ICS 35.040
L 80

中华人民共和国国家标准

GB/T 38561—2020

信息安全技术
网络安全管理支撑系统技术要求

Information security technology—
Technical requirements for cybersecurity management support system

2020-03-06 发布　　2020-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:浙江远望信息股份有限公司、公安部第一研究所、浙江省委办公厅信息化管理中心、浙江省公安厅科技通信管理局、浙江省高级人民法院信息中心、浙江省信息化推进服务中心、杭州市公安局科技信息化局、中电长城网际系统应用有限公司、北京江南天安科技有限公司。

本标准主要起草人:傅如毅、吴文、宣以广、殷云飞、毛林斌、栗红梅、周春燕、邵森龙、蒋行杰、马洪军、陈冠直、金江焕、周征宇、姚龙飞、蒋先浩、刘京玲、王雪玲。

信息安全技术
网络安全管理支撑系统技术要求

1 范围

本标准规定了网络安全管理支撑系统的技术要求，包括系统功能要求、自身安全性要求和安全保障要求。

本标准适用于网络安全管理工作的支撑系统的规划、设计、开发和测试。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/Z 20986—2007 信息安全技术 信息安全事件分类分级指南

3 术语和定义

GB/Z 20986—2007 界定的以及下列术语和定义适用于本文件。

3.1

网络安全管理支撑系统 cybersecurity management support system

基于组织的安全目标、对象、流程等，支撑组织开展网络安全管理工作的系统。

3.2

对象 object

网络安全管理中的实体。

注：主要包括硬件资产、软件资产、数据资产、组织人员等。

4 缩略语

下列缩略语适用于本文件。

CPU：中央处理器(Central Processing Unit)

DB：数据库(Data Base)

FTP：文件传输协议(File Transfer Protocol)

HTTP：超文本传输协议(HyperText Transfer Protocol)

IP：互联网协议(Internet Protocol)

MAC：媒体访问控制(Media Access Control 或 Medium Access Control)

SNMP：简单网络管理协议(Simple Network Management Protocol)

5 概述

网络安全管理支撑系统(以下简称支撑系统)是支撑组织开展网络安全管理工作的系统，实现对组

织的安全目标、对象、流程等进行信息化管理。本标准将支撑系统的技术要求分为系统功能要求、自身安全性要求和安全保障要求三类。

系统功能要求主要包括安全目标管理、应急预案管理、对象管理、信息安全事件监测、运行监测、流程处理、统计分析、考核管理、发布与展示、采集与处理、数据交换、备份与恢复等。

