ICS 35.040
L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 24294—2009

信息安全技术
基于互联网电子政务信息安全实施指南

Information security technology—Guide of implementation for internet-based E-government information security

2009-07-30 发布　　2010-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

GB/Z 24294—2009

中华人民共和国
国家标准化指导性技术文件
信息安全技术
基于互联网电子政务信息安全实施指南
GB/Z 24294—2009
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946　68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 2.25　字数 60 千字
2009年12月第一版　2009年12月第一次印刷
*
书号:155066·1-39257　定价 33.00 元

GB/Z 24294-2009

参 考 文 献

[1] GB/T 9387.2—1995 信息系统 开放系统互连 基本参考模型 第2部分:安全体系结构(ISO 7498-2:1989,IDT)

[2] GB/T 19715.2—2005 信息技术 信息技术安全管理指南 第2部分:管理和规划信息技术安全(ISO/IEC 13335-2:1997,IDT)

[3] GB/T 20270—2006 信息安全技术 网络基础安全技术要求

[4] GB/T 20274.1—2006 信息安全技术 信息系统安全保障评估框架 第一部分:简介和一般模型

目 次

C.6.4.8 安全事件处置

安全事件的处置满足GB/Z 20985的相应要求，评估事项包括：

a） 是否及时报告所发现的安全弱点和可疑事件，任何情况下用户均不应尝试验证弱点；

b） 是否制定安全事件报告和处置管理制度，规定安全事件的现场处理、事件报告和后期恢复的管理职责。

C.7 技术测试

使用测试工具对基于互联网电子政务系统进行安全扫描和渗透测试。

C.7.1 检测范围

测试范围应包括电子政务应用平台的安全防护设备和应用服务器，涉及的区域应包括安全管理区域、内部数据处理区域、公开数据处理区域、安全服务区域和办公区。

C.7.2 检测方法

C.7.2.1 安全扫描

通过收集系统的信息来自动检测远程或者本地主机安全性脆弱点。通过使用安全扫描，可以了解被检测端的大量信息。通过这些信息，可以了解到远程主机所存在的安全问题，从而能够及时修补系统存在的安全隐患。相关网络脆弱性扫描产品的功能与技术要求可以按照GB/T 20280的相应规定。

C.7.2.2 渗透测试

渗透测试是对安全扫描结果的进一步验证。渗透测试被设计用于描述安全机制的有效性和对攻击者的控制能力，从一个攻击者的角度出发对目标的安全性进行考察。

C.7.3 扫描测试

C.7.3.1 扫描测试点

应该包括内网检测点和外网检测点在内的多个扫描测试点。

C.7.3.2 扫描对象

具体包括：

a） 边界防护设备。主要包括VPN安全设备、防火墙和装有VPN客户端的移动安全接入终端。

b） 重要服务器。主要包括安全管理区域服务器、内部数据处理区域服务器、公开数据处理区域服务器和安全服务区域服务器。

C.7.3.3 扫描工具

具体包括：

a） 主机漏洞扫描工具。通过在主机本地的代理程序对系统配置、注册表、系统日志、文件系统或数据库活动进行监视扫描，搜集它们的信息，然后与系统的漏洞库进行比较，如果满足匹配条件，则认为安全漏洞存在。

b） 网络漏洞扫描工具。通过远程检测目标主机TCP/IP不同端口的服务，记录目标给予的应答，来搜集目标主机上的各种信息，然后与系统的漏洞库进行匹配，如果满足匹配条件，则认为安全漏洞存在；或者通过模拟黑客的攻击手法对目标主机进行攻击，如果模拟攻击成功，则认为安全漏洞存在。

C.7.4 渗透测试

渗透测试建立在扫描测试的基础上，针对开放的服务及发现的漏洞，利用工具对目标实施攻击，测评其是否能够提升攻击者的权限或能否对目标机的正常运行产生影响。渗透测试点与测试范围与扫描测试相同。渗透测试可能会对系统造成巨大损害，实际测试时应慎重，尤其对正式运行的系统要适度运行。

C.8 系统整改与评估结论

系统评估后应给出评估结论。并对于评估过程中出现的问题进行逐一整改，整改结果要经过评估人员的确认和复查。