ČESKÁ TECHNICKÁ NORMA

ICS 35.020; 35.040 **Červen 2008**

Systém managementu bezpečnosti informací - Směrnice pro management rizik bezpečnosti informací	ČSN 36 9790

idt BS 7799-3:2006

Information Security Management Systems - Guide for Information Security Risk Management

Tato norma je českou verzí britské normy BS 7799-3:2006. Překlad byl zajištěn Českým normalizačním institutem.

This standard is the Czech version of the BS 7799-3:2006. It was translated by Czech Standards Institute.

81079

Předmluva

Informace o citovaných normativních dokumentech

ISO/IEC 27001:2005 zavedena jako ČSN ISO/IEC 27001:2006 (36 9790) Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky

ISO/IEC 17799:2005 zavedena jako ČSN ISO/IEC 17799:2006 (36 9790) Informační technologie -

Bezpečnostní
techniky - Soubor postupů pro management bezpečnosti informací

ISO/IEC TR 13335-3:1998 zavedena jako ČSN ISO/IEC TR 13335-3:2000 (36 9786) Informační technologie -
Směrnice pro řízení bezpečnosti IT-Část 3: Techniky pro řízení bezpečnosti IT

ISO Guide 73:2002 zaveden jako Pokyn ISO/IEC 73 Management rizika - Slovník - Směrnice pro používání
v normách

Vysvětlivky k textu normy

Znění normy bylo terminologicky harmonizováno s dokumentem ČNI Pokyn ISO/IEC 73 Management rizika -
Slovník - Směrnice pro používání v normách

Vypracování normy

Zpracovatel: Ing. Marie ©ebestová, IČ 16112946

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

Obsah

Seznam obrázků

Seznam tabulek

0 Úvod

0.1 Obecně

Tento překlad britské normy BS 7799-3:2006 pro management rizik je určen pro ty podnikové manažery a jejich zaměstnance, kteří se v rámci ISMS (Systém managementu bezpečnosti informací) věnují činnostem souvisejícím s managementem rizik. Poskytuje návod a radu výhradně pro podporu implementace těch požadavků definovaných v normě ČSN ISO/IEC 27001:2006, které se vztahují k procesům managementu rizik a k souvisejícím činnostem. Tabulka E1 ilustruje vztah mezi těmito dvěma dokumenty.

