce zpracování v souladu se zákonnými požadavky, dopady prostředí jako např. vlhkost, teplota nebo teplotní šoky na digitální zařízení; znalost požadavků na balení, transport a ukládání důkazů.	Znalosti získávání důkazních auditních dokumentů; definování parametrů dokument; znalost zásad informační bezpečnosti, hrozeb, zranitelností a kontrolních mechanismů pro digitální důkazy.	Prakticky aplikovat opatření pro ochranu digitálních důkazů, od velkých zařízení po ta nejmenší příruční zařízení; procesy spojené s dokumentováním důkazních materiálů.

Zdroj: ISO 27037, 2012, s.36

3.2.4 ISO/TR 15801

Jak již název napovídá, jedná se o technickou zprávu (technical report) a zabývá se ukládáním dat v elektronické formě. Dokument si klade za cíl „*popsat způsoby, kterými může být kdykoliv prokázána že informace, které byly vytvořené nebo jsou uložené v informačním systému nebyly změněny od svého vytvoření nebo importu do systému*.“ (ISO 15801, 2017, s.vii, překlad autor) a zároveň v předmluvě dodává, že „*kde by elektronicky uložené informace*[47] *měly být vyžádány soudem nebo při jiné nepříznivé*

[47] anglická zkratka ESI – electronically stored information

situaci, měly by implementátoři tohoto dokumentu vyhledat právní radu pro zajištění přesných požadavků v příslušném právním prostředí.“ (ISO 15801, 2017, s.vii, překlad autor)

Zároveň definuje **důvěryhodný systém** jako „*systém, který zajišťuje, že všechny elektronicky uložené informace spravované systémem lze považovat za originální informace nebo za skutečné a přesné kopie originálních informací, nezávisle na původním formátu*.“ (ISO 15801, 2017, s.5, překlad autor) Také určuje, že by takovéto elektronicky uložené informace měly být chráněny před změnou nebo neoprávněným smazáním a zároveň musí existovat možnost nezávislého auditu procesů spojených se správou elektronicky uložených informací v důvěryhodném systému. Důvěryhodnost systému elektronicky ukládaných informací spojuje se zachováním autenticity, integrity a dostupnosti. Pro každý důvěryhodný systém by měla být vedena dokumentace.

Doporučuje zavést oddělení rolí, alespoň pro oblasti určení vstupních dat, kontrolu kvality, vkládání dat, mazání dat a bezpečnost informací.

Při přenosu informací by mělo být zváženo použití digitálního podpisu.

> „*Hashování, digitální podpisy, pečeti nebo časová razítka, například, mohou být použity k potvrzení, že elektronicky/digitálně podepsaná elektronicky uložená informace je naprosto přesně stejná jako odeslaná informace a pro potvrzení identity odesílatele. Potvrzení identity může být kompromitováno, pokud originální certifikát již není platný a udržovaný certifikační autoritou. Pokud certifikát elektronického/digitálního podpisu již není k dispozici nebo vypršela jeho platnost, poskytuje digitální podpis pouze informaci, zda byla elektronicky uložená informace (ne)změně pouze po dobu platnosti podpisu.*“ (ISO 15801, 2017, s.24, překlad autor)

Pro další snížení rizika v průběhu přenosu by měl příjemce potvrdit odesílateli přijetí zprávy. Toto potvrzení by mělo obsahovat potvrzení identifikaci transakce a identifikaci odesílatele. Jiným vhodným přístupem je použití kontrolního součtu (checksum) nebo výpočet hash po přijetí elektronicky uložené informace. Tímto způsobem lze automatizovaně detekovat chyby při přenosu. Tuto hodnotu hashe lze zapsat do logu a log pak chránit. (7.5.1)

Další možností ověření shody je použití digitálního podpisu. „*Digitální a elektronický podpis použitý k prokázání neměnnosti elektronicky uložené informace by měl obsahovat*

kontrolní součet nebo hodnotu hashe vloženou do elektronicky uložené informace nebo uložená v zabezpečeném systému vázaném na původní elektronicky uložené informace.“ (ISO 15801, 2017, s.34, překlad autor)

V kapitole 6.15.2 připomíná, že se nesmí zapomenout na fakt, že oblast šifer a šifrovacích klíčů se stále dynamicky mění a je potřeba stále dbát na aktuálnost používaných šifer a jejich používání řídit.

