ESET SERVICES

ESET Services
Specialista služeb informační bezpečnosti (dále jen „Služby“)

Nabídka

Služba: **Bezpečnostní testování webových aplikací Národní digitální knihovny**

Pro společnost: **Národní knihovna České republiky**
Klementinum 190, Staré Město
110 01 Praha

IČO: 000 23 221
DIČ: CZ00023221
(dále jen „Zákazník“)

Datum vypracování: 19.01.2022
Platnost nabídky: 19.03.2022

Kontaktní osoba: [redacted]
tel.: [redacted]
e-mail: [redacted]

Obsah

1) Základní údaje o Dodavateli a Poskytovateli Služby

Dodavatel:	**ESET software, spol. s r.o.**
Sídlo:	**Jankovcova 1037/49, 170 00 Praha**
Oddíl a vložka v Obchodním rejstříku:	**Obchodní rejstřík Městský soud Praha, oddíl: C, vložka: 84196**
Bankovní spojení:	[redacted]
IČO:	**264 67 593**
DIČ:	**CZ26467593**
Doba působení na českém trhu:	**od roku 2001**

(dále jen „ESET software“)

Společnost **ESET, spol. s r. o.** se sídlem ve Slovenské republice, na Einsteinova 24, 85101 Bratislava, Slovensko, zapsaná v obchodním rejstříku Okresního soudu Bratislava I, oddíl: Sro, vložka číslo: 3586 / B, IČ: 31 333 532 (dále jen "ESET"), vystupuje v České republice prostřednictvím svého distribučního zastoupení **ESET software, spol. s r.o.**, který je dodavatelem Služby, tedy ESET software zajišťuje obchodní vztahy s partnery a koncovými zákazníky. Výzkum, vývoj produktů a poskytování služeb je zajišťováno společností ESET a jejími vývojovými centry. V České republice je takovým centrem společnost **ESET Research Czech Republic s.r.o.**, která se jako subdodavatel společnosti ESET podílí na poskytování služeb ve smyslu této nabídky.

1.1 Kontaktní údaje

Pokud máte zájem o jakékoliv doplňující informace k této nabídce, prosím, kontaktujte následující kontaktní osoby (Dále jen „Odpovědná osoba“):

Osoba odpovědná pro obchodní kontakt:

[redacted]
Security Sales Representative
Mobile: [redacted]
e-mail: [redacted]

Osoba odpovědná pro případ nedostupnosti kontaktní osoby, nebo pro eskalaci řešení vašeho požadavku:

[redacted]
IS Security Director
Mobile: [redacted]
e-mail: [redacted]

Osoba odpovědná pro technické záležitosti:

Kontakt bude upřesněn po stanovení termínu pro dodání Služby.

1.2 Důvěrnost poskytovaných informací

Informace uvedené v této cenové nabídce (dále jen "Nabídka") nebo poskytnuté v souvislosti s ní ať ústně, písemně, elektronicky nebo v jiné formě, považujeme za důvěrné, a to i bez nutnosti jejich výslovného označení jako důvěrné (dále jen "Důvěrné informace"). Zákazník souhlasí s tím, že Důvěrné informace použije výhradně na vyhodnocení obchodní transakce, na realizování obchodní transakce nebo obchodního vztahu, a na jiný účel pouze tehdy, pokud s tím budeme explicitně písemně souhlasit. Tyto Důvěrné informace nesmějí být zpřístupněny třetí straně nebo zveřejněny bez našeho předchozího písemného souhlasu. Povinnost Zákazníka chránit Důvěrné informace trvá po dobu pěti (5) let ode dne jejich poskytnutí nebo zpřístupnění.

2) Odborný profil dodavatele

Dovolujeme si předložit klíčové důvody akceptace odborného profilu společnosti ESET:

- **zázemí společnosti ESET jako technologické firmy vytváří prostor pro akumulaci potřebných kompetencí,**
- **výzkum zranitelností IT systémů a infrastruktury sleduje nejnovější trendy IT bezpečnosti,**
- **velikost a odborné kvality realizačního týmu jsou zárukou dodání požadovaných služeb,**
- **zásady informační bezpečnosti nejen testujeme ale také se jimi řídíme.**

Následující kapitoly detailněji popisují jednotlivé výše uvedené charakteristiky odbornosti.

