Smlouva o dílo

uzavřená dle ustanovení § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších přepisů

Objednatel:	**Karlovarský kraj**
Sídlo:	Závodní 353/88, 360 06 Karlovy Vary
IČO:	70891168
DIČ:	CZ70891168
Zastoupený:	Mgr. Daniel Tovth, vedoucího odboru kancelář ředitelky úřadu
Bankovní spojení:	Komerční banka, a.s., pobočka Karlovy Vary
Číslo účtu:	

(dále jen „objednatel")

Zhotovitel:	**S&T CZ s.r.o.**
se sídlem:	Na Strži 1702/65, 140 00 Praha 4
IČO:	44846029
DIČ:	CZ44846029
Zastoupený:	Miroslav Bečka a Ing. Václav Kraus, jednatelé společnosti
Bankovní spojení:	ČSOB, a.s.
Číslo účtu:	[redacted]

Registrace ve veřejném rejstříku (u registrovaných): u Městského soudu v Praze, oddíl C, vložka 6033
(dále jen „*zhotovitel*")

Smluvní strany uzavřely následující smlouvu o dílo (dále jen „*smlouva*"):

I. Předmět smlouvy

1.1. Předmětem této smlouvy je provedení penetračních testů Krajského úřadu Karlovarského kraje (dále jen „*KÚKK*") se zaměřením na bezpečnost informačních systémů zhotovitelem (dále jen „*dílo*") způsobem a za podmínek stanovených v příloze č. 1 této smlouvy, která je nedílnou součástí smlouvy. Dílo zhotovitel provádí na svůj náklad a na své nebezpečí.

1.2. Zhotovitel se zavazuje provést a předat dílo bez vad a nedodělků dle specifikace uvedené v příloze č. 1, která je nedílnou součástí smlouvy, nejpozději v termínu do tří měsíců od podpisu smlouvy.

1.3. Dílo bude provedeno v sídle objednatele. Výsledek díla bude proveden v elektronické podobě (CD nosič dat) a tištěné podobě.

1.4. Zhotovitel je vázán mlčenlivostí týkající se všech skutečností, které v rámci provedení díla zjistí, příp. se kterými přijde do styku.

1. 5. Zhotovitel po protokolárním předání a převzetí výstupů, které budou bez vad a nedodělků, odstraní ze svých úložišť veškerá data, která při realizaci penetračních testů získal. Zhotovitel nebude po ukončení smlouvy disponovat informacemi o slabých místech informačního systému objednatele, které v průběhu testu získá. Odstranění dat zhotovitel doloží čestným prohlášením.

1.5. Zhotovitel je povinen postupovat při plnění této smlouvy s odbornou péčí; zavazuje se při plnění díla postupovat poctivě, pečlivě a s odbornou péčí, jak je vymezena v § 5 odst. 1 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, s použitím každého prostředku, kterého vyžaduje povaha předmětu díla, podle pokynů objednatele a v souladu s jeho zájmy, které jsou zhotoviteli známy nebo je musí znát či předpokládat.

1.6. Vyjde-li najevo, že zhotovitel se při provádění díla dle této smlouvy dopustil hrubé nedbalosti a že nejednal s odbornou péčí dle ustanovení § 5 odst. 1 občanského zákoníku a vznikne-li objednateli škoda z titulu takové hrubé nedbalosti zhotovitele, vzniká zhotoviteli povinnost k náhradě škody a objednateli právo tuto škodu po zhotoviteli vymáhat.

1.7. Pokud budou při protokolárním předání zjištěny vady nebo nedodělky díla, není objednatel povinen dílo převzít. V případě zjištění vad nebo nedodělků bude sepsán protokol s určením termínu pro odstranění nedostatků, a to nejvýše v délce 15 dnů. Zhotovitel v určeném termínu dílo bez vad a nedodělků předá, náhradní předání bude probíhat obdobně jako u prvního předání.

II. Cena díla a záruční doba

2.1. Objednatel se zavazuje uhradit zhotoviteli za dílo provedené v souladu s touto smlouvou cenu v celkové maximální výši 215.380,- Kč (slovy: dvě stě patnáct tisíc tři sta osmdesát korun českých) včetně DPH.

2.2. Cena za dílo uvedená odstavci 2.1. je nejvyšší možnou cenou za dílo. Objednatel se zavazuje cenu zaplatit zhotoviteli na základě faktury na účet uvedený v záhlaví smlouvy do 15 dnů od protokolárního převzetí řádně provedeného díla, které bude bez vad a nedodělků, objednatelem. Pokud ve lhůtě 15 dnů od protokolárního předání, ve lhůtě splatnosti, vyjdou najevo vady díla, má objednatel právo fakturu neuhradit. V takovém případě objednatel stanoví termín pro odstranění vad, a to nejvýše v délce 15 dnů. Zhotovitel vady odstraní a lhůta splatnosti po odstranění vad začne běžet znovu.

