

Smlouva

o dodávce Check Point DDoS Protector včetně poskytování podpory
uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, mezi:

Českou národní bankou

Na Příkopě 28

115 03 Praha 1

zastoupenou: Ing. Milanem Zirnsákem, ředitelem sekce informatiky

a

Ing. Zdeňkem Viriusem, ředitelem sekce správní

IČO: 48136450

DIČ: CZ48136450

(dále jen „objednatel“)

a

Corpus Solutions a.s.

zapsanou v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 5936

sídlo: Štětškova 1638/18, 140 00 Praha 4

zastoupenou: Ing. Tomášem Příbylem, předsedou představenstva

IČO: 25764616

DIČ: CZ25764616

č. účtu: 69474001/5500

(dále jen „poskytovatel“).

Článek I

Předmět smlouvy

1. Předmětem této smlouvy je závazek poskytovatele:
 - a. Provést v prostředí objednatelů upgrade technických i programových prostředků formou Replacementu (CPAC-TI-CREDIT) současných 2 ks Appliance Check Point DDoS Protector 1006 Dual Power Supply AC (CPAP-DP1006-D) na nové 2 ks Appliance Checkpoint DDoS Protector (CPAP-DP6-1-SME) se záložními napájecími zdroji (CPAC-PSU-AC-AL5208) (dále jen „zařízení“),
 - b. Provést instalaci, implementaci a konfiguraci výše uvedených nových zařízení v prostředí objednatelů.
2. Součástí dodávky jsou i navazující služby (dále jen „navazující služby“) po dobu trvání této smlouvy pro zařízení:
 - a. DDoS Management VA2 (CPSM-DP-VM-VA2-1Y),
 - b. APSolute Vision Analytics AMS (CPSB-AMS-20GBPS-1Y),

- c. DDoS Behavioral Protection and IPS Updates for DDoS Protector 6-1 (CPSB-DP6-1-SUS-1Y),
 - d. Active Attackers Feed Subscription for DDoS Protector 6-1 (CPSB-DP6-1-AAF-1Y).
3. Dále je předmětem po dobu trvání této smlouvy zajištění:
 - a. Podpory typu Collaborative Support Standard (CPCES-CO-STANDARD) od výrobce (dále jen „podpora od výrobce“) pro zařízení,
 - b. Podpory od poskytovatele (dále jen „podpora od poskytovatele“) pro zařízení.
4. Specifikace navazujících služeb a podpory dle odst. 2 a 3 tohoto článku jsou uvedeny v příloze č. 1 této smlouvy.

Článek II

Lhůta, místo a předání plnění

1. Poskytovatel předá objednateli plnění dle článku I odst. 1 a aktivuje navazující služby dle odst. 2, včetně úspěšného provedení ověřovacího provozu, do 3 měsíců od výzvy objednatele k zahájení plnění. Písemná výzva k zahájení plnění bude objednatelem doručena nejpozději do 3 měsíců od uzavření této smlouvy na mailovou adresu pověřené osoby poskytovatele. Plnění bude předáno podepsáním závěrečného akceptačního protokolu.
2. Místa plnění jsou sídlo objednatele na adrese Na Příkopě 28, Praha 1 a záložní pracoviště objednatele na adrese Strojírenská 175, Praha 5.
3. Plnění bude předáno v následujících etapách:
 - a. První etapa (dílčí akceptace) – předání zařízení v místech plnění dle odst. 2 tohoto článku a aktivace navazujících služeb.
 - b. Druhá etapa (dílčí akceptace) – provedení upgradu, instalace, implementace a konfigurace zařízení v prostředí objednatele (včetně navazujících služeb), aktivace podpory výrobce i poskytovatele, zařízení je naučené, resp. vyladěné na běžný provoz v rámci prostředí objednatele (interval učení je minimálně jeden týden).
 - c. Třetí etapa (dílčí akceptace) - zahájení ověřovacího provozu v délce 14 kalendářních dnů. Předmětem ověřovacího provozu bude ověření správné funkcionality zařízení v prostředí objednatele – propouštění legitimního provozu, detekce a zadržení neoprávněných provozů a provozů obsahujících škodlivý kód (malware). Pokud jsou v průběhu ověřovacího provozu zjištěny vady, je poskytovatel povinen provést jejich neprodlené odstranění. Od okamžiku odstranění vad může objednatel požadovat opakování celého 14 denního ověřovacího provozu. Ověřovací provoz bude považován za úspěšný, pokud v průběhu ověřovacího provozu nebudou zjištěny žádné vady.
 - d. Akceptace (závěrečný akceptační protokol) – předání plnění
4. Jednotlivé etapy dle odst. 3 písm. a) - c) budou úspěšně ukončeny na základě dílčích akceptačních protokolů. Po provedení všech dílčích akceptací dojde k předání plnění, a to na základě závěrečného akceptačního protokolu. Všechny akceptační protokoly musí být podepsány za každou smluvní stranu minimálně jednou pověřenou osobou.
5. Pověřenými osobami jsou:

za objednatele:

za poskytovatele:

6. Poskytovatel je povinen nahlásit případnou změnu osob uvedených v odst. 5 tohoto článku nejpozději následující pracovní den po provedení změny. V případě změny pověřených osob nebo jejich kontaktních údajů nejsou smluvní strany povinny uzavřít dodatek.
7. Poskytovatel zahájí poskytování podpory dle čl. I odst. 3 této smlouvy ode dne podpisu dílčího akceptačního protokolu dle čl. II odst. 3 písm. b) oběma smluvními stranami.

