SMLOUVA O DÍLO

uzavřená podle ustanovení § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“)

I. Smluvní strany

Společnost:	**PragoData a.s.**
Sídlo:	Opletalova 1418/23, Nové Město, 110 00 Praha 1
IČO:	05433622
DIČ:	CZ05433622
Jednající:	Ing. Břetislav Moc, předseda správní rady
Bankovní spojení:	115-3342060277/0100

zapsaná v obchodním rejstříku u Městského soudu v Praze pod spisovou značkou B 21892

(dále jen „**Dodavatel**“)

a

Organizace:	**Centrum pro zjišťování výsledků vzdělávání**, státní příspěvková organizace (CZVV)
Sídlo:	Jankovcova 933/63, 170 00 Praha 7, Holešovice
IČO:	72029455
DIČ:	není plátcem DPH
Jednající:	RNDr. Michaela Kleňhová, ředitelka
Bankovní spojení:	1235071/0710

(dále jen „**Objednatel**“)

Dodavatel byl vybrán cestou NEN (Národní elektronický nástroj) na základě zadávacího řízení „Kybernetická návnada“, systémové číslo NEN: N006/21/V00033840 (dále jen „VZ“).

II. Předmět plnění

1) Dodavatel se touto smlouvou zavazuje provést pro Objednatele dodávku pokročilé ochrany sítě pomocí inteligentní návnady jako ochrany před interními a externími kybernetickými útoky, integraci dodaného řešení s klíčovými komponentami ochrany sítě na straně Objednatele, instalaci a konfiguraci nabízeného řešení dle požadavků Objednatele. Dodavatel stvrzuje, že je certifikovaným partnerem výrobce pro dodávku a instalaci nabízeného technického řešení a má certifikované techniky, kteří budou provádět instalaci. Veškerý dodaný SW musí být v souladu s legislativou, zejména ZoKB a GDPR a musí k němu být v tomto smyslu dodána odpovídající technická dokumentace.

2) Přesná specifikace a technické požadavky celé dodávky jsou uvedeny v příloze č. 1 - Technická specifikace, která tvoří nedílnou součást této smlouvy (dále jen „technická specifikace“). Dodávka bude provedena rovněž v souladu s požadavky Objednatele, které byly součástí zadávacích podmínek v rámci zadávacího řízení VZ a v souladu s přílohou č. 2 této smlouvy - Projekt implementace v prostředí Objednatele. Jako součást dodávky vypracuje Dodavatel na základě analýzy požadavků Objednatele a v souladu se svou nabídkou, kterou dodavatel předložil v rámci zadávacího řízení, realizační projekt (dále jen „realizační projekt“). Po schválení realizačního projektu Objednatelem se tento považuje za součást technické specifikace a bude aplikován přednostně. Příloha č. 1 bude mít podpůrné využití a použije se v případě, že realizační projekt nebude upravovat danou otázku výslovně jinak. Schválením realizačního projektu nepřechází

na Objednatele odpovědnost za řádnou realizaci dodávky a její použitelnost pro účely plynoucí z této smlouvy.

3) Součástí realizačního projektu bude i popis akceptační procedury a kritérií, které musí instalovaná dodávka splňovat, aby mohlo být Objednatelem ověřeno řádné provedení dodávky a dodávka mohla na základě toho být převzata. Objednatel není povinen (je však oprávněn) převzít jakékoli plnění, které obsahuje vady nebo nedodělky, a to ani pokud by nebránily užití tohoto plnění.

4) Touto smlouvou se Dodavatel zavazuje dodat Objednateli výše uvedenou dodávku, včetně souvisejících činností a Objednatel se zavazuje při dodržení podmínek této smlouvy uvedenou dodávku a související činnosti řádně a včas převzít a zaplatit za ně dohodnutou cenu.

III. Dodací podmínky a doba plnění

1) Smlouva bude splněna dodáním zařízení do datového centra Objednatele v Praze (místo bude upřesněno po podpisu smlouvy) a poskytnutím souvisejících služeb, blíže specifikovaných v příloze č. 1 této smlouvy - Technická specifikace.

2) O úspěšné realizaci dodávky dle článku II. smlouvy bude mezi smluvními stranami sepsán Akceptační protokol.

3) Zodpovědným zástupcem Objednatele pro převzetí dodávky dle článku II. této smlouvy je zaměstnanec Objednatele RNDr. Aleš Vychodil [redacted]

4) Doba plnění je sjednána nejpozději do 90 dnů od uzavření této smlouvy. Plnění smlouvy bude probíhat dle přílohy č. 4 této smlouvy – Časový harmonogram plnění smlouvy.

5) Prodlení Dodavatele s dodávkou a souvisejícími činnostmi delší jak 30 pracovních dnů se považuje za podstatné porušení smlouvy a zakládá právo Objednatele od smlouvy odstoupit.

IV. Cena plnění

1) Cena za celkovou dodávku v rozsahu dle této smlouvy je oběma smluvními stranami sjednána ve výši: **1.845.000,- Kč bez DPH** (slovy jeden_milion_osm_set_čtyřicet_pět_tisíc korun českých).

2) Rozpis ceny jednotlivých částí dodávky je uveden v příloze č. 3 - Rozpis ceny plnění do jednotkových cen, která tvoří nedílnou součást této smlouvy.

3) Sjednaná cena je fixní platí až do předání a převzetí celé dodávky.

4) Smluvní cena bude Dodavateli uhrazena až po řádném předání a převzetí dodávky Akceptačním protokolem.

V. Platební podmínky

1) Dodavatel vystaví fakturu po protokolárním předání a převzetí celé dodávky Objednateli, ve které bude samostatně vyúčtována DPH u jednotlivých položek. Přílohou faktury bude kopie dokladu o předání a převzetí – Akceptační protokol. Objednatel nebude poskytovat zálohy ani dílčí platby.

2) Faktura musí obsahovat náležitosti stanovené zákonem č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů

3) Splatnost faktury se sjednává na 30 dnů od obdržení daňového dokladu Objednatelem. Dodavatel bude akceptovat přiměřené prodloužení této lhůty splatnosti vynucené případným státním rozpočtovým provizoriem.

