**SMLOUVA O PROVEDENÍ BEZPEČNOSTNÍCH TESTŮ MODULŮ STATISTICKÉHO INFORMAČNÍHO SYSTÉMU DOSTUPNÝCH Z INTERNETU**

**A WEBOVÉ PREZENTACE ČSÚ**

evid. č. ČSÚ: 098-2016-S

Níže uvedeného dne, měsíce a roku uzavřely smluvní strany:

**Česká republika – Český statistický úřad**

se sídlem: Na padesátém 3268/81, 100 82 Praha 10

IČO: 000 25 593

zastoupena: Mgr. Radoslavem Bulířem, ředitelem sekce ekonomické a správní

na základě pověření předsedkyně ČSÚ ze dne 16. 3. 2015

číslo účtu: 2923001//0710

(dále jen „objednatel“ nebo ČSÚ“) na straně jedné

a

**BDO IT a. s.**

se sídlem: Olbrachtova 1980/5, 140 00 Praha 4

IČO: 25056646

zastoupena: Danem Vaníčkem, předsedou představenstva

zapsaná v obchodním rejstříku vedeném Městským úřadem v Praze, oddíl B, vložka č. 4080

(dále jen „zhotovitel“) na straně druhé

(objednatel a zhotovitel dále též jen „smluvní strany“)

tuto

**smlouvu o provedení bezpečnostních testů modulů Statistického informačního systému dostupných z internetu a webové prezentace ČSÚ**

dle ust. § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „občanský zákoník“)

(dále jen „smlouva“):

**Článek I.**

**Úvodní ustanovení**

1. Tuto smlouvu uzavírají smluvní strany na základě výběrového řízení na veřejnou zakázku malého rozsahu s názvem „Bezpečnostní testy modulů Statistického informačního systému dostupných z internetu a webové prezentace ČSÚ“ zadávanou objednatelem jako zadavatelem pod interním evidenčním číslem objednatele 023/2016 (dále jen „veřejná zakázka“), v němž byla nabídka zhotovitele vybrána jako nejvhodnější.
2. Účelem této smlouvy je vymezení vzájemných práv a povinností smluvních stran při provedení ve smlouvě specifikovaných bezpečnostních testů zhotovitelem pro objednatele za sjednanou cenu.
3. Pro plnění předmětu této smlouvy jsou závazné rovněž všechny dokumenty vztahující se k veřejné zakázce, zejména zadávací dokumentace a nabídka zhotovitele.
4. Zhotovitel výslovně prohlašuje, že se detailně seznámil se zadávací dokumentací veřejné zakázky, že jsou mu známy veškeré technické a kvalitativní podmínky nezbytné k realizaci předmětu plnění dle této smlouvy, a že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro provedení předmětu této smlouvy za dohodnutou cenu.
5. Zhotovitel se zavazuje plnit své závazky plynoucí z této smlouvy v souladu s platnými právními předpisy a veškerými zadávacími podmínkami veřejné zakázky.

**Článek II.**

**Předmět smlouvy**

1. Zhotovitel se touto smlouvou zavazuje za podmínek uvedených v této smlouvě pro objednatele zhotovit dílo spočívající v provedení vnějších penetračních testů modulů Statistického informačního systému (dále jen „SIS“) dostupných z internetu a webové prezentace ČSÚ (dále jen „penetrační testy“ nebo „dílo“). Moduly, na kterých budou penetrační testy prováděny, jsou specifikovány v příloze č. 1 této smlouvy.
2. Předmětem díla je:
3. vnější penetrační test (včetně DDoS) webové aplikace požadavky-vykazy.czso.cz;
4. vnější penetrační test (včetně DDoS) webové aplikace danteweb.czso.cz;
5. vnější penetrační test (včetně DDoS) webové aplikace vdb.czso.cz;
6. vnější penetrační test (včetně DDoS) webové prezentace ČSÚ czso.cz; a
7. zpracování závěrečného hodnocení bezpečnosti testovaných aplikací v rozsahu popsaném v čl. IV. písm. c) této smlouvy a její příloze č. 1 (dále jen „hodnocení“).

Podrobnější vymezení předmětu veřejné zakázky a popis stávajícího stavu SIS je uveden v příloze č. 1 této smlouvy.

1. Objednatel se touto smlouvou zavazuje zaplatit zhotoviteli za provedení penetračních testů sjednanou cenu.

**Článek III.**

**Místo plnění**

Místem plnění podle této smlouvy je sídlo objednatele na adrese Na padesátém 3268/81, Praha 10, PSČ 100 82.

**Článek IV.**

**Penetrační testy**

Zhotovitel se zavazuje provádět penetrační testy pro objednatele za těchto podmínek:

1. Vnější penetrační testy webových aplikací budou zaměřeny na identifikaci bezpečnostních slabin minimálně v rozsahu metodiky OWASP Testing Guide v.4. Součástí testování bude prověření bezpečnosti aplikací jak z pohledu anonymního uživatele, tak se znalostí autentizačních údajů.
2. Testy webových aplikací a webové prezentace (DDoS) proběhnou takovým způsobem nebo v takových časech, aby negativně neovlivnily běžný provoz sítě zadavatele. Požadovány jsou minimálně testy odolnosti proti SYN flood (se sílou alespoň 1500 pps) a Slow HTTP POST nebo Slowloris. Veškeré testy budou provedeny bez destruktivních zásahů, tj. nebudou se provádět žádné změny, které by poškodily testovaný systém.
3. Jako součást výstupů zhotovitel zpracuje závěrečné zhodnocení bezpečnosti testovaných aplikací, které bude obsahovat popis rizika vyplývajícího z jednotlivých nalezených zranitelností, konkrétní návrhy na odstranění těchto zranitelností a nedostatků, případně návrhy na zvýšení bezpečnosti testovaných částí. Výstupy budou také obsahovat popisy jednotlivých provedených testů. Každá nalezená zranitelnost bude kategorizována z pohledu její závažnosti, pravděpodobnosti zneužití a náročnosti odstranění. Každá klasifikace bude obsahovat minimálně 3 kategorie (např. vysoká/střední/nízká pravděpodobnost zneužití). Jedním z výstupů bude také manažerské shrnutí průběhu testování s přehledem nalezených zranitelností a nedostatků.

