现代计算机技术与应用
2022 年 2 月第 4 卷第 1 期

浅析电子政务信息安全的技术防范

田　倩

广西职业技术学院，南宁

摘　要 | 电子政务信息安全性是电子政务系统最重要的防范策略。其实质是指由计算机系统作为国家政务的载体和工具而引发的信息安全问题。本文针对电子政务信息安全系统防范中所面临的主要威胁进行阐述，并依据此提出了电子信息安全的技术防范措施以供读者参考。

关键词 | 电子政务信息；威胁；技术防范

1　电子政务信息安全的威胁

随着网络的不断发展扩大，电子政务系统内容的不断增多，电子政务信息安全存在的威胁也在相对的增多。威胁主要来自系统安全、网络侵权、信息污染这几个方面。

1.1　系统的安全威胁

我国电子政务的网络系统本身网络防范能力较差，高端技术大多是购买国外开发的软件产品，没有一定的网络维护措施及网络平台更新的防范。开放的电子

作者简介：田倩，广西职业技术学院，计算机应用技术专业。
文章引用：田倩．浅析电子政务信息安全的技术防范［J］．现代计算机技术与应用，2022，4（1）：29–34.
https://doi.org/10.35534/mcta.0401005c

政务虽为政府与社会之间提供了互动的平台，但网络的威胁同样是波及政务信息的完整性与开放性的重大举措。致使政府的电子系统的安全直接受到影响。

（1）电子政务系统的漏洞

由于我国的电子政务系统的软件操作系统及程序的编制等来自于国外的软件开发的购买，针对软件在使用过程中的漏洞及缺陷的补救措施不明确，为攻击者利用。

（2）病毒及黑客的传播与攻击网上的病毒无处不在

由于系统自身的软弱性导致病毒泛滥成灾成为一大趋势，网上病毒泛滥成灾，熊猫烧香、魅影、金猪病毒、百度和 google 被黑等事件接二连三发生，加之网络系统本身的脆弱性，导致电子政务系统随时面临病毒感染破坏的威胁。据金山毒霸反病毒监测中心公布的资料显示，2007 年新增各类病毒 4.5 万种，累计感染的机器近 3600 万台，这一趋势仍在不断增长。网络黑客的恶意攻击，通过电子政务系统的薄弱环节随意进入，并对网站内部设置进行篡改与毁坏，导致政府系统内部的混乱。若得不到及时的处置，这将严重影响到政府的形象与日常的工作秩序。

1.2 网络侵权威胁

政府通过电子政务系统的传播，及时的了解社会大众对于政府的需求，并保证了政府政绩的透明化。但同时由于一些隐藏的电子机密信息等需保护的给网络保护带来了挑战。概括来看，电子政务所面临的网络侵权现象主要表现在：

（1）传统文学作品的数字化侵权

网络上共享传统形式作品的前提就是将该作品进行数字化，并将数字化后的作品上载到网络传播。将传统作品数字化并进行网络传播是属于作者的著作权。但一些信息的提供者为吸引访问群体的浏览量，随意刊载文学艺术作品，严重侵犯作者或出版社的权益。

（2）网络链接所造成的侵权

网络链接可快速从一个网站或网页连通到其他网站或网页，拓宽了信息共享的地域，节省了用户的查寻时间。但是，由于网络链接代表着网络信息的资

源来源，一些网站投机取巧进行网站的入口屏蔽等散发一些不法信息，影响网站的运营。

1.3 信息污染威胁

（1）虚假有害信息有增无减

由于网络的自由开放性，为一些不法分子提供了“温床”。不法分子为了谋取自身利益或其他目的，垃圾信息及虚假信息的捏造，制造混乱，危害社会稳定。

（2）黄色信息及过时信息的存在

网络的信息存在较大的时效性。信息资源的利用，在一定的时间内具有影响力及宣传力。网络的自由开放导致了网络信息的多样性。一些随意的转载、抄袭等成为网络的定势。导致一些资源大量的重复，占据大量的空间和信息的运作。信息的冗余性影响网站的更新与及时维护。

2 电子政务信息安全的防范技术

电子政务信息安全技术主要包括操作安全技术和密码保护技术。针对涉及到核心的信息的网络层面时这些技术对于拦挡一些垃圾信息及不安全的文件等起着重要的作用。且其应用技术主要包括：防火墙、VPN、SSL、线路加密、安全网关和网络安全监测；系统层则包括操作系统安全、数据库系统安全以及安全的传输协议；应用层安全技术主要涉及认证与访问控制、数据或文件加密和 PKI 技术。一般来说，实现网络信息安全主要是通过加密手段的繁杂、身份鉴别、密钥保护机制、安全鉴别机制 IC 卡、PCMCIAPC 卡等方式实施政务保护。另外保护系统安全的技术有网络隔离技术、访问控制技术、监控审计技术、安全评估技术等。

