Smlouva o dílo

(dále jen „smlouva“)
uzavřená podle ust. § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „občanský zákoník“) mezi dále uvedenými smluvními stranami podle svého prohlášení plně svéprávnými, a to:

Objednatel:	**Zdravotnická záchranná služba Královéhradeckého kraje**
se sídlem:	Hradecká 1690/2a, 500 12 Hradec Králové
IČ:	481 45 122
zastoupena:	MUDr. Liborem Senetou, ředitelem
bankovní spojení:	[redacted]
	účet č. [redacted]
zapsaná:	v obchodním rejstříku Krajského soudu v Hradci Králové pod sp. zn. Pr./829

(dále jen „**objednatel**“)

a

Zhotovitel:	**DATASYS s.r.o.**
se sídlem:	Praha 3, Jeseniova 2829/20, PSČ: 130 00
IČ:	612 49 157
DIČ:	CZ61249157, plátce DPH
zastoupena:	Bc. Martinem Novákem, prokuristou
bankovní spojení:	[redacted]
	účet č. [redacted]
zapsaná:	v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 28862
kontaktní osoba:	[redacted]

(dále jen „**zhotovitel**“)

(dále též společně jako „**smluvní strany**“)

Čl. I.
Úvodní ustanovení

1. Tato smlouva je uzavírána se zhotovitelem pro analýzu kybernetické bezpečnosti ICT objednatele s návrhem cílového stavu, provedení testu zranitelnosti.
2. Zhotovitel se zavazuje splnit předmět této smlouvy nejen v souladu s touto smlouvou, ale také v souladu s jeho nabídkou, která předcházela uzavření této smlouvy. Nabídka zhotovitele podle předchozí věty tvoří nedílnou součást této smlouvy jako příloha č. 1.

Čl. II.
Předmět smlouvy

1. Zhotovitel se zavazuje provést na svůj náklad a nebezpečí pro objednatele dílo v rozsahu a objemu dle této smlouvy vč. jejích příloh a objednatel se zavazuje provedené dílo převzít a zaplatit zhotoviteli za toto dílo dohodnutou cenu, to vše za podmínek stanovených dále touto smlouvou.
2. Pro účely této smlouvy se dílem rozumí souhrn těchto dílčích plnění:
    i. Hodnocení stavu kybernetické bezpečnosti provedené ve struktuře dle relevantních požadavků zákona č. 104/2017 Sb., novely zákona č. 181/2014 Sb., tzv. zákona o kybernetické bezpečnosti, a jeho doprovodné vyhlášky, přičemž součástí díla je: (a) Katalog IT služeb a jejich požadovaných parametrů, tzv. primárních aktiv; (b) Dokument „Analýza stavu kybernetické bezpečnosti" s návrhem doporučených opatření; (c) Přehledy dotazníkových šetření „Hodnocení kybernetické bezpečnosti".
    ii. Provedení testu zranitelnosti, realizovaného asistovanou zápůjčku hardwarové sondy nástroje Greenbone Security Manager (GSM) pro získání přehledu o zařízeních v síti a zejména pro zjištění a zvládání zranitelných služeb sítě. Hardwarová sonda je ve vlastnictví zhotovitele.
3. Dílo bude provedeno v souladu s požadavky na něj kladenými touto smlouvou. Zhotovitel se zavazuje poskytnout plnění v takové kvalitě, jež je s přihlédnutím k zájmům a požadavkům objednatele a okolnostem prováděného díla pro objednatele nejvhodnější.

Čl. III.
Cena díla a platební podmínky

1. Celková cena díla je **138 200 Kč** bez DPH (slovy: jedno sto třicet osm tisíc dvě stě korun českých).
2. Celková cena díla zahrnuje jednotlivá dílčí plnění, jak jsou uvedena a specifikována v Čl. II. této smlouvy takto:
    a. cena za dílčí plnění dle čl. II.2.i. činí 99 200,- Kč,
    b. cena za dílčí plnění dle čl. II.2.ii. činí 39 000,- Kč,
3. Celková cena díla je stanovena dohodou smluvních stran, zahrnuje veškeré náklady zhotovitele spojené se zhotovením díla, nebude měněna (je nepřekročitelná), kromě těch případů, kdy dojde ke změně právních předpisů, např. změny sazby DPH; případně nedohodnou-li se smluvní strany jinak.
4. Objednatel na předmětné dílo neposkytuje žádnou zálohu.
5. Cena díla bude uhrazena na základě daňového dokladu vystaveného po řádném, úplném a včasném dokončení dílčího plnění, resp. po protokolárním předání a převzetí bezvadného a řádně a včas dokončeného dílčího plnění a po odsouhlasení předávacího (akceptačního) protokolu určeným zástupcem objednatele.
6. Objednatel provede úhradu výhradně v české měně na základě příslušného daňového dokladu, který musí obsahovat všechny náležitosti dle § 28 a násl. zákona č. 235/2004 Sb., o dani z přidané hodnoty ve znění pozdějších předpisů (dále jen „zákon o DPH"). Faktura je splatná 30 dnů po doručení příslušné faktury v řádném stavu objednateli. Je-li faktura vystavena chybně, nebo není-li doložena sjednanými přílohami, je objednatel oprávněn ji vrátit, přičemž v tomto případě není v prodlení s úhradou pohledávky účtované příslušnou fakturou.

7. Smluvní strany si sjednaly, že veškerá další komunikace, není-li ve smlouvě stanoveno výslovně jinak, může být vedena v elektronické podobě, přičemž elektronická sdělení nemusí být opatřena uznávaným elektronickým podpisem a ani nemusí jít o autorizovanou konverzi dokumentů s výjimkou právních jednání, která v elektronické podobě musí být opatřena uznávaným elektronickým podpisem. Smluvní strany tímto zrovnoprávňují formu písemné a elektronické komunikace.

Čl. IV.
Termín a místo plnění

1. Zhotovitel se zavazuje provést dílčí plnění dle čl. II.2.i. a čl. II.2.ii této smlouvy nejpozději do 40 kalendářních dnů ode dne účinnosti této smlouvy.
2. Místem plnění díla je sídlo objednatele.