2.3. Zhotovitel poskytuje záruční dobu díla v délce 2 roky.

III. Smluvní pokuta

3.1. Smluvní strany se dohodly, že v případě prodlení zhotovitele s předáním díla dle čl. I. odst. 1.2 smlouvy, nebo v případě prodlení zhotovitele s odstraněním vad nebo nedodělků díla, je objednatel oprávněn uplatnit vůči zhotoviteli smluvní pokutu ve výši 0,1 % (slovy: jedna desetina procenta) z ceny za provedení díla, a to za každý i započatý den prodlení.

3.2. Smluvní pokuta dle tohoto článku je splatná do třiceti dní od data, kdy byla povinné straně doručena písemná výzva k jejímu zaplacení ze strany oprávněné strany, a to na účet oprávněné strany uvedený v písemné výzvě. Ustanovením o smluvní pokutě není dotčeno právo oprávněné strany na náhradu škody v plné výši.

IV. Závěrečná ustanovení

4.1. Smluvní strany shodně prohlašují, že si tuto smlouvu před jejím podpisem přečetly, že byla uzavřena po vzájemném projednání podle jejich pravé a svobodné vůle, určitě, vážně a srozumitelně, nikoliv v tísni a za nápadně nevýhodných podmínek. Smlouva je sepsána ve třech vyhotoveních, z nichž dvě obdrží objednatel a jedno zhotovitel. Změny a doplňky této smlouvy lze činit pouze písemně, číslovanými dodatky, podepsanými oběma smluvními stranami.

4.2. Smlouva nabývá platnosti podpisem oběma smluvními stranami a účinnosti uveřejněním v registru smluv.

4.3. Tato smlouva nabývá platnosti podpisem smluvních stran a účinnosti dnem uveřejnění v Registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů. Smluvní strany se dohodly, že uveřejnění smlouvy v registru smluv provede objednatel, kontakt na doručení oznámení o vkladu smluvní protistraně na e-mail hana.kleckova@sntcz.cz

V Karlových Varech dne 25.5.2020

[redacted]

objednatel

V Praze dne 15.5.2020

S&T CZ s.r.o.

[redacted]

Miroslav Bečka a Ing. Václav Kraus
jednatelé společnosti

Specifikace penetračních testů Krajského úřadu Karlovarského kraje se zaměření na bezpečnost informačních systémů

Penetrační testy budou provedeny bez destruktivních dopadů na zařízení objednatele, zhotovitel není oprávněn v rámci testů vyřadit informační systém objednatele z provozu a zhotovitel není oprávněn v rámci testů k poškození software nebo hardware objednatele.

1.1 Externí penetrační test

Při realizaci externího penetračního testu bude prověřena bezpečnost informačních systémů objednatele dostupných z veřejné sítě Internet.
Tyto testy budou spočívat v simulaci útoku na systémy objednatele útočníkem, který se pokouší o průnik z Internetu, nemá předběžné znalosti o IT infrastruktuře a nemá přístupové údaje k IT službám publikovaným z interního prostředí objednatele do Internetu.
Testy z této skupiny budou obsahovat:

- Vyhledání zranitelností v informacích veřejně dostupných o IT objednatele.
- Bezpečnost DNS domény objednatele, zejména:
  - počet, umístění a dostupnost DNS obsahu serverů,
  - možnost neautorizovaného transferu zóny,
  - zabezpečení proti neoprávněné změně DNS záznamů.
- Bezpečnost infrastruktury elektronické pošty objednatele, zejména:
  - ochrana pošty odesílané z domény objednatele,
  - ochrana pošty pro doménu objednatele: účinnost antispamu a antiviru,
  - prozrazení zneužitelných informací prostřednictvím protokolů a rozhraní použitých pro elektronickou poštu; zhotovitel nebude cílit na prozrazení obsahu zpráv elektronické pošty zaměstnanců objednatele, nýbrž na informace obsažené v hlavičkách (předmětu) e-mailů, formulářích apod.,
  - posouzení zabezpečení odesílání pošty z webu objednatele (z formulářů na webu objednatele).
- Bezpečnost vybraných služeb, portálů a informačních systémů publikovaných do Internetu (tj. weby: kr-karlovarsky.cz, krajkv.cz a kr-k.cz).

Testy se budou skládat z:

- Prvotní sken systému, po kterém bude následovat cílený test systému, které v rámci skenu vykazují chybu. Cílený test proběhne se znalostí přístupových údajů.
- testů k získání informací, identifikace funkčních systémů;
- všeobecných testů zranitelnosti;
- testů týkajících se charakteristiky infrastruktury systému;
- testů spolehlivosti konfigurace;
- testů existence backdoors (detekce otevřených míst v systému);
- testů autentizace a schémat pro kontrolu přístupu;
- testů firewallů;
- testů routerů;
- kontroly operačních systémů;
- testů aplikačních chyb a vad v systému;
- testů nedostatečného provozního zabezpečení.

