ČESKÁ TECHNICKÁ NORMA

ICS 03.100.70; 35.030 **Červen 2017**

Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002	ČSN ISO/IEC 27017 36 9710

Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Technologies de l,information – Techniques de sécurité – Code de pratique pour les contrôles de sécurité de l,information fondés sur l,ISO/IEC 27002 pour les services du nuage

Tato norma je českou verzí mezinárodní normy ISO/IEC 27017:2015. 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 27017:2015. 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

Recommendation ITU-T Y.3500 | ISO/IEC 17788 zavedena v ČSN ISO/IEC 17788 (36 9865) Informační technologie – Cloud computing – Přehled a slovník

Recommendation ITU-T Y.3502 | ISO/IEC 17789 zavedena v ČSN ISO/IEC 17789 (36 9866) Informační technologie – Cloud computing – Referenční architektura

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

ISO/IEC 27002:2013 zavedena v ČSN ISO/IEC 27002:2014 (36 9798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací

Souvisící ČSN

ČSN ISO/IEC 27001:2014 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

ČSN ISO/IEC 27005:2013 (36 9790) Informační technologie – Bezpečnostní techniky – Řízení rizik

bezpečnosti informací

ČSN ISO/IEC 27018:2017 (36 9709) Informační technologie – Bezpečnostní techniky – Soubor postupů na ochranu osobně identifikovatelných informací (PII) ve veřejných cloudech vystupujících jako zpracovatelé PII

ČSN EN ISO/IEC 27040:2017 (36 9849) Informační technologie – Bezpečnostní techniky – Zabezpečení úložišť dat

ČSN EN ISO 19440:2008 (97 4105) Podniková integrace – Jazykové konstrukty pro podnikové modelování

ČSN ISO 31000:2010 (01 0351) Management rizik – Principy a směrnice

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:

cloud, cloud computing, malware, snapshot, peer

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČ 40654419

Technická normalizační komise: TNK 20 Informační technologie

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

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002

ISO/IEC 27017
První vydání
2015-12-15

ICS 03.100.70; 35.030

Obsah

Strana

DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2015, Published in Switzerland
Veškerá práva vyhrazena. Není-li specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým ani mechanickým, včetně pořizování fotokopií nebo zveřejnění na internetu nebo intranetu, bez předchozího písemného svolení. O písemné svolení lze požádat buď přímo ISO na níže uvedené adrese, nebo členskou organizaci ISO
v zemi žadatele.
ISO copyright office
CH. de Blandonnet 8 · CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
copyright@iso.org
www.iso.org

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 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 technickými komisemi se rozesílají národním orgánům 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 identifikaci jakéhokoliv nebo všech patentových práv.

ISO/IEC 27017 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie,* subkomise SC 27 *IT Bezpečnostní techniky* ve spolupráci s ITU-T. Identický text je publikován jako doporučení ITU-T.X.1631 (07/2015).

Úvod

Pokyny obsažené v tomto doporučení | mezinárodní normě jsou pokyny navíc k pokynům uvedeným v ISO/IEC 27002 a tyto pokyny doplňují.

Konkrétně toto doporučení | mezinárodní norma poskytuje pokyny podporující implementaci kontrolních opatření bezpečnosti informací pro zákazníky cloudových služeb a poskytovatele cloudových služeb. Některé pokyny jsou určeny zákazníkům cloudových služeb, kteří implementují kontrolní opatření, a jiné jsou určeny poskytovatelům cloudových služeb na podporu implementace těchto kontrolních opatření. Výběr vhodných kontrolních opatření bezpečnosti informací a uplatnění poskytnutých pokynů k implementaci bude záviset na posouzení rizik a případných právních, smluvních, regulatorních nebo jiných požadavcích bezpečnosti informací specifických pro sektor cloudových služeb.

1 Předmět normy

Toto doporučení | mezinárodní norma uvádí pokyny pro kontrolní opatření bezpečnosti informací použitelné na poskytování a používání cloudových služeb poskytnutím:

– dodatečných pokynů k implementaci příslušných kontrolních opatření specifikovaných v ISO/IEC 27002;

– dodatečných kontrolních opatření s pokyny k implementaci, které se specificky vztahují ke cloudovým službám.

Toto doporučení | mezinárodní norma poskytuje kontrolní opatření a pokyny k implementaci jak pro poskytovatele cloudových služeb, tak pro zákazníky cloudových služeb.

Konec náhledu - text dále pokračuje v placené verzi ČSN.