Čl. V.
Práva a povinnosti objednatele

1. Objednatel je oprávněn dílo a jeho provádění kdykoliv kontrolovat, zda je prováděno v souladu s touto smlouvu.
2. Objednatel se zavazuje poskytovat zhotoviteli součinnost potřebnou k řádnému provedení díla. Zejména, nikoliv však výlučně, se jedná o poskytnutí veškeré relevantní dokumentace (popis rozhraní systémů objednatele; popis rozhraní externích systémů, popis procesů objednatele apod.), zajištění účasti svých zaměstnanců na vyžádaných konzultačních schůzkách, případně zajištění účasti zaměstnanců třetích stran na vyžádaných konzultačních schůzkách a přístup k IT infrastruktuře objednatele.

Čl. VI.
Práva a povinnosti zhotovitele

1. Zhotovitel se zavazuje dílo řádně provést, předat objednateli ve stanoveném termínu, požadované kvalitě a v požadovaném provedení.
2. Zhotovitel je povinen důsledně a komplexně zjistit veškeré potřebné informace, vyžádat si nezbytné podklady a prověřit veškeré možnosti daného řešení a takto zjištěné poznatky analyzovat. Zhotovitel je povinen při plnění předmětu díla postupovat s odbornou péčí.
3. Zhotovitel prohlašuje, že má dostatečné znalosti, schopnosti a prostředky k řádnému provedení díla.
4. Zhotovitel odpovídá za výkony svých zaměstnanců a zástupců, jakož i za přesnost a úplnost všech dat a informací předkládaných zhotovitelem objednateli pro účely poskytování plnění podle této smlouvy.
5. V případě, že objednatel nedodá zhotoviteli správné a úplné informace, neposkytne včas a řádně požadovanou součinnost či potřebné podklady anebo neumožní zhotoviteli přístup ke svým zaměstnancům anebo k IT infrastruktuře podle podmínek této smlouvy, pak zhotovitel neodpovídá za případné prodlení nebo vady díla. Zhotovitel si dále vyhrazuje právo prodloužit veškeré konečné termíny o dobu odpovídající každému takovému prodlení způsobenému objednatelem, v tomto

případě nebude mít objednatel právo požadovat po zhotoviteli zaplacení vzniklé škody či smluvní pokuty.

6. Objednatel souhlasí s tím, že zhotovitel může použít odkaz na obchodní firmu objednatele a typ poskytnuté služby jako referenci ve svých marketingových materiálech po dobu 3 let od udělení tohoto souhlasu.

Čl. VII.
Předání a převzetí díla

1. Zhotovitel splní svou povinnost provést dílo jeho řádným a včasným dokončením.
2. Zhotovitel je povinen písemně oznámit objednateli předem, že dokončené dílo bude připraveno k předání a převzetí. Objednatel je pak povinen do 5 pracovních dnů zahájit přejímací řízení.
3. Předání díla nastane na základě předávacího (akceptačního) protokolu. Předávací (akceptační) protokol bude datován a opatřen podpisy oprávněných pracovníků objednatele a zhotovitele.
4. Oprávněným zástupcem objednatele pro převzetí (akceptaci) díla je [redacted] e-mail: [redacted]

Čl. VIII.
Smluvní pokuty a náhrada škody

1. Ocitne-li se zhotovitel v prodlení s dokončením díla nebo jeho části, je objednatel oprávněn vyúčtovat zhotoviteli a zhotovitel se zavazuje zaplatit objednateli smluvní pokutu ve výši 0,05 % z hodnoty díla za každý i jen započatý den prodlení. Smluvní pokuta je splatná do 14 dnů od jejího uplatnění objednatelem a lze ji započíst proti nedoplatku ceny díla. Zaplacení smluvní pokuty nemá vliv na povinnost k náhradě škody, tedy zaplacením smluvní pokuty není dotčeno právo na náhradu škody vzniklé objednateli v příčinné souvislosti s porušením závazku zhotovitele provést dílo řádně a včas, a to i nad výši sjednané smluvní pokuty. Odstoupení od smlouvy nemá rovněž vliv na povinnost k úhradě smluvní pokuty dle tohoto bodu smlouvy. Smluvní strany prohlašují, že takto sjednaná smluvní pokuta je v souladu s dobrými mravy, poctivým obchodním stykem a její výše odpovídá hodnotě zajišťované povinnosti.
2. V případě prodlení se zaplacením peněžité částky je smluvní strana, která je se zaplacením v prodlení, povinna zaplatit druhé smluvní straně úrok z prodlení ve výši 0,05 % z nezaplacené částky za každý i jen započatý den prodlení.
3. V případě porušení povinností k ochraně důvěrných informací a závazku mlčenlivosti dle čl. X této smlouvy je smluvní strana, která poruší tyto povinnosti, zaplatit druhé smluvní straně smluvní pokutu ve výši 100 000 Kč za každé porušení takové povinnosti, a to do 14 dnů ode dne doručení faktury vystavené na její uhrazení.
4. Není porušením závazku objednatele nezajištění poskytnutí součinnosti třetích stran v případě, že objednatel učinil prokazatelně veškeré kroky vedoucí k získání takovéto součinnosti, které po něm lze spravedlivě vyžadovat s přihlédnutím ke všem okolnostem v dané situaci. V takovém případě zároveň není porušením závazku zhotovitele dodání díla v kvalitě odpovídající neposkytnutí součinnosti třetích stran a nelze dílo v příslušné části považovat za vadné.
5. Zaplacením smluvní pokuty není, jakkoliv dotčen nárok druhé smluvní strany na náhradu škody. Nárok na náhradu škody je druhá smluvní strana oprávněna uplatnit vedle smluvní pokuty v plné výši.

Čl. IX.
Záruka a odpovědnost za vady

1. Zhotovitel přejímá záruku za jakost provedeného díla a poskytuje záruku v délce trvání 6 měsíců (dále jen „záruční doba"), která počíná běžet dnem předání a převzetí celého řádně dokončeného díla, které je zbaveno všech vad a nedodělků. Zhotovitel není povinen aktualizovat dílo na základě událostí, ke kterým došlo po předání konečného díla a které nebylo možné před předáním konečného díla předpokládat.
2. Objednatel je povinen vady reklamovat u zhotovitele písemně, a to kdykoli po jejich zjištění. K projednání takto reklamovaných vad nastoupí zhotovitel bezodkladně, nejpozději však do 5 pracovních dnů, pokud nebude dohodnuto jinak. Z tohoto jednání bude pořízen zápis, který bude obsahovat údaje týkající reklamované vady a dohodu o termínu jejího odstranění. Reklamace může být učiněna i elektronicky, a to na shora uvedenou mailovou adresu. V případě změny této adresy je povinen zhotovitel neprodleně průkazně informovat objednatele o nové adrese.
3. Reklamaci lze uplatnit do posledního dne záruční doby, přičemž i reklamace odeslaná objednatelem v poslední den záruční doby se považuje za včas uplatněnou.
4. Pro případ vady díla sjednávají smluvní strany přednostně právo objednatele požadovat a povinnost zhotovitele poskytovat bezplatné odstranění vady, a to bez zbytečného odkladu.