Po obnovení dat ze zálohy je dle 6.13 nezbytné ověřit, že důvěryhodnost dat nebyla narušena po obnově elektronicky uložených informací.

Samozřejmostí je podle kapitoly 6.18 používání přesného času v organizaci, a to dokumentovaným způsobem.

Z pohledu práce nejzajímavější kapitola 8, která se zabývá přímo auditní stopou (kam logy spadají). „*Auditní stopy by měly obsahovat dostatečné a nezbytné informace které umožní prokázat důvěryhodnost řízených elektronicky uložených informací.*“ (ISO 15801, 2017, s.38, překlad autor) K těmto auditním stopám mohou vyžadovat přístup různé osoby – uživatelé, auditoři nebo představitelé zákonné moci. „*Auditní stopy by měly být, tak dalece jak je to možné, generovány automaticky systémem a v manuál popisující systém by měl být proces generování popsán. Nemělo by být možné přerušit nebo zastavit tvorbu auditních stop.*“ (tamtéž, překlad autor)

Datum a čas by měli být přiměřeně přesné, mělo by být uváženo použití důvěryhodného zdroje času.

Auditní stopy by měly být řízeny jako specifický typ dokumentu a měl by být uloženy alespoň tak dlouho, jako elektronicky uložená informace, ke které se vztahují a zabezpečeny. Uložené by měly být ve důvěryhodném systému (úložišti) a neměly by být upravitelné, ideálně na média určená pouze k zápisu (např. magnetické pásky).

3.2.5 HIPAA

Zákon Spojených států Amerických The Health Insurance Portability and Accountability Act of 1996 (zkráceně HIPAA nebo Kennedy-Kassebaum Act) slouží k ochraně osobních údajů ve zdravotních pojišťovnách, jeho účelem je zvýšit plynulost předávání informací mezi zdravotními pojišťovnami.

Relevantní je požadavek na auditní kontrolní mechanismy: „*Implementovat hardwarové, softwarové anebo procesní opatření, které nahrávají a zkoumají činnosti v informačních systémech, které obsahují nebo využívají elektronicky chráněné zdravotní informace*.“ (§ 164.312(b) HIPAA, 2012)

Tento požadavek je následně rozpracován v dokumentu NIST SP 800-66[48] do těchto klíčových oblastí:

1) „*Určit oblasti, které mají být sledovány nebo auditovány.*
2) *Vybrat vhodné nástroje určené pro auditní záznamy a přehled systémových aktivit.*
3) *Vypracovat a nasadit politiku logování informačního systému.*
4) *Vypracovat vhodné provozní postupy.*
5) *Implementovat metodiku kontroly logů.“* (NIST 800-66 Revision 1, 2008, s.42)

3.2.6 FISMA

The Federal Information Security Management Act (zkráceně FISMA) je III. hlavou zákona Spojených státu Amerických E-Government Act (Public Law 107-347). FISMA z roku 2002 požaduje po federálních agenturách a jejich dodavatelích zavedení informační bezpečnosti pro ochranu informačních systémů, procesů a majetku agentur. Tento zákon byl aktualizován v roce 2014 The Federal Information Security Modernization Act of 2014 a upřesnil požadavky ve věci bezpečnostních incidentů.

