

D1 – Metodika zmluvných vzťahov pri poskytovaní služieb digitálnej forenznej analýzy a reakcie na kybernetické incidenty



Projekt Automatizácia digitálnej forenznej analýzy a odpovede na incident (ADFIR) financovaný Európskou úniou – Next GenerationEU prostredníctvom Plánu obnovy a odolnosti Slovenskej republiky pod číslom projektu č. 09I05-03-V02-00079.

Obsah

1 Popis projektu.....	3
2 Úvod	3
2.1 Účel metodiky	3
2.2 Teoretické východiská digitálnej forenzej analýzy a reakcie na incident	6
2.3 Úloha KPB1.1.....	7
3 Zmluvné vzťahy pri poskytovaní digitálnej forenzej analýzy a reakcie na kybernetické incidenty	7
3.1 Fázy zmluvného vzťahu	8
3.1.1. Predzmluvná fáza	8
3.1.2. Uzatvorenie zmluvy	14
4 Prehľad.....	43
5 Zoznam použitej literatúry	46

1 Popis projektu

Projekt **Automatizácia digitálnej forenznej analýzy a odpovede na incident** (ďalej len „ADFIR“) je financovaný Európskou úniou – Next GenerationEU prostredníctvom Plánu obnovy a odolnosti Slovenskej republiky pod číslom projektu č. 09I05-03-V02-00079. Tento projekt sa zaoberá jednou z kľúčových výziev v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti – ako spracovať obrovské množstvo digitálnych dôkazov, ktoré vznikajú počas incidentov kybernetickej bezpečnosti alebo forezných vyšetrovaní. V súčasnosti je tento proces veľmi náročný z hľadiska ľudských zdrojov a času. Automatizácia pomocou metód strojového učenia môže preto výrazne **zlepšiť kvalitu digitálnej forenznej analýzy** a skrátiť čas potrebný na jej vykonanie. Celkovo to umožňuje bezpečnostným tímom efektívnejšie reagovať na kybernetické hrozby. Hlavné prínosy tohto projektu sú:

- **Rýchlejšie riešenie incidentov v oblasti kybernetickej bezpečnosti.** Projekt ADFIR zavádza automatizované prístupy k zberu, spracovaniu a analýze digitálnych stôp. Vďaka tomu môžu bezpečnostné tímy rýchlejšie identifikovať príčiny incidentov a prijať účinné opatrenia na ich riešenie.
- **Zníženie pracovnej záťaže forezných analytikov.** Rutinné a časovo náročné úlohy spojené so spracovaním digitálnych stôp budú nahradené automatizovanými metódami. To umožní analytikom sústrediť sa na zložitejšie prípady a strategické rozhodovanie.
- **Vyššia kvalita a konzistentnosť výstupov.** Použitie jednotných metodík a nástrojov zaručuje, že spracované digitálne stopy budú presnejšie, konzistentnejšie a ľahšie overiteľné. To výrazne znižuje riziko chýb spôsobených ľudskými faktormi.
- **Možné využitie v trestnom konaní.** Výstupy projektu budú vyvinuté v súlade s právnymi požiadavkami a normami, čo umožní, aby digitálne stopy boli akceptované ako relevantné dôkazy pre vyšetrovanie a súdne konania.

2 Úvod

2.1 Účel metodiky

Rozvoj informačných technológií a rastúca závislosť organizácií od informačných systémov vedú k nárastu kybernetických hrozieb, ako sú ransomware útoky, úniky údajov či neoprávnený prístup do systémov. Riešenie týchto incidentov si často vyžaduje zapojenie špecializovaných poskytovateľov digitálnej forenznej analýzy a reakcie na incidenty.

Účelom metodiky je vytvoriť jednotný rámec odporúčaní a postupov pre uzatváranie zmluvných vzťahov pri poskytovaní týchto služieb. **Cieľom je** zabezpečiť právnu istotu, ochranu údajov, zachovanie dôkaznej hodnoty digitálnych dôkazov a efektívne riešenie bezpečnostných incidentov.

Právny účel metodiky

Jedným zo základných cieľov metodiky je zabezpečiť súlad poskytovaných služieb s platným právnym poriadkom. Poskytovatelia digitálnych forenzných služieb pri svojej činnosti spracúvajú údaje a informácie, ktoré podliehajú ochrane podľa viacerých právnych predpisov. Ide najmä o oblasť ochrany osobných údajov, kybernetickej bezpečnosti, ochrany obchodného tajomstva, autorského práva, občianskeho a obchodného práva, prípadne aj trestného práva. Medzi najrelevantnejšie právne predpisy v oblasti poskytovanie digitálnej forenznej analýzy a riešenia kybernetických incidentov radíme:

- **zákon č. 513/1991 Zb. Obchodný zákonník** (napr. upravuje vznik zmluvného vzťahu, ale aj ďalšie otázky);
- **Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679** z 27.04.2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (GDPR), pričom na národnej úrovni GDPR dopĺňa **zákon č. 18/2018 Z. z. o ochrane osobných údajov** (GDPR napr. ovplyvňuje najmä zmluvné ustanovenia týkajúce sa právneho základu spracúvania údajov, bezpečnostných opatrení, mlčanlivosti, využívania subdodávateľov a rozdelenia úloh medzi prevádzkovateľom a sprostredkovateľom);
- **zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti** v znení neskorších predpisov (napr. upravuje povinnosti prevádzkovateľov základnej služby, riešenie kybernetických bezpečnostných incidentov a postavenie jednotiek CSIRT; jeho požiadavky môžu byť relevantné aj pri zmluvnom zabezpečení DFIR služieb);
- **Smernica Európskeho Parlamentu a Rady (EÚ) 2022/2555** zo 14.12.2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (napr. stanovuje požiadavky na riadenie kybernetických rizík, oznamovanie incidentov a využívanie bezpečnostných služieb).
- **zákon č. 301/2005 Z. z. Trestný poriadok** (ak sú digitálne dôkazy určené na použitie v trestnom konaní).
- **Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554** zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora (**nariadenie DORA**).

Okrem právnych predpisov zohrávajú dôležitú úlohu aj medzinárodné normy a štandardy, ktoré síce nie sú právne záväzné, ale môžu slúžiť ako kritérium odbornej starostlivosti. Ide napríklad o:

- **ISO/IEC 27037** – identifikácia, zber, získavanie a uchovávanie digitálnych dôkazov;
- **ISO/IEC 27041** – validácia a vhodnosť forenzných metód;
- **ISO/IEC 27042** – analýza a interpretácia digitálnych dôkazov; ISO/IEC 27043 – proces vyšetrovania incidentov.

Metodika má slúžiť ako nástroj na identifikáciu právnych požiadaviek, ktoré musia byť zohľadnené už pri príprave a uzatváraní zmluvného vzťahu (aj s poukazom na relevantné právne predpisy, po prípade normy a štandardy uvedené vyššie). Jej cieľom je pomôcť zmluvným stranám správne určiť rozsah oprávnení poskytovateľa služieb, podmienky spracúvania údajov, pravidlá mlčanlivosti, rozsah zodpovednosti za škodu, spôsob riešenia sporov a ďalšie právne aspekty spolupráce.

Účel metodiky z pohľadu ochrany digitálnych dôkazov

Významnou charakteristikou digitálnej forenzej analýzy je práca s digitálnymi dôkazmi. Na rozdiel od tradičných dôkazných prostriedkov majú digitálne dôkazy špecifické vlastnosti, ktoré si vyžadujú osobitný prístup. Môžu byť veľmi jednoducho modifikované, kopírované alebo zničené, pričom aj minimálna zmena môže ovplyvniť ich dôkaznú hodnotu.

Účelom metodiky je vytvoriť podmienky (najmä v predzmluvnej fáze a vo fáze uzatvárania zmlúv) na zachovanie autenticity, integrity a dôveryhodnosti digitálnych dôkazov počas celého procesu ich získavania, spracovania, uchovávanía a prípadného odovzdania oprávneným orgánom. Metodika má definovať základné pravidlá nakladania s digitálnymi dôkazmi a odporúčané zmluvné ustanovenia upravujúce vlastníctvo dôkazov, práva k ich používaniu, podmienky ich uchovávanía a pravidlá dokumentovania jednotlivých úkonov vykonaných počas vyšetrovania incidentu. Dôležitým cieľom je tiež zabezpečiť, aby výsledky forenzej analýzy mohli byť v prípade potreby využité ako relevantný dôkazný prostriedok v právnych konaniach.

Bezpečnostný účel metodiky

Metodika má taktiež podporiť efektívne zvládanie kybernetických incidentov prostredníctvom vopred definovaných pravidiel spolupráce medzi klientom a poskytovateľom služieb. Účelom metodiky je preto aj vytvoriť odporúčania pre zmluvné nastavenie procesov reakcie na incidenty, vrátane definovania reakčných časov, komunikačných kanálov, zodpovedností jednotlivých strán a postupov pri eskalácii incidentov. Tým sa zvyšuje pripravenosť organizácie na riešenie bezpečnostných udalostí a znižujú sa potenciálne škody spôsobené kybernetickými útokmi.

Účel metodiky z pohľadu ochrany osobných údajov

Počas vyšetrovania bezpečnostných incidentov dochádza veľmi často k spracúvaniu osobných údajov zamestnancov, zákazníkov alebo obchodných partnerov organizácie. Poskytovateľ služieb môže mať prístup k e-mailovej komunikácii, logom informačných systémov, používateľským účtom či databázam obsahujúcim osobné údaje.

Účelom metodiky je vytvoriť odporúčania, ktoré zabezpečia zákonné spracúvanie osobných údajov počas realizácie digitálnej forenzej analýzy a reakcie na incident.

Zmluvný a organizačný účel metodiky

Ďalším cieľom metodiky je štandardizácia zmluvných vzťahov v oblasti digitálnej forenzy a reakcie na incidenty. V súčasnosti neexistuje jednotný model zmluvy, ktorý by bol všeobecne

používaný všetkými poskytovateľmi týchto služieb. To môže viesť k rozdielnej kvalite zmluvnej dokumentácie a k nejasnostiam pri výkone práv a povinností zmluvných strán.

Metodika má preto poskytnúť odporúčania pre tvorbu zmluvnej, ale aj nadväzujúcej dokumentácie súvisiacej s poskytovaním služieb digitálnej forenznej analýzy a reakcie na kybernetické incidenty s poukazom na vyššie uvedené (napr. súlad s právnym poriadkom).

2.2 Teoretické východiská digitálnej forenznej analýzy a reakcie na incident

Digitálna forezná analýza a reakcia na kybernetické incidenty (Digital Forensics and Incident Response – DFIR) predstavujú odborné činnosti zamerané na identifikáciu, analýzu a riešenie bezpečnostných incidentov, ako aj na získavanie a spracúvanie digitálnych dôkazov. Ich realizácia často vyžaduje prístup k informačným systémom, osobným údajom, dôverným informáciám a ďalším chráneným údajom organizácie.

Z pohľadu tejto metodiky je význam DFIR daný najmä tým, že poskytovanie týchto služieb spravidla prebieha na základe zmluvného vzťahu medzi klientom a poskytovateľom odborných služieb. Vzhľadom na citlivosť spracúvaných informácií a potenciálne právne dôsledky vyšetrovania incidentov je nevyhnutné jasne upraviť rozsah oprávnení poskytovateľa, podmienky prístupu k údajom, pravidlá mlčanlivosti, ochranu digitálnych dôkazov, zodpovednosť zmluvných strán a ďalšie súvisiace otázky.

Digitálna forezná analýza zahŕňa činnosti smerujúce k získaniu, uchovaniu a vyhodnoteniu digitálnych dôkazov, zatiaľ čo reakcia na incidenty je zameraná na zvládnutie bezpečnostnej udalosti, obmedzenie jej následkov a obnovu bezpečnej prevádzky informačných systémov. Obe oblasti sú úzko prepojené a ich výkon si vyžaduje jasné organizačné a zmluvné pravidlá.

Pre účely tejto metodiky nie je cieľom podrobne rozoberať technické aspekty DFIR, ale poukázať na ich význam pre správne nastavenie právnych a zmluvných vzťahov medzi klientom a poskytovateľom služieb.

Riadne vykonané činnosti forenznej analýzy následne napomáhajú k zachovaniu nie len integrity potenciálnych dôkazov, ale aj prispieva k ich prípustnosti v právnych a disciplinárnych, či iných konaniach.¹

¹ MAKATURA, Ivan. *Ciele dokazovania v kybernetickej bezpečnosti*. In: *Acta Facultatis Iuridicae Universitatis Comenianae*, 2023, roč. 42, č. 1, s. 116 – 146

2.3 Úloha KPB1.1

Táto metodika je výstupom úlohy KPB1.1 pracovného balíka KPB1 „Právne otázky, manažment a CDE“ projektu ADFIR.

Úloha KPB1.1 – Analýza a určenie právnych požiadaviek na spracovanie digitálnych stôp pochádzajúcich zo zistených bezpečnostných incidentov, potrebných na vytvorenie datasetu a na zlepšenie analytických nástrojov. Zohľadnenie právnych osobitostí digitálnych stôp a ich porovnanie s tradičnými dôkaznými prostriedkami. Analýza možnosti uzatvárania právnych zmluvných vzťahov pri poskytovaní služieb v oblasti digitálnej forenznej analýzy a odpovede na bezpečnostné incidenty (EISI).

Predložená metodika nadväzuje na tretiu časť uvedenej úlohy a poskytuje jednotný rámec odporúčaní pre uzatváranie zmluvných vzťahov pri poskytovaní služieb digitálnej forenznej analýzy a reakcie na kybernetické incidenty. Právne osobitosti digitálnych stôp a požiadavky na ich spracovanie sú v nadväznosti na úlohy KPB1.2 a KPB1.3 podrobnejšie rozpracované v samostatných výstupoch projektu (Metóda na anonymizáciu digitálnych stôp; Metodológia postupu spracovania digitálnych stôp).

3 Zmluvné vzťahy pri poskytovaní digitálnej forenznej analýzy a reakcie na kybernetické incidenty

Na rozdiel od bežných zmlúv o poskytovaní IT služieb je pri DFIR nevyhnutné venovať zvýšenú pozornosť zmluvnej úprave vzájomných práv a povinností zmluvných strán. Dôvodom je najmä potreba zabezpečiť zákonnosť spracúvania údajov, ochranu dôvernosti informácií, zachovanie integrity digitálnych dôkazov a jasné vymedzenie zodpovednosti za škodu vzniknutú v súvislosti s riešením bezpečnostného incidentu. Nejednoznačne formulované zmluvné ustanovenia môžu viesť nielen k sporom medzi klientom a poskytovateľom služby, ale aj k spochybneniu dôkaznej hodnoty získaných dát alebo k porušeniu povinností vyplývajúcich z právnych predpisov.

Význam zmluvnej úpravy narastá aj v súvislosti s čoraz častejším využívaním externých špecializovaných DFIR tímov, cloudových služieb a cezhraničným spracúvaním údajov. Zmluva preto musí upravovať nielen rozsah a spôsob poskytovania služieb, ale aj pravidlá nakladania s digitálnymi dôkazmi, ochranu osobných údajov, využívanie subdodávateľov, bezpečnostné opatrenia, spôsob riešenia incidentov a rozdelenie zodpovednosti medzi jednotlivými subjektmi.

3.1 Fázy zmluvného vzťahu

3.1.1. Predzmluvná fáza

Účelom predzmluvnej fázy je najmä výmena informácií medzi budúcimi zmluvnými stranami, ale aj analýza ich potrieb a požiadaviek vo vzťahu k ich budúcej spolupráci. V oblasti DFIR má táto fáza osobitný význam, keďže poskytovateľ služieb často získava prístup k citlivým informáciám už pred uzatvorením zmluvy a klient musí posúdiť, či je poskytovateľ schopný zabezpečiť požadovanú úroveň odbornosti, dôvernosti a bezpečnosti.

Cieľom predzmluvnej fázy je taktiež vytvoriť dostatočný základ pre uzatvorenie zmluvného vzťahu, identifikovať právne, technické a organizačné riziká a nastaviť základné parametre budúcej spolupráce. Kvalitne realizovaná predzmluvná príprava môže významne znížiť riziko sporov, nejasností alebo bezpečnostných incidentov počas poskytovania služieb.

Identifikácia potrieb a cieľov klienta

V rámci identifikácie potrieb a cieľov klienta je nevyhnutné ešte pred začatím zmluvných rokovaní určiť, **aký charakter bude mať požadovaná spolupráca a aké činnosti bude poskytovateľ vykonávať**. Správne vymedzenie predmetu budúceho zmluvného vzťahu má zásadný význam pre samotné uzatváranie zmluvného vzťahu.

V predzmluvnej fáze je preto potrebné analyzovať, **či klient požaduje jednorazovú službu alebo dlhodobú spoluprácu**. Táto otázka významne ovplyvňuje nielen ekonomické podmienky zmluvy, ale aj rozsah práv a povinností jednotlivých strán. Ak klient požaduje jednorazovú digitálnu forenznú analýzu alebo vyšetrovanie konkrétneho bezpečnostného incidentu, pozornosť sa sústreďuje predovšetkým na vymedzenie konkrétnych systémov, zariadení alebo dát, ktoré budú predmetom analýzy. V takomto prípade je potrebné ešte pred uzatvorením zmluvy identifikovať, aké dôkazy majú byť zabezpečené, aký je účel vyšetrovania a či sa predpokladá ich využitie v internom vyšetrovaní, pracovnoprávnom spore, správnom konaní alebo v trestnom konaní. Odpovede na tieto otázky následne ovplyvňujú požiadavky na dokumentovanie postupov, zachovanie integrity dôkazov a vedenie reťazca držby (chain of custody).

