ICS 35.040 SLOVENSKÁ TECHNICKÁ NORMA Júl 2021

STN	**Informačné technológie Bezpečnostné metódy Sieťová bezpečnosť Časť 3: Referenčné sieťové scenáre Hrozby, techniky návrhu a problémy v opatreniach**	**STN ISO/IEC 27033-3 97 4103**

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

Informationstechnologie
Sicherheitstechniken
Netzwerksicherheit
Teil 3: Referenznetzwerkszenarien
Bedrohungen, Designtechniken und Sicherheitsmassnahmenprobleme

Táto norma obsahuje anglickú verziu ISO/IEC 27033-3: 2010.

This standard includes the English version of ISO/IEC 27033-3: 2010.

132973

Anotácia

Táto časť ISO/IEC 27033 popisuje hrozby, techniky návrhu a problémy s riadením spojené s referenč-nými sieťovými scenármi.

Pre každý scenár poskytuje podrobné usmernenia k bezpečnostným hrozbám a technikám a opatreniam návrhu bezpečnosti potrebným na zmiernenie súvisiacich rizík.

Prípadne obsahuje odkazy na ISO/IEC 27033-4 na ISO/IEC 27033-6, aby sa zabránilo duplikovaniu obsahu týchto dokumentov.

Informácie v tejto časti ISO/IEC 27033 sa používajú pri preskúmaní možností architektúry/dizajnu technického zabezpečenia a pri výbere a dokumentácii preferovanej architektúry/dizajnu technického zabezpečenia a súvisiacich bezpečnostných opatrení v súlade s normou ISO/IEC 27033-2.

Celkovo táto časť ISO/IEC 27033 významne pomáha pri komplexnom vymedzení a implementácii zabezpečenia pre sieťové prostredie akejkoľvek organizácie.

Národný predhovor

Normatívne referenčné dokumenty

Nasledujúce dokumenty, celé alebo ich časti, sú v tomto dokumente normatívnymi odkazmi a sú nevyhnutné pri jeho používaní. Pri datovaných odkazoch sa použije len citované vydanie. Pri nedatovaných odkazoch sa použije najnovšie vydanie citovaného dokumentu (vrátane všetkých zmien).

POZNÁMKA 1. – Ak bola medzinárodná publikácia zmenená spoločnými modifikáciami, čo je indikované označením (mod), použije sa príslušná EN/HD.

POZNÁMKA 2. – Aktuálne informácie o platných a zrušených STN možno získať na webovej stránke www.unms.sk.

ISO/IEC 27000 zavedená v STN EN ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník (ISO/IEC 27000) (36 9789)

ISO/IEC 27033-1 dosiaľ nezavedená

Vypracovanie normy

Spracovateľ: Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, Bratislava

Technická komisia: TK 37 Informačné technológie

Contents

Page

Foreword iv

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated terms 2

5 Structure 3

6 Overview 4

7 Internet access services for employees 6
7.1 Background 6
7.2 Security threats 7
7.3 Security design techniques and controls 7

8 Business to business services 9
8.1 Background 9
8.2 Security threats 9
8.3 Security design techniques and controls 10

9 Business to customer services 11
9.1 Background 11
9.2 Security threats 11
9.3 Security design techniques and controls 12

10 Enhanced collaboration services 13
10.1 Background 13
10.2 Security threats 14
10.3 Security design techniques and controls 14

11 Network segmentation 15
11.1 Background 15
11.2 Security threats 15
11.3 Security design techniques and controls 15

12 Networking support for home and small business offices 16
12.1 Background 16
12.2 Security threats 16
12.3 Security design techniques and controls 17

13 Mobile communication 18
13.1 Background 18
13.2 Security threats 18
13.3 Security design techniques and controls 19

14 Networking support for travelling users 20
14.1 Background 20
14.2 Security threats 20
14.3 Security design techniques and controls 20

15 Outsourced services 21
15.1 Background 21
15.2 Security threats 21
15.3 Security design techniques and controls 22

Annex A (informative) **An Example Internet Use Policy** 23

Annex B (informative) **Catalogue of Threats** 27

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27033-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 27033 consists of the following parts, under the general title *Information technology — Security techniques — Network security*:

— *Part 1: Overview and concepts*

— *Part 2: Guidelines for the design and implementation of network security*

— *Part 3: Reference network scenarios — Threats, design techniques and control issues*

The following parts are under preparation:

— *Part 4: Securing communications between networks using security gateways — Threats, design techniques and control issues*

— *Part 5: Securing virtual private networks — Threats, design techniques and control issues*

There may be future parts to cover topics such as local area networks, wide area networks, wireless and radio networks, broadband networks, voice networks, Internet Protocol (IP) convergence (data, voice, video) networks, web host architectures, Internet email architectures (including outgoing online access to the Internet, and incoming access from the Internet), and routed access to third party organizations.

INTERNATIONAL STANDARD **ISO/IEC 27033-3:2010(E)**

Information technology — Security techniques — Network security —

Part 3: Reference networking scenarios — Threats, design techniques and control issues

1 Scope

This part of ISO/IEC 27033 describes the threats, design techniques and control issues associated with reference network scenarios. For each scenario, it provides detailed guidance on the security threats and the security design techniques and controls required to mitigate the associated risks. Where relevant, it includes references to ISO/IEC 27033-4 to ISO/IEC 27033-6 to avoid duplicating the content of those documents.

The information in this part of ISO/IEC 27033 is for use when reviewing technical security architecture/design options and when selecting and documenting the preferred technical security architecture/design and related security controls, in accordance with ISO/IEC 27033-2. The particular information selected (together with information selected from ISO/IEC 27033-4 to ISO/IEC 27033-6) will depend on the characteristics of the network environment under review, i.e. the particular network scenario(s) and 'technology' topic(s) concerned.

Overall, this part of ISO/IEC 27033 will aid considerably the comprehensive definition and implementation of security for any organization's network environment.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*