XXXXX

等级保护安全建设方案

3 月

目录

1 项目背景 4

1.1 方案目标 4

1.2 项目范围 4

1.3 设计标准 4

1.4 参考标准 5

2 法院信息系统情况 5

2.1 系统组成 5

2.2.1XXXXX 现网网络拓扑图 6

2.2.2 存在安全问题分析 6

3 安全需求分析 7

3.1 安全指标与需求分析 7

4 信息安全体系框架设计 10

5 技术体系整改 11

5.1 边界安全 11

5.2 数据安全.....12

5.3 主机安全.....12

5.4 运维管理.....13

6 安全产品布署情况.....13

6.2 产品布署说明.....14

6.2.1 防病毒网关产品布署.....14

6.2.2 终端杀毒防御系统布署.....15

6.2.3 堡垒机产品布署.....16

6.2.4 日志审计产品布署.....18

6.2.5 数据库审计产品布署.....19

7 安全产品布署情况.....20

7.1.1 管理方法实现.....20

7.1.2 管理机构和人员设置.....20

7.1.3 管理制度建设和修订.....20

7.1.4 人员安全技能培训.....21

7.1.5 安全实施过程管理.....21

7.2 方案评审.....22

7.3 安全漏洞扫描 22

1 项目背景

近年来，勒索病毒威胁展现愈演愈烈之势，传输方式更多元，病毒更新迭代加紧，勒索病毒俨然成为近两年来最严峻网络安全威胁之一。而勒索病毒攻击方式也从原来广撒网逐步转变为定向攻击高价值目标，从对个人客户攻击逐步转移至以政府机构、主要行业为攻击对象。

针对勒索病毒安全事件频发以及暴发后巨大影响，最高法出台通知，要求全国各级法院依照要求进行整改，切实加强安全风险管控，确保法院专网安全稳定运行。11 月 12 日起，最高法经过办公厅秘书处，陆续向全国各法院公布《关于展开全国法院办公专网信息安全专题整改工作通知》。同时依照《国家网络安全法》、《信息系统安全等级保护基本要求》等相关法规及要求，以及 XXXXX 对信息系统安全稳定运行业务需求，经过事前威胁检测、事中联动防御、事后关联分析机制。全方面实现GBT22239-《信息安全技术信息系统安全等级保护基本要求》中对于三级系统安全要求。

1.1 方案目标

此次 XXXXX 关键业务系统等级保护安全建设主要目标是：

按照等级保护要求，结合实际业务系统，对法院关键业务系统进行充分调研及详细分析，将法院关键业务系统系统建设成为一个及满足业务需要，又符合等级保护三级级系统要求业务平台。

依照国家《国家网络安全法》、《信息系统安全等级保护基本要求》等相关法规及要求，以及 XXXXX 对信息系统安全稳定运行业务需求，经过事前威胁检测、事中联动防御、事后关联分析机制。全方面实现 GBT22239-《信息安全技术信息系统安全等级保护基本要求》中对于三级系统安全要求。

同时结合 XXXXX 网络现实状况及信息安全建设情况进行规划设计，依照信息系统定级情况、信息系统承载业务情况和安全需求等，设计合理、满足等级保护要求安全改造方案并以此为依据提出具备可执行性安全整改提议，经过实施安全整改，从技术和管理两方面达成国家等级保护基本要求，完善 XXXXX 信息系统安全技术防护方法、安全管理制度和安全运维体系，分期建设完整信息安全防护体系，最终目标是 XXXXX 网络及应用系统安全稳定运行以及经过最终测评。

1.2 项目范围

XXXXX 局域网基础系统、科技法庭系统、办公自动化系统（按照安全类别第 III 级（S3A3G3）标准设计）。

1.3 设计标准

在项目实施过程中，将遵照以下标准：

- 符合性标准：项目建设要符合国家等级保护政策和标准规范要求，经过专业等级保护测评机构测评，并到公安部门及上级主管单位完成立案；
- 适度安全标准：安全防护工作根本性标准，指安全防护工作应依照主要信息系统安全等级，平衡效益与成本，采取适度安全技术和管理方法；

- 可控性标准：指相关项目组人员应具备可靠职业素质和专业素质；项目实施过程中技术工具使用可控，防止引入新风险；项目过程可控性：要对整个安全防护项目进行科学项目管理，实现项目过程可控性；

- 最小影响标准：从项目管理层面和技术管理层面，项目标实施过程对信息系统正常运行影响降低到最低程度，以确保日常业务正常运行；

保密性标准：相关安全防护工作人员签署协议，承诺对所进行安全防护工作保密，确保不泄露主要信息系统安全防护工作主要和敏感信息。。

1.4 参考标准

在开展《信息系统等级保护安全体系建设方案》设计过程中将严格按照国家相关法律标准展开，为用户提供符合本身实际需求及满足等级保护建设规范优质方案，主要依据标准文件包含以下：

