Příloha č. 5 Smlouvy o dodávce a implementaci informačních a komunikačních technologií

Podmínky Služeb podpory a Služeb rozvoje

Obsah

Popis SLA, charakteristika 2
1. Definice pojmů (Legenda SLA) 2
2. Definice reakční doby 4
3. Upřesnění oznamovacích kanálů 4
4. Doba vyřešení incidentu 5
Co znamená "vyřešený incident"? 5
5. Pozastavení SLA 6
6. Požadovaná součinnost Objednatele 7
7. Co se nepočítá do SLA 8
8. Potvrzení vyřešení 8
9. Dokumentace vyřešení 9
10. Měření dodržování SLA 9
11. Eskalační matice 9
12. CMDB / Change Management 9
13. Zřetězení událostí SLA, Root Cause Based SLA 10
Služby implementace systému správy identit (IDM) – SLA 11
1. Definice incidentů dle obecného charakteru a zvyklostí služby IDM 11
2. Smluvní pokuty 13
Služby zajištění kybernetické bezpečnosti za pomoci dohledového centra SOC – SLA 14
1. Definice incidentů dle obecného charakteru a zvyklostí při zajištění kybernetické bezpečnosti za pomoci dohledového centra 16
2. Klasifikace řešených incidentů 16
3. Kapacita řešení incidentů 17
4. Typ řešení incidentů a typ výstupů při šetření incidentů 18
5. Reporting a komunikace 18
6. Rozvojové práce 19
7. Technická podpora 19

8. Smluvní pokuty 19
Služby zálohování a archivace ICT dat – SLA 21
1. Definice incidentů dle obecného charakteru a zvyklostí při zajištění služby zálohování a archivace ICT dat 21
2. Smluvní pokuty 22
Služby virtualizace a serverové infrastruktury – SLA 24
1. Definice incidentů dle obecného charakteru a zvyklostí při zajištění služby virtualizace a serverové infrastruktury 24
2. Smluvní pokuty 25
Služby návrhu a implementace WiFi datové sítě – SLA 26
1. Definice incidentů dle obecného charakteru a zvyklostí při zajištění WiFi sítě ARENA BRNO 26
2. Smluvní pokuty 29
Provozní datová síť ARENA BRNO – SLA 30
1. Definice incidentů dle obecného charakteru a zvyklostí při zajištění provozně datové sítě ARENA BRNO 30
2. Smluvní pokuty 31

Popis SLA, charakteristika

1. Definice pojmů (Legenda SLA)

1. **Pracovní den** – kalendářní den pondělí až pátek s výjimkou státních svátků České republiky podle platných právních předpisů.
2. **Pracovní hodina** – časový úsek mezi 8:00 a 17:00 hodinou středoevropského času (CET/CEST) v pracovním dni.
3. **Pracovní kalendář SLA** – režim dostupnosti podpory definovaný pro konkrétní službu, a to buď:
    - 24×7×365 – nepřetržitě bez omezení, nebo
    - 8×5 – pracovní dny 8:00–17:00.
    - Konkrétní režim je vždy uveden u dané služby.
4. **Režim 8×5 (běh SLA lhůt)** – u služeb poskytovaných v režimu 8×5 běží SLA lhůty pouze v pracovních dnech mezi 8:00–17:00 (CET/CEST). Incidenty nahlášené mimo tuto dobu jsou evidovány okamžitě, ale SLA lhůty začínají běžet až od 8:00 následujícího pracovního

dne. Pokud je incident nahlášen během pracovní doby, běh SLA se v 17:00 pozastavuje a pokračuje od 8:00 následujícího pracovního dne.

5. **Lhůta v pracovních dnech** – lhůta, která začíná běžet první pracovní den následující po vzniku rozhodné události a končí uplynutím posledního pracovního dne lhůty v 17:00.
6. **Incident** – neplánovaná událost způsobující nebo hrozící způsobit nedostupnost, degradaci výkonu, omezení funkčnosti nebo narušení bezpečnosti dodaných služeb nebo systémů.
7. **Bezpečnostní incident** – incident související s porušením nebo ohrožením důvěrnosti, integrity nebo dostupnosti dat či systémů, včetně podezření na kybernetický útok.
8. **Degradace služby** – stav, kdy je služba dostupná, avšak její výkon, stabilita nebo funkčnost jsou sníženy oproti běžnému provozu (např. zvýšená latence, snížená propustnost nebo omezená funkcionalita).
9. **Prodloužení pracnosti o více než 50 %** – stav, kdy běžné úkony obsluhy v systému (např. IDM nebo administrační nástroje) trvají oproti standardnímu provozu alespoň o polovinu déle nebo je obsluha vnímá jako výrazně zpomalené; posuzuje se podle reálné zkušenosti obsluhy nebo dostupného monitoringu.
10. **Nahlášení incidentu** – okamžik, kdy je incident oznámen prostřednictvím některého z kanálů definovaných v sekci 3 této přílohy. Od tohoto okamžiku začínají běžet SLA lhůty, pokud není SLA pozastaveno dle sekce 5.
11. **Reakční doba** – lhůta začínající okamžikem nahlášení incidentu Zhotoviteli, během níž je Zhotovitel povinen:
    - potvrdit převzetí incidentu lidským řešitelem,
    - přiřadit incident konkrétní odpovědné osobě nebo týmu,
    - zahájit řešení,
    - Za splnění reakční doby se nepovažuje pouze automatické potvrzení ticketem.
12. **Doba vyřešení incidentu** – lhůta od okamžiku nahlášení incidentu do okamžiku splnění podmínek „vyřešeného incidentu“ dle sekce 4 této přílohy.
13. **Vyřešený incident** – incident, u kterého došlo k plnému obnovení funkčnosti, schválenému alternativnímu řešení nebo k poskytnutí workaroundu v souladu s pravidly této přílohy.
14. **Workaround** – dočasné řešení umožňující pokračování provozu při přetrvávající závadě. Workaround nenahrazuje trvalé odstranění příčiny; trvalé řešení musí být evidováno samostatně.
15. **Pozastavení SLA** – dočasné přerušení běhu SLA lhůt z důvodů definovaných v sekci 5. Pozastavená doba se nezapočítává do reakční doby ani doby vyřešení. Zhotovitel je povinen pozastavení bezodkladně zaznamenat do ticketu včetně důvodu a času zahájení.

