STN ISO/IEC 27001 a jej implementácia v praxi

Ing. Ladislav Martinček

Mobil: +421 905 974 859 | E-mail: ladislav.martincek@lynx.sk

O SPOLOČNOSTI

LYNX®

Ponúkame špičkové služby v oblasti projektovania, výstavby, prevádzkovania a bezpečnosti informačných systémov, networkingu, komplexnej bezpečnosti organizácií a špeciálnych aplikácií.

LYNX®

je postavený na troch pilieroch

dôvera

profesionalita

talent

O SPOLOČNOSTI

- Pôsobenie na trhu od roku 1991
- 100 zamestnancov, sídla spoločnosti v Bratislave a v Košiciach
- Certifikát na úrovni NATO Secret
- Certifikát priemyselnej bezpečnosti od NBÚ
- Certifikácia spoločnosti podľa noriem:

  ISO 9001

  ISO 14001

  ISO/IEC 27001

  ISO/IEC 20000-1

  ISO 45001

  ISO 10006

  ISO 22301

KYBERNETICKÁ BEZPEČNOSŤ

- Bezpečnosť webových sídiel a služieb
- Budovanie SOC (Security Operation Center)
- Budovanie firemných IT dátových centier
- Budovanie infraštruktúr pre spracovanie citlivých informácií
- Analýzy a audity
- Implementácia produktov informačnej bezpečnosti

Viac informácií na www.lynx.sk

OBLASŤ KOMPLEXNEJ BEZPEČNOSTI

- Dokumenty bezpečnostnej politiky
- Analýzy, posúdenia a audity
- Bezpečnostné projekty
- Konzultácie
- Školenia v rámci realizácie projektu

Viac informácií na www.lynx.sk

História riadenia informačnej bezpečnosti

Bezpečnostné normy Aby bolo možné ohodnotiť bezpečnosť vzniknutého produktu či systému, je potrebné nezávislé odborné posúdenie riadiace sa všeobecne akceptovanými kritériami. Tieto sú spravidla zhrnuté v uznávaných normách a štandardoch.

Ich úlohou je predovšetkým:

- ponúknuť užívateľom metriky, na základe ktorých môžu sami zhodnotiť úroveň danej bezpečnosti
- ponúknuť výrobcom a návrhárom smernice pre zabudovanie bezpečnostných prvkov do ich produktov
- ponúknuť základ pre špecifikovanie bezpečnostných potrieb

Ďalej:

- zavádzajú jednotnú kultúru a stanovujú zrovnateľné kritériá
- uľahčujú audit, kontroly, jednanie s partnermi

História riadenia informačnej bezpečnosti

Prvým pokusom o stanovenie takýchto kritérií boli Trusted Computer Security Evaluation Criteria, známe tiež ako Oranžová kniha Ministerstva obrany USA.

Kritériá sú rozdelené do sekcií a v rámci nich do jednotlivých tried. Tieto kritéria sa stali základom aj pre niektoré ďalšie v súčasnosti rozšírene používané normy.

- Sekcia D: Minimálna ochrana - Táto sekcia obsahuje iba jednu triedu a je rezervovaná pre systémy, ktoré boli podrobené hodnoteniu, ale nesplnili požiadavky vyšších tried.
- Sekcia C: Voľná ochrana - Užívateľom je poskytnutá určitá miera ochrany, ktorú môžu využiť.
  - Triedy C1 a C2
- Sekcia B: Povinná ochrana - Určitý systém ochrany sú užívatelia povinní využívať a nemôžu ho nijakým spôsobom obísť.
  - Triedy B1, B2 a B3
- Sekcia A: Overená ochrana - Je charakteristická formálnymi metódami overovania bezpečnosti
  - Trieda A1

História riadenia informačnej bezpečnosti

Information Technology Security Evaluation Criteria je pokusom o zosúladenie jednotlivých národných kritérií do medzinárodne platného celku. V roku 1991 bol prijatý ako základ pre hodnotenie bezpečnosti systémov na spracovanie informácií v členských štátoch Európskej únie.