4) Objednatel má právo vrátit před termínem splatnosti neproplacenou fakturu k doplnění jako neúplnou, pokud tato nebude obsahovat veškeré náležitosti daňového a účetního dokladu a přílohu, případně další náležitosti dle podmínek této smlouvy a souvisejících právních předpisů. Dodavatel je v tomto případě povinen fakturu bez zbytečného prodlení přepracovat resp. doplnit a doručit ji Objednateli.

VI. Zahájení, průběh a ukončení dodávky

1) Dodavatel zajistí, že se jeho případní poddodavatelé zaváží dodržovat v plném rozsahu ujednání této smlouvy.

2) Přístup Dodavatele do rozvaděčoven, serveroven apod. bude umožněn pouze za přítomnosti odpovědného pracovníka Objednatele.

3) Dodavatel je při poskytování plnění dle Smlouvy oprávněn užívat data předaná mu Objednatelem či jiným způsobem získaná nebo vytvořená při plnění této Smlouvy (dále jen „Data“) pouze v rozsahu nezbytném ke splnění Smlouvy a pouze v souladu s touto Smlouvou a příslušnými právními předpisy, tj. zejména ZoKB a VoKB.

4) Před připojením zařízení do sítě Objednatele musí být provedeny bezpečnostní testy HW i SW na jejich bezpečnost a kompatibilitu v prostředí Objednatele (např. penetrační testy certifikovaným technikem nebo jiné certifikované testy prokazující nezávadnou funkčnost řešení).

5) Objednatel převezme plnění v souladu s touto smlouvou a Dodavatel předá Objednateli také veškerou dokumentaci a doklady, které se k dodávce vztahují (návody, záruční listy, licenční oprávnění).

6) Vlastnické právo ke zboží a právo k užití software nejméně v rozsahu nezbytném pro naplnění účelu této smlouvy a využití dodávky Objednatelem pro zamýšlené účely přechází na Objednatele okamžikem jeho převzetí.

VII. Záruka za jakost, servis

1) Dodavatel ručí za funkčnost předmětu této smlouvy v rozsahu a parametrech stanovených touto smlouvou. Záruka a technická a servisní podpora je na 4 roky v režimu 24x7x365.

2) V rámci záruky se Dodavatel zavazuje nahlášenou závadu na dodávce odstranit nejpozději do 15 dní, nevyplývá-li z technické specifikace kratší doba řešení.

VIII. Sankce

1) Pokud bude Dodavatel v prodlení s dodávkou nebo odstraněním nahlášené záruční závady, je povinen zaplatit Objednateli za každý i započatý den tohoto prodlení smluvní pokutu ve výši 1 000 Kč bez DPH.

2) V případě prodlení Objednatele s úhradou faktury je Dodavatel oprávněn uplatnit vůči Objednateli zákonný úrok z prodlení.

IX. Důvěrnost informací

1) Každá ze smluvních stran se zavazuje zachovávat v tajnosti všechny informace důvěrného charakteru, týkající se opačné smluvní strany, které se dozví v průběhu vzájemné spolupráce, a to i po skočení platnosti této smlouvy. Jakékoli tyto informace lze použít jen pro splnění předmětu této smlouvy. Za důvěrné informace se pro účely této smlouvy považují zejména informace obsažené v dokumentaci a materiálech dodaných nebo přijatých v jakékoli formě nebo poskytnuté některou smluvní stranou na základě této smlouvy a další informace týkající se některé smluvní strany, její činnosti či obchodních partnerů apod., které nejsou veřejně známé a dostupné a k jejichž zveřejnění dotčená smluvní strana výslovně neudělila souhlas. Smluvní strany se zavazují, že veškeré důvěrné informace, které jim budou poskytnuty, nesdělí ani jinak nezpřístupní třetím osobám s výjimkou osob zúčastněných na poskytování plnění dle této smlouvy; takové osoby musí být zavázány mlčenlivostí v rozsahu dle této smlouvy. Povinnost zachovávat závazek mlčenlivosti ve vztahu k důvěrným informacím trvá po celou dobu existence smluvního vztahu, tak i po jeho zániku do té doby, nežli se důvěrné informace stanou veřejně známými, aniž by smluvní strana porušila své povinnosti podle této smlouvy. Výše uvedená ustanovení a z nich vyplývající závazky se nevztahují na informace:

   - jejichž poskytnutí nebo sdělení bylo předem písemně schváleno chráněnou smluvní stranou,

- které smluvní strana označila výslovně jako veřejné, které se staly veřejně známými, aniž by smluvní strana povinná zachovávat mlčenlivost porušila povinnosti podle této smlouvy nebo ve smyslu této smlouvy,
- k jejichž sdělení je smluvní strana povinna podle právního předpisu nebo rozhodnutí soudu, správního či státního orgánu,
- uvedené v této smlouvě.

2) Dodavatel má zavedeno opatření pro ochranu osobních údajů v souladu s čl. 32 Nařízením EU 2016/679 (GDPR).

X. Ostatní ujednání

1) Dodavatel je povinen Objednatele bez zbytečného odkladu informovat o:
   - identifikovaných kybernetických bezpečnostních incidentech souvisejících s plněním Smlouvy, nejpozději však do 48 hodin od výskytu,
   - způsobu řízení rizik na straně Dodavatele a o zbytkových rizicích souvisejících s plněním Smlouvy,
   - významné změně ovládání Dodavatele, přičemž ovládáním se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů, či ekvivalentní postavení, a to do 5 pracovních dnů od uskutečnění této změny,
   - změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými Dodavatelem k plnění Smlouvy, a to do 5 pracovních dnů od uskutečnění této změny.
2) Dodavatel je povinen odsouhlasit a dodržovat bezpečnostní politiky Objednatele, které mu budou předány po podpisu smlouvy.
3) Objednatel má právo jednostranně odstoupit od smlouvy v případě významné změny kontroly nad Dodavatelem nebo změny kontroly nad zásadními aktivy využívanými Dodavatelem k plnění podle smlouvy.

XI. Provádění auditů

1) Dodavatel umožní jednou ročně provedení dodavatelského auditu.
2) Dodavatel poskytne veškerou nezbytnou součinnost k řádnému provádění a dokončení tohoto auditu.