2.1 Společnost ESET

Společnost ESET, založená v roce 1992, je světovým výrobcem bezpečnostního softwaru pro firemní klientelu a domácnosti a věnuje se celosvětovému boji proti vznikajícím počítačovým hrozbám. Je lídrem na trhu proaktivní detekce počítačových hrozeb. Společnost ESET má celosvětově **nejvíce za sebou následujících ocenění VB100** za detekci malwaru ze všech dodavatelů řešení internetové bezpečnosti. Od roku 2003 jsme úspěšně prošli každým testem.

Společnost ESET, globální lídr v oblasti kybernetické bezpečnosti, byla v roce 2021 ve zprávě Advanced Persistent Threat (APT) Protection Market Quadrant analytické společnosti Radicati jmenovaná již druhý rok po sobě za "předního hráče". Zpráva hodnotí dvanáct významných dodavatelů bezpečnostních softwarů na trhu, přičemž se zaměřuje na jejich funkčnost a strategickou vizi. Pouze šesti dodavatelům, mezi něž patří i společnost ESET, se podařilo získat status "předního hráče".

Zázemí technologické firmy, která se věnuje výhradně informační bezpečnosti, v současném rozsahu přibližně 1800 zaměstnanců celosvětově, respektive více než 1000 zaměstnanců v Česku a na Slovensku, dává předpoklad získání spolehlivého partnera pro projekty informační bezpečnosti.

2.2 Výzkum zranitelností IT systémů a infrastruktury

Společnost ESET pravidelně informuje o svém výzkumu v oblasti zranitelností IT systémů a infrastruktury na svém technologickém webu www.welivesecurity.com nebo i na lokálním webu www.eset.com/cz.

Níže uvádíme některé zajímavé výsledky související s nabízenými službami, které byly publikovány v posledním období:

- **D-Link camera vulnerability allows attackers to tap into the video stream**
  - https://www.welivesecurity.com/2019/05/02/d-link-camera-vulnerability-video-stream/
  - https://www.eset.com/sk/o-nas/press-centrum/malver/eset-zranitelnost-v-kamere-predavanej-aj-na-slovensku-umoznuje-sledovat-jej-zaznam/
- **DanaBot updated with new C&C communication**
  - https://www.welivesecurity.com/2019/02/07/danabot-updated-new-cc-communication/
- **Buhtrap backdoor and ransomware distributed via major advertising platform**
  - https://www.welivesecurity.com/2019/04/30/buhtrap-backdoor-ransomware-advertising-platform/

2.3 ESET Services

V roce 2009 byla vytvořena divize ESET Services, která poskytuje produkty pro řízení bezpečnosti a poradenství pro malé a střední podnikatele (SMB) i velké firemní (Enterprise) zákazníky. Výhradní zaměření na služby informační bezpečnosti sleduje poskytnutí maximální přidané hodnoty v této oblasti. Zázemí společnosti ESET, globálně uznávaného dodavatele bezpečnostních řešení, a důraz na odbornost pracovníků ESET Services je garantem kvality poskytovaných služeb.

ESET Services v jednom ze svých oddělení disponuje samostatným týmem více než 10 lidí, kteří se věnují primárně penetračnímu testování a auditním činnostem v Česku a na Slovensku. Všichni jsou kontinuálně certifikovaní a školení podle metodiky

společnosti ESET. Uvedení pracovníci jsou členy širšího týmu, který zajišťuje služby řízení informační bezpečnosti, výkonu auditní a testovací činnosti.

2.4 Odborné kvality realizačního týmu

Pro prokázání odborných kvalit uvádíme následující skutečnosti:

1. **Členové realizačního týmu provádějí bezpečnostní testování a audit vyvíjených produktů a systémů společnosti ESET. Kvalita jejich práce je po uvolnění produktů k užívání prověřena miliony uživatelů společnosti ESET.**
2. Všichni pracovníci realizačního týmu před svým přijetím do ESET Services absolvovali vstupní testy pro potvrzení odborných předpokladů pro výkon činností ve své roli. Vstupní testy se skládají ze sady praktických úloh.
3. Dalším prvkem vzdělávání je ESET Ethical Hacking Academy jako formát vzdělávání pro perspektivní studenty. Akademie se pravidelně koná každý rok, střídavě v Praze a Bratislavě. Informativní video je k dispozici zde: https://www.youtube.com/watch?v=EMKjt0ga2IE
4. V rámci interní metodiky jsou zaměstnanci realizačního týmu dále teoreticky a prakticky vzděláváni pro realizaci testování a ověřování bezpečnosti.
5. Pracovníci realizačního týmu se mají možnost účastnit domácích nebo zahraničních konferencí a školení.
6. Pro prokázání odborné kvalifikace dokážeme poskytnout relevantní certifikáty vybraných pracovníků realizačního týmu.

