**内蒙古自治区高级人民法院**

**网络（通信）基础设施**

**网络安全等级保护现场测评问题汇总表**

**测评委托单位：内蒙古自治区高级人民法院**

**测评实施单位：内蒙古信元网络安全技术股份有限公司**

**现场测评时间：2022年 月 日 — 月 日**

**被测系统级别：网络（通信）基础设施 (三级)**

| **测评控制类** | **问题描述** | **关联资产** | **备注** |
| --- | --- | --- | --- |
| **安全计算环境**  **（网络部分）** | 1.设备存在默认用户。 | 楼层交换机、审计区汇聚交换机、数据库区接入交换机、运维区汇聚交换机、服务器区接入交换机、移动专网防火墙、政法网IDS、政法网防火墙-1、数据库区防火墙、服务器区防火墙、运维区防火墙、日志审计、服务器区WEB防护-1、服务器区WEB防护-2、政法网IPS-2、政法网防火墙-2、审计管理区防火墙、政法网IPS-1、堡垒机、外部专网防火墙、移动专网单向光闸、移动专网视频交换系统、外部专网光闸-内、外部专网漏洞扫描、外部专网堡垒机、互联网单向光闸、互联网WAF、移动专网IPS、移动专网日志审计、移动专网漏洞扫描、移动专网堡垒机、堡垒机（安全设备）、数据库审计、安全审计、互联网漏洞扫描、互联网防毒墙、互联网IPS、互联网日志审计、互联网防火墙、互联网堡垒机、外部专网IPS、外部专网WAF、外部专网单向光闸、外部专网光闸-外、外部专网日志审计 |  |
| 2.未配置登录失败配置。 | 审计区汇聚交换机、楼层交换机、数据库区接入交换机、服务器区接入交换机、运维区汇聚交换机、堡垒机、外部专网堡垒机、移动专网堡垒机、互联网堡垒机 |  |
| 3.远程管理未采取必要措施防止鉴别信息在网络传输过程中被窃听（https、ssh）。 | 运维区汇聚交换机、服务器区接入交换机、数据库区接入交换机、楼层交换机、审计区汇聚交换机 |  |
| 4.未将日志外发至日志审计设备保存。 | 审计区汇聚交换机、楼层交换机、政法网路由器、数据库区接入交换机、服务器区接入交换机、运维区汇聚交换机、政法网IPS-2 |  |
| 5.网络中未提供实时备份功能；未将重要数据实时备份至备份场地。 | 审计区汇聚交换机、楼层交换机、核心交换机、数据库区接入交换机、政法网路由器、服务器区接入交换机、运维区汇聚交换机、移动专网防火墙、政法网防火墙-1、政法网IDS、堡垒机、政法网IPS-1、审计管理区防火墙、政法网防火墙-2、政法网IPS-2、服务器区WEB防护-2、服务器区WEB防护-1、日志审计、运维区防火墙、服务器区防火墙、数据库区防火墙、互联网堡垒机、安全准入、互联网防火墙、互联网日志审计、互联网IPS、互联网防毒墙、互联网漏洞扫描、网管平台、安全审计、态势感知（内网）、数据库审计、堡垒机（安全设备）、移动专网堡垒机、移动专网漏洞扫描、移动专网日志审计、移动专网IPS、互联网态势感知、互联网WAF、互联网单向光闸、外部专网堡垒机、外部专网漏洞扫描、外部专网光闸-内、移动专网探针、移动专网视频交换系统、移动专网单向光闸、外部专网防火墙、外部专网日志审计、外部专网光闸-外、外部专网单向光闸、外部专网WAF、外部专网IPS |  |
| 6.计算设备没有实现对系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | 审计区汇聚交换机、楼层交换机、核心交换机、数据库区接入交换机、政法网路由器、服务器区接入交换机、运维区汇聚交换机、移动专网防火墙、政法网防火墙-1、政法网IDS、堡垒机、政法网IPS-1、审计管理区防火墙、政法网防火墙-2、政法网IPS-2、服务器区WEB防护-2、服务器区WEB防护-1、日志审计、运维区防火墙、服务器区防火墙、数据库区防火墙、互联网堡垒机、安全准入、互联网防火墙、互联网日志审计、互联网IPS、互联网防毒墙、互联网漏洞扫描、网管平台、安全审计、态势感知（内网）、数据库审计、堡垒机（安全设备）、移动专网堡垒机、移动专网漏洞扫描、移动专网日志审计、移动专网IPS、互联网态势感知、互联网WAF、互联网单向光闸、外部专网堡垒机、外部专网漏洞扫描、外部专网光闸-内、移动专网探针、移动专网视频交换系统、移动专网单向光闸、外部专网防火墙、外部专网日志审计、外部专网光闸-外、外部专网单向光闸、外部专网WAF、外部专网IPS |  |