16. **Překlasifikace priority** – změna priority incidentu během jeho řešení na základě skutečného dopadu na provoz. Překlasifikace vyžaduje předchozí souhlas Objednatele.
17. **Priorita incidentu** – klasifikace závažnosti incidentu (např. CRITICAL, HIGH, MEDIUM, LOW) určující cílové SLA parametry reakce a řešení.
18. **Dostupnost služby (Availability)** – schopnost služby plnit definovanou funkci v produkčním prostředí. Služba je považována za nedostupnou, pokud není možné využívat její hlavní funkcionalitu nebo pokud selže monitorovací kontrola definovaná pro danou službu. Běh SLA lhůt může být v takovém případě pozastaven postupem dle sekce 5.
19. **Plánovaná odstávka** – předem oznámené a Objednatelem schválené přerušení služby za účelem údržby nebo změn, které se nezapočítává do dostupnosti ani do SLA lhůt.
20. **Ticketový systém** – nástroj pro evidenci incidentů a požadavků, který představuje závazný zdroj informací o časech, komunikaci a průběhu řešení.
21. **Eskalace** – postup předání řešení incidentu na vyšší úroveň řízení nebo odbornosti v případě překročení časových limitů, zvýšení dopadu nebo potřeby rozhodnutí.
22. **Root Cause (příčina incidentu)** – identifikovaný technický nebo procesní důvod vzniku incidentu určený na základě analýzy.
23. **Zřetězení událostí SLA (Root Cause Based SLA)** – princip, podle kterého se při výpadku nebo degradaci služby způsobené jinou vrstvou infrastruktury uplatní SLA té vrstvy, která je příčinou incidentu. Do doby určení příčiny se incident řídí nejpřísnější relevantní SLA; po identifikaci může být SLA upraveno se souhlasem Objednatele.
24. **Produkční prostředí** – prostředí používané pro běžný provoz organizace, na které se vztahují SLA závazky. Testovací nebo vývojová prostředí nejsou produkčním prostředím, pokud není výslovně uvedeno jinak.

2. Definice reakční doby

Reakční lhůta/doba začínající okamžikem nahlášení incidentu, během níž je Zhotovitel povinen:

- potvrdit převzetí incidentu lidským řešitelem,
- přiřadit incident konkrétní odpovědné osobě nebo týmu,
- zahájit řešení,
- Za splnění reakční doby se nepovažuje pouze automatické potvrzení ticketem.

3. Upřesnění oznamovacích kanálů

Incident je považován za oznámený v okamžiku:

- Vytvoření ticketu v ticketovém systému Zhotovitele, dostupném 24x7x365

- V případě incidentů s prioritou CRITICAL nebo HIGH postačuje oznámení telefonicky s následným e-mailovým potvrzením. Příslušný ticket v systému vytvoří Zhotovitel.

Ticketový systém:

- URL: https://helpdesk.tech.seyfor.com
- Objednatel má přístup 24x7x365
- Automatické potvrzení přijetí e-mailem do 10 minut

4. Doba vyřešení incidentu

Čas k vyřešení se měří od okamžiku nahlášení problému Objednatelem až do momentu, kdy Zhotovitel úspěšně dokončí nápravu.

Co znamená "vyřešený incident"?

Incident je považován za vyřešený, pokud je splněna jedna z následujících podmínek:

1. Plné obnovení funkčnosti (preferovaná metoda)

- Systém je vrácen do stabilního a plně provozuschopného stavu
- Funkčnost odpovídá stavu před vznikem problému
- Není třeba žádných workaroundů nebo náhradních řešení

2. Alternativní řešení

- Poskytnut funkční ekvivalent původní funkcionality
- Řešení je technicky proveditelné a akceptovatelné pro Objednatele
- Objednatel musí s alternativním řešením výslovně souhlasit

3. Dočasné řešení (workaround)

- Poskytnut postup, jak obejít problém a pokračovat v práci, s návrhem a odsouhlaseným termínem vyřešení
- Používá se, pokud trvalé řešení vyžaduje delší čas (např. update, patch od výrobce)
- Trvalé řešení musí být implementováno v samostatném ticketu s dohodnutým termínem

4. Překlasifikace priority

Priorita incidentu může být během řešení změněna na základě skutečného dopadu na provoz.

Ke změně priority dochází v těchto případech:

- Po provedení analýzy je zjištěno, že skutečný dopad je nižší, než byl původně odhadnut
- Během řešení se změní okolnosti ovlivňující dopad na provoz
- Zjistí se, že incident vyžaduje řešení v rámci rozvojových prací, nikoli jako provozní incident

Podmínky překlasifikace:

- Překlasifikace vyžaduje předchozí souhlas Objednatele
- Incident pokračuje v řešení s novou prioritou a odpovídajícím SLA

V případě překvalifikace na rozvojové práce:

- Zhotovitel navrhne zařazení do rozvojových prací
- Objednatel musí překlasifikaci na rozvojové práce odsouhlasit
- Zhotovitel předloží rozsah prací včetně ocenění dle ceníkové tabulky rolí
- Po odsouhlasení Objednatelem jsou práce realizovány v režimu rozvoje

5. Pozastavení SLA

SLA se pozastavuje v následujících případech, kde čas pozastavení se nezapočítává do reakční doby ani doby vyřešení:

1. Čekání na poskytnutí informací, přístupů, součinnost nebo souhlas ze strany Objednatele, kde obnovení SLA nastává okamžitě po poskytnutí požadované součinnosti
2. Dobu mimo pracovní kalendář SLA (u režimu 8×5)
3. Během doby, kdy je nezbytná součinnost výrobce dotčené technologie
4. **Cloudové technologie**
    a. Pozastavení SLA je akceptováno pouze při splnění všech následujících podmínek:
        i. Jde o výpadek infrastruktury třetí strany (AWS, Azure, Google Cloud, M365 apod.) mimo kontrolu Zhotovitele
        ii. Zhotovitel dodržel SLA poskytovatele cloudu (odpovídající service tier, replikace, zálohy)
        iii. Zhotovitel prokazatelně doloží informaci o výpadku třetí strany
    b. Pozastavení SLA neplatí, pokud:

i. Zhotovitel nedodržel SLA cloudu nebo nezajistil dostatečnou replikaci

5. **Hardwarové závady**
    a. Závada není způsobena chybným nastavením, konfigurací nebo instalací ze strany Zhotovitele
    b. Zhotovitel má aktivní HW podporu s garantovanou dobou dodání náhradních dílů
    c. Během doby potřebné k obnovení funkčnosti HW v případě závady HW
    d. Zhotovitel předloží, že problém s HW byl prokazatelně předán výrobci.
6. **Výpadek internetového připojení**
    a. Pozastavení SLA je akceptováno pouze při splnění všech následujících podmínek:
        i. Jde o výpadek na straně ISP mimo kontrolu Zhotovitele
        ii. Výpadek není způsoben chybnou konfigurací síťových zařízení, firewallu nebo routingu ze strany Zhotovitele
        iii. Zhotovitel musí Objednatele informovat o výpadku internetového připojení na základě aktivního monitoringu provozní datové sítě a WiFi sítě ARENY BRNO
7. **Nedostupnost vzdáleného přístupu**
    a. Objednatel neposkytl potřebné přístupy (VPN, firewall pravidla, účty) po předchozí písemné žádosti Zhotovitele
    b. Nedostupnost není způsobena chybnou konfigurací VPN, firewallu nebo bezpečnostních pravidel ze strany Zhotovitele

Základní zásada
SLA se pozastavuje pouze u závad a situací mimo kontrolu a odpovědnost Zhotovitele. Pokud je příčinou incidentu chyba v implementaci, konfiguraci, návrhu nebo nedostatečné zajištění podpory ze strany Zhotovitele, SLA pokračuje beze změny.

Příklad pozastavení:

10:00 - Incident nahlášen (SLA běží)
11:00 - Zhotovitel žádá o součinnost např. přístup k serveru (SLA se POZASTAVUJE)
14:00 - Objednatel poskytne přístup (SLA pokračuje od 14:00)
→ Čas 11:00-14:00 (3 hodiny) se NEPOČÍTÁ do SLA

6. Požadovaná součinnost Objednatele

SLA lhůty (reakční doba i doba vyřešení) začínají běžet okamžikem nahlášení incidentu dle této přílohy.

Pokud je pro pokračování řešení nezbytná součinnost Objednatele, zejména:

- poskytnutí doplňujících informací k diagnostice problému,
- dodání podkladů, které nemá Zhotovitel k dispozici (např. logy, konfigurace, screenshoty),
- zajištění technických podmínek nezbytných pro řešení (např. vzdálený přístup, VPN, účty),
- zpřístupnění dotčených systémů nebo prostředí,

může být běh SLA lhůt **pozastaven** postupem dle sekce 5 této přílohy.

Pokud Objednatel neposkytne požadovanou součinnost:

- SLA se pozastavuje do doby, než jsou informace/přístupy poskytnuty
- Zhotovitel informuje Objednatele o pozastavení a požadované součinnosti
- Čas čekání na součinnost se nezapočítává do doby vyřešení

7. Co se nepočítá do SLA

SLA se nevztahuje na následující situace:

- Plánované údržby schválené Objednatelem (min. 5 pracovních dnů předem)
- Testovací a vývojová prostředí (SLA platí pouze pro produkční prostředí)

8. Potvrzení vyřešení

Incident je formálně uzavřen, pokud:

- Zhotovitel označí incident jako vyřešený v ticketovém systému
- Objednatel potvrdí vyřešení NEBO neodmítne vyřešení do následujícího pracovního dne
- Pro CRITICAL incidenty je vyžadováno explicitní potvrzení Objednatele

Pokud Objednatel nesouhlasí s vyřešením:

- Incident zůstává otevřený
- SLA pokračuje v běhu (pokud již nebylo překročeno)
- Zhotovitel pokračuje v řešení dle připomínek Objednatele

9. Dokumentace vyřešení

Po vyřešení každého incidentu Zhotovitel dokumentuje:

- Popis problému - co se stalo
- Root cause - příčina problému
- Provedené kroky - jak byl problém vyřešen
- Preventivní opatření - jak zabránit opakování (pokud relevantní)

10. Měření dodržování SLA

Měření provádí:

- Zhotovitel prostřednictvím ticketového systému
- Objednatel má přístup k real-time datům 24×7
- Při sporu o čas je rozhodující timestamp v ticketovém systému

11. Eskalační matice

Zhotovitel je povinen navrhnout a doplnit po součinnosti s Objednatelem Eskalační procedury, matice a kontakty.

12. CMDB / Change Management

Objednatel požaduje, aby Zhotovitel společně s Objednatelemběhem předimplementační analýzy navrhl, implementoval a provozoval jednotný nástroj pro evidenci konfigurací a sledování změn v rámci dodaných služeb a technologií Zhotovitele. Cílem je zajistit plnou auditovatelnost a přehlednost změn prováděných v prostředí Objednatele, a to jak ze strany Objednatele, tak ze strany Zhotovitele.

Tento přístup vychází z předpokladu, že Objednatel bude disponovat odborně vyškolenými pracovníky, kteří budou oprávněni provádět konfigurační a technologické změny v dodaném prostředí. Veškeré takové změny musí být zaznamenány z důvodu bezpečnosti, posuzování plnění SLA, řešení incidentů a uplatňování záruk.

Vhodný přístup - CMDB (Configuration Management Database):

- Centrální evidence IT aktiv (servery, síťové prvky, aplikace, IDM systém) a jejich vzájemných vazeb
- Přehled o aktuálním stavu konfigurace prostředí

- Základ pro analýzu dopadu změn – před každým zásahem je zřejmé, co může být ovlivněno

Vhodný přístup - Change Management (řízení změn):

- Změna v konfiguraci (síťové prvky, IDM, aplikace, servery) musí být evidována, schválena a zdokumentována
- Jasný záznam kdo, kdy a co změnil – včetně rozlišení zda změnu provedl Objednatel nebo Zhotovitel
- Možnost zpětného dohledání stavu konfigurace k libovolnému datu
- Prevence neoprávněných nebo nezdokumentovaných zásahů do systému
- Podklad pro řešení incidentů – rychlé zjištění, zda příčinou výpadku byla nedávná změna

13. Zřetězení událostí SLA, Root Cause Based SLA

Při výpadku nebo degradaci jakékoliv dodané služby se vždy určí příčina incidentu. SLA se uplatní podle té vrstvy infrastruktury, která výpadek způsobila, nikoliv podle té, která na výpadek pouze reaguje nebo jej hlásí.

Příklad: pokud výpadek switche způsobí nedostupnost Wi-Fi, platí SLA provozní datové sítě, protože příčina leží v této vrstvě – Wi-Fi infrastruktura je pouze postižená strana. Naopak pokud provozní datová síť funguje bez závad a příčinou výpadku je selhání Wi-Fi AP, platí SLA Wi-Fi, protože příčina leží přímo v této vrstvě.

Služby implementace systému správy identit (IDM) – SLA

Garantovaná kvalita služby		**24x7x365**	
Popis služby	**Reakční doba**	**Čas na zajištění náhradního řešení**	**Čas vyřešení incidentu**
Garantovaná dostupnost HelpDesku	24 hodin 7 dní v týdnu		
Kritický/ bezpečnostní incident	1 hod.	3 hod.	2 pracovní dny
Středně závažný incident	2 hod.	12 hod.	5 pracovních dnů
Běžný / Nekritický incident	24 hod.	5 pracovních dnů	7 pracovních dnů

1. Definice incidentů dle obecného charakteru a zvyklostí služby IDM

Kritický, bezpečnostní incident

- Nefunkčnost backend serveru nebo databáze
- Kompletní výpadek IDM systému
- Nemožnost ovládat nebo odbavovat požadavky na základě dříve zadaných parametrů
- Nefunkčnost autentizace a autorizace uživatelů
- Bezpečnostní incident ohrožující integritu nebo důvěrnost dat
- Výpadek synchronizace s kritickými navázanými systémy

Středně závažný incident

- Nefunkčnost frontendu (administrační rozhraní, management IDM)
- Nemožnost přidávat, odebírat nebo upravovat záznamy přes GUI
- Problémy s auditními logy nebo monitoringem
- Prokazatelná nestabilita uživatelského rozhraní (více než 50% běžné odezvy)
- Workflow procesy fungují se zpožděním nebo omezeními

- Incident ovlivňující menší skupinu uživatelů
- Základní backend funkce jsou nedostupné (např. přes API)

Běžný, nekritický incident

- Drobné funkční nebo vizuální chyby v uživatelském rozhraní
- Problémy s načítám, importem, exportem nebo zobrazením dat (data jsou správná)
- Minimální nebo žádný dopad na uživatele
- Nekritické reporty nebo notifikace nefungují správně

2. Smluvní pokuty

V případě porušení garantované dostupnosti, stanovených reakčních dob a časů má Objednatel nárok na smluvní pokuty dle níže uvedeného:

- **Nedostupnost HelpDesku**
    - 500 Kč za každé jedno porušení garantované dostupnosti HelpDesku nebo za každý započatý den trvající nedostupnosti, jedná-li se o dlouhodobý výpadek.
- **Kritický/bezpečnostní incident**
    - 700 Kč za každé jedno porušení a každou započatou hodinu prodlení s reakcí oproti stanovené Reakční době;
    - 1 000 Kč za každé jedno porušení a každou započatou hodinu prodlení se zajištěním náhradního řešení oproti stanovenému Času na zajištění náhradního řešení;
    - 10 000 Kč za každé jedno porušení a každý započatý pracovní den prodlení s vyřešením incidentu oproti stanovenému Času vyřešení incidentu.
- **Středně závažný incident**
    - 400 Kč za každé jedno porušení a každou započatou hodinu prodlení s reakcí oproti stanovené Reakční době
    - 500 Kč za každé jedno porušení a každou započatou hodinu prodlení se zajištěním náhradního řešení oproti stanovenému Času na zajištění náhradního řešení;
    - 2 000 Kč za každé jedno porušení a každý započatý pracovní den prodlení s vyřešením incidentu oproti stanovenému Času vyřešení incidentu.

Služby zajištění kybernetické bezpečnosti za pomoci dohledového centra SOC – SLA

Parametr služby	**24x7x365**	
Dostupnost služby	**Doba reakce**	**Stabilizace a návrh protiopatření**
Závažný incident	30 min	1 hod.
Střední incident	4 hod.	8 hod.
Nízký incident	24 hod.	2 pracovní dny
Maximální počet zpracovaných, skutečně pozitivních bezpečnostních incidentů / měsíčně (očištěno o falešně pozitivní incidenty)	200 incidentů měsíčně: • Závažný incident - neomezeně • Střední incident - Počet v paušálu: 50 • Nízký incident - Počet v paušálu: 150	
Typ a podoba výstupů při šetření bezpečnostních událostí	1. Návrh krizového postupu pro zamezení šíření incidentu včetně okamžité technické reakce spočívající v izolaci zasažených prvků, blokaci kompromitovaných přístupů nebo zamezení dalšího šíření hrozby, a to zejména u infrastruktury dodávané a spravované Zhotovitelem. 2. Návrh systematického řešení pro prevenci opakování incidentu, který bude předložen k posouzení bezpečnostního, technického nebo organizačního týmu	

	Objednatele před zahájením jeho realizace. 3. Součinnost Zhotovitele při zavádění navržených opatření přesahujících rozsah okamžité stabilizace, a to po celou dobu jejich realizace bez ohledu na to, který interní tým Zhotovitele tuto součinnost zajišťuje. 4. Realizace opatření společně s infra týmem v rozsahu infrastruktury dodávané a spravované Zhotovitelem na základě předchozího schválení Objednatelem a v souladu s platným procesem řízení změn. Opatření přesahující rámec běžné provozní bezpečnosti a mající charakter rozvojových nebo infrastrukturních prací budou evidována jako samostatný požadavek na změnu nebo rozvojové zadání a řešena mimo rozsah standardní provozní smlouvy.	
Reporting	**Zasíláno 1× měsíčně** Manažerský reporting (plnění SLA), včetně společné schůzky 1h za měsíc k vyhodnocení předchozího měsíce	
Statusové schůzky	1× měsíčně	
Rozvojové práce	**4 hod. / měsíčně v ceně služby** úprava a tvorba nových detekčních pravidel, scénářů, připojení nových zdrojů, optimalizace SIEM nástroje apod.)	

1. Definice incidentů dle obecného charakteru a zvyklostí při zajištění kybernetické bezpečnosti za pomoci dohledového centra

Kategorie	Popis	Příklady
Závažný incident	Má dopad na poskytování klíčové služby, veřejnost nebo bezpečnost celé organizace	Ransomware útok, masivní data breach, kompromitace kritických systémů, DDoS útok znemožňující provoz, únik citlivých osobních údajů
Střední incident	Ovlivňuje činnost části organizace, může se rozšířit	Malware na více stanicích, phishing kampaň, neoprávněný přístup k necitlivým datům, podezřelá síťová aktivita, lokalizovaný výpadek
Nízký incident	Malý dopad, lokalizovaný problém bez přerušení služeb	Izolovaný malware na jedné stanici, neúspěšný pokus o útok, spam, podezřelý email

Příklady dohledovaných aktiv s možností definice kritičnosti: - Jednotlivé systémy a aplikace – Data (respektive úložiště) - Identity (např. konkrétní privilegované účty)

Priorita a kategorizace incidentů budou prováděny zejména v souladu se zákonem č. 205/2017 Sb., o kybernetické bezpečnosti (dále jen „ZoKB“), a vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních a kybernetických bezpečnostních incidentech, případně podle klasifikace služby kybernetické bezpečnosti zajišťované prostřednictvím dohledového centra SOC, dle klasifikačních pravidel příslušného SOC centra Zhotovitele. Charakter, závažnost a příklady incidentů však musí být s ohledem na povahu věci zachovány.

2. Klasifikace řešených incidentů

Vyřešený incident bude klasifikován dle vzorové klasifikace, případně podle klasifikace služby kybernetické bezpečnosti zajišťované prostřednictvím dohledového centra SOC dle klasifikačních pravidel příslušného SOC centra Zhotovitele. Charakter, závažnost a příklady incidentů však musí být s ohledem na povahu věci zachovány:

- **True Positive – KBI**
    - Událost byla vytvořena správně a jedná se o KBI

- **True Positive – Non-Issue**
    - Událost byla vytvořena správně, ale nejedná se o KBI, nebo o případ, kdy je potřeba Událost interně řešit.
- **True Positive – Policy Violation**
    - Událost byla vytvořena správně, nejedná se o KBI, ale je potřeba interně řešit.
- **False Positive – Tuned**
    - Událost není relevantní, chybné vyhodnocení, je nutná úprava pravidla.
- **Ignored**
    - Objednatel (protistrana) nereaguje, nebo nebyla poskytnuta součinnost více než X dní
- **Rule Test**
    - Událost vznikla jako důsledek testování nového Use Case.
- **Undetermined**
    - pro případy, kdy klasifikace není možná ani po analýze.

Za falešně pozitivní incidenty jsou považovány ty, které byly indikovány chybnou logikou detekčního pravidla či chybnými auditními záznamy. Za falešně pozitivní incidenty naopak nejsou považovány ty, které jsou detekovány správně, byla identifikována jejich příčina, ale neznamenají pro organizaci bezpečnostní riziko (např. anomálie v běžném provozu).

3. Kapacita řešení incidentů

- **Maximální počet zpracovaných skutečně pozitivních bezpečnostních incidentů** (očištěno o falešně pozitivní incidenty) je stanoven na 200 incidentů měsíčně:
    - Závažný incident
        - neomezeně
    - Střední incident
        - Počet v paušálu: 50
    - Nízký incident
        - Počet v paušálu: 150
    - SLA limit stanovuje maximální počet skutečně pozitivních bezpečnostních incidentů, které je Zhotovitel schopen měsíčně řešit. Falešně pozitivní incidenty a provozní anomálie jsou z tohoto limitu vyňaty, jelikož nepředstavují

bezpečnostní riziko a jejich objem nemá přímou vazbu na kvalitu poskytované bezpečnostní služby.

- Incidenty nad rámec uvedeného paušálu budou Objednateli účtovány na základě jednotkové ceny za incident uvedené ve Smlouvě.

4. Typ řešení incidentů a typ výstupů při šetření incidentů

Úrovně výstupů:

1. **Úroveň 1 (součást SOC):** Krizový postup pro zamezení šíření – okamžitá reakce (izolace, odpojení, blokace).
2. **Úroveň 2-3 (podpora/konzultace):** Návrh systematického řešení a asistence při implementaci – poskytováno jako podpora nebo v rámci konzultací.
3. **Úroveň 4 (rozvojová činnost):** Vlastní implementace opatření – pouze pokud Zhotovitel spravuje dané prostředí, jinak mimo rozsah SOC.

V rámci SOC musí být zajištěna minimálně úroveň 1 a dále Objednatel upřesňuje, že v případě, že Zhotovitel zároveň spravuje dotčené systémy jím dodané (firewall, servery apod.), je Zhotovitele povinen zajistit i úroveň 2-3 a 4 — tedy vlastní implementaci opatření přímo ve spravovaném prostředí. Tato úroveň reakce je logickým důsledkem správy infrastruktury, kdy Zhotovitel má přímý přístup k jím dodaným systémům, a proto je schopen incident nejen detekovat a izolovat, ale i vyřešit na základě scénářů vyplývajících z předimplementační analýzy nebo po dohodě s Objednatelem.

5. Reporting a komunikace

- **Manažerský reporting:**
- **Zasílán e-mailem a slouží i jako podklad pro technickou schůzku**
  - Zasíláno minimálně 1× měsíčně
    - Přehled plnění SLA
    - Přehled zpracovaných incidentů
  - Možnost navýšení frekvence (1× týdně) v rámci rozvojových prací
- **Technické schůzky:**
  - Účast minimálně 1× měsíčně
  - Zaměření na:
    - Optimalizaci detekčních mechanismů
    - Údržbu a rozvoj detekčních pravidel
    - Návrh nových automatizačních scénářů

        - Připojení nových datových zdrojů
        - Tvorbu nových dashboardů
        - Řešení specifických bezpečnostních výzev
    - Možnost navýšení frekvence (2× měsíčně)

6. Rozvojové práce

Hodinový rozsah zahrnutý v ceně služby – 4h/měsíc

Rozvojové práce zahrnují:

- Úprava a tvorba nových detekčních pravidel a scénářů
- Připojení nových zdrojů
- Optimalizace SIEM nástroje

7. Technická podpora

- **Dostupnost:** Hotline a ticket systém nepřetržitě (24×7)
- **Incident Response:** Reakce na bezpečnostní incident
- **Eskalace:** Koordinace s Objednatelem v případě hlášení směrem k národním autoritám (CSIRT.CZ, NÚKIB) při závažných incidentech
- **Technický report:** V případě vážné hrozby obsahující popis incidentu, dopad na organizaci, přijatá opatření a doporučení pro budoucí prevenci

8. Smluvní pokuty

V případě porušení stanovených reakčních dob a časů má Objednatel nárok na smluvní pokuty dle níže uvedeného:

- **Závažný incident**
    - 750 Kč za každé jedno porušení a každou započatou hodinu prodlení s reakcí oproti stanovené Době reakce;
    - 1 500 Kč za každé jedno porušení a každou započatou hodinu prodlení se zajištěním stabilizace a návrhem protiopatření oproti stanovené době pro stabilizaci a návrh protiopatření;
- **Střední incident**
    - 500 Kč za každé jedno porušení a každou započatou hodinu prodlení s reakcí oproti stanovené Reakční době;

- 900 Kč za každé jedno porušení a každou započatou hodinu prodlení zajištěním stabilizace a návrhem protiopatření oproti stanovené době pro stabilizaci a návrh protiopatření.

Služby zálohování a archivace ICT dat – SLA

Dostupnost služby – 8x5 (Po-Pá 8:00-17:00)		
Priorita	**Reakční doba**	**Čas na vyřešení incidentu**
Kritická závažnost	do 6 hodin	Do 12 hodin
Vysoká závažnost	do 12 hodin	Do 2 pracovních dnů
Střední závažnost	2 pracovní dny	Do 5 pracovních dnů
Minimální závažnost	4 pracovní dny	Do 7 pracovních dnů

1. Definice incidentů dle obecného charakteru a zvyklostí při zajištění služby zálohování a archivace ICT dat

CRITICAL (Kritická závažnost)

- Systém je z důvodu jeho selhání kompletně mimo provoz
- Nelze využít žádnou z jeho služeb ani funkcí

HIGH (Vysoká závažnost)

- Hlavní funkce a služby systému jsou významným způsobem omezeny
- Znemožňuje plné využívání systému uživateli nebo je významně omezuje
- Není možné pracovat se systémem, protože se prodloužila doba odezvy nebo pracnost o více než 50 %
- Problém nelze odstranit určeným technickým pracovníkem zákazníka
- Vyskytují se chyby v systému, které není možno nahradit jiným mimořádným postupem nebo jinými funkcemi systému (nelze obejít)

MEDIUM (Střední závažnost)

- Funkce a služby systému nejsou významným způsobem omezeny

- Tento stav má pouze částečný dopad na práci uživatelů
- Problém lze obejít pomocí alternativního postupu

LOW (Nízká závažnost)

- Drobné funkční nebo kosmetické chyby v systému
- Minimální nebo žádný dopad na práci uživatelů

Vazba na parametry obnovy dat

Časy vyřešení incidentů uvedené v tabulce výše se vztahují na obnovení funkčnosti zálohovacího systému jako takového. Parametry obnovy samotných dat se řídí hodnotami RPO a RTO definovanými v [Příloze č. 2, této smlouvy]:

- RPO ≤ 4 hodiny pro kritické systémy, RPO ≤ 24 hodin pro nekritické systémy
- RTO ≤ 4 hodiny pro kritické systémy s objemem dat do 2 TB (celkový součet kritických systémů), RTO ≤ 24 hodin pro nekritické systémy

Pro účely SLA platí:

- Incident kritické závažnosti je považován za vyřešený až v okamžiku, kdy je zálohovací systém funkční. Mimo SLA je dále požadována kontrola integrity a dostupnost posledních záloh.
- V případě, že obnova dat přesáhne garantované RTO, jde o samostatný incident klasifikovaný jako kritická závažnost bez ohledu na stav zálohovacího systému samotného.

2. Smluvní pokuty

V případě porušení stanovených reakčních dob a časů má Objednatel nárok na smluvní pokuty dle níže uvedeného:

- **Incident s prioritou CRITICAL**
    - 500 Kč za každé jedno porušení a každou započatou hodinu prodlení s reakcí oproti stanovené Reakční době;
    - 1 000 Kč za každé jedno porušení a každou započatou hodinu prodlení s vyřešením incidentu oproti stanovenému Času na vyřešení incidentu.

- **Incident s prioritou HIGH**
    - 300 Kč za každé jedno porušení a každou započatou hodinu prodlení s reakcí oproti stanovené Reakční době;
    - 2 500 Kč za každé jedno porušení a každý započatý pracovní den prodlení s vyřešením incidentu oproti stanovenému Času na vyřešení incidentu.
- **Incident s prioritou MEDIUM**
    - 1 000 Kč za každé jedno porušení a každý započatý pracovní den prodlení s reakcí oproti stanovené Reakční době;
    - 1 000 Kč za každé jedno porušení a každý započatý pracovní den prodlení s vyřešením incidentu oproti stanovenému Času na vyřešení incidentu.

Služby virtualizace a serverové infrastruktury – SLA

Dostupnost služby – 24x7x365		
Priorita	**Reakční doba**	**Čas na vyřešení incidentu**
Kritická závažnost	Do 1 hodin	Do 8 hodin od nahlášení
Vysoká závažnost	do 4 hodin	Do 12 hodin od nahlášení
Střední závažnost	Do 1 pracovního dne	Do 5 pracovních dnů
Minimální závažnost	Do 2 pracovních dnů	Do 7 pracovních dnů

1. Definice incidentů dle obecného charakteru a zvyklostí při zajištění služby virtualizace a serverové infrastruktury

CRITICAL (Kritická závažnost)

- Virtualizační platforma je kompletně nefunkční
- Nelze využít žádnou z jejích služeb ani funkcí
- Není možné spouštět, zastavovat ani přistupovat k virtuálním strojům

HIGH (Vysoká závažnost)

- Klíčové funkce virtualizační platformy jsou výrazně omezeny
- Znemožňuje nebo významně omezuje plnohodnotné využívání systému
- Práce s platformou je výrazně ztížena, doba odezvy nebo pracnost se zvýšila o více než 50 %
- Problém nelze vyřešit interními zdroji zákazníka
- Chyby nelze obejít alternativním postupem ani jinými funkcemi systému

MEDIUM (Střední závažnost)

- Funkce virtualizační platformy nejsou zásadně omezeny

- Dopad na využívání systému je pouze částečný
- Práce s platformou je možná, doba odezvy nebo pracnost se zvýšila o méně než 50 %
- Problém lze dočasně řešit pomocí alternativního postupu

LOW (Minimální závažnost)

- Funkce virtualizační platformy jsou dostupné bez významných omezení
- Dopad na běžné využívání systému je minimální
- Jedná se o drobné nedostatky, které nebrání standardnímu používání

2. Smluvní pokuty

V případě porušení stanovených reakčních dob a časů má Objednatel nárok na smluvní pokuty dle níže uvedeného:

- **Incident s prioritou CRITICAL**
    - 800 Kč za každé jedno porušení a každou započatou hodinu prodlení s reakcí oproti stanovené Reakční době;
    - 1 500 Kč za každé jedno porušení a každou započatou hodinu prodlení s vyřešením incidentu oproti stanovenému Času na vyřešení incidentu.
- **Incident s prioritou HIGH**
    - 600 Kč za každé jedno porušení a každou započatou hodinu prodlení s reakcí oproti stanovené Reakční době;
    - 1 000 Kč za každé jedno porušení a každou započatou hodinu prodlení s vyřešením incidentu oproti stanovenému Času na vyřešení incidentu.
- **Incident s prioritou MEDIUM**
    - 1 000 Kč za každé jedno porušení a každý započatý pracovní den prodlení s reakcí oproti stanovené Reakční době;
    - 1 000 Kč za každé jedno porušení a každý započatý pracovní den prodlení s vyřešením incidentu oproti stanovenému Času na vyřešení incidentu.

Služby návrhu a implementace WiFi datové sítě – SLA

Dostupnost služby – 24x7x365 pro kritickou, vysokou a střední závažnost		
Priorita	**Reakční doba**	**Čas na vyřešení incidentu**
Kritická závažnost	Do 1 hod.	Do 8 hodin od nahlášení
Vysoká závažnost	do 90 min.	Do 16 hodin od nahlášení
Střední závažnost	do 4 hod.	Do 48 hodin od nahlášení
Minimální závažnost	Do 2 pracovních dnů	Do 10 pracovních dnů, v pracovních dnech

1. Definice incidentů dle obecného charakteru a zvyklostí při zajištění WiFi sítě ARENA BRNO

CRITICAL (Kritická závažnost)

WiFi systém je z důvodu selhání kompletně mimo provoz a nelze využít žádnou z jeho služeb ani funkcí.

Příklady:

- Kompletní výpadek WiFi pokrytí v celém objektu
- Nefunkčnost všech WiFi kontrolérů nebo access pointů
- Výpadek autentizačního systému (guest portal, RADIUS) - nikdo se nemůže připojit
- Kritická bezpečnostní chyba ohrožující síťovou bezpečnost
    - Kritická bezpečnostní chyba zůstává v kategorii CRITICAL, protože může být způsobena chybnou konfigurací Zhotovitele, nikoli pouze chybou výrobce.
    - Pokud je příčinou chyba výrobce vyžadující patch, SLA se pozastavuje až do dodání patche.

    - Zhotovitel v této době nabídne proaktivní řešení situace (workaround, dočasná migrace, izolace postižené části).
    - Pokud je příčinou chybná konfigurace Zhotovitele, SLA pokračuje a Zhotovitel by měl okamžitě reagovat.
- Výpadek backendové infrastruktury WiFi (management systém nedostupný a nelze obnovit službu)

HIGH (Vysoká závažnost)

Hlavní funkce a služby WiFi systému jsou významným způsobem omezeny. Tento stav znemožňuje plné využívání systému uživateli, nebo je významně omezuje (není možné efektivně pracovat s WiFi, protože se prodloužila doba odezvy nebo propustnost klesla o více než 50 %) a nelze jej odstranit určeným technickým pracovníkem zákazníka. Lze takto označit problém, kdy se vyskytují chyby v systému a není je možno nahradit jiným mimořádným postupem nebo jinými funkcemi systému (obejít).

Příklady:

- Výpadek WiFi pokrytí ve významné části objektu (>50 % ploch nebo kritické zóny)
    - Kritickými zónami se rozumí vstupní prostory a plochy před vstupy v 1. nadzemním podlaží (vstupenková zóna, čtečky) a dále oblasti platebních terminálů u provozoven rychlého občerstvení a barů v 1.–5. nadzemním podlaží.
        - Na půdorysu 1NP je ve výkresové dokumentaci znázorněna potřeba, aby pokrytí bylo v místě vstupních a evakuačních dveří i v ploše bezprostředně před halou (2-5 m, pro potřeby čteček vstupenek).
- Nefunkčnost většiny access pointů (>50 %)
- Výrazné zpomalení WiFi (propustnost klesla o více než 50 %)
- Časté odpojování uživatelů nebo nemožnost se připojit
- Nefunkčnost roamingu mezi access pointy
- Selhání redundance nebo high availability mechanismů
    - Redundance zde neznamená zdvojení všech komponent (kontrolerů, switchů), ale pokrytí kritických ploch více než jedním access pointem připojeným do různých access switchů nebo jednim access pointem připojeným do dvou access switchů.

    - Pokud v kritické zóně selže jeden AP, další AP musí zajistit pokrytí. To je dle nás základní princip návrhu Wi-Fi, nikoliv nadstandardní redundance.
    - Co se týče HW, např. kontrolér není požadován jako redundantní (pokud není součástí redundance ve virtuálním prostředí).
    - Kategorii HIGH ponecháváme, protože výpadek >50% pokrytí nebo kritických zón je závažný provozní problém.
- Problémy s VLAN segmentací ovlivňující business provozu

MEDIUM (Střední závažnost)

Funkce a služby WiFi systému nejsou významným způsobem omezeny. Tento stav má pouze částečný dopad na využívání systému uživateli. Je možné pracovat s WiFi, i když se prodloužila doba odezvy nebo propustnost snížila o méně než 50 %. Může se jednat o problém ve funkčnosti, který lze dočasně náhradním uspokojivým způsobem obejít.