0.2 Procesní přístup

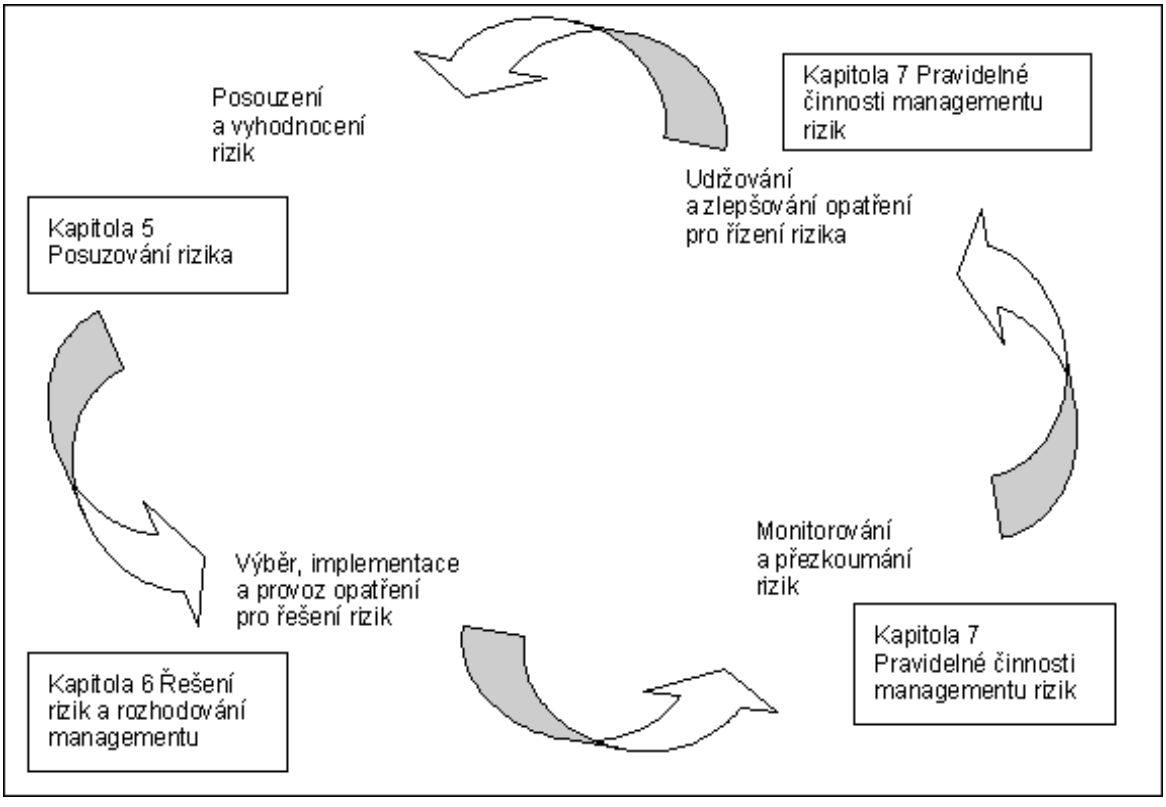
Tato norma podporuje přijetí procesního přístupu při posuzování rizik, řešení rizik a soustavné monitorování rizik. Procesní přístup podporuje jeho uživatele, aby kladli důraz na:

a) pochopení požadavků na bezpečnost informací společnosti a potřebu stanovit politiku a cíle bezpečnosti informací;

b) výběr, zavedení a využívání vhodných opatření v kontextu řízení celkových rizik byznysu;

c) monitorování a přezkoumání výkonnosti a efektivnosti systému managementu bezpečnosti informací (ISMS) pro řízení rizik byznysu;

d) neustálé zlepšování založené na objektivním měření rizik.



Obrázek 1 - Model procesu managementu rizik

Tento proces managementu rizik je zaměřen na provádění provozních činností s plným pochopením rizik, což organizacím následně umožní efektivní rozhodování ohledně jejich řízení. Proces managementu rizik je neustálá činnost, která má vést ke kontinuálnímu zlepšování jejich účinnosti a efektivity.

Proces managementu rizik by měl být aplikován na celý ISMS (jak je specifikován v ČSN ISO/IEC 27001:2006) a nové informační systémy by měly být zahrnuty do ISMS již ve fázi plánování a návrhu, aby bylo zajištěno, že jakákoliv rizika bezpečnosti informací jsou náležitě řízena. Tento dokument popisuje prvky a důležité aspekty tohoto procesu managementu rizik.

Rizika bezpečnosti informací je třeba posuzovat kontextu jejich byznysu a ve vzájemném vztahu s ostatními funkcemi byznysu, jako jsou lidské zdroje, výzkum a vývoj, výroba a provozy, administrativa, IT, finance, zároveň je třeba identifikovat potřeby zákazníků, aby bylo dosaženo celého a úplného obrazu těchto rizik. Toto zvažování

má zohlednit také organizační rizika a využívat pojetí a celkové představy o řízení. Toto vše, společně s byznysem organizace, efektivností, právním prostředím a předpisy, slouží jako podněty a motivace pro úspěšný proces managementu rizik. Detailnější popis je uveden v kapitole 4.

Důležitou částí procesu managementu rizik je posouzení rizik bezpečnosti informací, které je potřebné pro pochopení požadavků byznysu na bezpečnost informací a rizik, kterým jsou vystavena aktiva byznysu organizace. Jak je také popsáno v ČSN ISO/IEC 27001:2006, posouzení rizik zahrnuje následující kroky a činnosti, které jsou popsány detailněji v kapitole 5.

