Informačná bezpečnosť (7)

Informačná bezpečnosť na úrovni organizácie
Analýza rizík a ISMS

Obsah

- Dôvody riešenia IB v organizácii (Zákon o ochrane osobných údajov)
- Ako postupovať
- Analýza rizík podľa normy ISO/IEC 27005
- ISMS (ISO/IEC 27001 a 2)

Dôvody

- Objektívna potreba riešiť IB
- Legislatíva (zákon č. 136/2014 Z. z. o ochrane osobných údajov)
- Zákon o ISVS (č. 275/2006) a výnos MF SR 55/2014 o štandardoch pre ISVS
- Zákon o ochrane utajovaných skutočností (215/2004 Z.z.)
- Zákon o elektronickom podpise (215/2002 Z.z.)
- Zákon **45**/2011 o kritickej infraštruktúre
- Iný zákon
- Revízia bezpečnostného projektu
- Zavádzanie Systému manažmentu IB (ISMS)
- Záujem o certifikáciu
- Iné

Zákon 136/2014

§ 19
Zodpovednosť za bezpečnosť osobných údajov

(1) Za bezpečnosť osobných údajov zodpovedá prevádzkovateľ.

Prevádzkovateľ je povinný chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania. Na tento účel prijme primerané technické, organizačné a personálne opatrenia (ďalej len „bezpečnostné opatrenia“) zodpovedajúce spôsobu spracúvania osobných údajov, pričom berie do úvahy najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných osobných údajov, ako aj rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému.

Zákon 136/2014

§ 19
Zodpovednosť za bezpečnosť osobných údajov

(2) Bezpečnostné opatrenia podľa odseku 1 prevádzkovateľ zdokumentuje v bezpečnostnom projekte informačného systému (ďalej len „bezpečnostný projekt“), ak

a) v informačnom systéme prepojenom s verejne prístupnou počítačovou sieťou spracúva osobitné kategórie osobných údajov podľa § 13, alebo

b) informačný systém slúži na zabezpečenie verejného záujmu podľa § 3 ods. 1; ustanovenie § 20 sa pri vypracúvaní bezpečnostného projektu nepoužije len vtedy, ak pre konkrétny prípad je tu súčasne povinnosť vypracovať bezpečnostný projekt podľa osobitného predpisu.

Zákon 136/2014

§ 19
Zodpovednosť za bezpečnosť osobných údajov

(3) Prevádzkovateľ je povinný bez zbytočného odkladu zabezpečovať aktualizáciu bezpečnostných opatrení prijatých podľa odsekov 1 a 2 tak, aby zodpovedala prijatým zmenám pri spracúvaní osobných údajov, a to až do ukončenia spracúvania osobných údajov v informačnom systéme.
(4) Na požiadanie úradu prevádzkovateľ preukáže rozsah a obsah bezpečnostných opatrení podľa odsekov 1a 2.

Zákon 136/2014

§ 20

Bezpečnostný projekt

(1) Bezpečnostný projekt vymedzuje rozsah a spôsob bezpečnostných opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.

(2) Bezpečnostný projekt vypracúva prevádzkovateľ v súlade s bezpečnostnými štandardmi, právnymi predpismi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná.

(3) Rozsah a dokumentáciu bezpečnostných opatrení ustanoví všeobecne záväzný právny predpis, ktorý vydá úrad.

Podrobnosti o ochrane osobných údajov

- Vyhláška Úradu na ochranu osobných údajov SR č. 164/2013 Z.z. o rozsahu a dokumentácii bezpečnostných opatrení
- Novelizovaná Vyhláškou Úradu na ochranu osobných údajov SR č. 117/2014 Z.z.
- Podstatné požiadavky:
  - Primeranosť opatrení
  - Rozlišuje ručné a automatizované spracovanie osobných údajov
  - V prípade automatizovaného spracovania
    - Antivírová ochrana
    - Integrita informačného systému
    - Zálohovanie osobných údajov
  - Nerealistické požiadavky na riadenie prístupu (oprávnení všetko, neoprávnení nič)
  - Dokumentácia prijatých bezpečnostných opatrení
    - Vzťahujú sa na celý životný cyklus osobných údajov
    - Sú možné referencie na iné dokumenty

