Evidenční číslo Smlouvy Objednatele:	Evidenční číslo Smlouvy Dodavatele:
0122001869	ODR-2018-0007

DODATEK Č. 2 KE SMLOUVĚ O POSKYTOVÁNÍ SERVISNÍCH SLUŽEB A SLUŽEB RÁMCOVÝCH ÚPRAV CAODB A ROZHRANÍ MEZI CAODB A PROVOZNÍMI SYSTÉMY Č. 0122001869

(dále jen „**Dodatek**“):

Český Aeroholding, a.s.
se sídlem: Praha 6, Jana Kašpara 1069/1, PSČ 160 08,
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka B 17005,

IČO: 248 21 993,
DIČ: CZ699003361,
bankovní spojení: UniCredit Bank Czech Republic and Slovakia, a.s.,
číslo účtu (CZK): 2106286528/2700,
zastoupená: Ing. Radkem Hovorkou, místopředsedou představenstva a JUDr. Petrem Pavelcem, LL.M. členem představenstva

(dále jen „**Objednatel**“ nebo „**CAH**“)

a

Profinit EU, s.r.o
se sídlem: Praha 6, Tychonova 270/2, PSČ 160 00,
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 58081,
IČO: 04 43 40 81,
DIČ: CZ04434081,
bankovní spojení: Raiffeisenbank a.s.,
číslo účtu (CZK): 5011261241/5500,
zastoupená: Mgr. Tomášem Pavlíkem, jednatelem
(dále jen „**Dodavatel**“)

Objednatel a Dodavatel dále společně také „**Strany**“ či jednotlivě „**Strana**“.

Preambule

Vzhledem k tomu, že:

(A) Strany uzavřely dne 27. 8. 2015 Smlouvu o poskytování servisních služeb a služeb rámcových úprav pro CAODB a rozhraní mezi CAODB a provozními systémy ev. č. Objednatele 0122001869, ve znění dodatku č. 1 ze dne 1. 12. 2016 (dále jen „**Smlouva**“),

(B) Strany mají v souladu s ustanovením 13.6 Smlouvy zájem upravit znění Smlouvy,

dohodly se Strany v souladu s aplikovatelnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, v platném a účinném znění (dále jen „Občanský zákoník“), následovně:

1 ZMĚNY SMLOUVY

1.1 Do článku 7.6 Smlouvy se vkládá nový bod č. 7.6.9, který zní:

„7.6.9 Poskytovat Služby v souladu s podmínkami a požadavky uvedenými v příloze č. 11 této Smlouvy.“

1.2 Do Smlouvy se vkládá nová příloha č. 11, jejíž znění je uvedeno v příloze č. 1 tohoto Dodatku.

2 ZÁVĚREČNÁ USTANOVENÍ

2.1 Tento Dodatek nabývá platnosti a účinnosti dnem jeho podpisu oběma Stranami. Stanoví-li však zvláštní právní předpis, že tento Dodatek může nabýt účinnosti nejdříve k určitému dni, který je dnem pozdějším než den podpisu tohoto Dodatku poslední Stranou, nabývá tento Dodatek účinnosti až dnem, ke kterému může tento Dodatek nabýt dle takového právního předpisu účinnosti nejdříve.

2.2 Strany prohlašují, že žádné skutečnosti uvedené v tomto Dodatku a jeho přílohách netvoří obchodní tajemství ve smyslu § 504 Občanského zákoníku.

