Informačná bezpečnosť (7)

Informačná bezpečnosť na úrovni organizácie
Analýza rizík

Obsah

- Dôvody riešenia IB v organizácii
- Ako postupovať
- Analýza rizík podľa normy ISO/IEC 27005
-

Dôvody

- Objektívana potreba riešiť IB
- Legislatíva (zákon č. 428/2002 Z. z. o ochrane osobných údajov)
- Zákon o ISVS (č. 275/2006) a výnos MF SR 312/2010 o štandardoch pre ISVS
- Zákon o ochrane utajovaných skutočností (215/2004 Z.z.)
- Zákon o elektronickom podpise (215/2002 Z.z.)
- Iný zákon
- Revízia bezpečnostného projektu
- Zavádzanie Systému manažmentu IB
- Záujem o certifikáciu
- Iné

Postup (zovšeobecnený)

- 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 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 27000-27005
-

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 = 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 určiťkritériá
  - 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
  - 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
- Narušenie fungovania systému (domáceho aj spolupracujúcich)
- Strata obchodných príležitostí a finančná ujma
- Narušenie plánov a termínov
- Poškodenie reputácie
- Porušenie právnych, regulačných a zmluvných požiadaviek
-
-

Hranice akceptovateľných rizík

- Čo zohľadňujú
  - 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, podmienky na akceptáciu

Rozsah

- Môže byť rôzny
- Závisí od dôvodu, prečo sa zavádza manažment rizík a cieľa, ktorý sa 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 rizík

- Stanovenie rizík 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
- Stanovenie rizík pozostáva z
  - Identifikácie rizík
  - Analýzy rizík
  - Ohodnotenia rizík

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
  - Obchodné (business) procesy
  - 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
-

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 výpočtu rizík

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

Ohodnotenie rizík

- Vyčíslené riziká 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

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 tým chceme dosiahnuť?

- 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 vyžadovaťkomplikované 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**
-