XII. Závěrečná ustanovení

1) Tato smlouva se řídí právem České republiky, zejména zákonem č. 89/2012 Sb., občanský zákoník.
2) Smluvní strany se dohodly, že při ukončení Smlouvy z jakéhokoli důvodu vyvinou veškeré úsilí k tomu, aby do doby dokončení migrace Dat či převodu plnění dle Smlouvy k Objednateli nebo jinému provozovateli nedošlo k narušení parametrů plnění ve Smlouvě do té doby definovaných a aby případný nový provozovatel dostal veškeré informace o plnění Smlouvy potřebných pro pokračování nebo nahrazení takového plnění.
3) Dodavatel se zavazuje při plnění Smlouvy postupovat dle systému řízení změn Objednatele a v souladu s § 11 VoKB. Dodavatel prohlašuje, že v rámci své organizace má implementovaný systém řízení změn, tak aby byl schopen doložit veškeré předchozí verze SW či dokumentace, které byly Objednateli předloženy.
4) Smlouva nabývá platnosti dnem jejího podepsání oběma smluvními stranami a účinnosti po zveřejnění v Registru smluv dle odst. 6 níže. Měněna může být pouze písemnými, vzestupně číslovanými dodatky.
5) Dodavatel bere na vědomí, že se realizací této veřejné zakázky stane v souladu s ustanovením § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly

prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů nebo veřejné finanční podpory.

6) Tato smlouva bude zveřejněna v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Objednatel zašle tuto smlouvu správci registru smluv k uveřejnění bez zbytečného odkladu, nejpozději však do 30 dnů od uzavření smlouvy.

7) Tato Smlouva je vyhotovena v elektronické formě a smluvní strany prohlašují, že si ji přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují své uznávané elektronické podpisy dle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.

8) Nedílnou součástí smlouvy jsou přílohy:

   Příloha č. 1 – Technická specifikace;

   Příloha č. 2 - Projekt implementace v prostředí Objednatele;

   Příloha č. 3 – Rozpis ceny plnění do jednotkových cen;

   Příloha č. 4 – Časový harmonogram plnění smlouvy.

V Praze dne dle elektronického podpisu	V Praze dne dle elektronického podpisu
za Dodavatele:	za Objednatele:
.....	.....
PragoData a.s.	**Centrum pro zjišťování výsledků vzdělávání**
Ing. Břetislav Moc, předseda správní rady	RNDr. Michaela Kleňhová, ředitelka

Příloha č. 1

Technická specifikace

1. Popis způsobu splnění technických parametrů nabízeným řešením

Předmět plnění smlouvy je:

- dodávka pokročilé ochrany sítě pomocí inteligentní návnady jako ochrany před interními a externími kybernetickými útoky;
- integrace dodaného řešení s klíčovými komponentami ochrany sítě na straně Zadavatele;
- instalace a konfigurace nabízeného řešení dle požadavků Zadavatele;
- záruka a technická podpora výrobce v délce 4 roky v režimu 24x7x365 dle níže uvedené specifikace.

Dodávané řešení je navrženo jako modulární systém technologie [redacted] (HW appliance) tak, aby organizace byla schopna předcházet situacím/útokům a detekovat veškerá rizika podvodného jednání s cílem oklamat útočníky, odhalit je a eliminovat vnější a vnitřní hrozby dříve, než dojde ke vniknutí narušitele a významným škodám uvnitř organizace. Součástí plnění smlouvy je i zajištění podpory výrobce na všechny nabízené produkty a licence pro požadované subscription na 4 roky.

Realizace as instalace navrženého řešení bude probíhat právě a jedině zásahem do stávající LAN a bude prováděna za provozu. Jakékoli zásahy nebudou mít vliv na funkčnost LAN s dopadem na provoz v celém areálu Objednatele. Dodavatel svým zásahem do konfigurací bezpečnostních prvků nesmí svojí neodborností ovlivnit, omezit, narušit či odstavit provoz Objednatele v produkčních časech od 8:00 – 16:00 hod.

1.1 Splnění požadavků Objednatele na řešení inteligentní návnady

Předmětem plnění navrženého řešení inteligentní návnady jako proaktivní ochrany před podvodnými útoky je zajištění nejvyšší možné ochrany proti narušení organizace, a to také proaktivním způsobem. Řešení je navrženo tak, aby organizace byla schopna takovým situacím/útokům předcházet a detekovat veškerá rizika podvodného jednání s cílem oklamat útočníky, odhalit je a eliminovat vnější a vnitřní hrozby dříve, než dojde ke vniknutí narušitele a významným škodám uvnitř organizace.

Nabízené řešení inteligentní návnady sloužící pro detekci vnějších a vnitřních hrozeb kyberútoků plní nebo i převyšuje všechny Objednatelem požadované technické parametry, uvedené v následující tabulce:

ID	Požadovaná funkcionalita / vlastnost zařízení včetně všech modulů	Popis funkcionality či odkaz popis v nabídce či přiložené tech. dokumentaci Dodavatele
A1	Řešení ochrany na bázi inteligentní návnady (Honeypot) – odhalení a eliminace vnějších a vnitřních hrozeb. Proaktivní detekce rizika kyberútoku na IT a OT systémy.	[redacted] viz datasheet P1.1 [redacted].pdf
A2	HW appliance / VM na dodaném HW s vysokou dostupností	HW appliance
A3	Funkce komunikace s firewally	ANO, splňuje, podpora [redacted] (security fabric), PANW, Cisco ISE, obecný webhook, REST API za účelem zablokování stanice/serveru. [redacted] vyhodnotí stanici/server jako zdroj šíření škodlivého kódu v síti nebo zařízení napadené škodlivým kódem a Firewall zablokuje jeho provoz, viz dokument P1.2_Administration Guide [redacted] 4.1.0, str. 56
A4	Pokročilá detekce TTPs	ANO, splňuje, viz datasheet P1.1 [redacted].pdf
A5	Možnosti klamných nástrah prostředí (Windows, Linux, IoT, SCADA, SSL VPN)	ANO, splňuje, viz datasheet P1.1 [redacted].pdf

