Příloha č. 1 smlouvy: Detailní specifikace předmětu plnění

V rámci plnění Poskytovatel zajistí:

1. Převzetí prostředí
2. Na základě potvrzení o převzetí všech vstupních podkladů a přístupů Poskytovatel provede základní převzetí a nastavení celého prostředí, a to včetně potřebných úprav síťových a internetových nastavení (např. DNS záznamů) a to takovým způsobem, aby nedošlo k přerušení fungování systému stávajícího.

Součástí převzetí jsou lokality Objednatele v následujících lokalitách (počet uživatelů je přibližný):

* Centrála, Vinohradská 46 - 80 uživatelů
* Info centrum Vinohradská 46 - 4 uživatelé
* Info centrum Staroměstské náměstí 5 – 4 uživatelé
* Datové centrum Master Internet - Laconex a.s.,Svatoslavova 355/8, Praha 4
* Zahraniční zastoupení – 49 uživatelů – seznam zahraničních zastoupení tvoří přílohu č. 3 smlouvy
1. Dále Poskytovatel v rámci převzetí prostředí provede následující úkony:
2. Jednorázový bezpečnostní scan, přičemž výstupem bude seznam všech prvků, u kterých byl scan proveden, včetně jejich hodnocení a podrobným návrhem na odstranění případných nedostatků. Výstup musí obsahovat minimálně tyto informace:
	1. Typ scanovaného zařízení včetně podrobných informací o HW a SW.
	2. Seznam nalezených bezpečnostních problémů.
	3. Doporučení na jejich odstranění včetně příslušného finančního odhadu a doby potřebné na nápravu stavu.
3. Jednorázový asset management, na který Poskytovatel použije automatizovaný nástroj, přičemž výstupem bude:
	1. Kompletní soupis všech IT prvků Zadavatele, a to včetně koncových stanic, serverů, aktivních prvků, tiskáren, scannerů a dalšího IT vybavení, přičemž z provedeného scanu bude možné vytvářet libovolně definovatelné sestavy na základě požadavků Zadavatele, jako například seznam všech stanic s instalovaným určitým software, výpis HW určitého typu, porovnání vybavení stanic dle určitého typu HW, SW atd.
	2. Provedené scany bude možno uchovávat pro pozdější použití, bude možné je aktualizovat buď na základě pravidelného scanu či na základě požadavku Zadavatele.
	3. Výstup ze scanu bude možno exportovat do obecně použitelných formátů, minimálně souborů typu PDF, XLS a TXT.
	4. Výstupy z prvotního scanu musí umožnit specifikovat nejvíce problémové prvky (ať již z pohledu zastaralosti, neexistence podpory výrobce, typu softwarového vybavení atd.) a následně sestavit seznam nutných náprav včetně odhadu finančních nákladů.
	5. Software na asset management musí umožňovat i vzdálený přístup ve smyslu scanu stanic, které se nenacházejí v dosahu lokální sítě v centrále Zadavatele. Tyto dodatečné informace musí být schopen použitý software integrovat do celkového stavu soupisu HW a SW.
	6. Scan bude možno použít opakovaně a porovnávat automaticky rozdíly.
4. Vytvoření katalogu služeb. Vytvoření úvodního katalogu služeb, který bude obsahovat minimálně:
	1. Popis služby, definice rozsahu, popis SLA parametrů, způsob eskalačních mechanismů, způsob vykonávání služby, omezení platnosti, odpovědné osoby na straně dodavatele i Zadavatele, přičemž takto budou zpracovány katalogové listy minimálně pro následující kategorie:
		1. Hlavní aplikace Zadavatele
		2. Síťovou infrastrukturu
		3. Servery a jejich programové vybavení
		4. Koncové stanice
		5. Monitoring
		6. Správa perimetru
		7. Zálohování
	2. Seznam katalogových služeb včetně výše popsaných požadavků bude uveden jako jedna z příloh nabídky.
5. Vyčištění koncových stanic od nepodporovaného software, nastavení jednotného prostředí
6. Dle výše požadovaného scanu dojde k odinstalaci nepotřebného software, záznamu takto uvolněných licencí software a nastavení jednotného způsobu využívání lokálního software a prostoru na lokálních discích koncových stanic. Výstupem bude aktualizovaný souhrn vybavení, a to včetně provedeného asset managementu, který detailně zmapuje stav a využití koncové stanice, a to i z pohledu softwarového vybavení (tj. scan bude proveden 2x, úvodní a po tomto prvotním čistění a úpravách).

Tento výstup bude sloužit jako jeden z podkladů pro akceptaci této části ze strany Objednatele.

