**Specifikace požadovaných služeb**

Český statistický úřad (dále jen ČSÚ nebo dodavatel) má ve správě informační systém Registr osob (dále jenROS), který dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen Zákon) splňuje kritéria pro informační systémy kritické informační infrastruktury (KII) a dále informační systém IAIS ROS,který dle Zákona splňuje kritéria pro významné informační systémy (VIS). ČSÚ je povinen zajistit pravidelný audit ROS a IAIS ROS externí organizací, která se nepodílí na provozu a vývoji těchto systémů**.**

Objednatel požaduje:

1. provedení auditu se zaměřením na plnění organizačních opatření kybernetické bezpečnosti s cílem zjistit kompatibilitu objednatele se Zákonem a vyhláškou č.316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (dále jen Vyhláška) a dále se zaměřením na bezpečnostní dokumentaci zpracovanou pro ROS a IAIS ROS.
2. provedení auditu skutečného technického bezpečnostního nastavení u vybraných serverů ROS a IAIS ROS dle konfiguračních příruček.

**Předmět plnění**

V rámci dodávky služeb se požaduje posoudit stav při plnění organizačních opatření, systému řízení bezpečnosti informací (ISMS), řízení rizik, plnění požadavků bezpečnostní politiky, organizační bezpečnosti, bezpečnostních požadavků pro dodavatele, při řízení aktiv, opatření bezpečnosti lidských zdrojů, při řízení provozu a komunikací, řízení přístupu a bezpečného chování uživatelů, při řízení akvizic, vývoje a údržby, při zvládání kybernetických bezpečnostních událostí a incidentů, řízení kontinuity činností, provádění kontrol a auditů.

Dále se požaduje posoudit způsob zajištění fyzické bezpečnosti, používání nástroje pro ochranu integrity komunikačních sítí, nástroje pro ověřování identity uživatelů, nástroje pro řízení přístupových oprávnění, nástroje pro ochranu před škodlivým kódem, nástroje pro zaznamenávání činností vybraných IS (včetně uživatelů a správců), nástroje pro detekci kybernetických bezpečnostních událostí, nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí, způsob implementace aplikační bezpečnosti a kryptografických prostředků a také posoudit způsob používání nástrojů pro zajištění vysoké úrovně dostupnosti.

Při posuzování bezpečnostní dokumentace ROS a IAIS ROS se požaduje zaměřit audit na :

* strukturu bezpečnostní dokumentace a existenci vazeb na jednotlivé § Vyhlášky;
* popis řešení kybernetického bezpečnostního incidentu (evidence podle typů, kategorizace, forma a náležitosti hlášení), včetně způsobu řešení protiopatření;
* zpracování plánu činnosti manažera kybernetické bezpečnosti (KB) a plánu provádění auditů KB;
* stanovení typů aktiv, způsob hodnocení a úrovně aktiv, hodnocení rizik, plnění minimálních požadavků na kryptografické algoritmy;
* skutečnou odbornou kvalifikaci osob (kvalifikace manažera KB a architekta KB, kvalifikace interního auditora k provedení interního auditu kybernetické bezpečnosti).

Při auditu skutečného technického bezpečnostního nastavení u vybraných serverů ROS a IAIS ROS dle konfiguračních příruček se požaduje porovnat skutečný stav nastavení u 7 vybraných serverů ROS a IAIS ROS s pokyny v konfiguračních příručkách (z každého typu bude vybrán vždy 1 server). Zadavatel zajistí přístup testerů dodavatele k posledním verzím konfiguračních příruček, které jsou zpracovány dle těchto zdrojů (7 příruček):

* APPLICATION SERVICES SECURITY TECHNICAL IMPLEMENTATION GUIDE

(Version 1, Release 1 17 January 2006);

* Security Configuration Benchmark For Apache HTTP Server 2.2 (Version 3.0.0

May 18th, 2010);

* Security Configuration Benchmark For Cisco Firewall Devices (Version 3.0.0

September 27, 2011);

* Security Configuration Benchmark For Cisco IOS ( Version 3.0.0 September 21, 2011);
* Security Configuration Benchmark For HP-UX 11i (Version 1.5.0 September 17, 2009);
* Security Configuration Benchmark For Red Hat Enterprise Linux 5 (Version 1.1.2 June 2009);
* DISA Oracle Database Security Checklist (Version 8, Release 1.5).

Požadovaný výstup je závěrečná zpráva z auditu, včetně návrhu úprav dokumentace a návrhu konkrétních opatření na nápravu. Požaduje se zpracovat závěrečnou zprávu v listinné a elektronické podobě.