ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Září 2014**

Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací

ČSN ISO/IEC 27002
36 9798

Information Technology – Security techniques – Information security management systems – Code of practice for information security controls

Technologies de l,information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité
de l,information

Tato norma je českou verzí mezinárodní normy ISO/IEC 27002:2013. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 27002:2013. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 17799 (36 9790) ze srpna 2006.

Národní předmluva

Změny proti předchozí normě

Toto druhé vydání představuje technickou a strukturální revizi prvního vydání.

Informace o citovaných dokumentech

ISO/IEC 27000 zavedena v ČSN ISO/IEC 27000 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

Souvisící ČSN

ČSN ISO/IEC 20000-1 (36 9074) Informační technologie – Management služeb – Část 1: Požadavky na systém managementu služeb

ČSN ISO/IEC 20000-2 (36 9074) Informační technologie – Management služeb – Část 2: Pokyny pro použití systémů managementu služeb

ČSN ISO 22301 (01 2306) Ochrana společnosti – Systémy managementu kontinuity podnikání –

Požadavky

ČSN ISO/IEC 27001 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky

ČSN ISO/IEC 27005 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

ČSN ISO/IEC 27007 (36 9790) Informační technologie – Bezpečnostní techniky – Směrnice pro audit systémů řízení bezpečnosti informací

ČSN ISO 31000 (01 0351) Management rizik – Principy a směrnice

Vysvětlivky k textu převzaté normy

Pro účely této normy byl použit

- anglický termín „cloud computing“ v původním tvaru vzhledem k neexistenci českého ekvivalentu;
- anglický termín „malware“ v původním tvaru vzhledem k rozšíření tohoto termínu v odborné komunitě.

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČ 40654419

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Miroslav Škop

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 27002
Soubor postupů pro opatření bezpečnosti informací Druhé vydání
2013-10-01

ICS 35.040

Obsah

Strana

Strana

Published in Switzerland

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených dotyčnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují také další vládní i nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC1.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

ISO/IEC 27002 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *IT Bezpečnostní techniky*.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO nelze činit odpovědnou za identifikaci jakéhokoliv nebo všech patentových práv.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 27002:2005), jehož je technickou revizí.

0 Úvod

0.1 Původ a souvislosti

Tato mezinárodní norma je určena pro organizace k použití jako doporučení pro výběr opatření v rámci procesu zavádění systému řízení bezpečnosti informací (ISMS), založeného na normě ISO/IEC 27001[10], nebo jako pokyny pro organizace, implementující obecně přijatá opatření bezpečnosti informací. Tato norma je rovněž určena pro použití při vyvíjení směrnic pro řízení bezpečnosti informací specifických pro průmysl a organizace, s přihlédnutím k jejich konkrétnímu prostředí rizik pro bezpečnost informací.

Organizace všech typů a velikostí (včetně veřejného a soukromého sektoru, komerčních a neziskových) shromažďují, zpracovávají, uchovávají a předávají informace v mnoha formách, včetně elektronické, fyzické a verbální (například rozhovory a prezentace).

Hodnota informací přesahuje napsaná slova, čísla a obrázky: znalosti, koncepty, nápady a značky jsou příklady nehmotných forem informací. V navzájem propojeném světě jsou informace a související procesy, systémy, sítě a pracovníci podílející se na jejich provozování, nakládání s nimi a ochraně aktiva, která jsou, stejně jako jiná významná obchodní aktiva, cenná pro podnikání organizace, a proto si zaslouží nebo vyžadují ochranu proti různým rizikům.

Aktiva jsou vystavena jak úmyslným tak neúmyslným hrozbám, zatímco související procesy, systémy, sítě a lidé mají vlastní zranitelnosti. Změny obchodních procesů a systémů nebo jiné vnější změny (například nové zákony a předpisy), mohou vytvářet nová rizika bezpečnosti informací. Proto, vzhledem k množství způsobů, kterými mohou hrozby zneužít zranitelnosti k poškození organizace, jsou rizika bezpečnosti informací vždy přítomna. Efektivní bezpečnost informací snižuje tato rizika tím, že chrání organizaci před hrozbami a zranitelnostmi, a omezuje tedy dopady na její aktiva.

Bezpečnost informací je dosažena zavedením vhodné sady opatření, včetně politik, procesů, postupů, organizačních struktur a softwarových a hardwarových funkcí. Tato opatření je třeba stanovit, implementovat, monitorovat, přezkoumávat a zlepšovat tam, kde je to nutné, aby bylo zajištěno, že jsou splněny specifické cíle bezpečnosti a podnikatelské činnosti organizace. Systém ISMS, jako například systém specifikovaný v ISO/IEC 27001[10], používá holistický, koordinovaný pohled na rizika bezpečnosti informací organizace s cílem implementovat komplexní sadu opatření bezpečnosti informací v celkovém rámci uceleného systému řízení.

Mnoho informačních systémů nebylo navrženo tak, aby byly bezpečné ve smyslu normy ISO/IEC 27001[10] a této normy. Bezpečnost, které může být dosaženo technickými prostředky, je omezená a měla by být podporována vhodným řízením a postupy. Identifikace opatření, která by měla být zavedena, vyžaduje pečlivé plánování a věnování pozornosti detailům. Úspěšný systém ISMS vyžaduje podporu ze strany všech zaměstnanců organizace. To může také vyžadovat účast akcionářů, dodavatelů či jiných externích stran. Může také být potřeba poradenství specialisty z externích stran.

V obecnějším smyslu efektivní bezpečnost informací také zaručuje managementu a dalším zúčastněným stranám, že aktiva organizace jsou rozumně zabezpečena a chráněna proti poškození, a tím působí jako faktor podporující podnikatelskou činnost.

