Příloha č. 6 zadávací dokumentace

Technické specifikace – podrobné znění

V rámci podpory provozu WAN ČOI se požaduje poskytování služeb v oblasti správy provozovaného HW, správy provozovaného SW, provozu SOC ČOI, konzultací a školení. Seznam níže vymezeného HW a SW může být měněn podle aktuální situace ve smyslu vyřazení „starého“ či zařazení „nového“.

1. Rozsah provozovaného HW ČOI

A) Rozsah provozovaného HW ČOI v rámci datového centra lokality Praha

a) HPE serverový cluster:
   i) 3 x fyzický server HPE DL360 Gen11,
   ii) diskové pole HPE Alletra,
   iii) síťová infrastruktura.
b) Dell VRTX Chassis, 3 x fyzický server,
c) Server DELL - monitorovací systém Zabbix,
d) Server DELL - LOGmanager,
e) Zálohovací knihovna HPE MLS 3040,
f) Zálohovací technologie HPE StoreOnce,
g) Server Backup HPE DL 360 Gen10,
h) 2 x Fortigate firewall 500E v HA,
i) Nástroj FortiAnalyzer – fyzický HW,
j) Prvky bezdrátové sítě Fortinet AP – počet AP 20ks,
k) UPS APC od 1,5 kVA do 7,5 kVA,
l) Autentizační (bezpečnostní) tokeny, poskytovatel Česká pošta, a.s.

B) Rozsah provozovaného HW ČOI v rámci lokalit ČOI

Plzeň, Ústí nad Labem, Liberec, Hradec Králové, České Budějovice, Brno, Ostrava, Olomouc

Serverový HW na každé lokalitě (mimo Prahy)

- Fyzický server DELL, Virtualizace OS Win 2019, 2 x virtuální servery v roli DHCP, Radius, NPS a druhý v roli fileserver,
- Fortigate Firewall 60E,
- Aktivní síťové prvky Fortinet.

Klientský HW na pobočkách (cca 500 zařízení ve všech lokalitách včetně Prahy)

- Notebooky HP, Dell, Lenovo,
- Tisková multifunkční zařízení.

2. Rozsah „systémového“ provozovaného SW

a) MS Windows server 2012 R2, 2016, 2019, 2022 služby zejména v oblasti:
   i) Group Policy Object,
   ii) virtualizace využitím Hyper-V (v současnosti 3 nody, cca 72 virt. serverů),
   iii) Active Directory,
   iv) DNS, DHCP, NPS, WSUS služby.
b) MS Exchange 2019 včetně Hybridního prostředí s MS O365,
c) MS SharePoint 2016, Intranetový portál organizace,
d) MS SQL databáze: 2014, 2017, 2019, 2022 (Standard, Express),
e) MS Windows 10, Office 2021 LTSC,
f) SCOM, SCCM, SCVMM z rodiny produktů Microsoft Systém Center,
g) Veeam Backup Essential a Veeam Backup for Microsoft 365

3. Rozsah „nesystémového“ provozovaného SW

a) Agendový, kontrolní IS Mercurius, dodavatel firma INISOFT, s.r.o.,

b) Personální IS Okbase, dodavatel firma OKsystem, a.s.,
c) Spisová služba GINIS®, dodavatel firma Gordic, s.r.o.,
d) Ekonomický IS JASU® CS, dodavatel firma MÚZO Praha, s.r.o.,
e) Právní IS ASPI, dodavatel Wolters Kluwer ČR, a.s.
f) Kartové centrum IS, dodavatel MONET+, a.s.

4. Rozsah bezpečnostního provozovaného SW

a) IS pro správu SW, HW – AuditPro,
b) IS pro správu nestrukturovaných informací Varonis,
c) IS pro detekci nepovoleného SW Carbon Black,
d) Správa identit MidPoint,
e) SW produkty (FortiManager, FortiAnalyzer),
f) IS pro monitoring provozu System Center Operations Manager,
g) LOGmanager,
h) Zabbix.