Čl. X.
Ochrana informací a závazek mlčenlivosti

1. Důvěrnými informacemi se pro účely této smlouvy a po celou dobu trvání vzájemné spolupráce smluvních stran rozumí, bez ohledu na formu a způsob jejich sdělení či zachycení a až do doby jejich zveřejnění, jakékoli a všechny skutečnosti, které se smluvní strana v průběhu vzájemné spolupráce dozví, anebo které jí druhá smluvní strana v průběhu vzájemné spolupráce zpřístupní, jakož i sama existence těchto skutečností (dále jen „důvěrné informace").
2. Za důvěrné informace lze taktéž považovat zejména know-how, jímž se rozumí veškeré poznatky obchodní, výrobní, technické či ekonomické povahy související s činností smluvní strany a které nejsou běžně dostupné. Dále se považují za důvěrné informace takové informace, které jsou jako důvěrné výslovně některou ze stran označeny.
3. Smluvní strany jsou povinny zajistit utajení získaných důvěrných informací způsobem obvyklým pro utajování takových informací, není-li výslovně sjednáno jinak. Povinnost utajovat důvěrné informace zavazuje smluvní strany po dobu účinnosti této smlouvy a po dobu 2 let po ukončení smluvního vztahu založeného touto smlouvou. Strany mají právo požadovat navzájem doložení dostatečnosti utajení důvěrných informací. Strany jsou povinny zajistit utajení důvěrných informací i u svých zaměstnanců, zástupců, jakož i jiných spolupracujících třetích stran, pokud jim takové informace byly poskytnuty.
4. Smluvní strany se zavazují zachovávat plnou mlčenlivost o všech důvěrných informacích, ledaže se jedná o informace, které jsou veřejně přístupné, smluvní strana obdrží od zpřístupňující strany písemný souhlas zpřístupňovat danou důvěrnou informaci, či je-li zpřístupnění důvěrné informace vyžadováno zákonem nebo závazným rozhodnutím oprávněného orgánu.
5. V případě, že se zhotovitel v rámci provádění díla dostane k osobním údajům zaměstnanců, zákazníků nebo jiných osob, nebude tyto osobní údaje zpracovávat ani nikomu dalšímu ke zpracování předávat a zavazuje se o nich dodržet povinnost mlčenlivosti. Zhotovitel je povinen počínat si tak, aby jeho činností nedošlo k porušení zabezpečení osobních údajů. V případě, že by

v důsledku činnosti nebo nečinnosti zhotovitele přece jenom došlo k porušení zabezpečení osobních údajů, je zhotovitel povinen o tom bezodkladně, nejpozději však do 48 hodin, informovat objednatele.

6. Po ukončení účinnosti této smlouvy je každá ze smluvních stran povinna bez zbytečného odkladu po obdržení žádosti druhé strany vrátit druhé smluvní straně všechny poskytnuté materiály obsahující důvěrné informace včetně jejich případně pořízených kopií. O předání a převzetí se sepíše protokol podepsaný oběma smluvními stranami.

Čl. XI.
Odstoupení od smlouvy

1. Od této smlouvy může odstoupit kterákoliv smluvní strana, a to pro podstatné porušení této smlouvy druhou smluvní stranou. Právní účinky odstoupení od smlouvy nastávají doručením písemného oznámení o odstoupení druhé smluvní straně. Předpokladem pro takovéto odstoupení od smlouvy je předchozí písemné upozornění jedné strany straně druhé na existenci podstatného porušení smlouvy a neodstranění takovéhoto závadového stravu druhou smluvní stranou v určené přiměřené lhůtě, nejvýše však v délce 5 pracovních dnů.
2. Odstoupením od smlouvy se závazek zrušuje od počátku. V ostatním se odstoupení řídí obecnými ustanoveními občanského zákoníku.

Čl. XII.
Změna smlouvy

1. Tuto smlouvu lze měnit pouze písemným oboustranně potvrzeným ujednáním, výslovně nazvaným dodatek ke smlouvě. Jiné zápisy, protokoly apod. se za změnu smlouvy nepovažují. Tyto dodatky musí být číslovány.
2. Nastanou-li u některé ze stran skutečnosti bránící řádnému plnění této smlouvy, je povinna to ihned bez zbytečného odkladu oznámit druhé straně a vyvolat jednání zástupců oprávněných k podpisu smlouvy.

Čl. XIII.
Závěrečná ustanovení

1. Práva a povinnosti smluvních stran v této smlouvě výslovně neupravená se řídí českým právním řádem, zejména pak příslušnými ustanoveními občanského zákoníku a předpisy s tím souvisejícími.
2. Veškerá komunikace (s výjimkou právních jednání, pokud není výslovně ujednáno jinak) může být vedena elektronicky a nemusí být dle dohody stran podepsána uznávaným elektronickým podpisem. Příslušné e-mailové adresy si smluvní strany sdělí při podpisu této smlouvy. Smluvní strany zrovnoprávňují elektronickou a písemnou formu komunikace. Elektronicky mohou být zasílány i veškeré přílohy či podklady pro úkony stran činěné v souvislosti s touto smlouvou, aniž by muselo jít o autorizovanou konverzi dokumentů. Smluvní strany se zavazují doručení veškeré e-mailovou korespondence potvrzovat nejpozději následující pracovní den po jejím obdržení.
3. Případná neplatnost některého ustanovení této smlouvy nemá za následek neplatnost ostatních ustanovení. V případě, že kterékoliv ustanovení této smlouvy se stane neúčinným nebo neplatným,

smluvní strany se zavazují bez zbytečného odkladu nahradit takové ustanovení novým, které svým obsahem a smyslem odpovídá nejlépe obsahu a smyslu ustanovení původního.

