Audit informačnej bezpečnosti

„Audit detailne zhodnotil úroveň bezpečnosti v našej organizácií, posúdil mieru súladu s legislatívnymi požiadavkami a dobrou praxou v oblasti informačnej bezpečnosti a pripravil podklady pre ďalšie zlepšovanie stavu informačnej bezpečnosti. Výsledky auditu nám výrazne pomohli pri definovaní bezpečnostných požiadaviek pre informačné systémy a procesy v projekte zjednocovania daňovej a colnej správy."

RNDr. Michal Kubán, Manažér bezpečnosti, Daňové riaditeľstvo Slovenskej republiky

Daňové riaditeľstvo Slovenskej republiky

ZÁKAZNÍK

Daňové riaditeľstvo Slovenskej republiky (DRSR) je rozpočtovou organizáciou zriadenou Ministerstvom financií SR, ktoré prevádzkuje a riadi viac ako 100 daňových úradov na celom Slovensku. Hlavným poslaním daňovej správy SR je efektívny výber a správa daní, ako aj ochrana ekonomických záujmov štátu. Daňová správa SR plní úlohy stanovené štátnym rozpočtom a zároveň odzrkadľuje strednodobé ciele hospodárskej politiky Slovenskej republiky a Európskej únie.

VÝZVA

Vykonanie auditu informačnej bezpečnosti a preverenie súladu organizácie s:

- vnútornými predpismi (bezpečnostné politiky a smernice),
- zákonom č. 276/2006 Z.z. o informačných systémoch verejnej správy v znení neskorších predpisov a výnosom MFSR č. 312/2010 Z.z. o štandardoch pre informačné systémy verejnej správy,
- zákonom na ochranu osobných údajov č. 428/2002 Z.z.,
- požiadavkami normy ISO/IEC 27002:2005

a vyhodnotenie rizík vyplývajúcich zo zistených nedostatkov a spracovanie odporúčaní vo forme nápravných opatrení.

RIEŠENIE

Komplexnosť zadania si vyžadovala dobrú znalosť legislatívneho prostredia, bezpečnostných štandardov ISO, dobrých praktík v oblasti riadenia informačnej bezpečnosti a prevádzky informačných systémov a praktické skúsenosti pri vykonávaní technických bezpečnostných testov informačných systémov. Auditný tím pozostával z vedúceho audítora zodpovedného za organizáciu a kvalitu jednotlivých činností vykonávaných v rámci auditu, špecialistu na prevádzku informačných systémov verejnej správy, špecialistu na ochranu osobných údajov, špecialistu na bezpečnostné štandardy ISO a IT špecialistu, ktorý vykonával technické testy. Audit bol rozdelený na nasledovné fázy:

- Príprava auditu (oboznámenie sa s dokumentáciou, upravenie metodiky podľa potrieb zákazníka a zostavenie plánu auditu),
- Praktický výkon auditu (stretnutia, technické testy, fyzické obhliadky),
- Spracovanie výstupov (analýza, vyhodnotenie, vytvorenie výstupnej správy),
- Prezentácia výsledkov.

V rámci auditu bolo preštudovaných viac ako 1000 strán dokumentácie, realizovalo sa 50 stretnutí so zamestnancami, testovalo sa 60 systémov a aplikácií a 6 pracovných staníc. Celková dĺžka auditu, od podpisu zmluvy až po odovzdanie výstupov, trvala 6 mesiacov. Čistý čas odpracovaný na audite bol 32 človekodní.

Informačná bezpečnosť bola rozdelená do 11 oblastí, pričom plnenie jednotlivých požiadaviek normy, zákona alebo vnútorných predpisov sa posudzovali zvlášť. Zároveň sa vyhodnocovala celková vyspelosť prístupu k informačnej bezpečnosti v jednotlivých oblastiach v 5 stupňovej škále.

Výsledky auditu pomohli odstrániť viaceré nedostatky v informačnej bezpečnosti a prispeli k zvýšeniu celkovej úrovne zabezpečenia systémov a služieb, ktoré DRSR spravuje.