Podrobnosti o ochrane osobných údajov

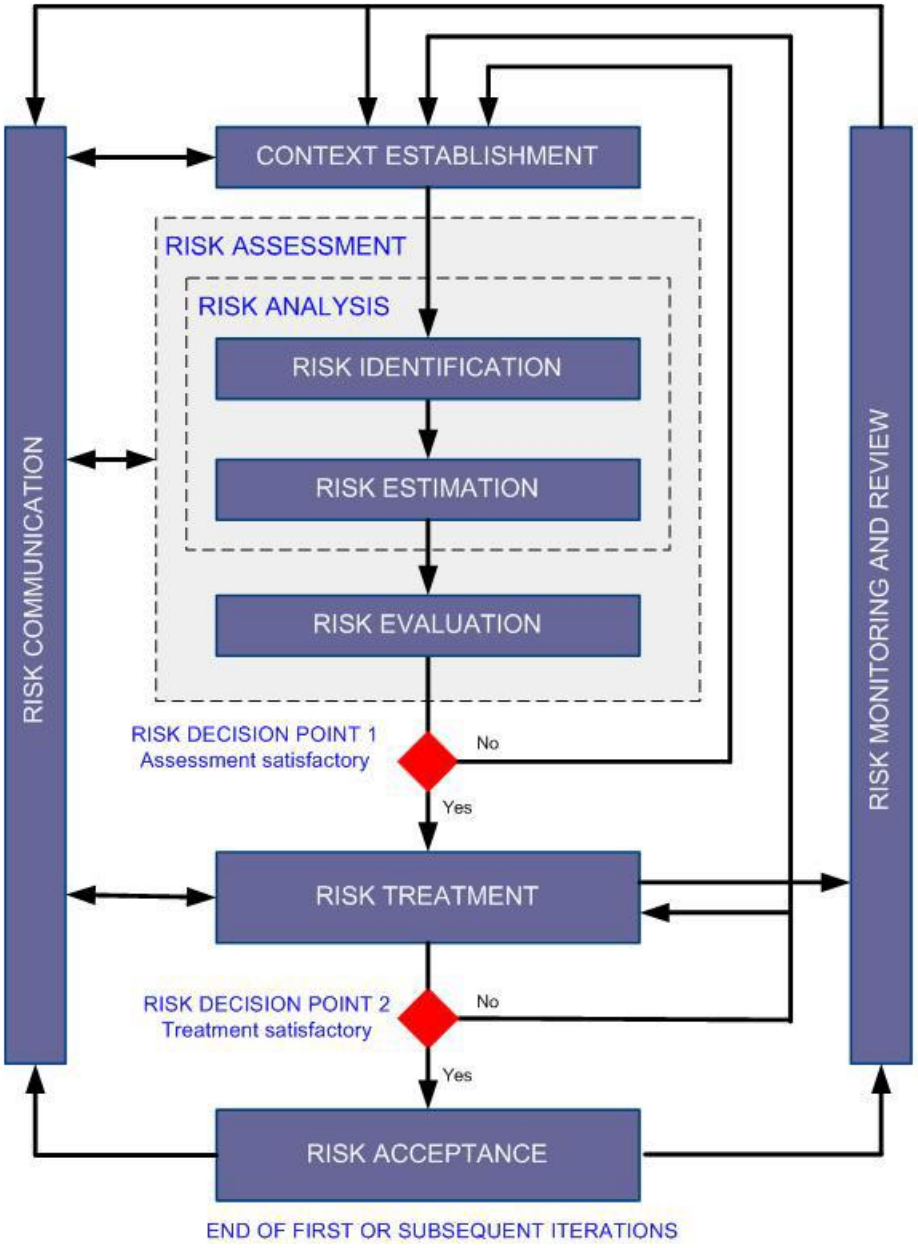
- § 3 výber bezpečnostných opatrení (príloha)
- § 4 bezpečnostné opatrenia zo zoznamu sú povinné, ak nerobíte analýzu rizík
- §5 bezpečnostný projekt IS
  - Názov IS
  - Bezpečnostný zámer
  - Analýza bezpečnosti IS
  - Bezpečnostná smernica
- Bezpečnostný zámer je *de facto* Politika informačnej bezpečnosti podľa ISO/IEC 27001 a 27002
- Analýza bezpečnosti IS je v skutočnosti analýza rizík podľa ISO/IEC 27005
- Text § 5 a prílohy ukážeme na záver