4. Zhotovitel není oprávněn postoupit své pohledávky vůči objednateli vzniklé z této smlouvy nebo v souvislosti s ní na třetí osobu bez předchozího písemného souhlasu objednatele. Zhotovitel není oprávněn převést ani žádná jiná svá práva ani žádné povinnosti z této smlouvy na třetí osobu bez předchozího písemného souhlasu objednatele.
5. Strany si nepřejí, aby nad rámec výslovných ustanovení této smlouvy byly jakákoliv práva a povinnosti dovozovány z dosavadní či budoucí praxe zavedené mezi stranami či zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu plnění této smlouvy, ledaže je ve smlouvě výslovně sjednáno jinak.
6. Tato smlouva je sepsána ve dvou (2) stejnopisech s platností originálu, z nichž každá ze smluvních stran obdrží jedno (1) vyhotovení.
7. Smluvní strany prohlašují, že si tuto smlouvu pozorně přečetly, jejímu obsahu rozumí a že obsahuje jejich skutečnou a svobodnou vůli, na důkaz čehož připojují své podpisy
8. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami, účinnosti pak nabývá zveřejněním v registru smluv.
9. Nedílnou součástí smlouvy jsou tyto její přílohy:
   - příloha č. 1 – Nabídka zhotovitele
10. V případě rozporu smlouvy a přílohy má přednost smlouva.

V Hradci Králové dne -5. 12. 2022

Objednatel:

[redacted]

za **Zdravotnická záchranná služba Královéhradeckého kraje**
MUDr. Libor Seneta,
Ředitel

Zdravotnická záchranná služba
Královéhradeckého kraje
Hradecká 1690/2A
500 12 Hradec Králové
IČO: 48145122

V Praze dne -2. 12. 2022

Zhotovi[redacted]

za **DATASYS s.r.o.**

Bc. Martin Novák
prokurista

Příloha č. 1 Nabídka zhotovitele

DATA SYS

NABÍDKA

Posouzení stavu kybernetické bezpečnosti s návrhem doporučených kroků

Zadavatel
Zdravotnická záchranná služba Královehradeckého kraje
Hradecká 1690/2A
500 12 Hradec Králové

DATASYS s.r.o.
Jesenova 2829/20, 130 00 Praha 3
+420 225 308 111
datasys@datasys.cz
www.datasys.cz

POBOČKY
HRADEC KRÁLOVÉ, Hořická 283/22, 500 02
PLZEŇ, Schwarzova 50, 301 00
DĚČÍN, Labská 694/24, 405 02
OSTRAVA, Shidenská 6202/17, 708 33

HOTLINE - SERVIS HW
Jesenova 2829/20, 130 00 Praha 3
+420 225 308 250
helpdesk@datasys.cz
IČO: 61249157 / DIČ: CZ61249157

Posouzení stavu kybernetické bezpečnosti s návrhem doporučených kroků	
ZÁKLADNÍ IDENTIFIKAČNÍ ÚDAJE	
Uchazeč	
Obchodní firma nebo název / obchodní firma nebo jméno a příjmení:	DATASYS s.r.o.
Sídlo / místo podnikání:	Jeseniova 2829/20, 130 00 Praha 3
IČO:	61249157
DIČ:	CZ61249157
Osoba oprávněná jednat jménem či za uchazeče:	Bc. Martin Novák, prokurista
Spisová značka:	C 28862 u Městského soudu v Praze
Bankovní spojení (číslo účtu):	[redacted]
Číslo účtu:	[redacted]
Kontaktní osoba:	[redacted]
Telefon:	[redacted]
Email:	[redacted]

Obsah

1. Předmět nabídky

Tento dokument je primárně nabídkou na systematické posouzení stavu kybernetické bezpečnosti informačních a komunikačních systémů Zadavatele a doplňkově též na provedení několika praktických bezpečnostních testů.

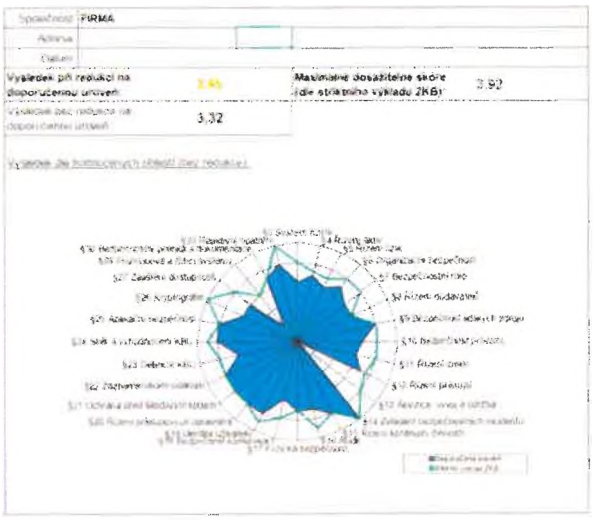
Hodnocení stavu kybernetické bezpečnosti bude provedeno ve struktuře dle relevantních požadavků zákona číslo 181/2014 Sb., tzv. zákona o kybernetické bezpečnosti, a jeho doprovodné vyhlášky[1]. Zohledněna budou též doporučení pro systém řízení bezpečnosti informací dle dlouhodobě uznávané normy ČSN ISO 27001 a na ní navazující normy ČSN ISO 27002, která je souborem doporučených opatření pro zajištění bezpečnosti informací.

Hodnocení stavu kybernetické bezpečnosti bude řízeno certifikovaným auditorem, zaměstnancem firmy DATASYS s certifikací CISA[2]. Sběr dat pro analýzu bude za DATASYS zajišťovat jeden bezpečnostní specialista. V rámci plnění dle této nabídky budou poskytnuty služby, jejichž cílem je zjistit a posoudit aktuální stav bezpečnosti IT infrastruktury Zadavatele a procesů spojených s provozem této infrastruktury, zejména pak stav technických i organizačních bezpečnostních kontrol, které jsou v provozním prostředí IT infrastruktury aplikovány. Výstupem budou též doporučená opatření vedoucí ke zlepšení stavu, ve kterých **budou zohledněna Zadavatelem již naplánovaná[3] opatření**.