本方案主要参考一下标准和依据：

国家标准：

GB 17859-1999　计算机信息系统安全保护等级划分准则

GB/T 22240- 信息安全技术 信息系统安全等级保护定级指南

GB/T 22239- 信息安全技术 信息系统安全等级保护基本要求

GB/T 25058- 信息安全技术 信息系统安全等级保护实施指南

2 法院信息系统情况

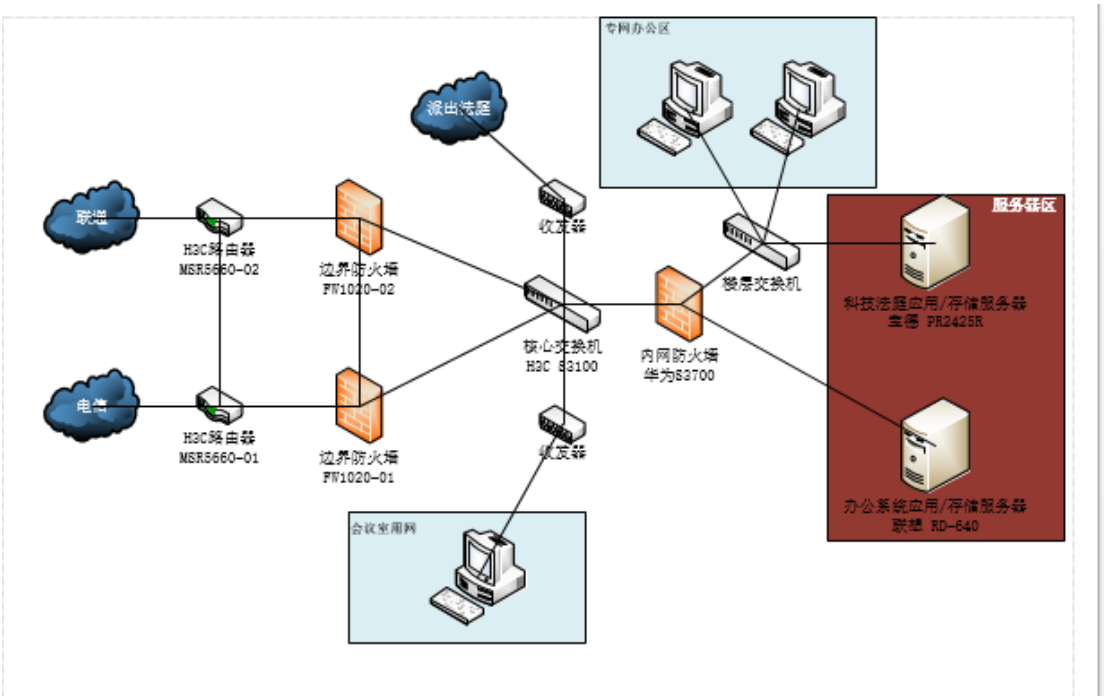
2.1 系统组成

XXXXX 信息系统主要包含外部网络（外网，连接互联网）和内部网络（内网，提供内部业务系统使用，与互联网逻辑隔离）。

系统有科技法庭系统和局域网基础系统以及办公自动化系统。

- 科技法庭系统（S3A3G3 级）
- 局域网基础系统（S3A3G3 级）
- 办公自动化系统（S3A3G3 级）

2.1.1 XXXXX 现网网络拓扑图



XXXXX 现有网络架构图 2-1

2.1.2 存在安全问题分析

- **边界安全方面**

未能依照业务需要对会话终止时间进行合理限制；未统计网络攻击行为日志信息；发生严重入侵事件时未能对攻击行为进行报警；网络边界处未布署恶意代码检测方法；多个月内恶意代码库未更新升级；未对管理员登录网络设备地址进行任何限制；未对全部业务确定主要性、优先级，制订业务相关带宽分配标准及对应带宽控制策略等等。

- **主机安全方面**

科技法庭系统： 未对主要文件访问权限作合理配置；假如是 Windows 系统，未关闭系统默认共享；假如是 Unix 系统查看主要目录访问权限；

局域网基础系统：未启用系统安全审计功效，未对用户主要操作进行日志统计；主机层未安装防病毒软件；网络层未布署防毒墙；主机层与网络层布署防恶意代码产品具备相同代码库；所安装防恶意代码软件为单机版，未能实现统一管理，统一更新，统一检测与查杀等等。

- **数据安全方面**

访问控制覆盖粒度未包含主体、客体及它们之间操作情况二：渗透测试发觉存在访问控制未能覆盖客体；非授权人员能够进行用户权限管理，实际授权与权限策略不一致，可进行越权操作；存在默认权限账户；未对审计统计进行统计、查询及分析，未生成升级报表；未提供对一个时间段内可能并发会话连接数进行限制；未提供系统服务水平检测功效；未提供服务优先级设置功效等等。

3 安全需求分析

3.1 安全指标与需求分析

XXXXX 关键业务系统安全建设关键需求即满足等级保护相关要求，所以将以满足等级保护指标为目标。依照前期监管机构检验结果，结合本身业务需求，能够确定需要满足等级保护指标以下表 3-1 所表示：

3.1.1

3.1.2