BEZPEČNOSŤ INFORMÁCIÍ – JEJ DÔLEŽITOSŤ A MOŽNOSTI ZABEZPEČENIA

Ing. Gabriela BOGDANOVSKÁ

Pracovisko: ***Ústav riadenia a informatizácie výrobných procesov, Fakulta BERG, TU Košice***
Adresa: ***B. Němcovej 3,040201 Košice, Slovensko***
Tel.: ***00421 55 6025170***
E-mail: *gabriela.bogdanovska@tuke.sk*

Abstract

Príspevok stručne popisuje ako zabezpečiť bezpečnosť informácií pomocou vytvorenia, zavedenia, následného certifikovania, udržiavania a neustáleho zlepšovania systému manažérstva informačnej bezpečnosti v organizácii podľa medzinárodnej normy ISO/IEC 27001:2005 „Informačné technológie. Zabezpečovacie techniky. Systémy manažérstva informačnej bezpečnosti. Požiadavky“, ktorá nahrádza normu BS 7799-2:2002.

This article description the basic objective of the standard is to help creating, implementing and maintenance an effective information management system, using a continual improvement approach. This standard is ISO 27001 “Information Security Management. Specification With Guidance for Use”, is the replacement for BS 7799-2:2002.

Key words

Informačná bezpečnosť, norma ISO 27001:2005, implementácia ISMS

Information Security Management, Standard ISO 27001:2005, implementation ISMS

Úvod

V súčasnosti sa neustále rozvíja informatizácia spoločnosti až do takej miery, že informácie sú najvýznamnejšie aktíva organizácie. V mnohých organizáciách sú jej najvýznamnejším produktom, preto je potrebné zabezpečiť ich ochranu pri uchovávaní, aktualizácii a poskytovaní. Informácie je treba chápať ako dáta použité pri rozhodovaní. Môžu mať rôznu formu, rôzne komunikovanú, napr. tlačenú, písanú, elektronickú alebo ústnu formu – know-how.

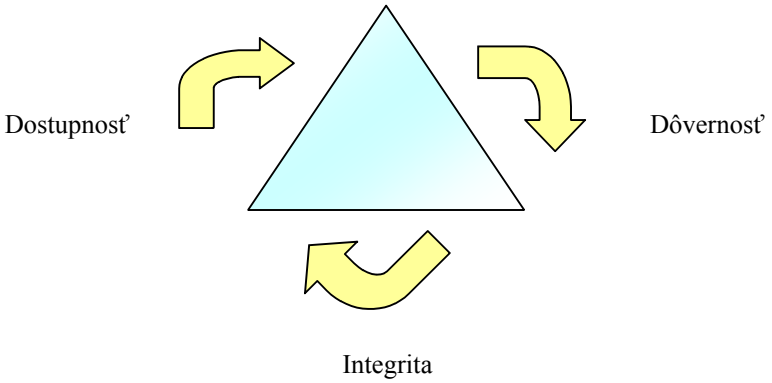
Cieľom manažmentu organizácií je zabezpečiť maximálnu bezpečnosť informácií, pretože ich zneužitie predstavuje rozsiahlu hrozbu. Pri ich zneužití môže dôjsť k strate kontinuity činnosti organizácie, maximalizácii obchodných strát a minimalizácii návratnosti investícií.

Návod na predchádzanie tejto nežiaducej situácii je rozpracovaný v norme STN ISO/IEC 27OO1:2006 „Informačné technológie. Zabezpečovacie techniky. Systémy manažérstva informačnej bezpečnosti. Požiadavky“.

Norma ISO 27001:2005 Systém manažérstva informačnej bezpečnosti

Norma popisuje systém manažérstva informačnej bezpečnosti – *Information Security Management System* (ISMS), založený na podobných princípoch ako systém manažérstva kvality podľa normy ISO 9001:2005 a systém environmentálneho manažérstva podľa normy ISO 14001:2004. Cieľom tohto systému je riadiť procesy narábania s informáciami pri zabezpečení troch prvkov:

- Dôvernosti – *confidentiality* – t.j. zabezpečenie toho, že informácie sú poskytnuté a prístupne len oprávneným osobám.
- Dostupnosti – *availability* – t.j. zabezpečenie toho, že k informáciám majú neobmedzený prístup len oprávnené osoby. Inými slovami, správne informácie, správnym ľuďom v správny čas.
- Integrity – *integrity* – t.j. zabezpečenie správnosti a úplnosti informácií z hľadiska obsahu a formy.



Obr. 1 Prvky pre ochranu údajov

Je potrebné si uvedomiť, že pre zabezpečenie všetkých troch oblastí musí organizácia nazerať na informačnú bezpečnosť ako na celok, zoskupujúci dostupnosť, dôvernosť ale aj integritu všetkých informácií (Obr.1).

Často je ISMS nesprávne chápaný ako systém zaoberajúci sa len bezpečnosťou informačného systému alebo informačných technológií. Systém informačnej bezpečnosti je určený pre všetky typy organizácií bez rozdielu zamerania či veľkosti. Môžu ho zaviesť a dať si certifikovať výrobné, obchodné, servisné, montážne, či poradenské a vzdelávacie organizácie zo všetkých oblastí priemyslu a služieb, čiže aj organizácie, ktoré informačné technológie vôbec nepoužívajú.

Dôvody pre zavedenie systému informačnej bezpečnosti

Častou motiváciou pre zavedenie systému manažérstva informačnej bezpečnosti je nutnosť vyhovieť legislatívnym požiadavkám, a tak ochrániť organizáciu pred prípadnými finančnými postihmi. Je množstvo predpisov súvisiacich s bezpečnosťou informácií. Medzi najvýznamnejšie patrí:

- Obchodný zákonník č. 513/1991 Zb.,
- Zákon č. 428/2002 Z.z. o ochrane osobných údajov,
- Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností,
- Zákon č. 215/2002 Z. z. o elektronickom podpise,
- Zákon č. 211/2000 Z.z. o slobodnom prístupe,
- a ďalšie.

Ďalším dôvodom zavedenia systému manažérstva informačnej bezpečnosti je uvedomenie si prínosov, a to:

- zmapovanie informačnej štruktúry spoločnosti, vrátane infraštruktúry, budov, prostredia so všetkými praktickými aspektmi, od poplašného systému, cez požiarnu ochranu, až po kontrolu prístupu,
- zefektívnenie a vytvorenie chýbajúcich procesov nielen v oblasti informačnej bezpečnosti,
- uvedomenie si bezpečnostných rizík,
- začatie s aktívnou a efektívnou ochranou pred rizikovými faktormi,
- ochrana životných firemných hodnôt –podstaty organizácie,
- priebežná optimalizácia systému – pravidelné audity,
- nižšie náklady a vyššia produkciu,
- konkurenčná výhoda,
- rozšírenie okruhu zákazníkov,
- dôvera domáceho aj svetového trhu.

Súvisiace normy

Oblasť riadenia procesov informačnej bezpečnosti je popísaná skupinou medzinárodných noriem, ktoré sa líšia rozsahom a účelom.

Norma ISO/IEC 27001:2005 a jej predchodkyňa BS 7799-2:2002 patria do skupiny noriem, ktoré popisujú základné požiadavky systému informačnej bezpečnosti a používajú sa pri certifikačných auditoch.

Na tieto normy nadväzuje norma ISO/IEC 17799:2005 (predchodkyňa BS 7799-1:2000) „Informačné technológie. Zabezpečovacie techniky. Pravidla dobrej praxe manažérstva informačnej bezpečnosti“, ktorá obsahuje odporúčania a všeobecné princípy pre stanovenie, zavedenie, udržiavanie a zlepšovanie systému manažérstva informačnej bezpečnosti. Táto norma tvorí návod k norme ISO/IEC 27001:2005, preto došlo 10. júla 2007 k jej prečíslovaniu na ISO/IEC 27002.2005.