Výstupem plnění dle této nabídky budou:

1. **Katalog IT služeb** a jejich požadovaných parametrů (tzv. primárních aktiv)
2. Dokument „**Analýza stavu kybernetické bezpečnosti**" s návrhem doporučených opatření
3. Přehledy dotazníkových šetření „**Hodnocení kybernetické bezpečnosti**" (tabulkové podklady studie)

Dokumenty budou zpracovány do deseti pracovních dnů od ukončení konzultací s pracovníky Zadavatele.
Potřebnou součinnost pracovníků, kteří se podílejí na řízení a zajištění běhu provozního prostředí IT infrastruktury zajistí Objednatel. Odhadovaná celková doba trvání (individuálních) konzultací s těmito pracovníky je 40 hodin.



Obsahem dokumentů hodnocení je souhrnný grafický přehled úrovní členěný dle paragrafů vyhlášky o kybernetické bezpečnosti i detailní tabulkový rozpad plnění požadavků vyhlášky. A samozřejmě nechybí přehledová manažerská zpráva z provedeného hodnocení úrovně kybernetické bezpečnosti. Ilustrativní ukázky těchto dokumentů uvádíme jako přílohu této nabídky.

[1] Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).
[2] Certified Information Systems Auditor.
[3] Opatření naplánovaná Zadavatelem zejména v souvislosti s podáním žádosti o dotaci IROP.

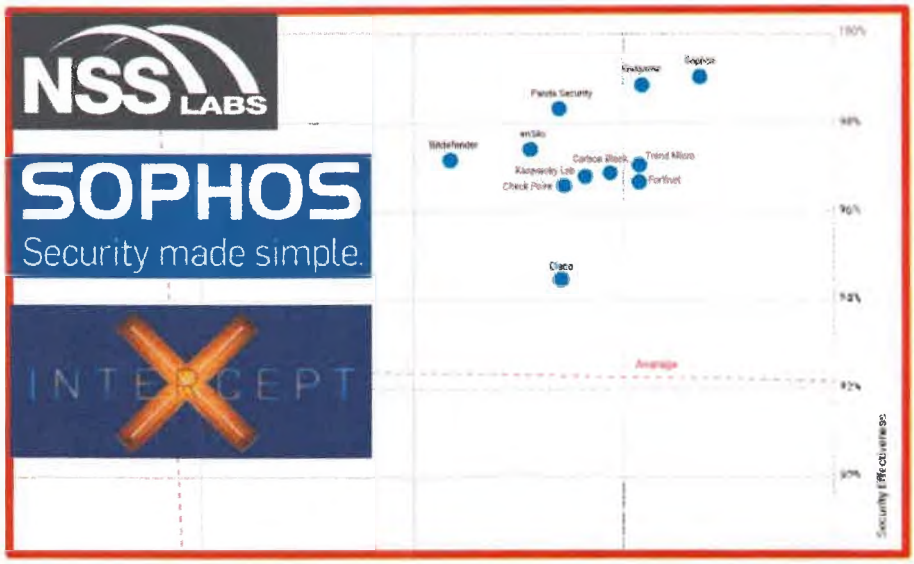
1.1 Praktické bezpečnostní testy – volitelný doplněk studie

K nabízenému hodnocení úrovně kybernetické bezpečnosti doporučujeme přiobjednat provedení několika základních technických testů pro praktické ověření reálné stávající úrovně zabezpečení vašeho IT, aby hodnocení studie nevycházelo jen z informací získaných z řízených rozhovorů s pracovníky IT a garanty aktiv.

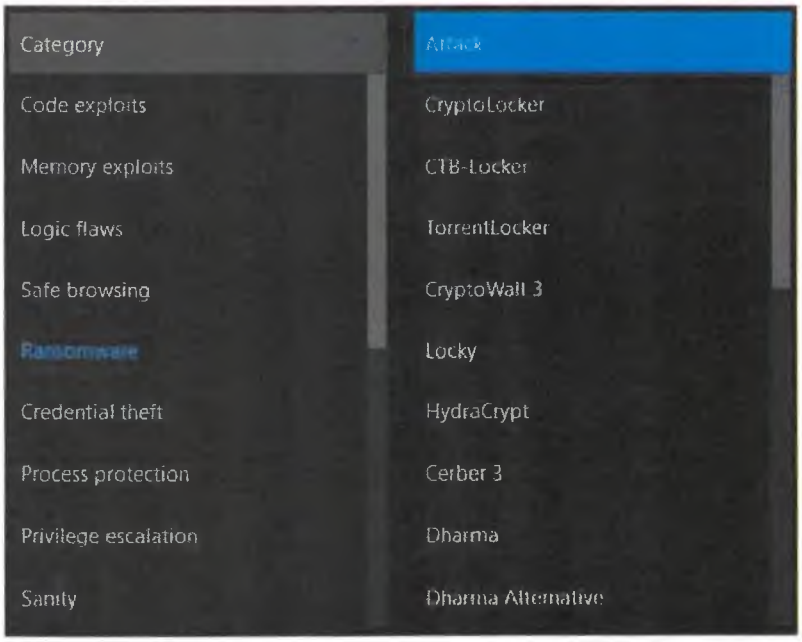
1. Test odolnosti vůči ransomwaru
2. Technický sken zranitelností služeb vaší počítačové sítě
3. Test odolnosti vašich uživatelů vůči klamavým e-mailovým kampaním, konkrétně vůči tzv. phishingu.

1.1.1 Test odolnosti vůči ransomwaru a dalším formám škodlivého kódu

Škodlivý kód typu ransomware stále představuje jednu z nejvážnějších hrozeb pro IT aktiva společností. Klasická antivirová řešení fungující na principu signatur v ochraně proti ransomwaru, zero-day útokům a dalším pokročilým hrozbám často selhávají. Velmi proto doporučujeme nasadit další vrstvu ochrany, která dokáže fungovat i souběžně s AV nástroji jiných výrobců, a to např. Sophos **Intercept X**. Systém, který pro detekci škodlivého kódu využívá moderní technologie založené na bázi umělé inteligence a strojového učení. Nástroj vyniká kombinací nejvyšší míry detekce a příznivé ceny.



Nabízíme prakticky otestovat, jak účinná je proti ransomwaru a dalším pokročilým hrozbám vaše stávající ochrana stanic. S využitím softwarového nástroje provedeme na několika určených stanicích test AV ochrany proti 14 kryptovirům a desítkám exploitů. Test je zcela neškodný, nejedná se o spouštění reálného malwaru, nýbrž o simulaci chování daného typu ransomwaru.



