政务网络安全隐患分析及解决措施探究

宋洪涛
（宁夏回族自治区科学技术发展战略和信息研究所，宁夏 银川 750011）

摘要：伴随着互联网技术的发展，电子政务已经成为方便广大人民群众的重要政务开展模式。电子政务在方便政务处理工作的同时，也带来了网络安全问题。政务系统中有大量的档案信息，政务系统的正常运行对于整个政府部门工作开展具有重要影响。本文将以政务网络安全相关内容介绍为切入点，通过对各种网络安全问题的分析，探索出较为理想的网络安全解决方案，旨在改善网络安全问题，保证电子政务网络运行质量。

关键词：网络安全；政府机构；电子政务；政务网络

党和政府出台了多项文件推动网络安全工作的发展，《中华人民共和国网络安全法》是一项针对网络安全的专门性法律文件，对于我国建立网络安全系统、应对网络安全挑战都具有重要意义。政务网站是一个标准化、开放化的政务处理平台，提供线上政务处理服务。线上政务处理与线下政务服务相互补充，为人民群众提供了更优质、更便捷的政府服务，更有助于政府部门为人民服务。在互联网时代，政务网站的重要性越来越突出，但与此同时，电子政务网络也存在着非法入侵、信息泄露等网络安全隐患，直接影响了政务网络效能的发挥。因此，做好政务网络安全隐患分析工作，维护好政务网络安全非常重要。

一、电子政务网络安全问题

政务网络安全问题主要有五种表现，分别是非授权访问、数据丢失或者泄露、破坏信息完整度、拒接服务攻击、传播病毒。其一，非授权访问，指未得到进网许可就对网络访问。非法入侵者护着借用其他身份，或者破坏网络许可通道对网络非法入侵，窃取信息或破坏网络；其二，数据丢失或者泄露。数据丢失或者泄露分为内外因两种，内因是由于网络管理系统内部疏忽导致网络软硬件丢失、受损，进而导致信息丢失和泄露，外因是黑客非法窃取信息导致信息丢失或泄露。数据丢失和泄露严重影响政府工作。其三，破坏信息完整度。黑客非法入侵网络系统，并对系统内部数据进行破坏，使得信息不完整。其四，拒接服务攻击。拒接服务通常是由计算机病毒导致，影响计算机系统的正常作业，使得系统响应速度变慢甚至导致系统瘫痪，无法开展正常的服务。其五，传播病毒。计算机病毒是影响网络安全的最主要的因素，通过不断自我复制破坏单机系统，影响网络正常使用。

《网络安全法》中明确指出了国家实行网络安全等级保护制度，也就是根据网络的重要性实施不同等级的保护制度，最大限度上确保网络安全，以免网络受到干扰、破坏或者非法访问。政务网络较为特殊，与社会稳定、政府建设、公共服务密切相关，对于网络安全、信息保密的需求级别较高，因此网络安全保护工作尤为重要，必须采用较高等级的网络安全保护工作，以免出现数据泄露、网络瘫痪问题，造成不可估量的损失。

互联网最显著的优势在于其具有较为突出的开放性与自由性，因此，很容易在使用过程中发生安全隐患，进而导致电子政务网络安全问题不断发生。网络安全严重影响了电子政务建设工作，因此，政务网络安全分析工作便刻不容缓。

一旦政府电子政务网遭受到以上攻击，将导致以下几种情况：其一，物理层的网络装置和环境被破坏，使得网络系统不能正常运行；其二， 黑客入侵网络系统擅自修改和删除所有的信息；其三，利用网络系统的脆弱性，对系统进行拒绝服务攻击和恶意攻击，从而降低网络系统的服务及时性；其四，政府对外沟通的窗口被破坏，政务信息的安全性也面临着严重的风险。

基于网络安全层面来分析，电子政务网络安全需求主要表现在三点上，分别是网络运行安全、网络信息安全和管理控制安全。其中，网络运行安全是指网络的运行环境安全；网络信息安全是指维护信息不被窃取、破坏，主要通过控制信息访问权限来实现，维护信息的可用性；管理控制指做好网络访问控制、病毒检测、网络监控、制定较为完善的网络管理制度，有效保证整个网络的安全运行。