Ak klient požaduje vyšetrovanie konkrétneho bezpečnostného incidentu, je potrebné už v predzmluvnej fáze získať základné informácie o incidente, jeho rozsahu a možných dôsledkoch. Poskytovateľ musí vedieť posúdiť, či ide o neoprávnený prístup do systému, únik dát, ransomvérový útok, kompromitáciu účtov alebo inú formu bezpečnostného incidentu. Zároveň je potrebné preveriť, či incident môže zakladať oznamovacie povinnosti podľa GDPR, právnej úpravy kybernetickej bezpečnosti alebo sektorových regulácií. Bez týchto informácií nie je možné správne nastaviť rozsah služieb ani zodpovednosť jednotlivých strán.

V prípade záujmu o dlhodobú podporu pri riešení incidentov alebo služby typu „Incident Response Retainer“ je potrebné už pred uzatvorením zmluvy analyzovať úroveň pripravenosti organizácie na riešenie bezpečnostných incidentov. Poskytovateľ by mal poznať organizačnú

štruktúru klienta, dostupnosť interných IT tímov, existujúce bezpečnostné procesy a technické vybavenie organizácie. Predmetom predzmluvnej komunikácie by malo byť aj určenie očakávaných reakčných časov, spôsobu aktivácie služieb a rozsahu podpory, ktorú klient očakáva počas trvania zmluvného vzťahu.

Osobitnú pozornosť si vyžaduje situácia, keď **klient požaduje zavedenie alebo rozvoj forenznej pripravenosti (Forensic Readiness)**. V takom prípade je potrebné ešte pred uzatvorením zmluvy posúdiť aktuálny stav procesov evidencie a uchovávaní logov, nastavenie bezpečnostného monitoringu, možnosti získavania digitálnych dôkazov a existenciu interných smerníc upravujúcich reakciu na incidenty. Výsledkom tejto analýzy býva identifikácia nedostatkov, ktoré sa následne stávajú predmetom zmluvného plnenia.

Pred uzatvorením zmluvy je zároveň **potrebné zistiť, či klient očakáva podporu pri komunikácii s orgánmi verejnej moci alebo regulačnými orgánmi**. Ak sa predpokladá komunikácia s orgánmi činnými v trestnom konaní, Úradom na ochranu osobných údajov, Národným bezpečnostným úradom alebo inými regulačnými orgánmi, je potrebné vopred určiť rozsah oprávnení poskytovateľa a formu jeho zapojenia do týchto procesov. Rovnako je potrebné identifikovať prípadné zákonné povinnosti klienta, ktorých splnenie bude poskytovateľ svojimi službami podporovať.

Dôležitou súčasťou identifikácie potrieb klienta je aj **zistenie, či výsledky činnosti poskytovateľa majú slúžiť ako dôkaz v budúcom súdnom, správnom alebo pracovnoprávnom konaní**. Ak sa takýto účel predpokladá, musí byť už v predzmluvnej fáze zohľadnená potreba zachovania forenznej správnosti postupov, dokumentovania všetkých úkonov a zabezpečenia dôveryhodnosti digitálnych dôkazov. Tieto požiadavky následne významne ovplyvňujú obsah budúcej zmluvy, najmä ustanovenia o nakladaní s digitálnymi dôkazmi, mlčanlivosti, ochrane údajov a zodpovednosti za škodu.

Na margo vyššie uvedeného, je potrebné uviesť, že v praxi čoraz častejšie dochádza k situáciám, kedy klienti majú uzatvorené tzv. Cyber Insurance. **Kybernetické poistenie (Cyber Insurance)** predstavuje špecializovaný druh poistenia, ktorého účelom je krytie finančných následkov kybernetických incidentov a bezpečnostných udalostí ovplyvňujúcich informačné systémy, siete, elektronické služby alebo spracúvané údaje organizácie. Predmetom poistného krytia môžu byť najmä náklady spojené s reakciou na incident, digitálnou forenznou analýzou, obnovou systémov a dát, právnym poradenstvom, plnením oznamovacích povinností, krízovou komunikáciou, prerušením prevádzky alebo náhradou škody spôsobenej kybernetickým incidentom.

V rámci predzmluvnej prípravy je preto vhodné preveriť, či klient disponuje uzatvoreným kybernetickým poistením a či poistné podmienky obsahujú požiadavky, ktoré môžu mať vplyv na spôsob poskytovania služieb digitálnej forenznej analýzy a reakcie na kybernetické incidenty (DFIR). Hoci poistný vzťah vzniká medzi klientom a poisťovňou, jeho podmienky môžu významne ovplyvniť rozsah služieb poskytovaných počas riešenia bezpečnostného

incidentu, požiadavky na dokumentovanie vykonaných úkonov, spôsob nakladania s digitálnymi dôkazmi alebo komunikáciu s ďalšími subjektmi zapojenými do riešenia incidentu.

Predbežná analýza prostredia klienta

Po identifikácii potrieb a cieľov klienta nasleduje v predzmluvnej fáze predbežná analýza jeho technického, organizačného a právneho prostredia. Jej cieľom je získať dostatočné množstvo informácií potrebných na správne nastavenie zmluvného vzťahu, určenie rozsahu poskytovaných služieb, odhad časovej a technickej náročnosti realizácie, ako aj identifikáciu právnych a bezpečnostných rizík, ktoré môžu mať vplyv na budúce poskytovanie DFIR služieb. **Nejde pritom o samotné vykonanie digitálnej forenznej analýzy ani o vyšetrovanie bezpečnostného incidentu, ale o zber informácií potrebných na prípravu vhodného zmluvného a procesného rámca spolupráce.**

Jednou z prvých oblastí, ktoré by mali byť predmetom posúdenia, je **charakter informačných systémov klienta a ich celková komplexnosť**. Poskytovateľ by mal získať základný prehľad o počte a type využívaných systémov, sieťovej architektúre, počte používateľov, využívaných operačných systémoch, platformách a ďalších technologických komponentoch. Rozdielne požiadavky budú kladené na organizáciu využívajúcu niekoľko lokálnych serverov a niekoľko desiatok pracovných staníc a na organizáciu prevádzkujúcu rozsiahlu distribuovanú infraštruktúru pozostávajúcu z viacerých dátových centier, cloudových služieb a tisícok koncových zariadení. Komplexnosť prostredia má priamy vplyv na rozsah budúcich služieb, potrebné odborné kapacity, časové nároky aj výslednú cenu poskytovaných služieb.

Významnou oblasťou posudzovania je aj **rozsah a charakter spracúvaných údajov**. Poskytovateľ by mal zistiť, či informačné systémy klienta obsahujú osobné údaje, obchodné tajomstvo, finančné údaje, zdravotnú dokumentáciu, údaje podliehajúce bankovému tajomstvu alebo iné kategórie citlivých informácií. Táto informácia je nevyhnutná na určenie právnych povinností, ktoré budú musieť byť následne premietnuté do zmluvy, najmä vo vzťahu k ochrane osobných údajov, mlčanlivosti, bezpečnostným opatreniam a prípadnému využívaniu subdodávateľov. Súčasne umožňuje identifikovať riziká spojené s možným únikom údajov alebo neoprávneným prístupom k nim počas poskytovania služieb.

Predmetom analýzy by mali byť aj **používané technológie a cloudové služby**. V súčasnosti veľká časť organizácií využíva hybridné alebo cloudové prostredia, pričom relevantné dáta môžu byť uložené u viacerých poskytovateľov služieb. Poskytovateľ DFIR služieb by mal preto zistiť, či klient využíva verejný, súkromný alebo hybridný cloud, aké služby sú prevádzkované prostredníctvom externých poskytovateľov a aké sú podmienky prístupu k týmto systémom. Táto otázka je významná najmä z pohľadu získavania digitálnych dôkazov, pretože klient nemusí mať vždy plnú kontrolu nad infraštruktúrou, v ktorej sa relevantné údaje nachádzajú.

Osobitnú pozornosť je potrebné venovať **geografickému umiestneniu dátových úložísk a miestam spracúvania údajov**. Ak sa údaje nachádzajú mimo územia Slovenskej republiky alebo Európskej únie, môžu vzniknúť dodatočné právne požiadavky týkajúce sa cezhraničného prenosu údajov, jurisdikcie alebo spolupráce so zahraničnými poskytovateľmi služieb. Táto

skutočnosť môže mať významný vplyv na spôsob získavania digitálnych dôkazov, ich uchovávanie a prípadné využitie v súdnych alebo správnych konaniach.

Predbežná analýza by sa mala zamerať taktiež na **existujúce bezpečnostné opatrenia klienta**. Poskytovateľ by mal získať základný prehľad o tom, či organizácia disponuje nástrojmi na monitorovanie bezpečnosti, systémami centralizovaného logovania, riešeniami na detekciu a reakciu na incidenty, nástrojmi EDR alebo SIEM a či má zavedené interné procesy riešenia bezpečnostných incidentov. Úroveň bezpečnostnej vyspelosti organizácie môže významne ovplyvniť rozsah budúcich služieb a zároveň napovedá, do akej miery bude klient schopný spolupracovať pri riešení incidentov alebo zabezpečovaní digitálnych dôkazov.

Súčasťou analýzy by malo byť aj **posúdenie interných kapacít klienta v oblasti informačnej a kybernetickej bezpečnosti**. Je potrebné zistiť, či organizácia disponuje vlastným bezpečnostným tímom, administrátormi schopnými poskytovať technickú súčinnosť alebo osobami zodpovednými za ochranu osobných údajov a riadenie bezpečnosti. Tieto informácie sú dôležité pre určenie rozsahu služieb, ktoré bude potrebné zabezpečiť externe, ako aj pre nastavenie komunikačných a eskalačných mechanizmov počas poskytovania služieb.

Významnú úlohu zohráva aj **identifikácia regulačných požiadaviek vzťahujúcich sa na klienta**. Poskytovateľ by mal preveriť, či klient podlieha osobitným sektorovým reguláciám, požiadavkám vyplývajúcim z GDPR, právnej úpravy kybernetickej bezpečnosti, smernice NIS 2 alebo iným špecifickým predpisom. Tieto požiadavky môžu mať zásadný vplyv na obsah budúcej zmluvy, najmä pokiaľ ide o uchovávanie údajov, oznamovacie povinnosti, bezpečnostné opatrenia alebo spôsob nakladania s digitálnymi dôkazmi.

Vhodné je tiež zistiť, **či organizácia v minulosti čelila bezpečnostným incidentom a akým spôsobom boli riešené**. Predchádzajúce skúsenosti môžu poukázať na existujúce slabé miesta, organizačné nedostatky alebo opakujúce sa bezpečnostné problémy, ktoré je potrebné zohľadniť pri návrhu rozsahu budúcej spolupráce. Zároveň môžu naznačiť úroveň pripravenosti organizácie na spoluprácu s externým DFIR tímom.

Pri získavaní informácií v predzmluvnej fáze je však potrebné rešpektovať zásadu minimalizácie údajov podľa článku 5 ods. 1 písm. c) GDPR. Poskytovateľ by mal získavať iba tie informácie, ktoré sú nevyhnutné na posúdenie rozsahu budúcej spolupráce a prípravu zmluvy. V tejto fáze spravidla neexistuje dôvod na sprístupňovanie samotných digitálnych dôkazov, obsahu komunikácie, osobných údajov zamestnancov alebo iných detailných údajov, ktoré nesúvisia s prípravou zmluvného vzťahu. Dodržiavanie zásady minimalizácie údajov nielen znižuje právne a bezpečnostné riziká, ale zároveň prispieva k budovaniu dôvery medzi budúcimi zmluvnými stranami.

Overenie odbornej spôsobilosti poskytovateľa

Pred uzatvorením zmluvy by mal klient vykonať primerané posúdenie odbornej a technickej spôsobilosti poskytovateľa. V prípade DFIR služieb je výber poskytovateľa založený

predovšetkým na dôveryhodnosti, skúsenostiach a schopnosti efektívne reagovať na bezpečnostné incidenty, pričom cena by nemala byť jediným rozhodovacím kritériom. Posudzovanie poskytovateľa by malo zahŕňať preverenie odborných certifikácií a kvalifikácie pracovníkov, personálne a organizačné kapacity, referencií z obdobných projektov, skúseností s riešením porovnateľných incidentov, technického vybavenia, interných bezpečnostných opatrení, procesov riadenia kvality, poistenia zodpovednosti za škodu a schopnosti zabezpečiť služby v požadovanom rozsahu a režime dostupnosti.

Ochrana dôverných informácií počas rokovaní

Nakoľko je predzmluvná fáza pri poskytovaní služieb DFIR **charakteristická intenzívnou výmenou informácií medzi budúim klientom a potenciálnym poskytovateľom služieb odporúča sa ešte pred ich sprístupnením zabezpečiť ich ochranu**. V praxi sa za najvhodnejší nástroj považuje uzatvorenie **dohody o mlčanlivosti (Non-Disclosure Agreement – NDA)**. Hoci ochrana určitých informácií môže vyplývať aj zo všeobecných právnych predpisov, najmä z ustanovení o ochrane obchodného tajomstva podľa § 17 až § 20 Obchodného zákonníka, osobitná dohoda o mlčanlivosti poskytuje zmluvným stranám vyššiu mieru právnej istoty a umožňuje presne definovať rozsah chránených informácií a pravidlá ich používania. V rámci dohody o mlčanlivosti je teda potrebné vymedziť, ktoré informácie budú považované za dôverné. V prostredí DFIR služieb môžu mať charakter dôverných informácií nielen obchodné a ekonomické údaje klienta, ale aj technické informácie o informačných systémoch, sieťovej infraštruktúre, bezpečnostných opatreniach alebo bezpečnostných incidentoch. Osobitnú hodnotu majú najmä informácie o architektúre informačných systémov, konfigurácii bezpečnostných riešení, využívaných technológiách, zraniteľnostiach systémov, výsledkoch penetračných testov, bezpečnostných auditov alebo interných vyšetrovaní. Takéto údaje môžu predstavovať významný zdroj informácií pre potenciálnych útočníkov, a preto si vyžadujú zvýšenú ochranu už v štádiu rokovaní.

Súčasťou dohody o mlčanlivosti by malo byť aj **jasné vymedzenie účelu, na ktorý môžu byť dôverné informácie použité**. Poskytovateľ by mal byť oprávnený využívať získané informácie výlučne na účely posúdenia možnosti budúcej spolupráce, prípravy návrhu zmluvy alebo vypracovania technického riešenia.

Dôležitou otázkou je aj **určenie okruhu osôb, ktoré budú mať k dôverným informáciám prístup**. Vzhľadom na špecializovaný charakter DFIR služieb býva často potrebné, aby sa do predzmluvných rokovaní zapojili aj externé subjekty. Klient by však mal mať istotu, že prístup k dôverným informáciám získajú len osoby, ktoré ho nevyhnutne potrebujú na splnenie predzmluvných dojednaní, po prípade následne aj na splnenie účelu zmluvy. Dohoda o mlčanlivosti **by mala obsahovať požiadavky na primerané technické a organizačné opatrenia, ktoré zabránia neoprávnenému prístupu k informáciám, ich strate alebo zneužitiu** (napr. využívanie šifrovaných komunikačných kanálov, zabezpečených úložísk alebo kontrolovaných prístupových mechanizmov).

Významnou súčasťou dohody o mlčanlivosti by mala byť aj **úprava nakladania s informáciami po skončení rokovaní**. Predzmluvné rokovania nemusia vždy viesť k uzatvoreniu zmluvy,

pričom aj v takom prípade zostáva potrebné zabezpečiť ochranu už sprístupnených údajov. Dohoda o mlčanlivosti by preto mala upravovať povinnosť vrátiť, vymazať alebo inak bezpečne zlikvidovať všetky poskytnuté informácie a ich kópie, pokiaľ ich ďalšie uchovávanie nevyžaduje právny predpis alebo oprávnený záujem niektorej zo strán. Súčasne by mala byť stanovená primeraná doba trvania povinnosti mlčanlivosti, po ukončení predzmluvných rokovaní, ktorá bude zodpovedať citlivosti sprístupnených informácií.

Vo väčšine prípadoch, vzhľadom na dôverný charakter informácií, dohoda o mlčanlivosti vymedzuje taktiež **úpravu zodpovednosti za porušenie povinností mlčanlivosti**. Najčastejšie ide o dojednanie zmluvnej pokuty, ktorej výška je ponechaná na dohode zmluvných strán. Navyše následkom porušenia povinností je aj uplatnenie nároku na náhradu škody, ktorá porušením konkrétnej povinnosti vznikla.

Pri zmluvných pokutách viazaných na porušenie povinnosti mlčanlivosti alebo pravidiel nakladania s údajmi je vhodné čo najpresnejšie vymedziť zabezpečenú povinnosť a okolnosti vzniku nároku na zmluvnú pokutu. Zmluvné strany by mali zároveň zabezpečiť primeranú dokumentáciu umožňujúcu prípadné porušenie preukázať, napríklad evidenciu prístupov k údajom, ich exportov, odovzdania alebo ďalšieho sprístupnenia (porov. rozsudok Krajského súdu v Košiciach sp. zn. 4Cob/46/2024 z 23. 4. 2025).

