ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Srpen 2006

Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací	ČSN ISO/IEC 17799 36 9790

Information technology - Security techniques - Code of practice for information security management

Technologies de l'information - Techniques de sécurité - Code de pratique pour la gestion de sécurité d'information

Tato norma je českou verzí mezinárodní normy ISO/IEC 17799:2005. Překlad byl zajištěn Českým normalizačním institutem. Má stejný status jako oficiální verze uvedené mezinárodní normy.

This standard is the Czech version of the International Standard ISO/IEC 17799:2005. It was translated by Czech Standards Institute. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 17799 (36 9790) z dubna 2005.

Národní předmluva

Změny proti předchozím normám

Mezi nejvýraznější změny v této aktualizované verzi patří to, že se řízení bezpečnostních incidentů stalo samostatnou oblastí bezpečnosti. Oproti předchozímu vydání normy bylo také odstraněno devět bezpečnostních opatření a sedmnáct nových jich přibylo.

Informace o citovaných normativních dokumentech

ISO/IEC 9796-2:2002 zavedena v ČSN ISO/IEC 9796-2:2004 (36 9780) Informační technologie - Bezpečnostní techniky - Schémata digitálního podpisu umožňující obnovu zprávy - Část 2: Mechanismy založené na faktorizaci celých čísel

ISO/IEC 9796-3:2000 zavedena v ČSN ISO/IEC 9796-3:2002 (36 9780) Informační technologie - Bezpečnostní techniky - Schémata digitálních podpisů umožňující obnovu zprávy - Část 3: Mechanismy založené na diskrétních logaritmech

ISO 10007:2003 zavedena v ČSN ISO 10007:2004 (01 0334) Systémy managementu jakosti - Směrnice managementu konfigurace

ISO/IEC 11770-1:1996 zavedena v ČSN ISO/IEC 11770-1:1998 (36 9785) Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 1: Struktura

ISO/IEC 12207:1995 zavedena v ČSN ISO/IEC 12207:1997 (36 9784) Informační technologie - Procesy v životním cyklu softwaru

ISO/IEC TR 13335-1:1996 zavedena v ČSN ISO/IEC TR 13335-1:1999 (36 9786) Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 1: Pojetí a modely bezpečnosti IT

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

ISO/IEC 14888-1:1999 zavedena v ČSN ISO/IEC 14888-1:2001 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 1: Všeobecně

ISO/IEC 14888-2:1999 zavedena v ČSN ISO/IEC 14888-2:2001 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 2: Mechanismy založené na identitě

ISO/IEC 14888-3:1999 zavedena v ČSN ISO/IEC 14888-3:2001 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 3: Mechanismy založené na certifikátu

ISO/IEC 15408-1:1999 zavedena v ČSN ISO/IEC 15408-1:2001 (36 9789) Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 1: Úvod a všeobecný model

ISO/IEC 15408-2:1999 zavedena v ČSN ISO/IEC 15408-2:2002 (36 9789) Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční požadavky

ISO/IEC 15408-3:1999 zavedena v ČSN ISO/IEC 15408-3:2002 (36 9789) Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 3: Požadavky na záruky bezpečnosti

EN ISO 19011:2002 zavedena v ČSN EN ISO 19011:2003 (01 0330) Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu

Souvisící ČSN

ČSN ISO/IEC 27001 (36 9790) Informační technologie - Bezpečnostní techniky - Sytém řízení bezpečnosti

informací - Požadavky

Vypracování normy

Zpracovatel: Risk Analysis Consultants, s.r.o., IČ 63672774

Technická normalizační komise: TNK 20 Informační technologie

Zaměstnanec Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA
Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací

ISO/IEC 17799
Druhé vydání
2005-06-15

ICS 35.040

ISO copyright office
Case postale 56, CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch

Obsah

Strana

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím technických komisí zřízených příslušnou organizací k tomu, aby se zabývaly určitou oblastí technické činnosti. V oblastech společného zájmu technické komise ISO a IEC spolupracují. Práce se zúčastňují i jiné mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou zpracovány v souladu s pravidly uvedenými v části 2 Směrnic ISO/IEC.