Článek III Cena plnění

1. Cena za provedení upgrade technických i programových prostředků 2 ks zařízení dle čl. I odst. 1 písm. a) této smlouvy činí 72 332 USD bez DPH.
2. Cena za instalaci, implementaci a konfiguraci 2 ks zařízení v prostředí objednatele dle čl. I odst. 1 písm. b) této smlouvy činí 66 600 CZK bez DPH.
3. Cena za navazující služby pro 2 ks zařízení dle čl. I odst. 2 této smlouvy činí 26 087,50 USD bez DPH / rok.
4. Cena podpory od výrobce pro 2 ks zařízení dle čl. I odst. 3 písm. a) této smlouvy činí 9 424 USD bez DPH / rok.
5. Cena podpory od poskytovatele pro 2 ks zařízení dle čl. I odst. 3 písm. b) této smlouvy činí 68 520 CZK bez DPH / rok.
6. V případě ukončení této smlouvy v průběhu období, za které jsou podpora a navazující služby dle bodů 3 až 5 tohoto článku uhrazeny, vystaví poskytovatel ke dni ukončení smlouvy daňový dobropis a alikvótní část uhrazené ceny podpory a navazujících služeb vrátí objednateli.
7. Ceny plnění uvedené v odst. 3 až 5 tohoto článku budou v prvním roce účinnosti této smlouvy účtovány v alikvótní výši podle počtu dnů poskytování plnění.
8. Ceny dle odst. 1, 3 a 4 tohoto článku budou poskytovatelem účtovány v CZK, přičemž k přepočtu cen v USD bude použit devizový kurz ČNB platný v den vystavení daňového dokladu.
9. K cenám plnění bude účtována DPH v sazbě platné v den uskutečnění zdanitelného plnění.
10. V cenách jsou zahrnuty veškeré náklady poskytovatele spojené s plněním této smlouvy včetně poskytnutí update a upgrade programových prostředků, nákladů spojených s cestou na místo plnění a náhradou za ztrátu času.
11. V případě oprav technických prostředků budou použity vždy nové díly či celá zařízení.

12. Úhrada ceny dle odst. 1 a 2 tohoto článku bude provedena na základě daňového dokladu vystaveného poskytovatelem nejdříve po dokončení upgrade, instalace, implementace a konfigurace zařízení, aktivaci navazujících služeb a po zdárném ukončení ověřovacího provozu a to na základě závěrečného akceptačního protokolu po dokončení těchto činností podepsaného pověřenými osobami obou smluvních stran.
13. Úhrada cen dle odst. 3 až 5 tohoto článku bude provedena předem, a to na základě daňového dokladu vystaveného poskytovatelem nejdříve v první den ročního období, na které se platí. Tímto dnem je 1. únor příslušného roku. V prvním roce účinnosti této smlouvy bude tímto dnem 1. den poskytování služeb dle čl. I, odst. 2 a 3.
14. Doklad k úhradě bude obsahovat údaje podle § 435 občanského zákoníku 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 náležitosti stanovené v zákoně o dani z přidané hodnoty. Nezbytnou náležitostí každého dokladu je také číslo této smlouvy (ve formátu ISDOC v poli ID ve skupině Contract References), nebo číslo objednávky (ve formátu ISDOC v poli External_Order_ID ve skupině OrderReference), jsou-li objednávky v rámci smlouvy vystavovány. Pokud doklad 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.
15. V případě, že bude v dokladu k úhradě uveden jiný, než určený účet, je poskytovatel povinen na základě výzvy objednatele sdělit na e-mailovou adresu, ze které byla výzva odeslána, zda má být zaplacen na bankovní účet uvedený v dokladu, nebo na určený účet. Uvedenou výzvu zašle objednatel na e-mailovou adresu poskytovatele monika.nedbalova@corpus.cz, jitka.hofmanova@corpus.cz. V tomto případě se doklad k úhradě nevrací s tím, že lhůta splatnosti začíná běžet až dnem doručení sdělení poskytovatele podle věty první.
16. Doklad k úhradě (fakturu) zašle poskytovatel elektronicky jako přílohu e-mailové zprávy na adresu faktury@cnb.cz ve formátu ISDOC. Pokud není možné vytvořit doklad ve formátu ISDOC, je možné zasílat jej ve formátu PDF. V jedné e-mailové zprávě smí být pouze jeden doklad k úhradě. Mimo vlastní doklad k úhradě může být přílohou e-mailové zprávy jedna až sedm příloh k dokladu ve formátech PDF, DOC, DOCX, XLS, XLSX. Přijaty budou i doklady k úhradě v jiném formátu, který bude v souladu s evropským standardem elektronické faktury. Nebude-li možné zaslat doklad k úhradě elektronicky, zašle jej poskytovatel v analogové formě na adresu:
Česká národní banka
sekce rozpočtu a účetnictví
odbor účetnictví
Na Příkopě 28
115 03 Praha 1
17. Splatnost dokladu k úhradě je 14 dnů od doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch účtu poskytovatele.
18. Smluvní strany se ve smyslu ustanovení § 1991 občanského zákoníku dohodly, že je objednatel oprávněn započíst jakoukoli svou peněžitou pohledávku za poskytovatelem, ať splatnou či nesplatnou, oproti jakékoli peněžitě pohledávce poskytovatele za objednatel, ať splatné či nesplatné.

