ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 25068.3-2022

Replacing GB/T 25068.4-2010

Information technology - Security techniques - Network security - Part 3: Threats, design techniques and control for network access scenarios

Issued on: October 12, 2022 **Implemented on: May 1, 2023**

Issued by: State Administration for Market Regulation, China National Standardization Administration

Table of Contents

foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for Standardization Work Part 1.Structure and Drafting Rules for Standardization Documents" drafting.

This document is part 3 of GB/T 25068 "Information Technology Security Technology Network Security". GB/T 25068 has issued the following part.

--- Part 1.Overview and concepts;

--- Part 2.Network Security Design and Implementation Guidelines;

--- Part 3.Threats, design techniques and controls for network access scenarios;

--- Part 4.Inter-network communication security protection using security gateways;

--- Part 5.Cross-network communication security protection using a virtual private network.

This document replaces GB/T 25068.4-2010 "Information Technology Security Technology IT Network Security Part 4.Remote Access Security Full Protection". Compared with GB/T 25068.4-2010, except for structural adjustment and editorial changes, the main technical changes are as follows.

---The main content of this document is changed from the security protection of remote access to the threat, design technology and control for network access scenarios;

---This document resummarizes and revises each technical application scenario in the original series of standards;

--- Deleted terms and definitions such as "access point", "Advanced Encryption Standard" and "callback", and added "malware", "opaqueness" and "outsourcing"

and other terms and definitions (see Chapter 3, Chapter 3 of the.2010 edition);

---Added "Employee Internet Access Services", "Business-to-Business Services", "Business-to-Customer Services", "Enhanced Collaboration Services"

"Network segmentation" and "providing network support for home offices and small business offices", etc., deleted the "remote access connection class

"Type", "Remote Access Connection Technology", "Selection and Configuration Guide" and other content (see Chapter 7~15, Chapter 6 of the.2010 edition

Chapter~Chapter 8);

--- Added "Threat Catalog" and "Internet Usage Policy Example", deleted "Remote Access Security Policy Example" and "RADIUS Implementation

and Deployment Best Practices" "Two Modes of FTP" "Secure Mail Services Checklist" "Secure Web Services Checklist" "Wireless

LAN Security Checklist" (see Appendix A, Appendix B, Appendix A~Appendix F of the.2010 edition).

This document is modified to adopt ISO /IEC 27033-3.2010 "Information Security Security Technology Network Security Part 3.Reference Network

Scenarios - Threats, Design Techniques, and Controls.

Compared with ISO /IEC 27033-3.2010, this document has made the following structural adjustments.

--- Adjust Appendix A to Appendix B, and Appendix B to Appendix A.

The technical differences between this document and ISO /IEC 27033-3.2010 and their reasons are as follows.

--- Replace ISO /IEC 27000 with normatively quoted GB/T 29246 (see Chapter 3 and Chapter 6), and replace with GB/T 25068.1

ISO /IEC 27033-1 (see Chapter 3), to adapt to the technical conditions of our country;

---Change the network segmentation guidance for government organizations such as federal countries or the European Union to the network segmentation guidance for multinational organizations in my country

guide, and appear in the form of "notes" (see 11.1).

The following editorial changes have been made to this document.

---Change some expressions applicable to international standards to expressions applicable to Chinese standards;

--- Added footnotes in Table 1;

---Expand the use requirements for blogs in Appendix A of the international standard to use requirements for all social platforms;

--- Adjust the suspension section in A.4.3 in Appendix A of the international standard to B.4.3.1 with serial numbers in Appendix B;

--- Deleted the definition A.6 in Appendix A of the international standard;

--- Added "References".

Please note that some contents of this document may refer to patents. The issuing agency of this document assumes no responsibility for identifying patents.

Introduction

The purpose of GB/T 25068 is to provide detailed guidance on security aspects for the management, operation, use and interconnection of information system networks.

This guide is intended to facilitate the adoption of this document by those responsible for information security, especially network security, within an organization to meet their specific needs. to be composed of six parts

constitute.

--- Part 1.Overview and concepts. The purpose is to present concepts related to cybersecurity and provide management guidance.

--- Part 2.Network Security Design and Implementation Guidelines. The purpose is to provide information on how organizations plan, design, and achieve high-quality network security

System to ensure that network security is suitable for the corresponding business environment to provide guidance.

--- Part 3.Threats, design techniques and controls for network access scenarios. The purpose is to enumerate the

The specific risks, design techniques, and controls associated with this document apply to all those involved in the planning, design, and implementation of cybersecurity architectural aspects.

--- Part 4.Inter-network communication security protection using a security gateway. The purpose is to ensure the security of inter-network communication using the security gateway.

--- Part 5.Cross-network communication security protection using a virtual private network. The purpose is to define the use of virtual private networks to establish secure connections

associated specific risks, design techniques and control elements.

--- Part 6.Wireless network access security. Intended to be necessary for the selection, implementation and monitoring of the use of wireless networks to provide secure communications

provides guidance on technical controls and is used in part 2 for review of technical security architecture or design options involving the use of wireless networks

Check and choose.

GB/T 25068 is based on GB/T 22081 "Information Technology Security Technical Information Security Control Practice Guidelines", further

Provides detailed implementation guidance for network security controls. GB/T 25068 only emphasizes the importance of business types and other factors affecting network security

without specifying.

Where this document involves the use of cryptography to solve the requirements of confidentiality, integrity, authenticity, and non-repudiation, it shall follow the relevant national standards for cryptography.

and industry standards.

information technology security technology cybersecurity

Part 3.Oriented to network access scenarios

Threats, Design Techniques and Controls

1 Scope

This document describes the threats, design techniques, and control issues associated with network access scenarios, providing capabilities for each network access scenario.

Detailed guidance on the three elements of security threats, security design techniques, and controls that can reduce associated risks.

This document is applicable to review the structure and design of the technical safety system in accordance with GB/T 25068.2, and to select and record the preferred technology

options for technical security architecture, design, and associated controls. The characteristics of the network environment being reviewed determine the selection of specific information (including from