Posúdenie spracúvania osobných údajov

V rámci predzmluvnej prípravy je potrebné identifikovať, či bude poskytovateľ počas poskytovania služieb pristupovať k osobným údajom alebo ich spracúvať. Táto otázka je obzvlášť významná pri forenzných analýzach, vyšetrovaní incidentov alebo analýze systémových logov, kde sa osobné údaje často nachádzajú.

Ak sa predpokladá spracúvanie osobných údajov, zmluvné strany musia vopred určiť svoje postavenie podľa právnych predpisov o ochrane osobných údajov, identifikovať právny základ spracúvania, posúdiť potrebu uzatvorenia zmluvy o spracúvaní osobných údajov a preveriť primeranosť technických a organizačných bezpečnostných opatrení. Zároveň je potrebné riešiť otázky cezhraničných prenosov údajov, uchovávaní údajov a postupov pri prípadnom porušení ochrany osobných údajov.

Výstupy predzmluvnej fázy

Výsledkom predzmluvnej fázy by malo byť vytvorenie komplexného základu pre uzatvorenie zmluvného vzťahu a následné poskytovanie DFIR služieb. Medzi hlavné výstupy patrí najmä:

- jednoznačné vymedzenie predmetu a cieľov spolupráce,
- identifikácia technických, bezpečnostných, právnych a organizačných rizík,
- určenie rozsahu poskytovaných služieb,
- uzatvorenie dohody o mlčanlivosti,
- identifikácia požiadaviek na ochranu osobných údajov a príprava súvisiacej dokumentácie,
- príprava návrhu zmluvy a jej príloh.

Kvalitne realizovaná predzmluvná fáza vytvára predpoklady pre transparentný, bezpečný a efektívny výkon služieb digitálnej forenznej analýzy a reakcie na kybernetické incidenty počas celého trvania zmluvného vzťahu.

3.1.2. Uzatvorenie zmluvy

Po ukončení predzmluvnej fázy a dosiahnutí základnej zhody medzi budúcimi zmluvnými stranami nasleduje fáza uzatvárania zmluvy. Ide o kľúčovú etapu zmluvného vzťahu, počas ktorej sa identifikované potreby klienta, technické požiadavky, bezpečnostné očakávania a právne povinnosti transformujú do záväzných zmluvných ustanovení. Kvalita zmluvnej úpravy v tejto fáze významne ovplyvňuje nielen priebeh poskytovania služieb digitálnej forenznej analýzy a reakcie na kybernetické incidenty, ale aj schopnosť zmluvných strán predchádzať budúcim sporom a efektívne riešiť situácie, ktoré môžu počas poskytovania služieb vzniknúť.

Voľba vhodného zmluvného modelu a zmluvnej dokumentácie

Prvým krokom pri uzatváraní zmluvy je určenie vhodného právneho a obchodného modelu spolupráce. V praxi môže byť poskytovanie DFIR služieb upravené rôznymi typmi zmlúv v závislosti od rozsahu a charakteru poskytovaných služieb.

Najčastejšie sa využívajú:

- jednorazová zmluva
- rámcové zmluvy o spolupráci,
- zmluva o rezervácii kapacít
- SLA dohoda (Service Level Agreement)
- a iné

Kritérium	Jednorazová zmluva	Rámcová zmluva	Zmluva o rezervácii kapacít	SLA
Rieši konkrétny incident	Áno	Nie	Nie	Nie
Dlhodobá spolupráca	Nie	Áno	Áno	Doplňkovo
Garantovaná dostupnosť	Nie	Nie	Áno	Len ak je súčasťou retaineru
Prioritná reakcia	Nie	Nie	Áno	Môže byť upravená
Rezervácia kapacít	Nie	Nie	Áno	Nie
Pravidelné poplatky	Nie	Spravidla nie	Áno	Nie
Vhodná pre krízové situácie	Obmedzene	Čiastočne	Áno	Podporne
Administratívna náročnosť pri incidente	Vysoká	Stredná	Nízka	Nízka

Pri dlhodobej pripravenosti na riešenie kybernetických incidentov môže byť vhodným modelom kombinácia rámcovej zmluvy a zmluva o rezervácii kapacít doplnenej o SLA. Takéto riešenie umožňuje vytvoriť stabilný právny základ spolupráce, zabezpečiť pripravenosť poskytovateľa na incidenty a zároveň presne definovať požadované reakčné časy a kvalitatívne parametre služieb.

Jednorazová zmluva je vhodná najmä pre organizácie, ktoré DFIR služby využívajú výnimočne alebo riešia izolovaný incident bez potreby dlhodobej spolupráce.

Hybridné zmluvné modely v praxi

Najrozšírenejším modelom poskytovania služieb digitálnej forenzej analýzy a reakcie na kybernetické incidenty je v súčasnosti **tzv. hybridný zmluvný model**, ktorý pozostáva z viacerých vzájomne prepojených zmluvných dokumentov. Základ spolupráce spravidla tvorí **rámcová zmluva**, ktorá upravuje všeobecné podmienky poskytovania služieb, práva a povinnosti zmluvných strán, pravidlá zodpovednosti za škodu, ochranu dôverných informácií, riešenie sporov a ďalšie základné aspekty spolupráce. Na rámcovú zmluvu zvyčajne nadväzuje **dohoda o mlčanlivosti (NDA)**, ktorej účelom je zabezpečiť ochranu obchodného tajomstva, technickej dokumentácie, informácií o zraniteľnostiach informačných systémov a ďalších dôverných údajov, s ktorými sa poskytovateľ môže počas výkonu svojej činnosti oboznámiť.

Ak poskytovanie služieb zahŕňa spracúvanie osobných údajov, súčasťou zmluvnej dokumentácie býva aj **zmluva o spracúvaní osobných údajov** (Data Processing Agreement – DPA), ktorá upravuje podmienky spracúvania osobných údajov v súlade s požiadavkami GDPR, vrátane bezpečnostných opatrení, rozsahu spracúvania údajov, využívania subdodávateľov a práv a povinností prevádzkovateľa a sprostredkovateľa. Dôležitou súčasťou hybridného modelu je tiež **dohoda o úrovni poskytovaných služieb** (Service Level Agreement – SLA), ktorá stanovuje požadovanú dostupnosť služieb, reakčné časy, klasifikáciu incidentov, eskalačné postupy a ďalšie merateľné parametre kvality poskytovaných služieb.

V prípade organizácií, ktoré požadujú vysokú pripravenosť na riešenie bezpečnostných incidentov, býva spolupráca doplnená o **zmluvu o rezervácii kapacít**. Jej podstatou je rezervácia odborných kapacít poskytovateľa za pravidelný poplatok, pričom klient získava garantovanú dostupnosť služieb a prioritnú reakciu pri vzniku incidentu. Jednotlivé vyšetrovania, incidenty alebo projekty sa následne realizujú prostredníctvom samostatných pracovných príkazov alebo čiastkových objednávok (Statement of Work – SOW), v ktorých sa konkretizuje rozsah požadovaných služieb, časový harmonogram, požadované výstupy a cenové podmienky konkrétneho zadania.

Výhodou hybridného zmluvného modelu je oddelenie všeobecných podmienok spolupráce od špecifických požiadaviek jednotlivých incidentov alebo projektov. Takýto prístup umožňuje vytvoriť stabilný právny rámec spolupráce, zabezpečiť pripravenosť poskytovateľa na riešenie bezpečnostných incidentov a zároveň zachovať dostatočnú flexibilitu pri objednávaní konkrétnych služieb podľa aktuálnych potrieb klienta.

Identifikácia zmluvných strán

Správna identifikácia zmluvných strán predstavuje základný predpoklad platného a efektívneho zmluvného vzťahu. Hoci ide o zdánlivo formálnu náležitosť zmluvy, v oblasti poskytovania služieb digitálnej forenzej analýzy a reakcie na kybernetické incidenty (DFIR) má jej správne nastavenie osobitný význam. Jednoznačná identifikácia účastníkov zmluvného vzťahu je nevyhnutná pre určenie práv a povinností strán, zodpovednosti za plnenie zmluvy, ochranu dôverných informácií, spracúvanie osobných údajov a uplatňovanie nárokov vyplývajúcich zo zmluvy.

V procese uzatvárania zmluvy je potrebné ešte pred podpisom overiť identitu zmluvných strán, ich právnu subjektivitu a oprávnenie konať a podpisovať zmluvu. Nedostatočné preverenie týchto skutočností môže viesť k právnej neistote, sporom o platnosť zmluvy alebo problémom pri vymáhaní zmluvných práv.

Popri identifikácii samotných zmluvných strán je vhodné už pri uzatváraní zmluvy určiť **osoby zodpovedné za komunikáciu a koordináciu plnenia zmluvy**. V oblasti DFIR služieb býva často potrebné zabezpečiť okamžitú komunikáciu počas riešenia bezpečnostných incidentov, preto by mali byť kontaktné osoby určené jednoznačne a vrátane náhradných kontaktov.

Odporúča sa identifikovať najmä:

- osoby oprávnené nahlasovať bezpečnostné incidenty;
- osoby oprávnené schvaľovať zásahy do informačných systémov;
- kontaktné osoby pre technickú komunikáciu;
- kontaktné osoby pre právne a zmluvné otázky;
- osoby oprávnené preberať výstupy poskytovaných služieb.

V prípade služieb poskytovaných v režime 24/7 je vhodné upraviť aj dostupnosť týchto osôb mimo bežnej pracovnej doby.

Ak poskytovateľ predpokladá **zapojenie subdodávateľov alebo iných externých subjektov**, odporúča sa už pri uzatváraní zmluvy transparentne definovať ich postavenie a rozsah ich zapojenia. Klient by mal mať možnosť vedieť, ktoré subjekty sa budú podieľať na poskytovaní služieb a aký rozsah prístupu k jeho systémom alebo údajom budú mať.

Vymedzenie predmetu zmluvy

Predmet zmluvy patrí medzi najdôležitejšie ustanovenia zmluvy. Mal by byť formulovaný dostatočne presne, aby nevznikali pochybnosti o rozsahu poskytovaných služieb. **Základným odporúčaním je, aby bol predmet zmluvy definovaný konkrétne a nie všeobecne.** V praxi to znamená, že nestačí používať formulácie typu „poskytovanie IT bezpečnostných služieb“, ale **je potrebné presne určiť, či ide o digitálnu forenznú analýzu, reakciu na kybernetický incident, alebo kombinovaný DFIR zásah.** V praxi je často problematické miešanie nesúvisiacich činností, ako je kombinácia DFIR služieb so správou IT infraštruktúry alebo vývojom softvéru, čo vedie k nejednoznačnosti právneho rámca. Súčasťou správne

definovaného predmetu by malo byť aj vymedzenie technických činností, ktoré bude poskytovateľ vykonávať (napr. zber a analýza digitálnych dôkazov, analýza malware, sieťová forenzika alebo práca s cloud prostrediami).

Dôležitou súčasťou predmetu zmluvy je aj **jasné stanovenie cieľov poskytovaných služieb**. Týmito cieľmi môže byť najmä identifikácia príčiny incidentu, určenie jeho rozsahu, zabezpečenie a analýza digitálnych dôkazov, obnova bezpečnosti systémov alebo podpora právnych a poistných konaní. **Predmet zmluvy by mal byť zároveň prepojený na časový a organizačný rámec poskytovania služby, najmä na reakčné lehoty, dostupnosť služby a mechanizmy eskalácie incidentov.**

Osobitnú pozornosť je potrebné venovať rozlíšeniu medzi reaktívnymi DFIR službami a preventívnymi činnosťami, ako je monitoring, audit alebo penetračné testovanie. Tieto oblasti majú odlišný účel aj právny režim, a preto ich miešanie v rámci jedného predmetu zmluvy môže viesť k nejasnostiam a zníženiu efektivity zásahu.

Osobitosti verejného obstarávania

Ak je klient verejným obstarávateľom alebo obstarávateľom, pri nastavení rozsahu DFIR služieb je potrebné zohľadniť aj pravidlá verejného obstarávania. Osobitnú pozornosť treba venovať následnému rozširovaniu rozsahu služieb prostredníctvom dodatkov, pracovných príkazov alebo čiastkových objednávok. Ak takéto rozšírenie predstavuje podstatnú zmenu pôvodne obstaraného predmetu, nemusí byť možné realizovať ho iba zmenou existujúcej zmluvy a môže byť potrebné uskutočniť nový postup verejného obstarávania. Z tohto dôvodu je vhodné už v pôvodnej dokumentácii dostatočne určiť vymedziť predpokladaný rozsah DFIR služieb, mechanizmy ich aktivácie a prípustné opcie alebo zmeny (porov. rozsudok Správneho súdu v Bratislave sp. zn. BA-1S/83/2020 z 29. 10. 2025).

Rozsah oprávnení poskytovateľa

Poskytovanie DFIR služieb si často vyžaduje rozsiahly prístup k informačným systémom klienta. Zmluva by preto mala presne upraviť rozsah oprávnení poskytovateľa. Nejasne formulované oprávnenia môžu viesť nielen k sporom medzi zmluvnými stranami, ale aj k vzniku bezpečnostných, prevádzkových alebo právnych rizík. **Rozsah oprávnení by preto mal byť vždy primeraný účelu poskytovaných služieb a založený na princípe minimálne potrebných oprávnení (Principle of Least Privilege), podľa ktorého poskytovateľ disponuje iba takými prístupmi a právomocami, ktoré sú nevyhnutné na splnenie dohodnutého účelu.**

Čo by mala zmluva obsahovať vo vzťahu k rozsahu oprávnení poskytovateľa?

- **Rozsah prístupových práv** - Zmluva by mala presne určiť, do ktorých systémov, aplikácií, databáz, cloudových prostredí alebo úložísk bude poskytovateľ oprávnený prístupovať. Súčasťou úpravy by malo byť aj vymedzenie úrovne prístupu, napríklad či pôjde o prístup iba na čítanie, administrátorské oprávnenia alebo oprávnenia umožňujúce vykonávať zmeny v systémoch).

- **Oprávnenie pristupovať k sieťovým zariadeniam** – Zmluva by mala určiť, či je poskytovateľ oprávnený iba získavať informácie a logy zo zariadení alebo aj vykonávať zmeny ich konfigurácie. V prípade oprávnenia vykonávať zásahy by mali byť jasne definované podmienky schvaľovania takýchto úkonov a osoby oprávnené udeľovať súhlas.
- **Oprávnenie analyzovať používateľské účty** - Vzhľadom na možný zásah do súkromia zamestnancov a spracúvanie osobných údajov by mala zmluva jasne definovať rozsah takéhoto oprávnenia, účel spracúvania získaných údajov a pravidlá ich ochrany. Zároveň je potrebné zabezpečiť súlad s právnymi predpismi o ochrane osobných údajov a pracovnoprávnymi predpismi.
- **Oprávnenie získavať logy a záznamy** - Definovanie aké typy logov môže poskytovateľ získavať a spracúvať, napríklad systémové logy, aplikačné logy, sieťové záznamy, autentifikačné záznamy, záznamy z bezpečnostných riešení alebo cloudových služieb.
- **Oprávnenie vytvárať forenzné kópie dát** - Keďže vytváranie forenzných kópií predstavuje zásah do informačného prostredia klienta a môže zahŕňať spracúvanie veľkého objemu údajov vrátane osobných údajov alebo obchodného tajomstva, zmluva by mala presne určiť rozsah tohto oprávnenia. Odporúča sa upraviť spôsob vytvárania forenzných obrazov, požiadavky na zachovanie integrity dát, evidenciu reťazca dôkazov (Chain of Custody), dobu uchovávanía získaných kópií a podmienky ich bezpečného zničenía alebo odovzdania klientovi po ukončení vyšetrovania.
- **Oprávnenie vykonávať aktívne zásahy do systémov** – Vzhľadom na to, že tieto činnosti môžu mať významný vplyv na dostupnosť systémov a prevádzku klienta, odporúča sa presne definovať, ktoré úkony môže poskytovateľ vykonávať samostatne, ktoré podliehajú predchádzajúcemu schváleniu klienta a ktoré sú prípustné iba v prípade kritického alebo bezprostredne hroziaceho incidentu.
- **Oprávnenie využívať automatizované nástroje** - Zmluva by mala upraviť rozsah používania automatizovaných nástrojov, zodpovednosť za ich konfiguráciu, podmienky ich nasadenia v produkčnom prostredí a prípadné obmedzenia týkajúce sa automatizovaných zásahov bez priameho zásahu človeka.
- **Podmienky zapojenia subdodávateľov alebo iných externých subjektov** - Úprava povinnosti predchádzajúceho súhlasu klienta, požiadaviek na odbornú spôsobilosť subdodávateľov a iných externých subjektov, rozsahu informácií, ku ktorým môžu získať prístup, ako aj povinnosti zabezpečiť rovnakú úroveň ochrany informácií, aká sa vyžaduje od hlavného poskytovateľa. Zodpovednosť za činnosť subdodávateľov a iných externých subjektov by mala zostať zachovaná na strane poskytovateľa, pokiaľ zmluva výslovne neustanovuje inak.

