ČESKÁ TECHNICKÁ NORMA

ICS 35.030 **Květen**
2018

Informační technologie – Bezpečnostní techniky –
Řízení incidentů bezpečnosti informací –
Část 1: Principy řízení incidentů

ČSN
ISO/IEC 27035-1

36 9799

Information technology – Security techniques – Information security incident management –
Part 1: Principles of incident management

Technologies de l,information – Techniques de sécurité – Gestion des incidents de sécurité de l,information –
Partie 1: Principes de la gestion des incidents

Tato norma je českou verzí mezinárodní normy ISO/IEC 27035-1:2016. 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 27035-1:2016. It was translated by
the Czech Standardization Agency. It has the same status as the official version.

Národní předmluva

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

ISO/IEC 27035-2 zavedena v ČSN ISO/IEC 27035-2 (36 9799) Informační technologie – Bezpečnostní techniky – Řízení incidentů bezpečnosti informací – Část 2: Směrnice pro plánování a přípravu odezvy na incidenty

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/IEC 20000-3 (36 9074) Informační technologie – Management služeb – Část 3: Pokyny pro vymezení rozsahu a použitelnosti ISO/IEC 20000-1

ČSN ISO/IEC 20000-6 (36 9074) Informační technologie – Management služeb – Část 6: Požadavky na orgány provádějící audit a certifikaci systémů managementu služeb

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/IEC 27003 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny

ČSN ISO/IEC 27004 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení

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

ČSN ISO/IEC 27031 (36 9801) Informační technologie – Bezpečnostní techniky – Směrnice pro připravenost informačních a komunikačních technologií pro kontinuitu činnosti organizace

ČSN ISO/IEC 27033-1 (36 9701) Informační technologie – Bezpečnostní techniky – Bezpečnost sítě – Část 1: Přehled a pojmy

ČSN ISO/IEC 27033-2 (36 9701) Informační technologie – Bezpečnostní techniky – Bezpečnost sítě – Část 2: Směrnice pro návrh a implementaci bezpečnosti sítě

ČSN ISO/IEC 27033-3 (36 9701) Informační technologie – Bezpečnostní techniky – Bezpečnost sítě – Část 3: Referenční síťové scénáře – Hrozby, techniky návrhu a otázky řízení

ČSN EN ISO/IEC 27037 (36 9846) Informační technologie – Bezpečnostní techniky – Směrnice pro identifikaci, sběr, získávání a uchovávání digitálních důkazů

ČSN EN ISO/IEC 27041 (36 9850) Informační technologie – Bezpečnostní techniky – Směrnice k zajištění vhodných a přiměřených metod zjišťování kolizních stavů

ČSN EN ISO/IEC 27042 (36 9851) Informační technologie – Bezpečnostní techniky – Směrnice pro analýzu a interpretaci uložených digitálních dat

ČSN EN ISO/IEC 27043 (36 9852) Informační technologie – Bezpečnostní techniky – Principy a procesy zjišťování kolizních stavů

ČSN ISO/IEC 30111 (36 9706) Informační technologie – Bezpečnostní techniky – Postupy zacházení se zranitelnostmi

Vysvětlivky k textu převzaté normy

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:

bot, botnet, hacking, malware, peer-to-peer, phishing, spam

Pro účely této normy byl použit:

– překlad anglického termínu „management“ jako „řízení“ s ohledem na jeho preferované používání v oblasti IT a v návaznosti na vydané normy z oblasti IT, zejména normy řady 27XXX;

– překlad anglického termínu „control“ jako „opatření“, „řízení“ nebo „kontrola“ s ohledem na význam v textu normy;

– v případech, kdy jsou u definice převzaté z odkazovaných norem uvedeny dva termíny (nebo více termínů), je první z nich preferovaně používaný v IT.

Upozornění na národní poznámky

V bibliografii je uvedena národní poznámka upozorňující na nesprávné označení dokumentu.

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 incidentů bezpečnosti informací – Část 1: Principy řízení incidentů

ISO/IEC 27035-1
První vydání
2016-11-01

ICS 35.030

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

Za tento dokument je odpovědná komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *IT Bezpečnostní techniky*.

Toto první vydání ISO/IEC 27035-1, společně s ISO/IEC 27035-2, zrušuje a nahrazuje ISO/IEC 27035:2011, které bylo technicky zrevidováno.

ISO/IEC 27035 se společným názvem *Informační technologie – Bezpečnostní techniky – Řízení incidentů bezpečnosti informací* se sestává z následujících částí:

– *Část 1: Principy řízení incidentů*

– *Část 2: Směrnice pro plánování a přípravu odezvy na incidenty*

Další části mohou následovat.

