Ohodnotenie rizík aktív IS – základný predpoklad dobrého manažmentu bezpečnosti IS

Doc. Ing. Ladislav Hudec, CSc., CISA
Certifikovaný audítor informačných systémov
Znalec pre bezpečnosť a ochranu informačných systémov
Fakulta informatiky a informačných technológií STU Bratislava
Pripravené pre Seminár k bezpečnostným štandardom
MF SR, dňa 21.7.2009

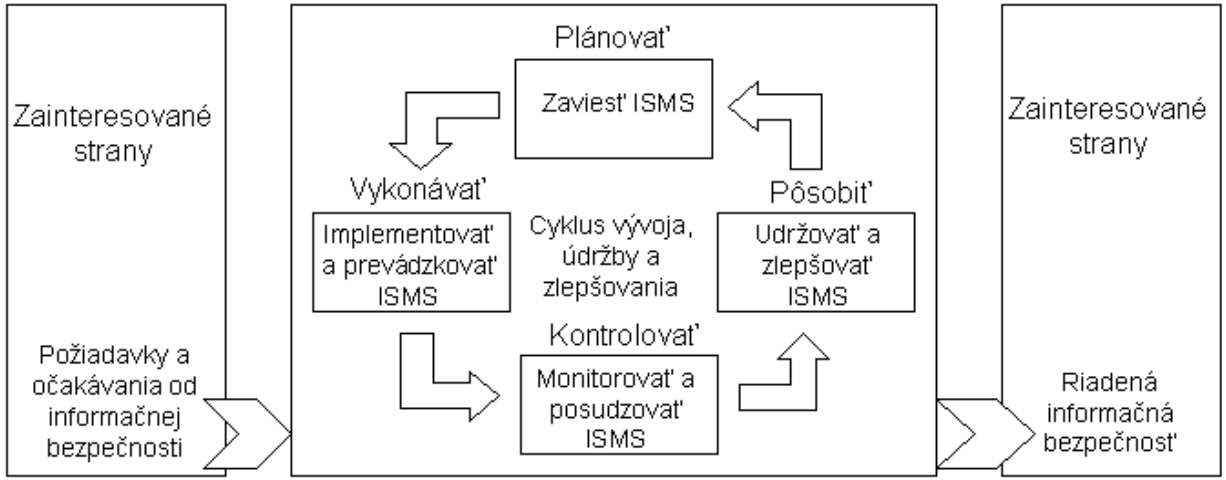
Globálny pohľad na budovanie ISMS

- Norma ISO/IEC 27001:2005 podporuje osvojenie si procesného prístupu k zavedeniu, implementácii, prevádzke, monitorovaniu, udržiavaniu a zlepšovaniu účinnosti ISMS spoločnosti.

- **Procesný prístup** podporuje jeho používateľov v zdôrazňovaní dôležitosti:
  - Chápania požiadaviek bezpečnosti informácií spoločnosti a potreby zaviesť politiku a ciele informačnej bezpečnosti
  - Implementovania a prevádzky opatrení v kontexte riadenia celkového podnikateľského rizika spoločnosti
  - Monitorovania a revidovania výkonnosti a účinnosti ISMS
  - Kontinuálneho zlepšovania ISMS založeného na objektívnom meraní.

- Model známy ako **PDCA** (Plan-Do-Check-Act, Plánovať-Vykonávať-Kontrolovať-Pôsobiť) bol osvojený touto normou a možno ho aplikovať na všetky procesy ISMS. Na nasledujúcom obrázku je ilustrácia, ako ISMS prijíma na vstupe požiadavky a očakávania informačnej bezpečnosti zainteresovaných strán a prostredníctvom potrebných činností a procesov vytvára výsledky informačnej bezpečnosti (t.j. riadenú informačnú bezpečnosť), ktoré tieto požiadavky a očakávania splňujú.

Globálny pohľad na budovanie ISMS – model PDCA pre proces ISMS



- Stručný opis vecného obsahu fáz modelu PDCA je takýto:
  - **Plánovať (Zaviesť ISMS)** – určiť bezpečnostnú politiku, ciele, procesy a procedúry relevantné pre riadenie rizika a zlepšovanie informačnej bezpečnosti s cieľom priniesť výsledky v súlade s celkovou politikou a cieľmi spoločnosti.
  - **Vykonať (Implementovať a prevádzkovať ISMS)** – implementovať a prevádzkovať politiku ISMS, opatrenia, procesy a postupy.
  - **Kontrolovať (Monitorovať a posudzovať ISMS)** – ohodnocovať a tam, kde je to vhodné, merať výkonnosť procesov oproti stanovenej politike.
  - **Pôsobiť (Udržiavať a zlepšovať ISMS)** – vykonávať nápravné a preventívne činnosti, založené na výsledkoch interných auditov ISMS, preskúmavaniach manažmentom alebo iných relevantných informáciách s cieľom dosiahnuť trvalé zlepšovanie ISMS.

