广西科学院学报
Journal of Guangxi Academy of Sciences

2009,25(4):350～352
Vol. 25,No. 4 November 2009

电子政务网络安全防护体系构建*
Construction of E-government Network Security System

李 森[1,2],李陶深[1],洪 茹[2]
LI Sen[1,2],LI Tao-shen[1],HONG Ru[2]

(1.广西大学计算机与电子信息学院,广西南宁 530004;2.广西互联网络中心,广西南宁 530022)
(1. School of Computer, Electronics and Information, Guangxi University, Nanning, Guangxi, 530004, China; 2. Guangxi Internet Network Center, Nanning, Guangxi, 530022, China)

摘要:介绍构建电子政务网络安全防护体系的安全策略,安全区域划分方式,安全防护技术,以及构建得出的电子政务网络安全防护体系结构。
关键词:网络安全 策略 技术 结构
中图法分类号:TP393.08 **文献标识码**:A **文章编号**:1002-7378(2009)04-0350-03
Abstract: The construction of an E-government network security system includes the application of network security policy, security technology and the methods of dividing security network. An E-government network security system architecture was presented in this paper.
Key words: network security, policy, technology, system architecture

电子政务网络安全防护体系建设是电子政务发展的切实需要,随着我国电子政务建设的推进,很多应用系统急需网络安全基础设施的支持。由于电子政务涉及到国家的安全机密信息,它比个人或商务信息更重要,需要更高的安全性;同时电子政务必须要与民众交流,需要一定的开放性。然而电子政务网络在物理层、链路传输、网络结构、系统安全、应用与管理等不同层次都存在安全风险。网络物理层存在地震、水灾、火灾等环境事故造成整个系统毁灭,电源故障造成设备断电以至操作系统引导失败或数据库信息丢失,设备被盗、被毁造成数据丢失或信息泄漏,电磁辐射可能造成数据信息被窃取或偷阅等安全风险。网络传输链路会被入侵者在传输线路上安装窃听装置,窃取用户在网上传输的重要数据,再通过一些技术读出数据信息,造成泄密或者做一些篡改来破坏数据的完整性。网络结构规划不合理会增大网络安全的风险,如果易感染病毒的主机与受保护主机,或者是脆弱主机与受保护主机处于同一子网就很容易受非法、非授权访问。网络的设备操作系统、网络服务器操作系统、网络应用系统常用到的Windows、UNIX操作系统以及其它厂商开发的应用系统本身大多存在安全漏洞,这些系统安全漏洞都将存在重大安全隐患。应用和管理方面也存在很多安全风险,比资源共享、电子邮件、数据信息传输、病毒侵害、黑客攻击,以及内部管理人员或员工把内部网络结构、管理员用户名及口令以及系统的一些重要信息传播给外人等等,都会给系统带来不安全因素。所以,电子政务网络需要考虑不同安全层次、不同部门的大规模、复杂交互应用,确保信息的机密性、真实性、可用性和可控性。

1 电子政务网络的安全策略

电子政务网络安全防护体系建设的目标是实现一个安全的网络环境,使电子政务信息的完整性、保密性、可用性、真实性、不可抵赖性、可控性、可审查性得到保证。为达到目标,构建电子政务网络安全防护体系必须贯彻执行4项安全策略。

(1)将保障电子政务网与互联网之间连接与交换的安全作为电子政务安全防护体系建设的重要内容。要解决政务网与互联网的逻辑隔离,要防范黑客入侵、身份冒充、非法访问各个安全域,要解决操作系统安全、数据库安全、病毒及恶意代码防范等问

收稿日期:2009-08-19
修回日期:2009-10-23
作者简介:李 森(1981-),男,硕士研究生,主要从事网络信息安全技术研究。
*广西自然科学基金项目(桂科自0832056)资助。

题,要解决移动接入用户身份鉴别和安全传输等问题。一方面要强化审计,监控安全域间的信息交换;另一方面要保障电子政务网自身安全防护体系的健全,防范内部攻击。

(2)利用 PKI、PMI、密码等技术建立电子政务网信任体系和授权管理体系,保障电子政务网中信息传输和应用的安全,要实现全网统一的身份鉴别和授权访问机制,要解决重要终端用户敏感信息和数据的完整性、可用性、保密性问题和数据的访问控制等问题。

(3)通过建立电子政务网网络安全管理中心,建立一支安全系统运行维护和应急支援技术队伍,加强安全管理和实现有效监控,考虑政策、法规、制度、管理权限、级别划分、安全域划分、责任认定、安全培训等,制定切实有效的管理制度和运行维护机制,建设支撑安全管理的技术支撑体系。

