ČESKÁ TECHNICKÁ NORMA

ICS 03.100.70; 35.030

Duben 2019

Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

ČSN ISO/IEC 27005

36 9790

Information technology – Security techniques – Information security risk management

Technologies de l,information – Techniques de sécurité – Gestion des risques liés a la sécurité de l,information

Tato norma je českou verzí mezinárodní normy ISO/IEC 27005:2018. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 27005:2018. It was translated by the Czech Agency for Standardization. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 27005 (36 9790) z července 2013.

Národní předmluva

Změny proti předchozí normě

Toto třetí vydání zrušuje a nahrazuje druhé vydání (ISO/IEC 27005:2011), které bylo technicky zrevidováno. V tomto vydání normy byly odstraněny odkazy na ISO/IEC 27001. Odstraněna byla příloha G a odkazy na tuto přílohu.

Informace o citovaných dokumentech

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

Souvisící ČSN

TNI 01 0350 (01 0350) Management rizik – Slovník (Pokyn 73)

ČSN EN ISO/IEC 27001 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

ČSN EN ISO/IEC 27002 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů

pro opatření bezpečnosti informací

ČSN ISO 31000 (01 0351) Management rizik – Směrnice

Vysvětlivky k textu převzaté normy

Pro účely této normy je anglický termín „guidance“ přeložen jako „pokyny“ vzhledem k jeho používání v oblasti IT a v návaznosti na vydané normy z oblasti IT, zejména souboru norem ISO/IEC 27XXX. Český ekvivalent „návod“ je vzhledem ke kontextu nevhodný a v praxi se v souvislosti se souborem norem ISO/IEC 27XXX nepoužívá.

Pro účely této normy byly použity následující anglické termíny v původní podobě, vzhledem k rozšíření těchto termínů v odborné komunitě a/nebo absenci českého ekvivalentu:

Bluetooth, cracker, FireWire, groupware, hacker, hacking, point-to-point

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

ISO/IEC 27005
Třetí vydání
2018-07

Obsah

Strana

ISO copyright office
CP 401 · Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Tel.: + 41 22 749 01 11
Fax: + 41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org
Publikováno ve Švýcarsku

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 svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oborech společného zájmu. Práce se zúčastňují také další vládní a nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnicích ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnicích ISO/IEC, část 2 (viz www.iso.org/directives).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržených ISO (viz www.iso.org/patents).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamená schválení.

Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT), jsou uvedeny na tomto odkazu URL:
www.iso.org/iso/foreword.html.

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

Jakákoliv zpětná vazba nebo otázky týkající se tohoto dokumentu by měly být směrovány na národní normalizační orgán uživatele. Úplný seznam těchto orgánů lze nalézt na www.iso.org/members.html.

Toto třetí vydání zrušuje a nahrazuje druhé vydání (ISO/IEC 27005:2011), které bylo technicky zrevidováno. Hlavní změny proti předchozímu vydání jsou následující:

– všechny přímé odkazy na ISO/IEC 27001:2005 byly odstraněny;

– byla přidána zřetelná informace, že tento dokument neobsahuje přímé pokyny k implementaci požadavků ISMS uvedených v ISO/IEC 27001 (viz Úvod);

– z kapitoly 2 bylo odstraněno ISO/IEC 27001:2005;

– ISO/IEC 27001 bylo přidáno do Bibliografie;

– příloha G a všechny odkazy na ni byly odstraněny;

– podle toho byly provedeny všechny redakční změny.

Úvod

Tento dokument poskytuje směrnice pro řízení rizik bezpečnosti informací v organizaci. Tento dokument však neposkytuje žádnou specifickou metodu pro řízení rizik bezpečnosti informací. Je na organizaci, jak bude definovat svůj přístup k řízení rizik, například v závislosti na rozsahu systému řízení bezpečnosti informací (ISMS), rámci řízení rizik nebo průmyslovém odvětví. K implementaci požadavků ISMS může být použito mnoho existujících metodik pod rámcem popsaným v tomto dokumentu. Tento dokument je založen na metodě identifikace rizika aktiv, hrozeb a zranitelností, kterou již ISO/IEC 27001 nepožaduje. Existují některé další přístupy, které je možno použít.

Tento dokument neobsahuje přímé pokyny k implementaci požadavků ISMS uvedených v ISO/IEC 27001.

Tento dokument je důležitý pro manažery a zaměstnance, kterých se týká řízení rizik bezpečnosti informací v rámci organizace a v případě potřeby externích stran podporujících takové činnosti.

1 Předmět normy

Tento dokument poskytuje směrnice pro řízení rizik bezpečnosti informací.

Tento dokument podporuje obecné koncepty specifikované v ISO/IEC 27001 a je navržen tak, aby pomáhal uspokojivě implementovat bezpečnost informací založenou na přístupu řízení rizik.

Znalost konceptů, modelů, procesů a terminologie popsaných v ISO/IEC 27001 a v ISO/IEC 27002 je důležitá pro úplné pochopení tohoto dokumentu.

Tento dokument je aplikovatelný na všechny typy organizací (například komerční společnosti, vládní úřady, neziskové organizace, které mají v úmyslu řídit rizika, která mohou ohrozit bezpečnost informací organizace.