ICS 35.020
L 70

团　　体　　标　　准

T/GDCSA 00*—2022

重要信息系统终端防范高级持续性威胁安全检查指南

Guide for security inspection of important information system terminals against advanced persistent threats

2022－00－00 发布　　2022－00－00 实施

******* 发 布

目　　次

前　　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由***提出。

本文件由***归口。

本文件起草单位：。

本文件主要起草人：。

重要信息系统终端防范高级持续性威胁安全检查指南

1 范围

本文件规定了重要信息系统终端防范高级持续性威胁安全检查的范围、方式、流程、方法和内容要求。

本文件适用于开展重要信息系统终端防范高级持续性威胁安全监督检查、委托检查工作，同时也适用重要信息系统运营单位开展重要信息系统终端防范高级持续性威胁防护工作自检查。

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，凡是标注日期的引用文件，仅注明日期的版本适用于本文件。凡是不注明日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 37027-2018 信息安全技术 网络攻击定义及描述规范

GB/T 37980-2019 信息安全技术 工业控制系统安全检查指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

重要信息系统 important information system

受到破坏后会对国家或行业安全、社会秩序、公共利益造成较大损害或带来严重经济损失的信息系统。

3.2

高级持续性威胁 APT advanced persistent threat

精通复杂技术的攻击者利用多种攻击方式对特定目标进行长期持续性网络攻击。

3.3

安全检查 security inspection

以查代促、以查促改、以查促管、以查促防，旨在推动提高信息安全工作能力和防护水平。

4 检查方式

4.1 监督检查

监督检查是指上级管理部门组织的或国家有关职能部门依法开展的检查。可依据本标准的要求，实施完整的重要信息系统终端防范高级持续性威胁安全检查过程，也可在自检查的基础上，对关键环节或重点内容实施检查。

4.2 自检查

自检查是指重要信息系统运营相关单位发起的对本单位重要信息系统终端防范高级持续性威胁安全状况进行的检查。自检查在本标准的指导下，结合系统特定的安全要求进行实施。

4.3 委托检查

受检单位或监督检查的组织部门不具备检查能力，可委托经相关主管部门认可的机构开展检查。

5 检查工作实施流程

5.1 计划准备阶段

5.1.1 计划准备阶段工作内容

根据检查工作的要求，明确检查工作的方式，包括监督检查、企业自查等。

明确检查工作的依据，包括国家、行业相关文件及标准，主管机构要求等。

明确检查工作的范围，包括被检查的单位、系统、涉及人员等。

明确检查工作的内容，相关要求详见本标准第 7 章。

明确检查所需的安全检查工作计划、工作方案等材料、人员、工具、办公条件准备及人员培训等工作。委托第三方服务机构实施现场检查工作的，检查机构安排专人陪同。

5.1.2 计划准备阶段的角色和职责

检查机构职责：

a) 向被检查单位介绍安全检查的意义和目的、检查内容、流程、工作方法及存在风险说明等；
b) 了解被检查单位的基本状况和指出所需基本资料；
c) 准备安全检查所需材料，包括安全检查工作计划、工作方案等；工作计划和方案需提前下发至被检查单位，明确要求被检查单位对必要的系统和数据进行备份；
d) 确定检查人员，包括确认分工安排、各工作组联系方式、沟通联络平台建立等；
e) 准备安全检查所需工具和文档；
f) 准备人员的培训，如组织参与工作的相关工作人员进行工作要求宣贯工作操作流程培训等。

被检查机构职责：

a) 向检查机构提供本单位基本情况介绍；
b) 准备检查机构所需的资料和提供办公条件；
c) 为检查机构提供支持和协调，安排对接人员；
d) 备份数据和相关系统，制定应急预案。

5.2 现场检查阶段

5.2.1 现场检查阶段工作内容

现场检查阶段，检查机构调研被检查单位的资产并填写“XX（单位名称）重要信息系统终端资产信息表”（包含终端品牌，型号，操作系统版本，使用终端安全软件情况）；

检查人员向被检查单位说明检查工作可能带来的风险及其规避措施，填写“XX（单位名称）检查风险提示单”，并由被检查单位签字确认。

检查人员现场填写“XX（单位名称）重要信息系统终端高级持续性威胁安全检查表”，检查完成后需要由被检查单位签字确认。

5.2.2 现场检查阶段的角色和职责

检查机构职责：

a) 调研检查被检查单位的资产范围。调研与重要信息系统相连接的终端，或者可访问重要信息系统的终端；

b) 明确检查工作方案，向被检查单位说明检查的工作步骤和工作方法；

c) 明确具体风险规避措施，向被检查单位说明检查工作可能带来的风险及其规避措施；

d) 检查工作现场实施：利用人员访谈、文档审查、配置核查和安全测试的方法检查系统的保护措施与本标准要求的符合情况，以及正确性和有效性。

被检查机构职责：

a) 协调配合检查的内部相关人员关系，有序开展受检工作；

b) 回答完成检查人员相关的问询、验证和测试；

c) 相关负责人员对检查的系列表单结果进行签字确认。

5.3 结果上报阶段

5.3.1 结果上报阶段工作内容

现场检查阶段工作完成后，由检查组对检查结果进行整理并分析上报，编写“XX（单位名称）检查结果报告”。

5.3.2 结果上报阶段的角色和职责

检查机构职责：

a) 分析检查结果，形成检查结论；

b) 上报上级或相关部门。

5.4 隐患整改阶段

5.4.1 隐患整改阶段工作内容

a) 汇总检查结果。运营单位内部的网络安全责任单位依据检查结果、意见进行梳理、汇总，从安全管理、技术防护等方面对检查发现的问题和隐患进行分类整理。

b) 分析问题隐患。运营单位内部的网络安全责任单位应对检查发现的问题和隐患逐项进行研究，深入分析产生的原因。结合年度网络安全形势，对本单位面临的网络安全威胁和风险程度、信息系统抵御网络攻击的能力进行评估。