Postup (zovšeobecnený)

- Rôzne zákony a štandardy definujú požiadavky na rozsah a úroveň bezpečnostných riešení, podstata však je podobná:
  - Zistiť, čo systému hrozí,
  - čo je vlastník povinný spraviť,
  - koľko na to má prostriedkov,
  - akú úroveň bezpečnosti potrebuje/môže si dovoliť,
  - vyhodnotiť riziká,
  - navrhnúť a implementovať opatrenia,
  - spravovať riziká,
  - napísať bezpečnostnú dokumentáciu,
  - robiť audit (pravidelne alebo potreby),
  - prípadne zaviesť systém riadenia informačnej bezpečnosti
  - Nechať si certifikovať systém

Začíname – analýza rizík

- Základ IB = manažment rizík
  - Určenie kontextu
  - Analýza rizík
  - Ohodnotenie rizík
  - Správa rizík (návrh a implementácia opatrení)
- Cyklický proces
- Použiteľné štandardy
  - Common criteria (ISO/IEC 15408)
  - ISO/IEC 27000, 27001, 27002, 27005
- Nasledujúci obrázok je prevzatý z normy ISO/IEC 27005


CONTEXT ESTABLISHMENT
RISK ASSESSMENT
RISK ANALYSIS
RISK IDENTIFICATION
RISK ESTIMATION
RISK EVALUATION
RISK DECISION POINT 1
Assessment satisfactory
No
Yes
RISK TREATMENT
RISK DECISION POINT 2
Treatment satisfactory
No
Yes
RISK ACCEPTANCE
END OF FIRST OR SUBSEQUENT ITERATIONS
RISK COMMUNICATION
RISK MONITORING AND REVIEW

Základné pojmy – opakovanie

- Aktívum = všetko čo pre organizáciu má cenu a vyžaduje si ochranu
- Hrozba
- Nositeľ hrozby
- Útočník
- Útočný potenciál
- Zraniteľnosť
- Pravdepodobnosť naplnenia hrozby
- Dopad hrozby
- Riziko = možnosť straty (zisku) nejakej hodnoty

Základné pojmy – opakovanie

- **information security risk** = potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization
- Hodnota rizika = pravdepodobnosť *dopad; niekedy všeobecnejšie (funkcia dopadu a pravdepodobnosti hrozby)
- Opatrenie = technický prostriedok, organizačné, programové alebo iné riešenie, ktoré znižuje pravdepodobnosť naplnenia hrozby alebo jej dopad

Manažment rizík

- Stanovenie kontextu
  - Prečo sa zaoberáme rizikami
  - Z toho vyplynú ciele, rozsah a úroveň manažmentu rizík
- Na začiatku potrebujeme určiť tri základné kritériá
  - ohodnotenia rizík (risk evaluation criteria)
  - na ohodnotenie dopadu (impact criteria)
  - a hranicu akceptovateľného rizika (risk acceptance criteria)

