ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 30282-2023

Information security technology - Technical specification for anti-spam products

信息安全技术 反垃圾邮件产品技术规范

Issued on: May 23, 2023 **Implemented on: December 1, 2023**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

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 replaces GB/T 30282-2013 "Information Security Technology Anti-spam Product Technical Requirements and Test Evaluation Methods", and Compared with GB/T 30282-2013, except for structural adjustment and editorial changes, the main technical changes are as follows:

--- Changed the "Terms and Definitions" chapter (see Chapter 3, Chapter 3 of the:2013 edition);

--- Increased the "Product Overview" chapter (see Chapter 5);

---Changed "Spam identification based on email sender address" (see 6:1:1:1, 5:1:1:1 of the:2013 edition);

--- Changed "Spam Identification Based on Email Content Characteristics" (see 6:1:1:2, 5:1:1:2 of the:2013 edition);

---Changed "Spam identification based on mail connection characteristics" (see 6:1:1:3, 5:1:1:3 of the:2013 edition);

--- Changed "spam processing" (see 6:1:2, 5:1:2 of the:2013 version);

--- Changed the "deployment method" (see 6:1:4:2, 5:1:3:2 of the:2013 edition);

--- Changed the "product upgrade" (see 6:1:4:3, 5:1:3:3 of the:2013 edition);

--- Added "audit data protection" (see 6:2:1:4);

--- Changed the "identity authentication" requirements (see 6:2:2, 5:2:2 of the:2013 edition);

--- Added "Access Control" requirements (see 6:2:3);

--- Added "safety management" requirements (see 6:2:4);

---Changed the "data security" requirements (see 6:2:5, 5:2:4 of the:2013 edition);

1 Scope

GB/T 30282-2023 specifies what an anti-spam product must do. Spam filtering is judged on two error rates that pull against each other, and only one of them is visible to the user: spam that gets through is annoying, while legitimate mail silently discarded is a business problem that nobody notices until a contract, an invoice or an alert has been missed. A product tuned to look good on the first number can be quietly failing on the second. The threat has also moved on from bulk advertising to targeted phishing and business email compromise, where a single message that gets through is the whole attack, and to the authentication mechanisms - SPF, DKIM and the policies built on them - that a product now has to evaluate correctly. This document specifies the technical requirements for anti-spam products and describes the corresponding testing and evaluation methods. It applies to the development, testing and evaluation of such products. Under ICS 35.030 and CCS L80, it is written for security product vendors, for the laboratories certifying them under China's security product regime, and for the enterprises and mail operators selecting one.

This document specifies the technical requirements for anti-spam products, and describes the corresponding test and evaluation methods: This document is applicable to the development, testing and evaluation of anti-spam products, as well as to guide the use and management of products:

2 Normative references

The contents of the following documents constitute the essential provisions of this document through normative references in the text: Among them, dated references For documents, only the version corresponding to the date is applicable to this document; for undated reference documents, the latest version (including all amendments) is applicable to this document:

GB/T 18336:1-2015 Information technology security technology Information technology security assessment criteria Part 1: Introduction and general Model

GB/T 25069 Information Security Technical Terms

3 Terms and Definitions

The following terms and definitions defined in GB/T 18336:1-2015 and GB/T 25069 apply to this document: 3:1 spam Emails that the user has not previously requested or consented to receive:

Note: Spam generally has the following characteristics:

--- Contains advertisements, promotional materials, etc: that users are unwilling to accept;

---Send to a large number of users at the same time;

--- Contains false information sources, senders, routing and other information;

--- Contains malicious code: 3:2 mail blacklist mailblacklist List of email addresses identified as spam: 3:3 mail whitelist mailwhitelist A list of email addresses that will not be identified as spam: 3:4 delivery send Anti-spam products do not identify and process emails, but send them directly to recipients: 3:5 label delivery labelandsend The process by which an antispam product marks a message as spam and sends it to the recipient: