SMLOUVA
o poskytování služby SOC

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., ve znění pozdějších předpisů (dále jen "OZ") mezi:

Českou národní bankou
Na Příkopě 28
115 03 Praha 1
zastoupenou: Ing. Vladimírem Mojžíškem, ředitelem sekce informatiky
a
Ing. Zdeňkem Viriusem, ředitelem sekce správní
IČO: 48136450
DIČ: CZ48136450

(dále jen „objednatel" nebo „ČNB")

a

T-Mobile Czech Republic a.s.
Tomíčkova 2144/1
148 00 Praha 4
zastoupenou: Radkem Podzemským, na základě pověření
č. účtu: 19-2271190247/0100
IČO: 64949681
DIČ: CZ64949681

(dále jen „poskytovatel")

Preambule

Objednatel provozuje systém managementu bezpečnostních informací a událostí SIEM (dále jen „SIEM") založený na produktu HP ArcSight.

Vzhledem k celosvětově stoupajícímu trendu kybernetických útoků je potřeba zajistit nepřetržitý monitoring a analýzu bezpečnostních událostí s využitím systému SIEM objednatele včetně návrhu na protiopatření v režimu 7x24x365. Rovněž je potřeba zajistit průběžnou úpravu pravidel v systému SIEM, aby byl schopen odhalovat nové hrozby, případně se zrychlilo jejich odhalení.

Vzhledem k důležitosti této služby nezbytné pro zabezpečení ostatních informačních systémů ČNB v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, stanovuje objednatel dále uvedené požadavky, lhůty, platební podmínky, smluvní pokuty a další smluvní ujednání, které z této důležitosti vycházejí.

Článek I
Předmět smlouvy

1. Poskytovatel se touto smlouvou zavazuje poskytovat objednateli za sjednaných podmínek na vlastní náklady a na své nebezpečí službu zahrnující:

a) nepřetržitý vzdálený dohled/monitoring bezpečnostních událostí s využitím systému SIEM objednatele, a to 24 hodin denně 7 dnů v týdnu po celý rok,
b) analýzu bezpečnostních událostí (KBU) zachycených systémem SIEM objednatele, včetně návrhu na protiopatření (řešení),
c) upozornění objednatele na zjištěné bezpečností incidenty (KBI) dle jejich závažnosti a v této smlouvě dohodnuté komunikační matice,
d) poskytování pravidelného měsíčního reportu zabezpečeným způsobem (bude definitivně stanoven v realizační studii), který bude obsahovat minimálně:
    i. statistiku sbíraných událostí a typů zdrojů těchto událostí,
    ii. seznam a způsob řešení jednotlivých zjištěných bezpečnostních událostí a incidentů (KBU/KBI),
    iii. návrhy na vylepšení bezpečnostního monitoringu o další scénáře v systému SIEM objednatele (pravidla, reporty, apod.) formou balíčků pro nástroj HP ArcSight nebo připravených filtrů s podrobným popisem jejich implementace,
    iv. počet skutečně odpracovaných hodin plnění dle odst. 1 písm. e), včetně podrobného rozpisu,
e) poskytování konzultačních služeb při případné úpravě pravidel, reportů a filtrů pro systém SIEM objednatele, které nespadají do plnění uvedeného v písm. a) – d) výše, v rozsahu 10 člověkodnů ročně,
f) poskytování konzultačních služeb při případné úpravě pravidel, reportů a filtrů pro systém SIEM objednatele, které jsou nad rámec rozsahu člověkodní dle písm. e) tohoto odstavce. V případě potřeby budou tyto služby prováděny na základě nabídky poskytovatele, jejíž součástí bude předpokládaná pracnost a harmonogram realizace požadované služby. V případě akceptace nabídky objednatelem bude na tyto služby vystavena samostatná objednávka.

2. Podrobná specifikace a parametry poskytované služby jsou uvedeny v příloze č. 1, která je nedílnou součástí této smlouvy.

3. Předmětem této smlouvy je dále závazek poskytovatele provést před zahájením poskytování služby dle odst. 1 přípravné činnosti specifikované v čl. II.

4. Služba uvedená v odst. 1 písm. a) až c) tohoto článku bude poskytována výhradně formou vzdáleného přístupu. Definice a parametry vzdáleného přístupu jsou uvedeny v příloze č. 7, která je nedílnou součástí této smlouvy. Náklady na zajištění vzdáleného přístupu až k přístupovému bodu VPN na perimetru ČNB hradí poskytovatel.

5. Předmětem této smlouvy je závazek objednatele poskytnout potřebnou součinnost a zaplatit za poskytnutá plnění cenu dle čl. V.

Článek II
Přípravné činnosti

1. Před zahájením poskytování služby dle č. 1 odst. 1 písm. a) – d) budou realizovány níže uvedené přípravné činnosti rozdělené do dvou etap, které budou předmětem akceptace dle čl. IV.

2. **1. etapa – Realizační studie**

    2.1 První etapa je zaměřena na detailní analýzu požadavků objednatele (příloha č. 2) a navrženého řešení služby poskytovatelem (příloha č. 1) s cílem ověřit realizovatelnost nabízené služby v podmínkách objednatele, ověřit a dokladovat soulad s požadavky objednatele, podrobně specifikovat technickou realizaci služby a případně identifikovat technické problémy či dosud neidentifikované změny a

požadavky, které by vznikly v souvislosti s implementací a provozováním služby v prostředí objednatele.

2.2 Výstupem této etapy bude podrobná realizační studie, pro jejíž tvorbu využije poskytovatel šablonu realizační studie uvedenou v příloze č. 6.

2.3 Sběr informací, které bude poskytovatel potřebovat pro vytvoření objednatelem požadované realizační studie, bude probíhat formou interview mezi odbornými pracovníky obou smluvních stran v místě plnění.

2.4 Ze studie musí být objednatel schopen ověřit, že navrhovaná služba a způsob jejího poskytování splňuje požadavky objednatele, vyhovuje jeho potřebám, jeho provozním zvyklostem a je implementovatelné ve lhůtách uvedených v této smlouvě. Dále u případně nově identifikovaných požadavků či změn souvisejících s implementací a provozováním služby v prostředí objednatele neuvedených v příloze č. 2 této smlouvy, musí realizační studie obsahovat návrh vypořádání takových požadavků či změn.

2.5 Tato etapa v sobě zahrnuje zejména následující činnosti:

a) seznámení odborných pracovníků poskytovatele s výpočetním prostředím ČNB, kritičností jednotlivých dozorovaných IS a aplikací,
b) seznámení se s konfigurací systému SIEM objednatele (reporty, alerty, pravidla, korelace, atd.),
c) návrh případné úpravy pravidel v SIEM objednatele formou balíčků pro nástroj HP ArcSight nebo připravených filtrů s podrobným popisem jejich implementace a připojení nových zdrojů událostí, je-li to potřeba pro zajištění kvality poskytované služby,
d) definování způsobů vzájemné komunikace obou smluvních stran (komunikační matice) a eskalace,
e) definování struktury a obsahu měsíčního reportu,
f) vytvoření realizační studie,
g) ve spolupráci obou smluvních stran akceptaci realizační studie,
h) uzavření ujednání o zpracování osobních údajů v souladu s přílohou č. 4.

2.6 Akceptovaná realizační studie je pro poskytovatele závazná a stává se volně připojenou přílohou č. 8 této smlouvy.

2.7 Činnosti prováděné v rámci této etapy se realizují v pracovní dny během standardní pracovní doby objednatele (7:45 až 16:15 - časové pásmo místa plnění), pokud se obě smluvní strany nedohodnou jinak.

3. **2. etapa – Implementace a ověřovací provoz**

3.1 Tato etapa je zaměřena na technické zprovoznění služby spočívající v potřebné konfiguraci zabezpečeného vzdáleného přístupu (dále jen „VPN“) a systému SIEM v prostředí objednatele a instalaci a konfiguraci VPN v prostředí poskytovatele, dále pak nastavení a aktivaci monitorovacích a reportovacích procesů, a to vše v souladu s akceptovanou realizační studií. Součástí této etapy je i jednoměsíční poskytování služby – ověřovací provoz.

3.2 Druhá etapa zahrnuje následující činnosti:

a) zajištění přístupů jednotlivých pracovníků poskytovatele, kteří se budou podílet na poskytování služby dle čl. I odst. 1 písm. a) až c):
   i. aktivace přístupů do webové konzole SIEM objednatele formou VPN,
   ii. předání certifikátů pracovníkům poskytovatele na jejich vlastní čipovou kartu (token) dle specifikace uvedené v příloze č. 2 (požadavek S33) pro

zajištění bezpečného přihlášení ke konzoli SIEM objednatele prostřednictvím VPN,

b) zprovoznění VPN u poskytovatele dle návodu od objednatele,
c) úprava pravidel v SIEM objednatelem, dle doporučení a podrobného návodu poskytovatele uvedeného v realizační studii,
d) poskytování služeb dle čl. 1 odst. 1 písm. a) – d) po dobu jednoho měsíce (dále jen „ověřovací provoz"),
e) ve spolupráci obou smluvních stran akceptaci měsíčního reportu ověřovacího provozu.

Článek III
Lhůty, místo plnění a pověřené osoby

1. Poskytovatel se zavazuje zahájit poskytování služby dle čl. I odst. 1 do 4 měsíců ode dne podpisu této smlouvy s tím, že první etapa dle čl. II bude dokončena nejpozději do 2 měsíců od podpisu smlouvy.
2. Smluvní strany se dohodly, že pokud bude nutno před uzavřením smlouvy o zpracování osobních údajů uvedené v čl. II odst. 2.5 písm. h) požádat Úřad pro ochranu osobních údajů o stanovisko, staví se lhůta pro ukončení 1. etapy a lhůta pro zahájení poskytování služby do doby obdržení tohoto stanoviska.
3. Za místo plnění se považuje sídlo objednatele na adrese Na Příkopě 28, Praha 1.
4. Pověřenými osobami jsou pro:

a) akceptaci jednotlivých etap:

i. za objednatele: Ing. Luboš Minár, lubos.minar@cnb.cz, tel. 224 412 606,
Ing. Robert Lederer, robert.lederer@cnb.cz, tel. 22441 2669
ii. za poskytovatele: Honza Petřík, tel.: 603 423 669, e-mail: jan.petrik@t-mobile.cz, Martin Šimonek, tel.: 603 418 615, e-mail: martin.simonek@t-mobile.cz;

b) provoz služby:

iii. za objednatele: Ing. Luboš Minár, lubos.minar@cnb.cz, tel. 224 412 606,
Ing. Robert Lederer, robert.lederer@cnb.cz, tel. 22441 2669
iv. za poskytovatele:

Tel.: +420 236 099 009, +420 225 988 366
Mobil.: +420 604 296 948
E-mail: SOC@t-mobile.cz

Úroveň	1	2	3
Jméno	Shift responsible	Jan Veselý	Michal Trejbal
Pozice	Service Management Centre Analyst	Head of Service Management Center	Senior Head of SMC and access network
Telefon	+420 236 099 009	+420 225 255 654	+420 225 255 456
Mobilní telefon	+420 604 296 948	+420 777 770 073	+420 602 258 768

Fax	+420 236 099 888	--	--
E-mail	SOC@t-mobile.cz	Jan.Vesely3@t-mobile.cz	Michal.Trejbal@t-mobile.cz
Dostupnost	24x7	8x5	8x5

c) otázky smluvní:

v. za objednatele: Ing. Luboš Minár, lubos.minar@cnb.cz, tel. 224 412 606, Ing. Robert Lederer, robert.lederer@cnb.cz, tel. 22441 2669;

vi. za poskytovatele: Honza Petřík, tel.: 603 423 669, e-mail: jan.petrik@t-mobile.cz, Ing. Lukáš Marhoul, tel.: 724 095 710, e-mail: lukas.marhoul@t-mobile.cz.

5. Smluvní strany se zavazují ohlásit změnu pověřených osob nebo kontaktních údajů podle předchozího odstavce nejpozději následující pracovní den po provedení změny na e-mailové adresy pověřených osob, přičemž taková změna se nepovažuje za změnu smlouvy.

Článek IV
Akceptace přípravných činností

1. Před ukončením každé etapy uvedené v článku II se uskuteční akceptační řízení. Akceptační řízení začne předložením všech potřebných podkladů k příslušnému předmětu akceptace kterékoliv pověřené osobě objednatele uvedené v čl. III odst. 4 písm. a).
2. Při akceptačních řízeních budou vady odstraňovány a připomínky vypořádány bez zbytečného odkladu.
3. O ukončení každého akceptačního řízení bude sepsán akceptační protokol, který vyhotoví objednatel. K akceptačnímu protokolu se vyjádří poskytovatel nejpozději do 3 pracovních dnů po jeho obdržení. Pokud tak neučiní, má se za to, že s uvedeným závěrem souhlasí. Akceptační protokoly podepisují pověřené osoby uvedené v čl. III odst. 4 písm. a) (postačuje jedna z nich za každou smluvní stranu).
4. Kterákoliv etapa bude považována za úspěšně provedenou, pokud bude prostá vad, nerozhodne-li se objednatel akceptovat danou etapu s výhradami. Akceptační protokol v případě akceptace s výhradami musí obsahovat výčet vad, způsob a lhůtu pro jejich odstranění. Pokud objednatel pro vady kteroukoliv etapu neakceptuje, uvede to v akceptačním protokolu spolu s odůvodněním.
5. Poskytovatel je oprávněn zahájit další etapu až poté, co objednatel akceptoval předchozí etapu.

Akceptace 1. etapy

6. Po realizaci všech činností v rámci 1. etapy předloží poskytovatel objednateli realizační studii k připomínkám. Objednatel uplatní písemně (poštou nebo elektronicky) připomínky nejpozději do 5 pracovních dnů od obdržení realizační studie.
7. Za vadu realizační studie se považuje zejména:

i. chybějící textová část dokumentace nebo nevyplněná či nevypracovaná část realizační studie, jejíž předepsaná struktura je uvedena v příloze č. 6,

ii. textová část studie neodpovídá skutečnosti popisované entity (např. systému, procesu, chybové zprávě, požadavkům uvedeným v přílohách 1 až 2) nebo je v rozporu s některým z povinných požadavků dle přílohy č. 2.

8. Rozhodnutí o akceptaci či neakceptaci realizační studie provede objednatel do 5 pracovních dnů od obdržení vypořádání připomínek. Během této doby si objednatel vyhrazuje právo pokládat další dotazy a návrhy na doplnění a úpravy studie (např. formou e-mailu) poskytovateli, které budou zodpovězeny či vypořádány poskytovatelem bez zbytečného odkladu.

9. Podmínkou akceptace 1. etapy je uzavření smlouvy o zpracování osobních údajů (příloha č. 4).

10. Objednatel je oprávněn kdykoliv před akceptací první etapy využít výhradu uvedenou v článku IX odst. 5, a to zejména v případech, kdy je z realizační studie zřejmé, že kvalita nabízené služby neodpovídá zvyklostem a standardům objednatele či v případě detekce dodatečných změn a nákladů uvedených v realizační studii, které by měly velké dopady na očekávaný rozpočet objednatele či zatížení jeho lidských zdrojů.

Akceptace 2. etapy

11. Po realizaci všech činností v rámci 2. etapy předloží poskytovatel objednateli report z měsíčního ověřovacího provozu k připomínkám, které objednatel uplatní písemně (poštou nebo elektronicky) nejpozději do 5 pracovních dnů.
12. Za vadu reportu z měsíčního ověřovacího provozu se považuje zejména:
    a. absence některých částí podle struktury uvedené v realizační studii,
    b. opomenutí detekovaného KBI včetně návrhu protiopatření,
    c. neúplné, chybné nebo nekonzistentní údaje.
13. Rozhodnutí o akceptaci či neakceptaci reportu provede objednatel do 5 pracovních dnů od obdržení vypořádání připomínek.
14. Podmínkou akceptace 2. etapy je úspěšně provedený ověřovací provoz, ve kterém nebyly detekovány vady, nebo byly všechny vady odstraněny do jeho ukončení.
15. Za vadu v ověřovacím provozu se považuje zejména:
    i. nedostupnost SIEM objednatele pro poskytovatele z důvodů na straně poskytovatele v rozsahu větším než 2 hodiny,
    ii. nedetekované KBU/KBI poskytovatelem, ačkoliv je objednatel detekoval.
16. Dnem podpisu akceptačního protokolu druhé etapy bude zahájeno poskytování služby dle čl. I odst. 1 písm. a) až e).

Článek V
Cena a platební podmínky

1. Cena za přípravné činnosti dle článku II činí celkem 97 945,- Kč bez DPH, z toho činí cena za realizaci 1. etapy 46 800,- Kč bez DPH a cena za realizaci 2. etapy 51 145,- Kč bez DPH.

2. Cena za poskytování služby podle čl. I odst. 1 písm. a) až e) činí 32 375,- Kč bez DPH měsíčně.

3. Cena za poskytování konzultačních služeb dle článku I odst. 1 písmene f) bude stanovena jako součin počtu skutečně poskytnutých hodin konzultací a hodinové sazby, která činí 1 376,- Kč bez DPH.

4. Cena dle odst. 1 za přípravné činnosti bude uhrazena na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve v den podpisu akceptačního protokolu o ukončení 2. etapy.

5. Cena dle odst. 2 za poskytování služby dle čl. I odst. 1 písm. a) až e) bude hrazena na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve poslední den kalendářního měsíce, za který se platí. Výše paušální ceny za období kratší než kalendářní měsíc se vypočte jako alikvotní část měsíčního paušálu.

6. Úhrada ceny dle odst. 3 bude prováděna na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve poslední den kalendářního měsíce, ve kterém byly konzultační služby poskytnuty. Přílohou daňového dokladu bude časový a věcný rozpis konzultací podepsaný pověřenou osobou objednatele.

7. Všechny ceny jsou uvedeny bez DPH; daň z přidané hodnoty bude účtována v sazbě platné ke dni vzniku daňové povinnosti. Ceny zahrnují veškeré náklady poskytovatele spojené s plněním podle této smlouvy včetně nákladů na činnost, kterou poskytovatel vykonává jakožto zpracovatel osobních údajů podle smlouvy o zpracování osobních údajů.

8. Doklady k úhradě (faktury) budou obsahovat údaje podle § 435 občanského zákoníku, evidenční číslo smlouvy ČNB a bankovní účet, na který má být placeno a který je uveden v záhlaví této smlouvy nebo který byl později aktualizován poskytovatelem (dále jen „určený účet"). Daňový doklad bude nadto obsahovat náležitostí stanovené v zákoně o dani z přidané hodnoty. V případě, že doklad k úhradě bude postrádat některou ze stanovených náležitostí nebo bude obsahovat chybné údaje, je objednatel oprávněn jej vrátit poskytovateli, a to až do lhůty splatnosti. Nová lhůta splatnosti začíná běžet dnem doručení bezvadného dokladu k úhradě.

9. V případě, že bude v dokladu k úhradě uveden jiný než určený účet, je pověřená osoba poskytovatele povinna na základě výzvy objednatele sdělit na e-mailovou adresu, ze které byla výzva odeslána, zda má být zaplaceno na bankovní účet uvedený v dokladu k úhradě, nebo na určený účet. V tomto případě se doklad k úhradě nevrací s tím, že lhůta splatnosti začíná běžet až dnem doručení sdělení poskytovatele podle předchozí věty.

10. Doklady bude poskytovatel zasílat elektronicky na adresu **faktury@cnb.cz**, přičemž doklad musí být vložen jako příloha mailové zprávy ve formátu PDF. V jedné mailové zprávě smí být pouze jeden doklad. Mimo vlastní doklad může být přílohou mailové zprávy jedna až tři přílohy k dokladu ve formátech PDF, DOC, DOCX, XLS, XLSX. Nebude-li možné zaslat doklad k úhradě elektronicky, zašle poskytovatel doklad na adresu:

    Česká národní banka
    sekce rozpočtu a účetnictví
    odbor účetnictví
    Na Příkopě 28
    115 03 Praha 1

11. Splatnost dokladů je 14 dnů ode dne jejich doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch účtu poskytovatele.

12. Smluvní strany se dohodly, že objednatel je oprávněn započíst jakoukoli svou peněžitou pohledávku za poskytovatelem, ať splatnou či nesplatnou, oproti jakékoli peněžité pohledávce poskytovatele za objednatelem, ať splatné či nesplatné.

Článek VI
Mlčenlivost, bezpečnostní požadavky objednatele

1. Poskytovatel se zavazuje zajistit, že jeho pracovníci či poddodavatelé a jejich pracovníci, kteří se budou na plnění podle této smlouvy podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se u objednatele seznámí a které nejsou veřejně dostupné.
2. Poskytovatel se zavazuje použít informace získané v souvislosti s plněním dle této smlouvy výhradně pro účely plnění této smlouvy.
3. Povinnost mlčenlivosti není časově omezena.
4. Poskytovatel, jeho pracovníci či poddodavatelé poskytovatele a jejich pracovníci se zavazují v plném rozsahu dodržovat bezpečnostní požadavky objednatele, které jsou uvedeny v přílohách č. 2 a 3 této smlouvy.

Článek VII
Odstraňování vad služby

1. V případě, že poskytování služby nebude odpovídat funkční specifikaci (příloha č. 1 a 2) nebo realizační studii (příloha č. 8) dle této smlouvy, půjde o vadu. Odstraněním vady se rozumí též poskytnutí řešení, které vykazuje z pohledu uživatele shodnou nebo obdobnou funkčnost.
2. Zjištěnou vadu oznamuje objednatel poskytovateli buď telefonem s následným potvrzením elektronickou poštou, nebo ohlášení provede prostřednictvím Help-deskového systému poskytovatele. Konkrétní kontaktní údaje budou uvedeny v komunikační matici uvedené v realizační studii (příloha č. 8).
3. Poskytovatel potvrdí příjem oznámení o vadě nejpozději do 4 hodin od jejího zaslání objednatelem. Vady mohou být odstraňovány jen v pracovní dny v době od 8:00 do 16:15 hodin a pracovníci poskytovatele jsou povinni vadu odstranit bez zbytečného odkladu, a to bez neodůvodněného přerušení v poskytování služby.
4. Kontaktní údaje uvedené v tomto článku mohou být měněny jednostranným oznámením (písemně nebo e-mailem) příslušné smluvní strany doručeným druhé smluvní straně.

Článek VIII
Smluvní pokuty, úrok z prodlení

1. V případě prodlení poskytovatele v kterékoliv lhůtě uvedené v čl. III odst. 1 je objednatel oprávněn požadovat smluvní pokutu ve výši 1 000 Kč za každý den prodlení. To neplatí, pokud k prodlení poskytovatele došlo z důvodů na straně objednatele.
2. V případě prodlení poskytovatele ve lhůtě uvedené v bodě 2. písm. b) přílohy č. 2 je objednatel oprávněn požadovat smluvní pokutu ve výši 2000 Kč za každou i započatou hodinu prodlení, nejvýše však 48 000 Kč za měsíc.
3. V případě porušení povinnosti stanovené v bodě 3. písm. a) přílohy č. 2 je objednatel oprávněn požadovat smluvní pokutu ve výši 5 000 Kč za každé takové porušení.
4. V případě porušení kterékoliv povinnosti poskytovatele, která bude předmětem písemného dodatku dle čl. XI odst. 3, poskytovatelem, je objednatel oprávněn požadovat smluvní pokutu ve výši 20 000 Kč za každé jednotlivé porušení.

5. V případě prodlení poskytovatele ve lhůtě stanovené v čl. VII odst. 3 je objednatel oprávněn požadovat smluvní pokutu ve výši 500 Kč za každou i započatou hodinu.
6. V případě prodlení objednatele s uhrazením daňového dokladu je poskytovatel oprávněn požadovat úrok z prodlení podle předpisů občanského práva.
7. V případě porušení povinnosti mlčenlivosti pracovníky poskytovatele či jeho poddodavatele dle čl. VI má objednatel právo požadovat smluvní pokutu ve výši 20 000,- Kč za každý jednotlivý zjištěný případ porušení této povinnosti.
8. V případě prodlení poskytovatele se splněním smluvní povinnosti ve stanovené lhůtě dle čl. XI odst. 2 smlouvy se poskytovatel zavazuje zaplatit objednateli smluvní pokutu ve výši 500,- Kč za každý den prodlení.
9. Smluvní pokuta a úrok z prodlení jsou splatné do 14 dnů od doručení dokladu k úhradě povinné smluvní straně. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu povinného ve prospěch účtu oprávněného.
10. Smluvní pokutou není dotčen nárok na náhradu škody. Případná odpovědnost poskytovatele za škodu způsobenou neplněním povinností vyplývajících z této smlouvy je omezena celkovou částkou ve výši 20 000 000,- Kč, kterou smluvní strany považují za předvídatelnou škodu.

Článek IX
Trvání a výpověď smlouvy, odstoupení od smlouvy, zrušení smlouvy zaplacením odstupného

1. Smlouva se uzavírá na dobu neurčitou.
2. Smlouvu lze ukončit písemnou výpovědí bez uvedení důvodu. Výpovědní doba činí v případě objednatele 3 měsíce, v případě poskytovatele 6 měsíců. Výpovědní doba počíná běžet prvním dnem kalendářního měsíce následujícího po doručení písemné výpovědi druhé smluvní straně. Poskytovatel může vypovědět smlouvu nejdříve za 2 roky od zahájení poskytování služby.
3. Smluvní strany se dohodly, že objednatel je oprávněn kdykoliv v průběhu insolvenčního řízení zahájeného na majetek poskytovatele vypovědět tuto smlouvu, a to ve 14 denní výpovědní době, která počíná běžet dnem následujícím po doručení písemné výpovědi poskytovateli.
4. Poruší-li kterákoliv strana podstatným způsobem závazky vyplývající z této smlouvy, má druhá strana právo odstoupit od smlouvy, a to písemným oznámením o odstoupení. Takové odstoupení je účinné dnem doručení oznámení druhé smluvní straně. Za podstatné porušení smlouvy strany považují zejména tyto případy:
   a) poskytovatel je v prodlení v kterékoliv lhůtě uvedené v článku III odst. 1 této smlouvy delším než 30 dnů,
   b) neuzavření, ukončení nebo porušení podmínek sjednaných ve smlouvě o zpracování osobních údajů,
   c) objednatel je v prodlení s úhradou kterékoliv platby dle této smlouvy delším než 30 dnů.
5. V souladu s ust. § 1992 OZ si smluvní strany sjednávají, že objednatel je oprávněn zrušit tuto smlouvu zaplacením odstupného ve výši 50 000,- Kč na účet poskytovatele, a to

kdykoliv před akceptací realizační studie (1. etapa). Zrušení smlouvy je účinné zaplacením sjednaného odstupného na bankovní účet poskytovatele, č. ú.: 19-2271190247/0100 Zaplacením odstupného zanikají všechna práva a povinnosti obou smluvních stran vyplývající ze zrušené smlouvy s výjimkou závazku mlčenlivosti poskytovatele.

Článek X
Uveřejnění smlouvy a skutečně uhrazené ceny za plnění smlouvy

1. Poskytovatel si je vědom zákonné povinnosti objednatele uveřejnit na svém profilu tuto smlouvu včetně všech jejích případných změn a dodatků a výši skutečně uhrazené ceny za plnění této smlouvy.
2. Profilem objednatele je elektronický nástroj, prostřednictvím kterého objednatel, jako veřejný zadavatel dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „ZZVZ") uveřejňuje informace a dokumenty ke svým veřejným zakázkám způsobem, který umožňuje neomezený a přímý dálkový přístup, přičemž profilem objednatele v době uzavření této smlouvy je https://ezak.cnb.cz/.
3. Povinnost uveřejňování dle tohoto článku je objednateli uložena § 219 ZZVZ.
4. Uveřejňování bude prováděno dle ZZVZ a příslušného prováděcího předpisu k ZZVZ.