2.3 Ostatní ustanovení Smlouvy tímto Dodatkem nedotčená zůstávají v platnosti beze změny.

2.4 Tento Dodatek je vyhotoven ve dvou (2) vyhotoveních, z nichž každá ze Stran obdrží po jednom (1) vyhotovení.

2.5 Nedílnou součástí této Smlouvy jsou následující přílohy:

2.5.1 Příloha č.1 - Znění přílohy č. 11 Smlouvy

SMLUVNÍ STRANY TÍMTO PROHLAŠUJÍ, ŽE SI TENTO DODATEK PŘEČETLY A ŽE SOUHLASÍ S JEHO OBSAHEM, NA DŮKAZ ČEHOŽ JEJ STVRZUJÍ SVÝMI PODPISY:

Datum:	Datum:
Za Objednatele:	Za Dodavatele:
Podpis: _____	Podpis: _____
Jméno: Ing. Radek Hovorka	Jméno: Mgr. Tomáš Pavlík
Funkce: Místopředseda představenstva	Funkce: jednatel
Podpis: _____	_____
Jméno: JUDr. Petr Pavelec, LL.M.	
Funkce: Člen představenstva	

Příloha č. 1 – Znění přílohy č. 11 Smlouvy

BEZPEČNOSTNÍ POŽADAVKY VE SMLUVNÍCH VZTAZÍCH

3 Úvod

Účelem tohoto dokumentu je definovat závazné bezpečnostní požadavky pro poskytovatele, jejichž předmětem plnění pro objednatele je (výhradně či jako součást předmětu plnění jiné služby) vývoj, implementace a/nebo servis software či hardware (dále také jen „**SW**“ či **„HW“**), a/nebo kteří v souvislosti s plněním pro objednatele přistupují do informačního a komunikačního systému objednatele (dále také jen „**systém ICT**“), a/nebo kteří v rámci poskytovaného plnění pro objednatele zpracovávají, a/nebo přenášejí a/nebo ukládají a/nebo archivují jakákoli data a informace objednatele a/nebo jeho zákazníků (dále také jen „**Bezpečnostní požadavky**“). Účelem tohoto dokumentu je současně definovat požadavky na dodavatele dle platné právní úpravy, především pak dle ustanovení § 5 odst. 2 písm. e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a § 7 vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), přičemž zohledňuje také ostatní související platné právní předpisy týkající se dané problematiky.

4 Obecné požadavky

Poskytovatel se při poskytování plnění pro objednatele zavazuje plnit následující povinnosti:

a) pokud poskytovatel využívá při poskytování plnění subdodavatele, poskytovatel se zavazuje zajistit dodržování Bezpečnostních požadavků rovněž ve smluvních vztazích se svými subdodavateli; přičemž tuto skutečnost se poskytovatel zavazuje doložit objednateli na vyžádání předložením příslušného smluvního vztahu uzavřeného s tímto subdodavatelem poskytovatele, případně předložením čestného prohlášení o řádném naplňování této povinnosti;

b) nestanoví-li dohoda stran jinak, poskytovatel jmenuje nejpozději do 3 dnů po uzavření smlouvy zodpovědnou kontaktní osobu pro potřeby zajištění plnění Bezpečnostních požadavků a související komunikace mezi smluvními stranami (dále také jen „**Kontaktní osoba**“).

c) Pokud při plnění předmětu smlouvy dochází ke zpracování osobních údajů, poskytovatel se zavazuje zajistit uzavření samostatných smluv ve smyslu příslušných ustanovení zákona č. 101/2000 Sb., o ochraně osobních údajů, v platném znění, zejména pak jeho ustanovení § 6;

d) dodržovat příslušná ustanovení bezpečnostních politik, metodik a postupů společnosti objednatele resp. platné řídící dokumentace objednatele či její části, pokud byl s takovými dokumenty nebo jejich částmi seznámen.

5 Bezpečnostní požadavky na vývoj SW

3.1. Poskytovatel se při poskytování plnění pro objednatele zavazuje:

a) poskytovat objednateli v termínech stanovených objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje SW či po jeho předání; rozsah požadované součinnosti bude vždy součástí Zadání objednatele dle čl. 6.1.1.

b) k dodání systémové a provozní bezpečnostní dokumentace nejpozději do doby předání a převzetí SW způsobem uvedeným ve smlouvě, a to minimálně v rozsahu stanoveném v odst. 4 této přílohy;

c) že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování SW a/nebo které jsou specifikovány výslovně ve smlouvě (zejména, že SW nebude obsahovat žádné

nepotřebné komponenty, žádné programové vzorky apod.). Tento závazek se však nevztahuje na součásti, které v současnosti výše uvedenou podmínku nesplňují, avšak v minulosti ji plnily.

