ČESKÁ TECHNICKÁ NORMA

ICS 35.030

Březen 2026

Informační technologie –
Management incidentů informační bezpečnosti –
Část 4: Koordinace

ČSN
ISO/IEC 27035-4

36 9799

Information technology – Information security incident management –
Part 4: Coordination

Technologies de l,information – Gestion des incidents de sécurité de l,information –
Partie 4: Coordination

Tato norma je českou verzí mezinárodní normy ISO/IEC 27035-4:2024. 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 27035-4:2024. 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 – Management incidentů informační bezpečnosti – Část 1: Principy a proces

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

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

Souvisící ČSN

ČSN EN ISO 22300:2023 (01 2301) Bezpečnost a odolnost – Slovník

ČSN EN ISO 22397:2019 (01 2340) Ochrana společnosti – Pokyny pro ustanovení partnerských dohod

ČSN EN ISO/IEC 29147:2020 (36 9713) Informační technologie – Bezpečnostní techniky –

Odhalování zranitelností

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článku „Informace o citovaných dokumentech“ 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).

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:

bot, botnet, phishing, rootkit, watering hole.

Vypracování normy

Zpracovatel odborného překladu: Ing. Vladimír Pračke, IČO 40654419

Technická normalizační komise: TNK 20 Informační technologie

Vydala: Česká agentura pro standardizaci, státní příspěvková organizace

Citované dokumenty a souvisící ČSN lze získat v e-shopu.

MEZINÁRODNÍ NORMA

Informační technologie – Management incidentů informační bezpečnosti – Část 4: Koordinace

ISO/IEC 27035-4

První vydání

2024-12

ICS 35.030

Obsah

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).

ISO a IEC upozorňují na možnost, že implementace tohoto dokumentu smí vyžadovat využití patentu (patentů). V souvislosti s tím ISO a IEC nezaujímají žádné stanovisko týkající se důkazů, platnosti nebo použitelnosti všech uplatňovaných patentových práv. Ke dni zveřejnění tohoto dokumentu ISO a IEC neobdržely oznámení o patentu (patentech), který smí být vyžadován pro implementaci tohoto dokumentu. ISO a IEC však upozorňují implementující organizace, že se nemusí jednat o nejnovější informace, které lze získat z databáze patentů dostupné na adresách www.iso.org/patents a https://patents.iec.ch. ISO a IEC nelze činit odpovědné za identifikaci jakéhokoliv nebo všech takových patentových práv.

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), viz www.iso.org/iso/foreword.html. V IEC viz www.iec.ch/understanding-standards.

Tento dokument vypracovala společná technická komise ISO/IEC JTC1 *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 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 adresách www.iso.org/members.html a www.iec.ch/national-committees.

Úvod

Koordinace je důležitým aspektem při managementu incidentů v oblasti informační bezpečnosti. Mohou nastat incidenty přesahující hranice organizace, které nelze snadno vyřešit v rámci jediné organizace. Vznikající hrozby jsou stále sofistikovanější a mohou mít mnohem větší dopad než dříve. Vzhledem k charakteristikám vznikajících hrozeb a útoků je koordinace incidentů napříč organizacemi naléhavější než kdy dříve.

Koordinace může zahrnovat příslušné strany v rámci organizace i mimo ni. Mezi relevantní strany v rámci organizace patří například obchodní manažeři a zástupci IT; externí zainteresované strany zahrnují týmy pro odezvu na incidenty externích organizací a organizace činné v trestním řízení. Úplný seznam viz ISO/IEC 27035-2:2023, kapitola 8. Tento dokument se však zabývá pouze koordinací mezi více organizacemi. Tento dokument poskytuje směrnice pro spolupráci více organizací při řešení incidentů informační bezpečnosti. Koordinační činnosti probíhají v rámci celého procesu řízení incidentů informační bezpečnosti, jak je definován v ISO/IEC 27035-1.

Tento dokument se zabývá koordinací řízení incidentů informační bezpečnosti mezi více organizacemi. Incidenty někdy zahrnují technické zranitelnosti. Pokyny pro koordinaci, zveřejňování a řešení technických zranitelností poskytují ISO/IEC 29147 a ISO/IEC 30111. Další informace o koordinaci technických zranitelností mezi více organizacemi poskytuje ISO/IEC TR 5895.

1 Předmět normy

Tento dokument poskytuje pokyny pro více organizací, které koordinovaně řeší incidenty informační bezpečnosti. Zabývá se také dopady externí spolupráce na interní řízení incidentů v jednotlivých organizacích a poskytuje směrnice pro jednotlivé organizace, jak se přizpůsobit koordinačnímu procesu. Dále poskytuje směrnice pro
koordinační tým, pokud existuje, k provádění koordinačních činností podporujících odezvu na incidenty napříč organizacemi.

Zásady uvedené v tomto dokumentu jsou obecné a jsou určeny k použití ve více organizacích, které spolupracují na řešení incidentů informační bezpečnosti bez ohledu na jejich typ, velikost nebo povahu. Organizace mohou pokyny uvedené v tomto dokumentu upravit podle svého typu, velikosti a povahy své činnosti ve vztahu k situaci v oblasti rizik informační bezpečnosti. Tento dokument je použitelný i pro jednotlivé organizace, které se účastní partnerských vztahů.