**Článek V.**

**Termín provedení penetračních testů**

Zhotovitel se zavazuje provést penetrační testy specifikované v čl. II. odst. 2 písm. a) až c) této smlouvy (v rozsahu specifikovaném v příloze č. 1 této smlouvy), zpracovat závěrečné hodnocení bezpečnosti testovaných aplikací specifikované v čl. II. odst. 2 písm. e) této smlouvy (v rozsahu specifikovaném v čl. IV. písm. c) této smlouvy) a předat hodnocení objednateli k akceptaci nejpozději do 40 (slovy: čtyřiceti) dní od uzavření této smlouvy. Zhotovitel splní závazek z této smlouvy předáním dokončeného díla, tedy akceptací díla bez výhrad podle čl. VI. odst. 2 písm. a) této smlouvy objednatelem.

**Článek VI.**

**Akceptace díla**

1. Objednatel je povinen do 10 (slovy: deseti) dnů od předložení hodnocení zhotovitelem prověřit jeho náležitosti a informovat zhotovitele s nejméně třídenním předstihem o termínu jednání k projednání akceptace díla.
2. O projednání akceptace díla bude sepsán akceptační protokol:
3. Neshledá-li objednatel v předloženém hodnocení žádné závažné vady anebo nedodělky, akceptuje dílo bez výhrad a oprávnění zástupci smluvních stran potvrdí akceptační protokol svými podpisy;
4. Shledá-li objednatel v předloženém hodnocení vady nebo nedodělky, dílo neakceptuje, do akceptačního protokolu uvede soupis výhrad se závazným termínem pro jejich odstranění, který stanoví po konzultaci se zhotovitelem a oprávnění zástupci smluvních stran potvrdí akceptační protokol svými podpisy. Po odstranění všech vad a nedodělků provedou smluvní strany nové akceptační řízení za stejných podmínek. Odmítne-li zhotovitel akceptační protokol potvrdit podpisem svého oprávněného zástupce, má se za to, že s vymezením vad a nedodělků díla objednatelem a s termínem jejich odstranění podle akceptačního protokolu souhlasí. V případě neakceptace díla pro vady a nedodělky nebo v případě, že zhotovitel odmítne podepsat akceptační protokol s uvedenými vadami a nedodělky, se zhotovitel ocitá v prodlení s dodáním díla od termínu jeho dodání podle článku V. této smlouvy až do úplného odstranění všech vytčených vad a nedodělků.
5. Akceptace díla bez výhrad podle článku VI. odst. 2. písm. a) této smlouvy je podmínkou oprávněnosti fakturace ceny díla podle článku VII. této smlouvy.

**Článek VII.**

**Cena díla a platební podmínky**

1. Za provedení penetračních testů v rozsahu podle článku II. odst. 2 písm. a) a b) a zpracování hodnocení podle článku II. odst. 2 písm. c) této smlouvy se objednatel zavazuje zaplatit zhotoviteli cenu ve výši 198 000,- Kč (slovy: jednostodevadesátosmtisíc korun českých) bez DPH (dále jen „cena díla“).
2. K ceně díla bude připočtena DPH v sazbě podle platných právních předpisů ke dni uskutečnění zdanitelného plnění.
3. Cena díla je sjednána jako cena nejvýše přípustná a zahrnuje veškeré náklady zhotovitele spojené s plněním předmětu této smlouvy, jakož i ceny za služby a dodávky, které nejsou výslovně uvedeny v zadávací dokumentaci veřejné zakázky nebo v této smlouvě, ale zhotovitel jako odborník o nich ví anebo má vědět, že jsou nezbytné pro řádné splnění smlouvy.
4. Zhotovitel přebírá nebezpečí změny okolností ve smyslu ustanovení § 2620 odst. 2 občanského zákoníku.
5. Cenu díla uhradí objednatel zhotoviteli na základě daňového doklady – faktury, kterou je zhotovitel oprávněn vystavit objednateli po akceptaci díla bez výhrad podle článku VI. odst. 2. písm. a) této smlouvy. V případě, že fakturační termín připadne na druhou polovinu prosince, vystaví z důvodu interních účetních předpisů objednatele poskytovatel příslušnou fakturu v lednu následujícího kalendářního roku.
6. Faktura zhotovitele musí obsahovat veškeré podstatné náležitosti daňového dokladu stanovené zejména v ust. § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění a v zákoně č. 563/1991 Sb., o účetnictví, v platném znění. Kromě těchto podstatných náležitostí musí faktura zhotovitele obsahovat evidenční číslo smlouvy objednatele, číslo účtu zhotovitele a všechny údaje uvedené v ust. § 435 odst. 1 občanského zákoníku a fakturovaná cena musí být vyjádřena výlučně v Kč.
7. Splatnost ceny díla sjednávají smluvní strany na 21 (slovy: dvacet jedna) dní od data doručení řádné faktury se všemi náležitostmi podle předchozího odstavce objednateli doporučenou listovní zásilkou, datovou schránkou nebo osobně do podatelny ČSÚ na adrese uvedené v záhlaví této smlouvy proti písemnému potvrzení.
8. Objednatel je oprávněn před uplynutí lhůty splatnosti vrátit zhotoviteli fakturu, která neobsahuje požadované náležitosti, která obsahuje cenu díla vyúčtovanou v rozporu s touto smlouvou nebo chybně vyúčtovanou DPH. Lhůta splatnosti ceny díla začíná v takovém případě znovu běžet ode dne doručení opravené faktury objednateli způsobem uvedeným v předchozím odstavci.
9. Cena díla se pokládá za uhrazenou okamžikem odepsání příslušné částky z účtu objednatele ve prospěch účtu zhotovitele.

