

Technická specifikace soutěžených služeb

Předmět plnění

Předmětem zakázky je poskytnutí služby penetračních testů a bezpečnostního auditu IS pro prezentaci výsledků voleb do krajských zastupitelstev a Senátu 2012 a prezidentských voleb 2013 (dále jen IS volby.cz) 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.

Základní vektory a způsoby testů

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

Bezpečnostní testy IS pro volby (pro volby 2012 a 2013):

- 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 vybraných webových aplikací (pro volby 2012):

- <http://www.czso.cz> - vlastní portál ČSÚ
- <http://vdb.czso.cz> - veřejná databáze

Dodavatel se zavazuje, že provede veškeré činnosti maximálně zodpovědně a provede v daném čase maximum 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
- destruktivní testy prováděné na produkčních prostředích (www.czso.cz) 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

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. Jedná se o třívrstvou architekturu, kdy na základě dotazu jsou generovány HTML stránky, které jsou zobrazeny uživatelům.

Webová prezentace ČSÚ je primárně umístěna na www.czso.cz a jsou do ní integrovány další veřejné databáze a 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 (PLSQL procedury)

Analýza zabezpečení komunikační infrastruktury pro přebírací místa

Analýza bude zaměřena na bezpečnost koncových zařízení na straně přebíracího místa a bezpečnost komunikace s centrálním systémem. 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.