Bezpečnostní požadavky jsou shrnuty v dokumentu NIST SP 800-53[49] Třetí kapitola se týká právě auditu a přičitatelnosti (audit and accountability) a shrnuje požadavky na obsah auditních záznamů (AU-3), řízení chyb v průběhu logování (AU-5), časová razítka (AU-8), ochrana auditních informací (AU-9), průkaznost (AU-10), generování auditních záznamů (AU-12).

Ochrana auditních informací (AU-9) má popsaná následující kontrolní doporučení:

1) Zápis na média, která nelze přepisovat,
2) Fyzické oddělení systému, který je zdrojem logu a úložiště logu

[48] National Institute of Standards and Technology Special Publication 800-66, Revision 1
[49] National Institute of Standards and Technology Special Publication 800-53, Revision 5

3) Kryptografická ochrana
4) Omezení přístupu uživatelů
5) Zavedení dvojí autorizace
6) Omezit přístupy k logům v režimu pouze ke čtení
7) Uložení logů na zařízení s jiným operačním systémem, než má zařízení, které je logováno

3.2.7 PSD2

Evropská směrnice PSD 2[50] je do české legislativy transponována do zákona č. 370/2017 Sb. o platebním styku. Jakkoliv tato směrnice řeší bezpečnost především z pohledu bezpečného ověření uživatele, přesto v článku 72 uvádí povinnost logovat:

> „*Členské státy vyžadují, aby v případě, že uživatel platebních služeb popírá, že provedenou platební transakci autorizoval, nebo tvrdí, že platební transakce nebyla provedena správně, musel poskytovatel platebních služeb poskytnout doklad o tom, že platební transakce byla ověřena, přesně zaznamenána, zanesena do účetnictví a že nebyla ovlivněna technickým selháním nebo jiným nedostatkem služby poskytnuté poskytovatelem platebních služeb*.“ (PSD2, 2015, čl. 72 odst. 1)

3.2.8 EBA

Evropská bankovní autorita (EBA) ve svých Obecných pokynech Evropského orgánu pro bankovnictví pro řízení rizik v oblasti IKT[51] a bezpečnosti uvádí pro logování v článku 52 tento požadavek: „*Finanční instituce by měly u kritických částí provozu IKT zavést postupy logování a sledování, které umožní odhalit, analyzovat a opravit chyby.“* (Evropská bankovní asociace, 2017, str. 16)

3.2.9 PCI DSS

Standard PCI DSS (Payment Card Industry Data Security Standard) slouží k sjednocení bezpečnostních požadavků pro zabezpečení platebních karet po celém světě. Vztahuje se

[50] Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25.listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2020/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES
[51] Informačních a komunikačních technologií

na také na všechny zpracovatele dat držitelů karet nebo citlivých autentizačních dat. Tento standard obsahuje konkrétní požadavky na zavedení bezpečnostních opatření.

Opatření vztahující se ke sledování všech přístupů uvnitř sítě a k datům držitelů karet jsou ve verzi 3.2.1 uvedeny v kapitole 10. Standard požaduje:

zaznamenávat všechny přístupy všech uživatelů v systému,

- mít logy, které umožní rekonstruovat vyjmenované události (přístup k datům držitelů karet, všechny činnosti administrátorů, přístup k logům, neúspěšné pokusy o přístup, změny v nastavení uživatelů, změny v logování, změny v systémových objektech),
- co má logový záznam obsahovat (identifikaci uživatele, typ události, datum a čas, úspěch či neúspěch provedení akce, zdroj události, název systému),
- že je nezbytné využívat technologii synchronizování času,
- zabezpečit auditní stopy (logy) před jejich změnou, omezit přístup osob k auditním logům, zálohovat logy do centrálního úložiště (log serveru), logy z technologiích na perimetru ukládat do centralizovaného zdroje, používat nástroj pro kontrolu integrity souborů,
- průběžně, alespoň denně, kontrolovat logy, vyhledávat v nich anomálie,
- ukládat auditní záznamy alespoň po dobu jednoho roku,
- ukládat selhání vyjmenovaných technických zařízení.