自身安全性要求主要包括身份鉴别、访问控制、权限管理、数据安全、安全审计等。

安全保障要求主要包括配置管理保障、开发、测试保障、交付与运维保障、指导性文档、脆弱性分析、生命周期支持等。

6 系统功能要求

6.1 安全目标管理

支撑系统具备组织安全目标管理功能，应满足以下要求：

a) 新增、删除、查询和修改安全目标；

b) 对安全目标进行分类管理；

c) 对安全目标进行发布与展示。

6.2 应急预案管理

支撑系统具备应急预案管理功能，应满足以下要求：

a) 新增、删除、查询和修改应急预案信息；

b) 对应急预案进行分类、分级管理。

6.3 对象管理

支撑系统具备对象管理功能，应满足以下要求：

a) 修改、删除和查询对象的信息；

b) 支持自动和人工方式采集对象的信息；

c) 对硬件资产、软件资产、数据资产、组织人员等信息进行管理，其中：

1) 对硬件资产信息进行管理，包括但不限于IP地址、MAC地址、硬件型号等；

注1：硬件资产主要包括计算机、网络设备、安全设备、存储设备、安防设备及办公设备等。

2) 对软件资产信息进行管理，包括但不限于软件版本、安装位置、安装时间等；

注2：软件资产主要包括安全系统、操作系统、工具软件、业务系统、网站等。

3) 对数据资产信息进行管理，包括但不限于文件位置、文件发布者等；

注3：数据资产主要包括数据库文件、文档文件、音视频文件、图片等。

4) 对组织人员信息进行管理，包括但不限于账号、权限等。

注4：组织人员主要包括管理人员、使用人员等。

6.4 信息安全事件监测

支撑系统具备信息安全事件监测功能，应满足以下要求：

a) 参照GB/Z 20986—2007，对信息安全事件进行分类、分级管理；

b) 具备自动和人工两种方式采集信息安全事件；

c) 对信息安全事件进行处置管理，包括事件告警和流程处置等。

6.5 运行监测

支撑系统具备运行监测管理功能，应满足以下要求：

a) 对接入的安全系统的基本信息、运维情况等进行管理；
b) 对安全系统的运行状态进行监测与日志记录，并提供异常日志的查询和导出；
c) 对安全系统的运行指标进行监测，并进行有效性评估。

6.6 流程处理

支撑系统具备流程处理功能，对信息安全事件、对象、运行监测等数据进行处置，应满足以下要求：

a) 支持告警流程处理；
b) 支持告警的自动触发功能；
c) 支持对产生的告警进行清除、确认和转换流程等处理；
d) 支持自动和人工方式发起流程；
e) 流程支持签收、反馈、审核/审批、归档等处理；
f) 配置流程模板、内容模版与回执模板等。

6.7 统计分析

支撑系统具备统计分析功能，应满足以下要求：

a) 根据组织、部门、类型、状态等，对硬件、软件、数据和人员等资产进行统计；
b) 根据组织、部门、类型、威胁级别等，对信息安全事件数据进行统计；
c) 根据组织、部门、正常率等，对运行监测数据进行统计；
d) 根据组织、部门、类型、状态、等级等，对告警数据进行统计；
e) 根据组织、部门、类型、状态等，对流程数据进行统计；
f) 对软硬件资产、信息安全事件进行关联分析；
g) 对数据进行综合性分析，提供安全报告，为决策提供数据支持。

6.8 考核管理

支撑系统具备考核管理功能，应满足以下要求：

a) 考核项的配置和修改；
b) 支持对考核项进行人工和自动评测；
c) 输出完整的考核报告，并提供报告导出。

6.9 发布与展示

支撑系统具备发布与展示功能，对应急预案、信息安全事件、运行监测等进行发布和安全态势展示，应满足以下要求：

a) 发布内容包括但不限于安全目标、通知通报及法律法规等；
b) 安全态势展示内容包括但不限于对象、信息安全事件、运行监测等，可采用地图展示、趋势图和比重图等表现形式。

6.10 采集与处理

支撑系统具备采集与处理功能，应满足以下要求：

a) 对信息安全事件数据和运行监测数据等进行采集；
b) 对第三方系统的检查结果数据、评估结果数据等进行采集，并支持多种数据采集方式和协议，包括但不仅限于 DB、HTTP、FTP 和 SNMP 等；
c) 对采集的数据进行处理和存储。