Článek XI
Ostatní ujednání

1. Poskytovatel je povinen mít po dobu účinnosti této smlouvy uzavřeno pojištění pro případ vzniku odpovědnosti za škodu způsobenou v souvislosti s plněním této smlouvy, a to s pojistným plněním ve výši nejméně 20 000 000 Kč (slovy: dvacet milionů korun českých) a jeho spoluúčast nepřevyšuje 5 %.
2. Poskytovatel se zavazuje, že pojištění v uvedené výši a rozsahu zůstane účinné po celou dobu účinnosti této smlouvy, a do 5 pracovních dnů od výzvy objednatele je poskytovatel povinen toto objednateli prokázat.
3. Smluvní strany se zavazují uzavřít písemný dodatek k této smlouvě, jehož předmětem bude úprava a doplnění práv a povinností smluvních stran vyplývajících z nově připravované vyhlášky o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), a to bez zbytečného odkladu poté, co předmětná vyhláška nabyde platnosti. Neuzavření tohoto dodatku v souladu s vyhláškou o kybernetické bezpečnosti je důvodem pro odstoupení objednatele od smlouvy.
4. Použije-li poskytovatel při své činnosti poddodavatele, nahradí škodu jím způsobenou, jakoby ji způsobil sám.
5. Poskytovatel je povinen:
   5.1 v souladu s ust. § 105 odst. 3 ZZVZ poskytnout objednateli identifikační údaje všech poddodavatelů, kteří nebyli identifikováni dle věty první uvedené v § 105 odst. 3 ZZVZ a kteří se následně zapojí do plnění předmětu dle této smlouvy, a to nejpozději před zahájením plnění předmětu dle této smlouvy poddodavatelem,

5.2 mít po celou dobu účinnosti této smlouvy platný certifikát ČSN ISO/IEC 27001:2014 (či jiný rovnocenný certifikát nebo doklad), který objednatel požadoval v zadávacích podmínkách zadávacího řízení na předmět této smlouvy. Poskytovatel je povinen kdykoliv po dobu účinnosti této smlouvy na požádání objednateli tuto skutečnost doložit, a to do 5 pracovních dnů ode dne doručení požadavku objednatele,

5.3 zajistit, aby jeho pracovníci, kteří se budou podílet na plnění této smlouvy, splňovali kvalifikační kritéria, která objednatel požadoval v kvalifikačních požadavcích zadávacího řízení na předmět této smlouvy. Poskytovatel je po dobu účinnosti této smlouvy povinen na požádání kvalifikaci jednotlivých osob objednateli doložit, a to do 5 pracovních dnů ode dne doručení požadavku objednatele. Změna v těchto osobách může být provedena pouze se souhlasem objednatele, a to po prokázání splnění kvalifikačních požadavků objednatele ve stejném rozsahu, jaký byl stanoven v zadávací dokumentaci veřejné zakázky na poskytování služeb uvedených v této smlouvě. Odsouhlasení změny osoby bude provedeno e-mailem alespoň jednou kontaktní osobou objednatele, bez povinnosti uzavřít dodatek k této smlouvě.

5.4 V případě poskytování služeb prostřednictvím poddodavatele platí všechna ustanovení tohoto článku také pro poddodavatele a jeho pracovníky, kteří se budou na plnění smlouvy podílet. V případě, že poskytovatel splnil některý z požadavků stanovených objednavatelem v zadávací dokumentaci zadávacího řízení na předmět této smlouvy prostřednictvím poddodavatele, je povinen v případě změny tohoto poddodavatele požádat objednatele o souhlas a prokázat, že nový poddodavatel tento požadavek splňuje, a to do 5 pracovních dnů přede dnem zahájení poskytování plnění dle této smlouvy poddodavatelem. Odsouhlasení změny poddodavatele bude provedeno e-mailem alespoň jednou kontaktní osobou objednatele, bez povinnosti uzavřít dodatek k této smlouvě,

5.5 Za plnění poskytovaná poddodavatelem je poskytovatel odpovědný jako by toto plnění poskytoval sám. Poskytovatel se zavazuje, že poskytne objednateli, pokud bude i část plnění poskytována poddodavatelem, seznam kontaktních údajů na osoby provádějící plnění za poddodavatele. Objednatel je oprávněn průběh plnění realizovaný poddodavatelem řešit napřímo s jeho pracovníky a poskytovatel není oprávněn tuto komunikaci s poddodavatelem či jeho pracovníky jakkoliv omezovat nebo mařit.

Nesplnění kteréhokoliv požadavku objednatele uvedeného v odst. 5.1 až 5.5 je považováno za podstatné porušení smlouvy.

6. Poskytovatel se zavazuje, že nebude využívat plnění pro objednatele (resp. označení České národní banky) jako veřejně dostupnou referenci bez předchozího písemného souhlasu objednatele.

Článek XII
Závěrečná ustanovení

1. Tuto smlouvu lze měnit pouze dohodou smluvních stran písemným dodatkem, není-li ve smlouvě stanoveno jinak.
2. Smluvní strany se dohodly, že případný spor, který vznikne z této smlouvy nebo v souvislosti s ní, bude rozhodován výlučně podle českého práva obecnými soudy v České republice.
3. Tato smlouva je sepsána v českém jazyce. Veškerá komunikace mezi smluvními stranami vztahující se k této smlouvě bude probíhat v českém nebo slovenském jazyce, nebude-li smluvními stranami v konkrétním případě dohodnuto jinak.
4. Práva a povinnosti vzniklé z této smlouvy mohou být postoupena pouze po předchozím písemném souhlasu druhé smluvní strany. Za písemnou formu se nepovažuje e-mail či jiné elektronické zprávy.
5. Odpověď stran této smlouvy podle § 1740 odst. 3 občanského zákoníku s dodatkem nebo odchylkou není přijetím nabídky, ani když podstatně nemění podmínky nabídky.
6. Uplatnění domněnky doby dojití dle § 573 občanského zákoníku se vylučuje.
7. V případě rozporu mezi některými ustanoveními smlouvy a jejími přílohami se smluvní strany dohodly na tom, že přednost má smlouva.
8. Tato smlouva je vyhotovena ve čtyřech stejnopisech s platností originálu, z nichž objednatel obdrží tři stejnopisy a poskytovatel jeden stejnopis.
9. Smlouva nabývá platnosti a účinnosti dnem podpisu oprávněnými zástupci obou smluvních stran.

Přílohy:

Příloha č. 1	Podrobný popis parametrů služby
Příloha č. 2	Technické požadavky objednatele
Příloha č. 3	Bezpečnostní požadavky objednatele
Příloha č. 4	Ujednání o zpracování osobních údajů
Příloha č. 5	Cenová tabulka
Příloha č. 6	Šablona realizační studie
Příloha č. 7	Popis systémového prostředí objednatele
Příloha č. 8	Realizační studie (volně připojená příloha)

V Praze dne: 5. 10. 2018

Za objednatele:

[redacted]

Ing. Vladimír Mojžíšek
ředitel sekce informatiky

[redacted]

Ing. Zdeněk Virius
ředitel sekce správní

[redacted]

ČESKÁ NÁRODNÍ BANKA
Na Příkopě 28, 115 03 Praha 1
48

V Praze dne: 2. 10. 2018

Za poskytovatele:

[redacted]

Radek Podzemský
na základě pověření

[redacted]

T-Mobile Czech Republic a.s.
Tomíčkova 2144/1
149 00 Praha 4
IČ: 649 49 681, DIČ: CZ64949681

Příloha č. 1

Podrobný popis parametrů služby

Obsah

1 Úvod

Oblast bezpečnosti je výrazně rostoucím tématem, které díky zvyšující se mobilitě a elektronizaci veškerých dat a informací, nabývá klíčového významu. V souvislosti s tímto trendem dochází v celé řadě společností ke změně pohledu a přístupu k řízení informační bezpečnosti.

T-Mobile, jako klíčový ISP poskytovatel a komunikační společnost poskytující komplexní ICT služby, v návaznosti na tento trend vytvořil koncept nazvaný Bezpečná firma (Secure company), jehož cílem je rozvíjet schopnosti T-Mobile v oblasti služeb informační bezpečnosti a to především v oblastech konzultace, zabezpečení síťové a aplikační vrstvy a prostředí koncových stanic.

Nedílnou součástí konceptu Bezpečná firma je oblast bezpečnostního dohledu, který se v důsledku rostoucí hrozby kybernetické kriminality a jejích dopadů, stává nutností pro celou řadu firem.

Vybudování vlastního centra bezpečnostního dohledu, často nazývaného jako SOC – Security Operation Center, je pro většinu středních a větších firem neefektivní cíl a to především s ohledem na vysoký provozní náklad, související s nutností zajištění vyškolených bezpečnostních specialistů s potřebnou zkušeností a jejich kontinuálního rozvoje.

Jako řešení se nabízí služba sdíleného SOC na úrovni ISP a ICT poskytovatele služeb. Zákazník přitom platí za určité služby SOC, které si vybere z katalogu služeb a to v rozsahu, který je poplatný jeho aktuální potřebě.

Vzhledem k výraznému vývoji bezpečnostních hrozeb a s ní související rostoucí poptávce po službách z oblasti informační bezpečnosti, se T-Mobile rozhodnul vytvořit svůj vlastní specializovaný SOC tým, který se věnuje výhradně dohledu bezpečnostních služeb, a jeho schopnosti nabízet jako součást svých služeb. Nepopiratelnou výhodou tohoto řešení je skutečnost, že se členové SOC týmu věnují svou pozornost jen a pouze problematice informační bezpečnosti, což jim umožňuje získat v této oblasti potřebnou odbornost a zkušenosti a tyto neustále rozvíjet.

Vytvoření dedikovaného SOC týmu poskytuje T-Mobile významnou výhodu proti konkurenci, která má funkci bezpečnostního dohledu ve většině případů koncipovánu jako sdílenou v rámci týmu síťového dohledu.

2 Pojmy a zkratky

Pojem	Vysvětlení
Alert	Emailová notifikace systému SIEM, která informuje o podezření na detekovonou KBU/KBI
B2B IT SMC	B2B IT SMC (Service Management Center) – interní označení týmů specialistů v T-Mobile, zahrnuje rovněž tým NOC (Network Operation Center)
Interní nástroj T-Mobile	Pro potřeby projektu bude použit nástroj WFM.
Kybernetická bezpečnostní událost (KBU)	Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.
Kybernetický bezpečnostní incident (KBI)	Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.
NOC	NOC (Network Operations Center) - Dohledové centrum - tým specialistů, kteří poskytují služby dohledu.
Provozní událost	Provozní událost nemá vlastnosti kybernetického bezpečnostního incidentu, tj. provozní událost není způsobena kybernetickou bezpečnostní hrozbou a/nebo kybernetickou bezpečnostní zranitelností.
Provozovatel	Provozovatelem informačního nebo komunikačního systému orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém.
SIEM	SIEM (Security Information and Event Management) – management bezpečnostních informací a událostí zabývající se dlouhodobým ukládáním událostí, jejich analýzou a hlášením problémů i monitoringem infrastruktury, korelacemi událostí a upozorňováním v reálném čase.
SOC	SOC (Security Operation Center) - Dohledové centrum bezpečnosti - tým specialistů, kteří poskytují služby specializující se na bezpečnostní dohled.

3 Základní popis služby SOC

Hlavní činností SOC týmu je proaktivní dohled nad chráněnými objekty z pohledu nestandardního provozu, samostatné řešení incidentních stavů, komunikace se zákazníky a dalšími složkami systému kybernetické ochrany (např. CERT).
Na základě bezpečnostní události, která se vyskytne v síti konkrétního zákazníka, SOC provádí činnosti v souladu s předem domluveným postupem, případně se proaktivně spojí se zákazníkem a sladí se s ním na dalším postupu řešení. SOC zajišťuje služby v reakčních časech, které jsou definovány v rámci SLA služby.
Základem SOC týmu je skupina operátorů, která zajišťuje službu L1 supportu bezpečnostního dohledu v režimu 24x7x365. Tato skupina je proškolena na problematiku síťového provozu a služeb, administraci síťových a bezpečnostních prvků, velmi dobře rozumí problematice kybernetických útoků, má velmi dobré analytické a kombinační schopnosti a proaktivní zákaznickou orientaci.
V případě, že si L1 support s danou bezpečnostní situací nedokáže poradit sám (za pomocí aktivace předem domluvených scénářů), eskaluje problém na L2 support z týmu technologické bezpečnosti. V případě nutnosti existuje pro L2 support tým smluvní možnost kontaktovat přímo dodavatele dotčených bezpečnostních technologií pro řešení HW problémů nebo L3 podporu výrobce.
SOC tým jako celek disponuje certifikacemi CCNP, CCNA a celou řadou certifikací, týkající se konkrétních bezpečnostních produktů (Arbor Networks, Fortinet, Cisco, CheckPoint, F5, HP ArcSight, IBM Q Radar, FlowMon…).
SOC je v režimu 24x7x365 dostupný na vyhrazeném telefonu či mailu pro případ, že zákazník zaznamená nějakou bezpečnostní událost sám a potřebuje jí ve spolupráci se SOC týmem řešit.
Témata, kterými se SOC tým často zabývá, jsou především problematika bezpečnosti sítí, internetové útoky typu DDoS (pomalé aplikační útoky, volumetrické útoky), útoky na web a SQL, problematika BOT sítí a CCC.
SOC rozesílá zákazníkům upozornění na výskyt botnet stanic a na „podezřelou komunikaci“. Každý měsíc řeší desítky DDoS alarmů jak pro zákaznické tak i pro interní cíle T-Mobile.
Úkolem SOC týmu je reagovat na zachycené události dle předem dohodnutého postupu, průběžně sledovat statistiku zachycených událostí a na základě zkušeností navrhovat případnou úpravu korelačních pravidel s cílem minimalizovat false-positive alarmy.