Pro potřeby vzdáleného přístupu bude využit software pro vzdálené ovládání, jehož licence je ve vlastnictví Objednatele.

1. Správa infrastruktury

# Správou infrastruktury se míní veškeré aktivní a pasivní prvky infrastruktury Objednatele, a to ve všech lokalitách vyjmenovaných výše této přílohy.

* 1. Seznam současné infrastruktury:

## Centrální Servery

|  |  |  |
| --- | --- | --- |
| Název zařízení | Datum pořízení | Popis zařízení |
| Server Mercury MP 1099SA | 26.06.2006 | SERVER MERCURY MP 1099SA |
| Server IBM X3400 | 02.08.2007 | SERVER IBM X3400 |
| Server IBMX3200 czech on-line | 01.07.2008 | SERVER IBMX3200 CZECH ON- |
| ServerIBMX3400 czech on-line | 01.07.2008 | SERVERIBMX3400 CZECH ON-L |
| IOP-5, Server DELL T110, X3430 | 01.07.2010 | IOP-5, SERVER DELL T110, |
| IOP-5, Server DELL T110, X3460 | 01.07.2010 | IOP-5, SERVER DELL T11001 |
| Poštovní Server Mercury MX4010SA= počítač | 04.04.2006 | PŘÍSTROJ POŠTOVNÍ SERVER |
| Web Server Mercury MX5010HS = počítač | 05.05.2006 | PŘÍSTROJ WEB SERVER MERCU |
| Server Mercury MX5015HA | 05.05.2009 | PŘÍSTROJ SERVER MERCURY M |
| Server IBM X3400 | 21.05.2009 | PŘÍSTROJ SERVER IBM X3400 |
| Server IBM X3400 | 21.05.2009 | PŘÍSTROJ SERVER IBM X3400 |
| Server Dell R 320 | 05.11.2013 | PŘÍSTROJ SERVER DELL R 32 |
| Server Dell R220 | 19.11.2014 | SERVER DELL R220 |
| Dell Poweredge 4400 | 22.01.2001 | PŘÍSTROJ DELL POWEREDGE 4 |
| Přístroj SuperStack3 3300 XM | 19.03.2001 | PŘÍSTROJ SUPERSTACK3 3300 |
| Přístroj SuperStack3 3300 XM | 19.03.2001 | PŘÍSTROJ SUPERSTACK3 3300 |
| Server Del PE 2500 | 01.06.2001 | PŘÍSTROJ SERVER DEL PE 25 |
| Server PowerEdge 2500 | 19.10.2001 | PŘÍSTROJ POČÍTAČ POWEREDG |
| Server Barbone Atlantis SX | 10.08.2003 | PŘÍSTROJ SERVER BARBONE A |

## Disková pole:

|  |  |  |
| --- | --- | --- |
| EMC VNXe-3100 |  | 12 disků 2TB RAID 6 |
| EMC VNXe-3100 |  | 6 disků 2TB RAID 6 |
| Netgear readyNAS 516 |  | 6x4 TB RAID 5 |
| Netgear readyNAS 516 |  | 6x4 TB RAID 5 |

## Síťové prvky

|  |  |  |
| --- | --- | --- |
| **místnost** | **kategorie** | **typ** |
| 201 | switch | 3Com Superstack 3C16985B |
| 400 | switch | Planet GSW-2401 |
| 400 | switch | Planet GSW-2401 |
| 402 | switch | Repotec RP-1705K |
| 405 | switch | ZyXEL GS-105B |
| 407 | switch | 3Com Office Connect 5 Port |
| 409 | switch | TP-LINK TL-SG1008D |
| 410 | switch | ZyXEL GS-105B |
| 500 | switch | Planet GSW-2401 |
|  |  |  |
| 601 | switch | Micronet SP684C |
| 601 | switch | Repotec RP-G2404W |
| 601 | switch | Repotec RP-G2404W |
| 601 | switch | Repotec RP-G2404W |
| 601 | switch | Cisco SG200-08 |
| 601 | switch | FortiMail 100 |
| 601 | switch | Cisco SG200-08 |
| 603 | switch | TP-Link TL-SG1005D |
| 609 | switch | TP-Link TL-SG1008D |
| 701 | switch | Planet GSW-2401 |
| 702 | switch | ZyXEL GS-105B |
| 713 | switch | ZyXEL GS-105B |
| info | switch | Micronet SP684C |
| info | switch | Micronet SP684C |

