PŘEDBĚŽNÁ ČESKÁ TECHNICKÁ NORMA

ICS 35.030 **Leden 2022**

Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Směrnice pro vývoj rámce kybernetické bezpečnosti	ČSN P ISO/IEC TS 27110 36 9773

Information technology, cybersecurity and privacy protection – Cybersecurity framework development guidelines

Sécurité de l,information, cybersécurité et protection de la vie privée – Lignes directrices relatives a l,élaboration d,un cadre en matiere de cybersécurité

Tato předběžná norma je českou verzí technické specifikace ISO/IEC TS 27110:2021. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This prestandard is the Czech version of the Technical Specification ISO/IEC TS 27110:2021. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Národní předmluva

Upozornění na používání této normy

Tato předběžná česká technická norma přejímá technickou specifikaci ISO/IEC TS 27110:2021 vydanou v souladu se směrnicemi ISO/IEC, část 1 a je určena k ověření. Případné připomínky k obsahu normy přijímá Česká agentura pro standardizaci.

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 TS 27100 zavedena v ČSN P ISO/IEC TS 27100 (36 9771) Informační technologie – Kybernetická bezpečnost – Přehled a pojmy

Souvisící ČSN

ČSN ISO/IEC 27032:2013 (36 9790) Informační technologie – Bezpečnostní techniky – Směrnice pro kybernetickou bezpečnost

ČSN ISO/IEC 30141 (36 9021) Internet věcí (IoT) – Referenční architektura

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).

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.

TECHNICKÁ SPECIFIKACE

Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Směrnice pro vývoj rámce kybernetické bezpečnosti

ISO/IEC TS 27110
První vydání
2021-02

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).

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 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), viz www.iso.org/iso/foreword.html.

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

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

Úvod

Kybernetická bezpečnost představuje naléhavý problém v souvislosti s používáním propojených technologií.
Kybernetické hrozby se neustále vyvíjejí, a proto je ochrana uživatelů a organizací neustálou výzvou. Aby se s touto výzvou vyrovnaly, vytvářejí podnikatelské skupiny, vládní agentury a další organizace dokumenty a nástroje nazývané rámce kybernetické bezpečnosti, které pomáhají organizovat činnosti organizací v oblasti kybernetické bezpečnosti a komunikovat o nich. Tyto organizace vytvářející rámce kybernetické bezpečnosti jsou označovány jako „tvůrci rámců kybernetické bezpečnosti“. Ostatní organizace a jednotlivci pak rámec kybernetické bezpečnosti používají nebo se na něj odvolávají při svých činnostech v oblasti kybernetické bezpečnosti.

Vzhledem k tomu, že existuje více tvůrců rámců kybernetické bezpečnosti, existuje i mnoho rámců kybernetické bezpečnosti. Současný soubor rámců kybernetické bezpečnosti je různorodý a pestrý. Organizace, které používají rámce kybernetické bezpečnosti, se potýkají s problémem sladění různých lexikonů a koncepčních struktur tak, aby vyhovovaly jejich požadavkům. Tyto rámce kybernetické bezpečnosti se pak stávají konkurenčními zájmy o koncové zdroje. Dodatečné úsilí by mohlo být lépe vynaloženo na implementaci kybernetické bezpečnosti a boj s hrozbami.

Cílem tohoto dokumentu je zajistit, aby se k definování rámců kybernetické bezpečnosti používal minimální soubor konceptů, který by pomohl zmírnit zátěž tvůrců rámců kybernetické bezpečnosti a uživatelů rámců kybernetické bezpečnosti.

Protože se tento dokument omezuje na minimální sadu konceptů, je jeho délka záměrně omezena na minimum. Tento dokument není určen k zneplatnění nebo nahrazení požadavků ISMS uvedených v ISO/IEC 27001.

Zásady tohoto dokumentu jsou následující:

- flexibilita – umožnit existenci více typů rámců kybernetické bezpečnosti;
- kompatibilita – umožnit sladění více rámců kybernetické bezpečnosti; a
- interoperabilita – umožnit platnost více způsobů použití rámce kybernetické bezpečnosti.

Tento dokument je určen zejména tvůrcům rámců kybernetické bezpečnosti.

1 Předmět normy

Tento dokument specifikuje pokyny pro vývoj rámce kybernetické bezpečnosti. Je použitelný pro tvůrce rámců kybernetické bezpečnosti bez ohledu na typ, velikost nebo povahu jejich organizací.