Článek IV Licenční ujednání

1. Poskytnuté programové a technické prostředky podle této smlouvy je objednatel oprávněn užívat od okamžiku instalace/implementace.
2. Poskytovatel poskytuje objednateli nevýhradní, místně neomezenou a časově omezenou (na předplacené období) licenci, umožňující užívat poskytnuté programové prostředky pouze pro vnitřní potřebu objednatele, a to bez omezení počtu uživatelů a počtu koncových zařízení objednatele.
3. Objednatel není povinen licenci využít.
4. Licence poskytnuté dle této smlouvy se vztahují i na veškeré poskytnuté aktualizace (tj. update/upgrade/patch/hotfix atd.).

Článek V Práva a povinnosti smluvních stran

1. Poskytovatel je povinen zajistit, že technickou část plnění dle této smlouvy budou provádět výhradně kvalifikované osoby - IT specialisté v oblasti bezpečnosti, z nichž každý má platnou certifikaci minimálně úrovně Check Point Certified Security Expert (CCSE). Dále je poskytovatel povinen disponovat po celou dobu trvání této smlouvy minimálně dvěma vzájemně zastupitelnými specialisty s touto úrovní certifikace. Poskytovatel je povinen kdykoliv po dobu účinnosti této smlouvy na výzvu objednatele tyto skutečnosti doložit, a to do 5 pracovních dnů od doručení výzvy.
2. Změna v kvalifikovaných osobách může být provedena pouze se souhlasem objednatele. Odsouhlasení změny bude provedeno e-mailem alespoň jedním pověřeným zástupcem objednatele, bez povinnosti uzavřít dodatek k této smlouvě.
3. Objednatel si vyhrazuje právo požádat e-mailem poskytovatele o výměnu některé z osob poskytujících plnění dle této smlouvy z důvodu opakované nespokojenosti s kvalitou jí odváděné práce nebo nedostatečnou komunikací s objednatelem. Poskytovatel se zavazuje tuto výměnu neprodleně provést.
4. Poskytovatel musí být oprávněn od okamžiku uzavření této smlouvy zakládat servisní požadavky na supportním portále společnosti Check Point Software Technologies (viz <https://help.checkpoint.com/s/create-new-sr>). Poskytovatel je povinen kdykoliv po dobu účinnosti této smlouvy na výzvu objednatele tyto skutečnosti doložit, a to do 5 pracovních dnů od doručení výzvy.
5. Poskytovatel bere na vědomí, že mu nemusí být objednatelem umožněn vzdálený přístup k podporovaným systémům Check Point, ani k jiným serverům.
6. Poskytovatel se zavazuje, že jeho pracovníci se budou pohybovat pouze ve vyhrazených prostorách v místech plnění a za přítomnosti oprávněné osoby objednatele.
7. Poskytovatel je oprávněn požadovat po objednateli po dobu trvání této smlouvy poskytnutí nezbytných informací, podkladů a dokladů nutných k plnění předmětu této smlouvy.
8. Poskytovatel je povinen upozornit včas objednatele písemně na nedostatečnou součinnost pověřených pracovníků objednatele, pokud z toho důvodu dojde nebo hrozí, že dojde k ohrožení kvality nebo termínů poskytovaných služeb.

9. Objednatel si vyhrazuje právo upozornit včas poskytovatele na nedostatečnou součinnost pověřených pracovníků poskytovatele, pokud by z tohoto důvodu mohlo dojít k ohrožení kvality poskytovaných služeb.
10. Poskytovatel se zavazuje dodržovat bezpečnostní požadavky objednatele uvedené v příloze č. 2 a č. 3 této smlouvy.