Kritériá ohodnotenia rizík

- Kritériá ohodnotenia rizík závisia od toho, ako dôležité je aktívum pre organizáciu a aké dôsledky by pre ňu malo jeho narušenie, výpadok alebo strata
- podrobnejšie
  - Strategickej hodnoty aktív (procesov) pre organizáciu
  - Kritickosti daných informačných aktív
  - Právnych a regulačných požiadaviek, zmluvných záväzkov
  - Dôležitosti dostupnosti, integrity a dôvernosti aktív
  - Požiadaviek/očakávaní zúčastnených na ochranu aktív
  - Možných negatívnych dopadov na dobré meno organizácie
- Môžu sa použiť na stanovenie priorít na riešenie rizík

Kritériá ohodnotenia dopadu

- Úroveň klasifikácie dotknutého informačného aktíva
- Narušenie informačnej bezpečnosti organizácie
- Narušenie fungovania systému (domáceho aj spolupracujúcich)
- Strata obchodných príležitostí a finančná ujma
- Narušenie plánov a termínov
- Poškodenie reputácie organizácie
- Porušenie právnych, regulačných a zmluvných požiadaviek

Hranice akceptovateľných rizík

- Nie všetky riziká sa podarí celkom eliminovať, potrebujeme vedieť, čím sa ešte máme zaoberať a ktoré riziká sú akceptovateľné
- Čo zohľadňujú hranice akceptovateľných rizík
  - Dopad na poslanie organizácie
  - Právne a regulačné aspekty
  - Fungovanie IKT systémov
  - Technológie
  - Náklady na opatrenia
  - Spoločenské a humanitárne faktory
- Nemusia byť univerzálne
- Nemusia mať trvalú platnosť
- Viacero úrovní, dodatočné podmienky na akceptáciu

Rozsah

- Môže byť rôzny
- Závisí od dôvodu, prečo sa zavádza manažment rizík a cieľa, ktorý sa tým sleduje
- IT aplikácia, systém, proces, časť organizácie, celá organizácia
- Príklady: subsystém pracujúci s utajovanými skutočnosťami, ochrana osobných údajov, CA, systém komunikujúci s externým systémom

Stanovenie/vyhodnotenie rizík

- Stanovenie rizík pozostáva z
  - Identifikácie rizík
  - Analýzy rizík
  - Ohodnotenia rizík
- Stanovenie rizík (risk assessment) znamená
  - Stanovenie hodnôt informačných aktív
  - Identifikácia relevantných hrozieb a zraniteľností
  - Určenie existujúcich opatrení a ich stanovenie vplyvu na identifikované riziká
  - Stanovenie potenciálnych dôsledkov
  - Usporiadanie rizík podľa priorít daných kritériami

Identifikácia rizík

- Týka sa aj rizík, ktorých zdroj je mimo organizácie, alebo je neznámy
  - Inventarizácia aktív
  - Identifikácia hrozieb
  - Identifikácia existujúcich opatrení
  - Identifikácia zraniteľností

Aktíva

- Primárne
  - Procesy prostredníctvom ktorých organizácia napĺňa svoje poslanie
  - Informácie
- Sekundárne
  - Hardware
  - Software
  - Siete
  - Personál
  - Sídlo
  - Organizačná štruktúra

Hrozby

- Fyzické poškodenie
- Prírodné živly
- Strata podstatných služieb
- Radiácia
- Kompromitácia informácie
- Technické poruchy
- Neoprávnená činnosti
- Kompromitácia funkcionality
- Ľudská činnosť
  - Hackeri
  - Počítačová kriminalita
  - Teroristi
  - Priemyselná špionáž
  - Vlastní zamestnanci
- Podrobnejší katalóg je v prílohe normy ISO/IEC 27005 - ukážka