1.2 Interní penetrační test

Interní penetrační testy provede zhotovitel z prostředí sítě objednatele, a to přímo ze sídla objednatele. Zaměří se na test používané infrastruktury a zabezpečení bezdrátové sítě bez a se znalostí hesla. Součástí je i pokročilá detekce na odhalení známých či neznámých hrozeb vyskytující se již v síti zadavatele (pokročilý malware, ransomware, apod.). Jejich cílem je prověření bezpečnosti systému v rámci jeho provozního prostředí a provozu, resp. jeho možné ohrožení z prostředí interní sítě a bezdrátové sítě a testování bezdrátové sítě samotné, tj. bude simulováno počínání potenciálního útočníka pokoušejícího se o průnik z nakaženého počítače umístěného uvnitř interní sítě.
Interní penetrační testy budou obsahovat:

- testy k získání informací, identifikace funkčních systémů;
- všeobecné testy zranitelnosti;
- testy týkajících se charakteristiky infrastruktury systému;
- testy spolehlivosti konfigurace;
- testy existence backdoors (detekce otevřených míst v systému);
- testy autentizace a schémat pro kontrolu přístupu;
- kontroly operačních systémů;
- testy aplikačních chyb a vad v systému;
- testy nedostatečného provozního zabezpečení;
- testy slabých míst zahrnující body selhání, s cílem způsobit odmítnutí služeb webových aplikací;
- odposlech komunikace se systémem;
- odchycení a přesměrování této komunikace;
- zneužití odchycených informací a komunikace směrem k aplikačním službám (serverům);
- útoky na uživatele systému prostřednictvím tohoto systému;
- testů wi-fi bodů přístupu.

1.3 Penetrační test s využitím sociotechnických metod

V rámci tohoto testu je požadováno prověření dodržování procesů a bezpečnostních zásad v rámci Krajského úřadu Karlovarského kraje, a to ve dvou etapách:

- **Phishingový test formou „podvodného" e-mailu**

Cílem testování je prověřit úroveň bezpečnostního povědomí zaměstnanců a přimět zaměstnance objednatele sdělit citlivé informace nebo vykonat určitou činnost.
Phishingová kampaň s podvrženými e-maily s cílem otestování uživatelských účtů (uživatelů) objednatele a to v podobě podvrženého e-mailu. Během testu nesmí dojít k infikování koncových uživatelských stanic objednatele, ale bude zaznamenána a změřena aktivní odezva na email – „proklik" na odkaz v e-mailu.

- **Test fyzické bezpečnosti**

Cílem testu je pokus o proniknutí neautorizované osoby do vnitřních prostor Krajského úřadu Karlovarského kraje a získání přístupu k prostředkům informačního systému nebo citlivým informacím.

Výsledky testování a výsledná zpráva

Výstupem penetračního testu bude závěrečná zpráva, která v přehledné podobě (číselné, grafické i slovní vyjádření) shrne provedené penetrační testy vč. zranitelností, stupně rizikovosti a návrhu opatření, které povedou k jejich odstranění nebo zmírnění rizika spojeného s těmito zranitelnostmi na přijatelnou úroveň. Závěrečná zpráva bude obsahovat alespoň tyto části:

1) Manažerské shrnutí – přehledně prezentované penetrační testy a celkové hodnocení bezpečnosti systému.
2) Popis postupů či metodiky provedených penetračních testů, zvlášť pro externí penetrační test, interní penetrační test a penetrační test za použití sociotechnických metod.
3) Log Book - přehled provedených prací, popis jednotlivých provedených testů. Dalším výstupem budou logy provedených testů z použitých bezpečnostních aplikací, které budou sloužit k ověření provedení

jednotlivých testů dle checklistu OWASP – seznamu první desítky nejzávažnějších bezpečnostních rizik webových aplikací.

4) Popis nalezených zranitelností – detailní popis jednotlivých nalezených zranitelností včetně stupně rizikovosti a jejich dopadu na testovanou aplikaci. U nalezených zranitelností bude součástí závěrečné zprávy i kód (ideálně HTTP, dotaz a odpověď), který umožňuje replikace testu objednavatelem.

Rizikovost bude rozdělena podle následujících kritérií:

a) Kritické – zranitelnost vedoucí k okamžitému a naprostému vyřazení služby.
b) Vysoké – zranitelnosti, které v kombinaci s jinými zranitelnostmi představují zásadní vysoké riziko.
c) Střední – musejí být splněny speciální podmínky na zneužití uvedených zranitelností nebo jejich případné zneužití má omezený dopad.
d) Nízké – drobné bezpečnostní problémy.

5) Navrhované opatření – popis navrhovaných opatření k jednotlivým identifikovaným zranitelnostem, která povedou k odstranění nalezených zranitelností nebo ke snížení míry rizika spojeného s těmito zranitelnostmi na akceptovatelnou úroveň.
6) Závěrečné shrnutí – shrnuje provedené externí penetrační testy, interní penetrační testy a penetrační testy s využitím sociotechnických metod a obsahuje celkové hodnocení úrovně bezpečnosti informačních systémů objednatele.