Článek VI

Smluvní pokuty a úrok z prodlení

1. V případě prodlení poskytovatele ve lhůtě k předání plnění dle čl. II odst. 1 této smlouvy je objednatel oprávněn požadovat smluvní pokutu ve výši 1000,- Kč za každý den prodlení.
2. V případě prodlení poskytovatele ve lhůtě k odstranění nahlášeného problému vysoké priority dle přílohy č. 1 této smlouvy je objednatel oprávněn požadovat smluvní pokutu ve výši 300 Kč za každou hodinu prodlení.
3. V případě prodlení poskytovatele ve lhůtě k odstranění nahlášeného problému střední priority dle přílohy č. 1 je objednatel oprávněn požadovat smluvní pokutu ve výši 200 Kč za každou hodinu prodlení.
4. V případě prodlení poskytovatele ve lhůtě k odstranění nahlášeného problému nízké priority dle přílohy č. 1 je objednatel oprávněn požadovat smluvní pokutu ve výši 100 Kč za každou hodinu prodlení.
5. V případě porušení závazku mlčenlivosti poskytovatele dle čl. IX odst. 3 je objednatel oprávněn požadovat smluvní pokutu ve výši 20 000 Kč, a to za každé takové porušení.
6. V případě prodlení objednatele v úhradě daňového dokladu má poskytovatel právo požadovat úrok z prodlení podle příslušných ustanovení předpisů občanského práva.
7. Smluvní pokuta i úrok z prodlení jsou splatné do 14 dnů od doručení příslušného dokladu povinné smluvní straně. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu povinného ve prospěch účtu oprávněného.
8. Smluvní pokutou není dotčeno právo na náhradu škody.

Článek VII

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 VIII **Výpověď, odstoupení od smlouvy**

1. Smlouva se uzavírá na dobu neurčitou.
2. Smlouvu lze ukončit výpovědí. V případě výpovědi ze strany objednatele výpovědní lhůta činí 3 měsíce a počíná běžet prvním dnem měsíce následujícího po měsíci, v němž byla výpověď doručena poskytovateli. Pokud smlouvu vypoví poskytovatel, výpovědní lhůta činí 6 měsíců. Poskytovatel není oprávněn vypovědět smlouvu v průběhu prvního roku účinnosti této smlouvy.
3. Smlouvu lze rovněž ukončit odstoupením v případě podstatného porušení smlouvy jednou ze smluvních stran.
4. Za podstatné porušení smlouvy je považováno zejména:
 - ze strany poskytovatele nefunkčnost/neposkytování služeb specifikovaných v příloze č. 1 této smlouvy, a to po dobu delší než 15 kalendářních dnů,
 - ze strany poskytovatele nedodržení kvalifikačních předpokladů dle čl. V, odst. 1,
 - za poskytovatele nedoložení kvalifikace dle čl. V odst. 1, a to ani v objednatelům dodatečně stanovené lhůtě,
 - za poskytovatele nesplnění požadavku dle čl. V odst. 4, a to ani v objednatelům dodatečně stanovené lhůtě,
 - za poskytovatele nedoložení pojištění dle čl. IX, a to ani v objednatelům dodatečně stanovené lhůtě,
 - ze strany objednatele prodlení s úhradou daňového dokladu, a to po dobu delší než 30 dnů.
5. Smluvní strany se dohodly, že objednatel je oprávněn kdykoliv v průběhu insolvenčního řízení zahájeného na majetek poskytovatele odstoupit od smlouvy.
6. Odstoupení od smlouvy je účinné dnem doručení oznámení o odstoupení druhé smluvní straně.

Článek IX **Ostatní ujednání**

1. Poskytovatel je povinen mít po dobu účinnosti této smlouvy uzavřeno pojištění pro případ vzniku odpovědnosti za škodu způsobenou třetí osobě v souvislosti s plněním této smlouvy, a to s pojistným plněním ve výši nejméně 5 000 000 Kč (slovy: pět milionů korun českých).
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. Poskytovatel se zavazuje zajistit, že jeho pracovníci, kteří se budou podílet na plnění podle této smlouvy, zachovají mlčenlivost o všech skutečnostech, se kterými se u objednatele v průběhu plnění seznámí a které nejsou veřejně známy. Povinnost mlčenlivosti trvá i po skončení platnosti této smlouvy.
4. Ústní i písemná komunikace mezi objednatelům a poskytovatelem bude probíhat v českém jazyce, pokud nebude smluvními stranami dohodnuto jinak.