Odhadovaná celková doba požadované součinnosti Zadavatele je 8 hodin.

1.1.2 Provedení testu zranitelnosti

Tento test bude realizován jako **asistovaná zápůjčka hardwarové sondy** nástroje Greenbone Security Manager (GSM) pro získání přehledu o zařízeních v síti a zejména pro zjištění a zvládání zranitelných služeb sítě. Asistovaná zápůjčka typicky Zadavateli slouží k ověření vlastností nástroje před jeho pořízením. Tato naše nabídka na provedení je vhodná pro téměř všechny typy společností, které nedisponují vlastním analogickým nástrojem. **Greenbone Security Manager** je renomovaný automatizovaného skener zranitelností německého výrobce.

Služba zápůjčky GSM zahrnuje:

- Zápůjčku dvouportové hardwarové sondy „GSM 100" na dva týdny
- Dopravu sondy k Objednateli, na místo určené k zapojení sondy do sítě (1 lokalita)
- Zapojení, instalaci a konfiguraci zařízení (ve spolupráci s IT oddělením Objednatele)
- Zaškolení pracovníků IT oddělení Objednatele
- Průběžné telefonické konzultace
- Sestavení přehledu doporučených kroků a závěrečný workshop
- Odpojení a odvoz sondy

Odhadovaná celková doba požadované součinnosti Zadavatele je 8 hodin.

Přednosti nabízeného řešení

- **Vysoká užitná hodnota**
  - Řízení zranitelností v síti výkonově škálovatelné a bez omezení na počet skenovaných IP adres
- **Jednoduché nasazení**
  - Žádné instalace agentů na servery nebo stanice
  - Žádné změny stávající architektury sítě
  - Přehledné uživatelské rozhraní
  - Centrální správa více sond
- **Příznivá cena**
  - Ve srovnání s konkurencí Greenbone neomezuje počet skenovaných IP adres

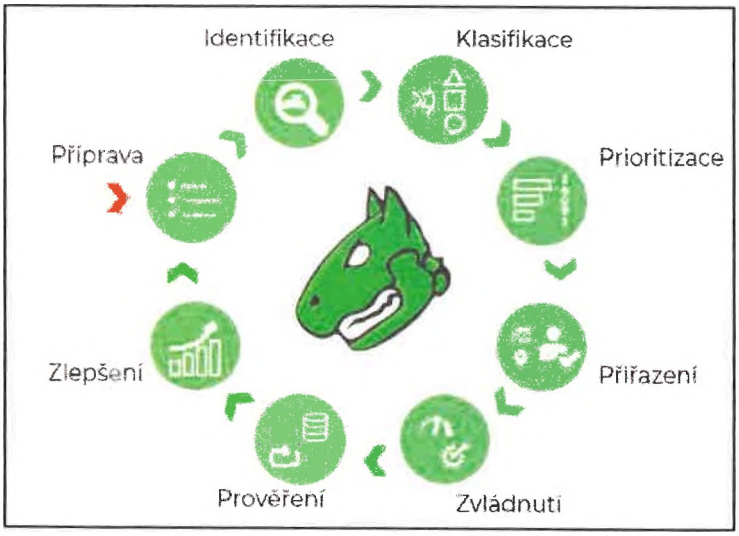
1.1.2.1 Informace o nástroji GSM

S nástrojem pro řízení zranitelností Greenbone Security Manager nahlížíte na vaši IT infrastrukturu pohledem zvenčí – stejně jako potenciální útočník. Cílem je nalézt jakoukoli zranitelnost, která by mohla existovat ve vaší IT infrastruktuře. Řešení od Greenbone transformuje jednorázové skenování zranitelností do řízeného procesu.

- ✓ Vysoká úroveň automatizace a užitečné typizované postupy řešení nálezů
- ✓ Integrace s dalšími bezpečnostními nástroji vylepší účinnost antivirových systémů a firewallů

Identifikujte a spravujte rizika

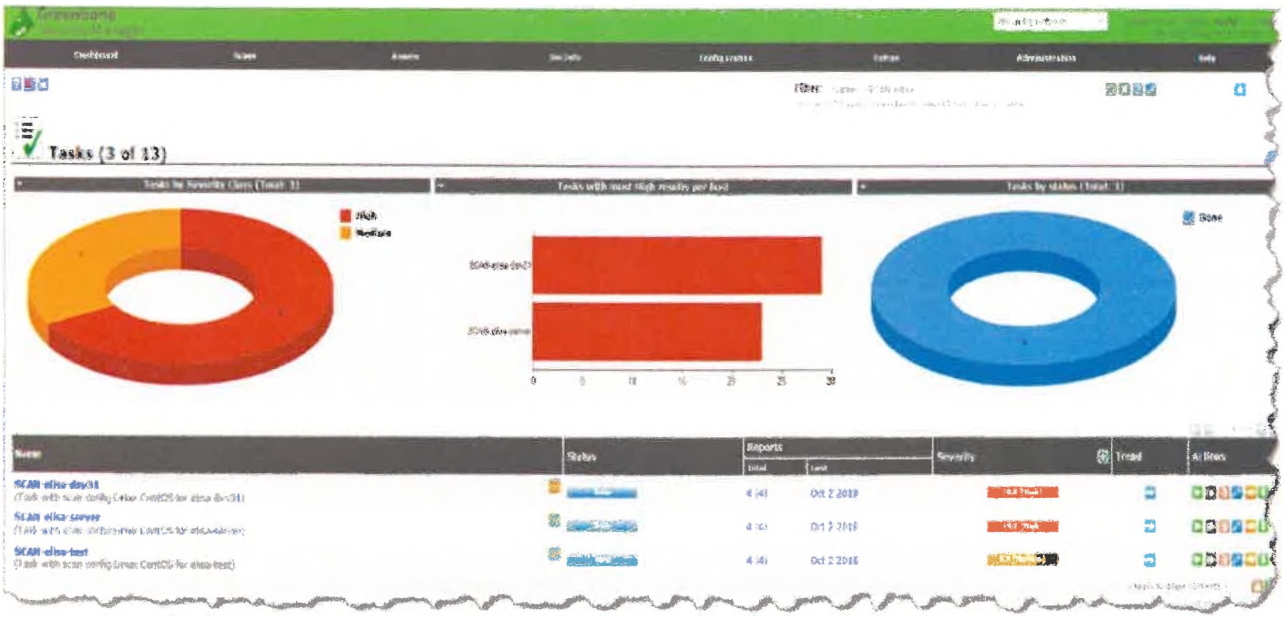
Typickými příčinami zranitelnosti jsou nesprávná konfigurace nebo chyby v programování, neoprávněné instalace nebo porušení bezpečnostních opatření. Greenbone Security Manager tyto a další zranitelnosti automatizovaně odhaluje a pomáhá vám prioritizovat jejich odstraňování. To ve výsledku pomáhá výrazně snížit riziko ztrát v důsledku kompromitace vašich informačních systémů.