**Článek VIII.**

**Další povinnosti smluvních stran**

1. Zhotovitel se zavazuje řídit se při provádění penetračních testů podle této smlouvy pokyny objednatele a jeho interními předpisy souvisejícími s předmětem plnění smlouvy, které objednatel zhotoviteli poskytne nebo pokyny jím pověřených osob.
2. Zhotovitel je povinen provádět svoje činnosti tak, aby nebyl v nadbytečném rozsahu omezen provoz v místě plnění.
3. Zhotovitel zajistí, aby všechny osoby, které se na jeho straně podílí na plnění předmětu smlouvy a které budou přítomny v místě plnění, dodržovaly všechny bezpečnostní a provozní předpisy, především „Bezpečnostní pokyny pro obchodní partnery v oblasti požární ochrany, bezpečnosti práce a ochrany majetku“, které jako příloha č. 2 tvoří nedílnou součást této smlouvy.
4. Zhotovitel odpovídá za přijetí přiměřených opatření zabraňujících škodám na majetku nebo zdraví v místě plnění a na zařízeních objednatele.
5. Zhotovitel souhlasí s tím, aby subjekty oprávněné dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, v platném znění, provedly finanční kontrolu závazkového vztahu vyplývajícího ze smlouvy s tím, že se zhotovitel podrobí této kontrole a bude působit jako osoba povinná ve smyslu ustanovení § 2, písm. e) uvedeného zákona.
6. Zhotovitel je povinen i bez pokynů objednatele provést neodkladné úkony související s předmětem plnění podle této smlouvy, které jsou nezbytné pro zamezení vzniku škody. V případě takových úkonů bude smluvními stranami podle jejich povahy projednána a provedena případná náhrada ve smyslu ust. § 2908 občanského zákoníku.
7. Zhotovitel je povinen po celou dobu trvání této smlouvy udržovat v platnosti pojištění odpovědnosti za škodu způsobenou zhotovitelem třetí osobě s limitem pojistného plnění ve výši minimálně 500.000 Kč (slovy: pět set tisíc korun českých). Zhotovitel se zavazuje, na výzvu objednatele, kdykoli v době trvání této smlouvy objednateli pojistnou smlouvu předložit.
8. Zhotovitel není oprávněn zajistit plnění podle této smlouvy anebo jeho dílčí část prostřednictvím subdodavatelů.
9. Zhotovitel se zavazuje, že jeho pracovníci po celou dobu plnění této smlouvy budou splňovat technicko-kvalifikační předpoklady vymezené ve výzvě a zadávacích podmínkách k této veřejné zakázce, tj. že:
10. vedoucího týmu bude mít:
* ukončené vysokoškolské vzdělání;
* znalost českého jazyka, resp. slovenského jazyka;
* odbornou praxi z oblasti řízení projektů informační bezpečnosti alespoň 3 let;
* odborná způsobilost potvrzená uznávanou autoritou (např. certifikace EC-Council CEH nebo certifikace (ISC)2 CISPP).
1. ostatní členové týmu
* komunikace v českém nebo slovenském jazyce;
* ukončené minimálně středoškolské vzdělání;
* minimálně 3 roky praxe v oboru bezpečnostního a penetračního testování.
1. Objednatel je povinen po celou dobu trvání této smlouvy poskytovat zhotoviteli veškerou potřebnou součinnost.

**Článek IX.**

**Sankce**

1. V případě prodlení s provedením penetračních testů včetně odevzdání závěrečného hodnocení bezpečnosti testovaných aplikací v termínu stanoveném v článku V. této smlouvy anebo s odstraněním vad a nedodělků ve lhůtě stanovené v akceptačním protokolu podle článku VI. odst. 2 písm. b) této smlouvy je objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši 3.500 Kč (slovy: tři tisíce pět set korun českých) za každý započatý den prodlení.
2. V případě porušení povinností podle článku VIII. odst. 7. nebo X. této smlouvy je objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši 100.000 Kč (slovy: jedno sto tisíc korun českých) za každý jednotlivý případ porušení smluvní povinnosti.
3. V případě porušení jiné smluvní povinnosti je objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši 1.000 Kč (slovy: jeden tisíc korun českých) za každý den trvání porušení smluvní povinnosti a jednotlivý případ porušení smluvní povinnosti.
4. Splatnost smluvních pokut nastává dnem porušení smluvní povinnosti. Zhotovitel je povinen zaplatit smluvní pokutu ve lhůtě uvedené ve výzvě objednatele k zaplacení smluvní pokuty.
5. Ujednáním o smluvních pokutách není dotčen nárok na náhradu případně způsobené škody, kterou je objednatel oprávněn požadovat v plné výši.
6. Objednatel je oprávněn jednostranně započíst svou pohledávku za zhotovitelem z titulu smluvní pokuty vůči jakékoli splatné pohledávce zhotovitele za objednatelem.
7. V případě prodlení objednatele s uhrazením ceny díla má zhotovitel nárok na úrok z prodlení v zákonné výši.

**Článek X.**

**Ochrana důvěrných informací**

1. Zhotovitel se zavazuje zachovávat mlčenlivost ohledně skutečností, které se v souvislosti s plněním smlouvy dozvěděl, nebo které objednatel označil za důvěrné, jakož i údajů dle zákona č. 89/1995 Sb., o státní statistické službě, v platném znění (dále jen „důvěrné informace“). Důvěrné informace budou zhotovitelem použity výhradně k činnostem, kterými bude zajištěno dosažení účelu smlouvy. Zhotovitel nesdělí či nezpřístupní žádnou z důvěrných informací třetím osobám, nevyužije ji k vlastnímu prospěchu nebo jinak nezneužije. Povinnost mlčenlivosti a zachování důvěrnosti informací se nevztahuje na informace, které se staly obecně známými za předpokladu, že se tak nestalo porušením některé z povinností vyplývajících ze smlouvy, nebo o kterých tak stanoví zákon, zpřístupnění je však možné vždy jen v nezbytném rozsahu.
2. Za důvěrné se nepovažují takové informace, které je objednatel jako organizační složka státu povinen zveřejňovat.
3. Zhotovitel se rovněž zavazuje pro případ, že se v průběhu plnění předmětu smlouvy dostane do kontaktu s osobními údaji, že je bude ochraňovat a nakládat s nimi plně v souladu s příslušnými právními předpisy, zejména se zákonem č. 101/2000 Sb., o ochraně osobních údajů, v platném znění (dále jen „zákon o ochraně osobních údajů“). Smluvní strany se v případě kontaktu s osobními údaji, který bude spadat pod zákon o ochraně osobních údajů, zavazují uzavřít dodatek ke smlouvě, jehož obsahem bude dohoda o zpracování osobních údajů.