Článek X Závěrečná ustanovení

1. Smlouva nabývá platnosti a účinnosti dnem podpisu obou smluvních stran.
2. Smlouva může být měněna a doplňována pouze formou písemných, vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran, není-li ve smlouvě stanoveno jinak.
3. Tato smlouva a právní vztahy s ní související se řídí zákonem č. 89/2012 Sb., občanský zákoník, a ostatními souvisejícími platnými právními předpisy České republiky.
4. 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.
5. Smlouva je vyhotovena ve třech vyhotoveních s platností originálu, z nichž objednatel obdrží dvě a poskytovatel jedno vyhotovení.
6. Součástí této smlouvy jsou následující přílohy:

Příloha č. 1	Dohoda o úrovni poskytovaných služeb, SLA
Příloha č. 2	Bezpečnostní požadavky objednatele
Příloha č. 3	Obecná pravidla pro dodavatele v oblasti bezpečnosti IT

V Praze dne: 3. 8. 2021

Za objednatele:

Ing. Milan Zirnšák
ředitel sekce informatiky

Ing. Zdeněk Vírůs
ředitel sekce správní

V Praze dne: 27. 7. 2021

Za poskytovatele:

Ing. Tomáš Příbyl
předseda představenstva



Corpus Solutions a.s.
Štětškova 1638/18
140 00 Praha 4
IČ: 25764616 DIČ: CZ25764616

Dohoda o úrovni poskytovaných služeb, SLA

Podpora a správa produktů Check Point

Service Level Agreement

Tento Service Level Agreement (SLA) je dohodnut mezi Objednatel a Poskytovatelem služby a popisuje způsob zajištění a provozování služby a s ní souvisejících procesů.

1. Podpora od výrobce:

Podpora Collaborative Enterprise Support - Standard - Podpora Objednateli na poskytnutá HW a SW licence od výrobce - společnosti Check Point:

Režim podpory **Collaborative Enterprise Support Standard** se řídí podmínkami na pokrytí služeb společnosti Check Point dle daného supportu.

Rozsah

Přímá odezva na prioritu 1 (dle specifikace výrobce dostupné na https://www.checkpoint.com/support-services/support-plans/)	30 minut
Přímá odezva na prioritu 2 (dle specifikace výrobce dostupné na https://www.checkpoint.com/support-services/support-plans/)	4 hod
CheckPoint Basic SLA (garance poskytovatele CCSP)	5*9h Pracovní den
Pokročilý přístup objednatel do rozšířené znalostní databáze CheckPoint	Ano
Hardware RMA (zaslání HW při reklamaci)	zaslání stejný pracovní den (při uznání závady TAC ¹ do 14 hod pražského času)
Hardware RMA (zaslání HW při reklamaci)	následující pracovní den (při uznání závady TAC ² po 14 hod pražského času)
Kontaktní úroveň podpory	první úroveň podpory
Hotfixy SW produktů CheckPoint	Ano
Upgrade a Update SW produktů CheckPoint	Ano
Originální CD/DVD média vydaná CheckPoint	2 ks

Služba DDoS Management (VA2)

- APSolute Vision je jednotný systém pro správu a monitorování Check Point zabezpečení sítě proti DDoS útokům. Poskytuje pokročilé možnosti správy prvků prostřednictvím jedinečného mechanismu podpory zařízení typu plug-and-play, včetně počátečního nastavení zařízení, průběžné údržby, správy certifikátů SSL, hlášení v reálném čase, měření využití kapacity, forenzní analýzy, plánování úkolů a dalších. Poskytuje automatizaci procesů monitorování a údržby napříč všemi zařízeními, která spravuje, a zahrnuje centrální úložiště důležitých informací o zařízeních pro IT manažery, kteří snadno najdou podrobnosti o hardwarové platformě, aktualizaci a správu verzí softwaru a nainstalované

¹ Stanoveno v rámci specifikace výrobce dostupné na <https://www.checkpoint.com/support-services/support-plans>

² Stanoveno v rámci specifikace výrobce dostupné na <https://www.checkpoint.com/support-services/support-plans>

licence. Ve výsledku zajišťuje nepřetržité poskytování služeb po celou dobu životnosti zařízení.

Služba **APSolute Vision Analytics (AMS)**

- roční subscripce na analytický nástroj k virtuální management appliance, kapacita útoků do 20 Gbps.

Služba **Active Attackers Feed (AAF)**

- informace týkající se zdrojů útoků nedávno zapojených do útoků DDoS
- inteligence v reálném čase
- preventivní ochrana před vznikajícími hrozbami specifickými pro DDoS, včetně vyvíjejících se botnetů IoT a nových vektorů útoků DNS.
- Ochrana před známými útočníky (sběr dat ze své cloudové DDoS ochrany, z honeypotů, dalších služeb).
- Data procházejí přes nástroje umělé inteligence (AI), z nich je vytvářen dynamický seznam, který se pravidelně updatuje do lokálního DDoS protektoru

Služba **DDoS Behavioral Protection and IPS Updates (SUS)**

- ochrana proti nejnovějším známým útočným nástrojům a zranitelnostem.
- aktualizace zahrnují DoS flooding nástroje, slow DoS útoky a nástroje, DoS single-packet zranitelnosti a kritické data center (DC) aplikační zranitelnosti.
- možnost blokovat pomocí GEO lokace v případě použití obou služeb AAF a SUS

