Všeobecné usmernenie TÚ SR k auditom informačnej bezpečnosti

V súvislosti s povinnosťou telekomunikačných podnikov preverovať stav informačnej bezpečnosti prostredníctvom nezávislých auditov vydáva TU SR nasledovné všeobecné usmernenie.

1) Požiadavky na audítorov

Kompetencia (odborná spôsobilosť)

Audítor musí byť odborne spôsobilý, dôkazom čoho sú medzinárodne akceptované certifikáty:

- v prvom rade ide o audítorské certifikáty ako **Certified Information Security Auditor**, CISA (ISACA), **Certified ISO/IEC 27001 Lead Auditor**, alebo
- certifikáty informačnej bezpečnosti, akými sú **CISSP** (ISC2), **SSCP** (ISC2), CISM (ISACA), **Information Security Professional** (GIAC), alebo ich možné ekvivalenty, alebo v prípade čiastkových, technicky orientovaných auditov
- certifikáty preukazujúce príslušné špecializované znalosti, ako sú certifikáty od Global Information Assurance Certification (**GIAC Systems and Network Auditor, GIAC Web Application Penetration Teste**r), od EC Council (**Certified Security Analyst, Certified Ethical Hacker, Licensed Penetration Tester**) alebo ich možné ekvivalenty.

Audítor musí mať viacročné skúsenosti v danej oblasti informačných a telekomunikačných systémov, čo sa preukazuje autorizovanými referenciami.

Nezávislosť

Auditor musí byť nezávislý od auditovaného subjektu do takej miery, že pri auditoch nesmie dochádzať ku konfliktu záujmov. Vo všeobecnosti sa za takýto konflikt záujmov považuje situácia, kedy sa audítor spolupodieľal na zavádzaní opatrení v oblasti fyzickej, logickej alebo procesnej bezpečnosti u auditovaného subjektu, a to buď konzultačne alebo predajom riešení alebo produktov, ktoré informačnú bezpečnosť u auditovaného subjektu riešia alebo ovplyvňujú.

Znamená to, že pri splnení hore uvedených podmienok je za nezávislý audit možné považovať aj audit, ktorý vykonal samostatný, organizačne oddelený útvar, oddelenie alebo inštitúcia auditovaného subjektu, s pôsobením na Slovensku alebo v zahraničí (materská spoločnosť). A naopak, za nezávislý audit sa automaticky nepovažuje audit vykonaný externou, treťou stranou, ktorá však nespĺňa podmienku konfliktu záujmov, napríklad tým, že má alebo v minulosti mala vplyv na výber produktov, riešení a bezpečnostných opatrení u auditovaného subjektu.

Akreditované audítorské spoločnosti

Dlhodobou snahou TÚ SR je dosiahnuť, aby všetky audity informačnej bezpečnosti pre účely Opatrenia č.O-30/2012 boli vykonávané iba tretími stranami, ktoré sú akreditované nezávislými odbornými organizáciami, pretože by mali byť najlepšou zárukou tak odbornej spôsobilosti ako aj nezávislosti audítorov. Pri pochybnostiach o skutočnej nezávislosti a obsahovej správnosti vykonaného auditu môže TÚ SR vyžadovať od telekomunikačnej spoločnosti doplnenie správy o audite v zmysle konkrétnych pokynov.

2) Všeobecné odporúčania

Vzhľadom na možnú obsiahlosť a zložitosť telekomunikačných produktov a služieb sa odporúča vopred zvažovať rozsah auditu, napríklad ako podrobne sa má posudzovať ktorá časť služby. Snaha auditovať všetko a naraz vedie k povrchným záverom, naopak snaha detailne posúdiť iba malú časť môže mať za následok plytvanie časom a zdrojmi.

Posúdenie rizík

Základným vstupom pre (akýkoľvek) **plán auditu** by malo byť aspoň všeobecné, vysoko-úrovňové posúdenie rizík a súčasného stavu opatrení voči týmto rizikám.

