OBJEDNÁVKA ODBORNÝCH A KONZULTAČNÍCH SLUŽEB AD-HOC - CHYTRÁ KARANTÉNA 2.0

Objednatel	**Poskytovatel**
Česká republika - Ministerstvo zdravotnictví	Národní agentura pro komunikační a informační technologie, s.p.
se sídlem: Palackého náměstí 4, 128 01, Praha 2	se sídlem: Kodaňská 46, Vršovice, 101 00, Praha 10
IČO: 24341	IČO: 4767543
zastoupena: MUDr. Pavlou Svrčinovou, Ph.D., hlavní hygieničkou ČR s postavením vrchní ředitelky pro ochranu a podporu veřejného zdraví	zastoupena: [redacted]

Číslo Objednávky:	S1005-2020/013-2023
Vystavována na základě:	Smlouvy o poskytování softwarových, odborných a mobilních služeb - chytrá karanténa 2.0, č. 1005/20.
Objednávané plnění:	Realizace Zadání Odborných a konzultačních služeb ad-hoc č. 013-2023 viz příloha.
Požadovaný termín dodání:	31. 10. 2023
Předpokládaný rozsah plnění (v člověkodnech / v Kč bez DPH):	**max. počet MD: max. počet MD: 13** **max. částka v Kč bez DPH: 134 368,-**

Objednatel

V Praze dne __.__.____

MUDr. Pavla Svrčinová, Ph.D.

Digitálně podepsal MUDr. Pavla Svrčinová, Ph.D.
Datum: 2023.09.20 13:20:33 +02'00'

.....

Česká republika – Ministerstvo zdravotnictví

MUDr. Pavla Svrčinová, Ph.D.

hlavní hygienička ČR s postavením vrchní ředitelky pro ochranu a podporu veřejného zdraví

ZADÁNÍ
ODBORNÝCH A KONZULTAČNÍCH SLUŽEB AD-HOC
Č. 013-2023

Objednatel	**Poskytovatel**
Česká republika - Ministerstvo zdravotnictví	Národní agentura pro komunikační a informační technologie, s.p.
se sídlem: Palackého náměstí 4, 128 01, Praha 2	se sídlem: Kodaňská 46, Vršovice, 101 00, Praha 10
IČO: 24341	IČO: 4767543
zastoupena: MUDr. Pavlou Svrčinovou, Ph.D., hlavní hygieničkou ČR s postavením vrchní ředitelky pro ochranu a podporu veřejného zdraví	zastoupena: [redacted]

Číslo Objednávky:	S1005-2020/013-2023
Vystavována na základě:	Smlouvy o poskytování softwarových, odborných a mobilních služeb - chytrá karanténa 2.0, č. 1005/20.
Objednávané plnění:	Realizace Změnového požadavku POS_ChK2.0-272 na Zajištění bezpečnostních testů aplikace Tečka v září a říjnu 2023
Požadovaný termín dodání:	31. 10. 2023
Předpokládaný rozsah plnění (v člověkodnech / v Kč bez DPH):	**Celkem: max. počet MD: 13 / max. částka v Kč bez DPH: 134 368,-**

Požadováno vytvoření Specifikace:	NE, Specifikace je již přílohou tohoto Zadání: POS_ChK2.0-272 na Zajištění bezpečnostních testů aplikace Tečka v září a říjnu 2023

POS_ChK2.0-272_Bezpečnostni_testy_Te

Kontaktní osoba Objednatele pro projektové řízení Objednávky:	[redacted] Email: [redacted] Tel: [redacted]

Objednatel

V Praze dne __.__.____

MUDr. Pavla Svrčinová, Ph.D.

Digitálně podepsal MUDr. Pavla Svrčinová, Ph.D.
Datum: 2023.09.20 13:21:03 +02'00'

.....

Česká republika – Ministerstvo zdravotnictví

MUDr. Pavla Svrčinová, Ph.D.

hlavní hygienička ČR s postavením vrchní ředitelky pro ochranu a podporu veřejného zdraví

Souhlas Zhotovitele

V Praze dne __.__._____

[redacted]

Národní agentura pro komunikační a informační technologie, s. p.