Hlavním úkolem společné technické komise je připravovat mezinárodní normy. Návrhy mezinárodních norem přijaté společnou technickou komisí se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Pozornost je třeba věnovat možnosti, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nenesou odpovědnost za identifikaci všech patentových práv nebo kteréhokoliv z nich.

Mezinárodní norma ISO/IEC 17799 byla připravena společnou technickou komisí ISO/IEC JTC 1 *Information technology*, subkomise SC 27, *IT Security techniques*.

Toto druhé vydání ruší a nahrazuje první vydání (ISO/IEC 17799:2000), které bylo technicky revidováno.

Technická komise ISO/IEC JTC 1/SC 27 připravuje soubor mezinárodních norem věnovaných systému řízení bezpečnosti informací (ISMS). Soubor norem zahrnuje požadavky na systém řízení bezpečnosti informací, managementu rizik, metriky a měření výkonu a doporučení k implementaci. Soubor těchto norem bude vydán v sérii 27000.

ISO/IEC 17799 by měla být do této nové řady začleněna v roce 2007 a to jako ISO/IEC 27002.

---

0 Úvod

0.1 Co je bezpečnost informací?

Informace jsou aktiva, která mají pro organizaci hodnotu. Je tedy nutné je vhodným způsobem chránit. Obzvláště se vzrůstající propojeností prostředí jednotlivých organizací je tato potřeba stále více aktuální. S rostoucí propojeností jsou informace vystaveny zvyšujícímu se počtu různých hrozeb a zranitelností (viz také Směrnice OECD pro bezpečnost informačních systémů a sítí: směrem ke kultuře bezpečnosti[1)].

Informace mohou existovat v různých podobách. Mohou být vytištěny nebo napsány na papíře, uloženy v elektronické podobě, posílány poštou nebo elektronickou cestou, zachyceny na film nebo vyřčeny při konverzaci.

Bezpečnost informací je zaměřena na širokou škálu hrozeb a zajiš»uje tak kontinuitu činností organizace, minimalizuje obchodní ztráty a maximalizuje návratnost investic a podnikatelských příležitostí.

Bezpečnosti informací lze dosáhnout implementací soustavy opatření, která mohou existovat ve formě pravidel, postupů, procedur, organizační struktury, programových a hardwarových funkcí. Tato opatření musí být ustavena, zavedena, provozována, monitorována, přezkoumávána a zlepšována proto, aby bylo dosaženo specifických bezpečnostních cílů organizace. Toto všechno by mělo být prováděno v souladu s ostatními řídícími procesy organizace.

0.2 Proč je nezbytná bezpečnost informací

Informace a podpůrné procesy, systémy a sítě jsou důležitými aktivy organizace. Vymezení, zavádění, podpora a zlepšování bezpečnosti informací může být zásadní pro udržení konkurenceschopnosti, peněžních toků (cash-flow), ziskovosti, právní shody a dobrého jména organizace.

Stále rostoucí měrou jsou organizace a jejich informační systémy vystavovány bezpečnostním hrozbám z různých zdrojů, včetně počítačových podvodů, špionáže, sabotáže, vandalizmu, požárů a povodní. Zdroje škod, jako jsou počítačové viry, útoky hackerů a útoky typu odepření služby (denial of service), jsou stále častější, roste jejich nebezpečnost a sofistikovanost.

Bezpečnost informací je důležitá z hlediska ochrany kritické infrastruktury a to jak v soukromém, tak

ve státním sektoru. V obou sektorech je bezpečnost informací důležitá pro existenci některých služeb, například e-governmentu nebo e-komerce a zároveň kvůli vyhnutí se nebo snížení relevantních rizik. Propojení veřejných a privátních sítí i sdílení informačních zdrojů zvyšuje obtížnost řízení přístupu. Trend směřující k distribuovanému zpracování oslabil efektivnost centrální kontroly prováděné specialisty.

