

2008

System 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.



© Český normalizační institut, 2008

Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány a rozšiřovány jen se souhlasem Českého normalizačního institutu.

81079

Strana 2

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

Strana 3

Systém managementu bezpečnosti informací -
Směrnice pro management rizik bezpečnosti informací

BS 7799-3
Druhé vydání
2006-03-17

Obsah

Strana

0

Úvod

.....
..... 5

0.1

Obecně

.....
..... 5

0.2 Procesní

přístup

.....
5

1	Předmět normy	6
2	Citované normativní dokumenty.....	6
3	Termíny a definice	7
4	Rizika bezpečnosti informací v kontextu organizace.....	9
4.1	Rozsah a politika systému řízení bezpečnosti informací.....	9
4.2	Filosofie/Přístup k riziku.....	10
5	Posouzení rizika	10
5.1	Proces posouzení rizika.....	10
5.2	Identifikace aktiv	11
5.3	Identifikace právních a byznysových požadavků.....	11
5.4	Ocenění aktiv	12
5.5	Identifikace a posouzení hrozeb a zranitelností.....	12
5.6	Posouzení hrozeb a zranitelností.....	13
5.7	Kalkulace rizika a hodnocení.....	13
5.8	Posuzovatel rizika	

.....	14
6 Řešení rizik a rozhodování managementu.....	14
6.1 Obecně	14
6.2 Rozhodování	14
6.3 Snížení rizika	15
6.4 Vědomě a objektivně přijmout riziko.....	16
6.5 Přenos rizika	16
6.6 Vyvarování se rizika	16
6.7 Zbytkové riziko	17
6.8 Plán zvládnání rizik	17
7 Pravidelné činnosti managementu rizik.....	17
7.1 Provozování managementu bezpečnostních rizik.....	17
7.2 Udržování a monitorování	18

7.3 Přezkoumání systému managementu.....	18
7.4 Přezkoumání rizik a nové posouzení.....	18
7.5 Audity	19
7.6 Řízení dokumentace	19
7.7 Nápravná a preventivní opatření.....	19
7.8 Reporting a komunikace	19
7.9 Manažer bezpečnostních rizik.....	20

Strana 4

Strana

Příloha A (informativní) Příklady plnění právních požadavků a předpisů.....	21
A.1 Obecně	21
A.2 Právní rámec	21
A.3 Národní bezpečnost	21
A.4 Řízení společností	22
A.5 Elektronické obchodování, právní rámec.....	22

A.6	Krádež identity, ochrana dat.....	23
A.7	Ochrana duševního vlastnictví.....	23
A.8	Odvětvová specifika.....	23
Příloha B (informativní) Rizika informační bezpečnosti a provozní rizika..... 24		
B.1	Procesy v organizacích a jejich vzájemné vztahy.....	24
B.2	Rizika organizací.....	25
B.3	Řízení společnosti.....	25
Příloha C (informativní) Příklady aktiv, hrozeb, zranitelností a metody posuzování rizik..... 26		
C.1	Identifikace aktiv.....	26
C.2	Příklad hrozeb.....	26
C.3	Příklady hrozeb a ČSN ISO/IEC 17799:2006.....	29
C.4	Příklady zranitelností a ČSN ISO/IEC 17799:2006.....	33
C.5	Příklady metod posuzování rizika.....	35
Příloha D (informativní) Nástroje managementu rizik..... 37		
D.1	Obecně.....	

..... 37

D.2 Výběr nástroje pro management

rizik..... 37

Příloha E (informativní) Vztah mezi ČSN ISO/IEC 27001:2006 a ČSN 36

9790:2008..... 38

Bibliografie

..... 39

Seznam obrázků

Obrázek 1 - Procesní model managementu

rizik..... 5

Obrázek C.1 - Typy

aktiv

..... 26

Seznam tabulek

Tabulka C.1 - Zranitelnosti, vztahující se k bezpečnosti lidských

zdrojů..... 33

Tabulka C.2 - Zranitelnosti, vztahující se k fyzické bezpečnosti a bezpečnosti

prostředí..... 33

Tabulka C.3 - Zranitelnosti, vztahující se k řízení komunikaci a řízení

provozu..... 34

Tabulka C.4 - Zranitelnosti, vztahující se k řízení

přístupu..... 34

Tabulka C.5 - Zranitelnosti, vztahující se k nákupu, vývoji a údržbě informačních