2. Podpora od poskytovatele:

Podpora objednateli na poskytnutá HW a SW licence od poskytovatele zahrnuje:

- Telefonní podpora při řešení systémových incidentů a problémů spojených se specifikovanými službami výše do lhůty uvedené dále po nahlášení problému na HelpDesk poskytovatele služeb.
- Vyžaduje-li situace zásah u objednatele, zajištění příjezdu technika na místo do lhůty uvedené dále od nahlášení problému na HelpDesk poskytovatele služeb.
- Poskytovatel garantuje odstranění problému nejpozději do lhůty uvedené dále po nahlášení problému na HelpDesk poskytovatele služeb.
- Podpora po emailu, při řešení provozních problémů.
- Garance vyřešení problémů na místě u objednatele v případě vadného HW Check Point (appliance), odvoz vadného a doručení nového HW, zajištění výměny u výrobce (při opravě budou použity vždy nové díly).
- Přímá pomoc při aplikaci nových verzí SW, řešení případných problémů při instalaci na zařízení objednatele na místě u objednatele.
- Provedení upgrade SW (na základě požadavku objednatele) jedenkrát ročně pro každý jednotlivý systém (dle seznamu Check Point licencí a služeb).
- Komunikace poskytovatele s výrobcem Checkpoint při řešení Ticketů založených při řešení uvedených problémů, případná eskalace těchto problémů v rámci podpory u výrobce.
- Garance vyřešení problémů v časech definovaných dle klasifikace jejich závažnosti (dále uvedeno).

▪ **Detaily autorizace a popis komunikace**

Problém ohlašuje oprávněná osoba objednatele na HelpDesk poskytovatele, primárně telefonicky na linku dispečinku poskytovatele. Náhradní způsob ohlášení problému je prostřednictvím webu do interního incident management systému poskytovatele nebo e-mailem. V případě telefonického nahlášení problému musí neprodleně následovat zaslání popisu e-mailem.

Hlášení problému (včetně závad) musí obsahovat

- datum a čas hlášení
- místo, adresu a jméno kontaktní osoby, která problém nahlásila
- stručný popis problému

Problém se hlásí na HelpDesk:

Telefon: +420 – 241 020 701 (v pracovních dnech od 8:00 – 18:00 hod.)
+420 – 241 020 701 (mimo pracovní dobu)

Email: helpdesk@corpus.cz

www stránky aplikace helpdesk: <https://jira.corpus.cz>

Problémy jsou hlášeny pouze oprávněnými osobami objednatele:

Jméno a příjmení	E-mail	Telefon	Mobil
------------------	--------	---------	-------

▪ **Provozní doba služby**

Vyjma závad HW poskytovatel poskytuje podporu na vady nahlášené objednatelem na Helpdesk poskytovatele v časovém období 8-18 hod v pracovních dnech v místech plnění objednatele, a to v reakčních dobách pro jednotlivé kategorie priorit dle níže uvedené tabulky

▪ **Podpora v rámci procesu HW RMA**

V rámci hardware RMA požadavku nahlásí objednatel poskytovateli dohodnutými standardními komunikačními kanály požadavek na zahájení RMA procesu u výrobce Checkpoint. Společně s požadavkem zašle objednatel popis stávající situace, která vede k požadavku RMA. Po ověření ze strany poskytovatele, zahájí poskytovatel proces RMA vůči výrobci dle jeho standardních procedur. Po schválení požadavku RMA ze strany TAC výrobce bude nové HW zařízení zasláno na adresu objednatele. Jakmile nové HW zařízení objednatel obdrží, bude neprodleně informovat poskytovatele. Ten do 24 hodin od obdržení informace o doručení HW zařízení na adresu objednatele zajistí přítomnost svých pracovníků v místě objednatele pro zajištění výměny vadného zařízení ve spolupráci se zaměstnanci objednatele. Poskytovatel zároveň ve spolupráci s pracovníky objednatele zajistí zpětné odeslání vadného HW zařízení zpět výrobci.

▪ **Cíle služby, termíny a standardní měřené parametry**

Poskytovatel se zavazuje, že vyvine maximální úsilí, které lze spravedlivě požadovat, k odstranění problému.

Standardní měřené parametry jsou:

- doba odezvy
- doba vyřešení problému

Parametry SLA pro DDoS s dobou plnění v pracovní dny od 8:00 do 18:00

Priorita	Doba odezvy(Response time)	Čas k odstranění problému (Fix time) do
Vysoká	30 minut	4 hodin
Střední	30 minut	24 hodin
Nízká	30 minut	do 16:00 následující pracovní den

▪ **Pravidla pro určení priority a dopadu**

V požadavku na vyřešení problému objednatel specifikuje jeho prioritu pro jednotlivá SW/zařízení v mezích dle níže uvedené tabulky:

Priorita	Popis	Příznaky
Vysoká	Závada se týká DDoS zařízení, jehož výpadek způsobuje, že významná část uživatelů a aplikací má znemožněn přístup z/do sítě LAN/WAN/DMZ/Internetu a neexistuje postup pro náhradní řešení problému. Zahrnuje i jednotlivé aplikace spadající pod Zákon o kybernetické bezpečnosti.	<ul style="list-style-type: none"> ▪ Nefunkční jednotlivé prvky modulárního řešení DDoS
Střední	Závada se týká DDoS zařízení, jehož výpadek způsobuje, že jen část uživatelů a aplikací má znemožněn přístup z/do sítě LAN/WAN/DMZ/Internetu a existuje postup pro náhradní řešení problému.	<ul style="list-style-type: none"> ▪ Výpadek jednoho DDoS prvku ve skupině řešení ▪ nefunkční část bezpečnostní řešení
Nízká	Provozní problémy, které omezují pouze jednotlivé uživatele.	<ul style="list-style-type: none"> ▪ bezpečnostní prvek je v provozuschopném stavu, přesto se v logu OS DDoS zařízení / Managementu celého řešení Checkpoint vyskytují chyby

Poskytovatel může po prozkoumání problému navržený stupeň důležitosti požadavku ve spolupráci – po schválení objednatelem překlasifikovat. V případě, že objednatel nesouhlasí se stanovením klasifikace, je problém eskalován podle Eskalačního procesu.

▪ **Eskalační proces**

V případě, že nestandardní situaci při řešení problému není možné vyřešit v rámci dané úrovně, pracovníci této úrovně řeší tuto situaci s pracovníkem nejbližší vyšší úrovně.

1. úroveň oprávněné osoby/Service Desk objednatele a HelpDesk poskytovatele
2. úroveň ředitel odboru objednatele a jmenovaný Service Manager poskytovatele
3. úroveň ředitel sekce informatiky objednatele a ředitel společnosti poskytovatele

▪ **Definice pojmů**

Response time (doba odezvy) – jedná se o reakční dobu, kdy je objednateli sděleno, že jeho požadavek byl zaevidován a je zpracován.

Fix time – jedná se o dobu od doby nahlášení do doby, kdy je nahlášený problém vyřešen a to ať dočasným řešením (work-around), ale z hlediska objednatele plně funkčním nebo je vyřešen (kompletně). V případě, že je požadavek znovu otevřen, je doba potřebná k jeho opětovnému vyřešení přičtena k době, po kterou byl požadavek již řešen.

Priorita vysoká – fix time 4 hod;

znamená, že nahlášený problém bude kompletně vyřešen nejpozději do 4 hodin od nahlášení, v garantované době poskytování služby. V případě nutnosti dodání nové verze SW, hotfixu, servis patce, upgrade atd. bude oprava provedena do 4 hodin od obdržení nové verze SW, hotfixu, servis patce, upgrade atd. od výrobce.

Priorita střední – fix time 24 hod;

znamená, že nahlášený problém bude kompletně vyřešen nejpozději do 24 hodin od nahlášení, v garantované době poskytování služeb. V případě nutnosti dodání nové verze SW, hotfixu, servis patce, upgrade atd. bude oprava provedena do 24 hodin od obdržení nové verze SW, hotfixu, servis patce, upgrade atd. od výrobce.

Priorita nízká – fix time do 16:00 následujícího pracovního dne;

znamená, že každý nahlášený problém bude kompletně vyřešen nejpozději do 16:00 následujícího pracovního dne od nahlášení v garantované době poskytování služby.

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“. 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 vyhlášenými 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 nepustit 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 započítáním 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.