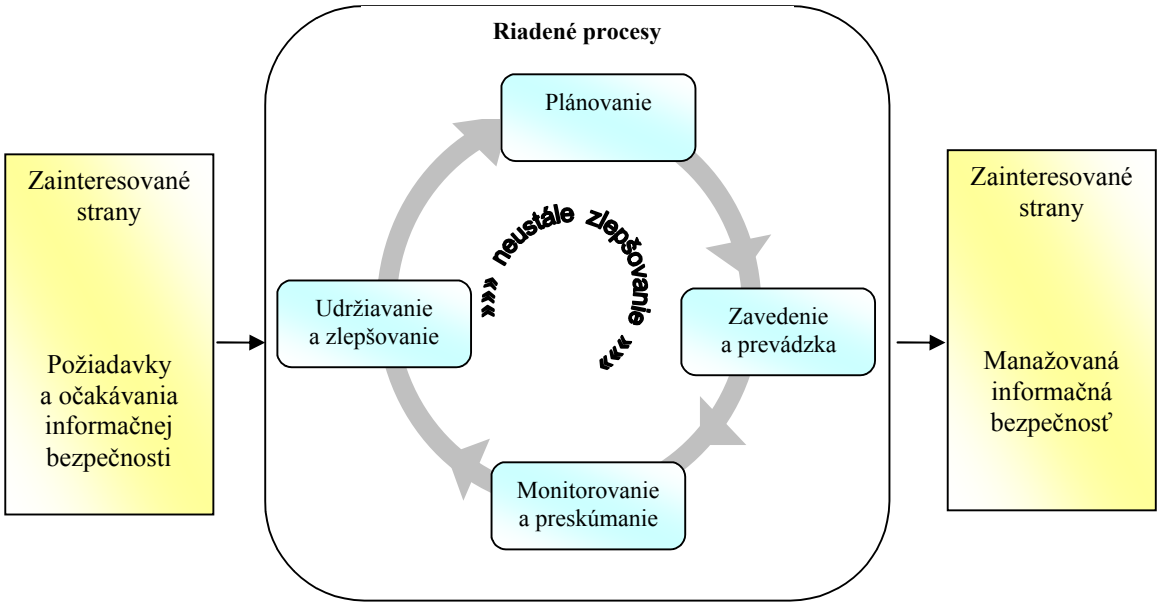
Ďalšiu skupinu súvisiacich noriem tvoria smernice pre riadenie bezpečnosti informačných technológií – ISO TR 13335 1-5 „„Informačné technológie. Návod pre manažérstvo bezpečnosti IT“ a ďalšie menej známe normy, ako napr. ISO/IEC 15408:2005 „Kritéria hodnotenia bezpečnosti IT “.

Implementácia systému manažérstva informačnej bezpečnosti

Pred samotnou implementáciou systému manažérstva informačnej bezpečnosti si organizácia musí ujasniť niekoľko hľadísk:

- prečo chce či musí systém manažérstva informačnej bezpečnosti zaviesť,
- ktorých oblastí činnosti organizácie sa bude systém manažérstva informačnej bezpečnosti týkať,
- v akom rozsahu bude systém zavedený, ktoré činnosti zahrnie,
- aké bude rozdelenie zodpovednosti a právomocí jednotlivých zamestnancov,
- aký bude postup a spôsob zavedenia systému.

Je potrebné si uvedomiť, že implementácia systému je kontinuálny proces, nie jednorazový projekt, inak hrozí veľké riziko, že po zavedení systému sa investície nevrátia. Pri zavádzaní systému manažérstva informačnej bezpečnosti treba vychádzať z Demingovho PDCA cyklu (Plan Do Check Act), ktorý je zobrazený na Obr.2.