Podrobnejší pohľad na fázu Plánovať (Zaviesť ISMS)

- Pri podrobnejšom pohľade na prvú fázu **Plánovať (Zaviesť ISMS)** modelu PDCA možno v nej vypozorovať tieto aktivity spoločnosti:
  - Stanovenie rozsahu ISMS
  - Stanovenie politiky ISMS
  - **Stanovenie systematického prístupu na ohodnotenie rizík**
  - **Identifikácia rizík**
  - **Ohodnotenie rizík**
  - **Identifikácia a vyhodnotenie možností narábania s rizikom**
  - **Vybratie cieľov ochrany a opatrení**
  - Príprava Prehlásenia o aplikovateľnosti
  - Získanie súhlasu manažmentu.

Proces ohodnotenia rizík

- **Ohodnotenie rizík** je proces realizujúci sa týmito krokmi:
  - Identifikácia a ohodnotenie aktív
  - Identifikácia všetkých bezpečnostných požiadaviek, t.j. hrozieb, zraniteľností, právnych a obchodných požiadaviek
  - Ohodnotenie pravdepodobnosti výskytu hrozieb a zraniteľností, ohodnotenie dôležitosti právnych a obchodných požiadaviek
  - Vypočítanie rizika vyplývajúceho z týchto faktorov
  - Výber vhodných možností narábania s rizikom
  - Výber opatrení na redukovanie rizík na akceptovateľnú úroveň.

Identifikácia aktív

- **Aktívum** je niečo, čo má hodnotu alebo je pre spoločnosť užitočné, pre jej obchodné operácie alebo kontinuitu činnosti. To znamená, že **aktíva potrebujú ochranu**, aby sa zaistili korektné obchodné operácie a kontinuita činnosti.
- **Vhodná správa aktív a účtovateľnosť** aktív je rozhodujúca na zaistenie ich primeranej ochrany. Tieto dva aspekty by mali byť dôležitou povinnosťou na všetkých manažérskych úrovniach.
- Príklady aktív zahrňujú:
  - Informačné aktíva: databázy a údajové súbory, systémová dokumentácia, používateľské manuály, školiace materiály, prevádzkové a podporné procedúry, havarijné plány
  - Papierová dokumentácia: kontrakty, návody, dokumentácia spoločnosti, dokumenty obsahujúce dôležité obchodné údaje
  - Softvérové aktíva: aplikačný softvér, systémový softvér, vývojové nástroje a utility
  - Fyzické aktíva: počítače a komunikačné zariadenia, magnetické médiá (pásky a disky), ďalšie technické zariadenia (zdroje energií, klimatizácia), nábytok,
  - Ľudia: obslužný personál, zákazníci, predplatitelia
  - Reputácia a obraz spoločnosti
  - Služby: výpočtové a komunikačné služby, ďalšie technické služby (kúrenie, osvetlenie, energie, klimatizácia).
- Výsledkom tohto kroku by mal byť inventárny zoznam obsahujúci všetky dôležité aktíva ISMS, ich umiestnenie a ich vlastníka.

Ohodnotenie aktív

- Ohodnotenie aktív sú zvyčajne vyjadrené vo forme potenciálneho dopadu na obchod (podnikanie) v dôsledku neželaných incidentov ako sú zverejnenie, modifikácia, nedostupnosť a/alebo zničenie informácií alebo iných aktív. Pokiaľ takéto incidenty nastanú, môžu viesť k finančným stratám, stratám príjmu, strate podielu na trhu alebo poškodeniu obrazu spoločnosti.
- Vstupy do ohodnotenia aktív **by mali byť poskytnuté vlastníkmi a používateľmi aktív**, teda tými, ktorí môžu záväzne hovoriť o dôležitosti aktív (najmä informácií) pre spoločnosť a jej podnikanie.
- Príkladom mierky ohodnocovania aktív môže byť základná mierka:
  - Vysoká - Poškodením, zničením alebo stratou dôvernosti, prípadne integrity aktíva (ďalej len narušením aktíva) dôjde alebo môže dôjsť k úplnému prerušeniu jedného alebo viacerých kľúčových procesov, k ohrozeniu zdravia alebo života; vzniknutá škoda môže byť veľmi vysoká, neohrozí však samotnú existenciu spoločnosti
  - Stredná - Narušením aktíva môže dôjsť k čiastočnému narušeniu jedného kľúčového procesu, k prerušeniu jedného alebo viacerých menej významných procesov spoločnosti; vzniknutá škoda bude mať pravdepodobne vplyv na aktuálny rozpočet organizácie
  - Nízka - Narušením aktíva môže dôjsť k narušeniu jedného alebo viacerých menej významných procesov spoločnosti; vzniknutá škoda nemá vplyv na aktuálny rozpočet spoločnosti
- Výsledkom tokto kroku je doplnenie inventára aktív o hodnotu aktíva pre každé aplikovateľné kritérium t.j. **dôvernosť, integrita, dostupnosť a prípadne ďalších kritérií**, ak existujú.