Úvod

Politiky bezpečnosti informací nebo opatření samotná nezaručují úplnou ochranu informací, informačních systémů, služeb nebo sítí. Po zavedení opatření je pravděpodobné, že zůstanou zbytkové zranitelnosti, které mohou snížit efektivnost bezpečnosti informací a usnadnit výskyt incidentů bezpečnosti informací. To může mít eventuálně přímý a nepřímý nepříznivý vliv na operace v podnikání organizace. Kromě toho je téměř jisté, že se vyskytnou nové případy předem neidentifikovaných hrozeb. Nedostatečná příprava ze strany organizace řešit takové incidenty bude mít za následek menší účinnost každé odezvy, a zvýší stupeň potenciálního nepříznivého dopadu na podnikání. Je proto pro každou organizaci podstatné požadovat silný program bezpečnosti informací, aby měla strukturovaný a plánovaný přístup k:

– zjišťování, podávání zpráv a posuzování incidentů bezpečnosti informací;

– odezvě na incidenty bezpečnosti informací zahrnující aktivaci příslušných opatření zabraňující dopadům, snižující dopady a zajišťující obnovu z dopadů;

– hlášení zranitelností bezpečnosti informací, aby mohly být náležitě posuzovány a řešeny;

– poučení se z incidentů bezpečnosti informací a zranitelností, ustavení preventivních opatření, a zajištění zlepšení celkového přístupu ke řízení incidentů bezpečnosti informací.

Aby se dosáhlo tohoto plánovaného přístupu, poskytuje ISO/IEC 27035 návod týkající se aspektů řízení incidentů bezpečnosti informací v následujících odpovídajících částech.

– ISO/IEC 27035-1 *Principy řízení incidentů* (tento dokument), uvádí základní koncepty a fáze řízení incidentů bezpečnosti informací, a jak řízení incidentů zlepšit. Tato část kombinuje tyto koncepty s principy ve strukturovaném přístupu k zjišťování, podávání zpráv, posuzování, a odezvám na incidenty, a aplikování poučení se z minulosti.

– ISO/IEC 27035-2 *Směrnice pro plánování a přípravu odezvy na incidenty* popisuje, jak plánovat a připravit se na odezvu na incidenty. Tato část pokrývá fáze „Plánování a příprava“ a „Poučení se z minulosti“ modelu popsaného v ISO/IEC 27035-1.

ISO/IEC 27035 má za cíl doplnit další normy a dokumenty, které poskytují návod týkající se vyšetřování a přípravy k vyšetřování incidentů bezpečnosti informací. ISO/IEC 27035 není komplexním pokynem, ale je odkazem na určité základní principy, jejichž cílem je zajistit, aby nástroje, techniky a metody byly vybrány účelně, vyvstane-li ta potřeba.

Zatímco ISO/IEC 27035 zahrnuje řízení incidentů bezpečnosti informací, pokrývá také některé aspekty zranitelností bezpečnosti informací. Návod ohledně odhalení zranitelností a zacházení se zranitelnostmi prodejci jsou uvedeny v ISO/IEC 29147 a ISO/IEC 30111, v tomto pořadí.

ISO/IEC 27035 také zamýšlí informovat pracovníky uskutečňující rozhodnutí, kteří potřebují určit spolehlivost jim předložených digitálních důkazů. To mohou použít organizace, které potřebují chránit, analyzovat a prezentovat potenciální digitální důkazy. Je to důležité pro orgány vytvářející politiku, která vytváří a hodnotí postupy týkající se digitálních důkazů, často jako část většího množství důkazů.

Další informace o normách týkajících se vyšetřování jsou uvedeny v příloze A.

1 Předmět normy

Tato část ISO/IEC 27035 je základem této mezinárodní normy o více částech. Předkládá základní koncepty a fáze řízení incidentů bezpečnosti informací a kombinuje tyto koncepty s principy ve strukturovaném přístupu ke zjišťování incidentů, podávání zpráv o incidentech, posuzování incidentů a reagující na incidenty, a použití poučení se z minulosti.

Principy uvedené v této části ISO/IEC 27035 jsou obecné a zamýšlené k použití pro všechny organizace, bez ohledu na typ, velikost nebo povahu. Organizace mohou upravit návod uvedený v této části ISO/IEC 27035 podle jejich typu, velikosti a povahy podnikání ve vztahu ke stavu rizik bezpečnosti informací. Tuto část ISO/IEC 27035 mohou také použít externí organizace poskytující služby řízení incidentů bezpečnosti informací.