政府电子政务外网信息安全等级保护差异分析与规划

（网神信息技术（北京）股份有限公司，北京 100085）

随着我国信息化建设的不断发展与深化，来自各方面的安全威胁严重影响现有信息系统稳定、持续的运行，而基层政府信息化系统面临着复杂的应用环境，系统安全环境十分复杂。本文以浙江省台州市路桥区政府（以下简称为路桥区政府）为例，探讨了基层政府政务外网在信息安全等级保护政策下的安全策略的可行性与必要性。

随着信息化程度的不断深入，区政府信息系统面临越来越复杂多样的安全威胁，迫切需要对区政府电子政务外网信息系统的信息安全建设有一个统一的、可执行的、有效的规划。这一信息安全建设规划与建设，一方面是要进一步落实《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发 [2003]27 号）文件要求，加强对区政府电子政务外网网络和信息系统的安全保障能力；另一方面也是进一步贯彻落实《浙江省信息安全等级保护管理办法》（浙江省政府第 223 号令）文件精神，按照《浙江省电子政务 2008 年度建设任务指导书》（浙政办发 [2008]15 号）的要求部署工作。

1 建设规划设计思路

信息安全建设规划的内容与路桥区电子政务外网信息安全建设现状紧密结合且符合国家等级保护要求。因此，在设计路桥区电子政务外网信息安全建设规划之前，必须对路桥区电子政务外网信息系统进行基于公安部《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）（以下简称《基本要求》）相关要求的差异化分析工作。

1.1 差异化分析

经与信息安全主管部门和其他相关机构的确认，路桥区电子政务外网中区办公自动化系统、市对区办公自动化系统、审批系统被定级为三级，电子政务外网主干网络定级为三级，其他信息系统与其他次要网络定级为二级。

结合公安部等级保护《基本要求》详细分析评估路桥区电子政务外网信息系统存在的缺陷，从物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理，以及系统运维管理等全方位的对路桥区电子政务外网和重要信息系统进行差异化分析，分析方法包括现场实地调研、问卷调查、各类设备操作等。此次差异化分析工作共登录操作 36 台安全设备、网络设备与应用系统，问卷调查对象包括信息中心主要领导、信息安全工程师、网络维护人员以及运维人员。

分析结果显示，路桥区电子政务网信息系统虽然经过了多年的持续的信息安全建设，但在物理、网络、应用、运维、管理上存在诸多的缺陷与安全威胁。

1.2 安全规划设计思路

在设计信息安全规划过程中都会涉及到安全控制，所有安全控制都包含策略、组织、技术和运作四个要素，即每条安全控制，都可以描述为“根据某某策略，由某某组织（或人员），利用某某技术，进行某某操作”。将安全控制的四要素分别综合起来，成为策略体系、组织体系、技术体系和运作体系。这四个体系构成了安全体系。

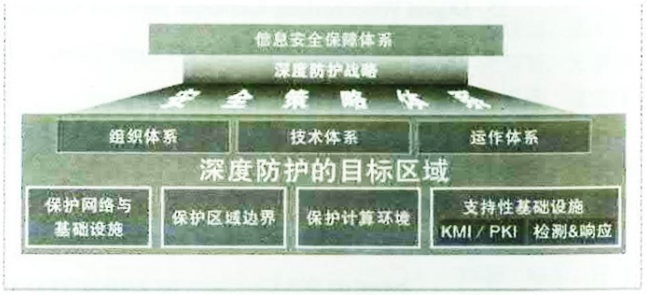

图1 路桥区政府外网信息系统安全体系架构图

图 1 最下面是路桥区政府电子政务外网信息系统的保护对象框架，根据信息资产逻辑图，我们将路桥区政府电子政务外网信息系统的保护对象分成计算区域、区域边界、通信网络和基础设施等。计算区域部分主要指提供业务的网络服务，计算区域内部可以根据路桥区政府电子政务外网信息系统的实际需求进一步细分为子区域、边界和通信网络。对不同区域、边界和通信网络，其安全需求是不同的。保护对象框架将路桥区政府电子政务外网信息系统安全问题细分为一组结构化的安全需求。

路桥区政府外网信息系统作为综合型业务系统，具有完整性要求高、可靠性要求高，实时性要求高的特点，需要具有强大安全防护措施。

2 信息安全建设规划方案评审

台州市政府、台州市保密局、台州市路桥区公安局等相关专家组成的专家组共同对路桥区政府电子政务外网信息安全建设规划方案进行评审。在评审会上，各位专家从不同的角度提出在信息安全建设过程中可能存在的安全威胁，而这些安全威胁在建设规划方案中都有了较为具体的、可执行的解决方案。该信息安全规划方案的完整性、可操作性以及前瞻性获得了与会专家的一致好评。

3 结束语

路桥区电子政务外网信息安全建设规划方案自 2010 年评审通过后，路桥区每年严格按照该方案的内容，有计划的、有步骤的进行分步建设。该信息安全建设规划方案不仅为今后路桥区政府电子政务外网信息安全建设指明了方向，还为全国各基层电子政务网站落实信息安全等级保护有关政策提供了有益尝试。（责编 张岩）

中华人民共和国公安部主管
公安部第三研究所主办
中国计算机学会计算机安全专业委员会

国际标准连续出版物号：ISSN1671-1122
国内统一连续出版物号：CN31-1859/TN

信息网络安全

NETINFO SECURITY

[等级保护]

- 构建证券行业虚拟化数据中心基础架构的信息安全研究

[技术研究]

- 操作系统中基于安全封装的访问控制实现方法
- 基于虚拟桌面技术的公安业务数据安全管控研究
- Android平台上基于WebKit引擎的安全浏览器的设计与实现

[理论研究]

- 信息安全服务外包管理思考

[权威分析]

- 2012年10月十大重要安全漏洞分析

ISSN 1671-1122
12>
771671 112125

中国核心期刊（遴选）数据库用刊
2012 第12期
总第144期