ID	Požadovaná funkcionalita / vlastnost zařízení včetně všech modulů	Popis funkcionality či odkaz popis v nabídce či přiložené tech. dokumentaci Dodavatele
A6	Podpora pro produkční a testovací prostředí	ANO, splňuje, viz dokument P1.2_Administration Guide [redacted] 4.1.0, str. 14
A7	Systém pro eliminaci interních a externích hrozeb v DMZ	ANO, splňuje, viz dokument P1.2_Administration Guide [redacted] 4.1.0, str. 48
A8	Podpora systémů SIEM a SOAR	ANO, splňuje, viz dokument P1.2_Administration Guide [redacted] 4.1.0, str. 119
A9	Aktivní notifikace, možnosti: • webové rozhraní • e-mail • SNMP	ANO, splňuje, viz dokument P1.2_Administration Guide [redacted] 4.1.0, str. 70
A10	Automatizované reakce na vzniklé hrozby prostřednictvím integrovaných modulů	ANO, splňuje, viz dokument P1.2_Administration Guide [redacted] 4.1.0, str. 60
A11	Integrace s bezpečnostním řešením třetích stran (API)	ANO, splňuje, viz dokument P1.2_Administration Guide [redacted] 4.1.0, str. 60
A12	Integrované nastavení návnad pro ochranu IT, OT, IoT	ANO, splňuje, viz dokument P1.2_Administration Guide [redacted] 4.1.0, str. 101
A13	Korelace incidentů do časové osy	ANO, splňuje, viz dokument P1.2_Administration Guide [redacted] 4.1.0, str. 50
A14	Aplikace návnad pro automatickou detekci podvodného chování útočníka, typy návnad: • RDP • SSH • SMB • SAMBA • SQL • FTP • GIT	ANO, splňuje, viz dokument P1.2_Administration Guide [redacted] 4.1.0, str. 36
A15	Zobrazení s podrobnými informacemi o systému, aktuálním stavu a seznamem možných hrozeb	ANO, splňuje, viz dokument P1.2_Administration Guide [redacted] 4.1.0, str. 76
A16	Systém integrované ochrany: • antivirus • honeypot • ransomware, malware • prevence narušení • analýza hrozeb • webová ochrana	ANO, splňuje, viz dokument P1.2_Administration Guide [redacted] 4.1.0, str. 74
A17	Všechny funkce musí být poskytovány lokálně (nikoliv jako cloud služba)	ANO, splňuje, viz datasheet P1.1 [redacted].pdf
A18	Funkce systému: • admin rozhraní pro správu • bezpečnostní reporty • analýzy • logování veškerých aktivit systému	ANO, splňuje, viz datasheet P1.1 [redacted].pdf

ID	Požadovaná funkcionalita / vlastnost zařízení včetně všech modulů	Popis funkcionality či odkaz popis v nabídce či přiložené tech. dokumentaci Dodavatele
A19	Integrovaný systém návnad s cílem detekce chování útočníka: • nasazení VM počítačů (Windows, Linux, SCADA) • generování návnad (data, aplikace / služby) • nasazení návnady na PC / servery uživatelů	ANO, splňuje, viz dokument P1.2_Administration Guide [redacted] 4.1.0, str. 7, 14 a 47
A20	Podpora Windows licencí BYOL	ANO, splňuje, viz dokument P1.2_Administration Guide [redacted] 4.1.0, str. 14
A21	Podpora karantény přímo na daném zařízení, podpora pravidelného reportingu	ANO, splňuje, viz dokument P1.2_Administration Guide [redacted] 4.1.0, str. 61
A22	Licenční model nezávislý na počtu chráněných uživatelů	ANO, splňuje, viz datasheet P1.1 [redacted].pdf
A23	Licence a podpora výrobce 24x7x365 na 1, 2, 3, 4 a 5 let	ANO, splňuje, viz datasheet P1.1 [redacted].pdf
A24	Podpora instalace klamných nástrah až do 12 VLAN	ANO, splňuje, viz datasheet P1.1 [redacted].pdf

1.2 Splnění požadavků na instalaci, záruku a technickou podporu

Nabízené řešení plní nebo i převyšuje všechny Objednatelem požadované technické parametry, uvedené v následující tabulce:

ID	Požadavek	Způsob splnění požadavku nabízeným řešením Dodavatele
D1	Instalace a konfigurace nabízeného řešení, zpracování základní provozní dokumentace instalovaného řešení, v rozsahu 15 MD (man-day)	ANO, služba instalace a konfigurace nabízeného řešení včetně zpracování základní provozní dokumentace v rozsahu do 15 MD je nedílnou součástí navrhovaného řešení a ceny.
D2	Zajištění 4-leté záruky a technické podpory výrobce na nabízené řešení v režimu 24x7x365	ANO, služba [redacted] pro zajištění 4-leté záruky a technické podpory výrobce je nedílnou součástí navrženého řešení a ceny.
D3	Integrace nabízeného řešení s firewally Fortinet FortiGate používané v prostředí Zadavatele	ANO, služba integrace nabízeného řešení v požadovaném rozsahu je nedílnou součástí navrhovaného řešení a ceny. Podrobně popsáno v bodu A3 výše.
D4	Zajištění, po dobu trvání podpory, poskytování informací o nových SW verzích a funkcionalitách, které mohou rozšiřovat nabízené řešení způsobem, který Zadavatel shledá ve shodě s potřebami dalšího rozvoje řešení	ANO, poskytování informací o nových SW verzích a funkcionalitách, které mohou rozšiřovat nabízené řešení, je součástí služby [redacted] a je nedílnou součástí navrhovaného řešení a ceny.
D5	Zajištění, po dobu trvání podpory, přístupu k dokumentaci výrobce zařízení a znalostní bázi, kterou výrobce v rámci své podpory poskytuje. Zadavatel musí mít možnost si sám legálně stahovat nové verze software a operačního systému nabízených zařízení přímo ze stránek výrobce	ANO, po dobu trvání podpory bude prostřednictvím služby [redacted] výrobce zajištěn přístup Objednatele k dokumentaci výrobce zařízení a znalostní bázi (FAQ). Objednatel bude mít možnost si sám legálně stahovat nové verze software a operačního systému nabízených zařízení přímo ze stránek výrobce.
D6	Seznámení max. 3 zástupců Zadavatele s nabízeným řešením a jejich základní proškolení pro práci s dodanými nástroji v rozsahu do 3 MD (man-day)	ANO, služba seznámení do 3 zástupců Objednatele s nabízeným řešením a jejich základní proškolení pro práci s dodanými nástroji v rozsahu do 3 MD je nedílnou součástí navrhovaného řešení a ceny.