Type	Threats	Origin
Physical damage	Fire	A, D, E
	Water damage	A, D, E
	Pollution	A, D, E
	Major accident	A, D, E
	Destruction of equipment or media	A, D, E
	Dust, corrosion, freezing	A, D, E
Natural events	Climatic phenomenon	E
	Seismic phenomenon	E
	Volcanic phenomenon	E
	Meteorological phenomenon	E
	Flood	E
Loss of essential services	Failure of air-conditioning or water supply system	A, D
	Loss of power supply	A, D, E
	Failure of telecommunication equipment	A, D
Disturbance due to radiation	Electromagnetic radiation	A, D, E
	Thermal radiation	A, D, E
	Electromagnetic pulses	A, D, E
Compromise of information	Interception of compromising interference signals	D
	Remote spying	D
	Eavesdropping	D
	Theft of media or documents	D
	Theft of equipment	D
	Retrieval of recycled or discarded media	D
	Disclosure	A, D
	Data from untrustworthy sources	A, D
	Tampering with hardware	D
	Tampering with software	A, D
	Position detection	D

Zraniteľnosti

- Vzťahujú sa na jednotlivé aktíva a umožňujú, aby sa voči aktívam uplatnili hrozby
- Existujú v nasledujúcich oblastiach
  - Organization
  - Processes and procedures
  - Management routines
  - Personnel
  - Physical environment
  - Information system configuration
  - Hardware, software or communications equipment
  - Dependence on external parties

Príklad zraniteľností – personál

Vulnerability	Threat
Absence of personnel	Breach of personnel availability
Inadequate recruitment procedures	Destruction of equipment or media
Insufficient security training	Error in use
Incorrect use of software and hardware	Error in use
Lack of security awareness	Error in use
Lack of monitoring mechanisms	Illegal processing of data
Unsupervised work by outside or cleaning staff	Theft of media or documents
Lack of policies for the correct use of telecommunications media and messaging	Unauthorised use of equipment

Identifikácia následkov

- Skúmajú sa scenáre a ich dopady najmä z hľadiska straty integrity, dostupnosti a dôvernosti informácií
- Konkrétnejší pohľad:
  - Čas na vyšetrovanie a opravu
  - Strata pracovného času
  - Strata príležitostí
  - Zdravie a bezpečnosť
  - Finančné náklady na odborníkov schopných opraviť poškodený systém
  - Poškodenie reputácie a dobrého mena

Analýza rizík

- Metodológia
  - Kvalitatívna alebo
  - Kvantitatívna
- Kvalitatívna
  - Pravdepodobnosti a dopady hrozieb, riziká sú vyjadrené deskriptívne (vysoké, stredné, nízke)
  - Častokrát nemáme k dispozícii presné hodnoty
  - Niektoré veci sa kvantitatívne nedajú merať
  - Môže byť prvým krokom ku kvantitatívnej analýze rizík
- Kvantitatívna – numerické hodnoty

Analýza rizík (2)