d) že pokud součástí plnění je i instalace operačního systému případně SW třetích stran, v průběhu jeho instalace, pokud se objednatel s poskytovatelem nedohodnou jinak, budou použity poslední otestované stabilní verze těchto produktů.

e) že veškerá data obsahující Důvěrné informace[1] dle článku 10 této smlouvy poskytnutá objednateli při realizaci plnění nebudou uchovávána v nešifrovaném tvaru a budou chráněna vůči neautorizovanému přístupu, nebude li mezi smluvními stranami v konkrétním případě dohodnuto jinak;

f) že v rámci poskytovaného plnění bude instalovat SW nebo jejich upgrade podle hardeningových bezpečnostních politik a v souladu s bezpečnostními standardy objednatele (platí pro poskytovatele, pokud byl s takovými bezpečnostními standardy seznámen). Pokud v případě změny bezpečnostních politik nebo bezpečnostních standardů objednatele dojde k navýšení pracnosti na straně poskytovatele, může poskytovatel odmítnout realizovat plnění podle těchto nových politik a standardů do doby, než budou příslušné změny a jejich dopady na cenu a SLA zaneseny ve formě dodatku k této smlouvě;

g) že v produkčním prostředí systému ICT bude obsažen pouze kompilovaný, respektive spustitelný kód, provozní logy a další nezbytná data pro provozování systému ICT;

h) před spuštěním dodaného SW v produkčním prostředí daného ICT systému provede kontrolu souladu daného SW s bezpečnostními požadavky hardeningových bezpečnostních politik v souladu s nabídkou na dodání SW a v případě zjištění nesouladu zajistí bez zbytečného odkladu soulad dodávaného SW s bezpečnostními požadavky hardeningových bezpečnostních politik (platí pro poskytovatele, pokud byl s takovými bezpečnostními standardy seznámen),

i) že ověří integritu zdrojového kódu a předá zdrojový kód objednateli bezpečnou formou, definovanou dohodou objednatele a poskytovatele a zajišťující integritu zdrojového kódu, přičemž bude průběžně evidovat a bezpečně ukládat zdrojové kódy provozovaných aplikací, a to i v případě, že budou zdrojové kódy předávány objednateli, přičemž při vývoji SW se poskytovatel zavazuje, že
    - zdrojový kód programů vyvíjených poskytovatelem bude předmětem procesu řízení verzí;
    - zdrojový kód programů je zálohován a uložen mimo produkční prostředí a současně je stanoven postup, jak sestavit systém ze zdrojového kódu.
    - provádění konfiguračních změn je v souladu s procesem změnového řízení objednatele. Tento proces je popsán v pracovním postupu ŘÍZENÍ ZMĚN ICT (CAH-PP-I1-008), vždy v odpovídající verzi.
    - konfigurační soubory jsou pravidelně průběžně zálohovány, pokud po dohodě objednatele a poskytovatele není toto zálohování odpovědností poskytovatele;
    - eviduje každou změnu konfigurace;

6 Požadavky na systémovou a provozní bezpečnostní dokumentaci.

Nedílnou součástí poskytovaného plnění je zdokumentování všech bezpečnostních nastavení, funkcí a mechanismů formou zpracování bezpečnostní dokumentace. Poskytovatel se v rámci poskytovaného plnění pro objednatele zavazuje předat objednateli dokumentaci minimálně v níže uvedeném rozsahu. Součástí dokumentace není popis plnění zajišťovaného objednatelem nebo popis součinnosti objednatele (například u dokumentace zálohování popíše poskytovatel pouze zálohování, které řeší vlastními prostředky. U

[1] Za důvěrné informace se ve smyslu této přílohy považují zejména identifikační údaje certifikátu, hesla, konfigurační soubory, obnovovací procedury apod. dle předané směrnice.

zálohování, které zajišťuje ČAH, nebude popis postupu zálohování součástí dokumentace předané poskytovatelem).

