ČESKÁ TECHNICKÁ NORMA

ICS 35.030 **Březen 2024**

Informační technologie – Management incidentů informační bezpečnosti –
Část 2: Směrnice pro plánování a přípravu odezvy na incidenty

ČSN ISO/IEC 27035-2

36 9799

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

Technologies de l,information – 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 27035-2:2023. 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 27035-2:2023. 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 27035-2 (36 9799) z května 2018.

Národní předmluva

Změny proti předchozí normě

Název normy byl změněn. Do normy byly doplněny nové články. Kapitola 7 byla reorganizována a byla aktualizována bibliografie.

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 27035-1:2023 zavedena v ČSN ISO/IEC 27035-1:2024 (36 9799) Informační technologie – Management incidentů informační bezpečnosti – Část 1: Principy a proces

Souvisící ČSN

ČSN EN ISO/IEC 27001:2023 (36 9797) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky

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

Požadavky

ČSN EN ISO 22313 (01 2316) Bezpečnost a odolnost – Systémy managementu kontinuity podnikání – Pokyny pro používání ISO 22301

ČSN EN ISO/IEC 27002:2023 (36 9798) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti

ČSN ISO/IEC 27005:2023 (36 9790) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Pokyny pro management rizik informační bezpečnosti

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

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

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

ČSN ISO 8601 (soubor) (97 8601) Datum a čas – Zobrazení pro výměnu informací

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, hacking, hoax, phishing, ransomware, warez.

Upozornění na národní poznámky

Do normy byla k článku 6.4 doplněna vysvětlující národní poznámka.

MEZINÁRODNÍ NORMA

Informační technologie – Management incidentů bezpečnosti informací – Část 2: Směrnice pro plánování a přípravu odezvy na incidenty

ISO/IEC 27035-2
Druhé vydání
2023-02

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.

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 27035-2:2016), které bylo technicky zrevidováno.

Hlavní změny jsou:

- název byl modifikován;
- byly doplněny nové role včetně týmu pro management incidentů a koordinátora incidentů a jejich odpovědnosti;
- obsah týkající se managementu zranitelností byl modifikován;
- v části 6.7 byl přidán obsah týkající se doporučeného procesu pro organizace;
- struktura kapitoly 7 byla reorganizována;
- část C.3 byla nahrazena jediným odstavcem;

– bibliografie byla aktualizována.

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

Tento dokument se zaměřuje na management incidentů informační bezpečnosti, který je v ISO/IEC 27000 uveden jako jeden z kritických faktorů úspěchu systému managementu informační bezpečnosti.

Mezi plánem organizace na incident a připraveností organizace na incident může být velká propast. Proto se tento dokument zabývá vývojem postupů pro zvýšení důvěry ve skutečnou připravenost organizace reagovat na incident informační bezpečnosti. Toho je dosaženo řešením politik a plánů souvisících s managementem incidentů, jakož i procesem vytvoření týmu pro odezvu na incidenty a zlepšováním jeho výkonnosti v průběhu času přijímáním získaných zkušeností a vyhodnocováním.

1 Předmět normy

Tento dokument obsahuje směrnice pro plánování a přípravu odezvy na incidenty a poučení se z odezvy na incidenty. Směrnice vycházejí z fází „plánování a přípravy“ a „poučení se“ modelu fází managementu incidentů informační bezpečnosti uvedeného v ISO/IEC 27035-1:2023, 5.2 a 5.6.

Mezi hlavní body fáze „plánování a přípravy“ patří:

- politika managementu incidentů informační bezpečnosti a závazek vrcholového vedení;
- politiky informační bezpečnosti, včetně těch, které se týkají managementu rizik, aktualizované jak na úrovni organizace, tak na úrovni systému, služeb a sítě;
- plán managementu incidentů informační bezpečnosti;
- ustavení týmu pro management incidentů (IMT);
- navázání vztahů a spojení s interními a externími organizacemi;
- technická a jiná podpora (včetně organizační a provozní podpory);
- instruktáže a školení týkající se managementu incidentů informační bezpečnosti.

Fáze „poučení se“ zahrnuje:

- určení oblastí pro zlepšení;
- identifikaci a provedení nezbytných zlepšení;
- vyhodnocení týmu pro odezvu na incident (IRT).

Pokyny uvedené v tomto dokumentu jsou obecné a mají být použitelné pro všechny organizace bez ohledu na jejich typ, velikost nebo povahu. Organizace mohou pokyny uvedené v tomto dokumentu upravit podle svého typu, velikosti a povahy činnosti ve vztahu k situaci v oblasti rizik informační bezpečnosti. Tento dokument je použitelný i pro externí organizace poskytující služby managementu incidentů informační bezpečnosti.