Identifikácia bezpečnostných požiadaviek

- **Bezpečnostné požiadavky** v každej spoločnosti, malej alebo veľkej, sú v skutočnosti odvodené z troch hlavných zdrojov a mali by byť dokumentované v ISMS:
  - Jedinečná množina hrozieb a zraniteľností, ktoré môžu viesť k významným obchodným stratám, pokiaľ nastanú
  - Zákonné alebo kontraktačné požiadavky, ktoré musí spoločnosť splniť, ktoré musia splniť obchodní partneri, zmluvní partneri a poskytovatelia služieb
  - Jedinečná množina princípov, cieľov a požiadaviek na spracovanie informácií, ktoré si vytvorila spoločnosť na podporu svojich podnikateľských operácií a procesov a ktoré aplikuje na informačný systém spoločnosti.
- Ako náhle sú tieto bezpečnostné požiadavky stanovené, odporúča sa formulovať ich vo vyjadrení požiadaviek na **dôvernosť, integritu a dostupnosť**.
- Najneskôr pred vykonávaním tohto kroku by mali byť identifikované **už implementované bezpečnostné opatrenia**. Toto je nevyhnutné na úplnú identifikáciu a realistické ohodnotenie hrozieb a zraniteľností a samozrejme, tiež na výber dodatočných opatrení, ktoré budú dobre fungovať s už existujúcimi opatreniami.

Identifikácia bezpečnostných požiadaviek - Hrozby

- Aktíva sú predmetom mnoho typov **hrozieb**:
  - Hrozba má potenciál spôsobiť neželaný incident, ktorý môže spôsobiť škodu systému, alebo spoločnosti a jej aktívam.
  - Škoda sa môže objaviť po priamom alebo nepriamom útoku na informácie spoločnosti, napríklad neautorizované zničenie, zverejnenie, modifikácia, poškodenie a nedostupnosť alebo strata.
  - Hrozby môžu vzniknúť z náhodných alebo úmyselných zdrojov alebo udalostí.
  - Hrozba musí zneužiť zraniteľnosť systému, aplikácie alebo služby používanej spoločnosťou, aby úspešne spôsobila škodu aktívu.
- Zoznam všeobecných hrozieb (ISO/IEC TR 13335-3: 1998, BS7799-3: 2006)
  - ...
  - Strata integrity
  - Strata záznamov
  - Strata služby
  - Chyba údržby
  - Chybná funkcia podporných prostriedkov
  - Škodlivý kód
  - Predstieranie používateľovej identity
  - Chybné použitie (zneužitie) auditných nástrojov
  - Chybné použitie (zneužitie) prostriedkov spracovania informácií
  - Chybné použitie (zneužitie) zdrojov alebo aktív
  - ...

Identifikácia bezpečnostných požiadaviek - Zraniteľnosti

- **Zraniteľnosti sú slabiny spojené s aktívami spoločnosti**. Tieto slabiny môžu byť využité (zneužité) hrozbou spôsobujúcou neželaný incident, ktorý môže skončiť stratou, škodou alebo poškodením aktíva.
- Zraniteľnosť sama o sebe nespôsobuje škodu, je iba podmienkou alebo množinou podmienok, ktoré umožňujú hrozbe pôsobiť na aktívum.
- Identifikácia zraniteľnosti by mala zisťovať slabiny aktíva vo vzťahu ku:
  - Fyzickému prostrediu
  - Personálu, manažérskych a administratívnych procedúr a opatrení
  - Hardvéru, softvéru alebo komunikačných zariadení a prostriedkov,

  ktoré môžu byť využité zdrojom hrozby na spôsobenie škody aktívu a obchodu, ktoré podporuje.
- Všeobecné zraniteľnosti (bezpečnosť ľudských zdrojov):
  - Nedostatočné bezpečnostné školenie
  - Absencia bezpečnostného povedomia
  - Absencia monitorovacích mechanizmov
  - Absencia pravidiel na správne používanie telekomunikačných médií a prenosu
  - Neodstránenie prístupových práv pri ukončení pracovného pomeru
  - Absencia procedúry zabezpečujúca navrátenie aktív pri ukončení pracovného pomeru
  - Nemotivovaný alebo nespokojný personál
  - Práca externého personálu bez dozoru alebo práca personálu mimo riadnych prevádzkových hodín

Ohodnotenie bezpečnostných požiadaviek

- Po identifikácii hrozieb a zraniteľností je nevyhnutné **ohodnotiť pravdepodobnosť**, že nastane **kombinácia hrozby a zraniteľnosti**. Pri ohodnotení pravdepodobnosti hrozieb by do úvahy malo byť vzaté:
  - Úmyselné hrozby: motivácia, dané schopnosti a potreba, dostupné zdroje možnému útočníkovi a predstava atraktívnosti
  - Náhodné hrozby: ako často sa môžu vyskytnúť, na základe skúsenosti, štatistík, atď, a geografických faktorov ako je blízkosť chemických fabrík, v oblastiach kde je vždy možné extrémne počasie, a faktory, ktoré môžu ovplyvniť ľudskú chybovosť a zlyhanie zariadenia.
- Rovnakým spôsobom ako boli ohodnotené hrozby a zraniteľnosti, mala by byť stanovená hodnota **pre zákonné a obchodné požiadavky**. Je to nevyhnutné na vypočítanie rizika súvisiaceho s týmito bezpečnostnými podmienkami.
- Aby sme mohli priradiť hodnotu špecifickej zákonnej alebo obchodnej požiadavke, je nevyhnutné stanoviť:
  - Ako vážny je obchodný dopad v prípade, že nie sú splnené zákonné/kontraktačné alebo obchodné požiadavky
  - Aké to môže mať dôsledky pre uvažované aktíva a pre celý ISMS
  - Aká je pravdepodobnosť, že to nastane.
- Výsledky predchádzajúcich úvah by sa mali použiť pre každé aktívum a každú zákonnú/kontraktačnú a obchodnú požiadavku na stanovenie primeranej hodnoty zo stupnice bezpečnostných podmienok.
- Výsledkom tohto kroku by malo byť ohodnotenie všetkých identifikovaných bezpečnostných požiadaviek.

Ohodnotenie bezpečnostných požiadaviek

- Pre ohodnocovanie bezpečnostných požiadaviek je nevyhnutné, podobne ako pri ohodnotení aktív, stanoviť mierku na toto ohodnotenie, ktorá je vhodná pre použitú metodológiu ohodnotenia rizík. V mnohých prípadoch sa používa jednoduchá mierka s tromi úrovňami Vysoká, Stredná a Nízka, ktorá je postačujúca a hlavne neúmerne nekomplikuje celý proces.
- Trojúrovňová mierka na **ohodnotenie hrozby**:
  - **Vysoká** - Očakáva sa výskyt hrozby, v minulosti boli incidenty alebo štatistiky alebo ďalšie informácie, ktoré indikujú, že takáto hrozba sa pravdepodobne vyskytne, alebo existuje vážne dôvody alebo motivácie pre útočníka vykonať takúto hrozbu
  - **Stredná** - Hrozba sa možno vyskytne, v minulosti boli incidenty alebo štatistiky alebo ďalšie informácie, ktoré indikujú, že takáto alebo podobné hrozby sa vyskytli niekedy v minulosti, alebo existuje indikácia, že by mohli existovať pre útočníka nejaké dôvody vykonať takúto hrozbu
  - **Nízka** - Je nepravdepodobné, že sa hrozba objaví, nevyskytli sa incidenty, štatistiky, motívy, atď, ktoré by indikovali že hrozba nastane
- Trojúrovňová mierka na **ohodnotenie zraniteľnosti**:
- Identifikácia zraniteľnosti by mala zisťovať slabiny aktíva vo vzťahu ku:
  - **Vysoká** - Je jednoduché využiť zraniteľnosť, sú implementované slabé alebo žiadne ochranné opatrenia
  - **Stredná** - Zraniteľnosť by mohla byť využitá, sú implementované nejaké bezpečnostné opatrenia
  - **Nízka** - Je obtiažne využiť zraniteľnosť, sú implementované dobré bezpečnostné opatrenia

Výpočet bezpečnostných rizík

- Cieľom ohodnotenia rizík je **identifikovať a ohodnotiť riziká** na základe predchádzajúcich krokov. Riziká sú počítané kombináciou ohodnotenia aktív a ohodnotených úrovní odpovedajúcich bezpečnostných požiadaviek.
- Existuje **viacero rôznych spôsobov** na kombinovanie týchto faktorov, napríklad na odmeranie rizík sa kombinujú ohodnotenia pridelené aktívam, zraniteľnostiam, hrozbám a zákonným a obchodným požiadavkám.
- Je dôležité poznamenať, že neexistuje „správny“ a „nesprávny“ spôsob výpočtu rizík. Treba len koncepty opísané skorej rozumným spôsobom kombinovať. Je na zvážení spoločnosti, aby stanovila metódu ohodnotenia rizík, ktorá je vhodná pre jej podnikateľské a bezpečnostné podmienky.
- Výsledkom tohto kroku by mal byť zoznam odmeraných rizík pre každý dopad zverejnenia, modifikácie, nedostupnosti a zničenia každého aktíva z rozsahu uvažovaného ISMS.

Identifikácia a vyhodnotenie možností na zaobchádzanie s rizikom

- Nasledujúcou úlohou spoločnosti je **identifikovať a vyhodnotiť najvhodnejšie akcie na zvládnutie rizík**. Rozhodnutie by sa malo vykonať na základe dotknutých aktív a obchodných dopadov. Ďalším dôležitým vstupom do tohto rozhodovania je **akceptovateľná úroveň rizika**, ktorá bola stanovená následne po výbere vhodnej metodológie ohodnotenia rizík.
- Pre identifikované a ohodnotené riziká existujú pre spoločnosť štyri možné riešenia narábania s rizikami:
  - Použiť vhodné opatrenia na **redukciu rizík**
  - Vedome a objektívne **akceptovať riziká**, dokumentujúc zrejmé splnenie politiky spoločnosti a splnenie kritérií na akceptovanie rizika
  - **Zamedziť rizikám**
  - **Preniesť súvisiace obchodné riziká na iné organizačné jednotky** spoločnosti (mimo uvažovaného ISMS) alebo iné spoločnosti (outsourcing).
- Pre každé riziko by mali byť vyššie uvedené možnosti vyhodnotené s cieľom určiť najvhodnejšiu možnosť. Výsledky týchto rozhodnutí by mali byť dokumentované a následne v použité v procese vytvorenia plánu narábania s rizikami.
- Výsledkom tohto kroku by mala byť stanovená a dokumentovaná vhodná voľba narábania s každým rizikom, ktoré bolo ohodnotené v predchádzajúcich krokoch.

Výber bezpečnostných opatrení

- Na redukciu ohodnotených rizík v rozsahu uvažovaného ISMS by mali byť stanovené a vybraté **vhodné a odôvodnené bezpečnostné opatrenia**. Cieľom výberu opatrení je redukcia rizík na úroveň, ktorá je akceptovateľná pre spoločnosť.
- Pri výbere opatrení na implementáciu by mali byť zvažované viaceré faktory:
  - Ľahké používanie opatrenia
  - Transparentnosť používateľovi
  - Poskytnutie pomoci používateľom pri vykonávaní ich funkcií
  - Relatívna sila opatrení
  - Typy vykonávaných funkcií – prevencia, odstrašenie, detekcia, obnova, oprava, monitorovanie a povedomie
- Vo všeobecnosti opatrenie bude splňovať viac ako jeden z vyššie uvedených faktorov a čím ich splňuje viacej tým je to lepšie. Pri preverovaní celkovej bezpečnosti alebo množiny použitých opatrení by mala byť zabezpečená rovnováha medzi uvedenými faktormi, pokiaľ je to možné. To napomáha celkovej bezpečnosti z pohľadu jej efektívnosti a účinnosti. **Výber opatrení by mal vždy zahrňovať vyváženosť prevádzkových (netechnických) a technických opatrení, ktoré sa navzájom podporujú a doplňujú.**
- Výsledkom tohto kroku by mal byť výber opatrení na redukciu všetkých takých rizík, ktoré boli identifikované na ošetrenie. Navyše malo by byť zdokumentované spojenie s ohodnotením rizík, a malo by byť zabezpečené, že všetky riziká sú redukované tak ako to bolo možné.