2.5 Zásady informační bezpečnosti nejen testujeme ale také se jimi řídíme

Společnost ESET je držitelem certifikace podle normy ISO/IEC 27001 při vývoji produktů a poskytování služeb. Pro odstranění pochybností jsou úlohy interního a certifikačního auditu zajišťovány externím dodavatelem. Zaměstnanci společnosti ESET jsou pravidelně testováni v situacích vyžadujících provedení správné reakce na situace spojené s informační bezpečností společnosti ESET a jejích zákazníků.

3) Předmět nabídky

3.1 Předmět projektu

Předmětem projektu je bezpečnostní testování webové aplikace [redacted] která slouží pro přihlášení do webové aplikace Národní digitální knihovna. Součástí testování je i webová aplikace určená pro knihovny, které přes aplikaci vytvářejí uživatelské účty do aplikace [redacted] Vytvoření účtů probíhá importováním seznamu uživatelů, kterým se následně pošle email s výzvou k nastavení hesla.

V rámci prověřování bezpečnosti aplikací bude hlavním cílem identifikace zranitelností a bezpečnostních nedostatků v aplikacích, které by mohly vést ke kompromitaci účtů testovaných aplikací. Testy proběhnou z pohledu autentizovaných a neautentizovaných uživatelů obou testovaných aplikací. Bezpečnostní testy webových aplikací budou probíhat na testovacím prostředí dle metodiky OWASP Web Security Testing Guide.

Součástí testů je i externí test infrastruktury serveru [redacted] který proběhne vůči produkčnímu prostředí a zahrnuje identifikaci otevřených portů, služeb a následně automatizovaný sken zranitelností u identifikovaných služeb spolu s manuálním prověřením. Potenciálně rizikové aktivity, resp. testy na produkčním prostředí budou probíhat v odsouhlaseném čase z důvodu potenciálního rizika omezení služeb.

3.2 Rizika testovaní

Bezpečnostní testovaní infrastruktury může mít vliv na chod a provoz zařízení, služeb a systémů (Denial of Services DoS) v testované síti. Jakkoliv cílem bezpečnostních testů není poškodit data testovaných zařízení v síti nebo způsobit jejich nedostupnost, upozorňujeme, že k tomu v ojedinělých případech může dojít. Ze zkušenosti víme, že tyto situace téměř nenastávají a ve většině případů se vůbec nestávají, nicméně na tento fakt upozorňujeme, a proto doporučujeme informovat o průběhu kompetentní osobu za správu sítě a její zařízení.

3.3 Metodika

Obecně při testovaní vycházíme z metodologie OSSTMM (www.osstmm.org) pro celkové řízeni a vyhodnocení testů. Pro samotné testovaní webových aplikací je použita metodologie OWASP (https://www.owasp.org), vybrané časti OWASP Web Security Testing Guide a OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).
Klíčovou metodikou pro testovaní, kterou ESET používá za účelem testovaní mobilních aplikací je příručka „OWASP Mobile Security Testing Guide“ (OWASP Mobile Security Testing Guide).

Bezpečnostní testování infrastruktury má 4 fáze:

1. **Získávaní informací,** během této fáze jsou získávány informace o testovaných systémech.
2. **Skenování,** představuje aktivní způsob zkoumání testovaných systémů, které většinou probíhá na síťové a transportní vrstvě. V této fázi je prováděn i celkový test dnes známých zranitelností pomocí vybraných automatizovaných nástrojů. Na základě informací získaných v této fázi bude možné určit další postup testování a případně bude konzultován s kontaktní osobou Zákazníka.
3. **Fáze průniku,** představuje poslední etapu testování. Představuje využití identifikovaných zranitelností a nevhodných konfigurací a jejich ověřování na testovaném systému. Eventuálně může po této následovat znovu od prvního bodu.
4. **Sestavění závěrečné zprávy**

3.4 Používané nástroje

Během testování používá ESET několik komerčních, jakož i open-source nástrojů. Tyto nástroje jsou uvedeny na webových stránkách http://www.owasp.org/index.php/Phoenix/Tools a http://tools.kali.org/tools-listing.

Použití konkrétních nástrojů závisí na testovacím prostředí a typu testů. Výsledky testů jsou následně ověřovány manuálně nebo prostřednictvím vlastních nástrojů ESET, které nelze blíže obecně specifikovat, protože jsou často vytvářeny v průběhu testování a jejich použití není univerzální.