Povinnosti klienta

Na rozdiel od mnohých iných služieb nie je poskytovateľ spravidla schopný vykonávať svoje činnosti samostatne bez aktívnej súčinnosti klienta, jeho zamestnancov alebo zodpovedných osôb. Úspešnosť vyšetrovania bezpečnostného incidentu, kvalita forenznej analýzy a schopnosť efektívne reagovať na bezpečnostné hrozby preto vo významnej miere závisia od rozsahu a kvality poskytovanej súčinnosti.

Zmluva by mala jednoznačne upraviť povinnosti klienta a zároveň definovať dôsledky ich nesplnenia. Nedostatočná alebo oneskorená súčinnosť môže viesť k predĺženiu reakčných časov, strate dôkazov, obmedzeniu možností vyšetrovania alebo k nemožnosti dosiahnuť požadované výsledky.

Medzi základné povinnosti klienta, ktoré by mala zmluva upravovať, patria najmä nasledujúce oblasti:

- zabezpečenie prístupu k systémom;
- poskytovanie potrebnej dokumentácie;
- určenie kontaktných osôb;
- poskytovanie pravdivých a úplných informácií;
- zabezpečenie spolupráce zamestnancov;
- vytváranie podmienok pre výkon služieb.

Na zabezpečenie jednoznačného rozdelenia právomocí a zodpovedností počas riešenia incidentov sa odporúča vypracovať maticu zodpovedností (RACI matrix). Ide o jeden z najefektívnejších nástrojov na elimináciu chaosu, ku ktorému dochádza počas kritického kybernetického incidentu. V zmluvách o poskytovaní DFIR služieb (najmä pri zmluvách typu *Incident Response Retainer - zmluva o rezervácii kapacít na reakciu na incidenty*) by mala byť RACI matica **priamou zmluvnou prílohou**, čím sa z nej stáva právne záväzný dokument. Pre potreby DFIR zmlúv sa používa štandardné delenie úloh: Nasledujúca RACI matica predstavuje ilustratívny príklad, ktorý je potrebné v každom konkrétnom prípade prispôbiť organizačnej štruktúre klienta, jeho právnym a regulačným povinnostiam a dohodnutému rozsahu služieb poskytovateľa.

- **R – Responsible (Zodpovedný za realizáciu):** Ten, kto reálne vykonáva technickú alebo organizačnú prácu.
- **A – Accountable (Konečne zodpovedný / Schvaľovateľ):** Osoba s rozhodovacou právomocou. Má právo vetovať alebo schváliť krok (v RACI matici pre danú úlohu smie byť vždy **iba jedno písmeno A**, spravidla na strane klienta).
- **C – Consulted (Konzultovaný):** Expert, ktorého názor alebo analýza sú potrebné pred vykonaním kroku (napr. právne oddelenie, externý forenzný tím).
- **I – Informed (Informovaný):** Osoba, ktorej sa iba oznamuje výsledok alebo stav po vykonaní kroku (napr. manažment, PR oddelenie).

Fáza incidentu / konkrétna úloha	Klient	Poskytovateľ	DPO	Vedenie
1. Detekcia, triáž a aktivácia				
Identifikácia podozrivej aktivity a prvotný zber logov	R	C	I	I

Aktivácia DFIR zmluvy (vyhlásenie incidentu) a spustenie SLA	C	R	I	A
2. Izolácia a Mitigácia (Zadržanie útoku)				
Rozhodnutie o odstavení produkcie (vypnutie infraštruktúry/internetu)	C	C	I	A
Technická realizácia izolácie napadnutých systémov a sietí	R	R/C		I
Zmena kompromitovaných prístupových údajov a admin účtov	R	C		I
3. Forenzná akvizícia a analýza				
Zabezpečenie forenzných dôkazov (RAM, HDD) podľa štandardov	C	R	I	I
Hĺbková analýza malvéru, logov a určenie vektora útoku (Koreňová príčina)	C	R		I
Identifikácia rozsahu kompromitovaných dát (či nastal únik/únos dát)	C	R	C	I
4. Sanácia a Obnova				
Schválenie stratégie obnovy (napr. obnova zo záloh vs. vyjednávanie)	C	C	C	A
Vyčistenie perzistencie útočníka (backdoors) z infraštruktúry	R	R/C		I
Finálny bezpečnostný audit (hardening) pred spustením produkcie	R	R		I
5. Právne povinnosti a uzatvorenie				

Hlásenie incidentu na NBÚ / CSIRT (v lehotách podľa aplikovateľnej právnej úpravy)	I	R	C	A
Posúdenie rizika a hlásenie na ÚOOÚ v zmysle GDPR (lehota 72 hod.)	I	R	C	I
Vypracovanie finálnej Forenznej expertnej správy	I	R	C	I

Tabuľka č. 2 – Vzor RACI matice

Špecifiká pri využívaní nástrojov umelej inteligencie a automatizácie

Zmluvná dokumentácia musí reflektovať špecifické právne a technologické riziká s tým spojené. Pri koncipovaní zmluvy je potrebné implementovať nasledujúce záruky:

- Algoritmická transparentnosť a overiteľnosť (Explainable AI) a forezná integrita:**
 Zmluva by mala upravovať postup poskytovateľa tak, aby závery, detekcie, selekcie dát alebo identifikácie digitálnych stôp získané prostredníctvom automatizovaných nástrojov boli v primeranom rozsahu spätne overiteľné, zdokumentované a preskúmateľné kvalifikovaným odborníkom. Zmluvná dokumentácia by mala podľa povahy používaného nástroja upraviť uchovávanie informácií potrebných na spätné preverenie výsledku, najmä údajov o použítom nástroji a jeho verzii, relevantných vstupoch, parametroch analýzy, časových údajoch a dostupných logoch analytického procesu. Vhodné je zároveň upraviť povinnosť poskytovateľa na požiadanie poskytnúť, v primeranom rozsahu a pri rešpektovaní ochrany práv duševného vlastníctva a dôverných informácií, informácie o použitej metodike, princípoch fungovania nástroja a známych obmedzeniach automatizovanej analýzy, ak sú potrebné na overenie alebo posúdenie výsledku. Ak sa má výsledok automatizovanej analýzy použiť ako podklad v súdnom, správnom alebo inom právnom konaní, jeho dostatočná dokumentácia a možnosť odborného preskúmania môžu byť významné pre posúdenie jeho dôveryhodnosti a dôkaznej hodnoty.
- Vlastníctvo dát, ochrana duševného vlastníctva a doložky o trénoch modelov:**
 Zmluva by mala upraviť, či a za akých podmienok je poskytovateľ oprávnený používať dáta klienta v systémoch umelej inteligencie. Bez výslovného zmluvného a právneho základu by poskytovateľ ani jeho subdodávateľia nemali dáta klienta používať na ďalšie tréningovanie, ladenie (fine-tuning) alebo validáciu modelov nad rámec účelu, na ktorý boli sprístupnené. Ak zmluva takéto ďalšie použitie výslovne umožňuje, mala by presne určiť jeho účel a rozsah, kategórie údajov, podmienky anonymizácie alebo inej primeranej úpravy údajov, ochranu osobných údajov, dôverných informácií a obchodného tajomstva, ako aj pravidlá nakladania s údajmi po skončení zmluvného vzťahu. Zmluvné strany by mali zároveň jasne určiť práva k finálnym analytickým výstupom, skriptom a ďalším výsledkom vytvoreným počas incidentu.

- **Alokácia zodpovednosti za chyby automatizácie, asymetriu detekcie a prevádzkové škody:** Zmluva by mala primerane upraviť rozdelenie rizík a zodpovednosti za chyby automatizácie, vrátane nesprávnej detekcie, prehliadnutia hrozby a prevádzkových škôd spôsobených automatizovaným zásahom. Vhodné je zmluvne vymedziť tzv. stupne autonómie a určiť kategórie incidentov, podmienky alebo prahové hodnoty, pri ktorých môže byť konkrétny automatizovaný zásah vykonaný bez predchádzajúceho ľudského schválenia; pri ostatných prípadoch by mal byť výsledok alebo navrhovaný zásah predmetom primeraného ľudského overenia. Rozsah zodpovednosti poskytovateľa je potrebné posudzovať podľa konkrétnych zmluvných povinností a okolností prípadu, najmä s prihliadnutím na požadovanú odbornú starostlivosť, dohodnutú mieru autonómie nástroja, jeho primeranú aktualizáciu a údržbu, rozsah ľudského overovania a kogentné limity platnej právnej úpravy. Zmluva by preto nemala automaticky vylučovať zodpovednosť za prehliadnutú hrozbu ani vytvárať dojem, že automatizovaný nástroj garantuje bezchybný výsledok.

Úprava SLA a reakčných časov

Pri poskytovaní služieb digitálnej forenznej analýzy a reakcie na kybernetické incidenty predstavuje dohoda o úrovni poskytovaných služieb (Service Level Agreement – SLA) jednu z najvýznamnejších častí zmluvnej dokumentácie. SLA ustanovenia určujú očakávanú úroveň dostupnosti služieb, reakčné časy poskytovateľa, pravidlá komunikácie a postupy riešenia incidentov. Ich správne nastavenie má zásadný význam pre efektívne zvládanie bezpečnostných incidentov, riadenie očakávaní klienta a predchádzanie sporom počas plnenia zmluvy.

Na rozdiel od bežných IT služieb môže mať pri DFIR službách aj krátke oneskorenie reakcie významný vplyv na rozsah škôd, dostupnosť informačných systémov, zachovanie digitálnych dôkazov alebo splnenie zákonných oznamovacích povinností. Z tohto dôvodu by mali byť SLA parametre formulované jednoznačne, merateľne a spôsobom, ktorý umožňuje objektívne posúdiť ich plnenie.

Z praxe vyplýva, že SLA najčastejšie upravujú nasledovné oblasti:

- **Dostupnosť služieb** – Presné definovanie časového rozsahu, v ktorom je poskytovateľ povinný zabezpečovať svoje služby. Rozsah dostupnosti závisí od charakteru klienta, úrovne rizika a významu poskytovaných služieb. V praxi môže ísť napríklad o poskytovanie služieb počas pracovných dní v určenom čase alebo o nepretržitú dostupnosť v režime 24/7. Pri kritickej infraštruktúre, významných prevádzkovateľoch alebo organizáciách s vysokými požiadavkami na kontinuitu prevádzky sa spravidla vyžaduje nepretržitá dostupnosť incident response tímu. Zmluva by mala zároveň upravovať spôsob zabezpečenia dostupnosti, minimálne personálne kapacity a podmienky poskytovania služieb počas dní pracovného pokoja, sviatkov alebo mimoriadnych situácií.
- **Spôsob oznamovania incidentov** – Zmluva by mala upravovať komunikačné kanály, prostredníctvom ktorých môže klient incident oznámiť, ako aj minimálne informácie,

ktoré musí oznámenie obsahovať. V závislosti od charakteru služieb môže byť incident oznamovaný prostredníctvom telefonickej linky, e-mailu, zákaznickeho portálu, ticketovacieho systému alebo iného komunikačného nástroja. Súčasne je vhodné určiť, ktoré spôsoby oznámenia sa považujú za oficiálne nahlásenie incidentu, od ktorého začínajú plynúť SLA lehoty.

- **Reakčné časy** – Ide o tzv. časový interval medzi nahlásením incidentu a prvou reakciou poskytovateľa. Reakciou sa pritom nemusí rozumieť samotné vyriešenie incidentu, ale napríklad potvrdenie prijatia hlásenia, začatie komunikácie s klientom alebo vykonanie úvodného posúdenia situácie. Pri určovaní reakčných časov je vhodné zohľadniť závažnosť incidentu a jeho potenciálny dopad na činnosť klienta. Kritické incidenty si spravidla vyžadujú reakciu v priebehu niekoľkých minút alebo hodín, zatiaľ čo menej závažné udalosti môžu podliehať dlhším reakčným lehotám.
- **Lehoty na začatie zásahu** – Odporúča sa upraviť aj maximálnu dobu, v ktorej musí poskytovateľ začať vykonávať konkrétne činnosti smerujúce k riešeniu incidentu.
- **Kategorizáciu incidentov** – Keďže nie všetky bezpečnostné incidenty majú rovnakú závažnosť, SLA by mala obsahovať pravidlá ich klasifikácie. Kategorizácia incidentov umožňuje prispôbiť reakčné časy a rozsah opatrení ich skutočnému významu. Kritériami klasifikácie môžu byť najmä rozsah ohrozenia informačných aktív, dopad na prevádzku organizácie, počet dotknutých systémov, riziko úniku údajov, finančné dopady alebo potenciálne regulačné dôsledky. Odporúča sa definovať niekoľko úrovní závažnosti, pričom ku každej úrovni by mali byť priradené konkrétne reakčné časy, eskalačné pravidlá a požadované opatrenia.
- **Eskalačné postupy** – Počas riešenia bezpečnostných incidentov môže vzniknúť potreba zapojenia ďalších odborníkov alebo manažérskych úrovní na strane klienta alebo poskytovateľa. Z tohto dôvodu by mala zmluva obsahovať jasne definované eskalačné mechanizmy. Eskalačné postupy by mali upravovať podmienky eskalácie, osoby oprávnené prijímať rozhodnutia, spôsob komunikácie a časové lehoty na riešenie eskalovaných situácií. Osobitnú pozornosť je potrebné venovať incidentom s potenciálnym dopadom na kritické procesy organizácie, ochranu osobných údajov alebo plnenie zákonných povinností.
- **Dostupnosť kontaktných osôb** – Je nevyhnutné určiť osoby, ktoré budú oprávnené komunikovať počas riešenia bezpečnostného incidentu, schvaľovať vykonanie jednotlivých úkonov a prijímať rozhodnutia nevyhnutné na zabezpečenie alebo obnovu prevádzky informačných systémov.
- **Sankcie za nedodržanie SLA** – Ich účelom nie je primárne sankcionovať druhú stranu, ale vytvoriť motivačný nástroj na dodržiavanie zmluvných povinností a zabezpečiť predvídateľnosť poskytovaných služieb. V prípade DFIR služieb sa sankcie najčastejšie viažu na nedodržanie reakčných časov, nedostupnosť dohodnutých odborných kapacít, nesplnenie termínov dodania výstupov alebo porušenie povinností súvisiacich s komunikáciou počas incidentu. V praxi sa často využívajú zmluvné pokuty, zľavy z odmeny za služby, poskytovanie dodatočných služieb bezplatne alebo iné kompenzačné mechanizmy. Zároveň je vhodné upraviť prípady, v ktorých sa sankcie neuplatnia, napríklad pri zásahu vyššej moci, nedostatočnej súčinnosti klienta alebo pri technických prekážkach spôsobených tretími stranami.

Integrálnou súčasťou úpravu reakčných časov bývajú aj tzv. matice závažnosti incidentov (Incident Severity Matrix). Definuje, ako rýchlo musí poskytovateľ reagovať (SLA) a aké zdroje musí na oboch stranách incident aktivovať. Bez nej hrozí, že klient bude vyžadovať okamžitý zásah kvôli zavírenému notebooku sekretárky, alebo naopak podcení tichý prienik. Matica závažnosti nemá zmluvnú hodnotu, ak na ňu nenaviazete **SLA (Service Level Agreement)**.

V zmluve je vhodné vymedziť klasifikáciu incidentov, pri ktorej je potrebné zohľadniť najmä:

- Biznisový dopad a kontinuita činností (Business Impact)
- Rozsah a rýchlosť šírenia incidentu (Scope & Velocity)
- Právny dopad, regulácia a povaha dát (Compliance & Data Sensitivity)
- Kontext a motivácia útočníka (Threat Actor Context)

Pri implementácii matice do zmluvy sa odporúča zaviesť pravidlo, že **výslednú závažnosť incidentu určuje najhorší dosiahnutý ukazovateľ v ktorejkoľvek kategórii**.

Zmluvy o poskytovaní služieb v oblasti DFIR, resp. na nich nadväzujúce SLA zmluvy najčastejšie upravujú kategorizáciu závažnosti incidentu podľa jeho stupňa (napr. kritický, stredný, vysoký, nízky) pričom na to nadväzuje aj popis, resp. charakteristika incidentu (napr. Incident s bezprostredným dopadom na fungovanie organizácie alebo s vysokým rizikom závažných škôd). Ak je na základe charakteristiky definovaná úroveň závažnosti incidentu, je nevyhnutné prepojiť tieto činitele na odporúčaný reakčný čas, teda na **maximálnu zmluvne garantovanú lehotu, do ktorej musí poskytovateľ DFIR služieb začať aktívne konať** od momentu, kedy mu klient oficiálne nahlási kybernetický incident. Zmluva môže obsahovať jednoduché určenie reakčného času (napr. do 2 hodín) alebo podrobnejšie určenie, a to napríklad s poukazom na dostupnosť, prvú odozvu a následne s poukazom na začiatok analýzy.

Vymedzenie reakčného času fázovito a exaktne je pre úspech forenzného vyšetrovania a právnu bezpečnosť zmluvy vhodnejší. Kybernetický incident v prostredí organizácie predstavuje dynamickú krízu, kde sekundy rozhodujú o rozsahu škôd a zachovaní dôkaznej situácie. Ak by bol reakčný čas definovaný len jedným sumárnym odhadom, poskytovateľ by bol v zmluvnom súlade aj vtedy, ak by počas celých dvoch hodín iba interné tímy koordinovali logistiku. Fázovité delenie zabezpečuje, že kým sa organizuje prípadný fyzický presun expertov na miesto incidentu (**on-site reakcia**), vzdialený tím už v prvej fáze (**vzdialená reakcia**) aktívne vykonáva izoláciu siete, blokovanie riadiacich serverov útočníka a zastavuje šírenie škôd.