[redacted]

Návrh požadavku na Odborné služby			
Registr/Aplikace	**CHK 2.0 Bezpečnostní testy - Tečka**	**Ze dne:**	1.9.2023
Název požadavku	Zajištění bezpečnostních testů aplikace Tečka v září a říjnu 2023		

Identifikátor	POS_ChK2.0-272_Bezpečnostní testy - Tečka
Datum	1.9.2023
Popis požadavku	V rámci měsíce září a října 2023 prosíme o Odborné služby Bezpečnostních testů aplikace Tečka.
Pracnost a analýza dopadů	# Navrhované testování zranitelností Na základě analýzy dosavadních poznatků o mobilní aplikaci Tečka jsme uvážlivě vypracovali návrh na provedení kyberbezpečnostních testování. Doporučujeme provést **testování zranitelnosti (Vulnerability Testing)**:

Testování zranitelnosti	**Vulnerability Testing**
Odpovídá na základní otázky: Jaké zranitelnosti existují v systému? Jak zranitelný je systém?	
Činnost testera: Tester identifikuje a vyhodnocuje potenciální zranitelnosti v systému. Navrhuje způsob minimalizace rizik spojených se zranitelnostmi.	
Poznámka: Z pohledu bezpečnostního testování na základě znalostní je tento test často označován za testování šedé skříňky (Grey Box). V případě navrhovaného testování doporučujeme inklinaci více k metodě tandem, kdy tester i cíl jsou na testování připraveni a předem znají všechny podrobné informace o testu; avšak není testována připravenost cíle na narušení; výhodou tandemového testu je důkladnost, protože tester má k dispozici dobrý přehled o systému; rozsah a hloubka se odvíjí nejen od samotného rozsahu informačního systému, ale závisí také na kvalitě informací poskytnutých testerovi před testováním (transparentnost) a na použitelných znalostech a dovednostech testera.	

Bylo zvažováno také penetrační testování, avšak takové testování předpokládá, a) že cíl není připraven nebo informován o testování, b) zároveň tester (útočník) nemá žádné předchozí informace o obraně, prostředcích, zdrojích a kanálech systému, c) je ověřována odolnost systému proti skutečným útokům (byť simulovaným). Z těchto předpokladů vyplývá nejen metodická neúplnost, ale také značná rizikovost penetračních testů. Avšak v souvislosti s testováním zranitelnosti **budeme nálezy uvažovat také v souvislosti s jejich využitím při potenciálním průniku** (pak z tohoto pohledu je možné takové testy interpretovat také jako penetrační). Pokud si klient bude přát vysloveně penetrační testování ve výše uvedeném smyslu, můžeme navrhnout doporučený design takového testování a nutná protiopatření pro snížení rizik takového testování.

Detailní design navrhovaného testování zranitelností může být podrobněji upřesněn v dalších informačních iteracích na základě této indikativní nabídky. Testování bude přizpůsobeno specifickým potřebám informačního systému a bude prováděno s důrazem na konkrétní požadavky a cíle klienta.

Specifikace prostředí

- Aplikace Tečka
- Mobilní platformy / OS (tzn. 2 samostatné aplikace):
  - Android
  - iOS
- Typy testovaných aplikací, resp. cílů:
  - ostrá (produkční) aplikace,
    - pro iOS dostupná přes App Store,
    - pro Android dostupná přes Google Play
  - testovací aplikace
- Testovaná rozhraní jsou provozována na těchto url:
  - portál pro vyzvednutí certifikátů – ocko.uzis.cz
  - testovací portál pro vyzvednutí – certifikátů ockotest.uzis.cz
- API pro poskytování dat pro Tečka:
  - ostrá (produkční) – https://dgcverify.mzcr.cz/index.html
  - Testovací – https://ockotest.uzis.cz/v4/index.html
- Na vnějším perimetru je provozován WAF, který balancuje provoz mezi několika servery, na nichž je provozován portál a API rozhraní. Všechny servery jsou virtuální na platformě HyperV s operačním systémem Windows DC. Serverů je více jak 5.
- Testovací rozraní je chráněno pomocí Whitelistu IP adres (z NAKIT by měl fungovat prostup), Ostré je chráněno systémovým certifikátem.