6.11 数据交换

支撑系统具备数据交换功能，应满足以下要求：

a) 支持各级支撑系统之间进行数据交换；

b) 数据交换的内容包括但不限于系统状态信息、安全策略信息和统计数据等。

6.12 备份与恢复

支撑系统具备数据备份与恢复功能，应满足以下要求：

a) 恢复六个月内所有的数据，包括但不限于信息安全事件、运行监测、告警、流程、统计和考核等数据；

b) 已存储的记录数据不被覆盖和删除，并在存储资源耗尽前告警。

7 自身安全性要求

7.1 身份鉴别

支撑系统身份鉴别应：

a) 在用户注册时，使用用户名和用户标识符标识用户身份。

b) 在用户登录时，使用受控的口令或具有相应安全强度的其他机制进行用户身份鉴别。

c) 采用至少两种身份鉴别机制，身份鉴别机制包括但不限于："用户名＋口令"鉴别方式、数字证书鉴别方式、生物特征鉴别方式。

d) 采用"用户名＋口令"的鉴别方式时，保证口令复杂度；并设定用户登录尝试阈值，当用户的不成功登录尝试超过阈值时，锁定管理员账号，并生成审计日志。

7.2 访问控制

支撑系统访问控制应：

a) 根据管理员用户角色和权限允许或禁止其对系统功能及数据资产等进行访问；

b) 对于越权访问的非法操作及尝试记录并告警。

7.3 权限管理

支撑系统权限管理应：

a) 采用三权分立的管理模式，管理员角色至少分为系统管理员、安全管理员、安全审计员三种，不同角色权限不应交叉；

b) 限定不同的管理员角色仅能通过特定的命令或界面执行操作；

c) 通过系统管理员负责用户账号的管理；

d) 通过安全管理员负责对用户账号进行授权；

e) 通过安全审计员负责对管理员和用户的操作进行日志记录，并对审计记录进行备份、整理。

7.4 数据安全

支撑系统数据安全应：

a) 对支撑系统的数据传输进行通信保护，确保各组件之间传输的数据（如数据采集、策略下发等）不被泄漏或篡改；

b) 具有数据安全备份与恢复功能，并支持在数据存储空间达到阈值时能够向管理员告警；

c) 检查支撑系统内存储数据的完整性和有效性；

d) 具有纠错报警和容错保护的能力，对录入数据、相关参数等进行有效性和完整性检查，并进行损坏恢复。

7.5 安全审计

支撑系统在安全审计方面应：

a) 对用户操作行为进行日志记录，日志记录应记录用户名、操作行为发生的日期和时间、功能模块、操作内容等，能进行组合查询、排序、数据输出，系统日志由安全审计员管理；

b) 对支撑系统自身各功能模块的工作状态进行检测，工作状态异常时告警。

8 安全保障要求

8.1 配置管理保障

配置管理保障应满足以下要求：

a) 针对不同用户提供唯一的授权标识；

b) 根据不同用户提供相应的配置管理文档。

8.2 开发

支撑系统开发应满足以下要求：

a) 描述系统的安全功能；

b) 描述所有安全功能接口的目的与使用方法；

c) 描述每个安全功能接口相关的所有参数；

d) 描述安全功能接口相关的安全功能实施行为；

e) 描述由安全功能实施行为处理而引起的直接错误消息；

f) 提供系统设计文档。

8.3 测试保障

在提供支撑系统的同时，提供该系统的测试文档，测试文档应包括：

a) 确定待测系统功能，描述测试目标；

b) 测试计划、测试过程描述、测试结果以及测试预期结果与测试结果的对比；

c) 在测试过程中记录测试每一项功能的实际情况。

8.4 交付与运维保障

提供安装和运维指南，详尽描述支撑系统的安装、配置和启动运行所必需的基本步骤。

8.5 指导性文档

提供支撑系统管理员指南，应包括：

a) 管理员使用的管理功能和接口；

b) 支撑系统的安全管理方法；

c) 管理员应进行控制的功能和权限；

d) 管理员在操作过程中的安全参数，并给出合适的参数值；

e) 管理员在操作过程中的安全配置指令；

f) 管理员在操作过程中的所有配置选项。

8.6 脆弱性分析

脆弱性分析应包括：

a) 执行脆弱性分析，并提供执行脆弱性分析相关文档；

b) 对被确定的脆弱性，明确记录采取的措施。

8.7 生命周期支持

生命周期支持应满足以下要求：

a) 建立一个生命周期模型对系统的开发和维护进行必要控制，并提供生命周期定义文档描述用于开发和维护系统的模型；

b) 提供开发安全文档，并描述为实现系统的开发所采取的必要的安全措施；

c) 提供在开发和维护过程中执行安全措施的证据。