| 7.未采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 | 审计区汇聚交换机、楼层交换机、核心交换机、数据库区接入交换机、政法网路由器、服务器区接入交换机、运维区汇聚交换机、移动专网防火墙、政法网防火墙-1、政法网IDS、堡垒机、政法网IPS-1、审计管理区防火墙、政法网防火墙-2、政法网IPS-2、服务器区WEB防护-2、服务器区WEB防护-1、日志审计、运维区防火墙、服务器区防火墙、数据库区防火墙、互联网堡垒机、安全准入、互联网防火墙、互联网日志审计、互联网IPS、互联网防毒墙、互联网漏洞扫描、网管平台、安全审计、态势感知（内网）、数据库审计、堡垒机（安全设备）、移动专网堡垒机、移动专网漏洞扫描、移动专网日志审计、移动专网IPS、互联网态势感知、互联网WAF、互联网单向光闸、外部专网堡垒机、外部专网漏洞扫描、外部专网光闸-内、移动专网探针、移动专网视频交换系统、移动专网单向光闸、外部专网防火墙、外部专网日志审计、外部专网光闸-外、外部专网单向光闸、外部专网WAF、外部专网IPS |  |
| 8.未对审计进程进行保护，防止未经授权的中断。 | 运维区汇聚交换机、服务器区接入交换机、数据库区接入交换机、楼层交换机、审计区汇聚交换机、核心交换机、政法网路由器、外部专网光闸-外、外部专网单向光闸、外部专网WAF、外部专网IPS、政法网防火墙-1、政法网IDS、政法网IPS-2、审计管理区防火墙、政法网防火墙-2、堡垒机、政法网IPS-1、服务器区WEB防护-2、服务器区WEB防护-1、运维区防火墙、服务器区防火墙、数据库区防火墙、互联网堡垒机、互联网防火墙、互联网IPS、互联网防毒墙、互联网漏洞扫描、堡垒机（安全设备）、移动专网堡垒机、移动专网漏洞扫描、移动专网IPS、互联网WAF、互联网单向光闸、移动专网防火墙、外部专网堡垒机、外部专网漏洞扫描、外部专网光闸-内、移动专网视频交换系统、移动专网单向光闸、外部专网防火墙 |  |
| 9．未配置登录地址限制。 | 政法网IDS、服务器区WEB防护-1、服务器区WEB防护-2、政法网IPS-1、堡垒机、政法网IPS-2、外部专网堡垒机、互联网WAF、移动专网IPS、移动专网堡垒机、堡垒机（安全设备）、互联网IPS、互联网堡垒机、外部专网IPS、外部专网WAF |  |
| **测评控制类** | **问题描述** | **关联资产** | **备注** |
| **安全通信网络** | 1.系统未采用校验码技术或密码技术进行通信完整性验证。 | |  |
| 2.云平台网络中没有采用密码技术保证通信过程中数据的保密性。 | |  |
| 3.通信设备没有基于可信根对系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证。 | |  |
| **测评控制类** | **问题描述** | **关联资产** | **备注** |
| **安全区域边界** | 1.互联网边界防病毒已过期，无法对互联网边界的恶意代码进行检测和清除。 | |  |
| 2.在互联网边界处未部署上网行为管理设备，无法对访问互联网的用户行为进行审计。 | |  |
| 3.没有基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界应用程序等进行可信验证。 | |  |
| **测评控制类** | **问题描述** | **关联资产** | **备注** |
| **安全管理中心** | 1.未实现通过软件定义化的方式对安全设备的安全策略进行集中管控。 | |  |
| **安全物理环境** |  |  |  |
|  |  |  |
| **测评控制类** | **问题描述** | | **备注** |
| **安全管理制度** |  | |  |
| **安全管理机构** |  | |  |
| **安全管理人员** |  | |  |
|  | |  |
|  | |  |
| **安全建设管理** |  | |  |
|  | |  |
| **安全运维管理** |  | |  |
| **漏洞扫描** | 详见漏洞扫描报告 | |  |
| **渗透测试** | 详见渗透测试报告 | |  |

**测评委托单位负责人： 测评单位负责人：**