

Fujitsu Technology Solutions s.r.o.

Martin Černý
V Parku 2336/22
148 00 Praha 4
Česká republika

Ministerstvo práce a sociálních věcí

Milan Hojer, MBA
Na Poříčnickém právu 1/376
128 00 Praha 2
Česká republika

Věc: Prohlášení o bezpečnosti dat v Integrovaných platformě

Požadavky na bezpečnost dat vycházejí z požadavků a standardů resortu MPSV. Celý návrh řešení a zabezpečení Integrovaných platformy byl připraven na základě těchto požadavků.

Služba je poskytována ze dvou datových center, která jsou umístěna v Praze, konkrétně ve Státní tiskárně cenin, s.p. a ČD Telematika, a.s. V rámci uvedených datových center **jsou umístěna data a provozovány systémy také pro jiné státní organizace** (např. Integrovaný informační systém Státní pokladny provozovaný Ministerstvem financí), nicméně vzhledem k tomu, že poskytovatel dodává službu resortu na platformě určené **výhradně pro resort MPSV**, nedochází ke sdílení výpočetního výkonu a datových úložišť s jinými organizacemi.

Datové centra odpovídají požadavkům zabezpečení dle mezinárodního standardu kategorie Tier III (provoz 24x7, dostupnost 99,982 %, redundance prvků N + 1). V obou datových centrech jsou nadstandardní bezpečnostní opatření, včetně fyzické nonstop ochrany, monitorování objektů a řízeným přístupem do objektů a do počítačových sálů. Počítačové sály jsou vybaveny protipožárními hlásiči, samozhášecími systémy. Datová konektivita a napájení datových center elektrickou energií je zálohované pro případ výpadků. Služby datových center jsou poskytovány v souladu se systémy řízení bezpečnosti informací, tzn. že jsou mj. pravidelně auditované. Systémy jsou navrženy a dimenzovány tak, že v případě výpadku nebo zničení jednoho z datových center, automaticky jsou poskytovány služby z druhého datového centra. Obě centra jsou umístěna mimo záplavové zóny.

„Naplnění jednotlivých bezpečnostních opatření vychází z provedené analýzy rizik a expertního hodnocení posuzovaného systému a je v souladu s doporučeními obsaženými v příslušných normách ČSN ISO/IEC 27001 a ČSN ISO/IEC 27002 pro oblast systémů řízení bezpečnosti a informační bezpečnost“. Bezpečnostní opatření byla v průběhu zpracování bezpečnostního projektu navržena tak, aby odpovídajícím způsobem zohledňovala připravované fyzické prostředí, navrhovanou architekturu systému a provozní režim systému a služby.

Architektura a implementační postupy pro nasazení systémové infrastruktury Integrovaných platformy resortu MPSV odpovídají všem doporučením pro zabezpečení komunikace a uložení dat, které pro použité technologie doporučuje společnost Microsoft jako výrobce systémového a aplikačního software, společnost Cisco jako výrobce síťové platformy i společnost Fujitsu jako dodavatel technologií pro ukládání a zálohování dat.

Veškerá komunikace se systémy a aplikacemi provozovanými v datových centrech Integrovaných platformy je šifrována anebo možnost ochrany dat šifrováním nabízí. Jedná se jak o komunikaci uživatelů s aplikačními servery, tak i o komunikaci systémů Integrovaných platformy s jinými systémy provozovanými v rámci resortu MPSV (a do budoucna i mimo resort).

Aplikace a systémy jsou jak dostupné z vnitřní sítě WAN MPSV, tak z Internetu. V obou případech jsou přístupy chráněny pomocí firewallových soustav, které v případě přístupu z Internetu navíc kombinují ochranu na úrovni sítě i na úrovni softwarové platformy.

Data jsou uložena na úložišti s garantovanou spolehlivostí dat a odolností proti výpadku dílčích komponent úložiště (disk, diskový řadič, konektivita apod.). Systémy, aplikace a zejména jejich data jsou pravidelně zálohována, přičemž zálohy jsou umístěny v jiném datovém centru, než je zálohovaný systém. Zálohy jsou také předávány MPSV na médiích pro účely archivace.

Systémy i aplikace mají nastaveny odpovídající oprávnění, která umožní uživatelům práci se systémy přesně dle požadavků resortu MPSV. Stejně tak správci jednotlivých vrstev systému mají oprávnění, která odpovídají jejich roli. Platí současně to, že přístup k systémům není kombinován s přístupem do aplikací. Tím je zajištěno, aby nebyla v rukou jednoho správce koncentrována příliš vysoká oprávnění umožňující jejich být jen potenciální zneužití. Požadavky na administrační úkony jsou autorizovány MPSV přes HelpDesk, jsou logovány a následně evidovány v provozním deníku, aby bylo možné snadno zjistit, který správce kdy a jak prováděl zásah.

Rozdělení rolí v provozu i během nasazování nových verzí aplikací přes více prostředí zabezpečuje, že **dodavatelé agendových aplikací nemohou mít přístup k produkčním datům.**

V Praze dne 3.2.2012
Fujitsu Technology Solutions s.r.o.
Martin Černý
vedoucí projektu