## Bezdrátové prvky:

|  |  |  |
| --- | --- | --- |
| **místnost** | **kategorie** | **typ** |
| 508 | wifi | ZyXEL NWA1100 |
| 605 | wifi | ZyXEL NWA1100 |
| 704 | wifi | Air Live FSH8PS |
| info | wifi | ASUS RT-N16 |
| staromak | wifi | ASUS WL-520g |

## Servery – DC Kodaňská 46, 101 00 Praha 10 (5 serverů a 1x PC)

|  |  |  |  |
| --- | --- | --- | --- |
| **Model** | **Označení** | **Sér.číslo** | **Umístění** |
| IBM x3400 | WWW server | KDXBNZX | serverovna Kodaňská, D255 |
| IBM x3400 | WWW server | KDXBPAA | serverovna Kodaňská, D261 |
| IBM x236 | WWW server | KDXNTL8 | serverovna Kodaňská, D1203 |
| Asus | FTPSERVER | NA | serverovna Kodaňská, D1279 |
| noname | TIC APP | 6BVB54J | serverovna Kodaňská, D1323 |
| noname | TIC DB | 7BVB54J | serverovna Kodaňská, D1321 |

* 1. Kromě zmíněných aktivních a pasivních součástí je nutno v rámci správy infrastruktury zabezpečit:
1. Správa DNS záznamů a všech činností souvisejících s doménami Objednatele a to i ve spolupráci s dalšími dodavateli Objednatele.
2. Správa IP adresního prostoru.
3. Zajištění základních síťových služeb pro lokální sítě a celou infrastrukturu (DNS, DHCP, NTP).
4. Zajištění správy hesel a dalších senzitivních informací dle bezpečnostních pravidel stanovených Objednatelem. Tyto zásady budou předány Poskytovateli v rámci předání vstupní dokumentace.
5. Součinnost při nastavování nových a aktualizovaných bezpečnostních pravidel v budoucnu
6. Zajištění kompletní a aktualizované dokumentace kompletního prostředí ICT Zadavatele (myšleno spravované části)
7. Poskytovatel je povinen zajistit zaznamenávání veškerých činností prováděných na aktivních prvcích infrastruktury pomocí nástroje na sběr provozních dat a tyto logy uchovávat na bezpečném úložišti a následně archivu pro potřeby Objednatele po dobu minimálně 12 měsíců online a dále archivovat dle požadavků Objednatele.
	1. Nástroj, kterým bude Poskytovatel celou infrastrukturu dohlížet a monitorovat musí splňovat minimálně tyto požadavky:
8. Monitorování infrastruktury v reálném čase, včetně možnosti nastavení alarmů v případě překročení specifikovaných mezních hodnot (treshholds)
9. Inteligentní reporty, tj. možnost jejich přizpůsobení, automatické generování, reporty postavené na bázi specifických dotazů
10. Integrace s monitorováním fyzických i virtuálních serverů
11. Záznam činností (trasholdů) a jejich odesílání na integrovaný helpdesk (servicedesk) a do zařízení (dále definovaným) na záznam provozních událostí
12. Základní analýza síťového provozu
13. Integrovaný configuration management, tj. možnost správy konfigurací prvků přes jednotné prostředí a jejich zálohování (tam kde to jednotlivé prvky umožňují)
14. IP address management jako volitelná součást monitorovacího nástroje
15. Integrovaný monitoring aplikací
16. Integrace s mobilními platformami
17. Zasílání reportů a alertů pomocí definovaných kanálů (email, SMS)
18. Možnost integrace s nástrojem na správu koncových stanic
19. Výstupy z monitoringu ve formě vhodné pro následnou analýzu pomocí nástrojů třetích stran (nebo dodatečného modulu stejného nástroje, pokud je taková možnost)
20. Možnost dohledu cloudových technologií, pokud Zadavatel takové aplikace používá či plánuje používat – nutná podpora minimálně prostředí Microsoft Office 365.
21. Správa aplikací a systémů
	1. Správa aplikací je vyžadována v lokálním prostředí Zadavatele, jakožto i v prostředí vzdáleném. Mezi základní podporované aplikace a systémy je nutno počítat následující:
22. Aplikace instalované a provozované na lokální infrastruktuře Objednatele, mezi které patří:
	1. Seznam serverových aplikací

Hlavní aplikace:

* Elektronická pošta Microsoft Exchange
* IS Helios (pro dostupnost historických dat)
* IS IRAP
* Avensio

Mezi další lze řadit:

* Frankovačka
* Profibanka KB
* Teamio
* PowerKey
	1. Aplikace provozované v rámci služeb Microsoft Office 365

Seznam aplikací – aktuálně zakoupené licence Microsoft Office 365 E3:

* + - Word
		- Excel
		- PowerPoint
		- Outlook
		- OneNote
		- Publisher (jenom PC)
		- SharePoint
		- OneDrive pro firmy
		- Skype
		- Access (jenom PC)

Cloudové služby:

* + - Exchange
		- OneDrive
		- SharePoint
		- Skype pro firmy
		- Microsoft Teams
		- Yammer
1. Systémová podpora serverů
	1. HW serverů je uveden v bodě 2.2
	2. Serverové operační systémy Microsoft a Linux
2. Ostatní webové služby
	1. Capsa
	2. Dropbox
	3. Image banka
	4. Brand manuál
3. Zálohování prostředí
	1. Podpora řešení DPM Backup.
4. Správa a aktualizace příslušné dokumentace
5. Služby bezpečnosti

Poskytovatel zabezpečí následující činnosti:

* 1. Správa perimetru

Lokální síť Objednatele je od Internetu oddělena pomocí řešení Kerio. Toto řešení bude následně nahrazeno HW řešením.

Objednatel požaduje následující činnosti:

1. Prvotní kontrola nastavení a to včetně úprav či smazání nepotřebných pravidel
2. Pravidelné čištění nepoužívaných a přebytečných pravidel
3. Přenos pravidel na novou infrastrukturu
4. Pravidelné scany zranitelnosti včetně vyhotovených reportů, a to minimálně v periodě jednou za 3 měsíce
5. Pravidelný patch management celého prostředí
6. Systémová správa prostředí perimetru.
7. Správa a aktualizace příslušné dokumentace
	1. Služba asset management
		1. Pro všechny IT prvky je požadována implementace automatické služby asset managementu, který bude probíhat v pravidelných intervalech a reporty budou požadovány ve stejné struktuře jako u požadavku uvedeného v kapitole 1 Převzetí prostředí. Pravidelné reporty budou Poskytovatelem předkládány v měsíčním intervalu.
		2. Reporty v části bezpečnosti budou umožňovat filtraci na potenciálně rizikové části sledovaných prvků infrastruktury, a to i s možností uvedení možností o nápravě takto nevyhovujícího stavu.
	2. Služba záznam provozních událostí
		1. Záznam provozních událostí z celé infrastruktury, kam patří všechny aktivní prvky, servery, aplikace, koncové stanice, tiskárny a případná další zařízení, je jednou z kritických služeb, které musí Poskytovatel zajistit s parametry dále specifikovanými.
		2. Minimální rozsah systému na záznam provozních událostí:

Schopnost zpracování všech logů zařízení a systémů uvedených v požadavcích výběrového řízení (tj. v seznamu zařízení v současné době v používání).

1. Aktualizace parserů pro nově instalovaná zařízení do 10 pracovních dní v případě, že takový parser nebude součástí základní výbavy systému na sběr provozních událostí.
2. Kapacita až 4.000.000 (čtyřimilióny) záznamů, možnost jejich prohledávání na základě nastavených pravidel, zobrazení histogramu a TOP hodnot minimálně z osmi různých kategorií online.
3. Průměrný příjem min 5000 událostí/s. Možnost ověření v 10minutovém intervalu pomocí například generátoru událostí.
4. Špičkový příjem min 10000 událostí/s, v případě vyššího počtu událostí je systém uloží do vyrovnávací paměti a zpracuje je později.
5. Konfigurace systémů Microsoft Windows Zadavatele tak, aby posílaly logy do systému
6. Možnost instalace Windows agenta na systémy požadované Zadavatelem a jeho konfigurace, případně automatické zpracování událostí generovaných přímo operačním systémem koncového zařízení
7. Všechny aktivní prvky Zadavatele (tam, kde stávající prvky odesílání logů podporují)
8. Aplikační záznamy v míře dostatečné pro možné pozdější vyhodnocení a zpracování logů a vyhověním požadavků GDPR
9. Nutností je možnost procházení těchto záznamů vhodným grafickým nástrojem s před-definovanými pravidly pro rychlé vyhledávání (například jako jsou změny v systémech provedené administrátory, seznam nově vytvořených účtů v MS AD za zvolenou periodu, změny v přístupových právech pro zadaného uživatele nebo k zadané složce a monitoring privilegovaných účtů, sdílených účtů a změn konfigurací apod.)
10. Vytvoření a uložení vlastního dashboardu a reportu, nastavení pravidelného odesílání reportu mailem vybraným pracovníkům Zadavatele.
11. Administrační prostředí a dokumentace v českém jazyce.
12. Značkování událostí, vytvoření Alertu dle zadání, možnost vytváření tresholdů
	* 1. Z důvodu podpory zákona o kybernetické bezpečnosti a obecného nařízení o ochraně osobních údajů musí systém Poskytovatele splňovat následující funkční požadavky, případně Poskytovatel uvede odkaz na stránky výrobce daného produktu.