- Identifikace aktiv.
- Identifikace právních a byznysových požadavků, které jsou významné pro identifikovaná aktiva.
- Ohodnocení identifikovaných aktiv, při zohlednění identifikovaných právních a byznysových požadavků a dopadů ztráty důvěrnosti, integrity a dostupnosti.
- Identifikace významných hrozeb a zranitelností pro vybraná aktiva.
- Posouzení pravděpodobnosti, že hrozby a zranitelnosti nastanou.
- Výpočet rizika.
- Ohodnocení rizik podle předdefinované škály rizik.

Dalším krokem v procesu managementu rizik je identifikace vhodné činnosti pro řešení rizika u každého z rizik, které bylo při posouzení rizik identifikováno. Rizika mohou být řízena pomocí kombinace preventivních a zjiš»ovacích opatření, taktikou vyhnutí se riziku, pojištěním a/nebo jednoduše přijetím rizika. Jakmile bylo riziko posouzeno, musí být přijato rozhodnutí ohledně toho, jaké kroky, pokud vůbec nějaké, mají být provedeny. Ve všech případech musí být rozhodnutí založeno na potřebě byznysu, která opravňuje toto rozhodnutí. To může být přijato nebo zpochybněno klíčovými zainteresovanými stranami. Různé možnosti nakládání s riziky a faktory, které mají vliv na rozhodování, jsou popsány v kapitole 6.

Jakmile byla přijata rozhodnutí o způsobu řešení rizik a následně po těchto rozhodnutích byla implementována vybraná opatření, musí začít činnosti trvalého managementu rizik. Tyto činnosti zahrnují proces monitorování rizik a aplikaci ISMS, aby bylo zajištěno, že implementovaná opatření fungují tak, jak bylo zamýšleno. Další činností je přezkoumání rizika a opětovného posouzení, které je nezbytné k přizpůsobení způsobu posuzování rizik změnám, ke kterým mohlo nastat během času v prostředí byznysu. Vykazování rizika a komunikace je nezbytná pro zajištění, že byznysová rozhodnutí jsou přijata v kontextu chápání rizik v rámci celé organizace. Koordinace různých procesů souvisejících s riziky musí zajistit, aby organizace mohla fungovat účinným a efektivním způsobem. Neustálé zlepšování je základní součást trvalých činností managementu rizik ke zvýšení efektivity implementovaných opatření směrem k dosažení cílů, které byly stanoveny pro ISMS. Činnosti trvalého managementu rizik je popsáno v kapitole 7.

Úspěšná implementace procesu managementu rizik vyžaduje, aby byly jasně definované role a odpovědnosti, prováděné v rámci organizace. Role a odpovědnosti, které jsou zapojeny do procesu managementu rizik, jsou v tomto dokumentu zmiňovány tam, kde je to důležité.

1 Předmět normy

Britská norma BS 7799-3:2006 a její český překlad podávají návod, jak splnit požadavky definované v normě ČSN ISO/IEC 27001:2006, které se týkají všech aspektů cyklu managementu rizik v ISMS. Tento cyklus zahrnuje posouzení a hodnocení rizik, implementaci opatření pro nakládání s riziky, monitorování a přezkoumání rizik, udržování a zlepšování systému opatření pro zvládání rizik.

Tato norma se zaměřuje na efektivní bezpečnost informací pomocí trvalého programu managementu rizik. Toto zaměření je úkolem bezpečnosti informací v kontextu rizik byznysu organizace.

Návod podaný v této publikaci je určený pro aplikaci ve všech organizacích bez ohledu na jejich typ, velikost a obor podnikání. Je určen pro ty manažery a jejich zaměstnance, kteří jsou zapojeni do činností managementu rizik v rámci ISMS (Systém řízení bezpečnosti informací).

-- Vynechaný text --