História riadenia informačnej bezpečnosti

Common Criteria

- **Metanorma Common Criteria (ISO/IEC 15408)** je založená na modeli, v ktorom môžu užívatelia špecifikovať svoje vlastné požiadavky na bezpečnosť. Stanovuje princípy a postupy, ako odvodzovať konkrétne technické normy pre vývoj, testovanie, výsledné vlastnosti a prevádzku technických bezpečnostných protiopatrení v rôznych prostrediach.

  Vychádza z troch historicky najuznávanejších štandardov:

  - ITSEC,
  - TCSEC
  - a CTCPEC (Canadian standard).

História riadenia informačnej bezpečnosti

BS 7799 bol štandard pôvodne publikovaný skupinou BSI v roku 1995. Norma bola pripravená vládou Spojeného kráľovstva úradom obchodu a priemyslu (DTI) a obsahovala tri časti.

- BS 7799 časť 1 (1998) - **Code of Practice for Information Security Management** (Kódex praxe manažérstva informačnej bezpečnosti).
- BS 7799 časť 2(1999) - **Specification for Information Security Management Systems**(Špecifikácia Systému manažérstva informačnej bezpečnosti).
- BS 7799 časť 3 (2005)**– Information Security Management Systems** – Guidelines for Information Security Risk Management)

História riadenia informačnej bezpečnosti

ISO/IEC 17799:2000 prevzatím BS 7799 založila príručku a všeobecné princípy na vytváranie, implementáciu, správu a zlepšovanie manažmentu informačnej bezpečnosti v organizáciách.

Implementácia modelu PDCA na zlepšovanie systému manažérstva informačnej bezpečnosti (SMIB)

História riadenia informačnej bezpečnosti

Požiadavky na to, ako systém manažérstva informačnej bezpečnosti v spoločnosti zaviesť poskytuje medzinárodná norma ISO/IEC 27001:2005, ktorej vlastníkom je ISO12 a IEC13.

Medzinárodná norma ISO/IEC 27001 bola vydaná v roku 2002 revidovaním verzie dokumentu britskej normy BS 7799-2:1999 (BS 7799-2:2002) (ISO/IEC 27001; BS 77999-3:2006)

História riadenia informačnej bezpečnosti

(ISO/IEC 27001:2005; ISO/IEC 27002:2005) obsahovali nasledujúce časti:

1. Bezpečnostná politika.
2. Organizácia bezpečnosti informácií.
3. Riadenie aktív.
4. Bezpečnosť ľudských zdrojov.
5. Fyzická bezpečnosť a bezpečnosť prostredia.
6. Riadenie komunikácie a riadenie prevádzky.
7. Riadenie prístupov.
8. Akvizície, vývoj a údržba informačných systémov.
9. Zvládanie bezpečnostných incidentov.
10. Riadenie kontinuity činnosti organizácie.
11. Súlad s požiadavkami.