ID	Požadavek	Způsob splnění požadavku nabízeným řešením Dodavatele
D7	Účastník bude povinen s dodávkou doložit oficiální potvrzení zastoupení výrobce o určení dodávaného HW (seznamu sériových čísel dodávaných zařízení) pro český trh a koncového zákazníka. Zadavatel požaduje originální zařízení, licencované ve jménu Zadavatele tak, aby bylo možné eskalovat případné závady na technickou podporu výrobce. V databázi výrobce musí být Zadavatel veden jako první uživatel dodaného zboží. Zadavatel požaduje originální a nové komponenty (výjimku tvoří využití stávajících komponent Zadavatele).	ANO, Dodavatel s realizací dodávky doloží požadované potvrzení. Předmětem dodání budou originální zařízení dle požadavku D7 Objednatele. Na portálu výrobce bude možné řešit a eskalovat závady. Na portálu výrobce bude Objednatel řádně registrován jako první uživatel zařízení.
D8	Zadavatel musí mít možnost se sám zaregistrovat na stránkách výrobce k odběru automatických mailových zpráv týkajících se poptávaných zařízení a upozorňujících s denní frekvencí na: 1) bezpečnostní incidenty, které vyžadují od Zadavatele povýšení operačního systému/firmware či aplikování změny konfigurace či záplaty. 2) konec prodeje či podpory. 3) nové verze operačního systému/firmware. 4) známé chyby operačního systému/firmware.	ANO, Objednatel bude mít možnost se sám zaregistrovat na stránkách výrobce k odběru požadovaných automatických e-mailových zpráv. Na portálu výrobce bude provedena registrace Objednatele s možností notifikace požadovaných zpráv (1-4).

1.3 Přílohy

Nedílnou součástí této Přílohy č. 1 smlouvy jsou následující samostatné dokumenty příloh v elektronické podobě:

- datasheet: **P1.1_[redacted].pdf** (https://www.[redacted]-sheets/[redacted].pdf)
- příručka administrátora: **P1.2_[redacted].pdf**

Příloha č. 2

Projekt implementace v prostředí Objednatele

Základní popis technologie navrženého řešení

Technologie [redacted] je technologické zařízení (HW appliance) navržené tak, aby podvodně lákalo útočníky a následně odhalovalo a eliminovalo vnější a vnitřní hrozby v rané fázi útoku.

Zařízení řady [redacted] e součástí komplexní řady technologií pro řešení bezpečnostní struktury výrobce [redacted] a poskytuje jednotnou komplexní ochranu s firewally [redacted] nové generace (NGFW) pro řešení pokročilých hrozeb. Přidání [redacted] jako součásti strategie ochrany proti narušení pomáhá rozvíjet obranu Objednatele z reaktivní na proaktivní s detekcí průniku a s kontextovou inteligencí. Zařízení [redacted]:

- automatizuje vyhledávání a blokování útočníků zaměřených na IT zařízení.
- automaticky vytvoří vrstvy návnad a pastí, které pomohou skrýt citlivá a kritická aktiva za vykonstruovaným falešným povrchem, který zmate a přesměruje útočníky a zároveň odhalí jejich přítomnost v síti.

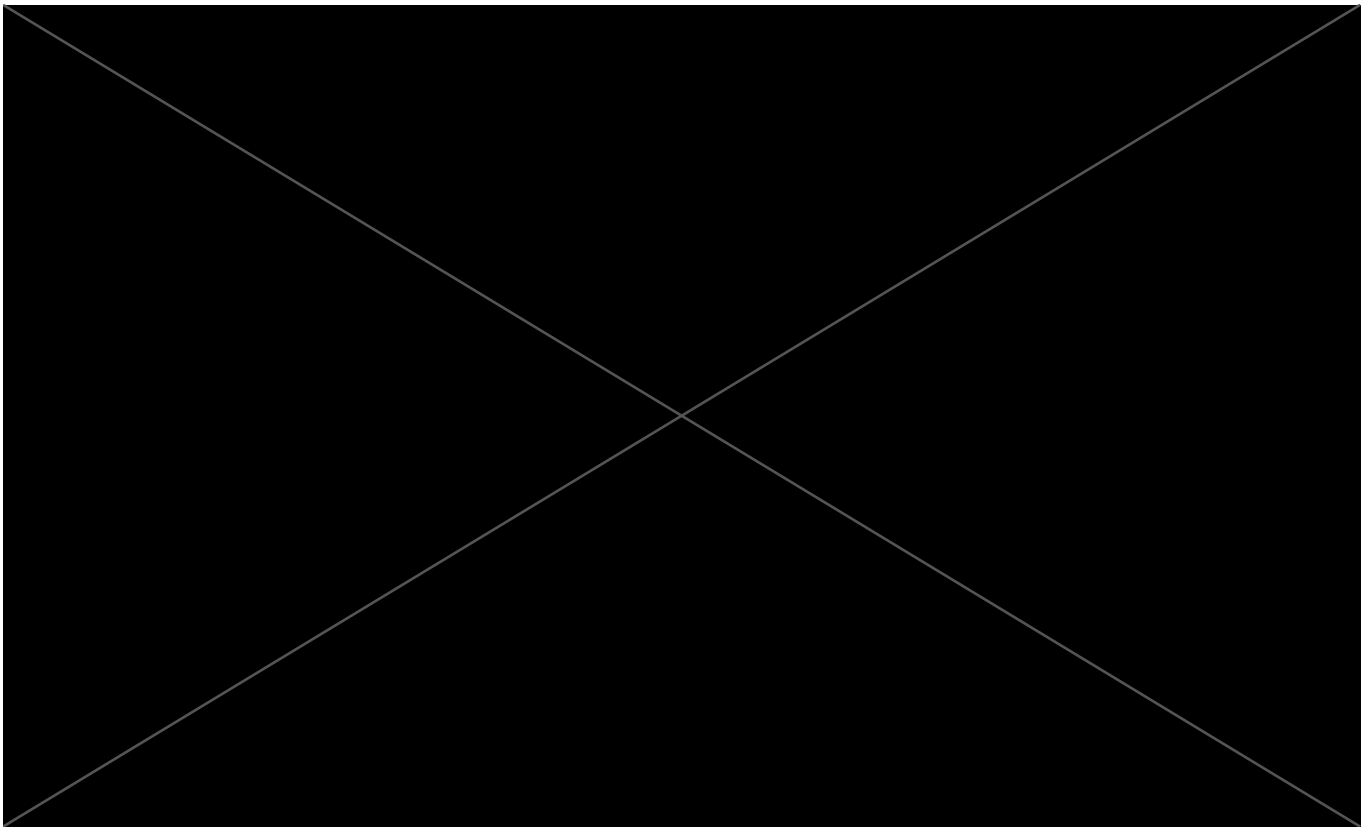
Klamáním externí a interní hrozby probíhá pomocí klamavých instancí virtuálních počítačů neboli návnad, spravovaných z jednoho centra. Nasadí se tak falešný podvrh skutečných virtuálních počítačů se systémem Windows, Linux, VPN, Medical IoT a SCADA se službami, které jsou k nerozeznání od skutečných aktiv, např. produkční servery, a lákadla zabudovaná do zařízení určených k odhalení útočníků. Odhalí se tím aktivita hackerů s včasnou a přesnou detekcí a výstrahami, které lze použít prostřednictvím trasování a korelace taktiky, nástrojů a postupů (TTP) útočníka a aktivního oznámení prostřednictvím webového uživatelského rozhraní, e-mailu, SNMP pastí i protokolů a událostí prostřednictvím technologií [redacted] a [redacted]. Následně se hrozby eliminují automatizací reakce na hrozby pomocí technologií [redacted], [redacted], [redacted] a bezpečnostních řešení třetích stran prostřednictvím [redacted] [redacted].

