ČESKÁ TECHNICKÁ NORMA

ICS 35.030 **Květen**
2018

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

Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response

Technologies de l,information – Techniques de sécurité – Gestion des incidents de sécurité de l,information –
Partie 2: Lignes directrices pour planifier et préparer une réponse aux incidents

Tato norma je českou verzí mezinárodní normy ISO/IEC 27035-2:2016. 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 27035-2:2016. It was translated by
the Czech Agency for Standardization. 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 27035-1:2016 zavedena v ČSN ISO/IEC 27035-1:2018 (36 9799) Informační technologie – Bezpečnostní techniky – Řízení incidentů bezpečnosti informací – Část 1: Principy řízení incidentů

Souvisící ČSN

ČSN ISO 8601 (97 9738) Datové prvky a formáty výměny – Výměna informací – Zobrazení data a času

ČSN EN ISO/IEC 27001:2014 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

ČSN EN ISO/IEC 27002:2014 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací

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 ISO/IEC 27033-4 (36 9701) Informační technologie – Bezpečnostní techniky – Bezpečnost sítě – Část 4: Zabezpečení komunikace mezi sítěmi s využitím bezpečnostních bran

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:

bedin, benchmarking, bootable, botnet, cloud, ethernet, firewall, hacking, helpdesk, malware, phishing, spam, warez

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.

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 2: Směrnice pro plánování a přípravu odezvy na incidenty

ISO/IEC 27035-2
První vydání
2016-11-01

ICS 35.030

Obsah

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 27035-2, společně s ISO/IEC 27035-1, 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

ISO/IEC 27035 je rozšířením řady norem ISO/IEC 27000 a je zaměřena na řízení incidentů bezpečnosti informací, které je identifikováno v ISO/IEC 27000 jako jeden z kritických klíčových faktorů pro systém řízení bezpečnosti informací.

Mezi plánem organizace pro incident a organizací, která ví, že je připravena na incident, může být velký rozdíl. Tato část ISO/IEC 27035 proto řeší vytvoření směrnic, aby zvýšila důvěru ve skutečnou připravenost organizace reagovat na incident bezpečnosti informací. Toho se dosáhne řešením politik a plánů spojených s řízením incidentů a ustavením týmu pro odezvu na incidenty a v průběhu času zlepšením jeho výkonnosti převzetím poučení se z minulosti a hodnocením.

1 Předmět normy

Tato část ISO/IEC 27035 poskytuje směrnice pro plánování a přípravu odezvy na incidenty. Směrnice vycházejí z fází „Plánování a příprava“ a „Poučení se z minulosti“ modelu „Fáze řízení incidentů bezpečnosti informací“ obsaženého v ISO/IEC 27035-1.

Hlavní body fáze „Plánování a příprava“ obsahují:

– politiku řízení incidentů bezpečnosti informací a závazek vrcholového vedení;

– politiky bezpečnosti informací včetně politik týkajících se řízení rizik, aktualizované jak na korporátní úrovni, tak na úrovni systému, služby a sítě;

– plán řízení incidentů bezpečnosti informací;

– ustavení týmu pro odezvu na incidenty (IRT);

– ustavení vztahů a kontaktů s interními a externími organizacemi;

– technickou a jinou podporu (včetně organizační a provozní podpory);

– instruktáže a školení o povědomí řízení incidentů bezpečnosti informací;

– testování plánu řízení incidentů bezpečnosti informací.

Principy uvedené v této části ISO/IEC 27035 jsou obecné a mohou je použít 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.