3.5 Výstupy projektu

Výstupem projektu (Dílem) bude závěrečná zpráva v **českém jazyce**.

Zpráva z projektu **Bezpečnostní testování externí a interní infrastruktury dle zadání Zákazníka** bude obsahovat následující části:

- **Shrnutí (Executive/Management Summary)** - dokument shrnující rozsah, metodiku, nálezy a doporučení ve formě vhodné pro management.
- **Detailní technická zpráva** - dokument pro technický personál zákazníka, který rozebírá: detailněji technický popis zranitelností (námi identifikovaných nejzávažnějších zranitelností), ohodnocení závažnosti každé zranitelnosti, podpůrné detailní příklady k zranitelnostem neboli PoC (v případě potřeby) a technické návrhy postupu jejich odstranění. Součástí zprávy mohou být i výstupy z testujících nástrojů.

3.6 Ukončení projektu

Formálním ukončením poskytované Služby je oboustranné podepsání akceptačního protokolu pro předmět projektu, po předání výstupů poskytované Služby Zákazníkovi.

4) Harmonogram a místo výkonu testů

Testovací okno: Časové období, kdy bude probíhat testování, přičemž přesné **datum bude určeno po dohodě se Zákazníkem.**

Termín předání závěrečné zprávy (Díla): Závěrečná zpráva bude předána **do pěti pracovních dnů** od ukončení realizačních prací. Přesný termín bude upřesněn později. Zjištění se závažností „Kritická“ budou nahlášeny Odpovědné osobě Zákazníka po jejich ověření.

Místo a pracovní doba: Bezpečnostní testování externí a interní infrastruktury bude probíhat formou „offsite“ vzdáleně prostřednictvím internetu, během **Pracovních dní**, v běžné **Pracovní době** od **08:00** do **18:00**.

5) Požadavky na součinnost

Pro realizaci výše uvedených činností je požadována následující součinnost:

- Pro potřeby koordinace činnosti a poskytovaní odpovídajících informací musí být na straně zadavatele ustanovena kontaktní osoba, která bude za spolupráci se společností ESET odpovědná a která bude vybavena příslušnými pravomocemi. S kontaktní osobou budou upřesněny všechny detaily spojené s obsahem a způsobem realizace projektu.
- Pro účely bezpečnostních testů infrastruktury Zákazník poskytne:
    - IP adresu a doménové jméno testovaného serveru.
- Pro účely bezpečnostních testů webových aplikací Zákazník poskytne:
    - URL adresy pro testované webové aplikace,
    - dva různé účty (účty dvou různých knihoven) do aplikace pro importování uživatelských účtů,
    - volitelně uživatelský účet s nejvyššími oprávněními, pro případné prověření eskalaci oprávnění v rámci testovaných aplikací.

V případě nedodržení součinnosti bez předchozího upozornění může dojít k jednání o rozsahu a ceně testů.

6) Cena

Cena za projekt bezpečnostního testování webových aplikací Národní digitální knihovny České republiky.

Služba	Cena v Kč bez DPH
Bezpečnostní testování webových aplikací Národní digitální knihovny	[redacted]
CELKEM po slevě pro Národní knihovna České republiky	[redacted]

7) Závěr

Nedílnou součástí této Nabídky jsou Všeobecné podmínky poskytování služeb informační bezpečnosti společnosti ESET software, spol. s r.o. (dále jen „Podmínky“), které jsou zveřejněny na webové stránce [redacted] a Prohlášení o podmínkách pro penetrační testování společnosti ESET software, spol. s r.o. („Prohlášení Zákazníka“). Odesláním e-mailu Odpovědné osobě pro obchodní kontakt uvedené v článku 1.1. této Nabídky, kterým Zákazník potvrdí tuto Nabídku, Zákazník prohlašuje, že si Podmínky přečetl, v celém rozsahu porozuměl jejich významu, souhlasí s nimi a je oprávněn jednat za Zákazníka v rozsahu nezbytném pro akceptování této nabídky. Společnost ESET začne poskytovat Služby nejdříve dnem podpisu Prohlášení o podmínkách pro penetrační testování Zákazníkem a doručením tohoto dokumentu na e-mailovou adresu kontaktní osoby ESET uvedené v odstavci 1.1 této Nabídky.

V případě jakýchkoliv dotazů jsme připraveni Vám je zodpovědět.

Věřím, že naše nabídka splní Vaše očekávání a bude podkladem pro úspěšnou spolupráci.

S úctou,

[redacted]
Security Sales Representative
ESET software, spol. s r.o.