Příklady:

- Výpadek WiFi pokrytí v menší části objektu (<50 % ploch, nekritické zóny)
- Nefunkčnost menšiny access pointů (<50 %)
- Mírné zpomalení WiFi (propustnost klesla o méně než 50 %)
- Problémy s guest WiFi (zaměstnanecká WiFi funguje)
- Nefunkčnost guest portálu (lze použít jiné přihlašovací metody)
- Problémy s QoS nebo traffic shapingem
- Nefunkčnost monitoringu nebo reportingu (WiFi funguje, ale nelze sledovat metriky)
- Problémy s některými typy zařízení (např. starší mobilní telefony)

LOW (Minimální závažnost)

Funkce a služby WiFi systému nejsou významným způsobem omezeny. Tento stav má minimální dopad na využívání systému uživateli. Může se jednat o drobné vady, nijak neomezující běžné používání WiFi.

Konkrétní příklady:

- Slabý signál v okrajových nebo méně využívaných zónách

    - Snížení výkonu nebo pokrytí AP z důvodu částečné závady (např. porucha antény, snížený výkon vysílače) v méně kritických zónách - AP funguje, ale s omezeným výkonem.

- Drobné problémy s roamingem (krátké výpadky při přechodu mezi AP)
- Problémy se statistikami nebo logy (WiFi funguje normálně)
- Drobné problémy s notifikacemi nebo alertingem
- Problémy s některými nekritickými funkcemi (captive portal styling, reporting)

Poznámka: Priorita incidentu může být během řešení změněna na základě skutečného dopadu na provoz WiFi služeb a počet dotčených uživatelů.

2. Smluvní pokuty

V případě porušení stanovených reakčních dob a časů má Objednatel nárok na smluvní pokuty dle níže uvedeného:

- **Incident s prioritou CRITICAL**
    - 1 250 Kč za každé jedno porušení a každou započatou hodinu prodlení s reakcí oproti stanovené Reakční době;
    - 2 500 Kč za každé jedno porušení a každou započatou hodinu prodlení s vyřešením incidentu oproti stanovenému Času na vyřešení incidentu.
- **Incident s prioritou HIGH**
    - 1 000 Kč za každé jedno porušení a každou započatou hodinu prodlení s reakcí oproti stanovené Reakční době;
    - 2 000 Kč za každé jedno porušení a každou započatou hodinu prodlení s vyřešením incidentu oproti stanovenému Času na vyřešení incidentu.
- **Incident s prioritou MEDIUM**
    - 500 Kč za každé jedno porušení a každou započatou hodinu prodlení s reakcí oproti stanovené Reakční době;
    - 1 000 Kč za každé jedno porušení a každou započatou hodinu prodlení s vyřešením incidentu oproti stanovenému Času na vyřešení incidentu.

Provozní datová síť ARENA BRNO – SLA

Dostupnost služby – 24x7x365		
Priorita	**Reakční doba**	**Čas na vyřešení incidentu**
Kritická závažnost	Do 30 min.	Do 12 hodin od nahlášení
Vysoká závažnost	do 4 hodin	Do 24 hodin od nahlášení
Střední závažnost	do 8 hodin	Do 2 pracovních dnů
Minimální závažnost	Do 2 pracovních dnů	Do 7 pracovních dnů

1. Definice incidentů dle obecného charakteru a zvyklostí při zajištění provozně datové sítě ARENA BRNO

CRITICAL (Kritická závažnost)

Systém nebo jeho část až do úrovně jednotlivých access switchů je z důvodu selhání kompletně mimo provoz a nelze využít žádnou z jeho služeb ani funkcí.

HIGH (Vysoká závažnost)

Hlavní funkce a služby Systému nebo jeho část až do úrovně jednotlivých access switchů jsou významným způsobem omezeny. Tento stav znemožňuje plné využívání Systému nebo jeho část až do úrovně jednotlivých access switchů uživateli, nebo je významně omezuje (není možné efektivně pracovat se Systémem nebo jeho část až do úrovně jednotlivých access switchů, protože se prodloužila doba odezvy o více než 50 %) a nelze jej odstranit určeným technickým pracovníkem zákazníka. Lze takto označit problém, kdy se vyskytují chyby v Systému nebo jeho část až do úrovně jednotlivých access switchů a není je možno nahradit jiným mimořádným postupem nebo jinými funkcemi Systému nebo jeho část až do úrovně jednotlivých access switchů (obejít).

MEDIUM (Střední závažnost)

Funkce a služby Systému nebo jeho část až do úrovně jednotlivých access switchů nejs ou významným způsobem omezeny. Tento stav má pouze částečný dopad na využívání Systému nebo jeho část až do úrovně jednotlivých access switchů uživateli. Je možné pracovat se Systémem nebo jeho část až do úrovně jednotlivých access switchů, i když se prodloužila doba odezvy o méně než 50 %. Může se jednat o problém ve funkčnosti, který lze dočasně náhradním uspokojivým způsobem obejít.

LOW (Minimální závažnost)

Funkce a služby Systému nebo jeho část až do úrovně jednotlivých access switchů nejsou významným způsobem omezeny. Tento stav má minimální dopad na využívání Systému nebo jeho část až do úrovně jednotlivých access switchů uživateli (může se jednat o drobné vady, nijak neomezující běžné používání Systému nebo jeho část až do úrovně jednotlivých access switchů).

2. Smluvní pokuty

V případě porušení stanovených reakčních dob a časů má Objednatel nárok na smluvní pokuty dle níže uvedeného:

- **Incident s prioritou CRITICAL**
    - 1 250 Kč za každé jedno porušení a každou započatou hodinu prodlení s reakcí oproti stanovené Reakční době;
    - 2 500 Kč za každé jedno porušení a každou započatou hodinu prodlení s vyřešením incidentu oproti stanovenému Času na vyřešení incidentu.
- **Incident s prioritou HIGH**
    - 1 000 Kč za každé jedno porušení a každou započatou hodinu prodlení s reakcí oproti stanovené Reakční době;
    - 2 000 Kč za každé jedno porušení a každou započatou hodinu prodlení s vyřešením incidentu oproti stanovenému Času na vyřešení incidentu.
- **Incident s prioritou MEDIUM**
    - 500 Kč za každé jedno porušení a každou započatou hodinu prodlení s reakcí oproti stanovené Reakční době;
    - 5 000 Kč za každé jedno porušení a každý započatý pracovní den prodlení s vyřešením incidentu oproti stanovenému Času na vyřešení incidentu.