4 Rozsah nabízené služby

Předmětem nabídky je služba T-Mobile SOC zahrnující:

a) nepřetržitý vzdálený dohled/monitoring bezpečnostních událostí s využitím systému SIEM objednatele, a to 24 hodin denně 7 dnů v týdnu po celý rok,

b) analýzu bezpečnostních událostí (KBU) zachycených systémem SIEM objednatele, včetně návrhu na protiopatření (řešení),

c) upozornění objednatele na zjištěné bezpečností incidenty (KBI) dle jejich závažnosti a v této smlouvě dohodnuté komunikační matice,

d) poskytování pravidelného měsíčního reportu zabezpečeným způsobem (bude definitivně stanoven v realizační studii),

e) poskytování konzultačních služeb při případné úpravě pravidel, reportů a filtrů pro systém SIEM objednatele.

5 Klíčové výhody nabízené služby

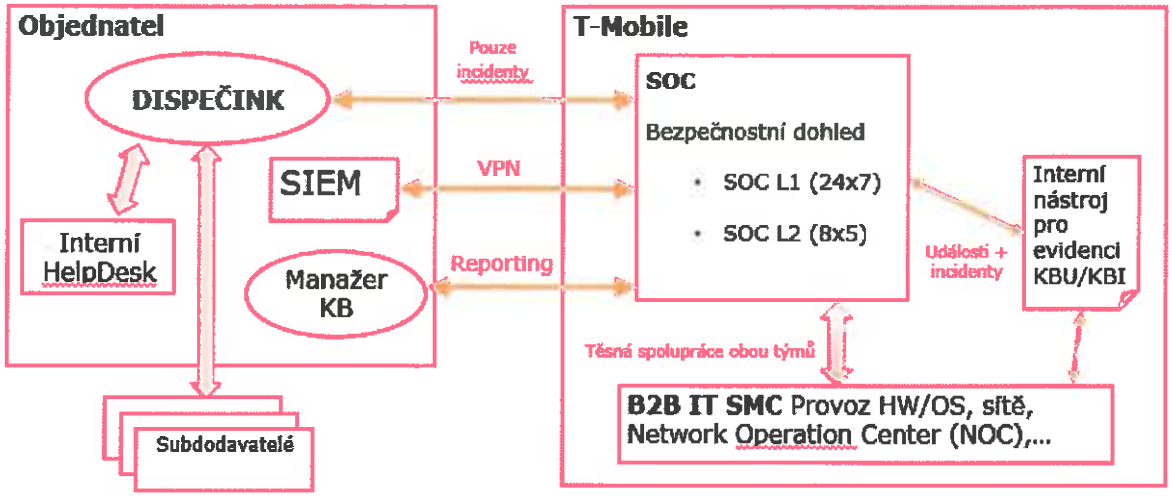
- zajišťuje analýzu dat generovaných při provozu podnikových systémů, která umožňuje rychlé rozpoznání nových hrozeb, útoků a porušení bezpečnostních pravidel.
- Vyskytne-li se narušení bezpečnosti nebo porušení definované bezpečnostní strategie, integrovaný pracovní postup metod nápravy umožňuje správcům IT okamžitě reagovat na základě předem určených úloh, regulačních požadavků a obchodní strategie.
- Technická a provozní podpora 24×7×365
- Garance SLA
- Vysoká kompetence a dlouholetá zkušenost
- Garance dlouhodobé stability a dalšího rozvoje Služby

6 Návrh organizace týmu pro řízení KBU/KBI

Tento odstavec popisuje návrh organizace týmu pro řízení KBU/KBI s ohledem na požadavky objednatele. Tento návrh bude upraven na základě informací získaných v rámci realizační studie.
Na zvládání identifikovaných a nahlášených KBU/KBI v projektu Zajištění bezpečnostního dohledu se podílí:

1. Dispečink objednatele.
2. SOC úrovně L1 až L2.
3. Manažer KB objednatele nebo pověřený zástupce.
4. Provozovatelé a subdodavatelé.

Organizační schéma týmu pro řízení KBU/KBI zachycuje obrázek níže s tím, že jednotlivé role a jejich zodpovědnosti jsou blíže popsány dále.



Obrázek 1: Návrh organizace týmu pro řízení KBU/KBI

6.1 Dispečink objednatele

Dispečink objednatele zajišťuje komunikaci mezi objednatelem a SOC v situacích, kdy je v souvislosti s výskytem a řešením KBU/KBI:

- potřeba objednatele informovat o vzniklé situaci bezodkladně,
- nutná rychlá reakce objednatele a zainteresovaných stran (subdodavatelů a/nebo provozovatelů),
- potřeba rozhodnutí odpovědných osob i mimo pracovní dobu

V procesu zvládání KBU/KBI

- přijímá hlášení o KBU/KBI od SOC a eviduje je v interním nástroji pro evidenci KBU/KBI.
  - SOC předává dispečinku objednatele informace o KBI e-mailem, SMS a telefonicky.

6.2 Manažer KB objednatele

Manažer KB objednatele v procesu zvládání KBU/KBI vyhodnocuje hlášení o KBU/KBI.
Manažer KB objednatele může pověřit výkonem odpovědností uvedených v tomto dokumentu pověřenou osobu (zástupce).
Dispečink objednatele předává Manažerovi KB objednatele hlášení o výskytu KBU/KBI telefonicky nebo prostřednictvím interního nástroje pro evidenci KBU/KBI.
SOC předává Manažerovi KB objednatele hlášení o výskytu KBI telefonicky, prostřednictvím SMS, nebo e-mailu.

Manažer KB objednatele je odpovědný za:

- konečnou klasifikaci KBU/KBI,
- klíčová rozhodnutí v procesu řešení KBU/KBI,
- hlášení KBI NÚKIB,
- sledování varování a reaktivních opatření vydaných NÚKIB.

6.3 Security Operation Center (SOC)

SOC je provozován společností T-Mobile. SOC zajišťuje detekci, sběr a vyhodnocování KBU/KBI dostupnými technickými prostředky a vyhodnocování úrovně dostupnosti vybraných prostředků prostřednictvím implementovaných nástrojů, především prostřednictvím SIEM objednatele.
SOC v rámci procesu zvládání KBU/KBI:

1. registruje ohlášené KBU v interním nástroji T-Mobile,
2. řeší KBU dle předem definovaných provozních scénářů
3. navrhuje klasifikaci KBU Manažerovi KB objednatele,
4. informuje Manažera KB objednatele o výskytu KBI,
5. provádí rekvalifikaci KBU na provozní události a předává je k řešení dle procesu pro provozní události tj. řešení standardních poruchových stavů,
6. na základě výzvy ISIRT poskytuje potřebnou součinnost při investigaci závažných KBI.

T-Mobile SOC se skládá z týmů popsaných v tabulce níže.

Tým	Popis činnosti týmu
SOC L1	SOC L1 poskytuje podporu 24/7. Provádí monitoring vybraných prostředků. SOC L1 postupuje dle předem schváleného postupu pro řešení KBU. Operátoři SOC L1 mají předem definované odpovědnosti v provozních scénářích. Operátoři SOC L1 provádí tyto činnosti: • Sledují SIEM konzoli a při výskytu KBU tyto řeší na základě definovaných provozních scénářů. • Monitorují stav bezpečnostních nástrojů (dostupnost komponent SIEM objednatele) • Komunikuji a konzultují další postup (nedefinovaný postup v provozním scénáři) se SOC L2, dispečinkem objednatele nebo s Manažerem KB objednatele. KBU v kompetenci SOC L1 jsou registrovány a administrovány v interním nástroji T-Mobile.
SOC L2	SOC L2 řeší KBU/KBI, které byly eskalovány ze SOC L1 v režimu 24x7. SOC L2 poskytuje konzultační podporu objednateli v režimu 8x5. Operátoři SOC L2 jsou specialisté týmu kybernetické bezpečnosti T-Mobile. Poskytují přímou podporu pro SOC L1 při kategorizaci KBU/KBI, dokumentaci standardních interních postupů pro řešení KBU a KBI, řešení nestandardních KBU, reportingu, analýze reportů, návrhu systematických opatření, analýze KBU/KBI a návrhů jejich řešení. SOC L1 zadává požadavky na SOC L2 prostřednictvím interního nástroje T-Mobile. Specialisté SOC L2 provádí tyto činnosti: • Ověřují KBU/KBI reportované SOC L1 • Ve spolupráci s Manažerem KB objednatele nastavují procesní a komunikační postupy SOC. • Vytvářejí dohodnuté pravidelné reporty pro Manažera KB objednatele. • Navrhují aktualizace pravidel pro logování a dohled v SIEM objednatele.

7 Zřízení služby

Tato kapitola popisuje základní fáze přípravných činností, které budou provedeny v rámci zřízení služby.

7.1 Realizační studie

Cílem fáze realizační studie je zajištění detailní analýzy požadavků objednatele a navrženého řešení služby poskytovatelem s cílem ověřit realizovatelnost nabízené služby v podmínkách objednatele, ověřit a dokladovat soulad s požadavky objednatele, podrobně specifikovat technickou realizaci služby a případně identifikovat technické problémy či dosud neidentifikované změny a požadavky, které by vznikly v souvislosti s implementací a provozováním služby v prostředí objednatele.
Realizační studie v sobě zahrnuje zejména následující činnosti:

i) seznámení odborných pracovníků poskytovatele s výpočetním prostředím ČNB, kritičností jednotlivých dozorovaných IS a aplikací,

j) seznámení se s konfigurací systému SIEM objednatele (reporty, alerty, pravidla, korelace, atd.),

k) návrh případné úpravy pravidel v SIEM objednatele formou balíčků pro nástroj HP ArcSight nebo připravených filtrů s podrobným popisem jejich implementace a připojení nových zdrojů událostí, je-li to potřeba pro zajištění kvality poskytované služby,

l) definování způsobů vzájemné komunikace obou smluvních stran (komunikační matice) a eskalace,

m) definování struktury a obsahu měsíčního reportu,

n) vytvoření realizační studie,

o) ve spolupráci obou smluvních stran akceptaci realizační studie,

p) uzavření ujednání o zpracování osobních údajů

7.2 Implementace a ověřovací provoz

Cílem této fáze je technické zprovoznění služby spočívající v potřebné konfiguraci zabezpečeného vzdáleného přístupu (dále jen „VPN“) a systému SIEM v prostředí objednatele a instalaci a konfiguraci VPN v prostředí poskytovatele, dále pak nastavení a aktivaci monitorovacích a reportovacích procesů, a to vše v souladu s akceptovanou realizační studií. Součástí této etapy je i jednoměsíční poskytování služby – ověřovací provoz.
Tato fáze zahrnuje následující činnosti:

a) zajištění přístupů jednotlivých pracovníků poskytovatele, kteří se budou podílet na poskytování služby

b) aktivace přístupů do webové konzole SIEM objednatele formou VPN,

c) předání certifikátů pracovníkům poskytovatele na jejich vlastní čipovou kartu (token) pro zajištění bezpečného přihlášení ke konzoli SIEM objednatele prostřednictvím VPN,

d) zprovoznění VPN u poskytovatele dle návodu od objednatele,

e) úprava pravidel v SIEM objednatelem, dle doporučení a podrobného návodu poskytovatele uvedeného v realizační studii,

f) poskytování služeb po dobu jednoho měsíce (dále jen „ověřovací provoz“),

g) ve spolupráci obou smluvních stran akceptaci měsíčního reportu ověřovacího provozu.

7.3 Předpoklady a podmínky realizace

Nezbytným předpokladem nasazení a poskytování služby SOC je dostatečná součinnost ze strany objednatele, a to zejména:

- včasné poskytnutí potřebných informací a podkladů
- zajištění a poskytnutí potřebných lidských zdrojů
- organizační koordinace na straně objednatele a jeho dodavatelů
- organizační koordinace s jednotlivými členy projektového týmu na straně objednatele a jeho dodavatelů
- poskytnutí konzultací při ladění konfigurace SIEM a spolupráce při identifikaci false-positive událostí
- zajištění konfiguračních oken v souladu s harmonogramem
- aktivní spolupráce

Nesplnění výše uvedených požadavků či pozdržení dodání potřebných materiálů může mít negativní vliv na úspěšné a včasné dokončení projektu.
Pro úspěšnou realizaci v průběhu všech fází předpokládáme zapojení odborných specialistů, zejména pak:

- aplikační architekt/specialista znalý architektury aplikací
- specialista/analytik bezpečnosti informačních technologií

7.4 Orientační implementační plán

Tabulka níže zachycuje orientační implementační plán, který předpokládá dostatečnou součinnost ze strany zákazníka.

Aktivita	Termín dokončení
Podpis smlouvy	T0
Realizační studie - detailní analýza požadavků objednatele a navrženého řešení služby poskytovatelem s cílem ověřit realizovatelnost nabízené služby v podmínkách objednatele.	T0 + 2 týdny
Implementace - konfigurace VPN a systému SIEM v prostředí objednatele, nastavení a aktivace monitorovacích a reportovacích procesů.	T0 + 4 týdny
Ověřovací provoz - jednoměsíční poskytování služby	T0 + 8 týdnů
Finalizace dokumentace	T0 + 8 týdnů
Zahájení poskytování služby	T0 + 8 týdnů

8 Poskytování (provoz) služby

Měsíční poskytování (provoz) služby zahrnuje následující oblasti:

8.1 Monitoring a analýza bezpečnostních událostí

Monitoring a analýza bezpečnostních událostí je v rámci nabízené služby T-Mobile SOC zajišťován v následujícím rozsahu:

1. provádění nepřetržitého vzdáleného dohledu/monitoringu bezpečnostních událostí s využitím systému SIEM objednatele a to 24 hodin denně 7 dnů v týdnu po celý rok.
2. vyhodnocování alertů detekovaných systémem SIEM objednatele **do 2 hodin od jejich detekce**, tj. okamžiku zobrazení alertu v seznamu v konzoli SIEMu, bez ohledu na to zda a kdy došlo k zaslání nebo doručení avíza ze systému SIEM objednatele emailem.
3. V rámci vyhodnocování alertů rozhodnutí o tom, zda se z alertu stává KBU nebo KBI v definované kategorii kritický, střední, nízký), či se jedná o „false positive" alert, kterým se již obě smluvní strany dále nezabývají.
4. vyhodnocování závažnosti KBU/KBI s ohledem na důležitost jednotlivých technických aktiv (serverů, aktivních prvků, stanic, databází…), mj. klasifikaci provozovaných informačních systémů podle zákona o kybernetické bezpečnosti.
5. V případě vyhodnocení detekované události jako KBI, nebo v případě podezření na KBI a nebo to není jednoznačné, odeslání zprávy objednateli a pokračování dále v analýze.
6. Během analýzy KBI i po jejím ukončení informovat objednatele v souladu s komunikační a eskalační maticí o opatřeních, které je potřeba udělat v informačních systémech objednatele, aby se zamezilo útoku, minimalizovaly se škody. K tomu T-Mobile SOC poskytne potřebné související informace.
7. Neprodleně informovat objednatele o nově zjištěných podstatných skutečnostech.
8. Garance vyhodnocení **50 událostí** detekovaných systémem SIEM **za kalendářní měsíc**
9. Monitoring **výpadků zdrojů logů z kritických systémů** (určených v rámci Realizační studie) a v případě že je delší než **2 hodiny**, informuje o tom T-Mobile SOC objednatele dle komunikační matice.

