ČESKÁ TECHNICKÁ NORMA

ICS 35.030 **Květen**
2023

Informační technologie – Management incidentů informační bezpečnosti – Část 3: Směrnice pro činnosti odezvy na incidenty ICT	ČSN ISO/IEC 27035-3 36 9799

Information technology – Information security incident management –
Part 3: Guidelines for ICT incident response operations

Technologies de l,information – Gestion des incidents de sécurité de l,information –
Partie 3: Lignes directrices relatives aux opérations de réponse aux incidents TIC

Tato norma je českou verzí mezinárodní normy ISO/IEC 27035-3:2020. 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 27035-3:2020. 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 27035-1 zavedena v ČSN ISO/IEC 27035-1 (36 9799) Informační technologie – Bezpečnostní techniky – Řízení incidentů bezpečnosti informací – Část 1: Principy řízení incidentů

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

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

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

Souvisící ČSN

ČSN EN ISO 22301 (01 2306) Bezpečnost a odolnost – Systémy managementu kontinuity podnikání –

Požadavky

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

ČSN EN ISO/IEC 27002 (36 9798) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti

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

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 27042:2017 (36 9851) Informační technologie – Bezpečnostní techniky – Směrnice pro analýzu a interpretaci uložených digitálních dat

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článcích „Informace
o citovaných dokumentech“ a „Souvisící ČSN“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných evropských/mezinárodních norem (včetně všech změn).

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:

CAPTCHAS, darknet, hacking, honeypot, netflow, phishing, proxy, rootkit, sandbox, shell, spamtrap, spyware

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČO 40654419

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 – Management incidentů informační bezpečnosti – Část 3: Směrnice pro činnosti odezvy na incidenty ICT

ISO/IEC 27035-3
První vydání
2020-09

ICS 35.030

Obsah

Strana

Strana

ISO copyright office
CP 401 · Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Tel.: + 41 22 749 01 11
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 i nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk.

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) nebo v seznamu patentových prohlášení obdržených IEC (viz http://patents.iec.ch).

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 www.iso.org/iso/foreword.html.

Tento dokument vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie,* subkomise SC 27 *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí.*

Seznam všech částí souboru ISO/IEC 27035 lze nalézt na webových stránkách ISO.

Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na www.iso.org/members.html.

Úvod

Incident informační bezpečnosti může, ale nemusí zahrnovat ICT. Například informace, která se neúmyslně rozšíří ztrátou papírových dokumentů, může velmi dobře představovat závažný incident informační bezpečnosti, který vyžaduje hlášení incidentu, vyšetřování, omezení, nápravná opatření a zapojení vedení. Tento typ managementu incidentů často provádí například hlavní ředitel pro informační bezpečnost (CISO) v rámci organizace. Pokyny pro management takových incidentů informační bezpečnosti lze nalézt v ISO/IEC 27035-1. Tento dokument se však zabývá pouze činnostmi odezvy na incidenty související s ICT, nikoliv incidenty informační bezpečnosti souvisejícími s papírovými dokumenty nebo jakýmikoli jinými incidenty, které se netýkají ICT. Kdykoli je v tomto dokumentu použit termín „informační bezpečnost“, je tak činěno v kontextu informační bezpečnosti související s ICT.

Organizační struktury pro informační bezpečnost se liší v závislosti na velikosti a oblasti podnikání organizací. Vzhledem k tomu, že dochází k různým a četným incidentům a jejich počet narůstá (jako jsou síťové incidenty, např. průniky, narušení dat a hackerské útoky), organizace mají stále větší obavy o informační bezpečnost. Bezpečné ICT prostředí nastavené tak, aby odolalo různým typům útoků (jako jsou DoS, červi a viry) pomocí zařízení pro zabezpečení sítě, jako jsou firewally, systémy detekce průniku (IDS) a systémy prevence průniku (IPS), by mělo být doplněno jasnými provozními postupy pro řešení incidentů spolu s dobře definovanými systémy podávání zpráv v rámci organizace.

K zajištění důvěrnosti, integrity a dostupnosti informací a k účinnému řešení incidentů je zapotřebí schopnost vykonávat činnosti odezvy na incidenty. Za tímto účelem by měl být zřízen tým pro odezvu na incidenty počítačové bezpečnosti (CSIRT), který bude provádět úkoly, jako je monitorování, detekce, analýza a odezvy na shromážděná data nebo bezpečnostní události. Tyto úkoly mohou být podporovány nástroji a technikami umělé inteligence.

Tento dokument podporuje opatření dle ISO/IEC 27001:2013, příloha A, týkající se managementu incidentů.

Ne všechny kroky v tomto dokumentu jsou použitelné, protože závisí na konkrétním incidentu. Například menší organizace nemusí použít všechny pokyny v tomto dokumentu, ale může je považovat za užitečné pro organizaci svých činností souvisejících s incidenty ICT, zejména pokud provozuje své vlastní ICT prostředí. Dokument může být také užitečný pro menší organizace, které své IT činnosti zajišťují pomocí vnějších zdrojů, aby lépe porozuměly požadavkům na činnosti související s incidenty a provádění těchto činností, a které by měly očekávat od svého dodavatele (dodavatelů) ICT.

Tento dokument je užitečný zejména pro organizace poskytující služby ICT, které zahrnují interakce mezi organizacemi činností souvisejících s incidenty s cílem dodržovat stejné procesy a podmínky.

Tento dokument také umožňuje lépe porozumět tomu, jak se činnosti související s incidenty vztahují k uživatelům/
zákazníkům, aby bylo možné definovat, kdy a jak má taková interakce probíhat, i když to není specifikováno.

1 Předmět normy

Tento dokument poskytuje směrnice pro odezvu na incidenty informační bezpečnosti v rámci činností ICT v oblasti bezpečnosti. Tento dokument se nejprve zabývá provozními aspekty činností ICT v oblasti bezpečnosti z hlediska lidí, procesů a technologií. Dále se zaměřuje na odezvu na incidenty informační bezpečnosti v rámci činností ICT v oblasti bezpečnosti včetně detekce incidentů informační bezpečnosti, podávání zpráv, třídění, analýzy, odezvy, omezení, eliminace dopadu, obnovy a uzavření incidentů informační bezpečnosti.

Tento dokument se nezabývá činnostmi odezvy na incidenty, které se netýkají ICT, jako je ztráta papírových dokumentů.

Tento dokument vychází z fáze „Zjišťování a podávání zpráv“, fáze „Posouzení a rozhodnutí“ a fáze „Odezvy“ modelu „Fáze managementu incidentů informační bezpečnosti“ uvedeného v ISO/IEC 27035-1:2016.

Zásady uvedené v tomto dokumentu jsou obecné a mají být použitelné pro všechny organizace bez ohledu na jejich typ, velikost nebo povahu. Organizace si mohou ustanovení uvedená v tomto dokumentu upravit podle svého typu, velikosti a povahy činnosti ve vztahu k situaci v oblasti rizik informační bezpečnosti.

Tento dokument je také použitelný pro externí organizace poskytující služby managementu incidentů informační bezpečnosti.