**Článek XI.**

**Kontaktní osoby**

Za účelem řádné realizace této smlouvy jmenují smluvní strany tyto kontaktní osoby ve věcech technických a administrativních:

* za objednatele: Bc. Pavel Charvát

e-mail:

tel.:

* za zhotovitele: Dan Vaníček

e-mail:

tel.:

**Článek XII.**

**Odstoupení od smlouvy**

1. Smluvní strany jsou oprávněny od této smlouvy odstoupit s účinky do budoucna v případě jejího podstatného porušení druhou smluvní stranou s tím, že za podstatné porušení smlouvy se pro účely tohoto ujednání pokládá zejména:
2. porušení povinnosti zhotovitele mít po celou dobu trvání této smlouvy v platnosti pojistnou smlouvu s limitem pojistného plnění ve výši podle článku VIII. odst. 7. této smlouvy;
3. porušení povinnosti zhotovitele podle článku VIII. odst. 8. této smlouvy;
4. porušení povinnosti zhotovitele podle článku X. této smlouvy.
5. Odstoupení od smlouvy podle předchozího odstavce se nedotýká práva na zaplacení smluvních pokut anebo úroků z prodlení.
6. Smluvní strany jsou povinny poskytnout si v případě předčasného ukončení této smlouvy veškerou potřebnou součinnost tak, aby žádné ze smluvních stran nevznikla škoda.

**Článek XIII.**

**Platnost a účinnost smlouvy**

Tato smlouva nabývá platnosti a účinnosti dnem jejího podpisu oprávněnými zástupci obou smluvních stran.

**Článek XIV.**

**Závěrečná ustanovení**

1. Práva a povinnosti smluvních stran plynoucí z této smlouvy nebo v souvislosti s ní, se řídí českým právním řádem, zejména občanským zákoníkem.
2. Poskytovatel uděluje bezvýhradní souhlas se zveřejněním plného znění této smlouvy v souladu s ust. § 147a zákona o veřejných zakázkách a ve smyslu zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů a dalších právních předpisů.
3. Smluvní strany se dohodly, že uveřejnění smlouvy v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, zajistí objednatel.
4. Neplatnost nebo neúčinnost některého ustanovení této smlouvy nezpůsobuje neplatnost nebo neúčinnost celé smlouvy. V případě, že některé ustanovení této smlouvy bude neplatné nebo neúčinné, zavazují se smluvní strany nahradit takové neplatné nebo neúčinné ustanovení platným a účinným ustanovením, které bude co do obsahu a významu neplatnému nebo neúčinnému ustanovení co nejblíže.
5. Veškerá oznámení podle této smlouvy musí být učiněna písemně a zaslána kontaktní osobě druhé smluvní strany prostřednictvím datové schránky, elektronické pošty nebo doporučenou poštou, případně předána osobně do podatelny, není-li ve smlouvě uvedeno jinak.
6. Smluvním jazykem je jazyk český a v českém jazyce bude probíhat veškerá komunikace ve všech věcech týkajících se této smlouvy.
7. Nedílnou součástí této smlouvy jsou:
* příloha č. 1 – Technická specifikace a popis stávajícího stavu
* příloha č. 2 – Bezpečnostní pokyny pro obchodní partnery v oblasti požární ochrany, bezpečnosti práce a ochrany majetku.
1. Tuto smlouvu lze měnit a doplňovat pouze vzestupně číslovanými písemnými dodatky podepsanými oprávněnými zástupci obou smluvních stran.
2. Tato smlouva byla vyhotovena ve čtyřech stejnopisech, z nichž po dvou obdrží každá ze smluvních stran.
3. Smluvní strany shodně prohlašují, že tato smlouva byla uzavřena na základě jejich pravé a svobodné vůle a byla sepsána určitě a srozumitelně.

V Praze dne 1. 9. 2016 V Praze dne 29. srpna 2016

…………………………………………………… ……………………………………………………..

Česká republika – Český statistický úřad BDO IT a. s.

Mgr. Radoslav Bulíř, ředitel Dan Vaníček

sekce ekonomické a správní předseda představenstva

**Příloha č. 1**

Smlouvy o provedení bezpečnostních testů modulů Statistického informačního systému dostupných z internetu a webové prezentace ČSÚ

1. **název veřejné zakázky**

|  |
| --- |
| **„Bezpečnostní testy modulů Statistického informačního systému dostupných z internetu a webové prezentace ČSÚ“** |

1. **Identifikační údaje zadavatele**

|  |  |
| --- | --- |
| Název: | **Česká republika – Český statistický úřad** (ČSÚ) |
| Sídlo: | Na padesátém 81, 100 82, Praha 10 - Strašnice |
| IČO: | 000 25 593 |
| Internetová adresa profilu zadavatele: | http://www.czso.cz/csu/redakce.nsf/i/verejne\_zakazky\_a\_vyberova\_rizeni |
| Osoba oprávněná jednat jménem či za zadavatele: | **Mgr. Radoslav Bulíř**,vrchní ředitel sekce ekonomické a správní |

**3. Podrobná specifikace předmětu plnění**

Předmětem plnění je:

1. penetrační a zátěžový (DDoS) test webové aplikace požadavky-vykazy.czso.cz
2. penetrační a zátěžový (DDoS) test webové aplikace danteweb.czso.cz
3. penetrační a zátěžový (DDoS) test webové aplikace vdb.czso.cz
4. penetrační a zátěžový (DDoS) test webové prezentace ČSÚ czso.cz

Penetrační testy webových aplikací budou zaměřeny na identifikaci bezpečnostních slabin minimálně v rozsahu metodiky OWASP Testing Guide v.4. Součástí testování bude prověření bezpečnosti aplikací jak z pohledu anonymního uživatele, tak se znalostí autentizačních údajů.

