海洋电子政务外网安全管理实践

韩　伟，刘　丰

（国家海洋信息中心　天津　300171）

摘　　要：结合国家海洋局电子政务外网实际情况，分析了该网络存在的安全隐患以及面临的主要问题，从管理、技术两方面，介绍了海洋电子政务外网安全管理应采取的主要措施。最后，为进一步加强国家海洋局外网安全管理提出工作建议。

关　键　词：电子政务；网络系统；安全管理；实践

随着“一窗式”政府的推行，以及国家电子政务工程的全面开展，利用网络技术实现各政府职能部门的互联，开展各类业务，已经成为时代趋势。海洋电子政务外网（以下简称“外网”）是国家海洋局发布政府公开信息的网络平台，为公众参与政府决策提供便捷渠道，同时提供数据资源共享、邮件服务以及其他网络服务。

近年来，国家对海洋重视程度不断提高，海洋划界和维权等敏感内容被境外组织广泛关注。海洋安全是当前和今后长时期内国家安全的重心，海洋网络信息安全则是海洋安全工作中的重中之重。因此，必须提高网络安全意识，建立完备的网络安全管理体系，完善网络安全管理制度，掌握最新的网络安全管理技术，部署网络安全保障设备，确保外网高效、稳定、安全地运行，避免发生泄密事件和信息安全事故发生。

1　海洋电子政务外网安全面临的主要问题

“凡事预则立，不预则废”。做好外网安全管理的前提是对安全威胁和面临的问题有充分的认识和预见性[1]。随着外网在带来各种便利的同时，也带来很多新的安全问题，主要存在以下几方面。

1.1　操作人员安全意识淡薄

个别人员安全意识淡薄，保密意识不强，在上网计算机上处理、储存或传输涉密文件，或存在一些无意的行为。如，不设置或者丢失口令、非法操作、资源访问控制不合理以及疏忽大意允许未授权的计算机接入外网等，都会对网络系统造成极大的破坏。

1.2　计算机病毒防范手段不强

计算机病毒呈多元化发展趋势，以网络为主要传播途径，主要危害是：破坏信息，盗取信息，篡改信息；占用计算机系统资源，影响运行速度；在网络内快速蔓延扩散，造成大部分计算机瘫痪；占用大量网络带宽，阻塞流量，形成拒绝服务攻击。彻底避免计算机感染病毒是不可能的，但要尽量减少病毒暴发造成的损失和提高恢复时延是完全可能的[2]。

1.3　网络安全核心技术的自主性缺乏

网络基础设施中的核心技术自主性不强，CPU、操作系统以及高端网络设备多数靠国外引进。因此，造成网络系统存在被攻击的潜在危险。如使用国外的技术或产品，其漏洞不可控，使网络和系统更易受到攻击，致使敏感信息泄露、系统停运等重大安全事件多发，安全状况堪忧。

1.4　黑客攻击威胁不断

黑客攻击是目前网络面临的最大的威胁。当前中国海洋安全形势严峻，面临着海岛归属、海域划界争议、海洋资源争端、海上通道安全和台湾问题等一系列传统安全和非传统安全的威胁与挑战，境外特务组织越发关注海洋事业的发展动向，以各种方式获取重要海洋信息，甚至是在不影响网络运行和计算机工作的情况下，伪装为合法用户进入外网，占用大量资源，

修改、窃取、破译重要敏感信息，执行破坏软件，在中间站点拦截和读取重要信息等，产生严重后果，导致个人利益和国家利益受损。

2 海洋电子政务外网安全管理应采取的主要措施

“三分技术，七分管理”，对于外网安全管理，技术手段和安全设备只是辅助手段，离开完善的管理制度，就无法发挥应有的作用，更不能建设良好的外网安全环境[1]。在外网安全管理过程中，外网安全技术措施是外网安全管理的基础，外网安全管理制度建设是外网安全的保证。

2.1 外网安全管理措施

外网安全管理贯穿整个安全体系，是安全体系的核心，代表了安全体系中人的因素。安全管理更主要的是对安全技术和安全策略的管理[3]。用户的安全意识是外网是否安全的决定因素，必须从制度上、技术上和应用上加强外网安全管理。

2.1.1 建立严格制度

制度建设是外网安全的保证，电子政务系统安全体系要真正发挥作用，还需制定安全制度并严格实施。一般意义上讲，安全制度包括人员安全管理、系统文档管理、环境安全管理、设备购置使用、系统开发管理、运维安全管理和应急情况处理等方面的内容。