Ochrana dôverných informácií

Ako bolo uvedené už v rámci predzmluvnej fázy, sprístupňovanie dôverných informácií v oblasti DFIR je jeho neoddeliteľnou súčasťou. Charakter týchto informácií spôsobuje, že ich neoprávnené sprístupnenie môže viesť nielen k majetkovej škode, ale aj k vzniku nových bezpečnostných incidentov, poškodeniu reputácie organizácie alebo k porušeniu zákonných povinností. **Zmluva by mala v prvom rade obsahovať dostatočne presnú definíciu dôverných informácií. Príliš úzka definícia môže viesť k tomu, že určitá kategória citlivých údajov**

nebude požívať zmluvnú ochranu, zatiaľ čo príliš všeobecná definícia môže spôsobovať interpretačné problémy a neistotu pri plnení zmluvy. V prostredí DFIR sa odporúča, aby definícia zahŕňala nielen informácie označené ako dôverné, ale aj všetky technické, organizačné, prevádzkové, bezpečnostné, ekonomické a právne informácie získané počas poskytovania služieb bez ohľadu na formu ich sprístupnenia.

Ochrana osobných údajov

Vzhľadom na charakter služieb v oblasti DFIR sa často predpokladá prístup poskytovateľa k informačným systémom klienta, elektronickej komunikácii, bezpečnostným logom, zálohám, dátovým úložiskám alebo digitálnym dôkazom, ktoré môžu obsahovať osobné údaje zamestnancov, zákazníkov, obchodných partnerov alebo iných fyzických osôb.

Prvým krokom pri príprave zmluvnej dokumentácie by malo byť posúdenie, či a v akom rozsahu bude počas poskytovania služieb dochádzať k spracúvaniu osobných údajov. S tým úzko súvisí aj určenie právneho postavenia jednotlivých zmluvných strán. Vo väčšine prípadov bude klient vystupovať ako prevádzkovateľ podľa článku 4 ods. 7 GDPR, keďže určuje účel a dôvody spracúvania osobných údajov. Poskytovateľ DFIR služieb bude spravidla vystupovať ako sprostredkovateľ podľa článku 4 ods. 8 GDPR a bude vykonávať jednotlivé spracovateľské operácie na základe pokynov klienta. V určitých prípadoch však môže byť právne postavenie odlišné. Môže ísť napríklad o vypracovanie znaleckého posudku, expertíznej správy alebo o situácie, keď poskytovateľ spracúva údaje na základe vlastnej zákonnej povinnosti. V prípade, ak je poskytovateľ služieb sprostredkovateľom je nevyhnutné v zmysle GDPR **uzatvoriť zmluvu o spracúvaní osobných údajov**. Zmluva musí obsahovať náležitosti vyžadované článkom 28 GDPR, a teda mal by v nej byť jasne definovaný účel spracúvania, rozsah vykonávaných operácií, kategórie osobných údajov, kategórie dotknutých osôb, doba spracúvania, ako aj práva a povinnosti oboch strán. Dôležitou súčasťou zmluvnej úpravy sú aj technické a organizačné opatrenia podľa článku 32 GDPR. Poskytovateľ by mal disponovať primeranými bezpečnostnými opatreniami zodpovedajúcimi rizikám spojeným so spracúvaním údajov. Vzhľadom na špecializovaný charakter DFIR služieb nemožno opomenúť ani otázku využívania subdodávateľov. Poskytovateľ môže pri plnení svojich povinností využívať externých expertov, cloudové služby alebo špecializované laboratória. Zmluva by preto mala upravovať podmienky ich zapojenia, rozsah údajov, ku ktorým môžu mať prístup, a zodpovednosť poskytovateľa za ich činnosť. Súčasťou ochrany osobných údajov sú aj ustanovenia týkajúce sa cezhraničného prenosu osobných údajov. Mnohé forenzné nástroje, cloudové služby alebo analytické platformy využívajú infraštruktúru umiestnenú mimo Slovenskej republiky alebo mimo Európskeho hospodárskeho priestoru. Zmluva by preto mala jasne upraviť, či môže dochádzať k prenosu údajov do tretích krajín, na akom právnom základe sa takýto prenos uskutočňuje a aké ochranné mechanizmy budú použité na zabezpečenie súladu s kapitolou V GDPR. Neopomenuteľnou súčasťou zmluvy o spracúvaní osobných údajov je aj úprava uchovávania

a likvidácie osobných údajov po skončení poskytovania služieb; úprava riešenia bezpečnostných incidentov týkajúcich sa ochrany osobných údajov.²

Nakladanie s digitálnymi dôkazmi

Jedným z kľúčových ustanovení v zmluvách týkajúcich sa poskytovanie služieb v oblasti DFIR je úprava nakladania s digitálnymi dôkazmi. Zmluva upravujúca poskytovanie DFIR služieb musí teda obsahovať osobitnú časť venovanú nakladaniu s digitálnymi dôkazmi, keďže ide o materiál, ktorý môže byť následne použitý v trestnom, civilnom alebo správnom konaní a zároveň často obsahuje osobné údaje. Z tohto dôvodu nestačí všeobecná úprava IT služieb, ale je nevyhnutné presne definovať terminológiu, ale aj procesy, ktoré zabezpečia právnu použiteľnosť a technickú integritu dôkazov.

V prvom rade musí zmluva **jednoznačne vymedziť, čo sa považuje za digitálny dôkaz**. Bez tejto definície vzniká neistota, na ktoré dáta sa vzťahujú povinnosti poskytovateľa DFIR služieb a ktoré výstupy majú povahu dôkazného materiálu. Do tejto kategórie sa spravidla zahŕňajú systémové a aplikačné logy, sieťové záznamy, diskové a pamäťové obrazy, elektronická komunikácia a auditné záznamy z cloudových prostredí. Presné vymedzenie je dôležité najmä preto, že zabráňuje sporom o rozsah zodpovednosti a určuje, ktoré dáta musia byť spracované forenzným spôsobom. Základné rozdiely oproti stopám z reálneho sveta sú najmä:

- Nehmotnosť;
- Latentnosť;
- Časová trasovateľnosť;
- Vysoká obsažnosť;
- Reštaurovateľnosť;
- Originálnosť;
- Priestor;
- Šifrovanie.

Ďalšou nevyhnutnou oblasťou je spôsob získavania digitálnych dôkazov. Zmluva by mala stanoviť, že akvizícia sa vykonáva forenzne korektným spôsobom, podľa povahy prípadu napríklad vytvorením bitovej kópie pôvodných dát, pričom zásahy do pôvodných systémov a dát majú byť obmedzené na nevyhnutný rozsah. Takýto postup podporuje zachovanie integrity a následnú overiteľnosť dôkazov. Ak zmluvná dokumentácia pravidlá získavania a dokumentovania digitálnych dôkazov neupravuje dostatočne, zvyšuje sa riziko spochybnenia spôsobu ich získania, autenticity, integrity alebo dôkaznej hodnoty a následne aj ich použiteľnosti v príslušnom konaní.

² HUDECOVÁ, Irena – CYPRICHOVÁ, Anna – MAKATURA, Ivan a kol. *Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR. Veľký komentár. 2. zväzok. 2. aktualizované vydanie*. Žilina: EUROKÓDEX, 2020

Slovenský právny poriadok požiadavky na zaobchádzanie s digitálnymi stopami explicitne nedefinuje a neustanovuje jednotné špecifické nároky na všetky postupy alebo obsah digitálnej forenznej analýzy. Po právnej stránke je rozhodujúce najmä to, aby boli dôkazy získané a použité v súlade s pravidlami príslušného konania. Porušenie pravidiel pri ich získavaní, zabezpečení alebo spracovaní môže viesť k spochybneniu ich zákonnosti, autenticity, integrity alebo dôkaznej hodnoty a v závislosti od konkrétneho procesného režimu aj k obmedzeniu alebo vylúčeniu ich použiteľnosti.

Vo vzťahu k spôsobu získania digitálnych dôkazov (ale aj k následnému zabezpečeniu a uschovávaniu dôkazov) je dôležitá **úprava reťazca držby (chain of custody)**, ktorý zabezpečuje sledovateľnosť každého pohybu a zásahu do dôkazu. Zmluva musí vyžadovať, aby bol každý dôkaz evidovaný od momentu jeho získania až po jeho archiváciu alebo zničenie, pričom musí byť zaznamenané kto, kedy a akým spôsobom s dôkazom manipuloval. Tento prvok je v praxi rozhodujúci, pretože ak chýba kontinuita reťazca držby, dôkaz môže byť ľahko spochybnený ako neautentický alebo neoveriteľný.

Popri zachovaní integrity a reťazca držby je potrebné zabezpečiť aj preukázateľnosť pôvodu a zákonnosti získania digitálnych dôkazov. Zmluvná dokumentácia by preto mala podľa povahy služby umožňovať spätne identifikovať zdroj údajov, spôsob a okolnosti ich získania, osobu alebo subjekt, ktorý ich poskytol, a právny alebo zmluvný základ oprávňujúci na ich získanie a spracovanie. Osobitný význam má táto požiadavka v prípadoch, keď sa predpokladá neskoršie použitie výstupov DFIR analýzy v súdnom alebo správnom konaní (porov. rozsudok Najvyššieho správneho súdu SR sp. zn. 4Sfk/110/2022 z 24. 4. 2024).

V nadväznosti na vyššie uvedené, tak zmluva musí zároveň upravovať aj **spôsob uchovávania a zabezpečenia dôkazov**. Dôkazy musia byť uložené v prostredí, ktoré zabezpečuje ich ochranu pred neoprávneným prístupom, zmenou alebo vymazaním. To zahŕňa šifrovanie dát, riadenie prístupových práv, oddelenie forezného úložiska od produkčných systémov a povinnosť logovania všetkých operácií.

Dôležitou súčasťou zmluvy je aj **úprava analytickej fázy**. Zmluva by mala vyžadovať, aby sa analýza podľa povahy incidentu vykonávala spôsobom minimalizujúcim zásah do pôvodných dát a, ak je to možné a primerané, na forezných kópiách. Významné postupy a zásahy by mali byť zdokumentované tak, aby boli preskúmateľné a v primeranom rozsahu reprodukovateľné. Tento aspekt je zásadný z hľadiska kontroly výsledkov, pretože v prípade sporu musí byť možné overiť, že závery DFIR analýzy sú technicky podložené a nezávisle overiteľné. Ak by tieto požiadavky neboli primerane upravené a dokumentované, výsledky analýzy môžu byť z hľadiska ich následného právneho použitia oslabené.

Napriek tomu, že sme sa úpravou osobných údajov v rámci zmlúv v oblasti poskytovanie DFIR zaoberali už vyššie, je potrebné zohľadniť aj osobné údaje obsiahnuté v získaných a uložených digitálnych dôkazoch. Je potrebné určiť právny základ spracúvania, zabezpečiť minimalizáciu údajov a obmedzenie účelu spracúvania na riešenie incidentu. V opačnom prípade hrozí porušenie GDPR, ktoré môže viesť k sankciám a zodpovednosti oboch zmluvných strán.

Poznanie zásad spracúvania digitálnych dôkazov umožní zmluvným stranám lepšie nastaviť zmluvné podmienky, čo sa odzrkadlí najmä pri ustanoveniach týkajúcich sa nakladania s digitálnymi dôkazmi. Medzi základné zásady spracovania digitálnych dôkazov radíme:

- **Integrita dôkazov** – zásahy do pôvodných dát je potrebné obmedziť na nevyhnutný rozsah a riadne dokumentovať; ak to povaha incidentu umožňuje, analytické úkony sa vykonávajú na forenzných kópiách.
- **Autenticita** – musí byť preukázateľné, že dôkaz pochádza z deklarovaného zdroja.
- **Auditovateľnosť** – každý úkon s dôkazom musí byť dokumentovaný a spätne rekonštruovateľný.
- **Nemennosť (immutability)** – originálne dáta by mali byť v maximálnej možnej miere uchovávané v zabezpečenom stave chrániacom ich pred neoprávnenou zmenou; nevyhnutné zásahy musia byť dokumentované.

V procese uzatvárania zmluvy v oblasti poskytovania DFIR a úpravy zmluvných dojednaní týkajúcich sa nakladania s digitálnymi **dôkazmi je dôležité, aby zmluvné strany brali na zreteľ aj právnu úpravu, po prípade usmernenia alebo štandardy** týkajúce sa tejto problematiky. Usmernenia pre špecifické činnosti pri zaobchádzaní s digitálnymi stopami poskytuje už napríklad medzinárodná technická norma **ISO/IEC 27037:2012** Informačné technológie – Bezpečnostné metódy Návod na identifikáciu, zber, získavanie a uchovávanie digitálnych dôkazov 4, vydaná medzinárodnou štandardizačnou organizáciou. Návod uvedený v ISO/IEC 27037 je vhodné dodržiavať pri každom vyšetrovaní, ktorého cieľom je zachovanie integrity, pôvodu a nepopierateľnosti digitálnych stôp a ktorého cieľom je uplatnenie takých metód pri získavaní potenciálnych digitálnych dôkazov, ktoré prispievajú k ich prípustnosti v trestnoprávných, či občianskoprávných sporoch, či správnych alebo disciplinárnych konaniach, ako aj v iných príslušných prípadoch. Norma ISO/IEC 27037 sa však nevzťahuje na spôsob analýzy digitálnych stôp. Analýza a ostatné procesy súvisiace a forenznými vedami a manažmentom digitálnych stôp sú čiastočne opísané v niekoľkých technických normách, napríklad v norme **ISO 21043-2:2018** Forensic sciences – Part 2: Recognition, recording, collecting, transport and storage of items, ktorá špecifikuje požiadavky na forenzný proces, najmä rozpoznávanie, evidenciu, zhromažďovanie, prepravu a uchovávanie vecí s potenciálnou forenznou hodnotou. Zahŕňa požiadavky na posudzovanie a skúmanie scén, ale vzťahuje sa aj na činnosti, ktoré sa vyskytujú v zariadení. Obsahuje aj požiadavky na kvalitu.³

Zodpovednosť za škodu

Úprava zodpovednosti patrí medzi najdôležitejšie časti zmluvy o poskytovaní služieb digitálnej forenzej analýzy a reakcie na kybernetické incidenty. Vzhľadom na povahu týchto služieb, ktoré zahŕňajú prístup k informačným systémom, spracúvanie citlivých údajov, prácu

³ Porov. MAKATURA, Ivan. Ciele dokazovania v kybernetickej bezpečnosti. In: Acta Facultatis Iuridicae Universitatis Comenianae, 2023, roč. 42, č. 1, s. 116 – 146.

s digitálnymi dôkazmi a realizáciu zásahov do produkčných prostredí klienta, môžu mať pochybenia jednej zo strán významné právne, finančné, prevádzkové aj reputačné následky. Cieľom zmluvnej úpravy zodpovednosti je **vytvoriť jasný rámec pre určenie práv a povinností strán v prípade vzniku škody, bezpečnostného incidentu, porušenia zmluvných povinností alebo iných nežiaducich udalostí**. Zároveň umožňuje primerane rozdeliť riziká medzi klienta a poskytovateľa a predchádzať sporom týkajúcim sa rozsahu zodpovednosti za vzniknuté následky.

Pri príprave DFIR zmluvy je potrebné zohľadniť, že poskytovateľ často pracuje v prostredí, ktoré je už kompromitované alebo postihnuté bezpečnostným incidentom. Samotná existencia incidentu preto automaticky neznamená zodpovednosť poskytovateľa za vzniknutú škodu. Rozsah jeho zodpovednosti musí byť posudzovaný vo vzťahu ku konkrétnym zmluvným povinnostiam a vykonaným činnostiam.

Všeobecná zodpovednosť za plnenie zmluvy

Každá zo zmluvných strán zodpovedá za riadne plnenie svojich povinností vyplývajúcich zo zmluvy. Poskytovateľ je povinný vykonávať služby s odbornou starostlivosťou, v súlade s aktuálnymi poznatkami v oblasti digitálnej forenziky, kybernetickej bezpečnosti a incident response. Klient je naopak povinný poskytovať potrebnú súčinnosť, zabezpečiť prístup k relevantným systémom a poskytovať pravdivé a úplné informácie potrebné na výkon služieb.

Zmluva by mala jasne definovať, že **poskytovateľ zodpovedá za odborné vykonanie dohodnutých činností, nie však za okolnosti, ktoré nemôže ovplyvniť**, ako sú napríklad neúplnosť poskytnutých údajov, skryté technické nedostatky prostredia klienta alebo následky incidentov vzniknutých pred začatím poskytovania služieb.

