ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Leden 2016**

Informační technologie – Bezpečnostní techniky – Směrnice pro připravenost informačních a komunikačních technologií pro kontinuitu činnosti organizace

ČSN
ISO/IEC 27031
36 9801

Information technology – Security techniques – Guidelines for information and communication technology readiness
for business continuity

Technologies de l,information – Techniques de sécurité – Lignes directrices pour mise en état des technologies
de la communication et de l,information pour continuité des affaires

Tato norma je českou verzí mezinárodní normy ISO/IEC 27031:2011. 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 27031:2011. 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 TR 18044:2004 nezavedena1)

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

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

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

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

Souvisící ČSN

ČSN BS 25999-1:2009 (01 0370) Management kontinuity činností organizace – Část 1: Soubor zásad

ČSN EN ISO 9000:2006 (01 0300) Systémy managementu kvality – Základní principy a slovník

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

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 EN 31010:2011 (01 0352) Management rizik – Techniky posuzování rizik

Vysvětlivky k textu převzaté normy

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

cloud, cluster, end-to-end, hacking, helpdesk, hosting, malware, router

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČ 40654419

Technická normalizační komise: TNK 42 Výměna dat

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

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 27031
Směrnice pro připravenost informačních a komunikačních technologií pro kontinuitu činnosti organizace

První vydání
2011-03-01

ICS 35.040

Obsah

Strana

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 svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. 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 vypracování 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 nelze činit odpovědnými za identifikování jakéhokoliv nebo všech patentových práv.

ISO/IEC 27031 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie,* subkomise SC 27 *IT Bezpečnostní techniky*.

Úvod

Během let se informační a komunikační technologie (ICT) staly nedílnou součástí mnoha činností, které jsou prvky kritických infrastruktur ve všech organizačních odvětvích, ať už veřejných, soukromých nebo dobrovolných. Rozšíření Internetu a dalších elektronických síťových služeb a dnešní schopnosti systémů a aplikací také znamenalo, že organizace se stále více spoléhají na spolehlivé, zajištěné a bezpečné infrastruktury ICT.

Mezitím byla rozpoznána potřeba řízení kontinuity činnosti organizace (BCM), včetně připravenosti na incidenty, plánování obnovy po havárii a reakce na mimořádné události a jejich řízení, a podporována specifickými oblastmi vědomostí, odborných znalostí a norem vyvinutých a uveřejněných v nedávných letech, včetně mezinárodní normy zabývající se BCM vyvinuté ISO/TC 223.

POZNÁMKA ISO/TC 223 je v procesu vývoje relevantní mezinárodní normy řízení kontinuity činnosti organizace (ISO 22301).

Selhání služeb ICT, včetně výskytu bezpečnostních problémů jako jsou průniky do systémů a nakažení malwarem, ovlivní kontinuitu provozní činnosti organizace. Proto řízení ICT a související kontinuity a jiných bezpečnostních aspektů tvoří klíčovou část požadavků kontinuity činnosti organizace. Navíc ve většině případů jsou kritické funkce činnosti organizace, které vyžadují kontinuitu činnosti organizace, obvykle závislé na ICT. Tato závislost znamená, že narušení ICT mohou představovat strategická rizika pro pověst organizace a její schopnosti fungovat.

Připravenost ICT je pro mnoho organizací základní součástí při implementaci řízení kontinuity činnosti organizace a řízení bezpečnosti informací. Jako součást implementace a provozu systému řízení bezpečnosti informací (ISMS) specifikovaného v ISO/IEC 27001 a systému řízení kontinuity činnosti organizace (BCMS) je rozhodující vyvíjet a implementovat plán připravenosti služeb ICT, aby pomohl zajistit kontinuitu činnosti organizace.

Výsledkem je, že efektivní BCM je často závislé na efektivní připravenosti ICT k zajištění toho, že cíle organizace mohou být i v době narušení nadále splněny. To je zvláště důležité, protože následky narušení ICT často způsobují další komplikace tím, že jsou neviditelné a/nebo je obtížné je detekovat.

Aby organizace dosáhla připravenosti ICT pro kontinuitu činnosti organizace (IRBC), potřebuje zavést systematický postup pro prevenci, předpovídání a řízení narušení a incidentů ICT, které mají potenciál narušit služby ICT. Toho může být nejlépe dosaženo uplatněním cyklických kroků Plánovat–Provádět–Kontrolovat–Jednat (PDCA) jako součásti systému řízení v ICT IRBC. Tímto způsobem IRBC podporuje BCM zajištěním, že služby ICT jsou stejně odolné jako vhodné a mohou být obnoveny na předem určené úrovně v časových lhůtách požadovaných a schválených organizací.

Tabulka 1 – Cyklus Plánovat–Provádět–Kontrolovat–Jednat v IRBC

Plánovat	Ustavit politiky, záměry, cíle, procesy a postupy týkající se řízení rizik a zlepšování připravenosti ICT pro dosažení výsledků v souladu s celkovými politikami a cíli kontinuity podnikání organizace.
Provádět	Zavést a provozovat politiky, opatření, procesy a postupy IRBC.
Kontrolovat	Posoudit a v příslušných případech měřit výkonnost procesů vůči politice, cílům a praktickým zkušenostem IRBC a předkládat výsledky vedení k přezkoumání.
Jednat	Uplatnit nápravné a preventivní kroky na základě výsledků přezkoumání vedením, aby se dosáhlo neustálého zlepšování IRBC.

Pokud organizace používá ISO/IEC 27001 k ustavení ISMS a/nebo používá relevantní normy k ustavení BCMS, ustavování IRBC by mělo pokud možno vzít v úvahu existující nebo zamýšlené procesy související s těmito normami. Tato vazba může podporovat ustavování IRBC a také umožňuje organizaci vyhnout se jakýmkoli zdvojeným procesům. Obrázek 1 shrnuje interakce IRBC a BCSM.

Při plánování a implementaci IRBC může organizace odkazovat k ISO/IEC 24762:2008 v jejím plánování a poskytování služeb obnovy po havárii ICT bez ohledu na to, zda jsou tyto služby organizaci poskytovány subdodavatelsky nebo interně.

Obrázek 1 – Integrace IRBC a BCMS

1 Předmět normy

Tato mezinárodní norma popisuje pojmy a principy připravenosti informačních a komunikačních technologií (ICT) pro kontinuitu činnosti organizace a poskytuje rámec metod a postupů k identifikování a specifikování všech aspektů (jako jsou výkonnostní kritéria, návrh a implementace) pro zlepšení připravenosti ICT organizace k zajištění kontinuity činnosti organizace. To lze uplatnit u jakékoliv organizace (soukromé, státní a nestátní neziskové, bez ohledu na velikost) rozvíjející svůj program připravenosti ICT pro kontinuitu činnosti organizace (IRBC) a vyžadující, aby její ICT služby/infrastruktury byly připraveny k podpoře provozu organizace v případě vzniku událostí a incidentů a sou-
visejících narušení, které mohou ovlivnit kontinuitu (včetně bezpečnosti) kritických podnikových funkcí. To také umož-
ňuje organizaci měřit parametry výkonnosti, které korelují s její IRBC konzistentním a rozpoznaným způsobem.

Předmět této mezinárodní normy zahrnuje všechny události a incidenty (včetně souvisejících s bezpečností), které mohou mít vliv na ICT infrastrukturu a systémy. To zahrnuje a rozšiřuje postupy řešení a řízení incidentů bezpečnosti informací a služby a plánování připravenosti ICT.