2.1.2 加强网络技术的培训

网络管理员必须不断地学习新的网络知识，掌握新的网络防范技能，了解网络病毒、密码攻击、分组窃听、IP 欺骗、拒绝服务和端口攻击等多样化的攻击手段，才能更好地管理好外网。

2.1.3 加强用户的安全意识

用户安全意识及其掌握的安全知识是整个安全体系高效、有效运行和正常维护的重要因素之一。因此，应建立完善的安全教育和培训体系，以定期或不定期对各级用户进行安全相关的教育和培训，加强用户的安全意识，引导用户自觉安装防病毒软件，打补丁，自动更新操作系统补丁，不随意安装不熟悉的软件，掌握安全防范的基本技能。

2.2 外网安全技术措施

在外网安全体系中各种安全技术要合理部署，互联互动，形成一个有机的整体，将不同区域、不同层面的安全保护措施形成有机的安全保护体系，落实物理安全、网络安全、主机安全、应用安全和数据安全，具体措施如下。

2.2.1 物理安全

在建设或改造机房时期，部署消防安全系统、温湿度监控系统、门禁监控系统、漏水检测系统和 UPS 系统等，并做防雷、防盗窃和防电磁泄漏等工作部署，切实保证机房物理安全。

2.2.2 网络安全

一是对主要通信线路做到线路冗余。二是划分并隔离不同安全域。根据不同需求和威胁，划分服务器区、用户区和管理区等区域。采用访问控制、权限控制的机制，控制不同的访问者对网络和设备的访问，防止内部访问者对无权访问的区域的访问和误操作。三是在边界部署防火墙、安全审计、入侵防范安全设备，对进出外网的服务和访问进行控制、阻断和审计[4]。

2.2.3 主机安全

定期对主机进行风险评估。在服务器区部署漏洞扫描评估系统，有计划地对服务器及重要系统进行漏洞扫描，并根据评估结果，调整策略，升级补丁或是进行相关技术操作。漏洞检测的结果实际上就是主机安全性能的一个评估，它指出了哪些攻击是有害的，因此成为安全方案的一个重要组成部分。

2.2.4 应用安全

（1）在政府网站服务器上安装网页防篡改软件，防治非授权用户对页面和内容进行篡改和非法添加。网页防篡改软件关注于应用层安全问题，采用“强认证”机制，与嵌入式过滤技术、实时阻断、事件触发等多种预防性保护技术相结合，形成针对网站文件的多层次纵深防御体系，是完全保护网站不发送被篡改内容并进行自动恢复 Web 页面保护软件，切实保证政府网站信息的完整性、真实性和可用性。

（2）部署浪潮 SSR 服务器安全加固系统。

该系统使用 USB－KEY 在系统层对服务器操作系统进行安全加固，保护了系统中重要数据和应用的安全，从根本上免疫了目前各种针对操作系统的攻击行为，防止了病毒、蠕虫和黑客攻击等对操作系统和数据库的破坏，最大限度地保护了信息安全。

2.2.5 *数据安全*

采用备份和恢复技术。政府网站服务器存储了大量公开的政府信息、历史数据以及其他重要内容，尽管已经采用了很多安全措施和手段，但没有绝对的安全，所以采取备份的技术也是最基本的方法，一旦出现故障，可以及时恢复。

3　结论

结合国家海洋局电子政务外网安全管理的实践，深刻地认识到，网络系统安全体系建设是一个长期的过程，新的安全技术手段会不断出现，新的攻击手段也会层出不穷。任何一个安全设计方案都不可能解决所有安全问题。但随着网络化、信息化进程的不断推进，我们对信息系统建设中的网络安全问题的认识会在理论、技术实践和管理实践等方面不断地深化，将根据国家信息安全等级保护建设要求，结合海洋电子政务系统实际进行设计，实现安全思路清晰、安全体系全面、安全重点突出，使网络安全建设既符合政府部门相关的安全保密要求，又满足海洋事业发展的需要。

参考文献

[1] 王超，林华．环保电子政务建设中网络安全管理[J]．环境保护科学，2007，33(3)．

[2] 刘峰．构建完善的电子政务系统安全体系[J]．计算机技术与发展，2008(18)．

[3] 朱亚兴．大型科技网络系统安全方案设计[J]．微型机与应用，2010(13)．

[4] 高咏欣，史科蕾．浅议网络安全管理体系的建立[J]．信息技术与信息化，2007(3)．