

2022

Správa a řízení bezpečnosti informací –
Směrnice pro pojištění kybernetických rizik

ČSN
ISO/IEC 27102

36 9720

Information security management – Guidelines for cyber-insurance

Tato norma je českou verzí mezinárodní normy ISO/IEC 27102:2019. 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 27102:2019. 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

Souvisící ČSN

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

ČSN EN ISO/IEC 27002 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací

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 technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v člancích

„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.

ICS 35.030

Obsah

Strana

Předmluva.....	5
Úvod.....	6
1 Předmět normy.....	7
2 Citované dokumenty.....	7
3 Termíny a definice.....	7
4 Struktura tohoto dokumentu.....	8
5 Přehled pojištění kybernetických rizik a smlouvy o pojištění kybernetických rizik.....	8
5.1 Pojištění kybernetických rizik.....	8
5.2 Smlouva o pojištění kybernetických rizik.....	8
6 Kybernetická rizika a pojistné krytí.....	9
6.1 Proces řízení rizik a pojištění kybernetických rizik.....	9
6.2 Kybernetické	

incidenty.....	9
6.2.1... Obecně.....	9
6.2.2... Typy kybernetických incidentů.....	9
6.3..... Dopad na podnikání a pojistitelné ztráty.....	10
6.3.1... Obecně.....	10
6.3.2... Typ pojistného krytí.....	10
6.3.3... Odpovědnost.....	10
6.3.4... Náklady na odezvu na incident.....	10
6.3.5... Náklady na kybernetické vydírání.....	12
6.3.6... Přerušení podnikání.....	12
6.3.7... Zákonné a regulační pokuty a sankce.....	12
6.3.8... Smluvní pokuty.....	12
6.3.9... Poškození systémů.....	12
6.4..... Riziko dodavatele.....	12
6.5..... Tiché nebo nepotvrzující krytí v jiných pojistných	

smlouvách.....	13
6.6 Dodavatelé a právní zástupci pro odezvu na incidenty.....	13
6.7 Výluky z pojištění kybernetických rizik.....	13
6.8 Limity pojistného krytí.....	13
7 Posouzení rizik podporující uzavírání pojištění kybernetických rizik.....	14
7.1 Přehled.....	14
7.2 Shromažďování informací.....	14
7.3 Posouzení kybernetických rizik pojištěného.....	14

7.3.1... Obecně.....	14
7.3.2... Vlastní posouzení kybernetických rizik.....	14
7.3.3... Posouzení opatření bezpečnosti informací.....	15
7.3.4... Přezkoumání předchozích kybernetických ztrát.....	15
8..... Úloha ISMS při podpoře pojištění kybernetických rizik.....	15
8.1..... Přehled.....	15
8.2..... ISMS jako zdroj informací.....	16
8.2.1... ISMS.....	16
8.2.2... Plánování.....	16
8.2.3... Podpora.....	17
8.2.4... Provoz.....	17
8.2.5... Hodnocení výkonnosti.....	17
8.2.6... Zdokonalování.....	18
8.3..... Sdílení informací o rizicích a opatřeních.....	18

8.4..... Plnění závazků z pojištění kybernetických rizik.....	18
--	----

Příloha A (informativní) Příklady ISMS dokumentů pro sdílení.....	19
--	----

Bibliografie.....	20
-------------------	----

 **DOKUMENT CHRÁNĚNÝ COPYRIGHTEM**

© ISO/IEC 2019

Veškerá práva vyhrazena. Žádná část této publikace nesmí být, není-li specifikováno jinak nebo nepožaduje-li se to v souvislosti s její implementací, reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým ani mechanickým, včetně pořizování fotokopii nebo zveřejňování na internetu nebo intranetu, bez předchozího písemného souhlasu. O souhlas lze požádat buď ISO na níže uvedené adrese, nebo členskou organizaci ISO v zemi žadatele.

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 směrnících 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 směrnících 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 obdržných ISO (viz www.iso.org/patents) nebo v seznamu patentových prohlášení obdržných IEC (viz <http://patents.iec.ch>).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamena 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

Kybernetické incidenty mohou nastat kdykoli a mají různé potenciální dopady na organizaci. Například informace a aktiva organizace jsou neustále pod útokem, protože kybernetické hrozby se stávají všudypřítomnějšími, vytrvalejšími a sofistikovanějšími.

Přijetí pojištění kybernetických rizik ke snížení dopadů následků kybernetického incidentu by organizace měla zvážit jako doplněk opatření bezpečnosti informací v rámci účinného přístupu k ošetření rizik.

Pojištění kybernetických rizik nenahrazuje robustní bezpečnost a efektivní plány odezvy na incidenty spolu s důkladným školením všech zaměstnanců.

Pojištění kybernetických rizik by mělo být považováno za důležitou součást celkového plánu organizace na ošetření rizik bezpečnosti s cílem zvýšit odolnost.

1 Předmět normy

Tento dokument poskytuje směrnice při zvažování pořízení pojištění kybernetických rizik jako možnosti ošetření rizik ke zvládnutí dopadu kybernetického incidentu v rámci řízení rizik bezpečnosti informací organizace.

Tento dokument poskytuje směrnice pro:

- a) zvažování pořízení pojištění kybernetických rizik jako možnosti ošetření rizika formou sdílení kybernetických rizik;
- b) využití pojištění kybernetických rizik jako pomoci při zvládnutí dopadů kybernetického incidentu;
- c) sdílení údajů a informací mezi pojištěným a pojistitelem za účelem podpory pojišťovacích, monitorovacích a likvidačních činností souvisejících s pojistnou smlouvou o pojištění kybernetických rizik;
- d) využití systému řízení bezpečnosti informací při sdílení příslušných údajů a informací s pojistitelem.

Tento dokument je použitelný pro organizace všech typů, velikostí a povah pro usnadnění plánování a pořízení pojištění kybernetických rizik organizací.

Konec náhledu - text dále pokračuje v placené verzi ČSN.