Technická specifikace soutěžených služeb

Předmět plnění

Předmětem zakázky je poskytnutí služby penetračních testů a bezpečnostního auditu IS pro prezentaci výsledků voleb a dalších aplikací pro Český statistický úřad.

Cílem je ověřit reálný stav zabezpečení pomocí vhodných testů, realizovaných na základě široce používaných standardů v této oblasti. Účelem je zejména ověření bezpečnosti použitých webových aplikací a komunikačních rozhraní, klíčových prvků celého řešení a posouzení celkové míry ochrany před neautorizovanými vstupy. Kromě odhalení případných bezpečnostních slabin budou vždy navržena účinná opatření k jejich eliminaci nebo snížení dopadu, včetně stanovení priorit při jejich realizaci.

Všechny testy musí proběhnout v termínu 3-7 týdnů před konáním voleb. Konkrétní harmonogram jednotlivých testů bude vždy domlouván pro konkrétní plnění tak, aby byl koordinován s dalšími činnostmi v rámci přípravy voleb (zátěžové testy, aplikační testy, plošné zkoušky)

Základní vektory a způsoby testů

V rámci zakázky předpokládáme ověření bezpečnosti dále uvedenými způsoby především v těchto oblastech:

Bezpečnostní testy IS pro volby:

- Externí penetrační testy a testy webové aplikace vnějšího webového rozhraní www.volby.cz a www.volbyhned.cz - včetně analýzy klíčových částí kódu aplikace.
- Analýza zabezpečení komunikační infrastruktury pro přebírací místa
- Ověření bezpečnostních nastavení koncových PC (přebírací místo).

Aplikační testy (vždy pro první volby v daném roce 2014, 2016 a 2018) pro 2 vybrané aplikace, které Objednatel specifikuje v rámci každé volební události.

Příklad rozsahu testů pro rok 2014:

- www.czso.cz - vlastní portál ČSÚ
- vdb.czso.cz - veřejná databáze

Dodavatel se zavazuje, že provede veškeré činnosti maximálně zodpovědně a provede v daném čase maximální šíři bezpečnostních testů a činností, které by měly přispět k potvrzení bezpečnosti a důvěryhodnosti služeb ČSÚ, které jsou provozovány v rámci prezentačních systémů ČSÚ.

Požadované metodiky provádění auditu a testů

Při provádění testů musí být dodržena následující pravidla:

- včasné hlášení a upozorňování na problémy
- jasné a konzistentní závěrečné zprávy
- testy musí být metodické a opakovatelné
- testy prováděné na produkčních prostředích (např. www.czso.cz), kde se očekává omezení funkce systémů (např. úplná i částečná nedostupnost, pády serverů), musí být realizovány mimo běžnou provozní dobu
- při testování webových aplikací zadavatel požaduje provedení testů v souladu s metodikou OWASP, přičemž výsledky budou prezentovány metrikou TOP TEN 2010 nebo novější
- průběžné hlášení závažných a kritických nedostatků (dříve než v závěrečné zprávě)
- provedení retestů po odstranění nalezených nedostatků
- jednorázové otestování útoku DDOS

Minimální rozsah a struktura nabízených služeb

Penetrační testy IS pro volby a vybraných webových aplikací

Aplikace www.volby.cz resp. www.volbyhned.cz představují základní rozhraní, které může využívat široká veřejnost, resp. zástupci médií k získání aktuálních nebo historických výsledků probíhajících nebo realizovaných voleb. Pro volby.cz se jedná o třívrstvou architekturu, kdy na základě dotazu jsou generovány HTML stránky, které jsou zobrazeny uživatelům. U volbyhned.cz je jedná o externě hostovanou prezentaci základních výsledků ve formě statických HTML stránek.

Webová prezentace ČSÚ je primárně umístěna na www.czso.cz a jsou do ní integrovány další veřejné databáze a dynamické aplikace.

Veřejná databáze (VDB) slouží jako základní a jednotný datový zdroj pro prezentaci statistických údajů určených pro veřejnost**.**

Zadavatel požaduje provedení následujících typů bezpečnostních testů:

- penetrační testy aplikací
- skenování známých zranitelností
- analýzu klíčových částí zdrojového kódu aplikací (v současnosti Oracle PL/SQL procedury, v budoucnosti s případnou možností změny technologie)

Analýza zabezpečení komunikační infrastruktury pro přebírací místa

Analýza bude zaměřena na bezpečnost koncových zařízení na straně přebíracího místa a bezpečnost komunikace s centrálním systémem i mezi jednotlivými koncovými zařízeními na jednom místě (více notebooků připojených do jednoho ADSL routeru). U koncových stanic zadavatel požaduje ověřit soulad s nejlepšími bezpečnostními praktikami v této oblasti.

Součinnost ze strany ČSÚ

Pro potřeby koordinace činnosti a poskytování odpovídajících informací bude na straně Českého statistického úřadu ustanovena kontaktní osoba, která bude za spolupráci s dodavatelem odpovědná a která bude vybavena příslušnými pravomocemi. S kontaktní osobou budou upřesněny všechny detaily spojené s obsahem a způsobem realizace projektu. Tato osoba bude zajišťovat konzultace a zpřístupnění informací a dokumentů, které jsou pro provedení penetračních testů nezbytné.

Pro provedení části testů bude možné využívat zařízení potřebné pro připojení (ADSL modem / router) a 1 plně nakonfigurovaný počítač, který bude ve stavu, kdy by měl být předán na PM. Dále bude k dispozici dokumentace, která specifikuje požadavky bezpečnostní politiky na PM (např. požadavky na fyzické zabezpečení počítačů atd.). Pro potřeby testů bude k dispozici také databázové schéma, nad kterým je postavena aplikace www.volby.cz a také relevantní části zdrojových kódů této aplikace.

Ing. Kateřina Škarková

Digitálně podepsal Ing. Kateřina Škarková
DN: c=CZ, o=ČR - Český statistický úřad [IČ 00025593], ou=Český statistický úřad - Ústředí - Odbor veřejných zakázek a právních služeb, ou=8233, cn=Ing. Kateřina Škarková, serialNumber=P3061, title=ředitelka
Datum: 2013.09.25 10:20:23 +02'00'