Obecná pravidla pro dodavatele v oblasti bezpečnosti IT

- 1) Pokud jsou tato obecná pravidla v rozporu s ustanovením textu smlouvy nebo zadávací dokumentace nebo její jinou přílohou, má přednost ustanovení textu smlouvy nebo zadávací dokumentace nebo její jiná příloha.
- 2) Dodavatel je povinen 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. Povinnost mlčenlivosti není časově omezena.
- 3) Dodavatel je rovněž povinen chránit informace, které nejsou veřejně dostupné, zejména předanou dokumentaci, před jejich prozrazením a/nebo zpřístupněním neoprávněným osobám a dále použít získané informace výhradně pro účely plnění smlouvy s ČNB.
- 4) Dodavatel nemá vzdálený přístup k systémům a do počítačové sítě ČNB.
- 5) Pracovníci dodavatele, kteří budou samostatně přistupovat k informačním systémům a systémovému prostředí ČNB, se před nebo při prvním přístupu musí seznámit s bezpečnostními požadavky a svými povinnostmi vyplývajícími z vnitřních předpisů ČNB.
- 6) Dodavatel a jeho pracovníci nejsou oprávněni:
 - a) obcházet bezpečnostní mechanismy prostředků výpočetní techniky;
 - b) sdělovat své přístupové údaje k systémům ČNB;
 - c) sdílet přístup k systémům ČNB (umožnit jinému pracovat pod uživatelským oprávněním);
 - d) provádět akce požadované třetí osobou (instalace softwaru, návštěva webových stránek apod.) bez ověření oprávněnosti požadavku.
- 7) Dodavatel a jeho pracovníci jsou povinni:
 - a) okamžitě nahlásit sekci informatiky ČNB, pokud identifikují možnost obejití bezpečnostních mechanismů prostředků výpočetní techniky. To neplatí pro dodavatele, jejichž předmět smlouvy obsahuje tuto činnost;
 - b) při opuštění pracovní stanice stanici uzamknout (např. vytažením multifukčního průkazu ze stanice) nebo se odhlásit, a ověřit, že k odhlášení/uzamčení opravdu došlo;
 - c) bezpečně zlikvidovat nepotřebná výměnná média (např. CD/DVD, flash disk, paměťová karta) prostřednictvím služby HelpDesku ČNB;
 - d) bez prodlení odebrat z tiskárny vytištěné dokumenty, popřípadě pro zajištění důvěrnosti použít zabezpečený tisk, pokud to nastavení tiskárny umožňuje;
 - e) v případě detekce viru nebo podezření na přítomnost škodlivého kódu neprodleně kontaktovat HelpDesk ČNB a stanici kompletně prověřit antivirovým programem za případné spolupráce HelpDesku ČNB.
- 8) Pracovníci dodavatele nesmí:
 - a) zaznamenávat heslo tak, aby mohlo být snadno identifikováno (týká se i zapisování do elektronických dokumentů, např. Notepad). Pro uchování je možné použít například bezpečné úložiště na čipové kartě uživatele (SmartNotes);

- b) používat stejná hesla v systémech ČNB a pro přístup do dalších systémů a aplikací mimo ČNB (např. soukromá e-mailová schránka, Facebook, LinkedIn).
- 9) Pracovníci dodavatele nejsou oprávněni:
- používat soukromou e-mailovou schránku pro činnosti související s plněním dle smlouvy, kromě výjimečné situace, která nesnese odkladu a při níž hrozí nebezpečí z prodlení v případě nedostupnosti nebo poruchy pracovního e-mailu;
 - nastavovat automatické přeposílání e-mailů z pracovní e-mailové adresy mimo systémové prostředí ČNB;
 - ukládat jiné než veřejné informace mimo úložiště pod správou ČNB nebo dodavatele (případně pod správou smluvně zajištěného partnera), zejména do cloudových služeb (např. uloz.to, leteckaposta.cz, Google Disk, Microsoft OneDrive a další).
- 10) Dodavatel a jeho pracovníci nejsou oprávněni:
- nepovoleně používat, kopírovat a šířit software, jako např.:
 - instalovat nebo spouštět na počítačích ČNB soukromě pořízený software (včetně softwaru licencovaného na uživatele jako soukromou osobu);
 - instalovat nebo spouštět na počítačích ČNB z internetu stažený software (včetně komerčního software, software typu shareware, freeware, public domain a software licencovaného modelem GPL – General Public Licence). To neplatí v případech, kdy předmět smlouvy obsahuje tuto činnost;
 - instalovat či přenášet software ve vlastnictví ČNB na jiné počítače ČNB, na své soukromé počítače nebo na počítače třetích stran nebo pořizovat kopie softwaru instalovaného v počítači ČNB. To neplatí
 - pro situace výslovně schválené a popsané v jiném vnitřním předpisu (např. vzdálený přístup ze zařízení, které není ve vlastnictví ČNB) a
 - v případech, kdy předmět smlouvy obsahuje tuto činnost;
 - používat nebo poskytnout neoprávněně jiným uživatelům sériová čísla, licenční klíče, hardwarové klíče nebo jiné technické prostředky sloužící k zajištění ochrany nebo jednoznačné identifikaci vlastníka licence softwaru získané v ČNB;
 - bránit spouštění nástrojů sloužících pro automatizované kontroly nainstalovaného a spouštěného softwaru a provádět činnosti, které by vedly ke zkreslení získaných dat z těchto nástrojů.

Archivace elektronické pošty

- Zpráva zaslaná tak, že alespoň jedním z adresátů zprávy je emailová adresa ...@cnb.cz, se ukládá současně s přijetím i do dlouhodobého archivního úložiště.
- Veškeré zprávy odesílané z emailové adresy ...@cnb.cz se ukládají do dlouhodobého archivního úložiště současně s odesláním.

Kontrola přístupu na Internet

Z důvodu zvláštní povahy činnosti ČNB a z toho plynoucí povinnosti zajištění bezpečnosti informačních systémů ČNB, z nichž některé jsou součástí kritické informační infrastruktury státu, jsou přístupy uživatelů na Internet ze sítě ČNB automaticky zaznamenávány na úrovni domén 2. řádu (tj. např. idnes.cz).