Klíčovým prvkem celé technologie je tzv. **Greenbone Security Feed**. Jedná neustále probíhající proces dílčích postupů, které vedou k odhalení známých bezpečnostních zranitelností. Tento proces má na starosti skenovací modul, kterým lze kontrolovat všechna zařízení připojená k vaší síti.

- •Aktualizace databáze zranitelností, a tudíž i stavu zabezpečení, několikrát za den
- •Podpora skenování i mechanismem přihlášení do kontrolovaného systému
- •Postupy řešení odhalených zranitelností
- •Víceúrovňové zajištění jakosti procesu

Greenbone OS zajišťuje komplexní a výkonný základ zařízení Greenbone. Hlavními prvky Greenbone OS jsou samotný operační systém, webové uživatelské rozhraní, administrativní rozhraní a aplikace pro skenování.



1.1.3 Phishingový test

Tento dokument je nabídkou na provedení jednorázového phishingového testu pro pracovníky Zadavatele, na který bude navazovat e-learningové školení uživatelů, kteří bezpečnostním testem neprošli. Pro školení bude využit LMS[4] nástroj provozovaný společností DATASYS. Předmětem naší nabídky jsou zejména tyto služby:

1. **Provedení prvotního bezpečnostního phishingového testu**
   a. Sestavení cílového konceptu a obsahu prvotního phishingového testu
   b. Příprava testovacího malwaru a mechanismu detekce jeho spuštění uživatelem
   c. Provedení prvotní phishingové kampaně a její vyhodnocení
2. **Školení uživatelů, kteří bezpečnostním testem neprošli**
   a. Zřízení samostatné instance LMS nástroje v hostingovém centru společnosti DATASYS
   b. Přiřazení e-learningových kurzů pracovníkům, rozeslání notifikací a podpora uživatelům
   c. Sledování průběhu vzdělávání, eskalace neaktivity nadřízeným
3. **Provedení ověřovacího phishingového testu**
   a. Sestavení obsahu ověřovacího phishingového testu
   b. Provedení ověřovací phishingové kampaně a její vyhodnocení

1.1.3.1 Phishingový test

Žádná z firem se neobejde bez základního komunikačního kanálu – emailové korespondence. A klíčovým faktorem úspěšnosti kybernetických útoků vedených prostřednictvím e-mailu se velmi často stává zaměstnanec. Dříve či později nastává situace, kdy právě sám uživatel musí učinit klíčové rozhodnutí: Smazat zprávu, nebo otevřít? A jelikož na tomto rozhodnutí může záviset úspěšnost hackerského útoku, měla by si každá společnost položit otázku, zda by její zaměstnanci obstáli.

1.1.3.2 Phishing

Phishing útoky se primárně zaměřují na e-mailovou komunikaci či jiné komunikátory a využívají metod sociálního inženýrství za účelem získání citlivých údajů, jako jsou uživatelská jména a hesla, bankovní spojení apod. Dle posledních statistik až 74 % phishingových útoků začíná právě podvrženým e-mailem. Až 30 % těchto útoků pochází z domény gmail a mezi nejčastější techniky získání osobních údajů patří phishingové útoky vydávající se za Microsoft. Denně reportuje takovéto útoky 41 % IT profesionálů. Nová bezpečnostní vrstva se jmenuje „uživatel".

1.1.3.3 Řešení

Nejlepší odpovědí na tuto intenzivní hrozbu jsou poučení a odolní zaměstnanci. Naši specialisté ve spolupráci s klientem připraví phishingovou kampaň, která je rozeslána na zaměstnance společnosti. A pak už se jen čeká, kolik zaměstnanců e-mail otevře, kolik klikne na odkaz nebo případně dokonce poskytne svoje přístupové údaje. Výsledkem celé kampaně je přehledný report s potřebnými statistikami, na který by mělo navazovat školení pracovníků, kteří bezpečnostním testem neprošli.

[4] LMS – Learning Management System

Hlavní přínosy služby:	Co služba umí?
✓ Odhalení nejrizikovějších uživatelů	▪ Testovací phishing kampaň
✓ Praktická edukace zaměstnanců na phishing	▪ Předpřipravené šablony
✓ Posílení bezpečnosti na úrovni uživatelů	▪ Možnost připravit kampaň na míru zákazníka
✓ Přehledný reporting reakcí uživatele na phishing	▪ Závěrečný report o výsledcích kampaně
✓ Ošetření nejběžnějšího vektoru útoku	▪ Návazné on-site / E-learning školení pro účastníky
✓ Testování různých typů phishingu	▪ Anonymizace poskytnutých přístupových údajů ze strany zaměstnanců

Přehledné reporty

Z reportů lze velmi jednoduše vyčíst všechna potřebná data. V přehledných grafech jsou zobrazeny statistiky s chováním uživatelů (zobrazený email, kliknutí na odkaz apod.). Report obsahuje také informace, z jakých OS bylo na podvrženou stránku přistupováno, a dokonce dokáže určit nejrizikovější skupiny uživatelů.

Poznámka: Ač se dá služba pořídit i formou jednorázové phishingové kampaně s možností rozšíření o následný e-learningový kurz, **velmi doporučujeme** tuto problematiku pojmout jako **neustálý koloběh** phishingových kampaní a následných školení, aby se zaměstnanci v problematice phishingu posouvali stále dál a byl jasně dohledatelný trend odolnosti firmy vůči útokům, které se v čase zdokonalují.