História riadenia informačnej bezpečnosti

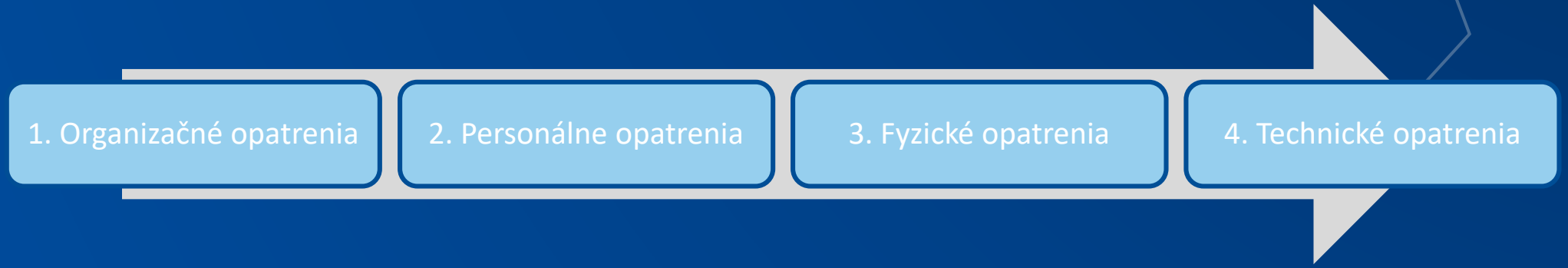
- Slovenská republika prevzala uvedenú normu pod označením STN EN ISO 27001:2006, ktorá umožňuje efektívne a prehľadne riadiť bezpečnosť informácií v spoločnosti.
- To znamená, že certifikát získaný podľa tejto normy má medzinárodnú platnosť – spoločnosť, ktorá získa certifikát SMIB ISO 27001 napr. na Slovensku, nemusí preukazovať znovu splnenie požiadaviek tejto normy v inej krajine.

Prax SMIB

ISO 27001 a jej verzie

- ISO 27001 – rok 2004 (11 oblastí, zlepšovanie procesov – model PDCA)
- ISO 27001 – rok 2013 (2019) (14 oblastí, voľný model systému zlepšovania procesov)
- 25. októbra 2022 vyšla nová verzia ISO/IEC 27001:2022

Hlavné zmeny, ktoré nová verzia prináša je zlúčenie opatrení do 4 skupín:



- 5 atribútov pre kontrolu, 12 kontrol

Prax SMIB

- SMIB je efektívny spôsob ochrany informácií pred stratou dôvernosti, dostupnosti, integrity a súčasne integruje tiež všetky zákonné, regulačné a zmluvné záväzky spoločnosti.
- Norma STN ISO/IEC 27001:2014 predkladá požiadavky na vytvorenie, zavedenie, udržiavanie a neustále zlepšovanie zdokumentovaného systému SMIB.
- Zavádza štruktúru vysokej úrovne, rovnaké názvy kapitol, rovnaký text, všeobecné výrazy a definície ako ich definuje Príloha SL Nariadenia ISO/IEC Časť 1 upraveného doplnku ISO čím udržiava kompatibilitu s inými normami riadiacich systémov, ktoré sa prijali v prílohe SL (integrované systémy manažérstva - ISO 9001, ISO 14001).

Prax SMIB

Tzv. SOA (vyhlásenie o aplikovateľnosti) – základný dokument

Implementácia ISO/IEC 27000 vyžaduje **dva druhy** dokumentácie:

vypracovanie internej riadiacej dokumentácie, (stratégia obnovy, politika IS, smernice, metodické návody – celkovo až 114 kontrol)

vedenie prevádzkovej dokumentácie (analýza rizík, BIA, plány BCP, DRP plány, záznamy z testovania, evidencie, ročné správy, plány, záznamy z kontrol a auditov)

Politika informačnej bezpečnosti

V rámci uplatnenia zásad riadenia informačnej bezpečnosti podľa normy STN ISO/IEC 27001 prijíma vedenie spoločnosti nasledovné záväzky v tejto oblasti:

- Zabezpečovať primeranú ochranu informačných aktív
- Prideliť zodpovednosti za informačnú bezpečnosť
- Stanoviť zodpovednosť za riadenie rizík a incidentov
- Zvyšovať povedomie informačnej bezpečnosti zamestnancov
- Brániť neautorizovanému fyzického prístupu do priestorov IKT
- Predchádzať neautorizovanému prístupu do informačných systémov
- Monitorovať neautorizované aktivity v súvislosti so spracovaním informácií
- Udržiavať riadený proces pre zostavovanie a implementovanie plánov kontinuity činnosti
- Chrániť informácie v zmysle platnej legislatívy
- Vykonávať audity informačných systémov s cieľom minimalizácie rizika prerušenia činnosti