4 Politika zachování autenticity logů

Politika autenticity logů sleduje životní cyklus logů od jejich vzniku do jejich použití jako přípustného soudního důkazu. Tato politika neřeší komplexní zabezpečení logů (např. jejich dostupnost), přesto alespoň v obecné rovině postihuje procesy a politiky navázané na hlavní činnosti této politiky. „*Je nutné mít na paměti, že žádný soubor opatření nemůže docílit úplnou bezpečnost informací*.“ (ISO 27000, 2002, s.22)

Aby bezpečnost byla prokazatelná, je nezbytné, aby měla organizace zavedenou politiku bezpečnosti informací, která bude vycházet z cyklu stálého zlepšování (P-D-C-A cyklus nebo též Demingův cyklus). „*Opatření bezpečnosti informací by měla být zvažována ve stádiu specifikace a návrhu požadavků systémů a projektů. Jestliže se opomene, výsledkem mohou být dodatečné náklady a méně efektivní řešení, a v nejhorším případě i nemožnost dosáhnout adekvátní bezpečnosti*.“ (tamtéž)

4.1 Před vznikem logu

Před vznikem logu je potřeba zaměřit zvážit a určit následující:

4.1.1 Zdroj a forma logu

Které činnosti a proč budou zaznamenávány na zdroji (zde bez rozlišení, jestli se jedná o informační systém, počítač, server nebo jinou technologii) je potřeba řádně zdůvodnit. Cílem diskuse je „*zdůvodnit, proč jsou vybrané události dostatečné pro podporu vyšetřování bezpečnostních incidentů*“ (Landoll 2016, s.184). Zároveň s problematikou, co bude logováno je nezbytné definovat jaké záznamy by log měl obsahovat.

Problematiku řeší např. ISO 27002 12.4.1; NIST 800-53 AU-2, AU-3; NIST 800-66 4.15; PCI DSS 10.2, 10.3 nebo §22 odst. 2 vyhl. č. 82/2018 Sb.

4.1.2 Doba uložení logu

Stanovovat délku držení logů je nezbytné v součinnosti s vlastníkem aktiva (někde také garant aktiva[52]) protože požadavky se budou lišit v závislosti na smluvních, zákonných a bezpečnostních požadavcích. Např. záznamy o přístupu k záznamům pacienta budou drženy déle než záznam o vnitřní teplotě procesoru zařízení. Tato netriviální činnost musí být řádně dokumentována, a především pravidelně procházet revizí, ideálně v jednoletém cyklu. Minimální doporučovaná délka je uváděna jako jeden rok[53]

Problematiku řeší např. PCI DSS 10.7, §22 odst. 3 a 4 vyhl. č. 82/2018 Sb., NIST 800-53 AU-11.

4.1.3 Nastavení zdroje času

Nezbytnou podmínkou pro možnost vyšetřování bezpečnostních událostí a incidentů je používat v celé síti stejný zdroj času. Organizace by jako ideální zdroj přesného času měla používat time server[54] ať již formou dedikovaného zařízení nebo určením konkrétního zařízení jako zdroje referenčního času (včetně určení časové zóny) pro zařízení organizace. Všechna zařízení v organizaci by se měla synchronizovat s time serverem alespoň jednou za 24 hodin[55] Změny času může provádět výhradně administrátor a všechny takové činnosti musí být logovány[56].

Problematiku řeší např. PCI DSS 10.8, §22 odst. 2 písm. e) vyhl. č. 82/2018 Sb., NIST 800-53 AU-8.

4.1.4 Nastavení logování

Logování v organizaci nastavuje systémový administrátor podle instrukcí výstupů kapitoly „zdroj a forma logu“, kterou v ideálním případě nastavuje bezpečnostní tým (bezpečnostní manažer), u malých firem pak IT oddělení ve spolupráci se zástupcem vedení. Kontrolu nastavení provádí bezpečnostní tým nebo externí konzultant zastupující vedení.