0.2 Požadavky bezpečnosti informací

Je nezbytné, aby organizace identifikovala své požadavky na bezpečnost. Existují tři hlavní zdroje požadavků na bezpečnost:

a. posuzování rizik pro organizaci, s přihlédnutím k celkové podnikatelské strategii a cílům organizace. Prostřednictvím posuzování rizik jsou identifikovány hrozby vůči aktivům, je vyhodnocena zranitelnost využitelná těmito hrozbami a pravděpodobnost výskytu a je proveden odhad potenciálního dopadu;

b. právní, zákonné, předpisové a smluvní požadavky, které organizace, její obchodní partneři, smluvní strany a poskytovatelé služeb musí splnit, a jejich sociální a kulturní prostředí;

c. soubor zásad, cílů a podnikatelských požadavků pro nakládání s informacemi, jejich zpracovávání, ukládání, sdělování/předávání a archivaci, které organizace vyvinula pro podporu své činnosti.

Zdroje použité při implementaci opatření je nutné udržovat v rovnováze vzhledem k podnikatelské škodě, přicházející v úvahu jako následek bezpečnostního problému v případě nepřítomnosti těchto

opatření. Výsledky posuzování rizik pomohou nasměrovat a určit odpovídající kroky managementu a priority pro řízení rizik bezpečnosti informací a pro implementaci opatření vybraných na ochranu proti těmto rizikům.

ISO/IEC 27005[11] poskytuje návod pro řízení rizik bezpečnosti informací, včetně doporučení v oblasti posuzování rizika, ošetření rizika, přijetí rizika, komunikace rizika, monitorování rizika a přezkoumání rizika.

0.3 Výběr opatření

Opatření mohou být vybrána z této normy nebo z jiných sad opatření, nebo mohou být navržena nová opatření tak, aby přiměřeně splňovala specifické potřeby.

Výběr opatření je závislý na organizačních rozhodnutích na základě kritérií pro přijetí rizika, možností ošetření rizika a obecného přístupu k řízení rizik platícího pro organizaci, a měl by také podléhat veškeré příslušné národní a mezinárodní legislativě a nařízením. Výběr opatření závisí také na způsobu, jakým na sebe opatření vzájemně působí, aby poskytovala hloubkovou ochranu.

Některá opatření v této normě mohou být považována za hlavní zásady pro řízení bezpečnosti informací a za použitelné pro většinu organizací. Opatření jsou vysvětlena podrobněji níže spolu s pokyny k implementaci. Více informací o výběru opatření a dalších možnostech ošetření rizik lze nalézt v ISO/IEC 27005[11].

0.4 Vytváření vlastních směrnic

Tato mezinárodní norma může být považována za výchozí bod pro vytváření směrnic specifických pro danou organizaci. Ne všechna opatření a návody v tomto souboru postupů mohou být použitelné. Kromě toho mohou být požadována další opatření a směrnice, které nejsou zahrnuty v této normě. Pokud jsou vytvářeny dokumenty, obsahující další pokyny nebo opatření, může být užitečné zahrnout křížové odkazy na kapitoly v této normě tam, kde lze usnadnit kontrolu shody auditory a obchodními partnery.

0.5 Přihlédnutí k životnímu cyklu

Informace má přirozený životní cyklus, od vytvoření a vzniku přes uchovávání, zpracovávání, použití a přenos až do jejího případného zničení nebo rozpadu. Hodnota aktiva a rizika týkající se aktiva se mohou během doby života aktiva měnit (například neoprávněné vyzrazení nebo odcizení finančních výkazů společnosti je daleko méně významné poté, co byly oficiálně zveřejněny), ale bezpečnost informací zůstává i nadále do určité míry důležitou ve všech fázích.

Informační systémy mají životní cyklus, ve kterém jsou koncipovány, specifikovány, navrženy, vyvinuty, testovány, implementovány, používány, udržovány a nakonec odstaveny a odstraněny. Bezpečnost informací by měla být vzata v úvahu v každé fázi. Vývoj nových a změny stávajících systémů představují pro organizace příležitosti aktualizovat a zlepšit opatření bezpečnosti, berouce v úvahu aktuální incidenty a současná a očekávaná rizika bezpečnosti informací.

0.6 Související normy

Zatímco tato norma poskytuje návod pro širokou škálu opatření v oblasti bezpečnosti informací, která se běžně uplatňují v mnoha různých organizacích, zbývající normy v řadě norem ISO/IEC 27000 poskytují doplňující doporučení či požadavky týkající se dalších aspektů celkového procesu řízení bezpečnosti informací.

Viz ISO/IEC 27000 pro obecný úvod do ISMS a norem této řady. ISO/IEC 27000 poskytuje slovník, formálně definující většinu pojmů používaných v řadě norem ISO/IEC 27000, a popisuje rozsah a cíle pro každou normu této řady.

1 Předmět normy

Tato mezinárodní norma poskytuje směrnice pro organizační normy bezpečnosti informací a postupy pro řízení bezpečnosti informací, včetně výběru, implementace a řízení opatření, s přihlédnutím k prostředí rizik bezpečnosti informací organizace.

Tato mezinárodní norma je určena pro použití organizacemi, které mají v úmyslu:

a. vybrat opatření v rámci procesu zavádění systému řízení bezpečnosti informací založeném na normě ISO/IEC 27001[10];

b. zavést obecně uznávaná opatření bezpečnosti informací;

c. vypracovat vlastní směrnice k řízení bezpečnosti informací.