

ICS 35.040
L71
备案号: 11941-2002

DB

北京市地方标准

DB11/T 145-2002

政务公开网站 通用安全技术要求

2002-01-30 发布

2002-02-20 实施

北京市质量技术监督局 发布

目 次

前言	V
引言	VI
1 范围	1
2 术语和定义	1
3 系统概述	3
4 安全环境	3
4.1 资产	3
4.1.1 系统内的数据	3
4.1.2 系统软件	4
4.1.3 系统硬件	4
4.2 系统具备的前提条件	4
4.2.1 系统设备维护(A.Maint_Sysdev)	4
4.2.2 系统软件安装维护(A.Maint_Inst_Syssoft)	4
4.2.3 系统管理员能力(A.Competent_Admin)	4
4.2.4 系统管理员不会滥用权限(A.No_Abuse_By_Admin)	4
4.2.5 系统数据毁坏(A.Acc_Ovrwrit_SysData)	4
4.2.6 远程用户(A.Remote_Access)	4
4.2.7 可信用户(A.Trusted_User)	4
4.2.8 物理访问(A.Prot_Against_Nature)	4
4.2.9 掉电保护(A.prot_of_Power_fault)	5
4.3 对系统的威胁	5
4.3.1 管理错误(T.Admin_Err_Commit)	5
4.3.2 管理疏忽(T.Admin_Err_Omit)	5
4.3.3 威胁主体的能力(T.Outsider_Med)	5
4.3.4 未授权的访问(T.Acs_to_Out)	5
4.3.5 攻击者尝试使资源拒绝服务(T.Hack_Avl_Resource)	5
4.3.6 传输错误(T.Trans_Err)	5
4.3.7 关键系统组件失效(T.Component_Failure)	5
4.3.8 恶意代码(T.Malicious_Code)	5
4.4 系统组织安全策略	5
4.4.1 安全设备选型或采购控制(P.Sel_device)	5
4.4.2 网络隔离(P.tec.Isolated)	5
4.4.3 站点监控与审计(P.Monitor and Audit)	6
4.4.4 漏洞扫描(P.Scan)	6
4.4.5 入侵检测(P.check and measure)	6

4.4.6 Web 页面监测与自动修复(P.Monitor and Recovery)	6
4.4.7 系统备份(P.Backup)	6
5 安全目的	6
5.1 系统安全目的	6
5.1.1 安全角色(O.Security_Roles)	6
5.1.2 安全功能管理行为(O.Security_Func_Mgt)	6
5.1.3 安全相关配置管理(O.Secure_Configuration)	6
5.1.4 管理安全属性(O.Security_Attr_Mgt)	6
5.1.5 管理安全关键数据(O.Security_Data_Mgt)	6
5.1.6 远程可信系统的可信通道(O.Comm_Trusted_Channel)	6
5.1.7 用户标识和鉴别(O.I&A)	6
5.1.8 系统访问控制(O.RBAC)	7
5.1.9 保护系统安全功能(O.Sys_Self_Protection)	7
5.1.10 采用补丁程序修改代码(O.Apply_Code_Fixes)	7
5.1.11 限定用户和服务的资源(O.Resource_Quotas)	7
5.1.12 保护和维持安全的系统状态(O.Secure_State)	7
5.1.13 系统功能运行的完整性测试(O.Integrity_Practice)	7
5.1.14 对已发现的攻击的响应(O.React_Discovered_Atk)	7
5.1.15 主页的完整性监视与恢复(O.Website_Mnt_Recovery)	7
5.1.16 控制系统数据的输入(O.Data_Imp_Control)	7
5.1.17 系统数据内部传递的完整性(O.Integ_Sys_Data_Int)	7
5.1.18 识别对接收信息的修改(O.Rcv_MsgMod_ID)	7
5.1.19 恢复对接收信息的修改(O.Rcv_MsgMod_Rcvr)	7
5.1.20 识别对发布信息的修改(O.Snt_MsgMod_ID)	7
5.1.21 支持在发布信息被修改后的恢复(O.Snt_MsgMod_Rcvr)	8
5.1.22 关键组件失效时保持安全状态(O.Fail_Secure)	8
5.1.23 关键组件运行错误容限(O.Fault_Tolerance)	8
5.1.24 出现恶意代码时能恢复对象和数据(O.Clean_Obj_Recovery)	8
5.1.25 审计管理角色(O.Audit_Admin_Role)	8
5.1.26 标识审计记录(O.Audit_Generation)	8
5.1.27 对可能丢失所保存的审计记录作出响应(O.Audit_Loss_Respond)	8
5.1.28 保护存储的审计记录(O.Audit_Protect)	8
5.1.29 确保可用的审计存储空间(O.Guarantee_Audit_Stg)	8
5.1.30 审计系统访问减少误用(O.Audit_Deter_Misuse)	8
5.1.31 系统备份(O.Sys_Backup_Procs)	8
5.1.32 检测备份硬件、固件、软件的修改(O.Sys_Backup_Verify)	8
5.1.33 网络隔离(O.Tec_Isolated)	9
5.2 环境安全目的	9
5.2.1 安装与操作控制(OE.Install)	9
5.2.2 物理控制(OE.Ph_Access)	9
5.2.3 授权管理员培训(OE.Train)	9