Smernice

V smerniciach uviesť zásady opatrení k oblastiam:

- Organizácia bezpečnosti informácií
- Riadenie komunikácie a riadenie prevádzky
- Zvládanie bezpečnostných incidentov
- Súlad s požiadavkami
- Riadenie aktív
- Riadenie prístupov
- Riadenie kontinuity činnosti organizácie
- Bezpečnosť ľudských zdrojov
- Akvizície, vývoj a údržba informačných systémov
- Fyzická bezpečnosť a bezpečnosť prostredia

Metodické návody

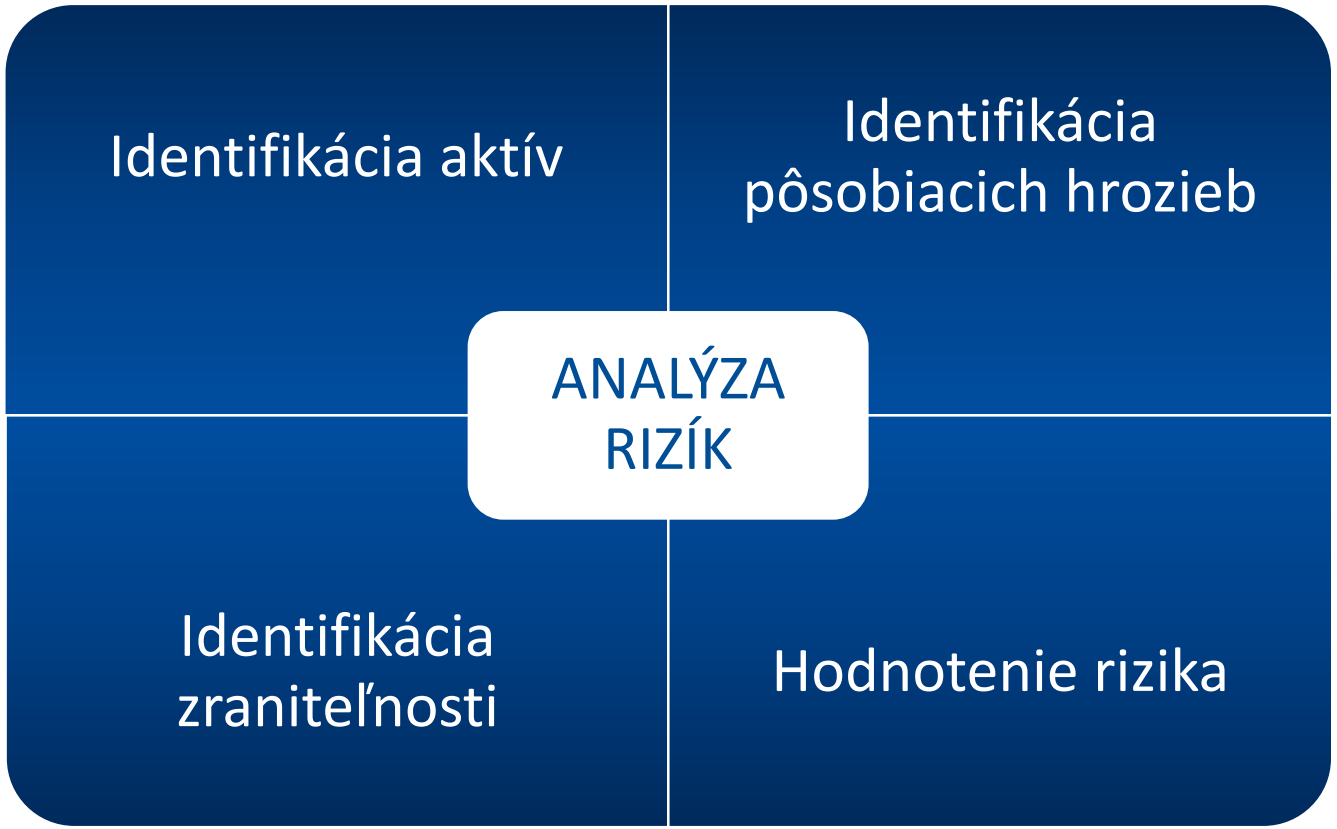
Metodické návody sú určené len pre špecifické skupiny rolí.

