ALEF

Trust the Strong

Nabídka na vytvoření procesu pro reakci na bezpečnostní incidenty

Obsah

1 Úvod

1.1 Účel dokumentu

Tento dokument obsahuje nabídku na vytvoření procesu pro reakci na bezpečnostní incidenty.

Název společnosti:	**Lesy České republiky, s. p.**
Sídlo:	Přemyslova 1106/19, 500 08 Hradec Králové
IČ:	42196451

1.2 Dodavatel

Název společnosti:	**ALEF NULA, a.s. (dále Dodavatel)** společnost je zapsaná v obchodním rejstříku Městského soudu v Praze, oddíl B., vložka 2727
Sídlo:	Pernerova 691/42, 186 00 Praha 8
IČ:	61858579
DIČ:	CZ61858579
Bankovní spojení:	Komerční banka, a.s.
č. účtu:	51-3717150237/0100
Jednající:	Milan Zinek, předseda představenstva
Telefon:	[redacted]
Fax:	[redacted]

1.3 Zástupce Dodavatele

Zástupcem dodavatele pověřený jednáním v souvislosti s touto obchodní nabídkou je [redacted], [redacted]

2 Informace o Dodavateli

2.1 Profil společnosti

Společnost ALEF NULA a.s. je předním dodavatelem zákaznických řešení pro komunikační infrastrukturu v České republice a je součástí nadnárodní skupiny Alef Group, působící v několika zemích střední Evropy.
Nejvyšší prioritou společnosti je dlouhodobá spokojenost zákazníků - tedy pozorné vnímání jejich potřeb a realizace řešení v nejvyšší kvalitě. I proto se ALEF NULA a.s. už od svého založení v roce 1994 orientuje na produkty renomovaných výrobců, především společnosti Cisco Systems. V této souvislosti je ALEF NULA a.s. držitelem nejvyšší partnerské certifikace Cisco Systems Partner – Gold Certified.
Kromě implementačních projektů tradiční LAN/WAN infrastruktury má ALEF NULA a.s. špičkové know-how, rozsáhlé zkušenosti i odborné certifikace v řadě dalších produktových oblastí – od datových center, přes síťovou bezpečnost a wireless až po IP telefonii, videokonferenční řešení a kontaktní centra. K tomu poskytuje ALEF NULA svým zákazníkům i konzultační služby, rychlou servisní podporu a školení. ALEF NULA je držitelem certifikace Cisco Learning Partner a patří mezi pět největších školicích středisek technologie Cisco v Evropě.
Systém řízení jakosti ALEF NULA a.s. je ve shodě s normou ISO 9001:2008.

2.2 Produktové certifikace ALEF NULA a.s.

Níže jsou uvedeny vybrané certifikace společnosti ALEF NULA, a.s.

- Cisco Gold Certified Partner,
- Cisco Advanced Collaboration Architecture Specialized Partner,
- Cisco Advanced Data Center Architecture Specialized Partner,
- Cisco Advanced Enterprise Networks Architecture Specialized Partner,
- Cisco Advanced Security Architecture Specialized Partner,
- Cisco Advanced Service Provider Architecture Specialized Partner,
- Cisco Express Specialized Partner,
- Cisco Learning Partner,
- Cisco Solution Partner.
- 2Ring Partner,
- AWS Consulting Partner,
- AWS Solution Provider & Training Partner,
- ATECO Partner,
- Commvault Partner,
- F5 Authorized Training Center,
- Flowmon Gold Partner,
- Microsoft Gold Technology Partner,
- MobileIron Partner,
- NetApp Contract Delivery Partner,
- Sewio Certified Partner,
- SPLUNK Associate Partner,
- VMware Solution Provider – Enterprise Partner,
- ZOOM Gold Partner.

3 Shrnutí požadavků Zákazníka

Zákazník poptává vytvoření dokumentu, který definuje základní procesy a postupy při reakci na kybernetické bezpečnostní incidenty v interním IT prostředí a umožní tak odhalené incidenty řešit efektivně a s minimálními dopady.

4 Popis nabízeného řešení

4.1 Analýza cílového prostředí a posouzení existujících procesů

V prostředí Zákazníka bude za pomoci osobního šetření a dotazování a případného přezkoumání relevantní interní dokumentace proveden sběr informací týkajících se

- organizačního (personální struktura a odpovědnosti, stávající role v oblasti IT a bezpečnosti,…) a
- technického (užívané bezpečnostní nástroje, řízení oprávnění uživatelů a administrátorů, úroveň logování,…)

fungování cílového prostředí. Na základě něj bude mj. provedena identifikace jakýchkoli existujících procesů s vazbou na reakci na kybernetické bezpečnostní události a incidenty.

