Poradenství ISMS

ISMS (zkratka pochází z anglického **I**nformation **S**ecurity **M**anagement **S**ystems – viz norma ISO/IEC 27001/2006, která nahradila britskou normu BS 7799-2 z prosince 2004) je, zjednodušeně řešeno, systém řízení činností souvisejících s pořizováním, zpracováváním, uchováváním a bezpečnou likvidací informací/dat, se kterými organizace nakládá v rámci realizace svých podnikatelských procesů.

Legislativní souvislosti

Vedle výše uvedených technických norem se k problematice bezpečnosti informací vztahuje také celá řada právních norem. Omezíme se na předpisy v ČR, i když samozřejmě platí právní úprava EU. Oblasti informačních technologií se bezprostředně týkají zejména následující právní normy:

- Zákon 247/2008 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů
- Zákon 412/2005 Sb., o ochraně utajovaných skutečností
- Zákon 499/2004 Sb., o archivnictví a spisové službě
- Zákon 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů
- Zákon 127/2005 Sb., o elektronických komunikacích
- Zákon 124/2002 Sb., o platebním styku
- Zákon 365/2000 Sb., o informačních systémech veřejné správy
- Zákon 227/2000 Sb., o elektronickém podpisu
- Zákon 151/2000 Sb., o telekomunikacích
- Zákon 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
- Zákon 106/1999 Sb., o svobodném přístupu k informacím

Implementace ISMS dle normy ISO/IEC 17021

Tato norma je určena pro všechny organizace, ať už komerční, neziskové, či státní správu a samosprávu. Jejím smyslem je, jak už bylo řečeno, ochrana dat, informací a dalších aktiv, která mají pro organizaci význam, a minimalizace případného poškození organizace v případě bezpečnostních incidentů.

Pokud jde jakoukoli firmu, její zákazníci ve všech oblastech se samozřejmě budou vždy plně spoléhat na to, že pokud poskytnou svému dodavateli k dispozici v obchodním styku informace, budou tyto informace (data) vždy dostatečně zabezpečeny.

Definice používaných pojmů

Co vlastně přesně znamená pojem informační bezpečnost (nebo bezpečnost informací)?

- **Informační bezpečnost** znamená zabezpečení tří základních oblastí, a to jsou:

⇨ Důvěryhodnost: zajištění, že přístup k informacím mají pouze osoby pro to autorizované
⇨ Integrita: přesnost a úplnost přenesené informace
⇨ Dostupnost: zabezpečení přístupu k informacím a informačním aktivům pro příslušné uživatele, kdykoli je to třeba

Uveďme si i definice některých dalších důležitých pojmů používaných v oblasti ISMS:

- **Aktivum:** cokoliv, co má pro společnost nějakou cenu (logo, SW, budova…).
- **Dostupnost:** zajištění, že informace je pro oprávněné uživatele přístupná
- v okamžiku její potřeby.
- **Důvěrnost (důvěryhodnost):** zajištění, že informace jsou přístupné nebo sdělené pouze těm, kteří jsou k tomu oprávněni
- **Bezpečnost informací:** zachování důvěrnosti, integrity a dostupnosti informací a dalších vlastností, jako např. autentičnost, odpovědnost, nepopiratelnost a spolehlivost.
- **Bezpečnostní událost:** identifikovaný stav systému, služby nebo sítě, ukazující na možné porušení bezpečnostní politiky nebo selhání bezpečnostních opatření. Může se také jednat o jinou předtím nenastalou situaci, která může být důležitá z pohledu bezpečnosti informací.
- **Bezpečnostní incident:** jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činností organizace a ohrožení bezpečnosti informací.
- **Integrita:** zajištění správnosti a úplnosti informací.
- **Zbytkové riziko:** riziko zbývající po uplatnění zvládání rizik.
- **Akceptace rizik:** rozhodnutí přijmout riziko zpravidla mající přijatelnou hodnotu.
- **Analýza rizik:** systematické používání informací k odhadu rizika a k identifikaci jeho zdrojů
- **Hodnocení rizik:** celkový proces analýzy a vyhodnocení rizik
- **Vyhodnocení rizik:** proces porovnávání odhadnutého rizika vůči daným kritériím pro určení jeho významu.
- **Management rizik:** koordinované činnosti sloužící k řízení a kontrole organizace s ohledem na rizika.
- **Zvládání rizik:** proces výběru a přijímání opatření ke změně rizika.
- **Prohlášení o aplikovatelnosti:** dokumentované prohlášení popisující cíle opatření a jednotlivá bezpečnostní opatření, která jsou relevantní a aplikovatelná v rámci ISMS organizace.