Rozsah a hloubka

Rozsah a hloubka testování budou:

- omezeny vyhrazenými časovými limity,
- definovány testováním aplikace pro Android a aplikace pro iOS,
- se zaměřením na ověření dle postupů kombinujících:
  - OWASP MASVS,
  - OWASP MASTG,
  - OWASP Top 10 Mobile Risks,
  - zkušenosti bezpečnostních expertů NAKIT, s. p.
- definovány vnějším perimetrem:
  - prostředí mobilního zařízení, tzn. mobilní zařízení samotné, na kterých aplikace běží, a to včetně možných bezpečnostních rizik spojených s těmito zařízeními,

- API: zohlednění aplikačních rozhraní (API) pro poskytování dat pro Tečka.

Prostředí bude používáno ostré (produkční) i testovací. Testovací prostředí bude použito pro testování, která lze považovat za rizikovější z pohledu dopadů na prostředí a uživatele – tzn. v tomto prostředí předpokládáme spíše aktivní typy testů. Oproti tomu ostré (produkční) testování bude použito pro méně rizikové testy – tzn. v tomto prostředí předpokládáme spíše pasivní typy testů.
Pasivní testy budou zahrnovat sledování a monitorování provozu aplikace v ostrém prostředí s minimalizací aktivního testování a odvozování zranitelností. To umožní alespoň získat reálná data o chování aplikace a identifikovat případné problémy a nedostatky.
Je důležité vyvážit potřeby testování s potenciálními riziky a dopady na ostré prostředí a uživatele. Zvolení správné kombinace testovacího a ostrého prostředí v závislosti na konkrétním testování zranitelnosti je klíčové pro dosažení optimálních výsledků a minimalizaci rizik.
Protože ostré (produkční) prostředí je vybaveno WAF, navrhujeme z důvodu zachování zabezpečení WAF nevypínat. Stav bez WAF bude ověřen v testovacím prostředí.

OWASP MASVS a MASTG

OWASP je nezisková nadace, jejímž cílem je umožnit organizacím vytvářet, vyvíjet, pořizovat, provozovat a udržovat aplikace, kterým lze bezpečnostně důvěřovat. Všechny OWASP projekty, nástroje, dokumenty, fóra atd. jsou zdarma a otevřené všem zájemcům o zlepšení bezpečnosti aplikací. Nabízí velmi rozsáhlé potřebné know-how pro oblast aplikační bezpečnosti, počítaje v to zejména webové a mobilní aplikace.
Pojmy:

- OWASP – Open Worldwide Application Security Project, dříve Open Web Application Security Project.
- MASVS – Mobile Application Security Verification Standard.
- MASTG – Mobile Application Security Testing Standard.

MASVS je průmyslový standard pro zabezpečení mobilních aplikací. Primárně se soustředí na využití architekty, vývojáři, bezpečnostními testery a analytiky mobilního softwaru, kteří se snaží vyvíjet bezpečné mobilní aplikace.

Zatímco MASVS především definuje model zabezpečení mobilních

aplikací a uvádí seznamy obecných požadavků na zabezpečení mobilních aplikací. MASTG mapuje stejnou základní sadu bezpečnostních požadavků, kterou nabízí MASVS, podrobněji se však zaměřuje na postupy bezpečnostního testování mobilních aplikací. V závislosti na kontextu mohou být použity samostatně nebo kombinovaně.