2.1 防火墙软件的升级

网络区域的不同直接影响着防火墙的可使用性。从网络安全性出发，网络的不同区域在设有防火墙保护的同时，进行网络各区域的相容性。在各网络区

https://doi.org/10.35534/mcta.0401005c

域的相交区一并设立防火墙技术。实施全面的软件升级。可以允许特定的用户进行网站间走动，并将不允许的用户排除，保证软件的自我维护能力和自我识别能力的有效实施。并使其达到保护高安全等级的子网、阻止外部攻击、限制入侵蔓延等目的。防火墙的弱点主要是无法防止来自防火墙内部的攻击。因此，把好网络外延的安全第一关。

2.2 内外网的隔离性的提高

我国的电子政务网络基本架构大致可分为三个部分：政务内网、政务专网和政务外网。政务内网是政务机关内部的共享的一些网络平台。如各个政务机关一样，电子政务机关内部所属于各个部门的管束也不同。其内部各有分工，进行物理隔离划分。政务专网是针对政务机密等一些机密的信息，维护政务信息的保密性专门针对政务机关的有关安全规划和要求，初步建立了由网络安全防护系统、安全管理平台、CA 系统组成的安全保障体系，实现了政务外网分级防护，为各部门业务应用提供了安全保障。政务外网与国际互联网实行逻辑隔离，为各接入部门提供了跨部门、跨地区的网络服务和互联网出口服务，通过 VPN 等技术手段，为有特殊需要的部门开通了虚拟专网服务和移动接入服务。

2.3 加强密码技术

密码技术是信息交换安全的基础，通过数据加密、数字签名及密钥交换等技术实现了数据机密性、数据完整性、不可否认性和用户身份真实性等安全机制，从而保证网络环境中信息传输和交换的安全。密码技术可以分为三类：对称密码算法、非对称密码算法和单向散列函数。在对称密码算法中，使用单一密钥来加密和解密数据。典型的对称密码算法是 DES、IDEA 和 RC 算法。这类算法的特点是计算量小、加密效率高。但加解密双方必须对所用的密钥保守秘密，为保障较高的安全性，需要经常更换密钥。因此，密钥的分发与管理是其最薄弱且风险最大的环节。在非对称密码算法中，使用两个密钥（公钥和私钥）来加密和解密数据。当两个用户进行加密通信时，发送方使用接收方的公钥加密所发送的数据；接收方则使用自己的私钥来解密所接收的数据。由于私钥不

在网上传送，比较容易解决密钥管理问题，消除了在网上交换密钥所带来的安全隐患，所以特别适合在分布式系统中应用。

2.4 网络设备配置监测

网络的更新及垃圾的及时处理等都会影峡谷网络的时效性。根据网络维护设备的配置，实施一定的网络监督，通过定期的对网络进行网络体检，可以帮助软件维护人员及时的找到病毒所在，是否被恶意的篡改及修改。SiteView 网络设备配置在正常的情况下，网络设备投入使用后是不会被改变的，除非网络改造或升级。所以正常情况下的配置改变很可能是黑客攻击造成的，及时发现对抵挡黑客进攻很有帮助。

2.5 网络维护管家

通过日常的网络测试及网络维护等时效性的操作和宣传，保证网络的优化与创新，是网络及时注入新型信息，并保证网络信息的安全性。实施网页的自动备份和恢复功能，根据病毒的侵犯具有自动的修复和完善功能。

3 结语

电子政务信息的安全不仅影响着政府办公的有效性，而且对于整个社会的融合与稳定有一定的保证作用 . 电子政务大多带有政务信息的保密性，关系到政府机构内部的机密性文件等都具有保密色彩。因此，有效地管理电子政务，提高我国的技术实施水平，保障电子政务信息的安全至关重要。

参考文献

[1] 王淼．电子政务系统安全域划分与等级保护方法的研究与应用 [D]．广东工业大学硕士学位论文（工学硕士），2010.

[2] 姚国章，吴倚天．中国电子政务案例 [M]．北京：北京大学出版社，2007.

[3] 杨兴凯．电子政务 [M]．大连：东北财经大学出版社，2010.

https://doi.org/10.35534/mcta.0401005c

Analysis of Electronic Government Information Security Technology Prevention

Tian Qian

Guangxi Vocational and Technical College, Nanning

Abstract: E-government information security is the most important defense strategy of e-government system. Its essence refers to the information security problem caused by the computer system as the carrier and tool of national government affairs. This paper expounds the main threats faced by the e-government information security system, and puts forward the technical measures of electronic information security for readers' reference.

Key words: E-government information; Threats; Technology to prevent