1.1.4 Školení uživatelů proti phishingu

V návaznosti na phishingový test doporučujeme realizovat e-learningové školení uživatelů, kteří tímto bezpečnostním testem neprošli. Pro školení bude využita školící platforma provozovaná společností DATASYS.

Předmětem školení budou tyto kurzy:

- Phishing – úvod do problematiky
- Phishing – rozeznání podvodných emailů
- Phishing – rozeznání podvodných URL
- Phishing – poskytování citlivých údajů

V případě zájmu lze nabídku služeb vzdělávání rozšířit o **kurzy vytvořené na míru** bezpečnostních politik a procesů ve společnosti Zadavatele nebo o další okruhy standardních kurzů jako například:

- Bezpečnost procházení webu
- Bezpečnost na sociálních sítích
- Bezpečnost mobilních zařízení
- Bezpečnost mobilních aplikací
- Bezpečnost zařízení USB
- Sociální inženýrství
- Osobní údaje

2. Doložení kvalifikace

Společnost Datasys svým zákazníkům poskytuje služby v oblasti kybernetické bezpečnosti dlouhodobě. Jedná se zejména o zpracování bezpečnostních studií a rizikových analýz, penetrační testy a technické prověrky. Nabízíme i služby potřebné pro úspěšné ustavení systému řízení bezpečnosti informací (ISMS) v organizaci, včetně zpracování návrhů bezpečnostních politik a směrnic. Dodávka služeb bude řízena pracovníkem s certifikací CISA (Certified Information Systems Auditor).

Rozsahem podobné bezpečnostní studie:

1. Město Veselí nad Moravou (2022)
2. Severomoravské vodovody a kanalizace (2020)
3. GECO, a.s. (2018)
4. Pramacom Group (2018)
5. ŽĎAS a.s. (2017)

Největší obdobné referenční projekty:

1. Analýza rizik v Informačním systému datových schránek (2022)
    a. Ustavení systému řízení bezpečnosti informací (ISMS) dle požadavků ZKB
    b. Implementace bezpečnostního monitoringu, včetně SIEM
2. Analýza rizik informačních systémů Generálního finančního ředitelství (2021)
3. Analýza rizik neklasifikovaných informačních systémů MZV ČR (2013)
    a. Implementace bezpečnostního monitoringu, včetně log management systému (2015)

3. Cena

Posouzení úrovně organizačních a technických opatření kybernetické bezpečnosti vůči požadavkům zákona o kybernetické bezpečnosti nabízíme provést **za cenu 99 200 Kč bez DPH**.

K nabízenému hodnocení úrovně kybernetické bezpečnosti doporučujeme za výhodnou cenu přiobjednat provedení několika základních technických testů pro praktické ověření reálné stávající úrovně zabezpečení vašeho IT, aby hodnocení studie nevycházelo jen z informací získaných z řízených rozhovorů s pracovníky IT a garanty aktiv.

Cenová nabídka praktických bezpečnostních testů:

Popis	Cena bez DPH
Test odolnosti vůči ransomwaru a dalším pokročilým formám škodlivého kódu	15 000 Kč
Sken zranitelností služeb počítačové sítě s návrhem doporučení k jejich odstranění	39 000 Kč
Phishingový test odolnosti uživatelů vůči klamavým e-mailovým kampaním	69 000 Kč
Celkem	**123 000 Kč**

3.1 Platnost nabídky, platební podmínky a harmonogram realizace

Platnost nabídky jsou 3 měsíce. DPH činí 21 %. Splatnost faktury vystavené na základě této nabídky je 30 dnů od protokolárního převzetí. Harmonogram realizace bude stanoven po dohodě se Zadavatelem. DATASYS je připraven práce zahájit do 2 týdnů od objednávky.

4. Závěr

Jménem společnosti DATASYS si dovolujeme vyjádřit přesvědčení, že výše uvedená nabídka bude po technické i ekonomické stránce vyhovovat potřebám Vaší organizace a její realizace přispěje ke zkvalitnění prostředí a služeb provozovaných informačních technologií a systémů.

Věříme současně, že náš výklad zadání, navržené postupy, stejně tak jako know-how, technické i lidské zdroje, kterými společnost DATASYS disponuje, skýtají záruky realizace předmětného projektu v nejvyšší kvalitě a k plné spokojenosti Vaší společnosti.

V Praze dne 29.9.2022

Nabídku zpracoval

Technický ředitel

DATA SYS

*Také v IT naleznete **rodinné společnosti**. DATASYS je jednou z nich. Na trhu působíme **od roku 1994** a přinášíme **spolehlivá řešení** v následujících oblastech:*

BEZPEČNOST

Jsme dodavatelem bezpečnostních řešení, nástrojů a služeb. Naší specializací je sledování vzdálených přístupů. Umíme však zabezpečit a monitorovat informační systémy na mnoha úrovních, náš přístup je pragmaticky vyvážený, realizace důsledná.

VÝVOJ A INOVACE

Pokrokové nápady převádíme v realitu. Dodáváme serverové back-end aplikace, klient/server řešení, webové aplikace i aplikace pro mobilní telefony. Dokážeme integrovat oddělené systémy i navrhovat zcela nová řešení.

INFRASTRUKTURA

Informační systémy nemohou fungovat bez pevných základů. Infrastruktura představuje páteř každého informačního systému a my se zaměřujeme na komplexní implementační a integrační služby.

IT AS A SERVICE

Umíme se postarat o všechny vaše IT. Vyřešíme vaše problémy se softwarem i hardwarem, jsme na příjmu 24 hodin denně, 7 dní v týdnu. Budeme vaším opravdovým partnerem pro inovace a IT vám doručíme jako spolehlivou službu.

NAŠI KLIENTI

ČESKÁ POŠTA · SKUPINA ČEZ · PRE · ČSOB · ŠKODA · Allianz · McDonald's

80+
kmenových zaměstnanců

415 mil. Kč
obrat v roce 2018

5000+
realizovaných projektů

25 let
zkušeností

Pojďme se potkat a společně najít vhodné řešení.

Držitel certifikátů ISO 9001:2015, ISO 14001:2015, BS OHSAS 18001:2007, ISO/IEC 20000-1:2011, ISO/IEC 27001:2013

PRAHA | HRADEC KRÁLOVÉ | PLZEŇ | DĚČÍN | OSTRAVA | WWW.DATASYS.CZ