Pozn.: definice vycházejí z norem řady ISO/IEC 27000.

Ztráta důvěrnosti informací na jedné straně může vést k poškození image organizace u zákazníků, nehledě na možné právní důsledky takového incidentu. Ztráta integrity, dostupnosti, autenticity a spolehlivosti dat na straně druhé může vést k problémům v oblasti plánování, přípravy zakázek, procesů realizace až k navazujícím činnostem (balení, expedice, následný servis apod.) a tím ohrozit (ne-li přímo znemožnit) vlastní činnost firmy.

S ohledem na důležitost zabezpečit dostatečnou ochranu informací a řídit bezpečnost systému informačních technologií (dále též pouze „IT“) uvnitř organizace již dnes používá řada firem více či méně dokumentovaná pravidla a postupy směřující k ochraně dat. Jsou to většinou požadavky týkající se jednak personální oblasti, jednak používaného SW, a jednak technického zázemí.

Vzhledem k tomu, že již dnes existuje celý soubor norem, které nabízejí ucelená řešení v této oblasti (viz normy řady ISO/IEC 27001), je nanejvýš vhodné pro vedení firmy analyzovat stávající situaci, vyhodnotit rizika a na základě tohoto vyhodnocení stanovit plán opatření např. dle „naší“ normy ČSN ISO/IEC 27001:2006, která slouží jako východisko pro následující činnosti:

- Zformulování politiky bezpečnosti IT
- Určení odpovědností, povinností a pravomocí v oblasti IT uvnitř organizace
- Analýza rizik
- Management rizik
- Monitorování, analýzy, revize

Smyslem implementace požadavků normy je vytvořit systémový přístup k řízení bezpečnosti informací a předejít tak možnému poškození, ztrátě či zneužití dat, a to následujícími kroky:

- Definováním pojetí v oblasti řízení bezpečnosti IT v podmínkách společnosti
- Identifikováním vztahu mezi systémem managementu společnosti obecně a systémem managementu IT
- Vytvořením vhodného modelu řízení bezpečnosti IT
- Realizací potřebných opatření

V oblasti ISMS nabízíme následující činnosti:

1. **Úvodní analýza**.
2. Provedení **identifikace aktiv** a stanovení jejich hodnoty. V rámci identifikace a ohodnocení aktiv společnost identifikuje všechna svá aktiva (věci hmotné, jako je třeba výpočetní technika, i „věci“ nehmotné, jako jsou data, znalosti, značka, apod.). Následuje stanovení hodnoty aktiv např. z hlediska integrity, dostupnosti a důvěrnosti, nákladů na jejich (znovu)pořízení apod.
3. **Analýza rizik**. Analýza rizik je dokument, na němž je následně postaven celý systém bezpečnosti informací.
4. Na analýzu rizik navazuje **návrh opatření**. Popisuje, jak bude společnost reagovat na nalezená kritická místa, definuje, jak by měl vypadat cílový stav, jak se k němu společnost dostane, termín splnění a případné nároky na zdroje.
5. **Prohlášení o aplikovatelnosti** dle přílohy A normy ISO/IEC 27001.
6. Vytvoření **dokumentace**. Pro přehlednost uvádíme souhrnný seznam nezbytných dokumentů v případě implementace ISMS dle ISO/IEC 27001:
    i. Rozsah a hranice ISMS
    ii. Politika ISMS
    iii. Definice a popis přístupu k hodnocení rizik
    iv. Identifikace rizik
    v. Analýza a vyhodnocení rizik
    vi. Identifikace a varianty pro zvládání rizik
    vii. Cíle opatření a bezpečnostní opatření pro zvládání rizik (viz příloha A normy)
    viii. Akceptace rizik
    ix. Získání povolení k provozování ISMS v rámci organizace
    x. Prohlášení o aplikovatelnosti
7. **Implementace** opatření.
8. **Monitoring, analýza, zlepšování**.
9. **Certifikace** (pokud ji vedení požaduje).

Kolik to stojí?

Cena je závislá zejména na rozsahu, formě a délce dohodnuté spolupráce. Platí základní sazba konzultace v ceně v rozmezí 450,- až 800,- Kč za hodinu. Kdykoli Vám samozřejmě také zpracujeme nezávazně cenovou nabídku přímo pro Vás.

Co mám dělat, pokud chci vaše služby?

Sdělit nám nějakým způsobem Vaše požadavky (e - mail, telefon, pošta apod.) – viz kontakty.

2010-02-05, „AEC“