c) 研究整改措施。运营单位内部的网络安全责任单位在深入分析问题隐患的基础上，研究提出针对性的改进措施建议。组织相关人员进行整改，对于不能及时整改的，要制定整改计划和时间表，整改完成后应及时进行再评估。

d) 编写总结报告。运营单位内部的网络安全责任单位对检查工作进行全面总结，编写检查报告，使用填报工具填报相关清单、自查检查结果统计表，并结合内部管理体系及应急预案情况及时上报。

e) 视情况，邀请上级管理单位、当地公安网安部门等相关单位进行指导协助。如管理部门要求进行溯源分析，则运营单位应当积极配合。

5.4.2 隐患整改阶段的角色和职责

检查机构职责：上级管理单位或公安网安部门等向被检查单位反馈意见函。

被检查机构职责：

a) 编制整改报告，按规定落实整改并上报后续的整改情况；

b) 积极响应并配合上级管理部门组织的或国家有关职能部门的相关安全专项行动等。

6 检查内容的选择方法

6.1 全覆盖法

选取安全检查内容的所有检查项。

6.2 重点项抽取法

根据上级管理部门或国家有关职能部门对重要信息系统终端防范高级持续性威胁安全检查工作的实际预期目标需求，从检查内容中确定重点检查项，只检查重点项。

6.3 增项检查法

根据上级管理部门或国家有关职能部门要求和 APT 防护发展态势等情况，设计检查内容中未包含的检查项作为新增检查项。

7 检查内容

7.1 概述

检查内容主要是对终端安全的防范检查，包括终端品牌、操作系统，终端安全软件情况的检查，主要涉及入侵防范、恶意代码防范、威胁检测与防御、可信验证、身份鉴别、访问控制、安全审计及数据完整性等方面。

7.2 恶意代码防范与入侵防范

应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。

a) 查看系统中安装的防病毒廉。询问管理员病毒库更新策略；

b) 查看系统中采取何种可信验证机制，访谈管理员实现原理等；

c) 询问系统管理员网络防病毒软件和主机防病毒软件分别采用什么病毒库；

d) 询问系统管理员是否采用统一的病毒更新策略和查杀策略；

e) 当发现病毒入侵行为时，如何发现，如何有效阻断，报警机制等。

7.3 威胁检测与防御

应采用威胁检测与防御技术措施，以威胁情报驱动终端安全防御，结合大数据平台对数据归类、关联分析，应核查是否与威胁情报及异常行为分析结合，对原始终端安全数据进行检索和关联分析。

a) 应检查是否通过终端安全行为分析技术检测和防御 APT 攻击；

b) 应检查是否通过终端全流量分析技术检测和防御 APT 攻击；

c) 应检查是否具备通过 ioc 或者恶意代码特征等技术手段识别 APT 组织的能力；

d) 应检查是否具备从内存保护技术的方式检测和阻断 APT 攻击的能力。

7.4 可信验证

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

a） 检查终端的启动，是否实现可信验证的检测过程，查看对哪些系统引导程序、系统程序或重要配置参数进行可信验证；

b） 修改其中的重要系统程序之一和应用程序之一，核查是否能够检测到并进行报警；

c） 是否将验证结果形成审计记录送至安全管理中心等。

7.5 身份鉴别

当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。应核查是否采用加密等安全方式对系统进行远程管理，防止鉴别信息在网络传输过程中被窃听。

7.6 访问控制

——应对登录的用户分配账户和权限：

a） 应核查是否为用户分配了账户和权限及相关设置情况；

b） 应核查是否已禁用或限制匿名、默认账户的访 i 问权限。

——应重命名或删除默认账户，修改默认账户的默认口令：

a） 应核查是否已经重命名默认账户或默认账户已被删除；

b） 应核查是否已修改默认账户的默认口令。

——应及时删除或停用多余的、过期的账户，避免共享账户的存在：

a） 应核查是否不存在多余或过期账户，管理员用户与账户之间是否一一对应；

b） 应测试验证多余的、过期的账户是否被删除或停用。

——应授予管理用户所需的最小权限，实现管理用户的权限分离：

a） 应核查是否进行角色划分；

b） 应核查管理用户的权限是否已进行分离；

c） 应核查管理用户权限是否为其工作任务所需的最小权限。

7.7 安全审计

——应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计：

a） 应核查是否开启了安全审计功能；

b） 应核查安全审计范围是否覆盖到每个用户；

c） 应核查是否对重要的用户行为和重要安全事件进行审计。

——审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息：应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

——应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等：

a） 应核查是否采取了保护措施对审计记录进行保护；

b） 应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。

7.8 数据完整性

应采用校验技术保证重要数据在传输过程中的完整性。

a) 应核查系统设计文档，鉴别数据、重要业务数据.重要审计数据.重要配置数据、重要视频数据和重要个人信息等在传输过程中是否采用了密码技术保证完整性；
b) 应测试验证在传输过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。

7.9 应急管理

应采取必要应急管理措施防止终端在日常使用中被入侵，应核查是否具备完善应急管理流程。

a) 应核查是否制定针对 APT 事件的应急预案框架，包括应急计划、组织结构、应急处置和上报监管和主管等流程；
b) 应核查是否定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；
c) 应核查应急保障队伍的建立情况，应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；
d) 应核查终端的失陷技术和分析，是否对失陷后终端制定应急处置和追踪溯源。