8.1.1 Pravidla pro určení závažnosti KBI

Závažnost KBI	Popis	Komunikace
Kritický	Incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod.	Telefonicky a e-mailem
Střední	Incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření incidentu včetně minimalizace vzniklých škod.	Emailem a SMS
Nízký	Incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření bezpečnostního incidentu včetně minimalizace vzniklých škod.	Emailem

8.2 Reporting

Reporting v rámci nabízené služby T-Mobile SOC zahrnuje vytvoření a odeslání pravidelného měsíčního reportu s informacemi za předchozí měsíc do 5. dne v měsíci, přičemž tento report bude obsahovat:

- statistiku sbíraných událostí,
- počet alertů ze systému SIEM objednatele analyzovaných poskytovatelem
- seznam a způsob řešení zjištěných incidentů (KBI),
- seznam nových hrozeb, o kterých se poskytovatel dozvěděl se stručným popisem, případně odkazem na podrobnosti, pokud je k dispozici
- návrhy na vylepšení bezpečnostního monitoringu o další scénáře v systému SIEM (pravidla, reporty, apod.) tak, aby byl schopen reagovat na nové hrozby, případně zpřesnit detekci stávajících a to formou balíčků pro nástroj HP ArcSight (SIEM používaný objednatelem) nebo připravených filtrů s podrobným popisem jejich implementace,
- návrh na nastavení sběru logů z nových zdrojů, které jsou pro detekci KBI významné
  - vlastní sběr logů zajistí objednatel
- počet skutečně odpracovaných hodin v rámci konzultačních služeb, včetně podrobného rozpisu.
- návrh úpravy sběru logů systémem SIEM, který vyplyne z expertního posouzení logů tj. činnosti, která zahrnuje zejména:
  - Kontrolu úplnosti logů z jednotlivých zdrojů potřebných pro zajištění kvality služby,
  - vyhledávání anomálií v počtu a typu logů z jednotlivých zdrojů,
  - pravidelně se opakující chybové záznamy.

9 Komunikační pravidla a kontakty

Veškerá komunikace probíhá dle závažnosti KBI a komunikační matice.

9.1 Kontakty na T-Mobile Security Operation Center (SOC)

Tel.: +420 236 099 009, +420 225 988 366
Mobil.: +420 604 296 948
E-mail: SOC@t-mobile.cz

9.2 Eskalační matice v rámci T-Mobile SOC

Tato eskalační matice může být použita kdykoliv, když není Smluvní partner spokojen se standardní procedurou řešení.

Úroveň	1	2	3
Jméno	Shift responsible	Jan Veselý	Michal Trejbal
Pozice	Service Management Centre Analyst	Head of Service Management Center	Senior Head of SMC and access network
Telefon	+420 236 099 009	+420 225 255 654	+420 225 255 456
Mobilní telefon	+420 604 296 948	+420 777 770 073	+420 602 258 768
Fax	+420 236 099 888	--	--
E-mail	SOC@t-mobile.cz	Jan.Vesely3@t-mobile.cz	Michal.Trejbal@t-mobile.cz
Dostupnost	24x7	8x5	8x5

8x5 – dostupnost v pracovní dny od 9:00 do 17:00

9.3 Další kontakty

Role	Kontaktní informace
Dispečink objednatele/Specialisté objednatele	e-mail, telefon Eskalační kontakt
Manažer KB objednatele	e-mail, telefon
Zástupce manažera kybernetické bezpečnosti objednatele	e-mail, telefon

10 Příklady provozních scénářů T-Mobile SOC

Níže uvedená tabulka obsahuje příklady provozních postupů pro SOC pro vybrané KBU. Scénáře jsou koncipovány v souladu s interními postupy objednatele pro řešení KBU/KBI:

Označení scénáře	Dotčené aktivum	Velikost dopadu	Bezpečnostní událost	Popis činností SOC L1	SOC L1 vs. SOC L2	Ukončení řešení události	Událost vs. incident
S01	Všechna aktiva	Velké dopady	Všechny s velkým dopadem	Kontaktovat telefonicky dispečink objednatele a prověřit skutečnou velikost dopadů. Pokud je dopad potvrzen, dispečink objednatele informuje Manažera KB objednatele nebo kontaktuje koordinátora ISIRT. U KBU s jinými než velkými dopady, SOC L1 posoudí, zda se jedná o opakovanou KBU, na jejíž řešení již existuje provozní scénář. Pokud ano, postupuje podle příslušného scénáře. Pokud ne, SOC L1 postupuje podle scénáře S02.	SOC L1 konzultuje SOC L2 v případě potřeby.	SOC L1 založí záznam o KBU v interním nástroji T-Mobile a další činnost koordinuje s dispečinkem objednatele a SOC L2.	KBU s velkým dopadem jsou KBI.
S02	Všechna aktiva	Jiné než velké dopady	Nestandardní KBU, pro kterou není popsán proces řešení.	Zadat požadavek na identifikaci příčiny na B2B IT SMC. Pokud není potvrzen B2B IT SMC, předat na SOC L2. Lze konzultovat dispečink objednatele.	SOC L2 řeší dle aktuální situace a na základě best practice.	O způsobu uzavření KBU/KBI rozhodne SOC L2.	SOC L2 rozhodne o tom, zda se jedná o KBU, nebo KBI.

Označení scénáře	Dotčené aktivum	Velikost dopadu	Bezpečnostní událost	Popis činnosti SOC L1	SOC L1 vs. SOC L2	Ukončení řešení události	Událost vs. incident
S03	SIEM	Jiné než velké dopady	Od sledovaného prostředku nepřicházejí po dobu 24 hodin žádné logy.	Kontaktovat správce aktiva (Viz Příloha č. 2 - Seznam aktiv monitorovaných SIEM), zda se nejedná o výpadek HW/OS. Pokud ano, ověřit zda po odstranění poruchy dojde k obnově logování do SIEM. Pokud ne, začít analyzovat příčinu problému napříč dalšími řešitelskými skupinami network, SIEM)	SOC L1 informuje Manažera KB objednatele a SOC L2 e-mailem (viz šablona v Příloze č. 1) a telefonicky (v provozní době subjektů) o **výpadku SIEM.**	SOC L2 informuje Manažera KB objednatele o KBI okamžitě jen v případě ztráty logů apod.	V případě, že je výpadek logování spojen s nedostupností HW/OS (HW porucha, odstávka…), evidujeme nadále jako KBU. V opačném případě evidujeme jako KBI.
S04	Privilegované účty	Jiné než velké dopady	Překročení x neúspěšných pokusů o přihlášení následované jedním úspěšným v intervalu y min.	SOC L1 kontaktuje správce aktiva (Viz Příloha č. 2 - Seznam aktiv monitorovaných SIEM) a ten osobu evidovanou k danému účtu (lze konzultovat i s dispečinkem objednatele). Správce aktiva ověří, že daná osoba provádí uvedenou činnost. Pokud ne, zablokuje účet nebo ponechá účet zablokovaný. O výsledku ověření a provedených opatřeních informuje zpět SOC L1.	SOC L1 informuje Manažera KB objednatele a SOC L2 e-mailem (viz šablona v Příloze č. 1) a telefonicky (v provozní době subjektů) o **úspěšném útoku** na účet/účty.	SOC L2 s Manažerem o kybernetické bezpečnosti objednatele a rozhodnou dalším postupu.	V případě, že uvedenou činnost prováděla kontaktovaná osoba, eviduje nadále jako KBU. V opačném případě se z KBU stává KBI.

11 SLA parametry

Následující tabulka obsahuje přehled SLA parametrů nabízené služby.

Typ/Aktivita	Režim služby	Dostupnost služby	Reakce	Řešení
Potenciální útok/incident	24x7	99,99%	2 hodiny[1]	Bez zbytečného odkladu na základě postupu dle příslušného scénáře.
Odstraňování vad	24x7	99,99%	4 hodiny[2]	Bez zbytečného odkladu, a to bez neodůvodněného přerušení v poskytování služby. Vady mohou být odstraňovány jen v pracovní dny v době od 8:00 do 16:15 hodin

[1] Doba reakce je v případě „Potenciálního útoku/incidentu" počítána od okamžiku zobrazení alertu v seznamu v konzoli SIEMu, bez ohledu na to zda a kdy došlo k zaslání nebo doručení avíza poskytovateli ze systému SIEM objednatele.

[2] Doba reakce je v případě „Odstraňování vad" počítána od okamžiku doručení oznámení o vadě sjednaným způsobem poskytovateli ze strany objednatele.

12 Vyhodnocení a zlepšování procesu

12.1 Ad-hoc schůzky

Po každém bezpečnostním incidentu je svolána ad-hoc schůzka, které se zúčastní zástupci dotčených týmů s cílem zhodnotit průběh řešení incidentu a navrhnout případně nápravná opatření.

12.2 Pravidelné schůzky

Kvartálně je svolána schůzka zástupců všech týmů.

Cílem je rekapitulovat uplynulé období z pohledu

- Počtu standardních a nestandardních událostí (vyřešených na SOC vs. eskalovaných na podpůrné týmy)
- Délky řešení incidentů (plnění OLA, dopad do SLA)
- Počtu událostí v jednotlivých kategoriích (podklad pro Problem Management)

a dohodnout se na případných změnách (procesy, nástroje…)

12.3 Vzdělávání

Cílem je postupné rozšiřování SOC kompetencí tj. standardizace řešení opakujících se událostí.

13 Závěr

Ve společnosti T-Mobile Czech Republic jsme připraveni s vámi spolupracovat tak, abychom Vám poskytli nejlepší možné řešení, které bude optimálně vyladěné dle Vašich aktuálních potřeb a umožnilo budoucí růst Vaší firmy. Prosím, neváhejte nás kontaktovat pro jakékoliv vysvětlení nebo doporučení týkající se tohoto návrhu. Rádi Vám také poradíme alternativní řešení, které Vám můžeme nabídnout.

14 Přílohy

14.1 Příloha č. 1 – Šablona informačního e-mailu

Předmět	**KBU - Oznámení o výskytu kybernetického bezpečnostní události**
Objekt	Název zastřešujícího projektu objednatele
ID nebo jméno dotčeného aktiva	identifikace koncového zařízení, uživatelského účtu…, kterého se oznámení týká
Kybernetická bezpečnostní událost / incident	*Např.* Překročení x neúspěšných pokusů o přihlášení následované jedním úspěšným v intervalu y min. *nebo* Od sledovaného prostředku nepřicházejí po dobu 2 hodin žádné logy.
Datum vzniku události / incidentu	11. 11. 2011
Čas vzniku události / incidentu	19:40:50
Příjemce oznámení	Dispečink objednatele, Manažer KB objednatele
Odesílatel oznámení	SOC (T-Mobile Czech Republic, a.s.) Email, telefon

14.2 Příloha č. 2 - Seznam aktiv monitorovaných SIEM

ID	Hostname	IP Address	Správce
1	Hostname01	IPv4, IPv6	Email, telefon
...			

Příloha č. 2

Technické požadavky objednatele

Níže jsou uvedeny základní věcné funkční požadavky na poptávanou službu SOC. Z pohledu objednatele se jedná o nejdůležitější požadavky, které mají umožnit splnit cíle uvedeného v preambuli této smlouvy.

U každého požadavku je uveden jak jeho název a definice dle objednatele, tak i popis tohoto požadavku. Dále jsou pak případně uvedeny konkrétní komponenty či produkty, které by dle objednatele umožňovaly splnění daných požadavků.

U všech požadavků se jedná o závazné požadavky.

1. Definice, akronymy a zkratky

Zkratka/Termín	Popis/Definice
Alert	Emailová notifikace systému SIEM, která informuje o podezření na detekovonou KBU/KBI
KBU	Kybernetická bezpečnostní událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.
KBI	Kybernetický bezpečnostní incident je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události. KBI vzniká po analýze pouze z některých KBU.
SOC	Security operations center zajišťující monitoring bezpečnostních událostí, jejich analýzu a návrh protiopatření k detekovaným událostem. V případě ČNB externí SOC neobsahuje reakční složku, tu stále zajišťuje ČNB.
SIEM	Security Information and Event Management. Management bezpečnostních informací a událostí, jejich monitoring a vyhodnocování.