Penetrační test webové prezentace czso.cz bude zaměřen na identifikaci bezpečnostních slabin webové prezentace potenciálně zneužitelných útočníkem z vnějšku minimálně v rozsahu metodiky OWASP Testing Guide v.4.

Zátěžové (DDoS) testy webových aplikací i webové prezentace czso.cz proběhnou takovým způsobem nebo v takových časech, aby negativně neovlivnily běžný provoz sítě ČSÚ. Požadovány jsou minimálně testy odolnosti proti SYN flood (se sílou alespoň 1500 pps) a Slow HTTP POST nebo Slowloris.

Veškeré testy budou provedeny bez destruktivních zásahů, tj. nebudou se provádět žádné změny, které by poškodily testovaný systém.

Součástí výstupů bude závěrečné zhodnocení bezpečnosti testovaných aplikací a webové prezentace, které bude obsahovat popis rizika vyplývajícího z jednotlivých nalezených zranitelností, konkrétní návrhy na odstranění těchto zranitelností a nedostatků, případně návrhy na zvýšení bezpečnosti testovaných částí. Výstupy budou také obsahovat podrobné popisy jednotlivých provedených testů (použité nástroje a popis jejich konfigurace/použitých parametrů). Každá nalezená zranitelnost bude kategorizována z pohledu její závažnosti, pravděpodobnosti zneužití a náročnosti odstranění. Každá klasifikace bude obsahovat minimálně 3 kategorie (např. vysoká/střední/nízká pravděpodobnost zneužití). Jedním z výstupů bude také manažerské shrnutí průběhu testování s přehledem nalezených zranitelností a nedostatků.

Popis aplikací

1. Požadavky-výkazy

Aplikace Požadavky-výkazy je součástí Statistického informačního systému (SIS) ČSÚ. Je určena pro zadávání požadavků externími uživateli systému. Umožňuje zadávání požadavků, přenos zadaných požadavků do interního systému Požadavky SIS ČSÚ a jejich sledování. Ukládání dat do aplikace se provádí průběžně v rámci celého roku, tedy bez časového omezení.

Přístup do aplikace je chráněn pomocí autentizace jménem a heslem. Účty jsou vygenerovány pouze definované skupině uživatelů vedených v aplikaci Registr uživatelů.

Aplikace se skládá ze 4 základních funkcionalit:

* **Prohlížení seznamu požadavků**

Uživatel má možnost volbou v menu Moje žádosti prohlížet, filtrovat a vyhledávat v seznamu požadavků jím zadaných. Též má možnost seznam požadavků setřídit podle zvoleného údaje klikáním na titulek sloupce údaje a to střídavě vzestupně nebo sestupně. Styl třídění je zobrazen v nadpisu sloupce malou šipkou, směrem nahoru pro vzestupné setřídění a směrem dolů pro sestupné setřídění. Zobrazení detailu požadavku



Obrázek Výsledek vyhledávání v seznamu požadavků

* **Zobrazení detailu požadavku**

Uživatel může zobrazit detail vybraného požadavku.

V pohledu na seznam požadavků uživatel vyhledá požadavek, jehož detail chce zobrazit. Kliknutím na ID požadavku systém zobrazí detail požadavku, který obsahuje záhlaví se základními údaji a dále následující záložky dle typu požadavku:

* + Popis a důvod – pro všechny typy požadavků
	+ Vyhláška – pouze pro typy požadavků nové zjišťování, změna zjišťování
	+ Správa požadavku – pro všechny typy požadavků
	+ Stanovisko – pro všechny typy požadavků



Obrázek - Zobrazení detailu požadavku

* **Založení nového požadavku**

Založení nového požadavku provádí uživatel v několika krocích pomocí průvodce zadáváním údajů.

Posun na následující krok se provádí vždy pomocí tlačítka „Následující“. Posun zpět na předchozí krok se provádí tlačítkem „Předchozí“. Zrušení akce zakládání nového požadavku může uživatel provést pomocí tlačítka „Storno“, které je dostupné na každé obrazovce průvodce.



Obrázek - Obrazovka pro vložení základních údajů požadavku Nové zjišťování

* **Založení požadavku z kopie**

Uživatel v navigačním panelu klikne na rozbalovací tlačítko „Založit požadavek“ a z nabídky vybere jednu z následujících funkcí, podle toho, jaký typ požadavku chce založit:

* Nové zjišťování – vytvořit z kopie
* Změna zjišťování – vytvořit z kopie
* Zrušení zjišťování – vytvořit z kopie
* Zjišťování beze změny – vytvořit z kopie

Systém zobrazí seznam „Výběr vzorového požadavku“, ve kterém jsou obsaženy existující požadavky zvoleného typu. Seznam je stránkovaný a je možné v něm nastavit velikost stránky. Seznam je možné seřadit podle libovolného sloupce. Pod seznamem je dostupné tlačítko Zrušit, kterým může uživatel zavřít seznam a zrušit akci zakládání nového požadavku z kopie.



Obrázek - Seznam pro výběr vzorového požadavku

1. VDB

Veřejná databáze (VDB) je budována jako součást nového statistického informačního systému ČSÚ a je určená k prezentaci agregovaných statistických údajů pro veřejnost, je tedy součástí funkčních bloků zajišťujících diseminaci statistických údajů.