systémů..... 35

Tabulka C.6 - Matice s hodnotami

rizik..... 36

Tabulka C.7 - Třídění incidentů podle míry

rizika..... 36

Tabulka E.1 - Vztah mezi ČSN ISO/IEC:2006 a ČSN 36

9790:2008..... 38

0 Úvod

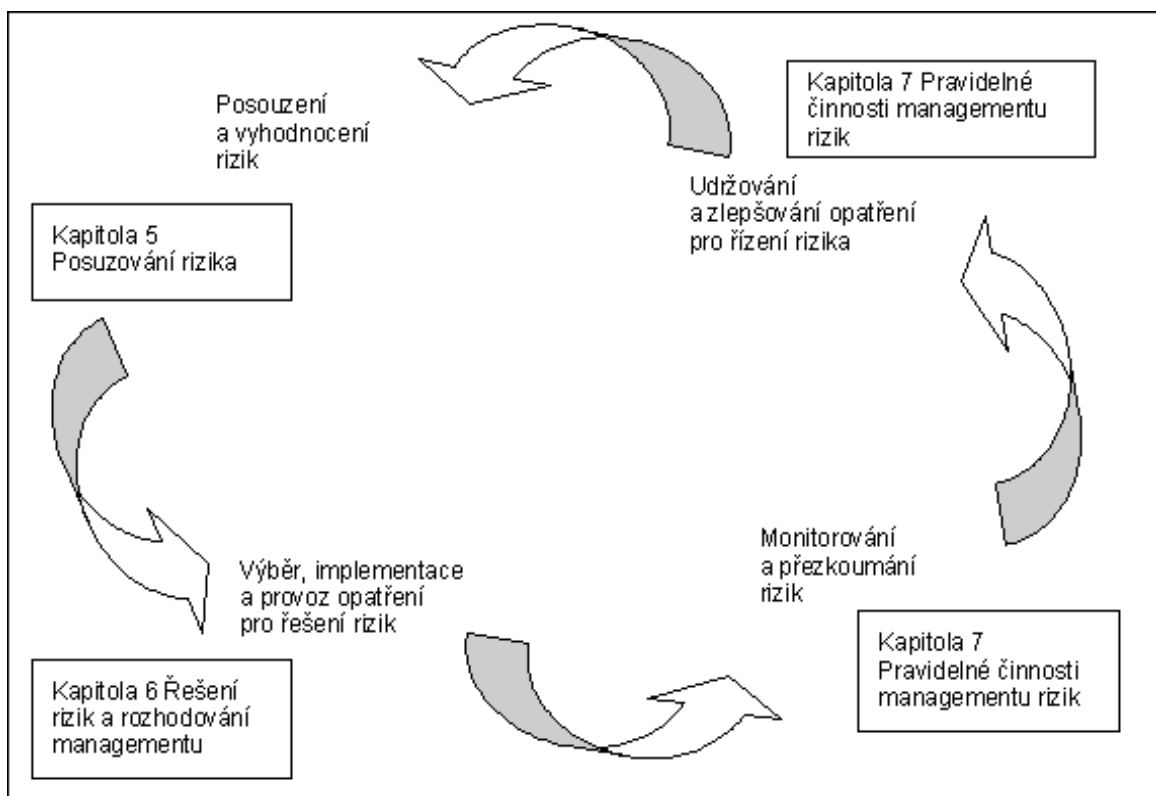
0.1 Obecně

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:

- počtení požadavků na bezpečnost informací společnosti a potřebu stanovit politiku a cíle bezpečnosti informací;
- výběr, zavedení a využívání vhodných opatření v kontextu řízení celkových rizik byznysu;
- monitorování a přezkoumání výkonnosti a efektivnosti systému managementu bezpečnosti informací (ISMS) pro řízení rizik byznysu;
- 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

Strana 6

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 zjišťovacích opatření, taktikou vyhnout 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 součástí 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 zvládnutí 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 --