2. Požadavky na monitoring a analýzu bezpečnostních událostí

a) Poskytovatel provádí nepřetržitý vzdálený dohled/monitoring bezpečnostních událostí s využitím systému SIEM objednatele a to 24 hodin denně 7 dnů v týdnu po celý rok.
b) Poskytovatel vyhodnocuje alerty detekované systémem SIEM objednatele do 2 hodin od jejich detekce, tj. okamžiku zobrazení alertu v seznamu v konzoli SIEMu, bez ohledu na to zda a kdy došlo k zaslání nebo doručení avíza ze systému SIEM objednatele emailem poskytovateli.
c) Do doby dle bodu b) rozhoduje Poskytovatel o tom, zda se z alertu stává KBU nebo KBI v definované kategorii, či se jedná o „false positive" alert, kterým se již obě smluvní strany dále nezabývají.
    a. Při vyhodnocování závažnosti KBU/KBI poskytovatel zohledňuje důležitost jednotlivých technických aktiv (serverů, aktivních prvků, stanic, databází…), mj. klasifikaci provozovaných informačních systémů podle zákona o kybernetické bezpečnosti.

b. V případě vyhodnocení detekované události jako KBI, nebo v případě podezření na KBI a nebo to není jednoznačné, odešle poskytovatel objednateli zprávu a pokračuje dále v analýze. O nově zjištěných podstatných skutečnostech neprodleně informuje objednatele.

d) Během analýzy KBI i po jejím ukončení, poskytovatel informuje objednatele v souladu s komunikační a eskalační maticí o opatřeních, které je potřeba udělat v informačních systémech objednatele, aby se zamezilo útoku, minimalizovaly škody, případně další související informace.

e) Poskytovatel musí garantovat vyhodnocení minimálně 50 událostí detekovaných systémem SIEM za kalendářní měsíc

f) Poskytovatel monitoruje výpadky zdrojů logů z kritických systémů (určené v Realizační studii) a v případě že je delší než 2 hodiny, informuje o tom objednatele dle komunikační matice v Realizační studii.

g) Veškerá komunikace probíhá dle závažnosti KBI a komunikační matice.

Pravidla pro určení závažnosti bezp. incidentu (KBI)

Závažnost bezp. incidentu	Popis	Komunikace
Kritický	Incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod.	Telefonicky a e-mailem
Střední	Incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření incidentu včetně minimalizace vzniklých škod.	Emailem a SMS
Nízký	Incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření bezpečnostního incidentu včetně minimalizace vzniklých škod.	Emailem

3. Požadavky na pravidelný měsíční report

a) Poskytovatel odešle objednateli do 5. dne v měsíci report s informacemi za předchozí měsíc.

b) Report bude obsahovat minimálně:
- statistiku sbíraných událostí,
- počet alertů ze systému SIEM objednatele analyzovaných poskytovatelem
- seznam a způsob řešení zjištěných incidentů (KBI),

- seznam nových hrozeb, o kterých se poskytovatel dozvěděl se stručným popisem, případně odkazem na podrobnosti, pokud je k dispozici
- návrhy na vylepšení bezpečnostního monitoringu o dalších scénáře v systému SIEM (pravidla, reporty, apod.) tak, aby byl schopen reagovat na nové hrozby, případně zpřesnit detekci stávajících a to formou balíčků pro nástroj HP ArcSight (v ČNB používaný SIEM) nebo připravených filtrů s podrobným popisem jejich implementace,
- návrh na nastavení sběru logů z nových zdrojů, které jsou pro detekci KBI významné, vlastní sběr zajistí objednatel
- počet skutečně odpracovaných hodin plnění dle čl. 1 odst. e), včetně podrobného rozpisu
- návrh úpravy sběru logů systémem SIEM, který vyplyne z expertního posouzení logů dle odst. 3c) této přílohy

c) Poskytovatel provede expertní posouzení logů v SIEM, které zahrnuje zejména:
   a. Kontrolu úplnosti logů z jednotlivých zdrojů potřebných pro zajištění kvality služby,
   b. vyhledávání anomálií v počtu a typu logů z jednotlivých zdrojů,
   c. pravidelně se opakující chybové záznamy.

4. Bezpečnostní požadavky

ID	Název	Popis požadavku
S1	Bezpečnost u subdodavatelů	Bezpečnostní požadavky na poskytovatele poskytovatel přenáší na subdodavatele jako součást smlouvy v rozsahu, který odpovídá charakteru dodávky.
S2	Certifikace řízení bezpečnosti	Poskytovatel má a udržuje po celou dobu plnění certifikovaný systém řízení bezpečnosti informací podle ISO/IEC 27001 nebo ekvivalentní, v jehož rozsahu jsou služby poskytované odběrateli a zařízení, která slouží k poskytování těchto služeb.
S3	Hlášení incidentu	Poskytovatel oznámí odběrateli co nejdříve každé narušení bezpečnosti systémů poskytovatele, které způsobilo nebo by mohlo způsobit prozrazení informací, které získal od odběratele, nebo neoprávněný přístup k systémům odběratele. Při tom použije stejný způsob informování jako při detekování bezpečnostní incidentu kategorie kritický u odběratele.
S5	Poučení uživatelů	Pracovníky poskytovatele, kteří mají přístup k systémům a informacím odběratele, poskytovatel před umožněním takového přístupu prokazatelně poučí o jejich povinnostech k zajištění bezpečnosti a o bezpečnostních opatřeních.
S6	Smazání informací	Nejpozději při ukončení smluvního vztahu poskytovatel odstraní ze svých informačních systémů (případně zlikviduje tištěné materiály) informace o bezpečnostních událostech a incidentech, informačních systémech objednatele a jejich konfiguracích.

Bezpečnostní požadavky na systém, ze kterého pracovníci poskytovatele přistupují k SIEM, případně k dalším systémům odběratele:

ID	Název	Popis požadavku
S10	Jednoznačný identifikátor uživatele	Každý uživatel má jednoznačný uživatelský účet. Sdílené účty (pokud jsou použity) jsou schváleny a dokumentovány a jejich použití monitorováno.

ID	Název	Popis požadavku
S11	Správa práv	Přidělování a odebírání přístupových práv uživatelským účtům se řídí dokumentovaným procesem. Přístupová práva jsou evidována.
S12	Řízení privilegovaných účtů	Uživatelské účty s privilegovaným oprávněním jsou schválené a dokumentované. Uživatelské účty s privilegovaným oprávněním jsou odlišné od uživatelských účtů. Uživatelské účty s privilegovaným oprávněním jsou pravidelně revidovány.
S13	Dočasná hesla	Dočasné tajné autentizační údaje (např. heslo) jsou předány uživatelům pouze po předchozí identifikaci uživatele, nesmí být uhodnutelné a musí být změněny po prvním použití.
S14	Defaultní účty	Defaultní účty jsou odstraněny nebo uzamčeny. Pokud to není možné, jsou změněny tajné autentizační údaje (např. hesla) k nim.
S15	Odebrání přístupu	Při ukončení pracovního poměru (nebo jiné smlouvy opravňující k přístupu) jsou uživateli odebrána všechna přístupová práva a deaktivován uživatelský účet.
S16	Autorizace	Před přístupem k datům a funkcím systému mimo těch, které jsou veřejné, je uživatel autentizován a je ověřen rozsah jeho oprávnění.
S17	Žádná nezměnitelná hesla	K žádné části systému není možné získat přístup s využitím autentizačních informací (hesel, kryptografických klíčů apod.), které není možné změnit. Tj. systém neobsahuje „hardcoded" hesla, „maintenance backdooor" apod.
S18	Bezpečná hesla	Používaná hesla musí splňovat požadavky zákona o kybernetické bezpečnosti č. 181/2014 Sb. a navazujících předpisů.
S19	Fyzická bezpečnost	Systémy mají zajištěnou fyzickou bezpečnost, tj. jsou chráněny před krádeží a přístupem neoprávněných osob.
S20	Likvidace médií	Média (flash disky, pevné disky atd.), na kterých byly uloženy informace získané od objednatele, jsou před dalším použitím bezpečně smazána. Po skončení životnosti jsou bezpečně zlikvidována.
S21	Logování	Systém zaznamenává informace o provozních a bezpečnostních činnostech. Tyto záznamy jsou chráněny proti pozdější modifikaci a neoprávněnému smazání.
S22	Synchronizace času	Čas na všech technických aktivech systému je synchronizován se zdrojem přesného času nejméně jednou za 24h.
S23	Pouze podporovaný software	Je provozovaný pouze dodavatelem podporovaný software nebo software s otevřeným kódem. (Není provozován software, který už není dodavatelem podporován.)
S24	Žádné modifikace software	Software dodaný výrobcem není před instalací modifikován.
S25	Instalace kritických aktualizací	Bezpečnostní aktualizace programového vybavení systému, které jeho výrobce označil jako kritické, jsou aplikovány do … dnů od vydání.
S26	Odstraňování zranitelností	Systém je pravidelně skenován na přítomnost známých zranitelností. Vysoce závažné zranitelnosti (Common Vulnerability Scoring System score 7 a vyšší) jsou odstraněny do 90 dnů. Není-li možné takovou zranitelnost v této lhůtě odstranit, poskytovatel o ní informuje odběratele.
S27	Ochrana před škodlivým kódem	Je zajištěna ochrana před škodlivým kódem, například nasazením pravidelně aktualizovaného antivirového programu prověřujícího spouštěné a otevírané soubory.
S28	Ochrana přenášených dat	Důvěrnost a integrita dat přenášených po sítích mimo prostory pod správou poskytovatele jsou chráněny kryptografickými opatřeními.
S29	Ochrana dat na médích	Důvěrnost a integrita dat ukládaných na vyměnitelná média a mobilní zařízení přenášené mimo prostory pod správou poskytovatele jsou zajištěny kryptografickými opatřeními.

ID	Název	Popis požadavku
S30	Bezpečná kryptografie	Použité kryptografické algoritmy, schémata a protokoly splňují požadavky zákona o kybernetické bezpečnosti č. 181/2014 Sb. a navazujících předpisů.
S31	Procesní zabezpečení VPN poskytovatelem	a) Poskytovatel si zajistí instalaci a konfiguraci pluginu Citrix Receiver a certifikátů na PC zaměstnanců SOC, dle návodu od objednatele. b) Poskytovatel oznámí objednateli nástup nového zaměstnance SOC minimálně 3 pracovní dny před požadavkem na vydání certifikátu objednatelem na adresu dle Komunikační matice dohodnuté v rámci realizační studie. Certifikát je zaměstnanci vydán na jeho vlastní čipovou kartu/token v sídle objednatele v pracovní době ČNB. c) V případě obnovy certifikátu z důvodu vypršení certifikátu, chyby nebo ztráty, bude zaměstnanci SOC vydán certifikát nový na jeho vlastní čipovou kartu/token v sídle objednatele v pracovní době ČNB. d) Maximální počet souběžně platných certifikátů všech zaměstnanců SOC je 10 e) Maximální počet současně připojených zaměstnancům k systému SIEM objednatele je 2, v případě analýzy KBU/KBI je tento počet 5
S32	Hlášení změny u osoby	Poskytovatel je povinen neprodleně oznámit objednateli rozvázání pracovního poměru se zaměstnancem SOC, změnu pracovního zařazení, případně ztrátu certifikátu, na jehož základě Objednatel zneplatní certifikát tohoto zaměstnance.
S33	Standard pro čipovou kartu či token poskytovatele	Poskytovatel v rámci karet či tokenů pro VPN si zajistí vlastní zařízení: Čipové karty od firmy SafeNet/Gemalto model eToken 4100/MD 840 nebo usb tokeny 5100/5110

Příloha č. 3

BEZPEČNOSTNÍ POŽADAVKY OBJEDNATELE

1. Poskytovatel odpovídá za to, že do objektů objednatele (dále jen „ČNB“) budou vstupovat nebo vjíždět pouze jeho pracovníci, kteří jsou jmenovitě uvedeni v písemném seznamu, schváleném ČNB (dále jen „seznam“). Tato povinnost se vztahuje i na posádky vozidel poskytovatele vjíždějících do garáží ČNB za účelem složení a naložení nákladu. Seznam poskytovatel předloží ČNB nejpozději v den podpisu smlouvy.

2. Seznam bude obsahovat tyto položky: jméno, příjmení a číslo průkazu totožnosti pracovníků poskytovatele. Součástí seznamu je „Prohlášení o získání souhlasu subjektů osobních údajů se zpracováním osobních údajů v ČNB ve smyslu zákona č.101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů“. Poskytovatel v něm prohlásí a nese odpovědnost za to, že jeho pracovníci uvedení v seznamu vydali souhlas se zpracováním osobních údajů Českou národní bankou v rozsahu: jméno, příjmení a číslo průkazu totožnosti. Důvodem předání těchto osobních údajů je zajištění evidence osob vstupujících do objektu ČNB a správy přístupového systému ČNB.

3. Požadavky na případné doplňky a změny schváleného seznamu pracovníků poskytovatele je nutno neprodleně oznámit ČNB. Případné doplňky a změny podléhají schválení ČNB. Osoby neschválené ČNB nemohou vstupovat do objektů ČNB, přičemž ČNB si vyhrazuje právo neuvádět důvody jejich neschválení.

4. Při příchodu do objektů ČNB pracovníci poskytovatele sdělí důvod vstupu, prokáží se osobním dokladem a podrobí se bezpečnostní kontrole. Osoby, které nejsou uvedeny na seznamu, nebudou do objektu ČNB vpuštěny.

5. Schválení pracovníci poskytovatele musí dbát pokynů bankovních policistů, které se týkají režimu vstupu, pohybu a vjezdu do objektu ČNB. Pracovníci poskytovatele budou do prostorů ČNB vstupovat a v těchto prostorách se pohybovat v režimu návštěv, to znamená vždy pouze v doprovodu zaměstnance ČNB nebo zaměstnance referátu bankovní policie ČNB.

6. V případě mimořádné události se pracovníci poskytovatele musí řídit pokyny bankovních policistů nebo dozorujícím zaměstnancem ČNB a dále instrukcemi vyhlašovanými vnitřním rozhlasem.

7. Pracovníci poskytovatele nesmí vnášet do prostor ČNB nebezpečné předměty, jako jsou střelné zbraně, výbušniny apod. O tom co je a není nebezpečný předmět, rozhodují bankovní policisté v souladu s vnitřními předpisy ČNB.

8. ČNB si vyhrazuje právo nevpustit do objektů ČNB pracovníka poskytovatele, který je zjevně pod vlivem alkoholu, drog nebo jiné omamné látky.

9. Bez písemného povolení ČNB je zakázáno fotografování a pořizování videozáznamů z interiéru objektů ČNB.

10. Ve všech prostorech objektů ČNB je přísný zákaz kouření a používání otevřeného ohně. O povolení práce se zvýšeným požárním nebezpečím požádá poskytovatel písemnou formou vždy nejpozději jeden pracovní den před zahájením prací, dozorujícího zaměstnance ČNB. Dále se pracovníci poskytovatele musí zdržet poškozování či zcizení

majetku ČNB, a dále zdržet se nevhodného chování vůči zaměstnancům a návštěvníkům ČNB.