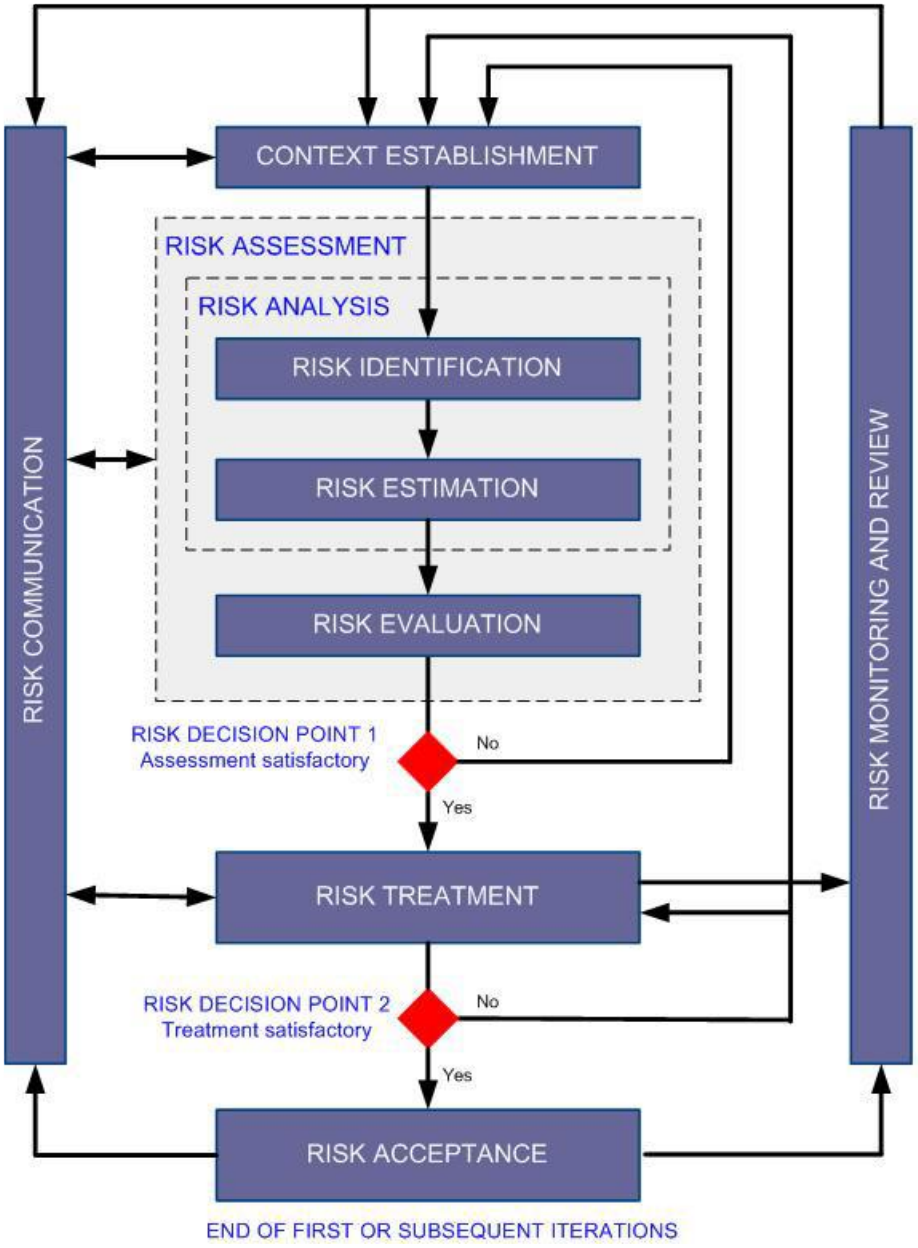
- Stanovenie dôsledkov
- Stanovenie pravdepodobnosti incidentov
  - Štatistiky
  - Útočný potenciál
  - Zraniteľnosti
  - Existujúce opatrenia
  - Vplyv prostredia (rizikové faktory)
- Určenie/výpočet rizík

Príklad metodiky výpočtu rizík

Pravdepodob. Dopad	nízka	stredná	vysoká
nízky	nízke	nízke	stredné
stredný	nízke	stredné	vysoké
vysoký	stredné	vysoké	vysoké

Ohodnotenie rizík

- Vyčíslené hodnoty rizika sú podkladom pre ohodnotenie rizík = stanovenie významnosti rizík pre organizáciu
- Zohľadňuje sa
  - Relevantnosť bezpečnostných aspektov informácie
  - Význam procesov podporovaných aktívami
  - Kumulatívny efekt čiastkových rizík
  - Hranica akceptovateľného rizika
- Výsledok
  - Zoznam rizík podľa priorít riešenia


CONTEXT ESTABLISHMENT
RISK ASSESSMENT
RISK ANALYSIS
RISK IDENTIFICATION
RISK ESTIMATION
RISK EVALUATION
RISK DECISION POINT 1
Assessment satisfactory
No
Yes
RISK TREATMENT
RISK DECISION POINT 2
Treatment satisfactory
No
Yes
RISK ACCEPTANCE
END OF FIRST OR SUBSEQUENT ITERATIONS
RISK COMMUNICATION
RISK MONITORING AND REVIEW

Ošetrenie rizík

- Čo sa dá robiť s rizikami:
  - Modifikácia rizika
  - Zachovanie rizika
  - Vyhnutie sa riziku
  - Zdieľanie rizika