4.2 Vytvoření plánu reakce na incidenty

V návaznosti na závěry výše popsané první fáze projektu bude vytvořen návrh obecného plánu pro reakci na kybernetické bezpečnostní incidenty (KBI) v prostředí Zákazníka, doplněný o popis doporučeného řešení vybraných dalších aspektů této problematiky. Výstupem bude textový dokument, který bude obsahovat obecný popis doporučení pro následující oblasti:

- Vytvoření virtuálního týmu pro reakci na KBI (jeho struktura, působnost,…)
- Obecný proces pro reakci na KBI (doplněný o vývojové diagramy postupů)
- Eskalační mechanismy a postupy při zvládání KBI
- Evidence a řízení KBI v rámci ticketovacího systému
- Interní a externí komunikace při reakci na bezpečnostní incidenty
- Reporting v oblasti KBI
- Kategorizace a klasifikace bezpečnostních incidentů a související SLA
- Obecné postupy pro analýzu a reakci na definované typy KBI (1. úroveň klasifikace RSIT[1]) v prostředí Zákazníka

4.3 Závěrečná prezentace

Obsah vytvořeného plánu reakce na KBI bude v rámci jednorázové závěrečné prezentace představen vybraným zástupcům Zákazníka.

[1] https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md

5 Vymezení rozsahu projektu

V rámci projektu bude připraven výše zmíněný textový dokument ve formátu DOCX, který bude obsahovat popis doporučení pro řešení vybraných aspektů v oblasti reakce na bezpečnostní incidenty v prostředí Zákazníka. Dokument se nebude jakkoli zabývat problematikou bezpečnostního monitoringu a možnostmi detekce bezpečnostních incidentů v cílovém prostředí, pouze problematikou reakce na vzniklé incidenty.
Zajištění implementace v dokumentu formulovaných doporučení bude ponecháno plně v kompetenci Zákazníka a nebude součástí projektu. Mimo rozsah projektu bude rovněž tvorba jakýchkoli materiálů nad rámec těch výše výslovně uvedených, nebo realizace jakýchkoli dalších aktivit nad rámec těch výše výslovně uvedených.

5.1 Požadovaná součinnost

Zákazník se zavazuje poskytovat následující součinnost:

a) Spolupráci na identifikaci existujících bezpečnostních procesů a analýze organizačního a technického prostředí (mj. zprostředkování schůzek se zástupci relevantních rolí z různých oddělení).

b) Poskytnutí jakékoli relevantní existující bezpečnostní dokumentace.

c) Poskytnutí podkladů týkajících se relevantních bezpečnostních technologií užívaných v infrastruktuře Zákazníka.

d) Participace na tvorbě a validaci relevantních procesů.

e) Poskytnutí informací o případných relevantních dodavatelích klíčových služeb a produktů souvisejících s kybernetickou bezpečností.

Za předpokladu včasného poskytnutí výše popsané součinnosti bude projekt dodán nejpozději do šesti týdnů od závazné objednávky.

6 Reference bezpečnostních projektů

6.1 Implementace bezpečnostních systémů

Vybrané implementace v oblasti řízení informační bezpečnosti ICT:

- Generální ředitelství cel
- Český hydrometeorologický ústav
- Krajský úřad Jihočeského kraje
- ČEZ Distribuce, a.s.
- Mero ČR a.s.
- NET4GAS, s.r.o.
- Krajská Nemocnice Liberec, a.s.
- Ad. …

6.2 Bezpečnostní služby a poradenství

Vybrané služby v oblasti bezpečnostního auditu, bezpečnostního designu a poradenství:

- Český hydrometeorologický ústav
- Komerční banka, a.s.
- ERA a.s.
- Energetický regulační úřad
- Moravskoslezský kraj
- Institut klinické a experimentální medicíny
- Krajský úřad Olomouckého kraje
- Krajský úřad Pardubického kraje
- Krajský úřad Ústeckého kraje
- Ministerstvo průmyslu a obchodu
- České dráhy
- Generální ředitelství cel
- Zdravotnická záchranná služba Jihomoravského kraje
- Ad. …

7 Cenová nabídka

7.1 Rozpis ceny

Předmět nabídky	Cena bez DPH
Vytvoření procesu pro reakci na bezpečnostní incidenty	206.000, - Kč

7.2 Platební podmínky

Splatnost faktur je 30 dní.