11. Pracovníci poskytovatele uvedení na seznamu se musí před započetím výkonu práce v objektech ČNB prokazatelně seznámit, ve smyslu předpisů o požární ochraně, bezpečnosti a hygieně práce, se specifikami daných objektů ČNB (např. způsob vyhlášení požárního poplachu, určení ohlašovny požáru, seznámení s únikovými cestami, poplachovými směrnicemi, evakuačním plánem, umístěním věcných prostředků požární ochrany apod.). ČNB je oprávněna kdykoliv podrobit kontrole kterékoliv pracovníka poskytovatele uvedeného na seznamu z dodržování těchto předpisů a ustanovení.

Příloha č. 4

Ujednání o zpracování osobních údajů
v souvislosti s **poskytováním služeb *"Security Operations Center"***
(dále také jen „***ujednání***")

Objednatel a poskytovatel se dohodli na tomto ujednání, které splňuje požadavky na smlouvu o zpracování osobních údajů podle ustanovení § 6 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „ZOOÚ").

Úvodní ustanovení

1. Objednatel v souladu se smlouvou **o poskytování služeb *"Security Operations Center"***, evidenční číslo: 92-051-18 (dále také jako „***smlouva***") určuje účel a prostředky zpracování osobních údajů subjektů údajů, kterými jsou uživatelé informačních systémů v systémovém prostředí objednatele a zaměstnanci objednatele (společně dále také „***subjekty údajů***"), kdy objednatel je v postavení správce osobních údajů ve smyslu § 4 písm. j) ZOOÚ.
2. Poskytovatel bude na základě smlouvy zpracovávat osobní údaje subjektů údajů a bude v postavení zpracovatele osobních údajů ve smyslu § 4 písm. k) ZOOÚ.

Článek II
Účel ujednání

1. Účelem tohoto ujednání je úprava práv a povinností smluvních stran při zpracování a v souvislosti se zpracováním osobních údajů zpracovatelem při plnění povinností ze smlouvy tak, aby zpracování probíhalo v souladu s právními předpisy o ochraně osobních údajů.

Článek III
Předmět ujednání

1. Toto ujednání upravuje vztahy mezi správcem a zpracovatelem osobních údajů, zejména pak vymezuje rozsah osobních údajů, které bude zpracovatel zpracovávat, prostředky a účel, pro který bude osobní údaje zpracovávat, dobu zpracování osobních údajů a podmínky a záruky zpracovatele osobních údajů z hlediska technického a organizačního zabezpečení ochrany osobních údajů.

Článek IV
Účel a rozsah zpracování osobních údajů

1. Zpracovatel bude zpracovávat veškeré osobní údaje subjektů údajů pouze v rozsahu nezbytném pro zajištění realizace smlouvy, ve znění pozdějších dodatků. Za osobní údaje jsou podle tohoto ujednání považovány veškeré informace v níže uvedených výčtech (dále také jako „***osobní údaje***").

2. Zpracovatel je oprávněn zpracovávat osobní údaje získané od správce pro účely řádného plnění povinností podle smlouvy, tj. zejména zajištění řádného provedení bezpečnostních auditů pouze v následujícím rozsahu nezbytném pro výkon práv a povinností podle smlouvy:
   - adresní a identifikační údaje (např. jméno, příjmení, datum a místo narození, rodinný stav, rodné číslo, státní příslušnost, adresa trvalého bydliště, telefonní spojení domů, do zaměstnání apod.)
   - údaje o jiné osobě (např. adresní a identifikační údaje člena rodiny, manžel/manželka, dítě apod.)
3. Zpracovatel bude osobní údaje zpracovávat pouze ve formě možného nahlédnutí zpracovatele do osobních údajů ve smyslu § 4 písm. e) ZOOÚ. Toto nahlédnutí přitom není cílem plnění smlouvy, ale může k němu v rámci spolupráce správce se zpracovatelem docházet.

4. Zpracovatel je ve všech případech při zpracování osobních údajů subjektů údajů vázán prokazatelnými pokyny správce. Zpracovatel nesmí bez předchozího prokazatelného výslovného souhlasu anebo pokynu správce zpracovávané osobní údaje nijak upravit nebo pozměnit, třídit nebo kombinovat, zpřístupnit ani předat třetí osobě, šířit ani zveřejňovat, ani jakýmkoli způsobem použít pro vlastní potřebu.

Článek V
Doba zpracování

1. Zpracovatel bude všechny osobní údaje zpracovávat pouze způsobem podle čl. IV odst. 3 po dobu nezbytně nutnou pro účel bezprostředního plnění smlouvy ve vztahu ke konkrétnímu informačnímu systému obsahujícímu osobní údaje.

Článek VI
Práva a povinnosti smluvních stran

1. Správce pověřuje zpracovatele zpracováním osobních údajů výhradně za účelem zajištění služeb bezpečnostního auditu informačních systémů a infrastruktury a za účelem splnění povinností stanovených platnými právními předpisy.

2. Zpracovatel se zavazuje, že osobní údaje nebudou zpracovatelem použity, zpřístupněny, zpracovávány či poskytnuty třetím osobám, nebudou předávány mimo území EU či s nimi nebude nakládáno jinak, než pouze za účelem, pro který byly osobní údaje zpřístupněny a v souladu s pokyny správce.

3. Zpracovatel je povinen zabezpečit osobní údaje a zachovávat mlčenlivost o osobních údajích a řídit se pokyny správce ve všech případech, kdy se jedná o zpracování či zabezpečení osobních údajů. Zpracovatel přijme technická, organizační a personální opatření adekvátní způsobu zpracování a v souladu s pokyny správce – přičemž toto zabezpečení bude odpovídat příslušným aktuálním používaným bezpečnostním standardům (podrobněji v odst. 5 a násl. tohoto článku VI. ujednání).

4. Správce stanoví opatření, která považuje za dostatečná pro technické a personální zabezpečení osobních údajů následovně:

   a) Technické zabezpečení osobních údajů se zajistí pomocí prostředků:

      (i) počítačové bezpečnosti; zpracovatel se zavazuje ke zpracování používat výhradně takové technické a programové prostředky, jejichž používání při vyloučení nepředvídatelných okolností eliminuje možnost narušení, neoprávněného přístupu k osobním údajům či neoprávněného nakládání s osobními údaji;

      (ii) komunikační bezpečnosti; zpracovatel se zavazuje dodržovat taková opatření k zabezpečení ochrany osobních údajů při jejich přenosu telekomunikačními kanály, jejichž povaha eliminuje při vyloučení nepředvídatelných okolností možnost narušení (šifrování);

      (iii) fyzické bezpečnosti; v tomto ohledu zpracovatel prohlašuje, že místo, ve kterém budou osobní údaje zpracovávány a ve kterém budou uchovávány spisy a dokumenty, bude mít charakter prostoru zabezpečeného před možností narušení.

   Zpracovatel bude plnit všechny povinnosti stanovené v ustanovení tohoto písm. a) využíváním prostředků odpovídajících dosaženému stupni technického pokroku a možnostem zpracovatele.

   b) Personální zabezpečení:

      (i) osobní údaje budou zpřístupněny pouze určeným osobám z oprávněného personálu zpracovatele a případně oprávněným osobám, které odpovídají za zajištění bezpečnosti systémů, kde jsou osobní údaje uloženy, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby;

      (ii) zpracovatel je povinen zabezpečit poučení všech osob, které mají v rámci zpracování osobních údajů přístup k těmto údajům, aby tyto osoby byly řádně poučeny o svých povinnostech při zpracovávání osobních údajů, zejména pak o povinnosti mlčenlivosti ve vztahu k těmto osobním údajům.

   c) Dále je zpracovatel povinen zabránit neoprávněným osobám v přístupu k osobním údajům a k prostředkům pro jejich zpracování a dále zabránit neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje.

5. Zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu s právními předpisy, zejména se ZOOÚ a dalšími předpisy regulujícími ochranu osobních údajů, jakož i provádět nejméně jednou ročně hodnocení efektivnosti přijatých opatření, a to včetně vedení a zpřístupnění následující dokumentace:

   - seznamu osob, které jsou oprávněny přistupovat k osobním údajům (včetně rozsahu oprávnění);

- elektronického přehledu informací o veškerých přístupech jednotlivých osob k osobním údajům;
- elektronického přehledu informací o nakládání s osobními údaji.

6. Zpracovatel bude neprodleně písemně informovat správce v případě jakýchkoliv potíží při plnění povinností z tohoto ujednání a o všech okolnostech týkajících se porušení povinností při zpracování a ochraně osobních údajů, zejména pokud dojde k neoprávněnému přístupu k osobním údajům, či k jejich ztrátě nebo zničení. V takovém případě zpracovatel přijme v nejkratším možném termínu veškerá nezbytná opatření k zajištění ochrany osobních údajů, notifikuje správce o těchto skutečnostech prostřednictvím kontaktní osoby/osob uvedených ve smlouvě a následně postupuje v souladu se ZOOÚ a pokyny správce, budou-li mu sděleny.

7. Zpracovatel plní informační povinnost vůči subjektům údajů v souladu se ZOOÚ a dle požadavků správce. V případě, že v souvislosti se zpracováním osobních údajů zpracovatelem bude zahájeno řízení ze strany orgánu veřejné správy, zpracovatel poskytne správci v těchto řízeních veškerou potřebnou součinnost.

8. Zpracovatel je správci na jeho žádost nápomocen při posuzování vlivu zpracovávání osobních údajů na ochranu osobních údajů a při konzultacích správce s dozorovým orgánem, při zohlednění povahy zpracovávání a informací, jež má zpracovatel k dispozici.

9. Zpracovatel je správci na jeho žádost nápomocen při výkonu práv subjektů osobních údajů, a to zejména při výkonu práva na přístup k osobním údajům, práva na opravu, výmaz a omezení zpracovávání osobních údajů, práva na přenositelnost údajů a práva vznést námitku vůči zpracovávání osobních údajů.

10. Zpracovatel nezapojí do zpracovávání osobních údajů dalšího zpracovatele bez předchozího písemného povolení správce. V případě, že jakákoliv část zpracovávání osobních údajů bude vykonávaná dalším zpracovatelem po předchozím písemném povolení správce, zůstává zpracovatel plně odpovědný vůči správci za zpracovávání osobních údajů. Správce si vyhrazuje právo uzavřít s dalším potencionálním zpracovatelem zvláštní smlouvu o zpracovávání osobních údajů.

11. Správce je oprávněn kontrolovat dodržování pravidel stanovených pro zpracování ZOOÚ či tímto ujednáním u zpracovatele, resp. na jiném místě, kde dochází ke zpracování údajů. Zpracovatel za tímto účelem zajistí zástupcům správce, kteří budou k provedení kontroly pověřeni, přístup ke všem relevantním informacím a na příslušná místa tak, aby mohlo dojít k hodnocení oprávněnosti zpracování. Zpracovatel poskytne správci na jeho vyžádání veškeré podklady o přijatých a provedených technicko-organizačních opatřeních k zajištění ochrany osobních údajů.

12. Po ukončení poskytování služeb dle smlouvy zpracovatel vrátí veškeré osobní údaje správci, s výjimkou těch údajů, které je zpracovatel povinen uchovávat na základě platných právních předpisů.

Článek VII
Odpovědnost za škodu a smluvní pokuty

1. Tento článek upravuje odpovědnost za škodu a smluvní pokuty pro případ porušení tohoto ujednání. Znění tohoto článku VII. se nevztahuje na smluvní pokuty a úrok z prodlení podle smlouvy, který zůstává zachován.

2. Zpracovatel se zavazuje odškodnit správce za jakékoliv nároky, a to zejména zadostiučinění, peněžité náhrady nebo pokuty, úspěšně uplatněné v soudním popř. správním řízení třetími osobami, a to zejména subjekty údajů nebo Úřadem na ochranu osobních údajů, které vznikly v příčinné souvislosti s porušením povinností stanovených ZOOÚ nebo tímto ujednáním ze strany zpracovatele.

3. Pokud dojde k prokazatelnému porušení ZOOÚ pouze v důsledku jednání té smluvní strany, které je uložena pokuta podle § 45 ZOOÚ, hradí náklady na uhrazení pokuty plně ta strana, která ZOOÚ porušila a jíž současně byla uložena pokuta.

4. V případě, že zpracovatel správci neumožní kontrolu ohlášenou v souladu s čl. VI. odst. 12 tohoto ujednání, anebo během ní správci neposkytne pro předmět kontroly potřebnou součinnost, je správce oprávněn po zpracovateli požadovat smluvní pokutu ve výši 1.000,- Kč za každý započatý pracovní den takto trvajícího prodlení na straně zpracovatele.

5. Zpracovatel je povinen odstranit kontrolou zjištěné nedostatky neprodleně, nejpozději ve lhůtě 5 dnů, nedohodnou-li se smluvní strany jinak. V případě, že zpracovatel neodstraní kontrolou zjištěné nedostatky ve lhůtě stanovené dle předchozí věty, je správce oprávněn po zpracovateli požadovat smluvní pokutu ve výši 1.000,- Kč za každý započatý den prodlení na straně zpracovatele.

6. V případě, že zpracovatel poruší kteroukoli z povinností sjednaných v čl. VI. (vyjma čl. VI. odst. 12) tohoto ujednání, je správce oprávněn po zpracovateli požadovat smluvní pokutu ve výši 5.000,- Kč za každý jednotlivý případ takového porušení.

7. Ujednáním o smluvní pokutě podle tohoto článku VII. není dotčeno právo správce na náhradu škody vzniklé z porušení povinnosti v plné výši.

Článek VIII
Trvání závazků

1. Povinnost zpracování osobních údajů se sjednává pouze na dobu existence závazkového vztahu vzniklého ze smlouvy, nejpozději do dne likvidace posledního zpracovávaného osobního údaje zpracovatelem ve smyslu povinnosti zlikvidovat osobní údaje podle ZOOÚ.

Článek IX
Další ujednání

1. Zpracovatel se zavazuje plnit veškeré povinnosti vyplývající z obecného nařízení o ochraně osobních údajů (Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze

dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES), a to ode dne jeho účinnosti (25. května 2018).