V DFIR prostredí je obzvlášť dôležité **odlíšiť zodpovednosť za samotný výkon služieb od zodpovednosti za výsledok vyšetrovania**. Poskytovateľ môže vykonať všetky potrebné úkony s odbornou starostlivosťou, avšak vzhľadom na charakter digitálnych dôkazov nemusí byť vždy možné jednoznačne identifikovať pôvodcu incidentu alebo obnoviť všetky stratené údaje. Poskytovateľ by teda mal nieť zodpovednosť za škodu spôsobenú porušením svojich zmluvných alebo zákonných povinností. Môže ísť najmä o situácie, keď:

- vykoná zásah do systémov bez potrebného oprávnenia,
- poruší dohodnuté bezpečnostné postupy,
- neoprávnene sprístupní dôverné informácie,
- nezabezpečí ochranu získaných údajov,
- poruší povinnosti pri spracúvaní osobných údajov,
- nezachová integritu digitálnych dôkazov,
- použije nevhodné alebo neprimerané forenzné postupy,
- nedodrží dohodnuté SLA parametre.

Zodpovednosť poskytovateľa by však mala byť posudzovaná s prihliadnutím na povahu poskytovaných služieb. DFIR služby často zahŕňajú činnosti vykonávané v časovej tiesni, pri nedostatku informácií a v prostredí, ktoré je ovplyvnené bezpečnostným incidentom. Pri hodnotení zodpovednosti je preto potrebné prihliadať na okolnosti konkrétneho prípadu a na odborné štandardy platné v čase vykonávania zásahu.

Zodpovednosť klienta

Zmluvná úprava by nemala riešiť iba zodpovednosť poskytovateľa, ale aj zodpovednosť klienta za plnenie jeho povinností. V praxi býva úspech vyšetrovania alebo reakcie na incident významne ovplyvnený kvalitou spolupráce zo strany klienta.

Klient môže niesť zodpovednosť najmä za:

- poskytnutie neúplných alebo nepravdivých informácií,
- neposkytnutie potrebnej súčinnosti,
- oneskorené oznámenie incidentu,
- neposkytnutie prístupu k systémom alebo údajom,
- porušenie odporúčaných bezpečnostných opatrení,
- neplnenie povinností vyplývajúcich zo zmluvy,
- neoprávnené zásahy do vyšetrovaného prostredia počas analýzy.

Ak konanie alebo opomenutie klienta znemožní alebo podstatne sťaží poskytovanie služieb, zmluva by mala upravovať možnosť obmedzenia alebo vylúčenia zodpovednosti poskytovateľa za následky, ktoré tým vzniknú.

Zodpovednosť za ochranu dôverných informácií

Pri poskytovaní DFIR služieb dochádza k spracúvaniu veľkého množstva citlivých informácií vrátane obchodného tajomstva, interných dokumentov, bezpečnostných opatrení, údajov o zraniteľnostiach a výsledkov vyšetrovania incidentov.

Zmluva by mala upraviť zodpovednosť za porušenie povinnosti mlčanlivosti a neoprávnené sprístupnenie dôverných informácií. Súčasťou úpravy môže byť povinnosť nahradiť vzniknutú škodu, oznámiť bezpečnostný incident alebo prijať nápravné opatrenia na minimalizáciu následkov. Zodpovednosť za porušenie ochrany dôverných informácií však v praxi často býva upravená samostatnou, už spomínanou, dohodou o mlčanlivosti.

Zodpovednosť za ochranu osobných údajov

Ak poskytovanie služieb zahŕňa spracúvanie osobných údajov, zmluva by mala upravovať rozdelenie zodpovednosti medzi prevádzkovateľa a sprostredkovateľa podľa príslušných právnych predpisov.

Poskytovateľ môže niešť zodpovednosť za porušenie povinností pri spracúvaní osobných údajov, najmä ak:

- spracúva údaje nad rámec pokynov klienta,
- nezabezpečí primeranú ochranu údajov,
- neoprávnene sprístupní údaje tretím osobám,
- nezabezpečí ochranu údajov pred stratou alebo zneužitím,
- poruší povinnosti vyplývajúce z právnych predpisov o ochrane osobných údajov.

Súčasne však klient nesie zodpovednosť za zákonnosť samotného spracúvania a za správne určenie právnych základov spracúvania osobných údajov. Úprava zodpovednosti za porušenie ochrany osobných údajov je však častokrát (ako aj v prípade porušenia mlčanlivosti) upravená v samostatnej zmluve o spracúvaní osobných údajov.

Obmedzenie zodpovednosti

V obchodnej praxi býva bežné, že zmluvy obsahujú ustanovenia obmedzujúce rozsah zodpovednosti zmluvných strán pri porušení ich povinností. V prípade DFIR služieb však musí byť takéto obmedzenie primerané a nesmie odporovať kogentným ustanoveniam právnych predpisov.

Zmluva môže upraviť napríklad:

- maximálnu výšku náhrady škody,
- vylúčenie zodpovednosti za nepriame škody,
- vylúčenie zodpovednosti za ušlý zisk,
- obmedzenie zodpovednosti za škody spôsobené tretími osobami,
- obmedzenie zodpovednosti za udalosti vyššej moci.

Pri nastavovaní týchto ustanovení je potrebné zohľadniť hodnotu poskytovaných služieb, mieru rizika a rozsah prístupov poskytovateľa k systémom klienta.

Poistenie zodpovednosti

Vzhľadom na možné následky bezpečnostných incidentov a vysokú hodnotu spracúvaných informácií sa odporúča, aby poskytovateľ disponoval primeraným poistením zodpovednosti za škodu.

Zmluva môže upravovať:

- minimálnu výšku poistného krytia,
- povinnosť preukázať existenciu poistenia,
- povinnosť udržiavať poistenie počas trvania zmluvy,
- oznamovanie zmien alebo zániku poistného krytia.

Poistenie síce nenahrádza zodpovednosť poskytovateľa, predstavuje však významný nástroj riadenia rizík pre obe zmluvné strany.

Pri poistení však v praxi dochádza k situáciám, kedy už priamo klient má uzatvorené tzv. Cyber Insurance. Preto, ak má klient uzatvorené kybernetické poistenie, odporúča sa túto skutočnosť zohľadniť už pri príprave zmluvnej dokumentácie. Mnohé poistné zmluvy totiž obsahujú osobitné podmienky týkajúce sa riešenia kybernetických incidentov, ktorých nesplnenie môže viesť k obmedzeniu alebo odmietnutiu poistného plnenia. Zmluvná dokumentácia by preto mala obsahovať ustanovenia umožňujúce splnenie požiadaviek poisťovne. Klient by mal byť povinný informovať poskytovateľa o existencii kybernetického poistenia a o relevantných poistných podmienkach, ktoré môžu mať vplyv na poskytovanie služieb. Dôvodom je, že poskytovateľ nemusí vedieť, že poisťovňa vyžaduje konkrétny postup vyšetrovania, použitie schváleného dodávateľa alebo dodržanie určitých lehôt. Ak o týchto požiadavkách nevie, môže neúmyselne spôsobiť porušenie poistných podmienok. Zmluva by mala upraviť rozsah súčinnosti poskytovateľa pri komunikácii s poisťovňou a pri príprave podkladov potrebných na likvidáciu poistnej udalosti, pretože poisťovne spravidla požadujú odborné podklady na preukázanie vzniku a rozsahu poistnej udalosti.

Zmluvné pokuty a sankcie

Na zabezpečenie plnenia zmluvných povinností možno v zmluve dohodnúť aj zmluvné pokuty alebo iné sankčné mechanizmy.

Tieto môžu byť naviazané najmä na:

- porušenie povinnosti mlčanlivosti,
- neoprávnené nakladanie s údajmi,
- porušenie SLA parametrov,
- nedodržanie bezpečnostných požiadaviek,
- neoprávnené využitie subdodávateľov,
- omeškanie s plnením zmluvných povinností.

Pri nastavovaní zmluvných pokút je potrebné prihliadať na zásadu primeranosti. Výška pokuty by mala zodpovedať významu porušenej povinnosti a potenciálnym následkom jej porušenia. Neprimerane vysoké sankcie môžu byť v praxi problematické a môžu viesť k sporom medzi zmluvnými stranami.

Okrem zmluvných pokút je vhodné upraviť aj vzťah medzi zmluvnou pokutou a náhradou škody. Zmluvné strany by mali jednoznačne určiť, či zaplatením zmluvnej pokuty zaniká nárok na náhradu škody alebo či je možné požadovať náhradu škody aj nad rámec zaplatenej pokuty. Pri DFIR službách sa spravidla odporúča zachovať možnosť uplatňovať náhradu škody aj popri zmluvnej pokute, najmä ak porušenie povinnosti spôsobí škodu prevyšujúcu výšku dohodnutej sankcie.

Pri nastavovaní sankčných mechanizmov sa odporúča vyvážený prístup. Sankcie by nemali byť jednostranne orientované len voči poskytovateľovi služieb. Aj klient môže svojím konaním významne ovplyvniť schopnosť poskytovateľa plniť zmluvné povinnosti, napríklad

neposkytnutím potrebnej súčinnosti, zamlčaním relevantných informácií alebo neoprávneným zásahom do vyšetrovaného prostredia. V odôvodnených prípadoch preto možno uvažovať aj o sankčných mechanizmoch viazaných na porušenie povinností klienta.

Pri SLA parametroch sa v praxi často využívajú tzv. **service credits (zľavy z ceny)** alebo zmluvné pokuty za nedodržanie garantovaných reakčných časov. Ich účelom nie je sankcionovať poskytovateľa za každé drobné omeškanie, ale vytvoriť mechanizmus kompenzácie v prípadoch, keď nedodržanie dohodnutých parametrov môže mať negatívny dopad na schopnosť klienta efektívne reagovať na incident.

Význam úpravy zodpovednosti v DFIR zmluvách

Precízna úprava zodpovednosti predstavuje jeden zo základných nástrojov riadenia právnych a prevádzkových rizík pri poskytovaní DFIR služieb. Umožňuje transparentne rozdeliť zodpovednosť medzi klienta a poskytovateľa, vytvára predvídateľný rámec pre riešenie škodových udalostí a zvyšuje právnu istotu oboch strán.

Vzhľadom na citlivosť spracúvaných informácií, význam digitálnych dôkazov a potenciálne vysoké následky bezpečnostných incidentov by mala byť otázka zodpovednosti upravená podrobne, jednoznačne a s prihliadnutím na špecifiká digitálnej forenznej analýzy a reakcie na kybernetické incidenty.

Zodpovednosť za digitálne dôkazy

Osobitnú pozornosť si zasluhuje zodpovednosť za digitálne dôkazy, ktorá predstavuje jednu z najšpecifickejších oblastí DFIR služieb. Digitálne dôkazy môžu byť rozhodujúce pri interných vyšetrovaniach, disciplinárnych konaniach, občianskoprávných sporoch, správnych konaniach alebo trestných konaniach.

Poskytovateľ by mal byť zodpovedný za zachovanie:

- autenticity dôkazov,
- integrity dôkazov,
- preukázateľnosti pôvodu dôkazov,
- nepretržitého reťazca nakladania s dôkazmi (Chain of Custody),
- bezpečného uchovávanía dôkazného materiálu.

Ak dôjde k narušeniu niektorého z týchto princípov, môže byť dôkaz spochybnený alebo úplne vylúčený z dokazovania. Následky takéhoto pochybenia môžu mať významný dopad na právne postavenie klienta.

Cena a platobné podmienky

Cena za poskytovanie DFIR služieb patrí medzi základné náležitosti zmluvy. Vzhľadom na špecifický charakter týchto služieb však býva spôsob odmeňovania často zložitejší než pri bežných IT službách. Náročnosť jednotlivých incidentov, ich rozsah, časová naliehavosť a potreba nasadenia špecializovaných odborníkov môžu významne ovplyvniť celkové náklady na poskytované služby.

Zmluva by preto mala jednoznačne upravovať spôsob určenia ceny, ako aj všetky okolnosti, ktoré môžu mať vplyv na jej zmenu. Cena môže byť stanovená ako:

- jednorazová odmena za konkrétnu službu alebo projekt,
- hodinová sadzba za vykonané práce,
- paušálny mesačný poplatok,
- kombinácia paušálu a hodinového účtovania,
- retainer model zabezpečujúci pripravenosť incident response tímu,
- odmena viazaná na rozsah alebo závažnosť incidentu.

Osobitnú pozornosť je potrebné venovať situáciám, keď rozsah incidentu nie je možné vopred predvídať. V takých prípadoch je vhodné upraviť mechanizmy schvaľovania prác nad rámec pôvodne dohodnutého rozsahu, ako aj spôsob informovania klienta o predpokladanom zvýšení nákladov.

Platobné podmienky by mali upravovať najmä splatnosť faktúr, spôsob fakturácie, podmienky úhrady preddavkov, náhradu cestovných a iných vedľajších nákladov, podmienky fakturácie pohotovostných služieb a režim účtovania prác vykonávaných mimo štandardného pracovného času.

Pri dlhodobých zmluvách je vhodné upraviť aj mechanizmy valorizácie cien alebo podmienky zmeny odmeny v prípade významnej zmeny rozsahu poskytovaných služieb.

Trvanie a ukončenie zmluvy

Ustanovenia upravujúce trvanie a ukončenie zmluvy patria medzi základné náležitosti každého zmluvného vzťahu. V prípade zmlúv o poskytovaní služieb digitálnej forenzej analýzy a reakcie na kybernetické incidenty (DFIR) však nadobúdajú osobitný význam vzhľadom na povahu poskytovaných služieb, ktoré často zahŕňajú prácu s citlivými informáciami, bezpečnostnými incidentmi, digitálnymi dôkazmi a prístupom k informačným systémom klienta.

Správne nastavenie podmienok trvania a ukončenia zmluvy zabezpečuje právnu istotu zmluvných strán, kontinuitu poskytovaných služieb a predchádza situáciám, ktoré by mohli ohroziť bezpečnosť informačných systémov alebo integritu vykonávaného vyšetrovania. Zmluva by preto mala jednoznačne upravovať vznik zmluvného vzťahu, dobu jeho trvania, možnosti jeho ukončenia, ako aj práva a povinnosti strán po skončení spolupráce.

Zmluva by mala presne určovať **okamih vzniku zmluvného vzťahu a nadobudnutia jej účinnosti**. V praxi nemusí byť deň podpisu zmluvy vždy totožný s dňom začatia poskytovania služieb.

Osobitne pri DFIR službách môže byť účinnosť zmluvy podmienená splnením ďalších podmienok, napríklad:

- podpísaním dohody o mlčanlivosti,
- uzatvorením zmluvy o spracúvaní osobných údajov,
- vykonaním vstupného bezpečnostného auditu,
- pridelením prístupových oprávnení,
- určením kontaktných osôb,
- absolvovaním onboarding procesu.

Jednoznačné určenie začiatku zmluvného vzťahu je dôležité najmä pre posudzovanie zodpovednosti strán, plynutie SLA lehôt a vznik nároku na odmenu.

Pri DFIR službách sa využívajú oba základné modely trvania zmluvného vzťahu. **Zmluvy uzatvárané na dobu určitú** sa využívajú najmä pri jednorazových projektoch, ako sú forenzné vyšetrovania konkrétneho incidentu, analýza kompromitácie systémov, znalecké posudky alebo expertné služby. Trvanie zmluvy býva naviazané na splnenie konkrétneho cieľa alebo odovzdanie definovaných výstupov.

Ak je zmluva uzatvorená na dobu určitú, odporúča sa upraviť podmienky jej prípadného predĺženia. V praxi sa často využíva automatické predlžovanie zmluvy, pokiaľ žiadna zo strán v stanovenej lehote neoznámí záujem zmluvu ukončiť.

V prípade DFIR služieb je vhodné, aby bolo predĺženie zmluvy spojené aj s preverovaním aktuálnosti technických a bezpečnostných požiadaviek, kontaktných údajov, SLA parametrov a rozsahu poskytovaných služieb. Tým sa zabezpečí, že zmluva bude reflektovať aktuálny stav informačného prostredia klienta.

Naopak, **zmluvy uzatvárané na dobu neurčitú** sa spravidla využívajú pri dlhodobej spolupráci, najmä pri poskytovaní služieb na reakciu na incidenty, služieb forenznej pripravenosti, priebežného monitorovania bezpečnostných udalostí alebo poskytovaní špecializovanej bezpečnostnej podpory.

Pokiaľ ide o **ukončenie zmluvného vzťahu**, tak jedným zo štandardných spôsobov ukončenia zmluvného vzťahu je **výpoveď**. Zmluva by mala jednoznačne upravovať oprávnenie strán vypovedať zmluvu, výpovedné dôvody a dĺžku výpovednej lehoty. Pri dlhodobých DFIR službách je vhodné nastaviť výpovednú lehotu tak, aby umožňovala bezpečné ukončenie spolupráce, odovzdanie dokumentácie a realizáciu potrebných bezpečnostných opatrení. Príliš krátka výpovedná lehota môže ohroziť kontinuitu bezpečnostných služieb a zvýšiť riziko vzniku incidentov. Osobitnú pozornosť si vyžadujú situácie, keď je v čase podania výpovede riešený bezpečnostný incident. V takých prípadoch sa odporúča upraviť povinnosť poskytovateľa dokončiť začaté činnosti alebo zabezpečiť primerané odovzdanie prípadu inému subjektu.

Ďalšou možnosťou ukončenia zmluvného vzťahu je odstúpenie od zmluvy. **Odstúpenie od zmluvy predstavuje** mimoriadny spôsob ukončenia zmluvného vzťahu a spravidla sa využíva pri závažnom porušení zmluvných povinností.