Tento požadavek se vztahuje pouze na Změny dle čl. 6 této Smlouvy. Poskytovatel není povinen upravit stávající dokumentaci Systému, pakliže tato úprava nebude předmětem Změny dle čl. 6 této Smlouvy.

Pokud nebude v rámci harmonogramu Změny dohodnuto jinak, dodá objednatel Poskytovateli kompletní seznam svých připomínek k dokumentaci nejpozději do 5 pracovních dní od předání dokumentace. Po dodání upravené verze dokumentace připomínkuje objednatel pouze zapracování předchozích připomínek a po zapracování těchto nových připomínek poskytovatelem proces končí. Připomínky k dokumentaci nejsou považovány za vady ve smyslu čl. 1.1.41 této smlouvy.

a) Administrátoriská dokumentace obsahující:
   - Stručný popis prostředí, kde je systém provozován (názvy a adresy serverů)
   - Popis konfiguračních parametrů (název a význam parametru, jeho umístění – název souboru či konfigurační tabulky, případný výčet možných hodnot)
   - Popis konfigurace logování (kde se nacházejí logy, kde se nachází konfigurace logování a klíčové logovací hlášky)
   - Základní postupy při administraci systému (postup nasazení nové verze, postup řešení 3 nejčastějších problémů)

b) Instalační dokumentace obsahující postup instalace (včetně názvů skriptů, které je třeba spustit) všech částí systému s výjimkou SW třetích stran, ke kterým výrobce poskytuje instalační postup v českém či anglickém jazyku. Při tvorbě dokumentace může poskytovatel vycházet z předpokladu, že dokumentaci budou používat odborně způsobilí administrátoři – v rámci dokumentace tedy není třeba popisovat obecně známé postupy (například připojení k databázovému serveru prostřednictvím SQL klienta).

7 Fyzická ochrana a bezpečnost prostředí

a) Poskytovatel se zavazuje dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny komponenty systémů ICT anebo datové nosiče (dále také jen „**Pracoviště**“).

b) Poskytovatel se zavazuje, že na Pracovišti neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k systému ICT, který je předmětem plnění dle této smlouvy. Objednatel poskytne poskytovateli nezbytnou součinnost.

8 Řízení přístupu

a) Poskytovatel bere na vědomí, že přístup k systému ICT je možné povolit pouze fyzické identitě zaměstnance poskytovatele / poddodavatele poskytovatele zaevidované v registru identit objednatele, a to na základě požadavku poskytovatele na přístup.

b) Poskytovatel bere na vědomí, že zaměstnanec poskytovatele musí prokazatelně souhlasit se zpracováním osobních údajů potřebných pro zřízení přístupu, v opačném případě objednatel není povinen přístup k systému ICT zaměstnanci poskytovatele povolit. Zaměstnanec poskytovatele s přiděleným přístupem (fyzickým, logickým) k systému ICT musí prokazatelně souhlasit se zpracováním osobních údajů zpracovávaných během vyhodnocování údajů o pohybu a prováděných aktivitách v prostorách objednatele (např.: monitoring pomocí řešení Security Incident and Event Monitoring), přičemž takový souhlas musí být proveden souhlasem písemným nebo digitálním formou emailu, není-li smluvními stranami dohodnuto jinak.

c) Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci poskytovatele musí být řízeno principem nezbytného minima a není nárokové. Pokud v důsledku nepřidělení či pozdního přidělení

oprávnění bude omezena schopnost poskytovatele splnit svoje závazky z této smlouvy, **proběhne jednání poskytovatele s objednatelem s cílem nalézt kompromis umožňující naplnění této smlouvy. Pokud se kompromis nepodaří nalézt a pokud poskytovatel vyvine ke splnění svých závazků z této smlouvy maximální úsilí, které po něm lze spravedlivě požadovat, a přesto dojde k porušení některého z těchto závazků**, nemá objednatel právo požadovat po poskytovateli smluvní pokutu či uplatňovat na poskytovateli náhradu škody.

d) Poskytovatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci poskytovatele nebo subdodavatele poskytovatele.

e) Poskytovatel se zavazuje, že přístup pro administraci ICT systému prostřednictvím mobilní aplikace bude vždy uskutečněn pouze prostřednictvím zabezpečeného připojení VPN.

f) Poskytovatel se zavazuje, že před připojením koncového zařízení, mobilní koncového zařízení nebo aktivního síťového prvku jako síťové switche, WiFi access pointy, routery či huby do počítačové sítě, která není přístupná veřejnosti a je provozována objednatelem, zažádá o schválení připojení kontaktní osobu na straně objednatele

g) Poskytovatel se zavazuje, že bez zbytečného odkladu deaktivuje všechny nevyužívané zakončení sítě anebo nepoužívané porty aktivního síťového prvku.

h) Poskytovatel se zavazuje, že bez schválené výjimky Objednatelem nebude instalovat a používat tyto typy nástrojů:
    - Keylogger,
    - Sniffer,
    - Analyzátor zranitelností a Port Scanner,
    - Backdoor, rootkit a trojský kůň nebo jinou podobu malware.

i) Poskytovatel se zavazuje, že všechny ICT systémy poskytovatele, které se připojují do síťové infrastruktury objednatele, jsou a budou chráněny proti malware.

j) Poskytovatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části systému ICT programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci systému ICT nebo nelegální získání dat a informací.

k) Poskytovatel se zavazuje zajistit, aby osoby při poskytování plnění v prostředí objednatele:
    - nenavštěvovaly internetové stránky s eticky nevhodným obsahem[2];
    - neukládaly a/nebo nesdíleli v prostředí objednatele data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno objednatele;
    - nestahovaly, nesdílely, neukládaly, nearchivovaly a/nebo neinstalovaly v prostředí objednatele datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem;
    - neukládaly a/nebo nesdílely data a informace společnosti na nepovolených datových úložištích nebo médiích (jejichž seznam objednatel poskytovateli předal) mimo domluvený komunikační kanál;
    - nezasílaly řetězové emaily.

l) Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění objednateli, kteří přistupují do interní sítě a/nebo systému ICT objednatele, respektovali a dodržovali následující omezení:
    - Zařízení typu notebook/počítač musí mít:

[2] Data a informace obsahující prvky extrémismu, terorismu, pornografie anebo podněcování k nesnášenlivosti a společenským předsudkům vztahujícím se ke společenské skupině identifikované na základě rasy, náboženství nebo víry, pohlaví, sexuální orientace, národnostní a etnické příslušnosti či jiné odlišnosti.

- aplikovány bezpečnostní záplaty (operačního systému, internetového prohlížeče a Javy)
- nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu;

m) Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění objednateli, kteří přistupují do interní sítě a/nebo systému ICT objednatele chránily autentizační prostředky a údaje k systémům ICT objednatele. Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako bezpečnostní incident ve smyslu příslušné řídící dokumentace a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu). Pokud v důsledku výše uvedeného bude omezena schopnost poskytovatele splnit svoje závazky z této smlouvy, nemá objednatel právo požadovat po poskytovateli smluvní pokutu či uplatňovat na poskytovateli náhradu škody pokud neprokáže, že k neúspěšným pokusům o autentizaci došlo vinou poskytovatele.

9 Monitorování

a) Poskytovatel bere na vědomí, že veškerá aktivita poskytovatele a jeho plnění realizované v systémovém prostředí objednatele budou objednatelem průběžně monitorovány a pravidelně vyhodnocovány s ohledem na obsah smlouvy a interních dokumentů objednatele, se kterými byl poskytovatel seznámen.

b) Poskytovatel se zavazuje, že záznamy/logy o úspěšných a neúspěšných přihlášeních a o správě uživatelů, které vznikají v rámci ICT Systému, předloží objednateli bez zbytečného odkladu po jejich vyžádání objednatelem. Tato povinnost platí po celou dobu platnosti smlouvy s výjimkou případů, kdy předložení logů brání důvody, které nejsou na straně poskytovatele (například chyba infrastruktury objednatele).