2. Smluvní strany se zavazují vstoupit v jednání o doplnění tohoto ujednání, jehož potřeba případně vzejde z účinnosti obecného nařízení podle odst. I tohoto čl. IX., a poskytnout si veškerou potřebnou součinnost ke sjednání dodatku smlouvy, pokud bude pro potřeby plnění požadavků tohoto obecného nařízení potřebný.

3. Za písemnou formu se pro účely tohoto ujednání nepovažuje e-mailová či jiná elektronická forma. Výjimkou je situace, v níž zpracovatel informuje správce ve smyslu čl. VI. odst. 7 tohoto ujednání (potíže při plnění povinností z tohoto ujednání a okolnosti týkající se porušení povinností při zpracování a ochraně osobních údajů) a oznámení kontroly ve smyslu čl. VI. odst. 12 ujednání, které lze provést i elektronickým oznámením prokazatelně doručeným druhé smluvní straně. V případě oznámení kontroly postačuje prokazatelné odeslání oznámení správcem na e-mailovou adresu uvedenou pro tento účel zpracovatelem. V případě oznámení kontroly postačuje prokazatelné odeslání oznámení správcem na e-mailovou adresu zpracovatele uvedenou ve smlouvě.

Příloha č. 5

Cenová tabulka

CENOVÁ TABULKA Dodávka služby SOC - Security Operation Centre				
Položka plnění		**Počet ks**	**Cena v Kč bez DPH za 1 měsíc**	**Celková cena v Kč bez DPH**
poskytování služby nepřetržitého monitoringu a analýzy bezpečnostních událostí (dle čl. I odst.1a -1e smlouvy)*		48	32375	1 554 000,00
		Počet ks	**Cena v Kč bez DPH**	**Celková cena v Kč bez DPH**
Přípravné činnosti - etapa č. 1		1,00	46 800,00	46 800,00
Přípravné činnosti - etapa č. 2 včetně 1 měsíce poskytování služby		1,00	51 145,00	51 145,00
		Předpokládaný počet hodin ročně	**Cena za 1 hodinu v Kč bez DPH**	**Celková cena za předpokládaný počet hodin v Kč bez DPH za 4 roky**
Poskytování konzultačních služeb (dle čl. I odst.1f smlouvy)*		32	1 376,00	176 128,00
Celková nabídková cena v Kč bez DPH				**1 828 073,00**

* Předpokládaný počet měsíců poskytování služby nepřetržitého monitoringu a analýzy bezpečnostních událostí a předpokládaný počet hodin poskytování konzultačních služeb uvedený v tabulce je v souladu se zákonem stanoven za období 48 měsíců, a je uveden pouze za účelem porovnání nabídek. Zadavatel si vyhrazuje právo uvedené množství čerpat dle svých reálných potřeb, tj. přečerpat, nedočerpat či vůbec nečerpat; skutečný počet měsíců se tak může od předpokládaného počtu měsíců lišit.

Dodavatel vyplní pouze podbarvená pole

Příloha č. 6

Šablona realizační studie

Pozn.: V níže uvedené šabloně lze přiměřeně měnit grafickou podobu a styl studie (fonty, formátování apod.), dále pak lze měnit/doplňovat/přizpůsobit členění kapitol v závislosti na nabízeném řešení služby a čitelnosti a srozumitelnosti textu. Nicméně struktura hlavních kapitol představuje rozsah oblastí, které by studie měla pokrýt a jejich zužování není povolena. V rámci podkapitol lze již úpravy připustit.

ČESKÁ ČNB NÁRODNÍ BANKA

Projekt *ID projektu*

„*Název projektu*“

Realizační studie

Verze	
Datum verze	
Autor	
Vedoucí projektu *poskytovatele*	
Vedoucí projektu *objednatele*	

Historie změn

Verze	Datum	Autor	Popis změny

Obsah

Úvod

I.1 Účel dokumentu

[Dokument realizační studie popisuje způsob realizace, aktivace a následného provozu služby včetně analýzy funkčních požadavků, softwarové architektury a systémových požadavků tak, aby byla prokázána realizovatelnost všech objednatelem zadaných požadavků. ***Text kurzívou v hranatých závorkách je návodem, neměl by zůstat součástí výsledného dokumentu.]***

I.2 Seznam pojmů a zkratek

[Výčet klíčových zkratek a pojmů s jejich vysvětlením]

Termín/Zkratka	Popis/Význam

1.3 Přehled použitých symbolů

[Popis použitých grafických symbolů v dokumentu]

Grafický symbol	Význam

Realizace věcného zadání

I.4 Analýza funkčních požadavků

[Kapitola obsahuje mapování funkčních požadavků na cílové řešení služby. Popis tak ve stručné formě představuje způsob realizace jednotlivých funkčních požadavků.]

I.5 Analýza bezpečnostních požadavků

[Kapitola obsahuje mapování funkčních požadavků na cílové řešení služby. Popis tak ve stručné formě představuje způsob realizace jednotlivých funkčních požadavků.]

I.6 Komunikační matice pro hlášení KBU/KBI

[Kapitola obsahuje popis komunikace mezi objednatelem a poskytovatelem v případě výskytu KBU/KBI v prostředí objednatele, případně výpadku sběru logů z kritických IS]

Pravidla pro určení závažnosti bezp. Incidentu (KBI)

Typ události	Popis	Komunikace
Kritický KBI	Incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod.	Telefonicky a e-mailem
Střední KBI	Incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření incidentu včetně minimalizace vzniklých škod.	Emailem a SMS
Nízký KBI	Incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření bezpečnostního incidentu včetně	Emailem

	minimalizace vzniklých škod.	
KBU		Emailem
Výpadky sběru logů z kritických IS	V případě výpadku sběru logů z kritických IS delším než 4hodiny	Emailem

I.7 Pravidelný měsíční report

[Kapitola obsahuje definování struktury a obsahu měsíčního reportu a způsob jeho předávání]

Technická realizace řešení

I.8 Integrace s IS ČNB

I.8.1 SIEM objednatele

[Kapitola obsahuje návrh na úpravu kontentu v SIEM (pravidla, reporty apod.), které bude poskytovatel potřebovat pro zajištění kvality služby. Poskytovatel zajistí požadované úpravy v podobě balíčků pro nástroj HP ArcSight (v ČNB používaný SIEM) nebo přímo v systému SIEM objednatele v součinnosti s objednatelem. Všechny takové změny budou prováděny v sídle objednatele v běžnou pracovní dobu objednatele (Po-Pá 7:45-16:15) a veškeré změny budou detailně zdokumentovány.
Kapitola může obsahovat i doporučení na sběr logů z dalších informačních systémů ČNB.]

I.8.2 Výpočetní prostředí ČNB

[Kapitola obsahuje závěr seznámení poskytovatele s kritičností jednotlivých IS objednatele. definování způsobu oznamování změn.]

I.8.3 VPN

[Kapitola obsahuje popis připojení poskytovatele k systému objednatele, definuje procesy při nástupu/ odchodu zaměstnance SOC. zneplatnění/obnovu certifikátu a způsob hlášení závad.]

Nefunkčnost VPN ohlašuje poskytovatel mailem na adresu:
Nefunkčnost SIEM ohlašuje poskytovatel mailem na adresu:
Plánovaný výpadek VPN/SIEM ohlašuje objednatel mailem na adresu:

I.8.4 Další

[Kapitola obsahuje popis dalších (pokud existují) výše nepopsané interakce se službami systémového prostředí ČNB (např. e-mail).]

I.9 Bezpečnost a ochrana osobních údajů

[Kapitola obsahuje popis řešení z hlediska bezpečnosti, integrity a důvěrnosti dat.]

I.9.1 Autentizace a autorizace, řízení přístupu

[V podkapitole je popsán princip řízení přístupů k informacím resp. informačním aktivům: jakým prostřednictvím přistupují interní a externí uživatelé, způsob automatického blokování účtů uživatelů při ukončení zaměstnaneckého poměru, povolené protokoly apod.]

I.9.2 Logování

[V podkapitole je popsán způsob logování a monitorování logů, napojení na SIEM.]

I.9.3 Zabezpečení síťové komunikace a uložených dat

[V podkapitole je popsán způsob, jak je zabezpečena síťová komunikace a zabezpečení uložených dat.]

I.9.4 Plnění požadavků na ochranu osobních údajů

I.10 Detailní harmonogram realizace

[Harmonogram realizace uvádí rozpad realizace projektu do jednotlivých etap a činností s ohledem na dodržení stanovených termínů/lhůt. Harmonogram *musí obsahovat milníky pro předání díla nebo jeho částí k akceptačnímu řízení.]*

Registr změn

[V kapitole je uveden seznam změn oproti předběžné studii/zadávací dokumentaci. jejich akceptace a jejich dopady do projektu – časové. zdrojové a finanční.]

ID změny	**Popis změny**	**Akceptována Ano/Ne**	**Realizace** (termín, zdroje a finance)

Příloha č. 7

Popis systémového prostředí objednatele

1. Systém SIEM objednatele

1.1. konfigurace SIEM systému

Položka	Popis
Název	HP ArcSight Express
Verze	6.11
Moduly	Konektory 7.7.x (cca 50, instalovány na 3 serverech)
Licence	Denní průměr 1000 EPS
Počet všech pravidel	628
Počet pravidel generujících kybernetické bezpečnostní události v rozhraní SIEM systému	426 Very-high 82 pravidel High 76 pravidel Medium 135 pravidel Low 132 pravidel unknown 1

Do SIEM systému jsou posílány logy z cca 900 datových zdrojů. Systém je zaměřen zejména (cca 2/3 všech datových zdrojů) na sběr logů aplikačních serverů, jejich databází a frontendů. Vstupní logy jsou tvořeny událostmi z běžně používaných informačních technologií a systémů a událostmi ve specifickém formátu z unikátních aplikací zadavatele. Na první typ událostí jsou aplikovány parsery a pravidla ze standardní výbavy ArcSight, dodaná výrobcem. Pro druhý typ událostí jsou připraveny parsery na míru.
Množství logů produkovaných jednotlivými systémy kolísá podle aktivity uživatelů.

1.2. Statistika sběru dat do SIEM systému ČNB

Parametr	Hodnota	Předpokládaný počet pro následující období
Denní průměr EPS	450-480	800
Maximum EPS	cca 700 (ve špičkách >2500)	1000 (ve špičkách >3500)
Minima EPS	200-250	300
Počet bezpečnostních událostí nahlášených SIEM systémem (za posledních 12 měsíců)	300	600

EPS = počet událostí za vteřinu

2. Standardní systémové prostředí objednatele

Níže je uveden stručný výtah z popisu standardního systémového prostředí objednatele. Nejedná se o úplný popis, ale o výtah informací relevantních k danému zadávacímu řízení.

2.1. Obecné informace

V ČNB jsou v provozu dvě výpočetní střediska. Obě tato střediska jsou provozována systémem aktiv-aktiv, tj. v obou střediscích jsou zpracovávány různé informační systémy. Obě střediska mají konektivitu do Internetu a tato konektivita je provozována v režimu active-passive; mezi středisky je zřízeno několik síťových příček v různých úrovních.
Běžný uživatel není schopen rozlišit, ve kterém středisku je jeho požadavek zpracován.

2.2. Komunikační infrastruktura

Obě výpočetní střediska jsou propojena optickými vlákny (single mode) dvěma nezávislými trasami.

2.2.1. Standardní komunikační vybavení

- LAN - strukturovaná kabeláž pro připojení uživatelů umožňující připojení rychlostí minimálně 100 Mbit/s. Standardní provedení je metalické (RJ-45), optická vlákna jsou typem doplňkovým;
- Páteřní LAN – Gigabit Ethernet až 10 Gbps;
- Připojení každé lokality do Internetu – 1 Gbps (provider T-mobile) v režimu active-passive;
- aktivní síťové prvky – platforma CISCO, plně přepínaná síť;
- LAN, MAN, WAN – multiplexory typu DWDM;
- Ethernet dle ISO 802.3 pro připojení uživatelských stanic;
- Protokol TCP/IP;
- Jmenné služby - DNS;
- Přesný čas – NTP.

Jako zdroj přesného času je použit SNTP (Simple Network Time Protocol) server MTS (Moba Time Server). Server je synchronizován externím časovým signálem s GPS (Global Positioning System). Protokolem NTP (Network Time Protocol) se pak synchronizují další síťová zařízení. Struktura synchronizace je hierarchická.

2.3. Aplikace a systémové služby

- SIEM – viz kapitola 1.1 této přílohy
- MS Active Directory – provozováno na MS Windows 2008 R2 serveru

Pozn.: Verze aplikací a služeb jsou platné ke dni vyhlášení zadávacího řízení. Později může být aplikován minoritní update či patch, který může uvedenou verzi povýšit.

3. Popis vzdáleného přístupu (VPN)

3.1. Technická realizace

Vzdálený přístup prostřednictvím VPN je realizován pomocí produktů platformy CITRIX, konkrétně se jedná o vypublikovanou aplikaci (webovská konzole SIEM) prostřednictvím Citrix XenApp 6.5 provozovaném na MS Windows Serveru 2008R2 Standard s aktuálními SP a záplatami.

Na perimetru ČNB je instalována Citrix Access Gateway (Netscaler), který slouží jako bezpečný vstupní bod mezi klientským zařízením, objednatele, který používá pro zobrazení konzole SIEM objednatele.

Tento vstupní bod zajišťuje:

- Šifrovaný komunikační kanál mezi ČNB a Poskytovatelem
- Prostřednictvím EPA agenta kontrolu bezpečnostní kvality koncového zařízení Poskytovatele (aktuálnost patchů, antivirové ochrany apod.).
- Ověřovací bod pro přihlášení uživatelů Poskytovatele.

K přihlášení pracovníka Poskytovatele se využívá dvoufaktorová autentizace – certifikát uložený na čipové kartě nebo tokenu aktivovaný PINem. Při vytváření VPN spojení je nejprve provedena kontrola bezpečnostních prvků klientského zařízení a poté je uživatel připojen na vypublikovaný desktop nebo konzole SIEM.