|  |  |
| --- | --- |
| Parametr | Popis funkčního požadavku |
| Analýza dat | systém musí disponovat možností náhledu na čistou podobu logů v plné formě, tak aby bylo možno sestavovat vlastní pohledy, které by umožnili přizpůsobení systému. |
| Vizualizace dat | systém musí být schopen snadným a rychlím způsobem zobrazit data v korelované podobě, tak aby Zadavatel mohl snadným způsobem identifikovat problémy, které nastali na úrovni sledovaných služeb |
| Upozornění na data (upozornění) | systém musí být schopen na základě sestavených dotazů vyhledat a upozornit na vzniklé situace, a to minimálně prostřednictvím emailu a zobrazit všechny události v přehledné podobě interně v systému |
| Automatické mapování prostředí | systém musí být schopen provést automatické mapování prostředí až na úroveň provázanosti procesů mezi jednotlivými monitorovanými zařízeními na úrovni TCP/IP spojení. |
| Kontrola systémů MS SQL | Výrobce databázové systému ve svých dokumentacích uvádí, jak by měl být systém nastaven s ohledem na dostupnost a bezpečnost. Systém proto musí disponovat automatickým vyhodnocením těchto nastavení, tak aby Zadavatel získal okamžitý přehled nad konfigurací databázových systémů |
| Kontrola systémů Active Directory | Výrobce Active Directory systému ve svých dokumentacích uvádí, jak by měl být systém nastaven s ohledem na dostupnost a bezpečnost. Systém proto musí disponovat automatickým vyhodnocením těchto nastavení, tak aby Zadavatel získal okamžitý přehled nad konfigurací doménových řadičů. |
| Kontrola operačních systémů Windows | Výrobce operačních systémů Windows ve svých dokumentacích uvádí, jak by měl být systém nastaven s ohledem na dostupnost a bezpečnost. Systém proto musí disponovat automatickým vyhodnocením těchto nastavení, tak aby Zadavatel získal okamžitý přehled nad konfigurací operačních systémů a mohl zajistit jejich nejlepší nastavení. |
| Kontrola přístupů do systému | Systém musí splňovat požadavek na kontrolu přístupů a zpracování bezpečnostních logů operačních systémů na platformě Windows a Linux, tak aby byl jednoduše identifikovatelný přístup zejména na protokoly Remote Desktop Services, SSH a přístup na internetové servery. |
| Kontrola poštovních služeb Microsoft Exchange | Systém musí být schopen sledovat dostupnost poštovních systémů Exchange, sledovat stavy služeb systému a chybové logy systému. Systém musí být schopen provést kontrolu databází a konfigurace systému a dále pak zobrazit stavy poslední zálohy dané databáze v jednotném a uceleném pohledu. |
| Kontrola lokálních úložišť certifikátů | Systém musí být schopen automaticky sledovat a hlídat lokální úložiště certifikátů serverů, tak aby Zadavatele upozornil v případě, že se blíží doba expirace certifikátu. |
| Kontrola certifikátů internetových serverů a sledování výkonu webových serverů bez nutnosti instalace agenta na server | Systém musí disponovat možností sledování libovolné internetové stránky pomocí URL adresy využívající protokol HTTP nebo HTTPS. S ohledem na výkon musí být systém schopen měřit v čase, jak dlouho trvá načtení internetové stránky, jak dlouho trvá překlad na úrovni veřejných DNS a tuto statistiku zobrazit v přehledových grafech. Pokud je dostupná adresa na protokolu HTTPS, pak je požadováno provedení analýzy certifikátu, který je v dané internetové stránce umístěn a je zobrazena doba expirace certifikátu a jméno certifikátu, případně i vydavatel. |
| Inventarizace software a hardware | Systém musí být schopen provést kontrolu nainstalovaných aplikací, přiřazených výpočetních prostředků, a to minimálně na platformě Microsoft Windows. Systém musí být schopen zobrazit informace o nainstalovaných rolích a funkcích Windows serverů, aby bylo možno předcházet zranitelnostem jako například ransomware. |
| Kontrola lokálních uživatelů a skupin v rámci Windows Server | Systém musí být schopen zobrazit všechny lokální uživatele a skupiny, které jsou nastaveny na lokálních serverech Microsoft Windows Zadavatele, včetně zobrazení změn členství ve skupinách. |