Řešení je jednoduché a snadno použitelné v prostředích IT/OT/IoT a je založené na průvodcích, obecných návnadách a návnadách vyladěných pro cílové prostředí, které centrálně spravuje distribuované nasazení podvodů napříč cílovým IT / OT prostředím Objednatele.

Vyšetřování hrozeb je inteligentní s korelací incidentů do časové osy kampaně všech aktivit, včetně přístupu, použitých nástrojů, bočního pohybu a dalších, vrstvených kontextovými informacemi o hrozbách od [redacted] Labs. Řešení eliminujte útoky v rané fázi pomocí integrace [redacted] a třetích stran. [redacted] nasazuje návnady s různými typy operačních systémů vybavených návnadami (např. RDP / SMB / Credentials / HoneyDocs), které se zdají být nerozeznatelné od skutečných IT / OT aktiv a jsou vysoce interaktivní.

- [redacted] tak působí jako systém včasného varování, který odhaluje škodlivý záměr útočníka a sleduje jeho pohyb, což se promítá do výstrah v reálném čase, odesílaných do [redacted], stejně jako [redacted] a [redacted] pro jejich kontrolu a ověření. [redacted] aplikuje analytiku založenou na [redacted] Labs, [redacted] a analýze [redacted] na konsolidovanou sadu bezpečnostních událostí a koreluje je s kampaněmi s časovou osou aktivit.
- [redacted] umožňuje bezpečnostnímu analytikovi manuálně prozkoumat a následně použít buď ruční nápravu nebo automaticky zablokovat tyto útoky na základě jejich závažnosti ještě předtím, než dojde ke skutečnému poškození prostřednictvím integrace s [redacted], [redacted] a [redacted].

Principy implementace technologie [redacted] do topologie sítě Objednatele



Detailní popis způsobu implementace navrženého řešení bude nedílnou součástí realizačního projektu, který Dodavatel vypracuje v souladu s požadavky smlouvy na základě úvodní analýzy požadavků a obdrženého popisu topologie sítě Objednatele.

[redacted] NÁVNADY

Úlohou modulu [redacted] je přidat tokeny na skutečné koncové body a servery a přesměrovat útočníka tak, aby se zapojil do návnady namísto skutečného aktiva. Návnady na klamání jsou obvykle distribuovány v rámci skutečných koncových bodů a serverů v síti aby se rozšířila plocha klamání.

Efektivní technologie klamání podporuje následující funkcionality:

- Možnost nasazovat data a konfigurace klamných návnad, kde útočníci shromažďují informace.
- Umísťovat klamné návnady je pro koncové uživatele neviditelné a nemá vliv na funkčnost koncového bodu.
- Návnada klamání je přístupná s oprávněními na úrovni uživatele, aby k ní útočníci měli přístup a mohli být včas odhaleni. To šetří čas privilegovaného eskalačního útoku.