Prezentace údajů VDB je zajištěna prezentační aplikací. Teprve v okamžiku výběru předdefinovaných výstupních objektů (PVO) se dotahují potřebné statistické údaje z primární databáze. Zobrazované statistické údaje v HTML formátu lze exportovat (PDF, XLS, XML). VDB umožňuje i přímý přístup k agregovaným datům s možností vytváření a ukládání vlastních (uživatelských) dotazů (statistických tabulek). Vedle prezentace PVO poskytuje i možnost zobrazovat speciální stránky (profily území), vytvářet uživatelské tabulky, prohlížet seznamy statistických proměnných a vyhledávat k nim PVO, podporuje i fulltextové vyhledávání, pro každý statistický údaj načtený z primární databáze je možno zobrazit sérii metainformací (identifikačních i doplňkových). Přístupy k aplikaci jsou monitorovány několika systémy (monitoring diseminace ČSÚ, Google Analytics, vlastní měření přístupů k PVO)

Prezentace pro externí uživatele umožňuje nabízet pouze PVO schválené pro externí použití (existuje také část pro interní uživatele, která je dostupná pouze z vnitřní sítě ČSÚ). Během synchronizace statistických údajů mezi interní a externí databází se důvěrná data skrývají, uživatelům se místo konkrétních údajů zobrazuje náhradní text. Prezentační aplikace neumožní prezentovat údaje mimo interval zveřejnění.

Uživatel se může do aplikace zaregistrovat, jako přihlášený externí uživatel pak může využívat některé nadstandardní služby, např. generování uživatelských tabulek v off-line režimu a zaslání výsledku na e-mailovou adresu nebo ukládání vlastních dotazů pro příští použití.

Prezentace pro interní i externí uživatele tvoří základní součást prezentačního systému ČSÚ. To vyžaduje eliminaci výpadků na minimální dobu. Pro rozložení zátěže je využíván cluster několika serverů a load-balancer, a to jak pro interní, tak externí prostředí.



Obrázek - ukázka aplikace VDB

1. DanteWeb

DanteWeb je aplikace, která umožňuje zpravodajským jednotkám vyplnit výkazy **přímo na internetu.**Pro práci v aplikaci je potřeba **provést registraci**, přihlašovací údaje potřebné pro registraci jsou součástí Oznámení o zpravodajské povinnosti.

Aplikace Dante Web umožňuje respondentům vyplňovat statistické formuláře, ke kterým má příslušná zpravodajská jednotka přístup. Aplikace kontroluje některá pořízená data online (během pořizování) a některá při ukládaní formuláře. Aplikace poskytuje respondentům přístup do již vyplněných a uložených formulářů za minulá období i průběžné vyplňování formuláře, kde formulář je možné uložit rozpracovaný a následně se k němu vrátit později.

Uživatelská příručka s detailním popisem aplikace je veřejně dostupná na webu ČSÚ. Na adrese: <https://www.czso.cz/documents/11304/25713657/danteweb_uzivatelska_prirucka_150122.pdf>

1. Webová prezentace czso.cz

Webové stránky ČSÚ slouží vedle snadného vyhledávání základních informací o úřadu především k prezentaci aktuálních statistik a jako takové jsou tedy nesmírně důležitým informačním zdrojem nejen pro širokou veřejnost, ale i pro ostatní orgány veřejné správy. Z povahy věci vyplývá, že požadavky na dostupnost a integritu prezentovaných údajů jsou velmi vysoké, neboť je s nimi přímo spojena kredibilita jejich původce – ČSÚ.

Webové stránky jsou dostupné na adrese: [www.czso.cz](http://www.czso.cz)

Součástí prezentace je redakční systém dostupný z vnitřního prostředí ČSÚ po autentizaci pouze pro autorizované správce.

Součástí poptávaných testů nejsou testy webových aplikací dostupných z webové prezentace ČSÚ (mimo těch přímo specifikovaných v tomto dokumentu).

,

Obrázek – Úvodní stránka webové prezentace czso.cz

Technické informace o aplikacích

Aplikace Statistického informačního systému jsou realizovány jako třívrstvá aplikační architektura složená z prezentační, aplikační a databázové vrstvy.

* **prezentační**

Jako aplikační rámec pro běh aplikací bude použitý systém JBoss Application Server. Aplikace provozované na tomto serveru jsou vyvinuté na platformě založené na technologiích definovaných standardem J2EE.

Aplikace VDB je psána technologii IceFaces, konkrétní implementací podle specifikace JSF (Java Server Faces).

Webová prezentace a redakční systém je postaven na technologii Liferay Community Portal a Java portletech.

* **aplikační**

Aplikační vrstvu tvoří aplikační server, který zabezpečuje byznys logiku, řízení transakcí, provedení workflow, administrátorské, ověřovací a bezpečnostní služby.

Jednotlivé části byznys logiky jsou poskytované prezentačnímu systému ve formě webových služeb. Klientské aplikace komunikují s aplikačním serverem pomocí protokolu HTTP případně HTTPS.

Aplikační vrstva je koncipovaná jako skupina J2EE web aplikací a webových služeb postavená na platformě JBoss Application Server.

Aplikace VDB běží na Oracle WebLogic server.

* **datová**

Datová vrstva zajišťuje uložení dat, pro něž využívá databázový systém ORACLE 11g.

Aplikace jsou chráněny systémem IPS, jsou za FireWallem operujícím na 3 vrstvě ISO/OSI a z důvodu zajištění rozložení zátěže a vysoké dostupnosti jsou v prostředí využívány load-balancery.