Mnoho informačních systémů nebylo navrženo tak, aby byly bezpečné. Bezpečnost, která může být dosažena technickými prostředky, je nedostačující a měla by být doplněna odpovídajícím řízením a postupy. Pro určení opatření, která je třeba přijmout, je nutné pečlivé plánování a rozbor každého detailu. Řízení bezpečnosti informací proto vyžaduje alespoň nějakou spoluúčast všech zaměstnanců organizace. Může rovněž zahrnovat spolupráci majitelů organizace (akcionářů), dodavatelů, třetích stran, zákazníků a dalších externích subjektů. V neposlední řadě může být potřebná i rada od specialistů z jiných organizací.

0.3 Jak stanovit bezpečnostní požadavky

Je nezbytné, aby organizace určila své bezpečnostní požadavky. K tomu existují tři hlavní zdroje.

1) Prvním zdrojem je hodnocení rizik, která organizaci hrozí, beroucí v potaz celkovou strategii a cíle organizace. V rámci hodnocení rizik se identifikují hrozby působící vůči aktivům, zranitelnosti, které mohou být hrozbami využity i pravděpodobnost jejich výskytu, a provádí se odhad jejich potenciálního dopadu.

2) Druhým zdrojem jsou požadavky zákonů a podzákonných norem, smluvní ujednání a místní zvyklosti, které organizace, její obchodní, smluvní partneři a poskytovatelé služeb musí splňovat.

3) Třetím zdrojem jsou konkrétní principy, cíle a požadavky na zpracování informací, které si organizace vytvořila pro podporu své činnosti.

0.4 Hodnocení bezpečnostních rizik

Požadavky na bezpečnost jsou stanoveny za pomoci metodického hodnocení bezpečnostních rizik. Výdaje na bezpečnostní opatření by měly odpovídat ztrátám způsobeným narušením bezpečnosti.

[1)] OECD Guidelines for the Security of Information systems and Network – Towards a Culture of Security.

Výsledky hodnocení rizik pomohou určit vedení organizace odpovídající kroky i priority pro řízení bezpečnostních rizik u informací a pro realizaci opatření určených k zamezení jejich výskytu.

Hodnocení rizik by mělo být prováděno periodicky, aby bylo možné včas reagovat na jakékoliv změny v bezpečnostních požadavcích.

Více informací o hodnocení rizik je uvedeno v 4.1 „Hodnocení bezpečnostních rizik“.

0.5 Výběr opatření

Jakmile jsou identifikovány bezpečnostní požadavky a rizika, a bylo rozhodnuto jakým způsobem bude se zjištěnými riziky naloženo, měla by být vybrána a implementována opatření zajiš»ující snížení rizik na přijatelnou úroveň. Taková opatření mohou být vybrána z tohoto dokumentu nebo i z jiných souborů opatření. Pro pokrytí specifických potřeb mohou být vytvořena zcela nová opatření. Výběr konkrétních opatření je na rozhodnutí každé organizace. Rozhodnutí je založeno na kritériích určujících akceptaci nebo zvládání rizika a celkovém přístupu organizace k řízení rizik. Při výběru opatření by měla být zohledněna příslušná národní a mezinárodní legislativa a regulace.

Některá opatření v tomto dokumentu mohou být chápána jako základní doporučení pro řízení bezpečnosti informací a mohou být využita ve většině organizací. Detailněji jsou vysvětlena v části „Východiska bezpečnosti informací“.

Další informace o výběru opatření a způsobech zvládání rizik jsou uvedeny v 4.2 „Zvládání bezpečnostních rizik“.

0.6 Východiska bezpečnosti informací

Řada opatření může být považována za základní principy představující dobrá východiska pro implementaci bezpečnosti informací. Mohou vycházet ze základních legislativních požadavků nebo jsou obecně považována za nejlepších způsob řešení bezpečnosti informací.