(4)在电子政务网的建设中,严格遵循国家法规,选购和使用经国家批准的安全设备与技术。

2　电子政务网络的安全域划分和保护等级

划分安全域的目的是识别系统信息资产,明确安全保护对象,以采取相应的防护措施。在安全域划分时应遵循下面一些基本原则:整个电子政务网相对于其它网络是一个安全域,政务网内部要划分安全子域,政务网内部安全域划分要充分考虑网络业务使命及流程,安全域划分要利于安全设备的部署,安全域划分要保障业务正常开展,要按照等级保护要求形成安全域防护基本要求。

在安全体系设计中,将对不同的安全域采取不同的安全等级保护措施。电子政务网络按如下方式划分6个安全域:(1)互联网出口区,是逻辑隔离电子政务网和互联网的区域。(2)互联网服务区,是对外发布政务信息,与民众沟通的区域,含政府机构门户网站、网上办公等应用业务。(3)骨干网核心交换区,是核心网互联区。(4)CA 区,是认证、授权应用业务区。(5)公用网络区是政务网数据中心和运维管理中心,含公共数据库、视频会议、数据交换体系等应用业务。(6)接入节点单位网络,是政务网的真实用户接入区域,含各部委、厅局等接入单位。

按照国家标准,电子政务网网络管理中心安全域至少要达到第三级的要求,接入节点单位网络安全域至少达到信息安全等级保护第二级的要求。

3　电子政务网络的安全防护技术

电子政务网络在物理层安全要充分利用各种条件,保证设备位置的安全,如人员准入控制和监控;机房电力、温度、湿度、灰尘、消防等可满足、高可靠;硬件、磁介质、电缆、光缆等放置在适宜、安全的物理环境下,以及异地容灾等。

电子政务网络层安全一方面要考虑城域网的接入用户与网络管理中心的网络接入安全,主要采用第三层 VPN 接入认证系统予以实现,并利用基于 PKI 技术实现设备管理和认证;同时重点考虑实现电子政务网与因特网的逻辑隔离,采用防火墙、网闸、网络入侵检测、网络入侵防御系统、抗拒绝服务攻击系统、非法外联监控、实时监控系统(网络审计系统)等技术和手段,按照政务网与互联网联接的原则,对电子政务网与因特网联接的出口严格控制,统一管理。(1)防火墙系统,支持正反向代理技术,是以电子政务网安全域间实现逻辑隔离的技术手段,实现访问控制,防止 IP 地址欺骗和日志安全审计。在网络层,从外网进入的访问请求只能访问防火墙开放的端口和服务,防火墙作为内部对外的访问的代理,使用内部网络的 IP 地址不暴露在外网。在应用层,防火墙系统通过对应用层协议的分析来实现应用层的访问控制。防火墙系统的端口只要加限制,就可以有效防止黑客利用 IP 地址欺骗的方法从因特网访问政务网络。防火墙系统记录进出网络的访问行为,为网络访问行为的分析和事故审查提供依据,实现日志安全审计。(2)网闸,通过协议转换的手段,以信息摆渡的方式实现数据交换,而且只有被系统明确要求传输的信息才可以通过,起到物理隔离的安全效果。(3)入侵防御系统,可以实现从数据链路层到应用层的数据报文检测与分析的能力,实时阻断恶意网络流量的攻击与破坏,如阻止各种针对系统漏洞的攻击,屏蔽蠕虫、病毒和间谍软件,防御 DOS 及 DDOS 攻击,阻断或限制 P2P 应用等,从而达到对电子政务网网络基础设施的保护、应用的保护和网络性能的保护。(4)抗拒绝服务攻击系统,可以智能识别网站和网络中发生的 DDoS 攻击,并通过流量建模、反欺骗、协议栈行为模式分析、特定应用防护、用户行为模式分析、动态指纹识别、带宽控制等多种技术手段,准确、迅速地阻断攻击流量,从而保证正常流量的通过。(5)VPN 网关和安全认证网关,实现面向移动用户和不同网络安全域之间的可信接入与传输。各接入单位和个人主要采用客户透明模式、客户启动模式和净荷加密方式建立基于 PKI 技术的安全认证网关,实现基于 CA 的身份认证,与授权管理系统相结合,实现网络访问的集中授