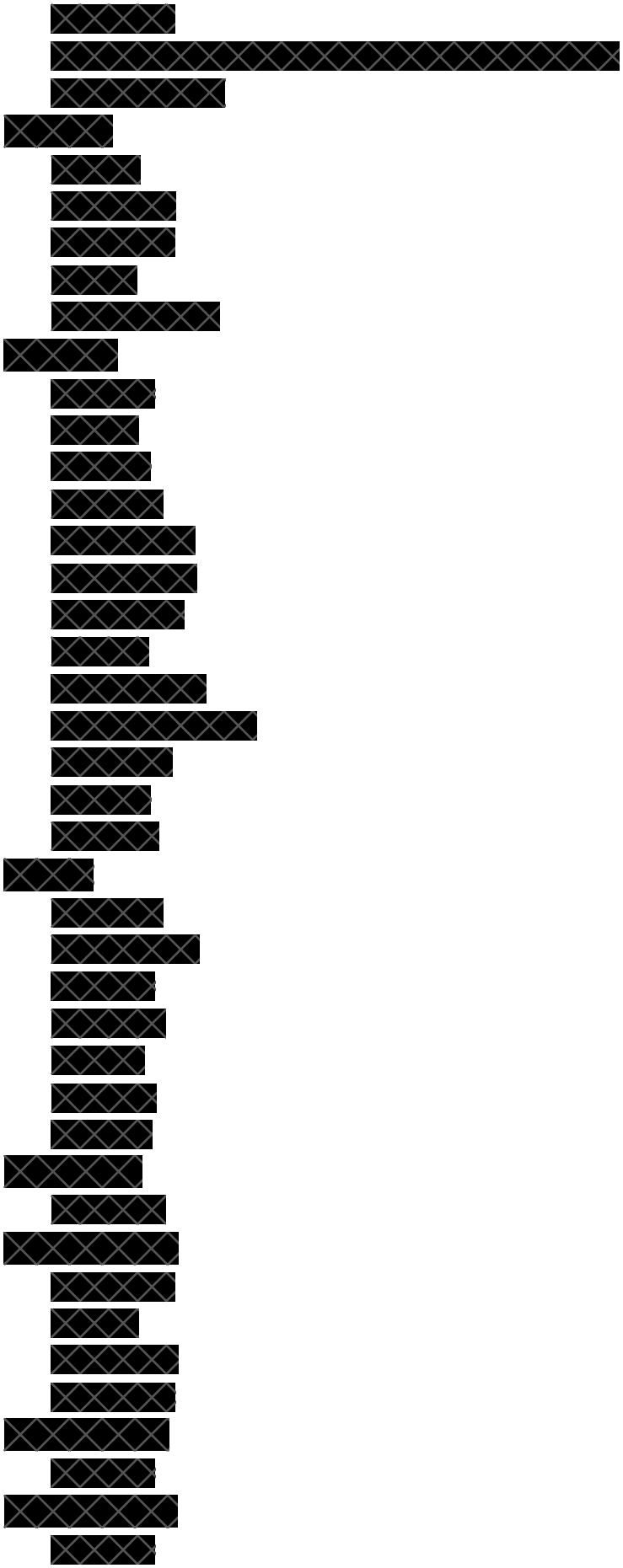
[redacted]

[redacted]

[redacted] NÁVNADY

[redacted] vytváří síť návnad pro nalákání útočníků a sledování jejich aktivit v síti. Když útočníci zaútočí na návnadu, nejprve se vygeneruje výstraha a následně jsou jejich škodlivé aktivity zachyceny a analyzovány v reálném čase, aby se vytvořila odpovídající reakce na zmírnění a nápravu, která síť ochrání.

[redacted]



Osvědčené postupy pro implementaci klamných návnad u koncových bodů Windows, MAC nebo Linux

RDP návnada:

- Nastavit několik návnad serveru Windows, které podporují přístup RDP.
- Nastavit vhodné názvy hostitelů návnady jako Terminal-XX, VDI-XX a další, které zvýší úroveň autenticity, pokud se návnady serveru Windows přidají do domény společnosti.
- Dodržovat zásady uživatelského jména a hesla společnosti.
- Vygenerovat 2-3 klamné návnady a rozmístit je v několika různých skupinách uživatelů AD.

SMB návnada:

Pro koncové body Windows použít návnadu SMB nebo návnadu SAMBA, ale nepoužít obě.

- Nastavit alespoň dvě návnady serveru Windows, které podporují dva falešné sdílené síťové přístupy.
- Vygenerovat alespoň dvě návnady se dvěma různými sdílenými názvy.
- Použít sdílený název podobný struktuře společnosti.
- Nastavit vhodné názvy hostitelů jako FileSRV-XX, File-Server a další, které zvýší úroveň autenticity, pokud se návnada Windows serveru přidá do firemní domény.
- Dodržovat zásady uživatelského jména a hesla společnosti.
- Vygenerovat jeden balíček podvodných návnad a nasadit jej na všechny koncové body sítě.

SAMBA návnada:

Pro koncové body Windows použijte návnadu SMB nebo návnadu SAMBA. Nepoužívejte obojí.

- Nastavte alespoň dvě návnady serveru Linux, které podporují sdílený síťový přístup.
- Nastavte vhodné názvy hostitelů jako Storage-XX, Backup-Server a další.
- Vygenerujte alespoň dvě návnady se dvěma různými sdílenými názvy.
- Použijte sdílený název podobný struktuře společnosti.
- Dodržovat zásady uživatelského jména a hesla společnosti.
- Vygenerujte jeden balíček podvodných návnad a nasaďte jej na všechny koncové body sítě.

SSH návnada:

- Nastavit několik linuxových serverových návnad, které podporují přístup SSH.
- Nastavit vhodné názvy hostitelů jako JumpHost-XX, Control-XX, Cloud-XXX a další.
- Použít složité heslo, které v útočníkovi vyvolává dojem, že se jedná o kritický server.
- Vygenerovat 2–3 klamné návnady a nasadit je pouze na skupinu koncových IT bodů, protože útočníci neočekávají, že uvidí klienty SSH na běžném desktopu.

Návnada na přihlašovací údaje v mezipaměti:

Tato podvodná návnada vyžaduje, aby návnada Windows byla součástí síťové domény. Možnost návnady nebude v GUI viditelná, dokud nebude návnada součástí domény.

- Nastavit alespoň dvě přizpůsobené návnady serveru Windows, které jsou součástí firemní domény.
- Vytvořit alespoň 2 doménové uživatele v síťové doméně a omezit jejich přístup na konkrétní IP adresy a přidat IP adresy návnady k oklamání útočníka.
- Nakonfigurovat výše uvedené uživatele domény v konfiguraci pověření uložených v mezipaměti, přičemž je možné skutečné uživatelské heslo domény nebo falešné heslo v závislosti na požadované úrovni zapojení návnady.
- Vygenerovat jediný balíček podvodných návnad a nasadit jej na všechny koncové body sítě.

Návnada HoneyDocs:

Tato návnada generuje soubory (Word & PDF), které spustí výstrahu, jakmile je otevře aktér hrozby.