Opatření, která by měla být pro organizaci podstatná z pohledu legislativy, jsou:

a) ochrana osobních údajů (viz 15.1.4);

b) ochrana důležité dokumentace organizace, jako například účetních záznamů (viz 15.1.3);

c) ochrana duševního vlastnictví (viz 15.1.2).

Opatření, považovaná za základ nejlepších praktik (best practices) pro zajištění bezpečnosti informací, jsou:

a) dokument bezpečnostní politiky informací (viz 5.1.1);

b) přidělení odpovědností v oblasti bezpečnosti informací (viz 6.1.3);

c) vzdělávání, školení a zvyšování povědomí v oblasti bezpečnosti informací (viz 8.2.2);

d) bezchybné zpracování v aplikačních systémech (viz 12.2);

e) řízení technických zranitelností (viz 12.6);

f) řízení kontinuity činností organizace (viz 14);

g) zvládání bezpečnostních incidentů a kroky k nápravě (viz 13.2).

Tato opatření fungují ve většině organizací a prostředí.

Ačkoliv všechna opatření uvedená v tomto dokumentu jsou důležitá, je nutné si uvědomit, že o výběru a aplikaci konkrétních opatření by mělo být rozhodnuto až ve světle specifických rizik, kterým organizace čelí. I když výše uvedené doporučení může být považováno za dobré východisko, nenahrazuje výběr opatření vycházející z hodnocení rizik.

0.7 Kritické faktory úspěchu

Jak ukazuje zkušenost, pro úspěšnou implementaci bezpečnosti informací v organizaci jsou často kritické následující faktory:

a) bezpečnostní politika, bezpečnostní cíle a činnosti, které respektují cíle činností organizace;

b) přístup k zavádění, udržování, monitorování a zlepšování bezpečnosti informací v souladu s kulturou organizace;

c) zřetelná podpora a angažovanost ze strany vedení organizace;

d) dobré pochopení bezpečnostních požadavků, hodnocení a managementu rizik;

e) účinný marketing bezpečnosti vůči vedení organizace, zaměstnancům a jiným stranám;

f) rozšíření směrnic a norem bezpečnostní politiky informací mezi všechny zaměstnance, vedení organizace a třetí strany;

g) zdroje na financování činností souvisejících s řízením bezpečnosti informací;

h) realizace odpovídajících školení, vzdělávání a programů zvyšování povědomí;

i) zavedení procesu zvládání bezpečnostních incidentů;

j) komplexní a vyvážený systém pro ohodnocení míry účinnosti[2] řízení bezpečnosti informací a získávání návrhů ke zlepšení na základě zpětné vazby.

0.8 Vytváření vlastních směrnic

Tento soubor postupů může být chápán jako východisko pro vytváření specifických směrnic organizace. Ne všechna doporučení a opatření tohoto souboru postupů mohou být použitelná. Kromě toho mohou být nezbytná i další opatření, která nejsou v tomto dokumentu uvedena. V takovém případě je užitečné zanechat v nich odkaz na tuto normu a usnadnit tak ověření shody prováděné auditory a obchodními partnery.

[2] Měření účinnosti implementovaného ISMS je mimo rozsah této normy.

1 Předmět normy

Tato mezinárodní norma poskytuje doporučení a obecné principy pro vymezení, zavedení, udržování a zlepšování systému managementu bezpečnosti informací v organizaci. Cíle, popsané v normě, poskytují rady o obecně přijímaných cílech managementu bezpečnosti.

Cíle opatření a jednotlivá opatření obsažená v této mezinárodní normě by měla být implementována na základě požadavků zjištěných v rámci analýzy rizik. Norma může sloužit jako praktický průvodce při vývoji bezpečnostních standardů organizace, účinných řídících bezpečnostních postupů a také při

budování důvěry mezi organizacemi.

-- Vynechaný text --