---

[52] „*Garant aktiva je bezpečnostní role odpovědná za zajištění rozvoje, použití a bezpečnost aktiva.“* (§7 odst. 3 vyhl. č. 82/2018 Sb.)
[53] PCI DSS 10.7, §22 odst. 4 vyhl. č. 82/2018 Sb. u významných informačních systémů
[54] Jedná se o server, který poskytuje v interní síti přesný čas, který průběžně aktualizuje, obvykle přes GPS, radiový signál, atomové hodiny nebo časové služby na internetu.
[55] Požadavek §22 odst.2 písm. e) vyhl. č. 82/2018 Sb.
[56] Požadavek PCI DSS 10.4.2

4.2 Ochrana logu při komunikaci

Každé zařízení generující logy musí být nastaveno, aby posílalo vygenerované logy do centrálního úložiště logů. Organizace musí prokázat, že logy v průběhu komunikace nebyly změněné.

4.2.1 Šifrování komunikace

„*Asi nejznámějšími a nejvíce používanými kryptografickými protokoly v transportní vrstvě jsou protokoly TLS a protokol SSH.*“ (Burda, 2019, s.48) Pro posílání logů mezi zdrojem a úložištěm je nutné použít šifrovanou komunikaci. Pro tento účel je vhodné použít protokol TLS. Tento způsob šifrování je založen na symetrické šifře a ověřuje, zda dorazila zpráva celá a nepoškozená. Šifrování pak stěžuje případné útoky na komunikaci (např. man in the middle attack).

Je nezbytně nutné používat aktuální verze šifrovacích algoritmů, nyní verze 1.2 a 1.3 (v souladu s politikou řízení kryptografie), zdrojem může být například doporučení Národního Úřadu pro kybernetickou a informační bezpečnost dostupného na webových stránkách[57] nebo publikace NIST SP 800-52 Revision 2[58].

4.3 Centrální úložiště logů

Jako centrální úložiště logů lze v organizaci využít specializovaný nástroj na správu logů, které jsou dostupné v placených i open source verzích. Nad tímto úložištěm jsou v organizacích budovány nadstavby v podobě SIEM (Security Information and Event Management) nástrojů. Ani jedno není pro potřeby zachování důvěryhodnosti logů potřebné, jakkoliv jsou to nepopiratelně užitečné nástroje, pokud jejich potenciál umí organizace využít.

[57] Dostupný na https://www.nukib.cz/download/uredni_deska/Kryptograficke_prostredky_doporuceni_v1.0.pdf
[58] Dostupný na https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

4.3.1 Elektronická pečeť

Pro potvrzení integrity logů je užitečné využít alespoň uznávaný (lépe kvalifikovaný) elektronický podpis, protože pouze takový podpis je uznávaný jako průkazný. Takový elektronický podpis je spojený s konkrétní osobou (právnické osoby pak využívají elektronickou značku) a je spojena s elektronickým dokumentem. K dokumentu také připojuje hash (otisk dokumentu, který umožňuje ověřit, zda (ne)došlo ke změně dokumentu). Vzhledem k tomu, že elektronický podpis využívá negarantovaný zdroj času, je zároveň pro prokázání časové souslednosti použít také časové razítko, které přidá k elektronicky podepsanému dokumentu také přesný čas. Kvalifikované (nebo alespoň uznávané) časové razítko je generováno mimo organizaci, je tedy nezbytné mít on-line přístup pro vytvoření časového razítka (právnické osoby využívají elektronickou pečeť).