Zmluva by mala obsahovať výpočet okolností, ktoré zakladajú právo na odstúpenie od zmluvy. Môže ísť najmä o:

- závažné porušenie povinnosti mlčanlivosti,
- neoprávnené sprístupnenie informácií tretím osobám,
- opakované porušovanie SLA parametrov,
- závažné porušenie bezpečnostných povinností,
- porušenie povinností pri ochrane osobných údajov,
- neposkytnutie potrebnej súčinnosti klientom,
- omeškanie s úhradou ceny za služby,
- stratu odborných oprávnení alebo certifikácií nevyhnutných na poskytovanie služieb.

Odporúča sa tiež upraviť povinnosť poskytnúť druhej strane primeranú lehotu na odstránenie zisteného porušenia, ak to povaha porušenia umožňuje.

Jednou z osobitostí DFIR zmlúv je **možnosť ukončenia zmluvného vzťahu v čase, keď prebieha riešenie bezpečnostného incidentu**. Takáto situácia môže predstavovať významné bezpečnostné riziko a môže negatívne ovplyvniť vyšetrowanie alebo realizáciu nápravných opatrení.

Z tohto dôvodu by mala zmluva upravovať osobitný režim ukončenia spolupráce počas incidentu. Vhodné je ustanoviť, že poskytovateľ dokončí minimálne nevyhnutné úkony smerujúce k stabilizácii situácie alebo zabezpečí riadne odovzdanie všetkých relevantných informácií klientovi alebo novému poskytovateľovi služieb. Takáto úprava prispieva k zachovaniu kontinuity vyšetrowania a minimalizácii bezpečnostných rizík.

Ukončením zmluvného vzťahu spravidla nezanikajú všetky práva a povinnosti zmluvných strán. **V prípade DFIR služieb zostávajú mnohé povinnosti relevantné aj po skončení poskytovania služieb.**

Zmluva by mala upravovať najmä:

- odobratie prístupových oprávnení poskytovateľa,
- ukončenie vzdialených pripojení a technických prístupov,
- vrátenie alebo odovzdanie dokumentácie,
- odovzdanie výsledkov analýz a záverečných správ,
- odovzdanie digitálnych dôkazov a forenzných kópií,
- vymazanie alebo anonymizáciu údajov,
- spôsob likvidácie záloh a pracovných kópií,
- zachovanie mlčanlivosti po skončení zmluvy.

Osobitnú pozornosť si vyžaduje nakladanie s digitálnymi dôkazmi, ktoré môžu byť potrebné pre budúce súdne, správne alebo trestné konania. Po skončení poskytovania služieb by mal

poskytovateľ odovzdať klientovi všetky výstupy vytvorené počas plnenia zmluvy. Môže ísť najmä o:

- forenznú správu,
- technické analýzy,
- záznamy o vykonaných úkonoch,
- logy a získané dôkazy,
- odporúčania na odstránenie zistených nedostatkov,
- dokumentáciu reťazca dôkazov (Chain of Custody),
- výstupy z použitých nástrojov.

Zmluva by mala upraviť formu odovzdania, spôsob zabezpečenia integrity údajov a prípadné podmienky ďalšieho uchovávanie kópií na strane poskytovateľa.

Zmluva by mala zároveň rozlíšiť povinnosť zachovať potenciálne relevantné digitálne dôkazy od všeobecného uchovávanie všetkých získaných údajov. Retenčné a likvidačné pravidlá by mali určiť, ktoré údaje sa uchovávajú, po akú dobu, za akých podmienok sa môže uplatniť dočasné pozastavenie vymazania z dôvodu prebiehajúceho alebo predpokladaného konania a akým spôsobom sa vykonané vymazanie alebo zničenie dokumentuje. V následnom konaní môže byť významné aj to, ktoré pôvodné záznamy boli zachované alebo zničené a z akého dôvodu (porov. rozsudok Krajského súdu v Bratislave sp. zn. 3To/55/2019 zo 17. 9. 2019).

Navyše, **niektoré ustanovenia zmluvy by mali zostať účinné aj po jej ukončení**. Ide najmä o ustanovenia týkajúce sa:

- ochrany dôverných informácií,
- ochrany osobných údajov,
- nakladania s digitálnymi dôkazmi,
- zodpovednosti za škodu,
- riešenia sporov,
- ochrany práv duševného vlastníctva.

Trvanie týchto povinností by malo byť v zmluve určené jednoznačne, pričom pri povinnosti mlčanlivosti sa často odporúča zachovanie účinkov aj niekoľko rokov po skončení zmluvného vzťahu.

Dôsledná úprava podmienok trvania a ukončenia zmluvy predstavuje významný nástroj riadenia právnych a bezpečnostných rizík. Umožňuje zabezpečiť kontinuitu poskytovaných služieb, ochranu citlivých informácií, riadne ukončenie prístupov k informačným systémom a zachovanie integrity digitálnych dôkazov.

V oblasti digitálnej forenznej analýzy a reakcie na kybernetické incidenty má táto časť zmluvy mimoriadny význam, pretože nesprávne alebo neúplne upravené ukončenie spolupráce môže viesť k strate dôkazov, narušeniu vyšetrovania alebo vzniku ďalších bezpečnostných

incidentov. Z tohto dôvodu by mala byť úprava trvania a ukončenia zmluvy považovaná za jednu z kľúčových súčastí každej DFIR zmluvy.

Riešenie sporov

Aj pri dôsledne pripravenej zmluve nemožno úplne vylúčiť vznik sporov medzi klientom a poskytovateľom služieb. V oblasti DFIR služieb môžu spory vzniknúť najmä v súvislosti s rozsahom vykonaných služieb, vyhodnotením bezpečnostných incidentov, dodržiavaním SLA parametrov, otázkami zodpovednosti za škodu alebo výškou odmeny.

Zmluva by preto mala **obsahovať mechanizmy riešenia sporov a určiť postup**, ktorý budú zmluvné strany uplatňovať pred začatím formálneho súdneho konania.

Odporúča sa upraviť najmä:

- povinnosť strán pokúsiť sa o zmierlivé vyriešenie sporu,
- interné eskalačné mechanizmy,
- lehoty na prerokovanie sporných otázok,
- možnosť využitia mediácie,
- možnosť využitia odborného znaleckého posúdenia,
- rozhodné právo,
- príslušnosť súdov alebo rozhodcovských orgánov.

V prípade medzinárodných zmlúv je nevyhnutné jednoznačne určiť rozhodné právo a jurisdikciu, pretože rozdielne právne úpravy môžu významne ovplyvniť práva a povinnosti zmluvných strán. Pri sporoch týkajúcich sa technických otázok môže byť vhodné zakotviť možnosť využitia nezávislého odborného posudku alebo expertného stanoviska pred začatím súdneho konania.

Úprava výstupov z poskytovanie služieb DFIR

Výstupy predstavujú jeden z najvýznamnejších prvkov zmluvného vzťahu pri poskytovaní DFIR. Práve prostredníctvom výstupov dochádza k naplneniu účelu zmluvy, keďže klient získava informácie o bezpečnostnom incidente, jeho príčinách, priebehu, dôsledkoch a odporúčaníach na prijatie nápravných opatrení. Na rozdiel od mnohých iných služieb v oblasti informačných technológií však **výstupy DFIR služieb nemajú len technický charakter**. Veľmi často majú významné právne, organizačné, bezpečnostné a ekonomické dôsledky. Môžu byť použité pri interných vyšetrovaniach, pri uplatňovaní nárokov voči zamestnancom alebo dodávateľom, pri komunikácii s regulačnými orgánmi, poisťovňami alebo ako dôkazné prostriedky v súdnych a správnych konaniach. Z uvedeného dôvodu je potrebné venovať ich zmluvnej úprave mimoriadnu pozornosť.

Základným predpokladom kvalitnej zmluvnej úpravy je **presné vymedzenie toho, aké výstupy bude poskytovateľ klientovi odovzdávať**. V praxi sa často stretávame so situáciou, keď je predmet zmluvy definovaný pomerne všeobecne, napríklad ako „*poskytovanie služieb digitálnej forenznej analýzy*“ alebo „*riešenie bezpečnostných incidentov*“, avšak absentuje konkrétna špecifikácia výsledkov, ktoré má klient na konci procesu obdržať. Takýto prístup

môže viesť k sporom o rozsah plnenia, kvalite dodaných výstupov alebo splnení zmluvných povinností. Preto by mala zmluva už v úvodných ustanoveniach obsahovať zoznam výstupov, ktoré budú poskytované v rámci jednotlivých druhov služieb.

V rámci DFIR služieb možno identifikovať viacero kategórií výstupov. Prvou skupinou sú **operatívne alebo priebežné výstupy**, ktoré vznikajú počas riešenia incidentu. Ich účelom je zabezpečiť priebežnú informovanosť klienta o aktuálnom stave incidentu a o prijatých opatreniach. Ide najmä o situačné správy, hlásenia o priebehu zásahu, priebežné analýzy alebo upozornenia na kritické zistenia. Zmluva by mala **určiť frekvenciu ich poskytovania, spôsob komunikácie a osoby oprávnené tieto informácie prijímať**. V prípade závažných incidentov môže byť vhodné ustanoviť povinnosť poskytovať klientovi priebežné aktualizácie v pravidelných časových intervaloch alebo po dosiahnutí vopred definovaných míľnikov.

Druhou skupinou výstupov sú **predbežné analytické správy**. Tieto dokumenty bývajú **vypracované krátko po začatí vyšetrovania incidentu a ich cieľom je poskytnúť klientovi základný prehľad o situácii**. Obsahujú spravidla informácie o povahe incidentu, predpokladanom spôsobe kompromitácie systému, rozsahu dotknutých aktív a predbežnom odhade rizík. Keďže v tejto fáze nemusí byť vyšetrovanie ukončené, je potrebné v zmluve výslovne uviesť, že ide o predbežné zistenia, ktoré môžu byť v ďalších fázach vyšetrovania doplnené alebo spresnené.

Kľúčovým výstupom väčšiny DFIR služieb je **záverečná forenzná správa**. Ide o **komplexný odborný dokument sumarizujúci celý priebeh vyšetrovania**. V záujme zabezpečenia jednotnej kvality výstupov by mala zmluva obsahovať minimálne požiadavky na jej obsah. Správa by mala obsahovať identifikáciu incidentu, opis použitých metodík a nástrojov, zoznam analyzovaných systémov a dátových zdrojov, chronologický priebeh incidentu, identifikované zraniteľnosti, opis zistených aktivít útočníka, zoznam zabezpečených dôkazov a odborné závery. Súčasťou správy by mali byť aj odporúčania na odstránenie zistených nedostatkov a prevenciu obdobných incidentov v budúcnosti.

Záverečnú foreznú alebo technickú správu poskytovateľa je potrebné odlišovať od znaleckého posudku vypracovaného podľa osobitných právnych predpisov. To však nevylučuje jej využitie ako odborného podkladu alebo dôkazného prostriedku v konkrétnom konaní, ak to príslušné procesné pravidlá umožňujú. Zmluva by preto mala klásť dôraz najmä na konkrétnosť, úplnosť a preskúmateľnosť správy, identifikáciu zdrojov údajov a použitých postupov a na možnosť overenia jej záverov (porov. rozsudok Krajského súdu v Košiciach sp. zn. 6S/115/2018 z 3. 6. 2021).

Osobitnú pozornosť zastávajú aj **digitálne dôkazy ako samostatný typ výstupu**. Na rozdiel od analytických správ nejde o interpretáciu zistení, ale o samotné dáta získané počas vyšetrovania. Môže ísť o forenzné obrazy pevných diskov, kópie logov, záznamy sieťovej komunikácie, obsah operačnej pamäte, výpisy databáz alebo iné elektronické údaje. Keďže tieto dôkazy môžu byť využité v právnych konaniach, zmluva musí detailne upravovať podmienky ich získavania, uchovávaní a odovzdávania. Odporúča sa ustanoviť povinnosť

dokumentovať celý proces manipulácie s dôkazmi prostredníctvom tzv. chain of custody, teda evidencie všetkých osôb, ktoré s dôkazmi nakladali, a všetkých vykonaných úkonov.

Ak sa z pôvodných digitálnych dát vytvárajú odvodené materiály, napríklad prepisy, exporty, screenshoty, tabuľky alebo analytické súhrny, zmluva by mala podľa povahy služby upraviť aj zachovanie pôvodných zdrojových dát alebo ich forenznej kópie tak, aby bolo možné pôvod, správnosť a úplnosť odvodeného výstupu následne overiť. Samotný odvodený výstup totiž nemusí byť v následnom konaní dostatočný bez možnosti jeho overenia voči pôvodnému záznamu (porov. v kontexte hodnotenia zvukovo-obrazových záznamov a ich prepisov uznesenie Krajského súdu v Košiciach sp. zn. 4To/106/2021 zo 17. 6. 2022).

Zmluva by mala riešiť aj **otázku formy výstupov**. V praxi môže byť potrebné odovzdávať výstupy v rôznych formátoch a na rôznych nosičoch. Forenzne správy bývajú spravidla poskytované vo forme elektronických dokumentov vo formáte PDF, zatiaľ čo digitálne dôkazy môžu byť odovzdávané na šifrovaných externých úložiskách alebo prostredníctvom zabezpečených dátových úložísk. Súčasťou zmluvy by mali byť požiadavky na šifrovanie, autentifikáciu prijímateľa a potvrdenie prevzatia výstupov.

Významnou otázkou je **určenie lehôt na dodanie jednotlivých výstupov**. Čas má pri riešení kybernetických incidentov zásadný význam. V prípade bezpečnostného incidentu môže klient potrebovať výsledky analýzy v priebehu niekoľkých hodín alebo dní, napríklad na splnenie oznamovacích povinností podľa právnych predpisov, vrátane legislatívy v oblasti ochrany osobných údajov alebo kybernetickej bezpečnosti. Zmluva by preto mala rozlišovať medzi lehotami na poskytovanie priebežných informácií, predbežných správ a konečných výstupov. Zmluvná úprava by mala riešiť aj **vlastnícke a používacie práva k výstupom**. V prípade forenznych správ sa spravidla predpokladá, že klient získava právo tieto dokumenty používať na účely ochrany svojich práv a záujmov. Súčasne však môže byť potrebné upraviť práva poskytovateľa k vlastným metodikám, postupom alebo analytickým nástrojom, ktoré použil pri spracovaní výstupov. Ak poskytovateľ plánuje využívať získané údaje alebo poznatky na výskumné účely, vytváranie datasetov, testovanie alebo zlepšovanie analytických nástrojov, vývoj nových detekčných mechanizmov alebo tvorbu databáz hrozieb, musí byť táto možnosť výslovne upravená v zmluve. Zmluva by mala určiť rozsah takéhoto ďalšieho použitia, podmienky anonymizácie alebo inej primeranej úpravy údajov, ochranu osobných údajov, dôverných informácií a obchodného tajomstva, ako aj pravidlá nakladania s údajmi po skončení zmluvného vzťahu.

Mimoriadne dôležitou oblasťou je **ochrana dôverných informácií**. Výstupy DFIR služieb často obsahujú podrobné informácie o technickej infraštruktúre klienta, bezpečnostných opatreniach, identifikovaných slabínach a niekedy aj osobné údaje zamestnancov alebo zákazníkov. Zmluva by preto mala obsahovať **prísne pravidlá týkajúce sa mlčanlivosti, prístupu k výstupom, ich uchovávaní a ďalšieho šírenia**. Odporúča sa tiež určiť, ktoré osoby budú oprávnené s výstupmi nakladať a za akých podmienok môžu byť sprístupnené tretím stranám.

Pri zmluvnej úprave výstupov je **potrebné myslieť aj na ich budúcu dôkaznú použiteľnosť**. Ak existuje predpoklad, že výstupy budú použité v správnom, civilnom alebo trestnom konaní, mala by zmluva vyžadovať dodržiavanie medzinárodne uznávaných forenzných štandardov, najmä odporúčaní publikovaných National Institute of Standards and Technology v dokumente NIST SP 800-86 alebo noriem ISO/IEC 27037, ISO/IEC 27041 a ISO/IEC 27042. Dodržiavanie týchto štandardov významne zvyšuje dôveryhodnosť výsledkov a minimalizuje riziko ich spochybnenia.

Z pohľadu metodiky uzatvárania DFIR zmlúv možno konštatovať, že výstupy by nemali byť chápané iba ako technický výsledok poskytovanej služby. Predstavujú súčasne právne relevantné dokumenty, nositeľov digitálnych dôkazov a zdroj informácií nevyhnutných pre ďalšie rozhodovanie klienta. Preto by mala byť ich zmluvná úprava podrobná, jednoznačná a mala by pokrývať nielen ich obsah a formu, ale aj vlastníctvo, ochranu, dôvernosť, dôkaznú použiteľnosť, spôsob odovzdania a podmienky ich ďalšieho využívania. Takto nastavený zmluvný rámec významne prispieva k právnej istote zmluvných strán a k efektívnemu riešeniu kybernetických incidentov.

Špecifické požiadavky na zmluvné vzťahy v prostredí finančného sektora (Nariadenie DORA)

Ak je klient finančným subjektom (napr. banka, poisťovňa, správcovská spoločnosť, obchodník s cennými papiermi), uzatváranie zmluvných vzťahov v oblasti DFIR môže podliehať osobitným požiadavkám podľa Nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora (nariadenie DORA). Pri iných subjektoch zapojených do dodávateľského reťazca finančného subjektu je potrebné uplatnenie týchto požiadaviek posúdiť podľa konkrétneho postavenia subjektu a zmluvného vzťahu.