* + 1. Dodávaný produkt nebo služba musí splňovat níže uvedené nefunkční požadavky zejména z důvodu udržitelnosti a zajištění stability prostředí

|  |  |
| --- | --- |
| Parametr | Minimální přípustná hodnota |
| Výkon | Systém musí být schopen odbavit požadavky nejméně 60 paralelně běžících systémů, které odesílají jak informace z logů systému nebo z výkonových monitorů systému. Systém musí být schopen zpracovávat logy ze síťového provozu síťových adaptérů serverů. |
| Doba odezvy | Systém musí být schopen zobrazit informace, které do sebe stáhl nejpozději do 10 minut od odeslání do systému. |
| Škálovatelnost | Systém musí splňovat požadavky na automatické vertikální a horizontální škálování výkonu bez zásahu uživatele (správce aplikace nebo služby). |
| Dostupnost | Zadavatel požaduje garanci služby minimálně na úrovni 99,9 %, jelikož se jedná o klíčový bezpečnostní prvek infrastruktury, který bude obsahovat velmi citlivá data s ohledem na bezpečnost infrastruktury Zadavatele. |
| Rozšiřitelnost a modifikovatelnost | Cena za provoz aplikace nebo služby nesmí být podmíněna cenou výkonu dané služby nebo aplikace, Zadavatel požaduje, aby cena byla účtována maximálně na monitorované zařízení, případně za navýšení datového prostoru, který budou logy služby využívat, případně za předpokladu, že bude nutné zajistit uložení logů delší než 1 měsíc od jeho záznamu v systému. |
| Zpracovatelnost | Systém musí být snadno spravovatelný a nezávislý na operačním systému. Zadavatel požaduje minimálně sledování operačních systému Windows a Linux, včetně možnosti připojení stávajícího monitorovacího řešení například Zabbix nebo Nagios. Případně napojení fyzických zařízení skrze prostředníka, kterým může být například syslog server. |
| Bezpečnost | Data umístěná v aplikaci musí být zabezpečena na maximální možné úrovni, nesmí být umístěna v produkční infrastruktuře Zadavatele a nesmí být modifikovatelná při přenosu nebo při uložení. Dalším požadavkem na bezpečnost je nemožnost provedení vymazání informací správcem aplikace ani dodavatelem aplikace. |
| Přístupy | Systém musí disponovat alespoň třemi rolemi přístup, a to plný přístup, přístup pro zápis a přístup pro čtení. |
| Licence | Aplikaci musí být možné nainstalovat i na zařízení, která nejsou ve vlastnictví Zadavatele a nesmí dojít k rozporu s licenční politikou výrobce nebo dodavatele. |
| Konzole pro správu prostředí | Zadavatel požaduje, aby systém byl přístupný skrze webové rozhraní, které bude zabezpečeno. Dalším vhodnou metodou pro správu prostředí je dostupnost mobilní aplikace pro platformy minimálně Android a iOS. |
| Integrace | Zadavatel požaduje, aby systém disponoval možností integrace se systémy třetích stran, a to zejména s otevřenými platformami Linux (Nagios, Zabbix) |
| Doporučení | Zadavatel požaduje, aby systém disponoval doporučeními k zajištění rychlého řešení případných problémů v jeho prostředí. Doporučení dodá osoba (konzultant) dodavatele, tak aby bylo možné zahájit přiměřeně rychlou reakci, na straně zákazníka, k nápravě chyb nebo ošetření zranitelností a hrozeb systému. |

* 1. Služby expertního centra
		1. V rámci pravidelně poskytovaných služeb zajistí Poskytovatel pravidelné sledování bezpečnostních hrozeb a tento report posílat minimálně v týdenní periodě vybranému pracovníkovi Zadavatele.
		2. Tato služba musí umožňovat minimálně následující:
1. Obsah bude připravován tak, aby byl srozumitelný bezpečnostním manažerům i správcům konkrétních aktiv, a aby mohl sloužit jako podklad pro kvalifikované rozhodnutí, zda je nutné a vhodné hrozbu řešit. Pokud se zástupce Objednatele rozhodne hrozbu řešit, musí report obsahovat informace pro administrátory, kterým informace poskytne jako přímočarý návod pro eliminaci hrozby. Report musí být připraven v českém jazyce (kromě nezbytných částí, kde je možno či nutno použít jazyk jiný – například název zranitelnosti či odkaz na externí stránky výrobce atd.).
2. Všechny takto publikované hrozby budou i zpětně k dispozici Objednateli tak, aby si je mohl filtrovat a procházet dle vlastního uvážení a potřeb.
3. Report relevantních hrozeb by měl být rozdělen minimálně na kategorie zranitelnost, ransomware, malware, phishing, případně další dle uvážení Uchazeče či potřeb Objednatele.
4. Report, respektive takto připravené sledování hrozeb, musí být dostupné online, ideálně formou webové stránky, či aplikace pro mobilní zařízení (iOS, Android).
	1. Uvedení infrastruktury do souladu s nařízením GDPR o ochraně a nakládání s osobními údaji
		1. Migrací na nové prostředí (ať již nových koncových zařízení nebo pouze v rámci migrace na prostředí Microsoft Office 365) dojde k čištění lokálně uložených dat s ohledem na nařízení GDPR. Tento proces nebude brán jako finální stav zajišťující soulad s uvedeným nařízením (nelze zaručit ukončení projektu GDPR před implementací tohoto projektu), nicméně každý uživatel bude seznámen s informacemi, které nelze na lokálním disku uchovávat a jakým způsobem s takto nalezenými daty má zacházet – a to buď na základě interní směrnice, nebo na základě doporučení ze strany dodavatele. Konzultační činnosti
	2. Konzultační činnosti v oblasti bezpečnosti

