

# ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Březen 2015**

**Informační technologie - Bezpečnostní techniky -  
Bezpečnost sítě -  
Část 3: Referenční síťové scénáře - Hrozby, techniky návrhu  
a otázky řízení**

**ČSN**  
**ISO/IEC 27033-3**  
36 9701

Information Technology - Security techniques - Network security -  
Part 3: Reference networking scenarios - Threats, design techniques and control issues

Technologies de l'information - Techniques de sécurité - Sécurité de réseau -  
Partie 3: Scénarios de réseautage de référence - Menaces, techniques conceptuelles et questions de  
contrôle

Tato norma je českou verzí mezinárodní normy ISO/IEC 27033-3:2010. 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 27033-3:2010. 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

ISO/IEC 27033-1 dosud nezavedena

Vysvětlivky k textu převzaté normy

Pro účely této normy byly použity následující anglické termíny v původním tvaru, vzhledem k rozšíření těchto termínů v odborné komunitě a/nebo absenci českého ekvivalentu:

backend, botnet, broadcast, chat, cross-site scripting, exploit, instant messaging, man-in-the-middle, malware, multicast, on-board, peer-to-peer, phishing, ping sweep, point-and-shoot, rootkit, spyware, SQL injection, stream, webhosting

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČ 40654419

Technická normalizační komise: TNK 20 Informační technologie

## MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 27033-3

Bezpečnost sítě – První vydání

Část 3: Referenční síťové scénáře – Hrozby, 2010-12-15

techniky návrhu a otázky řízení

ICS 35.040

## Obsah

Strana

Předmluva 6

**1** Předmět normy 7

**2** Citované dokumenty 7

**3** Termíny a definice 7

**4** Zkrácené termíny 8

**5** Struktura normy 8

**6** Přehled 9

**7** Služby přístupu k Internetu pro zaměstnance 11

**7.1** Základní informace 11

**7.2** Bezpečnostní hrozby 11

**7.3** Techniky a opatření návrhu bezpečnosti 12

**8** Služby typu společnost – společnost 14

**8.1** Základní informace 14

**8.2** Bezpečnostní hrozby 14

**8.3** Techniky a opatření návrhu bezpečnosti 14

**9** Služby typu společnost – zákazník 15

**9.1** Základní informace 15

**9.2** Bezpečnostní hrozby 15

**9.3** Techniky a opatření návrhu bezpečnosti 16

<b>10</b>	<b>Rozšířené služby založené na spolupráci</b>	<b>17</b>
<b>10.1</b>	<b>Základní informace</b>	<b>17</b>
<b>10.2</b>	<b>Bezpečnostní hrozby</b>	<b>17</b>
<b>10.3</b>	<b>Techniky a opatření návrhu bezpečnosti</b>	<b>18</b>
<b>11</b>	<b>Segmentace sítě</b>	<b>18</b>
<b>11.1</b>	<b>Základní informace</b>	<b>18</b>
<b>11.2</b>	<b>Bezpečnostní hrozby</b>	<b>19</b>
<b>11.3</b>	<b>Techniky a opatření návrhu bezpečnosti</b>	<b>19</b>
<b>12</b>	<b>Síťová podpora pro domácí kanceláře a malé firmy</b>	<b>19</b>
<b>12.1</b>	<b>Základní informace</b>	<b>19</b>
<b>12.2</b>	<b>Bezpečnostní hrozby</b>	<b>20</b>
<b>12.3</b>	<b>Techniky a opatření návrhu bezpečnosti</b>	<b>20</b>
<b>13</b>	<b>Mobilní komunikace</b>	<b>21</b>
<b>13.1</b>	<b>Základní informace</b>	<b>21</b>
<b>13.2</b>	<b>Bezpečnostní hrozby</b>	<b>21</b>
<b>13.3</b>	<b>Techniky a opatření návrhu bezpečnosti</b>	<b>22</b>
<b>14</b>	<b>Síťová podpora pro cestující uživatele</b>	<b>23</b>
<b>14.1</b>	<b>Základní informace</b>	<b>23</b>
<b>14.2</b>	<b>Bezpečnostní hrozby</b>	<b>23</b>
<b>14.3</b>	<b>Techniky a opatření návrhu bezpečnosti</b>	<b>23</b>
<b>15</b>	<b>Služby zajišťované subdodavatelsky</b>	<b>24</b>
<b>15.1</b>	<b>Základní informace</b>	<b>24</b>
<b>15.2</b>	<b>Bezpečnostní hrozby</b>	<b>24</b>
<b>15.3</b>	<b>Techniky a opatření návrhu bezpečnosti</b>	<b>25</b>
<b>Příloha A</b>	<b>(informativní) Příklad politiky pro používání Internetu</b>	<b>26</b>
<b>Příloha B</b>	<b>(informativní) Katalog hrozeb</b>	<b>30</b>