Pri uzatváraní zmluvy s finančným subjektom je potrebné v prvom rade posúdiť, či poskytované DFIR služby predstavujú službu informačných a komunikačných technológií v zmysle DORA. Vo väčšine prípadov bude digitálna forenzná analýza, incident response, spadať pod definíciu IKT služieb (čl. 3 bod 21 Nariadenia DORA). Táto skutočnosť má zásadný význam pre obsah zmluvy, keďže DORA vyžaduje, aby finančné subjekty mali s externými poskytovateľmi uzatvorené zmluvy obsahujúce presne vymedzené povinné náležitosti.

Ak služby odozvy na incidenty (Incident Response) alebo digitálnej forenznej analýzy podporujú kritickú alebo dôležitú funkciu finančného subjektu, zmluvný vzťah musí zohľadňovať aj dodatočné požiadavky DORA pre takéto služby. V takom prípade musí zmluva okrem všeobecných náležitostí podľa článku 30 ods. 2 obsahovať aj dodatočné zmluvné prvky vyžadované **článkom 30 ods. 3 nariadenia DORA**.

Zmluva uzatvorená medzi finančným subjektom a poskytovateľom DFIR služieb musí jednoznačne upravovať práva a povinnosti oboch strán a **mala by byť vyhotovená v písomnej forme**. Súčasťou zmluvy by mali byť aj dohodnuté úrovne poskytovaných služieb (SLA), ktoré určujú očakávanú kvalitu, dostupnosť a parametre poskytovaných služieb.

Základným predpokladom súladu s požiadavkami DORA je **presné vymedzenie predmetu plnenia, teda poskytovaných služieb**. Zmluva by mala obsahovať podrobný opis všetkých poskytovaných DFIR služieb vrátane rozsahu digitálnej forenznej analýzy, reakcie na incidenty, zberu a spracovania digitálnych dôkazov, analýzy škodlivého kódu, podpory pri oznamovaní incidentov a vypracovávaní odborných správ. **Ak sa predpokladá zapojenie subdodávateľov, musia byť jasne definované podmienky ich využívania a rozsah činností, ktoré môžu vykonávať.**

Osobitná pozornosť by mala byť venovaná **lokalizácii poskytovaných služieb a spracúvaných údajov**. Finančný subjekt musí mať prehľad o tom, kde budú údaje analyzované, uchovávané alebo zálohované. Poskytovateľ by mal mať povinnosť informovať klienta o každej plánovanej zmene lokality spracúvania údajov alebo o presune služieb do iného štátu či dátového centra. Táto požiadavka je mimoriadne významná najmä pri využívaní cloudových riešení.

Zmluva musí upravovať aj **ochranu údajov a bezpečnostné opatrenia**. Poskytovateľ DFIR služieb by mal garantovať primeranú úroveň ochrany dôvernosti, integrity, dostupnosti a autenticity spracúvaných údajov. V prípade práce s osobnými údajmi musí byť zabezpečený súlad s požiadavkami GDPR a ďalších relevantných právnych predpisov. Súčasťou zmluvy by mali byť pravidlá šifrovania, riadenia prístupových práv, evidencie činností a ochrany digitálnych dôkazov.

Dôležitou zmluvnou požiadavkou je **zabezpečenie prístupu k údajom a ich návrat klientovi**. Poskytovateľ musí byť schopný odovzdať finančnému subjektu všetky spracúvané údaje vrátane digitálnych dôkazov, logov, forenznych obrazov a analytických výstupov v použiteľnom a bežne dostupnom formáte. Táto povinnosť musí byť zabezpečená aj v prípade ukončenia zmluvy, ukončenia podnikateľskej činnosti poskytovateľa alebo jeho platobnej neschopnosti.

Pre oblasť DFIR služieb je mimoriadne významná povinnosť poskytovať súčinnosť pri riešení incidentov. **Poskytovateľ by mal mať zmluvne stanovenú povinnosť bezodkladne asistovať klientovi pri vyšetrowaní bezpečnostného incidentu, poskytovať odbornú podporu, analyzovať vzniknuté udalosti a zabezpečiť potrebné informácie pre splnenie oznamovacích povinností voči regulačným orgánom.** Odporúča sa, aby zmluva presne stanovovala reakčné časy, spôsob eskalácie incidentov a formu komunikácie počas incidentu.

Osobitnou požiadavkou DORA je **spolupráca s dohliadacími a regulačnými orgánmi**. Poskytovateľ DFIR služieb by mal byť pripravený poskytovať súčinnosť nielen klientovi, ale aj orgánom dohľadu, ak je to potrebné na účely vyšetrowania incidentu alebo výkonu regulačnej kontroly. Táto povinnosť by mala byť v zmluve výslovne zakotvená.

Ak poskytované DFIR služby podporujú kritické alebo dôležité funkcie finančného subjektu, rozsah zmluvných požiadaviek sa ďalej rozširuje. V takom prípade je potrebné detailne **definovať kvalitatívne a kvantitatívne ukazovatele poskytovaných služieb, vrátane presne**

merateľných výkonnostných cieľov. Finančný subjekt musí mať možnosť priebežne monitorovať plnenie týchto parametrov a vyžadovať nápravu v prípade ich nedodržania.

Zmluva by mala upravovať aj **povinnosti poskytovateľa v oblasti kontinuity činností a krízového riadenia.** Poskytovateľ by mal disponovať vlastnými plánmi kontinuity prevádzky, plánmi obnovy po incidente a pravidelne testovať ich funkčnosť. Súčasne by mal byť povinný implementovať primerané technické a organizačné bezpečnostné opatrenia zodpovedajúce významu poskytovaných služieb.

Významným prvkom požadovaným nariadením DORA sú **auditné práva finančného subjektu.** Klient musí mať možnosť overovať spôsob poskytovania služieb, kontrolovať dodržiavanie bezpečnostných požiadaviek a vykonávať audity poskytovateľa. Rovnaké oprávnenia musia byť zabezpečené aj pre príslušné orgány dohľadu. Poskytovateľ by mal byť povinný poskytnúť potrebnú dokumentáciu, umožniť výkon kontroly a poskytovať súčinnosť počas auditov alebo inšpekcií.

Neoddeliteľnou súčasťou zmluvy musí byť aj **stratégia ukončenia zmluvného vzťahu.** Táto stratégia by mala zabezpečiť, aby ukončenie spolupráce nemalo negatívny dopad na prevádzku finančného subjektu. Poskytovateľ by mal počas dohodnutého prechodného obdobia pokračovať v poskytovaní služieb a zabezpečiť odovzdanie všetkých údajov, dokumentácie a výstupov potrebných na prechod k inému poskytovateľovi alebo na prevzatie činností samotným finančným subjektom.

Pri príprave DFIR zmlúv vo finančnom sektore je preto potrebné vnímať zmluvu nielen ako obchodný nástroj upravujúci poskytovanie služieb, ale aj ako jeden z kľúčových prvkov systému digitálnej prevádzkovej odolnosti finančnej inštitúcie. Dôsledné zohľadnenie požiadaviek DORA významne prispieva k ochrane finančného subjektu, zvyšuje právnu istotu zmluvných strán a podporuje efektívne zvládanie kybernetických incidentov.⁴

4 Prehľad

Metodika systematizuje uzatváranie zmluvných vzťahov pri poskytovaní služieb DFIR do dvoch nadväzujúcich fáz. V predzmluvnej fáze ide najmä o identifikáciu potrieb a cieľov klienta, predbežnú analýzu jeho prostredia, overenie spôsobilosti poskytovateľa, ochranu dôverných informácií a posúdenie spracúvania osobných údajov. Vo fáze uzatvorenia zmluvy ide o voľbu vhodného zmluvného modelu, vymedzenie predmetu zmluvy a rozsahu oprávnení, úpravu SLA a reakčných časov, ochranu informácií a osobných údajov, nakladanie s digitálnymi dôkazmi,

⁴ Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora (nariadenie DORA).

zodpovednosť za škodu, cenu, trvanie a ukončenie zmluvy, riešenie sporov a úpravu výstupov. Nasledujúce schémy zhŕňajú odporúčaný postup v oboch fázach.

PREDZMLUVNÁ FÁZA PRI POSKYTOVANÍ SLUŽIEB DFIR

Predzmluvná fáza je kľúčová pre správne nastavenie zmluvného vzťahu, minimalizáciu rizík a zabezpečenie, že spolupráca bude právne bezchybná, efektívna a v súlade s technickými a regulačnými požiadavkami.



i Dôsledné vykonanie predzmluvnej fázy znižuje riziko nedorozumení, neoprávneného prístupu, porušenia právnych predpisov a zabezpečuje efektívne riešenie incidentov.

Schéma č. 1: Kroky v rámci predzmluvnej fázy

POSTUP PRE UZATVORENIE PRÁVNE BEZVADNEJ A EFEKTÍVNEJ DFIR ZMLUVY

Cieľ: zabezpečiť právnú istotu, ochranu údajov, efektívnu spoluprácu a dôkaznú použiteľnosť.



1) ČO BY MAL KLIENT UROBIŤ / ZVÁŽIŤ PRED UZATVORENÍM ZMLUVY

KROK	ČO UPRAVIŤ	PREČO
ANALÝZA POTRIEB A RIZIK	- Identifikovať typy incidentov, ktoré môžu nastať - Urobiť kritické systémy a údaje - Stanoviť požadovanú úroveň reakcie a forenzných nástupov	Zabezpečiť, že zmluva pokrýva reálne potreby a riziká organizácie.
POSÚDENIE POSKYTOVATEĽA	- Overiť skúsenosti v DFIR, referencie, certifikácie (napr. CREST, ISO 27037) - Posúdiť technické kapacity, nástroje a metódy - Shodnotiť finančnú stabilitu a poistné krytie	Minimalizuje riziko zlyhania poskytovateľa a zabezpečí profesionálny prístup.
PRÁVNÁ A REGULAČNÉ POSÚDENIE	- Overiť súlad so zákonmi (GDPR, zákon o kybernetickej bezpečnosti, tržné právo, pracovné právo) - Zvážiť ochranné prenosy údajov - Posúdiť potrebu DPA (ak je poskytovateľ spracovateľom)	Zabezpečuje zákonnosť spracovania údajov a predchádza sankciám.
TECHNICKÁ PRÍPRAVA	- Zabezpečiť logovanie a uchovávanie logov - Prípraviť prístup a postupy pre DFIR tímu - Zvážiť kompatibilitu nástrojov a forenznú prípravu	Umožní rýchlu a efektívnu reakciu bez zbytočných oneskorení.
INTERNÉ SCHVÁLENIA A ROZPOČET	- Získať súhlas manažmentu a právneho oddelenia - Zabezpečiť rozpočet (vrátane prípadných extra nákladov) - Overiť súlad s internými politikami a procesmi	Predchádza interným rizikám a zabezpečuje podporu pre spoluprácu.
PRÍPRAVA NA KRÍZOVÉ SECNÁRE	- Zadefinovať kontaktné osoby a komunikačné kanály - Zvážiť komunikačný plán (interný aj externý) - Prípraviť plán eskalácie	Zabezpečí koordinovanú reakciu a minimalizuje chaos pri incidente.

2) ČO BY MALA ZMLUVA UPRAVOVAŤ (KLÚČOVÉ OBLASTI) A PREČO

OBLASŤ V ZMLUVU	ČO UPRAVIŤ	PREČO
PREDMET A ROZSAH SLUŽIEB	- Presný rozsah DFIR služieb (ruskta, forenzná analýza, reporty, konzultácie) - Co je zahrnuté / Co je mimo rozsahu	Predchádza nejasnostiam a sporom o rozsah služieb.
DOSTUPNOSŤ A SLA	- Reakčné časy, dostupnosť (24/7) - SLA metríky a spôsob merania	Zabezpečuje otáčanú úroveň služby a merateľné výstupy.
ZÍSKAVANIE A NAKLADANIE S DIGITÁLNYMI DOKAZMI	- Spôsob získavania (forenzný korektný postup) - Hasťovanie, chain of custody, uchovávanie, prenos, šifrovanie - Použitie dokazov len na účel incidentu	Zabezpečuje dôkaznú použiteľnosť a integritu dát.
OCHRANA ÚDAJOV (GDPR)	- Uloha strán (správca / spracovateľ / sprostredovateľ) - Inštrukcie na spracovanie, bezpečnostné opatrenia - Suhodávateľka, nechnočné prenosy, práva dotknutých osôb	Zabezpečuje súlad s GDPR a minimalizuje právne riziká.
ZODPOVEDNOSŤ ZA ŠKODU	- Rozdelenie zodpovednosti medzi stranami - Umýtie zodpovednosti, vylúčenia (nepriama škoda, ušľý sisk) - Vymýtky (umýsľ, hrubá nebanlivost)	Chráni obe strany pred neprimeranými finančnými rizikami.
DÓVERNOSŤ A BEZPEČNOSŤ	- Povinnosť mlčanivosti, prístupové práva - Peziská a environmentálna bezpečnosť - Opatrenia na ochranu informácií	Chráni citlivé informácie a dôveru organizácie.
SUBDODAVATEĽIA	- Možnosť využitia subdodavateľov - Schvaľovací proces, zodpovednosť, rovnaké záväzky	Zabezpečuje kontrolu nad tretími stranami.
PLATONÉ PODMIENKY	- Odměna (paušál / hodinová sadba / retainer) - Fakturácia, splatnosť, náklady navyše	Predchádza finančným nejasnostiam.
UKONČENIE ZMLUVY	- Vypovedná podmienky, odstúpenie - Odoberanie / vrátenie dát a dokazov - Likvidácia alebo archivácia	Upravuje ukončenie spolupráce a ochranu dát.
RIEŠENIE SPOROV A ROZHODNÉ PRÁVO	- Rozhodné právo a jurisdikcia - Mechanismus riešenia sporov (mediácia / arbitráž / súd)	Umožňuje efektívne riešenie prípadných sporov.

KLÚČOVÉ ZÁSADY ÚSPEŠNEJ ZMLUVY

Zákonnosť a súlad Súlad s právom a internými politikami.	Jasnosť Presné definície, rozsah a očakávanie.	Vyváženosť Spravidlivé rozdelenie práv a povinností.	Bezpečnosť a dôkaznosť Ochrana údajov a integrita digitálnych dokazov.	Flexibilita a revízia Možnosť opravy podľa vývoja rizík a technológií.
--	--	--	--	--

Schéma č. 2: Postup pri zmluvnej fáze

5 Zoznam použitej literatúry

Literatúra a odborné zdroje

BAJTOŠ, Tomáš – SOKOL, Pavol – BAČO, Ladislav. Digitálna forenzná analýza I. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2020. Dostupné na: <https://unibook.upjs.sk/img/cms/2020/pf/digitalna-forenzna-analyza-1.pdf>

HUDECOVÁ, Irena – CYPRICHOVÁ, Anna – MAKATURA, Ivan a kol. Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov/GDPR. Veľký komentár. 2. zväzok. 2. aktualizované vydanie. Žilina: EUROKÓDEX, 2020.

KENT, Karen – CHEVALIER, Suzanne – GRANCE, Tim – DANG, Hung. Guide to Integrating Forensic Techniques into Incident Response. NIST Special Publication 800-86. Gaithersburg: National Institute of Standards and Technology, 2006.

MAKATURA, Ivan. Ciele dokazovania v kybernetickej bezpečnosti. In: Acta Facultatis Iuridicae Universitatis Comenianae, 2023, roč. 42, č. 1, s. 116 – 146.

OLEJÁR, Daniel a kol. Základy kybernetickej a informačnej bezpečnosti. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, 2020.

SELINŠEK, Liljana. Některé právní aspekty forenzní analýzy digitálních dat. In: Acta Universitatis Carolinae – Iuridica, 2008, č. 4, s. 131 – 140.

Technické normy

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence.

ISO/IEC 27041:2015 Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method.

ISO/IEC 27042:2015 Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence.

ISO/IEC 27043:2015 Information technology – Security techniques – Incident investigation principles and processes.

ISO 21043-2:2018 Forensic sciences – Part 2: Recognition, recording, collecting, transport and storage of items.

Judikatúra

Rozsudok Najvyššieho správneho súdu Slovenskej republiky sp. zn. 4Sfk/110/2022 z 24. 4. 2024, ECLI:SK:NSSSR:2024:6021200033.1.

Rozsudok Krajského súdu v Košiciach sp. zn. 6S/115/2018 z 3. 6. 2021, ECLI:SK:KSKE:2021:7018200828.2.

Rozsudok Krajského súdu v Bratislave sp. zn. 3To/55/2019 zo 17. 9. 2019, ECLI:SK:KSBA:2019:1518010031.1.

Uznesenie Krajského súdu v Košiciach sp. zn. 4To/106/2021 zo 17. 6. 2022, ECLI:SK:KSKE:2022:7217010310.2.

Rozsudok Krajského súdu v Košiciach sp. zn. 4Cob/46/2024 z 23. 4. 2025, ECLI:SK:KSKE:2025:6123373185.1.

Rozsudok Správneho súdu v Bratislave sp. zn. BA-1S/83/2020 z 29. 10. 2025, ECLI:SK:SpSBA:2025:1020200456.1.