



SYSTÉMY ŘÍZENÍ

Bezpečnost informací

TO NEJCENNĚJŠÍ, CO KAŽDÝ MÁ, JSOU INFORMACE. V dnešní době jsou informace, a to v jakékoli formě, tím nejcennějším zbožím na trhu a neobejde se bez nich žádná organizace. Skoro všechny organizace jsou na svých informacích existenčně závislé a jejich nedostupnost, vyzaření konkurenci nebo poškození znemožní další podnikání nebo vede k velkým ztrátám. Vůbec při tom nezáleží, zda jsou informace na papíře, v hlavách zaměstnanců, v počítačích nebo na jiných nosičích. Některé informace často není možné získat znovu. Informace je tedy potřeba odpovídajícím způsobem chránit. Odpovídajícím způsobem chránit znamená, že budou realizována taková opatření, jejichž cena nebude vyšší než cena chráněných informací a přitom budou opatření dostatečně účinná.

Jak informace odpovídajícím způsobem chránit?

Jediným efektivním způsobem ochrany informací je řídit bezpečnost svých informací s využitím nejlepších zkušeností jiných. Nejlepší světové zkušenosti a praktiky jsou mezinárodními organizacemi neustále shromažďovány a vydávány jako standardy. V oblasti bezpečnosti informací je takovým světovým standardem soubor norem ISO/IEC 27000. Hlavní normou tohoto standardu je ISO/IEC 27001, která definuje systém řízení bezpečnosti informací - ISMS.

Co je tedy systém řízení bezpečnosti informací nazývaný ISMS?

ISMS podle normy ČSN ISO/IEC 27001:2006 je komplexní soubor činností a opatření, která efektivním způsobem zvýší ochranu informací organizace, před reálnými hrozbami, které mohou způsobit nedostupnost (tj. i ztrátu), poškození, nebo vyzaření těchto informací a tím narušit činnost organizace nebo jí způsobit závažnou škodu.

Co je cílem takového systému?

Cílem takového systému řízení bezpečnosti informací je efektivně chránit důležité informace a další důležité prostředky organizace před hrozbami a zajistit tak kontinuitu činností organizace.

Jak takový systém funguje?

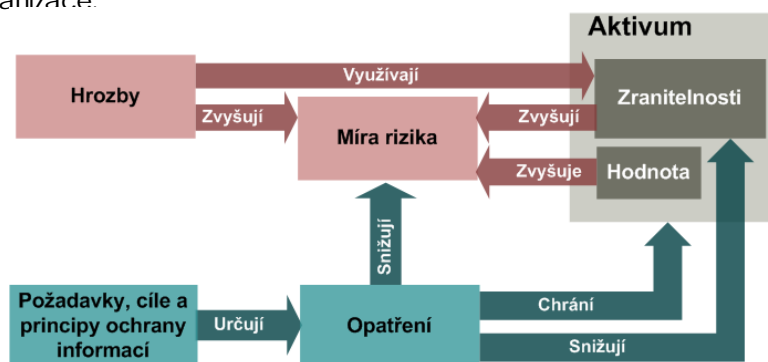
Na bezpečnost informací mají vliv tři hlavní prvky, které vždy existují a vzájemně na sebe působí ve stejném místě a ve stejném čase. Těmito prvky jsou AKTIVA, HROZBY a OPATŘENÍ. Vzájemné působení těchto prvků je vyjádřeno hodnotou nazývanou MÍRA RIZIKA.

AKTIVA (informace a prostředky pro jejich zpracování) mají z pohledu organizace svoji hodnotu a podle formy, ve které jsou zpracovávány a uloženy i své zranitelnosti, které mohou být hrozbou (útočníkem) využity.

HROZBA je naproti tomu událost, nezávislá na vůli organizace, která může využít zranitelnosti aktiva a aktivum poškodit (zničit, změnit, vyrazit).

OPATŘENÍ jsou nástroje, které zabraňují hrozbám využít zranitelnosti aktiv.

MÍRA RIZIKA pro dané aktivum je funkcí hrozby, aktiva a účinnosti opatření.



SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ:

- n** stanovuje požadavky na ochranu informací a
- n** identifikuje aktiva, hrozby a jejich vzájemné vazby,
- n** navrhuje opatření ke zvládnutí rizik a
- n** přidává nástroje pro neustálé zlepšování celého systému s využitím obecného modelu PDCA.

Jak takový systém zavést?

- 1) Prvním a nejdůležitějším krokem je uvědomit si jaké informace organizace vlastně má a jakou pro ni mají hodnotu.
- 2) Druhým krokem je identifikovat hrozby, které reálně mohou působit na aktiva (tj. na informace a prostředky pro jejich požívání, zpracovávání a ukládání) a vypočítat míry rizik pro jednotlivá aktiva.
- 3) Dalším krokem je definovat politiku bezpečnosti informací jako koordinovaný soubor cílů a principů, který povede k zajištění požadovaného stupně ochrany informací.
- 4) Následuje krok návrhu souboru opatření (nástrojů organizačního, technického, administrativního nebo jiného charakteru), který sníží míry rizik nebo omezí možný dopad hrozby v případě, že se vyskytne.
- 5) Další krok zahrnuje zavedení souboru opatření do prostředí organizace.
- 6) Předposledním krokem je nastavení postupů, které zajistí zlepšování účinnosti, spolehlivosti a efektivnosti jak souboru opatření k zajištění bezpečnosti informací, tak celého ISMS.
- 7) Posledním a nutným krokem je pak příprava a provedení certifikace fungujícího ISMS.

Certifikovat ISMS?

Certifikace je proces, kdy nezávislá třetí strana (certifikační autorita) dává záruku, že systém splňuje požadavky, které jsou na něj kladené právě normou ČSN ISO/IEC 27001:2006. Tato záruka je vydávána formou certifikátu, který pak slouží organizaci jako:

- n** důkaz o tom, že informace a prostředky pro jejich zpracování jsou chráněny v souladu s požadavky mezinárodního standardu,
- n** důkaz důvěryhodnosti organizace vůči svým zákazníkům a třetím stranám,
- n** důkaz o tom, že jsou plněny požadavky zákonů související s informacemi,
- n** důkaz neustálého zlepšování ochrany informací.

Získání certifikátu může být i konkurenční výhodou a někdy i zákazníky vyžadovanou nutností. Systém nebo jeho část však může správně fungovat i bez certifikace. Certifikovat systém je vhodné, pokud je to účelné a z nějakého důvodu je výhodné vlastnit certifikát.

Jak vám můžeme pomoci my?

Naše společnost, která na trhu působí od roku 1990, se zabývá poradenstvím v oblastech:

- n** procesního řízení,
- n** řízení organizací,
- n** vytváření, zavádění a provozování všech systémů řízení, včetně ISMS.

Má dostatek zkušených a certifikovaných konzultantů, aby vám navrhla a pomohla zavést ISMS „ušitý“ na míru potřebám vaší organizace. Jsme odpůrci univerzálních „baličků“, které nikdy nemohou vystihnout konkrétní potřeby dané organizace. Jsme zastánci vytváření účinných a efektivních systémů, a proto systém ochrany informací navrhujeme vždy tak, aby informace byly chráněny ekonomicky a při tom účinně v daném prostředí organizace.