二、政务网络安全隐患解决措施

电子政务网络安全应根据信息系统的安全保护等级展开网络安全保护工作，以确保政务系统具有基本的安全保护能力，各电子政务网络对于政务安全的等级要求也不同，基本安全需求主要通过基本技术安全、基本管理安全两方面来实现，包括物理安全、网络安全、主机安全、应用安全和数据安全四个层次，主要解决措施是通过改善网络的软硬件运行环境，进而保证网络的安全运行功能。政务网络安全维护工作涉及政务网络运行中的各个主体，通过对各角色进行控制，从制度、规范、流程、政策等方面去实现。

（一）强化物理层的防范能力

技术人员严格把控网络授权，科学管理内外网用户，有效防范非授权访问，进而保护网络系统内部重要信息不被窃取和破坏。网络访问授权可以有效防范外部服务攻击，从源头防范危险。除了网络访问授权工作，还需要从设置登录密码、展开登录验证等用户身份管理方面确保网络运行安全，以优化网络服务。重点加强对交换机、服务器、路由器、网络机柜和基础线路保护，为网络信息安全建立第一道保护屏障。

（二）完善网络病毒防御工作

当前，网络病毒的危害日益凸显，网络病毒扩散对政府信息系统的安全构成了严重的威胁。因此，要加强病毒防御工作，基于电子政务网络的特点财务针对性的病毒防范措施，设置更为系统完整的病毒防御体系。较为常见的病毒防御技术主要表现为三种：其一，病毒防御技术，病毒防御软件在网络系统内部长期保存，对系统内存进行优先控制，全面监控系统，及时清理异常程序，以免病毒入侵。常用的病毒防御技术有加密可执行程序、引导区保护、安装防病毒卡等；其二，检测病毒技术，病毒检测是从计算机病毒分析、判断入手，找到病毒类型，为后续病毒消杀工作奠定技术基础。病毒检测技术常用的有自身校验、关键字校验两种；其三，杀毒技术。杀毒技术通过分析病毒代码，采用有效、针对性的病毒清除程序和文件恢复制度。因为病毒在不断升级，因此病毒防御技术也需要不断更新，政府部门应当定期对病毒防御系统进行更新与升级。

（三）网络访问控制及隔离

当连接公共网络或者其他网络时，必须实施物理隔离。在进

行网络设计的时候，政府机构要根据安全要求和实际使用情况，合理地分配系统子网，从而有效地减少网络的安全风险。

1. 安全物理隔离。由于电子政务网的特性比较特殊，所以不推荐将其直接接入到公共网络中。由于与公共网络相连存在着很大的安全隐患，因此，在接入政务网的时候，必须将内网和外网进行物理隔离，并在内网中安装一张物理隔离卡，以减少公网使用者对内网信息的攻击。

2.VirtualPrivate Network。VPN 也就是虚拟私有网络，它是一个临时的，安全的连接，是一条穿过混乱的公共网络的安全、稳定的通道。利用该系统，可以使远距离用户与政府局域网进行可靠、安全的联接，实现信息的安全传递。

3. 设置防火墙（firefox）。设置防火墙是一种比较常见的物理隔离技术，防火墙具有良好的隔离效果，而且经济、安全。利用防火墙，将内外部网络访问进行控制与隔离，对可能存在风险的外部访问进行限制和拒接，可双向或者单向控制，有效地管控网络流量与时间。另外，防火墙具有网络地址变换功能，也能够实现对内部网机构的有效遮蔽，从而可以很好地解决合法 IP 不足的问题。

对于部门局域网安全维护工作，可通过身份鉴别、数据分级授权和用户权限分级三种途径来实现，通过有效的部门网络管理制度，将部门局域网内外部用户身份进行却分，进而做好访问权限控制。做好网络入侵管理，通过监测网络状态，有效防范外部的网络攻击，最大程度上保证计算机操作系统和应用系统的安全。

（四）动态链接链路层的风险防范

政府部门应该按照国家相关规定，在已有的网络之外，设立专用的网络，使用密码、身份验证等技术来保证数据的安全。同时，政府机构要做好信息传输的加密工作，要使用 IPsec 和其他加密方法，对数据传输过程进行有效的保护，这样才能有效地防止数据在传输过程中被篡改。

信息隐藏技术网络安全技术中常用的数据保密技术之一，通过信息认证、控制访问来阻止非法用户的入侵，进而有效保证用户的网络安全。将信息隐藏到所传信息的后面，以保证非法入侵者不能识别信息，进而也就无法实现信息窃取。