Modifikácia rizika

- Podstata: eliminovať alebo aspoň znížiť riziko
- Ako: zavedením, alebo modifikáciou opatrení
- Obmedzenia
  - Time constraints
  - Financial constraints
  - Technical constraints
  - Operational constrains
  - Cultural constraints
  - Ethical constraints
  - Environmental constraints
  - Legal constraints
  - Ease of use
  - Personnel constraints
  - Constraints for integrating new and existing controls

Zachovanie rizika, vyhnutie sa riziku a zdieľanie rizika

- **Zachovanie rizika** – len v prípade, keď je riziko akceptovateľné
- **Vyhnutie sa riziku**: prijatie iného riešenia, ako je to, ktoré viedlo k riziku
- **Zdieľanie rizika**
  - Zapojenie tretej strany
  - Nedá sa celkom preniesť (zákazníci vnímajú incident ako chybu organizácie a nie jej partnera)
  - typické riešenie – poistenie

Akceptovanie rizika

- Popísané aktivity neeliminovali všetky riziká, ostali zvyškové riziká
- O zvyškových rizikách treba vedieť a prijať rozhodnutie, čo sa s nimi bude robiť (správa rizík)
- Kto: vrcholový manažment
- Niektoré riziká nemusí akceptovať

Informovanie o rizikách

- O rizikách by mali vedieť manažéri, ale aj ostatní, ktorých sa to týka
- Čo:
  - Existencia
  - Podstata
  - Forma
  - Pravdepodobnosť
  - Závažnosť
  - Ošetrenie
  - Akceptovateľnosť
- Komunikácia o rizikách musí byť obojstranná

Čo chceme dosiahnuť komunikáciou rizík?

- To provide assurance of the outcome of the organization's risk management
- To collect risk information
- To share the results from the risk assessment and present the risk treatment plan
- To avoid or reduce both occurrence and consequence of information security breaches due to the lack of mutual understanding among decision makers and stakeholders
- To support decision-making
- To obtain new information security knowledge
- To co-ordinate with other parties and plan responses to reduce consequences of any incident
- To give decision makers and stakeholders a sense of responsibility about risks
- To improve awareness

Monitoring a revízia rizík

- Podmienky sa môžu meniť
- Ohodnotenie rizík a prijaté opatrenia nemusia byť aktuálne
- Čo by sa malo monitorovať
  - New assets that have been included in the risk management scope
  - Necessary modification of asset values, e.g. due to changed business requirements
  - New threats that could be active both outside and inside the organization and that have not been assessed
  - Possibility that new or increased vulnerabilities could allow threats to exploit these new or changed vulnerabilities
  - Identified vulnerabilities to determine those becoming exposed to new or re-emerging threats
  - Increased impact or consequences of assessed threats, vulnerabilities and risks in aggregation resulting in an unacceptable level of risk
  - Information security incidents

Monitoring, revízie a vylepšovanie manažmentu rizík

- Cieľ: udržanie potrebnej úrovne manažmentu rizík
- Manažment môže byť v poriadku, môžu sa zmeniť externé podmienky
  - Legal and environmental context
  - Competition context
  - Risk assessment approach
  - Asset value and categories
  - Impact criteria
  - Risk evaluation criteria
  - Risk acceptance criteria
  - Total cost of ownership
  - Necessary resources

Čo ďalej?

- Nezaoberali sme sa detailne opatreniami, niektoré riziká si môžu vyžadovať komplikované opatrenia (napr. havarijné plány, plány obnovy)
- Ak je cieľom systematický prístup k riešeniu informačnej bezpečnosti, tak v organizácii má zmysel uvažovať o systéme manažmentu informačnej bezpečnosti
- Analýza rizík – základ/súčasť bezpečnostných projektov
- Vychádzali sme zo štandardu ISO/IEC 27005 **Information technology — Security techniques — Information security risk management**