„*Zdůrazněme si, že časové razítko neříká, jak dlouho již existuje to, co je časovým razítkem právě opatřováno. Elektronický podpis na dokumentu, ke kterému je připojováno časové razítko, mohl vzniknout jen o zlomky sekund dříve, ale stejně tak mohl vzniknout o mnoho hodin, dnů, týdnů či roků dříve. To z časového razítka není patrné.*“ (Peterka, 2011, s.77)

Problémem používání certifikátů je jejich exspirace. Certifikát pro elektronický podpis se obvykle vydává na 1 rok (certifikáty spojené s časovým razítkem pak na 3-5 let). Pokud certifikát exspiruje, pak jeho pravost nelze ověřit. To neznamená, že podepsaný dokument ztrácí platnost, přesto je potřeba tuto situaci řešit a v praxi se řeší časovým razítkem, které také vytváří hash, ale především prokazuje, že dokument daného hashe existoval před připojením časového razítka. Organizace proto musí dbát na včasné přerazítkovávání dlouhodobě uložených logů. Aby bylo vše průkazné, je potřeba dokument opatřit novým časovým razítkem ještě před exspirací certifikátu starého časového razítka.

4.3.2 Zabezpečení důvěrnosti centrálního úložiště logů

Centrální úložiště logů musí být šifrované, aby bylo chráněno před neoprávněnou změnou nebo neoprávněným přístupem. Držitelem klíče je Manažer kybernetické bezpečnosti. Držitelem šifrovacího klíče k centrálnímu úložišti logů nesmí být osoba odpovědná za správu tohoto úložiště (systémový administrátor), protože tímto způsobem by byl schopný upravovat logy, které sám svou činností vytváří.

Organizace definuje tzv. blok – tedy množinu logů v centrálním úložišti logů, která bude opatřena elektronickým podpisem a elektronickou pečetí. Tento blok může být definován velikostí (např. 1 GB logů) stejně jako časovým parametrem (např. logy za 24 hodin).

4.4 Řízení přístupových oprávnění

Přístupy k logům je umožněn pouze osobám, které přístup k nim potřebují pro výkon svého povolání, a to výhradně v režimu pro čtení. Nastavování centrálního úložiště logů by mělo probíhat za přítomnosti alespoň dvou osob – systémového administrátora a zástupce bezpečnostního oddělení, aby nemohlo dojít k zneužití administrátorských práv k neoprávněným změnám. Všechny činnosti systémového administrátora musí být logovány.

5 Závěr

Práce si stanovila jako cíl na základě prozkoumání současných právních požadavků na dokazování, logování a správy elektronických dokumentů společně s mezinárodními bezpečnostními standardy vytvořit Politiku zachování autenticity logů (tedy jejich důvěrnosti a integrity).

Navržená politika nebyla (zatím) v praxi vyzkoušena, žádná organizace ji neimplementovala, tedy ani nebyla zkoumána pro potřeby uznání důkazu. Důvody jsou ryze praktické – změna bezpečnostní politiky v organizacích je zdlouhavý, a především poměrně drahý proces (do ceny se započítává nejenom pořízení hardware a software, ale především čas zaměstnanců, který je spojený se zapracováním změn do stávajícího systému řízení bezpečnosti informací (ISMS), ale také edukací uživatelů, nastavováním všech v politice nastíněných nebo daných požadavků a kontrolou. Náklady na implementaci jsou proto v řádech stovek tisíc korun.

Nad rámec navržené politiky zachování autenticity práce také shrnuje další povinnosti organizace, které musí splnit z pohledu ochrany osobních údajů a pracovního práva, protože jejich nesplnění by mohlo vést k zamítnutí použití takových důkazů.

I Summary and keywords

The thesis deals with the issue of processing records of employee activities in organization's information systems. The aim of the thesis is to design organizational, procedural and technical measures that will allow the use of records of employee activities as admissible evidence in a dispute with an employee. To create a suitable policy, a methodology based on the procedures of implementing an Information Security Management System (ISMS) is used and an analysis of legislative requirements and requirements of internationally recognized standards such as ISO, FIPS, NIST for content, storage and security of logs is performed. The thesis also takes into account the requirements of the Personal Data Processing Act and the Labor Code. The output is a policy proposal that provides for chosen organization comprehensive solution for processing records while meeting all relevant requirements of the organization.