10 Předání a převzetí plnění

a) Poskytovatel bere na vědomí, že nedodržení Bezpečnostních požadavků daných bezpečnostní směrnicí (ve verzi platné ke dni akceptace zadání) nebo specifikovaných v zadání včetně požadavku na předání dokumentace v rozsahu dle čl. 6 předávaného předmětu je vadou bránící převzetí předmětu smlouvy (je vadou kategorie A), přičemž objednatel není do doby odstranění příslušné vady plnění povinen plnění převzít. Objednatel bere na vědomí, že dokumentace v požadovaném rozsahu bude pokrývat pouze plnění poskytnuté po datu účinnosti tohoto dodatku (poskytovatel není povinen zpětně zdokumentovat Systém v požadovaném rozsahu, pakliže to nebude předmětem Změny dle čl. 6)

b) Poskytovatel odpovídá za to, že systémy ICT budou obsahovat nejnovější bezpečnostní aktualizace (patche)[3] dle smluvně odsouhlasených pravidel Objednatele.

11 Výměna informací

a) Pokud je předmětem smlouvy výměna informací mezi smluvními stranami, musí být mezi smluvními stranami uzavřena dohoda o ochraně předmětných informací, zejména při jejich výměně, uložení, archivaci a ukončení smlouvy.

b) Obě strany se zavazují, že veškerý přenos dat a informací musí být dostatečně zabezpečen z pohledu bezpečnostní klasifikace a tedy požadavků na důvěrnost, integritu a dostupnost dat a informací.

c) Poskytovatel se zavazuje, že on-line transakce realizované prostřednictvím webových technologií budou chráněny SSL certifikáty (zajištění certifikátů je zodpovědností objednatele). Platí bez výhrady u dodaných řešení po platnosti uzavření tohoto dodatku.

[3] Aktualizace software na vyšší vývojovou verzi.

12 Zvládání bezpečnostních incidentů[4]

Poskytovatel se při poskytování plnění pro objednatele zavazuje, že:

a) neprodleně nahlásí bezpečnostní událost přes Kontaktní osobu objednatele uvedenou ve smlouvě;

b) v případě vzniku bezpečnostní události a následného zvládání a vyhodnocování bezpečnostního incidentu a/nebo v případě podezření na bezpečnostní incident, poskytne objednateli požadovanou součinnost (např.: poskytne logy a identifikační údaje (např. IP adresa, MAC adresa, HW typ, sériové číslo případně IMEI) dotyčného koncového zařízení nebo mobilního koncového zařízení zaměstnance poskytovatele nebo zaměstnance poddodavatele podílející se na realizaci plnění, k analýze obsahu, případně bez zbytečného odkladu zrealizuje opatření požadovaná objednatelem).

provede analýzu příčin bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že poskytovatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

[4] Pojem bezpečnostní incident a bezpečnostní událost je ekvivalentní pojmům Kybernetická bezpečnostní událost / Kybernetický bezpečnostní incident, vydefinovaných zákonem č. 181/2014 Sb. o kybernetické bezpečnosti. Pro potřeby tohoto dokumentu jsou pojmy vydefinovány takto:
Bezpečnostní událost: možné porušení bezpečnostní politiky nebo na selhání bezpečnostních opatření. Může se také jednat o jinou situaci, která dříve nenastala a může být z pohledu bezpečnosti informací důležitá. Může být příčinou nebo mít vliv na vznik bezpečnostního incidentu.
Bezpečnostní incident: jedna nebo více nežádoucích nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace procesů/činností společnosti objednatele a ohrožení bezpečnosti informací.