Obr. 2 Aplikácia PDCA cyklu v systéme manažérstva informačnej bezpečnosti

Plan	Plánovanie	-	bezpečnostnej politiky, cieľov, procesov a procedúr relevantných pre riadenie rizika a zlepšovanie informačnej bezpečnosti, s cieľom priniesť výsledky v súlade s celkovou politikou a cieľmi organizácie.
Do	Zavedenia a prevádzka	-	politiky ISMS, opatrení, procesov a postupov.
Check	Monitorovanie a preskúmanie	-	vhodnosť procesov voči politike ISMS, cieľom a praktickým skúsenostiam.
Act	Udržiavanie a zlepšovanie	-	vykonávaním nápravných a preventívnych činnosti, založených na výsledkoch z interných auditov ISMS, preskúmaniach manažmentu alebo iných relevantných informáciách.

Zavádzanie systému manažérstva informačnej bezpečnosti prebieha v prvej fáze v týchto etapách (obr.3):

1. **Stanovenie rozsahu, stratégie a cieľa**

   Pred samotným stanovením a vypracovaním dokumentu, ktorý popisuje rozsah, stratégiu a ciele systému manažérstva informačnej bezpečnosti je potrebné vykonať analýzu súčasného stavu bezpečnosti informácií. V tejto etape sa taktiež určí zodpovedný pracovník za informačnú bezpečnosť.

2. **Vypracovanie analýzy rizík**

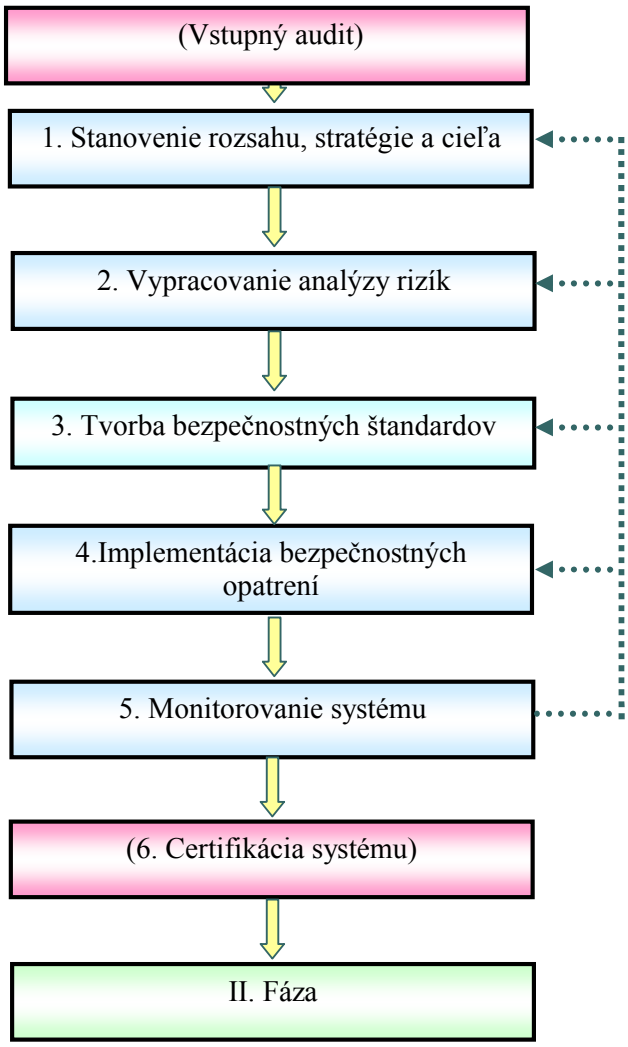
   Táto etapa je z celého systému najdôležitejšia. Organizácia musí zvoliť vhodnú metódu pre posúdenie rizík a analyzovať rizika, ktoré najviac ohrozujú jej činnosť.

   Súčasťou tejto etapy je taktiež vytvorenie:

   - plánu zvládnutia rizík – Risk Treatment Plan,
   - prehlásenie o aplikovateľnosti – Statement of Applicability.