#### Odmítnutí odpovědnosti za manipulaci s PDF souborem

Tento soubor PDF může obsahovat vložené typy písma. V souladu s licenční politikou Adobe lze tento soubor tisknout nebo prohlížet, ale nesmí být editován, pokud nejsou typy písma, které jsou vloženy, používány na základě licence a instalovány v počítači, na němž se editace provádí. Při stažení tohoto souboru přejímají jeho uživatelé odpovědnost za to, že nebude porušena licenční politika Adobe. Ústřední sekretariát ISO nepřijímá za její porušení žádnou odpovědnost.

Adobe je obchodní značka „Adobe Systems Incorporated“.

Podrobnosti o softwarových produktech použitých k vytvoření tohoto souboru PDF lze najít ve Všeobecných informacích, které se vztahují k souboru; parametry, na jejichž základě byl PDF soubor vytvořen, byly optimalizovány pro tisk. Soubor byl zpracován s maximální péčí tak, aby ho členské organizace ISO mohly používat. V málo pravděpodobném případě, že vznikne problém, který se týká souboru, informujte o tom Ústřední sekretariát ISO na níže uvedené adrese.



### DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2010

Veškerá práva vyhrazena. Není-li specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně pořizování fotokopíí 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

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail [copyright@iso.org](mailto:copyright@iso.org)

Web [www.iso.org](http://www.iso.org)

Published in Switzerland

#### Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených dotyčnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i další mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázaly pracovní styk. ISO a IEC ustavily v oblasti informačních technologií společnou technickou komisi, ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnici 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.

ISO/IEC 27033-3 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *Bezpečnostní techniky IT*.

ISO/IEC 27033 se skládá z následujících částí se společným názvem *Informační technologie – Bezpečnostní techniky – Bezpečnost sítě*:

- Část 1: *Přehled a pojetí*
- Část 2: *Směrnice pro návrh a implementaci bezpečnosti sítě*

- *Část 3: Referenční síťové scénáře – Hrozby, techniky návrhu a otázky řízení*

Následující části se připravují:

- *Část 4: Zabezpečení komunikací mezi sítěmi s využitím bezpečnostních bran – Hrozby, techniky návrhu a otázky řízení*
- *Část 5: Zabezpečení virtuálních privátních sítí – Hrozby, techniky návrhu a otázky řízení*

V budoucnu mohou následovat další části zahrnující témata, jako jsou například lokální sítě, sítě WAN, bezdrátové a rádiové sítě, širokopásmové sítě, hlasové sítě, konvergence IP protokolu (data, hlas, video), architektury webhostingu, architektury Internetového e-mailu (včetně odchozího on-line přístupu k Internetu a příchozího přístupu z Internetu), a směrovaný přístup k třetím stranám.

## 1 Předmět normy

Tato část ISO/IEC 27033 popisuje hrozby, techniky návrhu a otázky řízení spojené s referenčními síťovými scénáři. Pro každý scénář poskytuje podrobné pokyny ohledně bezpečnostních hrozeb a technik návrhu bezpečnosti a opatření potřebných ke zmírnění souvisejících rizik. Pokud je to relevantní, obsahuje odkazy na ISO/IEC 27033-4 až ISO/IEC 27033-6, aby se zabránilo duplikování obsahu těchto dokumentů.

Informace uvedené v této části ISO/IEC 27033 jsou určeny pro použití při přezkoumání možností technické architektury/návrhu bezpečnosti a při výběru a dokumentování preferované technické architektury/návrhu bezpečnosti a souvisejících opatření bezpečnosti, v souladu s normou ISO/IEC 27033-2. Vybrané konkrétní informace (spolu s informacemi vybranými z ISO/IEC 27033-4 až ISO/IEC 27033-6) budou záviset na charakteristikách přezkoumávaného síťového prostředí, tj. na konkrétním síťovém scénáři (scénářích) a příslušných „technologických“ tématech.

Celkově tato část ISO/IEC 27033 podstatně pomůže komplexní definici a implementaci bezpečnosti pro síťové prostředí jakékoli organizace.

Konec náhledu - text dále pokračuje v placené verzi ČSN.