**Příloha č. 2**

Smlouvy o provedení bezpečnostních testů modulů Statistického informačního systému dostupných z internetu a webové prezentace ČSÚ

**BEZPEČNOSTNÍ POKYNY PRO OBCHODNÍ PARTNERY V OBLASTI POŽÁRNÍ OCHRANY, BEZPEČNOSTI PRÁCE A OCHRANY MAJETKU**

**Článek I.**

**Úvod**

Tento dokument:

1. je písemnou informací o rizicích a dokladem o dohodnuté koordinaci mezi stranami při zajišťování bezpečnosti a ochrany zdraví při práci, ve smyslu ustanovení platného znění zákoníku práce, tak, aby ohrožení bezpečnosti a zdraví bylo minimalizováno,
2. se současně stává dokladem o způsobu zabezpečování povinností na úseku požární ochrany ve smyslu § 30, odst. 2, písm. h), vyhlášky č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci),
3. zavazuje obchodního partnera, jeho zaměstnance a osoby jím vyslané k dodržování pravidel stanovených Českým statistickým úřadem k ochraně majetku.

Obchodním partnerem se v tomto dokumentu rozumí firma, která provádí práce nebo služby v budově ČSÚ na základě požadavku ČSÚ.

Zaměstnancem se v tomto dokumentu rozumí obchodní partner, pokud je fyzickou osobou, zaměstnanci obchodního partnera a osoby vyslané obchodním partnerem k provedení práce nebo služeb.

Tento dokument může být operativně doplňován písemnou i ústní formou.

**Článek II.**

**Požární ochrana a Bezpečnost a ochrana zdraví při práci**

1. **Požární ochrana**
	1. Podle ustanovení § 4 odst. 2 písm. g) zákona č. 133/85 Sb., o požární bezpečnosti, ve znění pozdějších předpisů, se objekt Českého statistického úřadu, Na padesátém 81, 100 82 Praha 10, zařazuje do kategorie činností se zvýšeným požárním nebezpečím. Toto začlenění bylo provedeno na základě § 28 vyhlášky č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci).
	2. V celé budově ČSÚ je vyhlášen přísný zákaz kouření (vyhrazené místa pro kuřáky je zřetelně označeno) a používání otevřeného plamene nebo jiného zdroje zapálení kromě činností, na které je zpracován technologický postup nebo je vypracován příkaz ke svařování podle vyhlášky č.87/2000 Sb., kterou se stanoví podmínky požární bezpečnosti při svařování a nahřívání živic v tavných nádobách. Pro vykonávání svářečských prací je obchodní partner povinen stanovit organizační a technická opatření k zajištění požární ochrany a odpovídá za zajištění požární bezpečnosti po celou dobu výkonu svářecích prací. Následný požární dohled po skončení svařování může po dohodě zajistit ČSÚ. Tato skutečnost musí být potvrzena v písemném příkazu ke svařování.
	3. Zaměstnanci jsou povinni si počínat tak, aby nedošlo ke vzniku požáru.
	4. Zaměstnanci, kteří provádějí práce, které nejsou časově omezeny, musí absolvovat školení o požární ochraně. K tomuto školení obchodní partner určí vedoucího zaměstnance, jehož proškolení provede technik požární ochrany (dále jen „PO“) ČSÚ. Vedoucí zaměstnanec pak školí své podřízené zaměstnance podle tematického plánu a časového rozvrhu školení o PO objednatele.
	5. Vždy nejpozději do dvou dnů po každém opakovaně provedeném školení předloží vedoucí skupiny kopii záznamu o školení požárnímu technikovi PO ČSÚ.
	6. **Zaměstnanci jsou povinni se seznámit s Požárním řádem, Požárními poplachovými směrnicemi a Evakuačním plánem Českého statistického úřadu.** Požární řád, Požární poplachové směrnice a Evakuační plán jsou vyvěšeny na chodbách v prostoru u výtahů, event. na dalších vybraných volně přístupných místech.
	7. Ohlašovnou požáru je recepce v 1. nadzemním podlaží.
	8. Hlásiče požáru jsou zřetelně označeny, v určených prostorách jsou rozmístěny hasicí přístroje.
	9. **Každý poplach** (nejen požární, ale i poplach vyhlášený při mimořádných událostech) **je vyhlašován vnitřním rozhlasem.** Po jeho vyhlášení se automaticky odblokují turnikety a elektromagnetické zámky. **Při opuštění budovy se zaměstnanci řídí Evakuačním plánem.**

**Je zakázáno zejména:**

1. používat únikové východy v jiných než mimořádných situacích,
2. blokovat dveře na únikových cestách, zastavět tyto cesty nebo snižovat jejich průchodnost (např. zastavěním těchto cest inventářem, materiálem apod.),
3. znemožnění přístupu k rozvodům vody a el. energie, k požárním hydrantům a přenosným hasicím přístrojům.
4. **Bezpečnost a ochrana zdraví při práci**
	1. Činnost ČSÚ je převážně administrativního charakteru s odpovídajícími pracovními riziky.
	2. K minimalizování ohrožení bezpečnosti a zdraví jsou zaměstnanci povinni dodržovat tato pravidla:
* přísný zákaz kouření v celé budově ČSÚ (výjimkou je kuřárna),
* nemanipulovat se žádným zařízením, pokud není určeno k výkonu prací obchodního partnera.
	1. Pro výkon své činnosti musí mít obchodní partner zpracován svůj seznam pracovních rizik pro výkon prací a je povinen v rámci svého bezpečnostního školení s těmito riziky své zaměstnance seznámit.
	2. Zaměstnanci musí mít k výkonu dané práce potřebnou odbornou a zdravotní způsobilost a příslušné instrukce k činnostem, které mají provádět.
	3. K činnosti, kterou mají zaměstnanci vykonávat, musí být vybaveni osobními ochrannými pracovními prostředky odpovídajícími ohrožení, jež vyplývá z prováděných prací, popř. rizika pracoviště, dále vhodnými pracovními pomůckami a prostředky (nářadí).

**Článek III.**

**Ochrana majetku**

#### **Ohlašování prací**

Práce prováděné obchodními partnery v pracovní i mimopracovní době hlásí ředitel příslušného odboru předem písemně Odboru bezpečnosti a krizového řízení s uvedením názvu obchodního partnera, účelu prací, doby jejich trvání, kontaktních osob obchodního partnera i ČSÚ, jména a příjmení osob vykonávajících práce a čísla jejich občanského průkazu. Zaměstnanci se hlásí v recepci, kde se evidují jako návštěva. O jejich příchodu vyrozumí strážný kontaktní osobu ČSÚ.