权管理、访问控制以及用户行为审计。客户透明模式是由终端认证网关发起 IPSec 隧道，这种方式主要用于单位的整个网络的接入。客户启动模式是由终端实体安装桌面安全套件，发起 VPN 呼叫，建立 IPSec 隧道，通过认证实现网络接入，这种方式主要用于个人用户和单个终端的移动接入。净荷加密方式是不对 IP 报文头加密，直接对数据部分进行加密处理，可以穿透应用层的代理服务器，这种方式主要用于网络内设置了代理服务器的接入单位。(6)网络安全审计，这是全方位、分布式、多层次的强审计概念，真正全面实现 CC 国际标准的安全审计功能要求。电子政务系统中需要重点审计的有：网络通信系统审计、重要服务器主机操作系统审计、重要服务器主机应用平台软件审计、重要应用系统的审计和重要网络区域的客户审计等。网络通信系统审计主要包括对网络流量中典型协议分析、识别、判断和记录，还包括流量监测以及对异常流量的识别和报警、网络设备运行的监测等。重要服务器主机操作系统审计主要包括系统运行情况、系统配置情况、病毒或蠕虫感染情况、资源负载情况、系统日志、对重要文件的访问等的审计。重要服务器主机应用平台软件审计主要包括重要应用平台进程的运行、中间件系统、数据库系统和其他维护管理操作、对重要数据的访问和更改、数据完整性等的审计。重要应用系统的审计主要包括办公自动化系统、公文流转和操作、网页完整性、相关政务业务系统等的审计。重要网络区域的客户机审计主要包括病毒感染情况、通过网络进行的文件共享操作、文件拷贝/打印操作、通过 Modem 擅自连接外网的情况、非业务异常软件的安装和运行等的审计。

电子政务网络系统层安全主要考虑采用漏洞扫描技术和补丁分发系统，对系统中的漏洞进行定期的检测和及时的修补。采用操作系统和数据库安全加固等技术对关键业务主机(如门户系统、电子邮件系统、数据库系统)实现系统层的加固保护。

电子政务网络应用层安全考虑的重点主要是邮件系统和主机防病毒。采用设置防病毒网关和配置网络防病毒软件相结合的方式，及时将病毒清除或者阻断。整个电子政务网络病毒防治体系应统一策略管理、统一病毒特征码升级，形成一个统一的整体。实现基于 CA 和 VPN 技术的身份认证和集中授权管理以及访问控制、设置审计系统对安全事件进行记录和分析、提供数据加密和密钥安全管理的服务、通过安全认证实现电子政务网中的业务应用系统与因特网之间的安全数据交换。

4 电子政务网络安全防护体系结构

根据电子政务网络安全防护体系的安全策略，按照安全域划分和保护等级，采用上述网络安全防护技术构建出电子政务网络安全防护体系结构如图1所示。

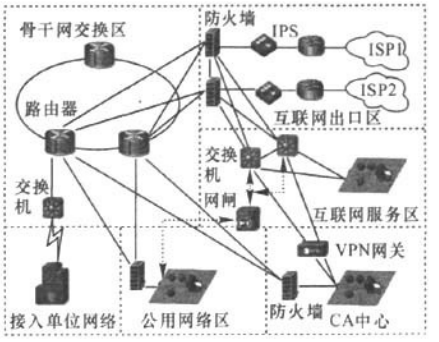

图1 电子政务网络安全防护体系结构

图1的电子政务网络划分为6个安全域，域间根据不同安全级别通过网闸、防火墙或 vlan 技术隔离。其中公用网络区是安全级别最高的安全域，承载着政务网的公共数据，通过网闸与互联网物理隔离，区域内部部署抗拒绝服务攻击系统、网络入侵检测系统、防病毒系统、主机加固系统、主页防篡改系统、漏洞扫描系统和补丁分发系统等来保护信息安全；互联网服务区承载着政府部门对外公开业务，通过防火墙和入侵防御系统与互联网逻辑隔离；同时对政务网内部接入终端 PC 应用终端准入系统，从内部防范入侵行为。

从业务需求的角度看，同一系统内的数据交换通过 VPN 技术实现，保证了部门内部数据的安全性和私密性；部门间的数据交换通过公用网络区互访；电子政务网移动用户通过 VPN 网关和安全认证网关访问内部网；电子政务网内部用户受控访问互联网；互联网用户仅能访问互联网服务区。

电子政务网络安全防护体系结构体现了安全域划分和安全等级保护的思想，考虑到了不同部门的内部业务需求，其中部署的一系列安全产品正是网络安全技术在应用上的体现，有效地起到了保护电子政务信息安全的作用，能够更好地实现网络安全，推动国家电子政务的快速发展。

(责任编辑：邓大玉)