Key words: logs, log protection, confidentiality, integrity, judicial evidence, electronic records, record of activities

II Seznam použitých zdrojů

Monografie

Jirásek, P., Novák, L., & Požár, J. (2013). *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary* (2., aktualiz. vyd). Policejní akademie ČR v Praze, s.12, s. 93.

Kent, K., & Souppaya, M. (2006). *Guide to Computer Security Log Management: Recommendations of the National Institute of Standards and Technology*. National Institute of Standards and Technology.

Šámal, P. (2010). *Trestní zákoník: komentář*. C.H. Beck.

Kolouch, J. (2016). *Cybercrime.* CZ.NIC, z.s.p.o.

Kolouch, J., & Bašta, P. (2019). *CyberSecurity*. CZ.NIC, z.s.p.o.

Burda, K. (2019). *Kryptografie okolo nás*. CZ.NIC, z.s.p.o.

Peterka, J. (2011). *Báječný svět elektronického podpisu*. CZ.NIC, z.s.p.o.

WILLIAMS, Barry L. (2016). *Information security policy development for compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA standard, PCI DSS V2.0, and AUP V5.0*. Boca Raton, FL: CRC Press, Taylor & Francis Group

LANDOLL, Douglas J. 2016. *Information security policies, procedures, and standards: a practitioner's reference*. Boca Raton: CRC Press, Taylor & Francis Group

Právní předpisy a mezinárodní smlouvy

Zákon. č. 262/2006 Sb., zákoník práce, v aktuálním znění.

Usnesení č.2/1993 Sb., usnesení předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky, v aktuálním znění.

Zákon č. 141/1961 Sb. o trestním řízením soudním, v aktuálním znění.

Zákon č. 40/2009 Sb. trestní zákoník v aktuálním znění.

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

Zákon č. 89/2012 Sb. občanský zákoník, v aktuálním znění.

Zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů, v aktuálním znění.

Vyhláška č. 357/2012 Sb. o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, v aktuálním znění.

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů, v aktuálním znění.

Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, v aktuálním znění.

Vyhláška č. 523/2005 Sb. o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, v aktuálním znění.

Zákon č. 365/2000 Sb. o informačních systémech veřejné správy a o změně některých dalších zákonů, v aktuálním znění

Vyhláška č. 529/2006 Sb. o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy, v aktuálním znění

Vyhláška č. 530/2006 Sb. o postupech atestačních středisek při posuzování dlouhodobého řízení informačních systémů veřejné správy, v aktuálním znění

Vyhláška č. 357/2012 Sb. o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, v aktuálním znění

Vyhláška č. 503/2020 Sb. o výkonu znalecké činnosti

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES

Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce, v aktuálním znění

The Health Insurance Portability and Accountability Act of 1996 Public Law 104-191 104th Congress - An Act To amend the Internal Revenue Code of 1996 to improve

portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25.listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2020/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES

Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV

Rozhodnutí a stanoviska veřejných úřadů

Rozsudek Nejvyššího soudu ze dne 20. 12. 2007, sp. zn. 21 Cdo 360/2006, ECLI:CZ:NS:2007:21.CDO.360.2006.1

Rozsudek Nejvyššího soudu ze dne 22. 8. 2017, sp. zn. 21 Cdo 3635/2016, ECLI: ECLI:CZ:NS:2017:21.CDO.3635.2016.1.

