ČESKÁ TECHNICKÁ NORMA

ICS 35.030 **Březen 2024**

Informační technologie – Management incidentů informační bezpečnosti – Část 1: Principy a proces

ČSN ISO/IEC 27035-1

36 9799

Information technology – Information security incident management – Part 1: Principles and process

Technologies de l,information – Gestion des incidents de sécurité de l,information – Partie 1: Principes et processus

Tato norma je českou verzí mezinárodní normy ISO/IEC 27035-1:2023. 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 27035-1:2023. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 27035-1 (36 9799) z května 2018.

Národní předmluva

Změny proti předchozí normě

Název normy byl změněn. Do normy byly doplněny nové články a nová příloha D. Celý text normy byl redakčně zrevidován.

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

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: Návod pro použití systémů managementu služeb

ČSN ISO/IEC 20000-3 (36 9074) Informační technologie – Management služeb – Část 3: Návod 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 27001:2023 (36 9797) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí –
Systémy managementu informační bezpečnosti – Požadavky

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

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 bezpečnost, kybernetická bezpečnost a ochrana soukromí – Pokyny pro management rizik informační bezpečnosti

ČSN ISO/IEC 27031:2016 (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 27035-2:2024 (36 9799) Informační technologie – Management incidentů informační bezpečnosti –
Část 2: Směrnice pro plánování a přípravu odezvy na incidenty

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

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

ČSN EN ISO/IEC 27038 (36 9847) Informační technologie – Bezpečnostní techniky – Specifikace pro digitální zpracování dokumentů

ČSN EN ISO/IEC 27040 (36 9849) Informační technologie – Bezpečnostní techniky – Zabezpečení úložišť dat

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 EN ISO/IEC 29147 (36 9713) Informační technologie – Bezpečnostní techniky – Odhalování zranitelností

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

ČSN EN ISO/IEC 30121 (36 9044) Informační technologie – Správa forenzního rámce rizik

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 je anglický termín „guidance“ přeložen jako „pokyn“ vzhledem k jeho používání v oblasti IT a v návaznosti na vydané normy z oblasti IT, zejména souboru norem ISO/IEC 27XXX. Český ekvivalent „návod“ je vzhledem ke kontextu nevhodný a v praxi se v souvislosti se souborem norem ISO/IEC 27XXX nepoužívá.

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, broadcast, phishing, push.

MEZINÁRODNÍ NORMA

Informační technologie – Management incidentů informační bezpečnosti – Část 1: Principy a proces

ISO/IEC 27035-1
Druhé vydání
2023-02

ICS 35.030

Obsah

Strana

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.

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 nebo www.iec.ch/members_experts/refdocs).

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 https://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. V IEC viz www.iec.ch/understanding-standards.

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

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 27035-1:2016), které bylo technicky zrevidováno.

Hlavní změny jsou:

- název byl modifikován;
- v kapitole 3 jsou definovány nové termíny „tým pro management incidentů“ a „koordinátor incidentů“;
- v kapitole 4 jsou doplněny nové články 4.5, 4.6 a 4.7;
- název kapitoly 5 byl změněn na „Proces“;
- příloha C byla aktualizována;
- byla doplněna nová příloha D;
- text byl redakčně zrevidován.

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

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
a www.iec.ch/national-committees.

Úvod

Soubor ISO/IEC 27035 poskytuje další pokyny k opatřením pro management incidentů v ISO/IEC 27002. Tato opatření mají být zavedena na základě rizik informační bezpečnosti, kterým organizace čelí.

Samotné politiky nebo opatření informační bezpečnosti nezaručují úplnou ochranu informací, informačních systémů, služeb nebo sítí. Po zavedení opatření pravděpodobně zůstanou zbytkové zranitelnosti, které mohou snížit efektivnost informační bezpečnosti a usnadnit výskyt incidentů informační bezpečnosti. To může mít potenciálně přímé i nepřímé nepříznivé důsledky na činnosti organizace. Kromě toho je nevyhnutelné, že nové případy dříve neidentifikovaných hrozeb způsobí výskyt incidentů. Nedostatečná příprava organizace na vypořádání takových incidentů snižuje efektivnost jakékoli odezvy a zvyšuje míru potenciálních nepříznivých důsledků na činnost organizace. Proto je pro každou organizaci, která touží po silném programu informační bezpečnosti, nezbytné mít strukturovaný a plánovaný přístup k:

- plánování a přípravě managementu incidentů informační bezpečnosti, včetně politiky, organizace, plánu, technické podpory, školení o povědomí a dovednostech atd.;
- detekci incidentů informační bezpečnosti, podávání zpráv o nich a jejich posouzení a detekci zranitelností spojených s incidentem, podávání zpráv o nich a jejich posuzování;
- odezvě na incidenty informační bezpečnosti, včetně aktivace příslušných opatření k prevenci a omezení a zotavení z dopadu;
- náležitě řešit nahlášené zranitelnosti informační bezpečnosti související s incidentem;
- poučit se z incidentů informační bezpečnosti a zranitelností souvisejících s incidentem, zavést a ověřit preventivní opatření a zlepšit celkový přístup k managementu incidentů informační bezpečnosti.

Soubor ISO/IEC 27035 je určen k doplnění dalších norem a dokumentů, které poskytují pokyny pro vyšetřování a přípravu na vyšetřování incidentů informační bezpečnosti. Soubor ISO/IEC 27035 není vyčerpávajícím pokynem, ale odkazem na určité základní principy a definovaný proces, které mají zajistit, aby v případě potřeby bylo možné vhodně vybrat nástroje, techniky a metody a prokázat jejich vhodnost pro daný účel.

Ačkoli soubor ISO/IEC 27035 zahrnuje management incidentů informační bezpečnosti, pokrývá také některé aspekty zranitelností informační bezpečnosti. Pokyny týkající se odhalování zranitelností a zacházení se zranitelnostmi ze strany dodavatelů jsou rovněž uvedeny v ISO/IEC 29147, resp. ISO/IEC 30111.

Cílem souboru ISO/IEC 27035 je rovněž informovat osoby s rozhodovací pravomocí při určování spolehlivosti digitálních důkazů, které jim jsou předkládány. Je použitelný pro organizace, které potřebují chránit, analyzovat a prezentovat potenciální digitální důkazy. Je relevantní pro orgány vytvářející politiky, které vytvářejí a hodnotí postupy týkající se digitálních důkazů, často jako součást většího souboru důkazů.

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

1 Předmět normy

Tento dokument je základem souboru norem ISO/IEC 27035. Představuje základní koncepty, principy a proces s klíčovými činnostmi managementu incidentů informační bezpečnosti, které poskytují strukturovaný přístup k přípravě na incidenty, jejich detekci, podávání zpráv o incidentech, posuzování incidentů a odezvě na incidenty a uplatňování získaných poznatků.

Pokyny k procesu managementu incidentů informační bezpečnosti a jeho klíčovým činnostem uvedené v tomto dokumentu jsou obecné a mají být použitelné pro všechny organizace bez ohledu na jejich typ, velikost nebo povahu. Organizace si mohou pokyny 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.