MASVS i MASTG se soustředí na následující oblasti:
MASVS-STORAGE: Bezpečné ukládání citlivých dat. Tato kategorie má vývojářům pomoci zajistit, aby veškerá citlivá data záměrně uložená aplikací byla řádně chráněna bez ohledu na cílové umístění. Zahrnuje také neúmyslné úniky, ke kterým může dojít v důsledku nesprávného používání rozhraní API nebo systémových funkcí. (data-at-rest)

- MASVS-CRYPTO: Kryptografické funkce používané k ochraně citlivých dat. Účelem kontrol v této kategorii je zajistit, aby ověřovaná aplikace používala kryptografii v souladu s osvědčenými postupy v oboru, které jsou obvykle definovány v externích standardech, jako jsou NIST.SP.800-175B a NIST.SP.800-57.
- MASVS-AUTH: Mechanismy ověřování a autorizace používané mobilní aplikací. Cílem kontrolních mechanismů v této kategorii je zajistit, aby aplikace bezpečně implementovala mechanismy ověřování a autorizace, chránila citlivé informace o uživateli a zabránila neoprávněnému přístupu. Je důležité poznamenat, že zabezpečení vzdáleného koncového bodu by mělo být rovněž ověřeno pomocí oborových standardů, jako je například standard OWASP Application Security Verification Standard (ASVS).
- MASVS-NETWORK: Zabezpečená síťová komunikace mezi mobilní aplikací a vzdálenými koncovými body. Tato kategorie má zajistit, aby mobilní aplikace nastavovala zabezpečená připojení za všech okolností. Konkrétně se zaměřuje na ověření, zda aplikace vytváří bezpečný šifrovaný kanál pro síťovou komunikaci. Kromě toho tato kategorie pokrývá situace, kdy se vývojář může rozhodnout důvěřovat pouze určitým certifikačním autoritám, což se běžně označuje jako připnutí certifikátu nebo připnutí veřejného klíče. (data-in-transit)
- MASVS-PLATFORM: Zabezpečená interakce se základní mobilní platformou a ostatními nainstalovanými aplikacemi. Tato kategorie zahrnuje ovládací prvky, které zajišťují, aby interakce aplikace s mobilní platformou probíhaly bezpečně. Tyto kontroly zahrnují bezpečné používání mechanismů IPC poskytovaných platformou,

konfigurace WebView, které zabraňují úniku citlivých údajů a odhalení funkcí, a bezpečné zobrazování citlivých údajů v uživatelském rozhraní aplikace. Zavedením těchto kontrolních mechanismů mohou vývojáři mobilních aplikací zabezpečit citlivé informace uživatelů a zabránit neoprávněnému přístupu útočníků.

- MASVS-CODE: Bezpečnostní osvědčené postupy pro zpracování dat a udržování aplikace v aktuálním stavu. Tato kategorie zahrnuje chyby kódování, které vznikají z externích zdrojů, jako jsou vstupní body dat aplikace, operační systém a softwarové komponenty třetích stran. Vývojáři by měli ověřovat a sanitizovat všechna příchozí data, aby zabránili útokům typu injection a obcházení bezpečnostních kontrol. Měli by také prosazovat aktualizace aplikace a zajistit, aby aplikace používala aktuální platformy, a chránit tak uživatele před známými zranitelnostmi.
- MASVS-RESILIENCE: Odolnost vůči pokusům o zpětné inženýrství a manipulaci. Cílem kontrol v této kategorii je zajistit, aby aplikace běžela na důvěryhodné platformě, zabránit manipulaci za běhu a zajistit integritu zamýšlené funkce aplikace.

OWASP Mobile Top 10 zahrnuje popis statisticky nejčastějších a zároveň zpravidla nejzávažnějších bezpečnostní zranitelností v mobilních aplikacích a uvádí osvědčené postupy, které pomáhají tyto bezpečnostní problémy napravit a minimalizovat.
V nejnovější verzi OWASP Mobile Top 10 2023 jsou uvažovány zranitelnosti:

- M1: Insecure Authentication/Authorization
- M2: Insecure Communication
- M3: Inadequate Supply Chain Security
- M4: Inadequate Privacy Controls
- M5: Improper Credential Usage
- M6: Insufficient Input/Output Validation
- M7: Security Misconfiguration
- M8: Insufficient Cryptography
- M9: Insecure Data Storage
- M10: Insufficient Binary Protections