Stanovisko Úřadu pro ochranu osobních údajů č. 2/2009 dostupné online: https://www.uoou.cz/files/stanovisko_2009_2.pdf

Pracovní skupina podle článku 29, Stanovisko 2/2017 ke zpracování údajů na pracovišti, schváleno dne 8. června 2017 dostupné online: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

Pracovní skupina podle článku 29, Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679, přijaté dne 4.října 2017 v aktualizovaném znění, dostupné online: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Úřad pro ochranu osobních údajů, Seznam druhů zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů Verze 1.0, dostupné online: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940

Usnesení Nejvyššího soudu ze dne 27. 8. 2008, sp. zn. 5 Tdo 1412/2007, ECLI:CZ:NS:2008:5.TDO.1412.2007.1

Usnesení Nejvyššího soudu České republiky ze dne 13.12.2017, sp.zn. 5 Tdo 1085/2017, ECLI:CZ:NS:2017:5.TDO.1085.2017.1

Věštník Ministerstva vnitra, VMV čá. 107/2020 (část II), i. Podmínky pro udělení autorizace k výkonu kontaktního místa veřejné správy Czech POINT, dostupné online https://www.mvcr.cz/soubor/107vmv-pdf.aspx

Usnesení Nejvyššího soudu České republiky ze dne 23.8.2017, sp.zn. 5 Tdo 781/2017-23, ECLI:CZ:NS:2017:5.TDO.781.2017.1

Bezpečnostní normy a nařízení

ČSN EN ISO/IEC 27000:2020, Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Přehled a slovník, Česká agentura pro standardizaci, 2020

ČSN ISO 31000:2018, Management rizik – Směrnice, Česká agentura pro standardizaci, 2018

ČSN ISO/IEC 27001:2014, Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky, Česká agentura pro standardizaci, 2014

ČSN ISO/IEC 27002:2014, Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací, Česká agentura pro standardizaci, 2014

ČSN ISO/IEC 27037:2014, Informační technologie – Bezpečnostní techniky – Směrnice pro identifikaci, sběr, získávání a uchování digitálních důkazů, Česká agentura pro standardizaci, 2017

ISO/TR 15801:2017, Document management – Electronially stored Information – Recommendations for trustworthiness and reliability, ISO copyright office, 2017

National Institute of Standards and Technology Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, National Institute of Standards and Technology, 2020 https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology Special Publication 800-66, Revision 1, An Introductory Resource Guide for Implementing the Health Insurance Portability an Accountability Act (HIPAA) Security Rule, National Institute of Standards and Technology, 2008 http://dx.doi.org/10.6028/NIST.SP.800-66r1

Ostatní a internetové zdroje

Interpol, Global guidlines for digital forensics laboratories (s.13), dostupné online http://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

Evropská bankovní asociace, Obecné pokyny Evropského orgánu pro bankovnictví pro řízení rizik v oblasti IKT, dostupné online https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/Updated%20Translations/880808/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management_COR_CS.pdf

PCI Security Standards Council, LLC., Standard PCI DSS, dostupné online https://www.pcisecuritystandards.org/document_library

Úřad pro ochranu osobních údajů, Úřad k návrhu nařízení o soukromí a elektronických komunikacích, dostupné online https://www.uoou.cz/urad%2Dk%2Dnavrhu%2Dnarizeni%2Do%2Dsoukromi%2Da%2Delektronickych%2Dkomunikacich/d-49300

Hospodářské noviny, Pohled do továrny Tesly, vězení i nemocnic: hackeři získali přístup k tisícům bezpečnostních kamer, 10.3.2021, dostupné online https://tech.ihned.cz/internet/c1-66894460-pohled-do-tovarny-tesly-vezeni-i-nemocnic-hackeri-ziskali-pristup-k-tisicum-bezpecnostnim-kamer

E-ZU Solutions, 95% of Cyber Security Breaches are due to Human Error, 16.6.2020, dostupné online https://www.e-zu.co.uk/2020/06/16/95-of-cyber-security-breaches-are-due-to-human-error/

Enterpreneur, Eployee Are Your Weakest Link Against Cyberattacks. Don’t Put Them on the Front Lines, 29.1.2020, dostupné online https://www.entrepreneur.com/article/345638

III Seznam tabulek