Napríklad:

- METODICKY_NAVOD_PRE_TVORBU_BCP_DRP_PLANOV
- METODIKA_RIADENIE_KONFIGURACIÍ
- PROFYLAKTICKE_CINNOSTI
- RIADENIE_INTERNEJ_INFRASTRUKTURY (zálohovanie)
- RIADENIE_INTERNYCH_AUDITOV

Prevádzková dokumentácia

Analýza rizík - využívanie princípov ISO/IEC 27005



Manažment rizika

4 základné spôsoby manažovania rizík:

Riadenie procesov

BIA (Business impact analysis - analýza funkčných dopadov – analýza dosahu činností) **ISO/TS 22317**

- všeobecné informácie o procese (názov, manažér, organizačný útvar)
- požiadavky pre obnovu (RTO - požadovaná doba obnovy)
- RPO - prípustná doba straty údajov, obdobia, v ktorých má výpadok základnej služby najvyšší dopad)
- finančné a nefinančné dopady nedostupnosti procesov
- činnosti vykonávané v rámci procesu
- závislosti od vstupov (názov vstupu, na ako dlho môže vstup vypadnúť, zdroj vstupu)
- definované výstupy (názov výstupu, ako sa výstup používa, kde je výstup uložený)
- potrebné aplikácie (názov aplikácie, do akej doby musí byť aplikácia sprevádzkovaná)
- spracovávané informačné aktíva
- súlad s legislatívou a závislosť od dodávateľov
- personálna bezpečnosť (identifikácia kľúčových zamestnancov, nedostupnosť kľúčového zamestnanca).

Plány DRP a BCM

Výstupy BIA:

DRP	• plány obnovy
BCM	• plány kontinuity

Testovanie jednotlivých plánov:

- kontrolný zoznam (checklist) – každý člen tímu kontroluje zoznam, ktorý obsahuje body, ktoré je nutné splniť,
- revízia plánov (walk-through test) – členovia emergency response tímu sa zídu a prechádzajú plány, detekujú nedostatky a problémy,
- simulovaný test (simulation test) – všetko sa robí iba ako,
- paralelný test (parallel test) – nedochádza k prerušeniu prevádzky, pokus zduplikovať činnosť v inom DC;
- plné prerušenie (full interruption test) – preruší sa beh systému v primárnom DC, pokus o obnovu v alternativnom DC.

Záznamy - Plán realizácie opatrení

- Úlohy z externých auditov
- Úlohy z interných auditov
- Úlohy z analýzy rizík
- Úlohy z riadenia incidentov
- Úlohy z testovania plánov
- Úlohy z požadovaného technického rozvoja

Záznamy - prevádzková dokumentácia

- Evidencia incidentov, riešenie incidentov
- Z testovania plánov (BCM, DRP)
- Dokumentácia z metodických návodov – (napr. test motorgenerátora)
- Ukladanie záloh – médií
- Prístupové účty, práva, časové obmedzenia
- Pridelenie a evidencia schváleného softvéru
- Topológia siete
- Konfigurácie bezpečnostných prvkov, sieťových prvkov
- Záznamy zo zvyšovania povedomia

Vzťahy na legislatívu SR

STN ISO/IEC 27001 je základom na riadenie bezpečnosti IS

Zákony:

- Zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností
- Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti
- Zákon č. 95/2019 Z.z. o informačných technológiách verejnej správy

Ďakujem za pozornosť

Ing. Ladislav Martinček

Mobil: +421 905 974 859 | E-mail: ladislav.martincek@lynx.sk