Prístup k ohodnoteniu rizík

- Ako už bolo spomenuté, je na spoločnosti, aby si vybrala vhodný prístup na ohodnotenie rizík.
- **Rôzne prístupy k ohodnoteniu rizík sa menia v rozsahu potrebného času a úsilia a hĺbke analýzy detailov**. Aj napriek faktu, že spoločnosť si môže zvoliť prístup k ohodnoteniu rizík, je potrebné zaistiť, že použitá metóda ohodnotenia rizík je vhodná a dostatočne detailná vo vzťahu k podnikateľským a bezpečnostným požiadavkám spoločnosti.
- Ak napríklad, spoločnosť alebo ISMS a jeho aktíva má prevažne bezpečnostné požiadavky nízkej alebo strednej úrovne, pre takúto spoločnosť môže byť postačujúci **prístup základného ohodnotenia rizík**.
- Ak sú bezpečnostné požiadavky vyššej úrovni (strednej a vysokej), vyžaduje sa detailné a špeciálne ohodnotenie. Potom môže byť nevyhnutné použiť **prístup detailného ohodnotenia rizík.**
- V každom prípade by sa však malo zabezpečiť, že vybratý prístup k ohodnoteniu rizík splňuje všetky náležitosti procesu stanoveného na začiatku.

Základný prístup k ohodnoteniu rizík

- Prístup základného ohodnotenia rizík zahrňuje výber bezpečnostných opatrení na základe jednoduchého a priamočiareho použitia procesu opísaného v prezentácii.
- Tento prístup umožní spoločnosti zaviesť ISMS dosiahnutím **základnej úrovni ochrany** (baseline level of security), ktorá vychádza z identifikácii a ohodnotení základných a podstatných potrieb a požiadaviek spoločnosti.
- Dosiahnutá základná úroveň bezpečnosti, použitím tohto jednoduchého a priamočiareho prístupu, je vhodná pre **útvar spoločnosti s nízkou úrovňou bezpečnostných požiadaviek** alebo, v niektorých prípadoch, dokonca aj pre celú spoločnosť, pokiaľ bezpečnostné požiadavky sú na dostatočne nízkej úrovni.
- Pri prípadnej certifikácii ISMS však **musí spoločnosť zdôvodniť**, prečo prístup základného ohodnotenia rizík je pre ňu postačujúci.

Aktivity základného prístupu k ohodnoteniu rizík

Úlohy ohodnotenia a spravovania rizík	Aktivity základného ohodnotenia rizík
Identifikácia a ohodnotenie aktív	Vytvoriť zoznam aktív majúcich súvis s podnikateľským prostredím, obchodnými operáciami a informáciami, ktoré sú ohodnocované v rámci rozsahu ISMS, identifikácia ich hodnôt použitím jednoduchej ohodnocovacej mierky.
Identifikácia a ohodnotenie bezpčnostných požiadaviek	Identifikovať bezpečnostné požiadavky (požiadavky môžu byť zisťované pomocou dotazníka so všoebecnými alebo všeobecne známymi hrozbami a zraniteľnosťami) a ohodnotiť všetky identifikované bezpečnostné požiadavky pomocou jednoduchej ohodnocovacej mierky.
Výpočet rizika	Vypočítať riziká na základe informácií o aktívach a bezpečnostných požiadavkách použitím jednoduchého kalkulačného vzorca.
Stanovenie a vyhodnotenie možností narábania s rizikom	Stanoviť vhodné akcie narábania s rizikami pre každé identifikované riziko, dokumentovať výsledky plánu narábania s rizikami.
Výber bezpečnostných opatrení, redukcia rizika a akceptácia	Pre každé identifikované aktívum stanoviť ciele ochrany a opatrenia podľa ISO/IEC 17799: 2005. Zaistiť, aby ciele ochrany a vybrané opatrenia redukovali riziko na akceptovateľnú úroveň.

Tabuľka č.1: Aktivity základného ohodnotenia rizík

Základný prístup k ohodnoteniu rizík

- Tento prístup môže byť realizovaný použitím **zjednodušenej matice**, ktorá napríklad zahrňuje iba dve úrovne bezpečnostných požiadaviek (Nízka a Vysoká) a ohodnotenie aktív použitím preddefinovanej mierky (Nízka hodnota, Stredná hodnota a Vysoká hodnota). Čísla v Tabuľke č.2 reprezentujú mieru rizika v škále od 0 do 4.