Ve starší verzi Mobile Top 10 2016 a OWASP Top 10 2014 byly uvažovány:

- Mobile Top 10 2016
    - M1: Improper Platform Usage
    - M2: Insecure Data Storage
    - M3: Insecure Communication
    - M4: Insecure Authentication

- M5: Insufficient Cryptography
  - M6: Insecure Authorization
  - M7: Client Code Quality
  - M8: Code Tampering
  - M9: Reverse Engineering
  - M10: Extraneous Functionality
- OWASP Mobile Top 10 2014:
  - M1: Weak Server Side Controls
  - M2: Insecure Data Storage
  - M3: Insufficient Transport Layer Protection
  - M4: Unintended Data Leakage
  - M5: Poor Authorization and Authentication
  - M6: Broken Cryptography
  - M7: Client Side Injection
  - M8: Security Decisions Via Untrusted Inputs
  - M9: Improper Session Handling
  - M10: Lack of Binary Protections

Zkušenosti bezpečnostních expertů NAKIT se zaměří na neopomenutí důležitých aspektů testování zranitelnosti systému, počítaje v to především několik klíčových oblastí: odhalování zranitelností specifických pro mobilní zařízení, manipulace s uživatelskými daty (ověření, zda aplikace řádně chrání uživatelská data a zda je náchylná k manipulaci dat, jako jsou injektování SQL, cross-site scripting (XSS) podvržení identit apod.), specifické oblasti zabezpečení autentizace a autorizace, zabezpečení API (zohledníme také OWASP API Security Top 10 2023), zneužitelnost uživatelského rozhraní, zvážení útočných souvislostí atp.

Výstupy z kyberbezpečnostního testování jsou důležité pro poskytnutí komplexního obrazu o bezpečnostní situaci vašeho informačního systému. Zde je seznam potenciálních výstupů:

- Celková závěrečná zpráva:
  - Budou vyhotoveny 2 závěrečné zprávy (1 pro Android aplikaci a 1 pro iOS), případně také zpráva z retestování.
  - Obsahuje shrnutí provedených testů, výsledky a závěry.
  - Obsahuje celkový přehled o stavu kyberbezpečnosti systému.
  - Zhodnocuje zjištěná bezpečnostní rizika a zranitelnosti.
  - Identifikuje konkrétní zranitelnosti a slabiny systému.
  - Poskytuje doporučení a návrhy na opravy a zlepšení bezpečnosti.
  - Detailněji popisuje provedené testy a jejich výsledky.
- Prezentace výsledků klientovi:
  - Slouží k prezentaci klíčových zjištění a doporučení.
  - Shrnuje výsledky jednotlivých testů a zranitelností.
  - Vysvětluje význam a důsledky identifikovaných bezpečnostních rizik.
  - Nabízí prostor pro diskusi, odpovědi na otázky a vysvětlení

technických detailů.

Součinnost:

Pro úspěšné provedení testování zranitelnosti mobilní aplikace budeme potřebovat následující součinnost od klienta:

- Klient musí určit kontaktní osobu, která má adekvátní pravomoci, pro účely koordinace a zajištění odpovídajících informací. Tato osoba bude zodpovědná za spolupráci s NAKIT. S kontaktní osobou budou upřesněny všechny detaily spojené s obsahem a způsobem realizace. Během testování a po jeho dokončení může být potřeba komunikace s klientem, aby se vyjasnily některé technické detaily.
- Případné odborné informace budou zjišťovány formou konzultací s odbornými pracovníky na straně klienta, kteří jsou schopni komentovat jednotlivé technické detaily (např. konstrukce ve zdrojovém kódu, nastavení v konfiguraci prostředí atd.). Řešitelům NAKIT musí být též zpřístupněny informace a dokumenty, které během příprav testování i v samotném průběhu testování jsou či budou nezbytné.
- Poskytnutí mobilní aplikace: Klient musí poskytnout plnou verzi mobilní aplikace, kterou chce nechat otestovat. Je důležité, aby aplikace byla ve stavu, ve kterém se hodlá nasadit do ostrého prostředí. V tomto případě jsou uvažovány aplikace v rámci:
    - ostrého (produkčního) prostředí a
    - testovacího prostředí.
- Přístup k testovacím a ostrým prostředím: Klient by měl poskytnout přístup k testovacímu a ostrému prostředí.
    - Testovací prostředí by mělo být zajištěno tak, aby umožňovalo provádění rizikovějších testů. Tzn. lze očekávat zvýšenou zátěž vlivem použití skenovacích nástrojů, lze předpokládat snížení uživatelského komfortu testovacího prostředí vlivem zpomalení až (výjimečně) nedostupnosti či možnou změnu chování funkcionality a obsahu (taková rizika budeme minimalizovat).
    - Ostré prostředí by mělo být dostupné pro pasivní testy a monitorování provozu aplikace.
- Zajištění několika testovacích účtů běžných uživatelů s dohodnutým nastavením práv Předpokládáme nejméně 3 pro každé prostředí.
    - Pro testovací prostředí.
    - Pro ostré (produkční) prostředí.
- Informace o požadovaných časových limitech: Klient by měl definovat požadované časové limity pro testování zranitelnosti mobilní aplikace. Například pokud si přeje invazivnější testy provádět mimo provozní špičku v konkrétní časy.
- Detaily o mobilních zařízeních: Klient by měl poskytnout informace o mobilních zařízeních, pro která je aplikace určena. To nám umožní zohlednit možná bezpečnostní rizika spojená s těmito zařízeními při testování.
- Informace o aplikačních rozhraních (API): Klient by měl sdělit, zda aplikace využívá nějaká aplikační rozhraní pro poskytování dat. Tyto

<table>
<tr><td></td><td>
informace nám umožní zahrnout testování týkající se zabezpečení těchto API. Některé informace jsou uvedeny již v předchozích kapitolách – v případě tohoto bodu tedy pouze případné dodatečné informace.
• Spolupráce při retestech: Pokud budou identifikovány zranitelnosti nebo nedostatky během testování, bude klientovi požádáno o provedení oprav a zlepšení bezpečnosti. Následně budou provedeny retesty, abychom ověřili, zda byly provedené úpravy úspěšné a zranitelnosti byly opraveny.
• Předpokládáme, že bude zajištěna:
  o neměnnost testovaného prostředí po dobu testů a
  o exkluzivita testovaného prostředí (především vyhnutí se kolizi s jinými testy, například zátěžovými).

<table>
<tr><th>Role</th><th>Počet MD</th></tr>
<tr><td>Bezpečnostní manažer</td><td>13</td></tr>
</table>

Realizace požadavku ovlivní:
<table>
<tr><th>Oblast</th><th>Dopady (ANO / NE)</th></tr>
<tr><td>Analytické dokumenty a podklady</td><td>NE</td></tr>
<tr><td>Provozní dokumentace</td><td>ANO</td></tr>
<tr><td>Bezpečnostní dokumentace</td><td>NE</td></tr>
<tr><td>Zdrojové kódy</td><td>NE</td></tr>
<tr><td>Vlastnické, užívací právo a standardní software</td><td>NE</td></tr>
</table>

Celkem (max. počet MD): 13
Celkem (max. částka v Kč bez DPH): 134 368,- Kč
</td></tr>
<tr><td>Požadavky na součinnost Objednatele</td><td>Budou projednávány na jednání projektu a zaznamenávány v nástroji Daktela a Archirepo.</td></tr>
<tr><td>Priorita</td><td>Vysoká</td></tr>
<tr><td>Způsob platby</td><td>Platba ad-hoc na základě smlouvy MZČR, o poskytování softwarových, odborných a mobilních služeb – Chytrá karanténa 2.0, ze dne 31.7.2020.</td></tr>
</table>