Jedná se o zajištění konzultačních činností v oblasti informační bezpečnosti.

* 1. Ostatní služby v oblasti bezpečnosti

Poskytovatel zajistí následující služby v rozsahu minimálně jednou ročně:

1. DLP scan vybraných úložišť Objednatele s detailním reportem výstupu a s možností definice vstupních hodnot, pro které DLP scan bude prováděn
2. Vulnerability scan celé infrastruktury Objednatele s detailním reportem, který bude obsahovat i návrhy řešení případně nalezených hrozeb v infrastruktuře Zadavatele.

Poskytovatel doplní nástroje, které bude pro tyto činnosti používat (a které specifikoval ve své předložené nabídce).

* Rapid7
* TrendMicro
1. Podpora koncových uživatelů

V rámci této části Poskytovatel zajistí dále specifikované činnosti. Poskytovatel může dále specifikované služby vykonávat i definovaným vzdáleným způsobem (pomocí nástroje Objednatele), přičemž je požadováno následující:

1. Minimálně jeden pracovník Poskytovatele vykonává činnosti minimálně podpory koncových uživatelů v sídle Objednatele, a to v režimu 5x4.
2. Vzdálená správa bude realizována za využití nástroje Objednatele. Předpokládá se využití TeamVieweru nebo obdobného nástroje v aktuální verzi, nástroj bude pořizován samostatně.
	1. Školení koncových uživatelů na produkty implementovaných cloudových služeb Microsoft Office 365 E3

Poskytovatel zrealizuje vybrané školení koncových uživatelů na používání vybraných technologií, způsobů práce s technologiemi v prostředí Objednatele a taktéž pravidelných školení v oblasti bezpečnosti. Školení budou určena pro všechny pracovníky Objednatele, a to včetně zahraničních zastoupení. Školení bude prováděno minimálně ve čtvrtletním intervalu.

Výstupem bude vždy minimálně seznam proškolených uživatelů a elektronická forma použitých výukových materiálů (pokud budou pro vlastní školení použity a budou předatelné standardním způsobem).