网络最基本的功能在于两方面，其一是处理信息，其二是传输信息。为了达到信息保密的目标，常常需要对传输过程中的信息进行加密。当前我国常用的信息加密技术主要分为两种形式，其一线路加密，也即根据网络传输线路的不同设计不同的加密技术，以实现信息的识别和保护。但是这一技术很容易忽视信号源，这是线路加密技术的一个弊端；其二是端对端的数据加密，也就是在发送端对信息进行加密，以不可识别的状态将信息上传至互联网上，之后在信息接收端对信息进行解析，有效方式信息在传输过程中被窃取。

（五）做好身份验证工作

身份验证技术可以有效地验证用户的身份，防止未经授权的用户进入。因为网络系统中大部分的身份认证都是以静态口令为主导的，所以它也存在着一些问题，具体表现为：①易破解：用户一般都会选择一些常见的单词来作为密码，这样就很容易被破译工具所破解。②口令外泄：由于人员流动比较频繁，有可能发生口令外泄，或者同一个口令被重复使用；③黑客可能通过电话、网络等方式对用户的口令进行拦截，从而很容易得到用户的关键资料；④单位内部人员在取得了合法的权限后，未能根据相关的规范来使用权限。

通过对关键程序、重要部门的访问用户进行身份验证，能够有效组织越权访问和非法访问。动态口令是常用的身份验证方法，能够精准识别访问者的身份信息。动态密码认证系统由认证服务器、备份服务器和管理工作站三部分组成。其中，认证服务器是整个身份认证系统的核心，其在政务网机房中，与服务器连接，全面控制用户网络访问情况，对访问者身份信息进行认证，身份认证之后给予网络访问者相应的权限。通常而言，认证服务器包括加密算法软件，实时运算，认证管理等几个方面，这种服务器具有很好的数据安全性，会加密和存储所有的数据，并且在进行数据交换时，通过加密的形式进行数据的传输。管理工作站则主要负责认证服务器管理界面供给工作，会在认证服务器与网络管理员间设置操作界面，便于管理人员进行用户管理与系统维护等一系列工作。

（六）制定完善的网络安全管理制度

网络系统安全管理制度的建设是政务网络安全工作的核心，一方面，政府部门应当根据本区域和本部门的网络建设实际需求建立相应的安全管理机制，充分利用网络技术，科学地把安全管理规范应用到信息化建设工作中，以规范化的管理制度促进政府部门的信息化建设，持续提升政务网络技术水平。需要引进更新更高效的反威胁设备和技术，从上网行为管理设备、流量控制设备，至服务器群的 WEB 应用防火墙、漏洞扫描、下一代防火墙，以及网络杀毒软件、关键服务器区的网闸设备、堡垒机等方面着手，打造多道屏障维护网络信息安全。部署网络安全态势感知平台，实现事前预警、事中防控、事后审计。另一方面，要对过去政务网络安全问题进行总结分析，分析政务网络突发事件，制订出一套具有高度可行性的应急方案，并建立相应的应急机制，尽可能地降低网络突发事件所带来的不利影响，为电子政务网络的运行提供保证。

三、结语

通过以上分析，我们可以清楚地认识到政府信息系统的重要性，在电子政务的重要性日益突出的背景下，我们需要把网络信息安全作为工作的头等大事来抓。在本文中，我们分析了政务网络可能发生的安全隐患问题，提出各政府机构要加强对电子政务网络的重视。网络信息安全不仅仅要依靠网络信息管理工作人员，也不是部署了安全设备就可以高枕无忧，而是需要让每一个网络使用者参与其中，充分利用网络安全设备，提高安全意识，增强安全防护技术知识的学习，协同推进政务网络信息安全建设，实现理想化电子政务网络安全防护模式，建立一个安全、稳定的网络环境，确保政务网络价值在政府机构工作中得到更好地发挥。

参考文献：

[1] 龙钰 . 军用计算机网络面临的安全隐患和解决措施探析 [J]. 中国新通信，2020，22（13）：129.

[2] 王懿嘉 . 新形势下计算机通信网络安全隐患及其对策探讨 [J]. 科技创新导报，2020，17（17）：132-133.

[3] 付成海 . “互联网 +”背景下计算机网络安全隐患及管理措施 [J]. 山东工业技术，2019（03）：143.

[4] 张振华 . 浅析计算机网络安全的主要隐患及管理措施 [J]. 科技风，2018（25）：91.

[5] 王然然 . 论云计算下的网络安全及措施 [J]. 电子技术与软件工程，2018（01）：224-225.