Audit informačnej bezpečnosti sa má zameriavať na v prvom rade na oblasti s najväčšími identifikovanými rizikami pre dostupnosť, integritu a dôvernosť telekomunikačným produktov a služieb (teda v poradí dôležitosti - 1. dostupnosť, 2. integrita a 3. dôvernosť).

Periodicita auditov

Audit overujúci zhodu s bezpečnostnými požiadavkami vo všetkých oblastiach (oblasti 1 až 5 Metodických pokynov) sa má vykonať **raz za rok**.

V prípade rozsiahlych telekomunikačných systémov je možné vykonať čiastkové audity kľúčových komponentov **raz za dva roky** (oblasť 3. Metodických pokynov, bezpečnosť systémov a zariadení), a to základe určenia priorít vyplývajúceho z posúdenia rizík.

3) Plán auditu a správa o audite (odporúčaná forma a obsah)

Správa o audite musí byť v slovenskom, českom alebo anglickom jazyku a musí obsahovať minimálne nasledovné časti – Plán auditu, Konečné zistenia, Prehlásenie auditovaného subjektu.

Plán auditu

Plán auditu má obsahovať cieľ, predmet, rozsah a spôsob vykonania.

Cieľ auditu

Cieľom auditu je overovanie zhody s požiadavkami na bezpečnosť a integritu verejných sietí a služieb podľa Opatrenia Telekomunikačného úradu Slovenskej republiky z 18. mája 2012, č. O-30/2012.

Predmet

Ktoré služby, produkty alebo ich časti boli auditované (napr. mobilný hlas/dáta, fixný hlas/dáta, VoIP, ISP, iné služby), a ak to nie zrejmé, vzhľadom na komplexnom predmetu auditu, aj vyhradenie tých častí alebo komponentov, ktoré auditované neboli.

Rozsah

Na ktoré oblasti z Metodických pokynov o ďalších podrobnostiach a detailoch k spracovaniu minimálnych bezpečnostných opatrení, (1-5), sa audit zameriava.

Je možné a vhodné uvádzať aj krížové referencie na požiadavky iných všeobecne známych štandardov alebo odporúčaní, napr. ISO/IEC 27001-2, COBIT, PCI DSS, a to najmä v prípadoch, kedy telekomunikačná spoločnosť už takéto audity štandardne vykonáva (napr. ENISA SD1.1 je to isté ako ISO 27002 Ch5.1.1).

Tak bude možné využiť výsledky jedného auditu, napr. pre účely ISO 27001, aj pre účely TÚ SR.

Spôsob vykonania auditu

- interview, pozorovanie, revízia dokumentácie, walk-through testy (praktické overenie účinnosti opatrení ich vykonaním), použitie špecializovaného auditovacieho softwaru,
- použité vzorkovacie metódy (štatisticky reprezentatívny výber populácie).

Konečné zistenia

V tejto časti majú byť uvedené všetky konečné, teda auditovanou stranou akceptované zistenia, (zistenie = konštatovanie nesúladu s požadovaným, odborne zaužívané "finding"):

- sumárny prehľad preskúmaných oblastí podľa uvedeného rozsahu vyššie a počet zistení na každú skúmanú oblasť
- stručný opis všetkých zistení o nesúlade s požadovanými opatreniami musí mať sumarizačnú podobu, teda nemá obsahovať dôkazné [1]podklady ani v správe ani v jej prílohách ([1] logy, printscreeny, ukážky prístupových práv alebo konkrétnych dokumentov),

- nesúlad musí byť uvedený v troch úrovniach (od najvyššej po najnižšiu, teda vážnejšie veci skôr): 3. systémová nezhoda, 2. nezhoda, 1. odporúčanie,
- každé zistenie musí uvádzať návrh možností a termínu jeho vyriešenia.

Prehlásenie auditovaného subjektu

Správa o audite musí obsahovať také prehlásenie auditovaného subjektu, z ktorého je zrejmé, že jeho zodpovední predstavitelia schválili príslušné kroky na nápravu a nesú zodpovednosť za konečný stav.