- Balíček HoneyDocs bude používat výchozí soubory šablon nebo soubory, které koncový uživatel nahraje prostřednictvím konfigurace zdroje Návnady.
- Balíček HoneyDocs bude součástí balíčku Windows Návnady a bude nainstalován do adresáře posledních dokumentů [redacted]
- Koncový uživatel může přistupovat k souboru honeydoc.json nad adresáři windows\resdirectory a měnit umístění souboru.

Návnada na záznamy ARP:

- Tato podvodná návnada je součástí všech balíčků (Windows, Linux a MAC) a vkládá falešné položky ARP do koncového bodu, aby oklamala útočníka na úrovni sítě.
- Tato klamná návnada nevyžaduje žádnou konfiguraci a je generována automaticky.

Poznámka: Na rozdíl od zbytku návnady Deception vyžaduje tato návnada k instalaci pověření správce.

Osvědčené postupy pro integraci AD

Active Directory (AD) je proprietární adresářová služba společnosti Microsoft, která běží na Windows Server a umožňuje správcům spravovat oprávnění a přístup k síťovým zdrojům. Služba Active Directory ukládá data jako objekty, přičemž objekt je jeden prvek (např. uživatel, skupina, aplikace) nebo zařízení (např. tiskárna).

Pro detekci útok na AD pomocí technologie klamání se použije následující příklad konfigurace klamání:

- [redacted]

Vlastní návnady v doméně sítě:

- Přidat několik vlastních návnad systému Windows do síťové domény zákazníka.
- V doméně Windows nakonfigurovat skripty naplánovaných úloh tak, aby se spouštěly pomocí falešných uživatelů (např. jako je ten z návnady pověření mezipaměti).
- Přidat do každé návnady domény maximální počet IP adres a ujistit se, že se jedná o statické IP adresy.
- Na síťovém serveru DNS nakonfigurovat návnadu DNS.
    - Přidat DNS záznamy ke každé IP adrese návnady.
    - Nastavit atraktivní názvy hostitelů pro každou IP adresu návnady.
- Vytvořit a nasadit přední návnadu pro malé a střední podniky v návnadě domény, aby byla eliminována detekce nástroji jako HoneyBuster.

Služby řízení projektu a ostatní služby související s realizací předmětu plnění

Detailní popis instalace a konfigurace dodávaného zařízení F[redacted] bude součástí Realizačního projektu a bude vycházet z požadavků a detailních informací o architektuře IT prostředí Objednatele, které Objednatel poskytne v úvodní analytické fázi projektu, a které zcela samozřejmě nemohly být součástí Zadávací dokumentace a ani by to z hlediska zajištění bezpečnosti informací nebylo vhodné.

Pro projektové řízení realizace plnění smlouvy bude využito principů vycházejících ze standardizované metodiky projektového řízení Prince2®. Nezbytné detaily organizace a řízení projektu řízení budou popsány v Realizačním projektu, vypracovaném v souladu s harmonogramem plnění dle Přílohy č. 4 smlouvy.

Nedílnou součástí Realizačního projektu bude i popis způsobu řešení incidentů pro poskytovanou záruku a technickou podporu výrobce, způsob realizace akceptační procedury, popis akceptačních testů a průběhu akceptace, předání a zahájení rutinního provozu, struktury provozní dokumentace a provedení proškolení.

Příloha č. 3

Rozpis ceny plnění do jednotkových cen

V tabulce níže je uveden rozpis celkové ceny za plnění smlouvy do jednotkových cen položek plnění v Kč bez DPH.

P/N	popis položky plnění	počet	cena za ks	cena celkem
[redacted]	[redacted]	1	450.000,-	450.000,-
[redacted]	[redacted]	12	36.000,-	432.000,-
[redacted]	[redacted]	12	14.000,-	168.000,-
[redacted]	[redacted]	3	80.000,-	240.000,-
[redacted]	3 Years 24x7 [redacted]	1	260.000,-	260.000,-
[redacted]	1 Year 24x7 [redacted]	1	70.000,-	70.000,-
Služby	Poskytnutí souvisejících služeb dle Přílohy č. 1 smlouvy	1	225.000,-	225.000,-
			Cena celkem v Kč bez DPH	**1.845.000,-**
			Cena celkem v Kč včetně DPH	**2.232.450,-**

Příloha č. 4

Časový harmonogram plnění smlouvy

Rámcový harmonogram plnění je zpracován s ohledem na potřebu zajištění řádné implementace předmětu plnění smlouvy.

#	projektový milník plnění smlouvy	termín[1]
1	Nabytí platnosti a účinnosti smlouvy	**T**
2	Analýza požadavků Objednatele	T + 14 dnů
3	Vypracování Realizačního projektu	T + 21 dnů
4	Akceptace Realizačního projektu	T + 25 dnů
5	Dodávka a implementace řešení dle Realizačního projektu včetně integrace s klíčovými komponentami ochrany sítě Objednatele	T + 60 dnů (viz upozornění níže)
6	Instalace a konfigurace realizovaného řešení dle požadavků Objednatele specifikovaných v Realizačním projektu	T + 70 dnů
7	Poskytnutí souvisejících služeb dle Přílohy č. 1 smlouvy	T + 85 dnů
8	Testování a akceptace plnění dle specifikace Realizačního projektu	T + 88 dnů
9	Předání plnění a zahájení rutinního provozu	T + 90 dnů

Upozornění:

Dodavatel nemůže za současné celosvětově kritické situace distribučních a logistických kanálů výrobců zcela garantovat pevné datum dodání zařízení [redacted] protože termín dodání zařízení je zcela mimo kontrolu a možnost ovlivnění ze strany Dodavatele a v plné míře závisí na výrobci zařízení, společnosti [redacted], jeho distribučním kanálu v České republice (společnost DNS) a době vlastní dopravy.

Dodavatel se zavazuje neprodleně informovat Objednatele o předpokládaných termínech dodání zařízení, jakmile je obdrží od výrobce zařízení, popř. z distribučního kanálu.

Dodavatel na základě výše uvedených skutečností nenese odpovědnost za případné zpoždění dodávky zařízení Objednateli způsobené výrobcem nebo jeho distribučním / logistickým kanálem.

[1] Nejzazší termín dokončení projektového milníku plnění smlouvy.