		Úroveň bezpečnostných požiadaviek	
		Nízka	Vysoká
Hodnota aktíva	Nízka hodnota	0	2
	Stredná hodnota	1	3
	Vysoká hodnota	2	4

Tabuľka č.2: Príklad matice ohodnotenia rizík

Základný prístup k ohodnoteniu rizík, výhody a nevýhody

- Prístup základného ohodnotenia rizík má **viacero výhod**, ako napríklad:
  - Na ohodnotenie rizik sú potrebné minimálne zdroje, je redukovaný čas a úsilie potrebné na výber opatrení
  - Rovnaké alebo podobné opatrenia môžu byť použité pre niekoľko aktív. V prípade, že veľké množstvo aktív společnosti je prevádzkovaných v spoločnom prostredí a obchodné a bezpečnostné požiadavky sú porovnateľné, poskytujú tieto opatrenia cenovo efektívne riešenie.
- **Nevýhodami** základného prístupu sú:
  - V prípade, že bezpečnostná úroveň je nastavená príliš vysoko, môžu byť pre niektoré aktíva vybraté príliš drahé alebo reštriktívne opatrenia. V prípade, že bezpečnostná úroveň je nastavená príliš nízko, pre niektoré aktíva môže byť implementovaná bezpečnosť nedostatočná.
  - Môžu existovať ťažkosti pri spravovaní bezpečnostne relevantních zmien. Napríklad, ak sa vyskytne zmena celkového charakteru podnikania ISMS, môže byť obtiažne ohodnotiť, či pôvodné opatrenia sú ešte postačujúce.

Detailný prístup k ohodnoteniu rizík

- Tento prístup zahrňuje vykonanie **detailného ohodnotenia rizík**, ktorý zahrňuje **detailnú identifikáciu a ohodnotenie aktív** a stanovenie a ohodnotenie úrovní bezpečnostných požiadaviek.
- Tieto informácie sa použijú na ohodnotenie rizík a následne sa použijú na stanovenie a výber bezpečnostných opatrení.
- Výber opatrení je zdôvodnený zistenými rizikami pôsobiacimi na aktíva a zaisťuje, že riziká sú redukované na akceptovateľnú úroveň, pokiaľ bola vybratá táto voľba narábania s rizikom.
- Detailné ohodnotenie rizík môže zahrňovať veľa zdrojov, preto je potrebné **starostlivo definovať hranice podnikateľského prostredia, prevádzky, informácií a hodnotených aktív v rámci rozsahu ISMS**.
- Na základe ohodnotenia rizík môžu byť vybraté opatrenia podľa normy ISO/IEC 17799:2005 splňujúce bezpečnostné ciele. Takýto celkový prístup je odlišný od prístupu základného ohodnotenia rizík v tom, že sa vykonáva **podstatne detailnejšia analýza aktív a bezpečnostných požiadaviek**. Samozrejme sa pritom sleduje všeobecný postup naznačený v prezentácii.

Aktivity detailného prístupu k ohodnoteniu rizík

Úlohy ohodnotenia a spravovania rizík	Aktivity detailného ohodnotenia rizík
Identifikácia a ohodnotenie aktív	Vytvoriť zoznam aktív majúcich súvis s podnikateľským prostredím, obchodnými operáciami a informáciami, ktoré sú ohodnocované v rámci rozsahu ISMS, definovať hodnotiacu mierku a každému aktívu priradiť hodnotu z tejto mierky (jednu hodnotu pre každú položku: dôvernosť, integrita, dostupnosť, prípadne ďalšiu hodnotu, pokiaľ sa aplikuje).
Identifikácia bezpečnostných požiadaviek	Identifikovať všetky bezpečnostné požiadavky (hrozby,a zraniteľnosti, právne a obchodné požiadavky) spojené so zoznamom aktív v rámci rozsahu ISMS.
Ohodnotenie bezpečnostných požiadaviek	Stanoviť vhodnú hodnotiacu mierku pre bezpečnostné požiadavky a priradiť primeranú hodnotu pre každú stanovenú bezpečnostnú požiadavku.
Výpočet rizika	Vypočítať riziká (na základe aktív a bezpečnostných požiadaviek, a ich hodnôt podľa ohodnotenia uvedeného vyššie) napríklad použitím prístupu uvedeného nižšie alebo iný variant alebo podobný typ metódy, ktorý je vhodný pre bezpečnostné požiadavky uvažovaného ISMS.
Stanovenie a vyhodnotenie možností narábania s rizikom	Stanoviť akcie vhodného narábania s rizikami pre každé zistené riziko. Vyhodnotiť, či stanovené voľby sú realistické, vhodné a sú v súlade so všetkými obchodnými a bezpečnostnými požiadavkami. Dokumentovať výsledky plánu narábania s rizikami.
Výber bezpečnostných opatrení, redukcia a akceptácia rizika	Pre vybratú metodológiu ohodnotenia rizík stanoviť akceptovateľnú úroveň rizika. Zaistiť, že táto úroveň akceptovateľného rizika je primeraná obchodným a bezpečnostným požiadavkám uvažovaného ISMS. Pre tie riziká, pre narábanie s ktorými bola zvolená redukcia, vybrať vhodné bezpečnostné ciele a opatrenia podľa normy ISO/IEC 17799: 2005. Ohodnotiť ako vybraté opatrenia redukovali riziko. Pre každé riziko, ktoré nemôže byť redukované na akceptovateľnú úroveň, stanoviť dodatočné akcie s rizikom (alebo manažérske rozhodnutie o jeho akceptovaní alebo o jeho neskoršej redukcii).

