ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Říjen 2013**

Informační technologie – Bezpečnostní techniky – Směrnice pro kybernetickou bezpečnost

ČSN ISO/IEC 27032
36 9790

Information technology – Security techniques – Guidelines for cybersecurity

Technologies de l,information – Techniques de sécurité – Lignes directrices pour la cybersécurité

Tato norma je českou verzí mezinárodní normy ISO/IEC 27032:2012. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 27032:2012. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 27000 zavedena v ČSN ISO/IEC 27000 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

Souvisící ČSN

ČSN EN ISO 9001:2009 (01 0321) Systémy managementu jakosti – Požadavky

ČSN ISO/IEC 15408-1 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT - Část 1: Úvod a všeobecný model

ČSN ISO/IEC 19770-1 (36 9043) Informační technologie – Správa softwarových aktiv – Část 1: Procesy

ČSN ISO/IEC 20000-1 (36 9074) Informační technologie – Management služeb – Část 1: Požadavky na systém managementu služeb

ČSN ISO/IEC 27001 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky

ČSN ISO/IEC 17799 (36 9790) Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací

ČSN ISO/IEC 27005 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení rizik

bezpečnosti informací

ČSN ISO 31000 (01 0351) Management rizik – Principy a směrnice

TNI 01 0350 Management rizik – Slovník (Pokyn 73)

Upozornění na národní poznámky

Do normy byly k článkům 13.5.2 a A.2.1 doplněny národní poznámky.

Vypracování normy

Zpracovatel: Risk Analysis Consultants, s. r. o., IČ 63672774

Technická normalizační komise: TNK 20 Informační technologie

Zaměstnanec Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Miroslav Škop

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail copyright@iso.org

Web www.iso.org

Published in Switzerland

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 27032
Směrnice pro kybernetickou bezpečnost První vydání 2012-07

ICS 35.040

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 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 a nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

Hlavním úkolem společné technické komise je vypracování mezinárodních norem. Návrhy mezinárodních norem přijaté společnou technickou komisí jsou rozesílány národním členům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikování jakéhokoliv nebo všech patentových práv.

Mezinárodní norma ISO/IEC 27032 byla připravena společnou technickou komisí ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *IT Bezpečnostní techniky*.

Úvod

Kybernetický prostor je komplexní prostředí vyplývající ze vzájemné komunikace lidí, softwaru a služeb na Internetu podporované celosvětově fyzicky propojenými informačními a komunikačními technologiemi, ICT zařízeními a sítěmi. Existují však bezpečnostní problémy, které osvědčené postupy současné bezpečnosti informací, bezpečnosti Internetu, bezpečnosti sítí a bezpečnosti informačních a komunikačních technologií nepokrývají, protože jsou mezi těmito doménami mezery i nedostatek komunikace mezi organizacemi a poskytovateli v kybernetickém prostoru. Je to proto, že zařízení a připojené sítě, jež podporují kybernetický prostor, mají mnoho vlastníků, každého se svými vlastními obchodními, provozními a regulačními zájmy. Rozdílný způsob v nahlížení na jednotlivé oblasti bezpečnosti mezi organizacemi a poskytovateli, a žádné nebo jen omezené sdílení informací mezi jednotlivými organizacemi a poskytovateli, má za následek nejednotný přístup k bezpečnosti v kybernetickém prostoru.

První oblast této mezinárodní normy se zabývá bezpečností kybernetického prostoru nebo problematikou kybernetické bezpečnosti, která spočívá v překlenutí mezer mezi různými bezpečnostními doménami v kybernetickém prostoru. Tato mezinárodní norma poskytuje zejména technická doporučení pro řešení obecných rizik kybernetické bezpečnosti, včetně:

- útoků prostřednictvím sociálního inženýrství;
- hackingu;
- šíření škodlivého softwaru (“malwaru”);
- spywaru; a
- jiného potenciálně nechtěného softwaru.

Technická doporučení nabízí bezpečnostní opatření pro řešení těchto rizik, včetně opatření pro:

- přípravu na útoky, například škodlivým softwarem, jednotlivými zločinci nebo zločineckými organizacemi na internetu;
- detekování a monitorování útoků; a

- reakce na útoky.

Druhá oblast této mezinárodní normy je zaměřena na spolupráci, protože mezi zainteresovanými stranami existuje potřeba účinného sdílení informací, koordinace a zvládání incidentů v kybernetickém prostoru. Tato spolupráce musí probíhat bezpečným a spolehlivým způsobem, který rovněž chrání soukromí jednotlivců, jichž se to týká. Mnoho z těchto zainteresovaných stran může sídlit v různých geografických lokalitách a časových pásmech a jsou pravděpodobně řízeny různými regulačními požadavky. Zainteresované strany zahrnují:

- uživatele, kterými mohou být různé typy organizací nebo jednotlivců; a
- poskytovatele, kteří zahrnují poskytovatele služeb.

Tato mezinárodní norma také poskytuje rámec pro

- sdílení informací;
- koordinaci; a
- zvládání incidentů.

Tento rámec obsahuje

- klíčová hlediska pro ustanovení důvěryhodnosti;
- nutné procesy pro spolupráci, výměnu a sdílení informací; jakož i
- technické požadavky na integraci systémů a interoperabilitu mezi různými zainteresovanými stranami.

Vzhledem k rozsahu této mezinárodní normy jsou poskytnutá opatření na obecné úrovni. Pro další doporučení jsou v rámci této mezinárodní normy uvedeny podrobné normy technické specifikace a směrnice aplikovatelné pro každou oblast.

1 Předmět normy

Tato mezinárodní norma poskytuje doporučení pro zlepšení stavu kybernetické bezpečnosti. Nastiňuje specifické aspekty dané činnosti a jejich závislosti na jiných oblastech bezpečnosti, zejména:

- bezpečnosti informací;
- bezpečnosti sítě;
- bezpečnosti internetu; a
- ochraně kritické informační infrastruktury (CIIP).

Pokrývá základní bezpečnostní postupy pro zainteresované strany v kybernetickém prostoru. Tato mezinárodní norma poskytuje:

- přehled o kybernetické bezpečnosti;
- vysvětlení vztahu mezi kybernetickou bezpečností a jinými typy bezpečnosti;
- definici zainteresovaných stran a popis jejich rolí v kybernetické bezpečnosti;
- doporučení pro řešení běžných problémů kybernetické bezpečnosti; a
- strukturu, která umožňuje zainteresovaným stranám spolupracovat na vyřešení problémů kybernetické bezpečnosti.