5. Požadavky na provoz bezpečnostního dohledového centra (SOC) ČOI

V prostředí ČOI jsou implementovány nástroje pro zajištění sběru a vyhodnocení provozu infrastruktury zejména LOGmanager, FortiAnalyzer, Varonis, Zabbix a další. Objednatel požaduje poskytnutí dohledových a expertních bezpečnostních služeb v souvislosti s provozem SOC pro infrastrukturu Objednatele. Jedná se o infrastrukturu datového centra a centrální síťové infrastruktury, serverové a síťové infrastruktury regionálních pracovišť, provozovaných informačních systémů a služeb. SOC provádí kontinuální provozní monitoring a detekci potenciálního kybernetického bezpečnostního incidentu 24x7x365.

Konkrétní požadavky na SOC

a) provoz dohledového centra 24x7x365, nonstop telefonická hotline obsluhovaná operátorem,
b) proaktivní podpora provozu systémů a infrastruktury ČOI operátorem dohledového centra od 6h do 21h , 365 dní v roce , zajištění reakce a eskalace dle eskalačních postupů,
c) návrhy opatření k předcházení incidentů narušujících bezpečnost,
d) řešení bezpečnostních incidentů a událostí,
e) poskytování součinnosti regulační autoritě (NÚKIB) k posouzení úrovně bezpečnosti,
f) export dat, provozních údajů (auditní stopa) spojených s provozem IS Mercurius, Okbase, EIS, GINIS dle vyžádání Objednatele,
g) monitorování pokusů o průnik v rámci střeženého perimetru a ochrana proti nim,
h) přímý zásah k omezení dopadů incidentu a koordinační činnost v rámci ČOI,
i) realizace procesu zvládání a ponaučení se (zvyšování bezpečnostního povědomí) z bezpečnostních incidentů,
j) realizace zajištění kontinuity činností ČOI při krizových situacích,
k) zajištění souladu opatření (interní směrnice a nařízení ČOI) se související legislativou týkají se ochrany informací,
l) zpracování logů o událostech z provozovaného HW a SW na síti,
m) zpracování, korelace a vyhodnocení logů a flows v reálném čase,
n) vyhodnocení detekce hrozeb APT a “Zero-Day“ útoků, včetně behaviorální analýzy,
o) monitorování chování v síti,
p) identifikace a kategorizace zranitelností,
q) informace o nalezené zranitelnosti, popis hrozby při jejím potenciálním zneužití a případné návrhy řešení, jak zranitelnost odstranit,
r) vyhodnocování nalezených zranitelností a jejich prioritizace, eskalace,
s) realizace změnových požadavků v rámci provozovaných monitorovacích systémů,
t) týdenní provozní reporting.

6. Konzultace a školení

Konzultace a školení budou poskytovány Dodavatelem v rozsahu technologií zahrnující služby dle kap. 1-2, 4-5. Budou objednány emailem na adresu Dodavatele.

7. Forma poskytované služby

Požadované služby budou poskytovány prostřednictvím měsíčního paušálu nebo formou objednání konkrétní „Ad-hoc“ služby takto:

Paušální služby zahrnují:

a. instalace, konfigurace, aktualizace a kontrola provozovaného HW dle bodu 1,
b. instalace, konfigurace, aktualizace a kontrola provozovaného SW dle bodu 2-4,
c. zajištění provozu dohledového centra 24x7x365 dle bodu 5,
d. konfigurace centrálních politik (GPO, SCCM),
e. kontrola funkce systému zálohování.

Ad-hoc služby:

a. Expertní práce v oblasti serverové infrastruktury Objednatele,
b. Expertní práce v oblasti síťové infrastruktury Objednatele,
c. FAZ – reporty: modifikace stávajících, vytváření nových,
d. LOG – use case: modifikace stávajících, vytváření nových,
e. BI – reporty: modifikace stávajících, vytváření nových,
f. EA – modely ČOI: úprava stávajících, vytváření nových,
g. Testování DR a řešení obnovy prostředí po havárii,
h. Migrace dat dle požadavků,
i. Interní, externí penetrační testy,
j. O365: migrační a rozvojové služby v dané oblasti,
k. Odborná školení, konzultace dle bodu 6.

Pozn: BI – bussines inteligence, DC – datové centrum, EA – Enterprise Architektura (jazyk ArchiMate), FAZ – FortiAnalyzer, LOG – LOGmanager, ÚI – ústřední inspektorát, SOC – dohledové centrum.

„Ad-hoc“ služby budou předem objednávány e-mailem nebo prostřednictvím helpdesku zástupcem Objednatele, kterým je vedoucí Oddělení digitalizace a informatiky [redacted] nebo jeho zástupce [redacted]. Tito zástupci Objednatele jsou jedinými oprávněnými osobami k odsouhlasení výkazu práce.

8. Klasifikace havarijních stavů

Havarijními stavy rozumíme jakoukoliv nefunkčnost, bezpečnostní incident či událost. Rozlišujeme 4 kategorie havarijních stavů:

Havarijní stav: kategorie A
Kybernetický incident/událost dle zákona 181/2014 Sb. Prvek IT/služba není použitelná ve svých základních funkcích nebo se vyskytuje funkční závada znemožňující používání služby. Tento stav může ohrozit běžný provoz, případně může způsobit větší finanční nebo jiné škody.
Havarijní stav: kategorie B
Prvek IT/služba je ve svých funkcích degradována tak, že tento stav omezuje běžný provoz.
Havarijní stav: kategorie C
Ostatní incidenty/vady které nespadají do kategorií A a/nebo B a které nejsou způsobeny software třetích stran.
Havarijní stav: kategorie D
Incidenty/vady, které jsou způsobeny software třetích stran.

Pozn: Havarijní stavy způsobené „3. mocí“ tzn. totální zničení DC (požár, zemětřesení, výbuch, voda) nejsou řešeny touto smlouvou.

9. Parametry SLA

Kategorie h. stavů	Potvrzení převzetí požadavku	Garantovaná doba zahájení prací	Garantovaná doba vyřešení po řádném nahlášení
A	do 1 hod.	2 hod.	Nejpozději do 24 hod.
B	do 1 hod.	4 hod.	Následující pracovní den
C	do 1 hod.	Následující pracovní den	Do 5 pracovních dnů
D	do 1 hod.	Následující pracovní den	BE (Best Effort) dle možností v co nejkratší době

Do doby vyřešení incidentu se nezapočítává:

a) čekání Dodavatele na vyžádanou součinnost Objednatele,
b) prodlevy způsobené závadami na zařízeních mimo rozsah systémů, na nichž Dodavatel drží podporu,
c) prodleva způsobená zásahem vyšší moci.

10. Sankce za nedodržení podmínek SLA

U havarijních stavů je Objednatel oprávněn uplatnit vůči Dodavateli sankci za nedodržení parametrů SLA dle následující tabulky:

Kategorie incidentu	Výše sankce
A	15 000,- Kč
B	10 000,- Kč
C	5 000,- Kč
D	1 000,- Kč

11. Způsob zadávání požadavků (havarijní stavy, požadavek na Ad-hoc služby)

Objednatel může kontaktovat Dodavatele minimálně tímto způsobem:

- prostřednictvím formuláře v aplikaci Helpdesk Dodavatele dostupný 24x7x365,
- telefonem na hotline Dodavatele dostupný 24x7x365,
- e-mailem na Dodavatele dostupný 24x7x365,
- osobně při návštěvě v místě Dodavatele.

12. Poskytování služeb helpdesku a hotline Dodavatelem

a) helpdesk

- webová aplikace provozovaná Dodavatelem s vysokou dostupností,
- každý tiket a jakákoliv změna musí být evidována včetně času a původce,
- schvalovací řízení je součástí aplikace,
- tikety jsou automaticky distribuovány na jednotlivé řešitele Dodavatele,
- počet uživatelů, řešitelů a schvalovatelů není omezen,
- aplikace má schopnost reportingu tiketů dále elektronicky zpracovatelných (MS Excel).

b) hotline

- hotline musí být provozována z České republiky s česky mluvícími operátory,
- hotline poskytuje na vyžádání informaci o průběhu řešení tiketu.