Tabuľka č.3: Aktivity detailného ohodnotenia rizík

Detailný prístup k ohodnoteniu rizík

- Podľa rozhodnutia spoločnosti je zvolená mierka ohodnotenia aktív napríklad 0 (?) až 4. Odpovede na hrozby a zraniteľnosti stanovujú každej hrozbe a zraniteľnosti nejakú úroveň z preddefinovanej mierky. Preddefinovaná mierka úrovní hrozieb a úrovni zraniteľnosti môže byť vyjadrená v kvalitatívnej mierke Nízka úroveň (N), Stredná úroveň (S) a Vysoká úroveň (V). Hodnota aktíva a úrovne hrozieb a zraniteľností môžu byť dané dohromady na ohodnotenie rizika tak, ako je to uvedené v Tabuľke č.4, kde mierka pre úroveň rizika je od 1 do 8.
- Matica ohodnotenia rizík sa môže meniť v počte úrovní hrozieb, úrovní zraniteľností a v počte úrovní hodnôt aktív. Môže byť ušitá na mieru potrebám spoločnosti. Po ukončení prvého preskúmania ohodnotenia rizík by mali byť výsledky preskúmania (aktíva a ich hodnoty, úrovne hrozieb, zraniteľností a úrovne rizika. stanovené opatrenia) uložené a dokumentované, napríklad v databáze.

	Úroveň hrozby	**Nízka**			**Stredná**			**Vysoká**		
	Úroveň zraniteľnosti	**N**	**S**	**V**	**N**	**S**	**V**	**N**	**S**	**V**
Hodnota aktíva	**0**	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Tabuľka č.4: Príklad matice ohodnotenia rizík

Detailný prístup k ohodnoteniu rizík, výhody a nevýhody

- **Výhody** tohto prístupu sú:
  - Získa sa presný a detailný pohľad na bezpečnostné riziká, ktorý vedie na stanovenie bezpečnostných úrovní odrážujúcich požadavky spoločnosti na bezpečnost aktív a ISMS.
  - Spravovanie bezpečnostne relevantných zmien je jednoduchšie, pretože môže využiť dodatočné informácie získané v detailnom ohodnotení rizík.
- **Nevýhodou** tohto prístupu je to, že vyžaduje významne veľa času, úsilia a skúseností, aby boli získané použiteľné výsledky.

Kombinovaný prístup k ohodnoteniu rizík

- **Kombinovaný prístup:**
  - Tento prístup zahrňuje **najprv** identifikáciu takých aktív v rámci rozsahu ISMS, ktoré sú potenciálne vysoko rizikové alebo sú kritické pre obchodné činnosti.
  - Na základe týchto výsledkov sa potom aktíva v rámci rozsahu ISMS kategorizujú do skupiny aktív, ktoré vyžadujú prístup **detailného ohodnotenia rizík** s cieľom dosiahnutia primeranej ochrany, a do skupiny aktív, pre ktoré je postačujúci prístup **základného ohodnotenia rizík**.
  - Kombinovaný prístup využíva výhody základného aj detailného ohodnotenia rizík.
  - Následne, kombinovaný prístup ponúka dobrú rovnováhu medzi minimalizáciou času a úsilia potrebných na stanovenie opatrení, pričom stále zaisťuje všetkým aktívam spoločnosti primerané ohodnotenie a ochranu.
- Okrem **kombinácie výhod** prístupov základného a detailného ohodnotenia rizík má kombinovaný prístup ohodnotenia rizík výhodu v tom, že náklady a zdroje na ohodnotenie môžu byť použité tam, kde budú najužitočnejšie.
- **Nevýhodou** kombinovaného prístupu je to, že môže viesť k nepresným výsledkom v prípade, že identifikácia vysoko rizikových informačných systémov je nesprávna. To znamená, že systém, pre ktorý je potrebné detailné ohodnotenie rizík, bol uvažovaný iba pre základné ohodnotenie rizík.

ĎAKUJEM
ZA POZORNOSŤ

TEŠÍM SA NA ĎALŠIE STRETNUTIA