   Organizácia v pláne zvládnutia rizík popisuje, ktoré riziká bude riadiť a ktoré riziká sú akceptovateľné.

   Prehlásenie o aplikovateľnosti obsahuje zoznam všetkých aplikovateľných aj neaplikovateľných opatrení požadovaných normou a popis ich realizácie.



Obr. 3 Schéma implementácie systému manažérstva informačnej bezpečnosti

3. Tvorba bezpečnostných štandardov

Na etapu vypracovania rizík nadväzuje etapa tvorby bezpečnostných štandardov/ smerníc. Rozsah a obsah smerníc závisí od typu organizácie, informačného systému a identifikovaných rizík. Súčasťou tvorby bezpečnostných štandardov je aj vypracovanie bezpečnostnej politiky organizácie a jej integrácia do celkovej politiky organizácie. Dôležitou súčasťou tejto etapy je aj preškolenie a oboznámenie pracovníkov a zainteresovaných strán so systémom informačnej bezpečnosti.

4. Implementácia bezpečnostných opatrení

Cieľom tejto etapy je dosiahnuť požadovanú informačnú bezpečnosť, napr. zmenou alebo verifikáciou niektorých procesov, technológií a pod.

5. Monitorovanie systému

Monitorovanie a následné vyhodnocovananie výsledkov musí prebiehať v pravidelných intervaloch, napr. aj formou auditov a rôznych testov. S touto etapou súvisí aj evidencia

a hodnotenie záznamov o informačnej bezpečnosti, ktoré slúžia ako podklad pre pravidelné preskúmanie fungovania systému.

6. Certifikácia

Po zavedení systému manažérstva informačne bezpečnosti môže organizácia overiť úplnosť a účinnosť systému pomocou certifikácie. V prípade úspešného certifikačného auditu získa organizácia certifikát, čím preukáže svojím zákazníkom a dodávateľom, že aktívne riadi svoje rizika v oblasti informačnej bezpečnosti.

Tak ako aj pri budovaní iných manažérskych systémov (kvality, environmentu) aj pri ISMS je platnosť certifikátu obmedzená na 3 roky. Po jeho získaní – skončení prvej fázy, nasleduje druhá fáza, ktorá je udržiavacia a zlepšovacia alebo tzv. pocertifikačná. Pred uplynutím platnosti certifikátu (až 6 mesiacov) má organizácia právo rozhodnúť či požiada o recertifikáciu, alebo bude udržiavať systém bez recertifikácie.

Záver

Norma ISO/IEC 27OO1:2005 je celosvetovo overeným návodom pre implementáciu systému manažérstva informačnej bezpečnosti. Organizácie, ktoré sa rozhodnú zabezpečiť ochranu svojich informácií prostredníctvom tohto „návodu“, si môžu byť isté, že pokryjú celú oblasť informácií, ktorým hrozí nebezpečenstvo. Ale ani tento „návod“ nezabezpečí funkčný a efektívny systém manažérstva informačnej bezpečnosti, ak v organizácii nie je aktívna podpora vedenia a uvedomelá účasť všetkých.

Tento príspevok vznikol v rámci riešenia grantovej úlohy VEGA 1/0194/08.

Literatúra

1. ISO 27001 Online. ISO 27001 Security. [online].[Cit. 2008-01-20] Dostupné na internete: http://www.27001-online.com/
2. ISO27k infosec management standards. ISO 27001 security.].[Cit. 2008-01-20] Dostupné na internete: http://iso27001security.com/
3. STN ISO/IEC 27OO1:2006 „Informačné technológie. Zabezpečovacie techniky. Systémy manažérstva informačnej bezpečnosti. Požiadavky“.
4. ZEMAN, M.: Systém řízení informačnej bezpečnosti podle normy ISO 27001. In: Perspektivy Jakosti 1/2007. Ročník IV. Praha 1: Česká společnost pro jakost. s.39-40. ISSN 1214-8865.

Lektoroval:
Ing. Václav Štverka