#### **Přidělování přístupových karet a klíčů**

Přístupové karty a klíče od určených prostor mohou být na základě písemné žádosti ředitele odboru vydány zaměstnancům, kteří se dlouhodobě nachází na jeho pracovišti, pokud to charakter práce vyžaduje (např. úklidové práce apod.). Ztrátu či zcizení přístupové karty nebo klíče, jejich zneužití nebo poškození, které brání funkčnosti, ohlásí zaměstnanci řediteli příslušného odboru, který neprodleně informuje Odbor bezpečnosti a krizového řízení, a to písemně nebo telefonicky s následným písemným potvrzením. Obchodní partner je povinen uhradit veškeré náklady spojené s pořízením nové karty, klíče nebo změnami klíčového režimu.

**Vjezd a parkování**

Ve výjimečných případech je možné krátkodobé parkování vozidel zaměstnanců, a to pouze v 1. podzemním podlaží, pokud není z provozních důvodů možné použít technický vjezd. Potřebu takového parkování sdělí písemně ředitel příslušného odboru strážní službě s uvedením firmy a účelu požadovaného parkování.

**Zaměstnanec je povinen respektovat zejména tato nařízení:**

1. V garážích je nutné dodržovat platné dopravní předpisy.
2. Není povolen vjezd automobilů na pohon LPG.
3. Je zakázáno zdržovat se s vozidlem v prostoru vjezdu do garáží a výjezdu z nich.
4. Vozidlo musí být zaparkováno tak, aby umožnilo volný průchod k výtahům, schodišti a do technického zázemí. Zároveň musí být umožněn volný přístup k požárním hydrantům, přenosným hasicím přístrojům a požárním hlásičům.
5. Průchod osob příjezdovým tunelem nebo příjezdovými vraty je možný pouze v mimořádných případech za dodržení zvýšené opatrnosti a zajištění dozoru strážného.

#### **Dodržování pravidel**

**Zaměstnanec zejména:**

1. Nesmí na pracovišti požívat alkohol nebo jiné návykové látky a nesmí pod jejich vlivem nastoupit do práce.
2. Nesmí poškozovat, zapůjčovat si nebo zcizit majetek ČSÚ.
3. Nesmí používat prostředky a předměty ČSÚ, pokud to není dohodnuto nebo nezbytně nutné pro výkon sjednané práce.
4. Nesmí otevírat uzamčené i neuzamčené části zařízení kanceláře nebo jiných prostor.
5. Je zavázán mlčenlivostí o skutečnostech, které se dozví během své činnosti, a to i po ukončení prací nebo pracovního poměru.
6. Má zakázáno nahlížet do materiálů umístěných nebo uložených v místnosti, ani je nebo jejich části jakýmkoliv způsobem kopírovat, upravovat, pořizovat z nich výpisy, seznamovat s obsahem nebo jeho částí další osoby a rovněž si je nesmí zapůjčovat nebo je zcizit, ani k těmto činnostem napomáhat.
7. Má povinnost chovat se tak, aby nedošlo ke zneužití materiálů, jejich poškození nebo zničení.
8. Nesmí nikomu poskytovat svěřený klíč ani vyrábět jeho kopie.
9. Nesmí klíč nijak označovat ani upravovat.
10. Vždy po ukončení prací uzamkne kancelář nebo jiný prostor, ve kterém prováděl práce.
11. Používá a ukládá klíč tak, aby nedošlo k jeho ohnutí nebo jinému poškození, které by způsobilo jeho nefunkčnost, nebo by vedlo k jeho ztrátě či zcizení.
12. Používá a ukládá přístupovou kartu tak, aby nedošlo k jejímu ohnutí, prasknutí, poškrábání, jinému poškození nebo její ztrátě či zcizení.
13. Nesmí přístupovou kartu polepovat, popisovat, proděravět nebo jinak upravovat.

**Je zakázáno zejména:**

1. Umožnit vstup do budovy nepovolané osobě.
2. Poskytovat osobní průkazy, vstupní kartu, svěřené klíče nebo jiné pomůcky sloužící k ochraně majetku neoprávněným osobám.
3. Jakkoliv manipulovat s prvky bezpečnostních technologií a poškozovat je.
4. Nechávat otevřená okna během pracovní i mimopracovní doby, pokud by mohlo dojít k ohrožení nebo poškození majetku ČSÚ.
5. Blokovat dveře ovládané čtecím zařízením.
6. Používat výtah jinak, než v souladu s provozními pokyny, dveře výtahu nesmí být v žádném případě blokovány.
7. Vstupovat na střechy /výjimkou je kuřárna/ a slunolamy (pokud to nevyžaduje charakter práce), odkládat nebo vhazovat na ně předměty nebo je jinak znečisťovat.

**Článek IV.**

**Organizační opatření**

1. Chce-li obchodní partner provést výměnu vedoucího zaměstnance, musí informovat ČSÚ s předstihem nejméně 14 dnů, aby ČSÚ mohl včas zajistit školení o požární ochraně nového vedoucího zaměstnance dodavatele.
2. Pracovní úrazy zaměstnanců vyšetřuje, ohlašuje a záznamy o úrazu zasílá v souladu s nařízením vlády č. 201/2010 Sb., o způsobu evidence úrazů, hlášení a zasílání záznamu o úrazu, kterým se stanoví vzor záznamu o úrazu a okruh orgánů a institucí, kterým se ohlašuje pracovní úraz a zasílá záznam o úrazu, obchodní partner.
3. Obchodní partner se zavazuje zajistit dodržení výše uvedených bezpečnostních pokynů a potvrzuje, že pracoviště, na kterém se mají práce vykonávat, bylo řádně předáno.