* 1. Zajištění podpory uživatelů
		1. Poskytovatel zajistí jednotné kontaktní místo pro uživatelskou podporu včetně dostupnosti pro zahraniční zastoupení agentury. Součástí podpory bude definovaná dostupnost pracovníků Poskytovatele v prostorách Objednatele. Objednatel specifikuje požadavky na dostupnost takové podpory následujícím způsobem:
1. Možnost zadávat požadavky v režimu 7x24
2. Definovaná doba odezvy během pracovních dní v rozsahu 5x10 maximálně 30 minut
3. Doba vyřešení problému pro kritické uživatele je v rozsahu 5x10 stanovena na 2 hodiny
4. Doba vyřešení problému pro ostatní uživatele je v rozsahu 5x10 stanovena na 6 hodin
5. Mimo pracovní dobu a během státních svátků a víkendů může být vyžadována stejná podpora, pokud bude nahlášena 2 pracovní dny před takto definovanou potřebou podpory.
6. Ostatní požadavky v rámci podpory uživatelů budou řešeny nejpozději následující pracovní den.
7. Schopnost předávat uživatelské požadavky třetím stranám, je myšleno předávání požadavků ostatním subdodavatelům Zadavatele.
	* 1. Požadavky na jednotné kontaktní místo:
* Založené na standardech ITIL
1. ITIL Incident Management. Nástroj musí pokrýt celý životní cyklus incidentu od nahlášení události a založení tiketu přes kategorizaci, automatické přidělení, předdefinovanou nebo dynamickou prioritizaci, diagnostiku a eskalaci incidentu, jeho vyřešení, nápravu a uzavření, až po zpětnou vazbu od zákazníka/uživatele.
2. ITIL Problem Management. Nástroj musí umožňovat analýzu původní příčiny všech opakujících se incidentů a minimalizace dopadu problému na organizaci. Pro vyřešení takových událostí je třeba mít k dispozici řadu reaktivních i proaktivních nástrojů, které umožní ve stejném čase řešení probíhajících incidentů i předejití pravděpodobným nechtěným událostem v budoucnu.
3. Change Management. Důvodem využívání změnového řízení je zajištění požadavku na dokončení změny s minimálním rizikem či negativním dopadem na ostatní procesy. Je nutno mít možnost nastavit v rámci nástroje procesy tak, aby průběh změny zdárně prošel všemi fázemi svého životního cyklu (tj. není dostačující pouze změnu začít a schválit její provedení manažerem a tím považovat za vypořádanou). Minimálně je nutno podporovat funkce typu např. typy změn, kolegium/management pro řízení změny, role, milníky, šablony, status změny, workflow.
4. Service Catalog. Možnost vytvářet a dále spravovat jednotlivé poskytované služby a jejich provázanost s ostatními službami nástroje. Katalog služeb musí umožnit strukturovat procesy do formalizovaných forem, aby byly plně v souladu s požadavky ITIL.
5. Integrace s řešením na řízení aktiv, které je možno aktualizovat automaticky a online.
6. ITIL CMDB. Nástroj musí obsahovat centrální úložiště konfiguračních dat (Configuration Items) obsahující relevantní informace o všech důležitých prvcích či pro organizaci kritických IT konfiguračních datech/záznamech a jejich vzájemných vazbách. Tato funkcionalita může být řešena samostatným modulem.
7. Řízení nákupu. Nástroj musí umožnit doplnit funkcionalitu, která bude obsluhovat kompletní katalog produktů dle jejich typů, evidovat dodavatele a ceny, optimálně vytvářet objednávky a automaticky zařazovat nově pořízená aktiva do katalogu, automaticky vyplňovat políčka objednávek, sledovat průběh objednávání, vyhledávat v objednávkách, analyzovat trendy (např. pro vyjednávání lepších podmínek u dodavatelů).
8. Správa smluv. Nástroj musí umožnit snadné monitorování smluv, které mohou mít mnoho podob dle jejich účelu (podpora, údržba, pronájem atd.). v rámci toho musí být možno poskytovat přehled nad smlouvami se třetími stranami, zaznamenávat specifické atributy kontraktů a oznamovat jejich vypršení spolu s dalšími rozšířenými funkcemi, jako je např. řízení dodatků smluv či vazeb na konkrétní aktiva.
9. Reporty. Nástroj musí umožnit modifikace reportů dle vlastních potřeb včetně nastavení periodicity, zasílání přes email v pdf, xls, csv a html formátu. Mezi základní typy reportů patří např. Všechny požadavky, Narušení SLA, Všechny problémy, Problémy aktuálně řešené, Všechny změny, Změny aktuálně řešené, Zpětné vazby od uživatelů, auditní reporty atd. Všechny reporty mohou být kategorizovány dle lokality, úrovně, módu, priority, požadavku, technika, který je řešil atd.
10. Tento systém musí umožnit komunikaci s třetími stranami, tj. s dalšími dodavateli Zadavatele, a to jednoznačným způsobem tak, aby nemohlo dojít k rozporu ohledně parametrů služby předávaného požadavku.
11. Zajištění možnosti vazby na měsíční vyúčtování a automatického reportingu.
12. Ostatní požadované služby

Poskytovatel zajistí:

1. Jednorázové konzultace pro potřeby rozvoje IT technologií, jejich obměny a celkového směrování IT podpory. Součástí těchto hodin bude i koordinace s dalšími IT dodavateli Zadavatele. Časová náročnost je 16 hodin měsíčně.
2. Podpora na akcích pořádaných Objednatelem. Objednatel pro své aktivity často používá externích služeb a prostředí, přičemž i pro takové akce je nutno zajistit IT podporu. Kromě vzdálené podpory, která je definována výše jako standardní podpora uživatelů a služeb, je nutno nabídnout technického pracovníka, který bude schopen podporovat vybranou akci či skupinu uživatelů Objednatele kdekoli v rámci ČR. Časová náročnost je požadována v rozsahu maximálně 20 člověkodní za kalendářní rok.