ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Prosinec 2014**

Informační technologie – Bezpečnostní techniky – Řízení incidentů bezpečnosti informací

ČSN
ISO/IEC 27035
36 9799

Information technology – Security techniques – Information security incident management

Technologies de l,information – Techniques de sécurité – Gestion des incidents de sécurité de l,information

Tato norma je českou verzí mezinárodní normy ISO/IEC 27035:2011. 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 27035:2011. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

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 (všechny části) (36 9074) Informační technologie – Management služeb

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

ČSN ISO/IEC 27002 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací

ČSN ISO/IEC 27003 (36 9790) Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací

ČSN ISO/IEC 27004 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření

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

Vysvětlivky k textu převzaté normy

Pro účely této normy byl použit:

- překlad anglického termínu „management“ jako „řízení“ s ohledem na jeho preferované používání v oblasti IT a návaznosti na vydané normy z oblasti IT, zejména normy řady 27XXX;
- překlad anglického termínu „control“ preferovaně jako „opatření“ před významy „řízení“ nebo „kontrola“ a to z důvodu návaznosti na vydané normy řady 27XXX;
- v případech, kdy jsou u definice převzaté z odkazovaných norem uvedeny dva termíny (nebo více termínů), je první z nich termín preferovaně používaný v IT.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

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 27035
Řízení incidentů bezpečnosti informací První vydání
2011-09-01

Obsah

Strana

DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2011

Veškerá práva vyhrazena. Pokud není specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně fotokopií a mikrofilmů, bez písemného svolení buď od organizace ISO na níže uvedené adrese, nebo od členské organizace ISO v zemi žadatele.

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.org

Web www.iso.org

Published in Switzerland

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 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.

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

Hlavním úkolem společné technické komise je příprava mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají národním orgánům k hlasování. Vydání mezinárodní

normy vyžaduje souhlas alespoň 75% hlasujících národních orgánů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikování jakéhokoliv nebo všech patentových práv.

ISO/IEC 27035 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie,* subkomise SC 27 *IT Bezpečnostní techniky*.

Toto první vydání ISO/IEC 27035 zrušuje a nahrazuje ISO/IEC TR 18044:2004, která byla technicky revidována.

Úvod

Obecně samotné politiky nebo opatření v oblasti bezpečnosti informací nezaručují úplnou ochranu informací, informačních systémů, služeb nebo sítí. Po zavedení opatření se pravděpodobně vyskytnou zbytkové zranitelnosti, v jejichž důsledku může být bezpečnost informací neefektivní a mohou se tedy vyskytnout incidenty bezpečnosti informací. To může mít potenciální přímé i nepřímé nepříznivé dopady na činnosti organizace. Nutně také dojde k výskytu nových případů předem neidentifikovaných hrozeb. Nedostatečná připravenost organizace zabývat se takovými incidenty způsobí, že jakákoliv odezva bude méně efektivní a zvýší stupeň potenciálního nepříznivého dopadu na činnost organizace. Pro kteroukoliv organizaci, která to myslí s bezpečností informací vážně, je proto nejdůležitější, aby měla strukturovaný a plánovaný přístup k:

- detekování incidentů bezpečnosti informací, podávání zpráv o těchto incidentech a jejich posuzování;
- reagování na incidenty bezpečnosti informací, včetně aktivace vhodných opatření pro prevenci, snížení, a zotavení se z dopadů (například podporou oblastí krizového managementu);
- podávání zpráv o zranitelnostech bezpečnosti informací, které dosud nebyly zneužity k vyvolání událostí bezpečnosti informací a eventuálně incidentů bezpečnosti informací, a jejich přiměřeného posuzování a zabývání se jimi;
- poučení se z incidentů a zranitelností bezpečnosti informací, ustavení preventivních opatření a realizace zlepšování celkového přístupu k řízení incidentů bezpečnosti informací.

Tato mezinárodní norma poskytuje v kapitolách 4 až 9 návod k řízení incidentů bezpečnosti informací. Tyto kapitoly se skládají z několika článků, obsahujících podrobný popis každé fáze.

Termín „řízení incidentů bezpečnosti informací“, použitý v této mezinárodní normě, zahrnuje řízení nejen incidentů bezpečnosti informací, ale také zranitelností bezpečnosti informací.

1 Předmět normy

Tato mezinárodní norma poskytuje strukturovaný a plánovaný přístup k:

a. detekování incidentů bezpečnosti informací, podávání zpráv o těchto incidentech a jejich posuzování;
b. reagování na incidenty bezpečnosti informací a jejich zvládání;
c. detekování, posuzování a zvládání zranitelností bezpečnosti informací; a
d. neustálému zlepšování řízení bezpečnosti informací a incidentů jako výsledku zvládání incidentů a zranitelností bezpečnosti informací.

Tato mezinárodní norma poskytuje návod na řízení incidentů bezpečnosti informací pro velké a střední organizace. Menší organizace mohou použít základní sadu dokumentů, procesů a obvyklých postupů, popsaných v této mezinárodní normě, v závislosti na jejich velikosti a typu činnosti ve vztahu ke stavu v oblasti rizik bezpečnosti informací. Poskytuje také návod pro externí organizace, které poskytují procesu řízení incidentů bezpečnosti informací své služby.

Konec náhledu - text dále pokračuje v placené verzi ČSN.