●王欢喜

电子政务信息安全风险分析与防范策略*

摘 要 我国电子政务信息安全风险主要存在于观念、技术、管理和法律方面。要强化电子政务环境下公务员的信息安全意识,建立电子政务信息安全管理机构,完善信息安全基础设施和扶持国有信息安全产业的发展。参考文献 13。

关键词 电子政务 信息安全 风险 策略
分类号 G350

ABSTRACT In China, information security in e-government exists mainly in idea, technological, management and legal aspects. The author recommends raising the information security awareness of public servants, establishing e-government security management mechanisms, improving information security infrastructure, and supporting the development of state-owned information security industry. 13 refs.

KEY WORDS E-government. Information security. Risk. Strategy.
CLASS NUMBER G350

1 电子政务信息安全的内涵

电子政务是政府管理方式的革命,它是运用信息以及通信技术打破行政机关的组织界限,构建一个电子化的虚拟机关,使公众摆脱传统的层层关卡以及书面审核的作业方式,并依据人们的需求、人们可以获取的方式、人们要求的时间及地点等,高效快捷地向人们提供各种不同的服务选择。政府机关之间以及政府与社会各界之间也经由各种电子化渠道进行相互沟通。电子政务的建立将使政府成为一个更符合环保精神的政府,一个更开放透明的政府,一个更有效率的政府,一个更廉洁勤政的政府[1]。然而,电子政务的职能与优势得以实现的一个根本前提是信息安全的有效保障。因为电子政务信息网络上有相当多的政府公文在流转,其中不乏重要信息,内部网络上有着大量高度机密的数据和信息,直接涉及政府的核心政务,它关系到政府部门、各大系统乃至整个国家的利益,有的甚至涉及国家安全。如果电子政务信息安全得不到保障,电子政务的便利与效率便无从保证,对国家利益将带来严重威胁。电子政务信息安全是制约电子政务建设与发展的首要问题和核心问题。

电子政务的信息安全可以理解为:

(1)从信息的层次看,包括信息的完整性(保证信息的来源、去向、内容真实无误)、保密性(保证信息不会被非法泄露扩散)、不可否认性(保证信息的发送和接收者无法否认自己所做过的操作行为)等。

(2)从网络层次看,包括可靠性(保证网络和信息系统随时可用,运行过程中不出现故障,遇意外事故能够尽量减少损失并尽早恢复正常)、可控性(保证营运者对网络和信息系统有足够的控制和管理能力)、互操作性(保证协议和系统能够互相联接)、可计算性(保证准确跟踪实体运行达到审计和识别的目的)等。

(3)从设备层次看,包括质量保证、设备备份、物理安全等。

(4)从管理层次看,包括人员可靠、规章制度完整等[2]。

2 电子政务信息安全风险分析

现阶段,我国电子政务信息安全系数比较低。公安部 1998 年 8 月在江苏、上海、广东等省(市)对 169 信息网进行检测,发现其设防能力十分脆弱,难以抵御任何方式的电子攻击[3]。电子政务信息安全风险主要存在 4 个方面。

2.1 观念方面

*本文系湖北省软科学项目"电子政务信息安全法规研究"成果之一。

著名信息安全专家、中国工程院院士沈昌祥从国家安全利益出发,提出应把信息系统安全建设提高到研制"两弹一星"的高度去认识[4]。1999 年政府上网工程启动以来,政府部门越来越重视网络系统建设,看重网络带来的便利与高效,但是有些地方对信息安全工作未引起足够重视。据估计,我国在网络工程中网络安全的投入费用不到 2 %,同国外的 10 %相比有较大差距[5]。现阶段,电子政务网络的开放程度不高,一些机密信息目前还没有上网,再加之公众对计算机犯罪的态度较为"宽容",认为并没有造成直接的人员财产损失,这都使得公务员和普通大众对信息安全问题关注不够,信息安全意识淡薄。

2.2　技术方面

(1)计算机系统本身的脆弱性,使得它无法抵御自然灾害的破坏,也难以避免偶然无意造成的危害。如:洪水、火灾、地震的破坏,系统所处环境的影响(温湿度、磁场、碰撞、污染等),硬件设备故障,突然断电或电压不稳定及各种误操作等。这些危害会损害操作系统设备,有时会丢失或破坏数据,甚至毁掉整个系统。

(2)网络本身存在缺陷。首先,软件本身缺乏安全性。操作系统的设计一般着重于提高信息处理的能力和效率,对于安全只是作为一项附带的条件加以考虑。因此,操作系统中的安全缺陷相当多。其次,通信与网络设备本身有弱点。绝大多数电子政务信息网络运行的是 TCP/ IP , NetBEUI , IPX/ SPX 等网络协议,而这些网络协议并非专为安全通讯而设计。利用这些网络进行服务,本身就可能存在多方面的威胁,加之使用者信息安全意识淡薄,管理者管理措施不力等原因,会造成一些常见的安全问题:对物理通路的干扰;网络链路传送的数据被窃听;非授权用户非法使用,信息被拦截或监听;操作系统存在的网络安全漏洞;应用平台的安全,如数据库服务器、电子邮件服务器等均存在大量的安全隐患,很容易受到病毒、黑客攻击;直接面向用户的应用系统存在的信息泄露、信息篡改、信息抵赖、信息假冒等[6]。再次,目前世界上还缺乏统一的操作系统、计算机网络系统和数据库管理系统,缺乏统一的信息安全标准、密码算法和协议,因而无法进行严格的安全确认[7]。

(3)我国具有自主知识产权的信息设备、技术、产品较少,如计算机芯片、骨干路由器和微机主板等基本上从国外进口,且对引进技术和设备缺乏必要的技术改造,尤其是在系统安全和安全协议的研究和应用方面。而美欧等发达国家对我国限制和封锁信息安全高密度产品,出口到我国的信息产品中留有安全隐患。例如,美国出口我国的计算机系统的安全系统只有 C2 级,是美国国防部规定的 8 个安全级别之中的倒数第三[8];在操作系统、数据库管理系统或应用程序中预先安置从事情报收集、受控激发破坏的"特洛伊木马"程序,一旦发生重大情况,那些隐藏在软件中的"特洛伊木马"就能够在某种秘密指令下激活,造成我国电子政务关键软件系统的瘫痪[9]。

2.3　管理方面

对现有的网络攻击和入侵事件的一项统计报告显示:国外政府入侵的安全风险指数为 21 %,黑客入侵的安全风险指数为 48 %,竞争对手入侵的安全风险指数为 72 %,组织内部不满雇员入侵的安全风险指数为 89 %[10]。这说明,电子政务信息安全不是单纯的技术问题。如果没有从管理制度、人员和技术上建立相应的电子化业务安全防范机制,缺乏行之有效的安全检查保护措施,再好的技术和设备都无法确保其信息安全。管理上的漏洞,例如,机房重地随意进出,微机或工作站管理人员在开机状态下擅离岗位,敏感信息临时存放在本地的磁盘上,这些信息处于未保护状态,都会为外部入侵,更为内部破坏埋下隐患。其中,来自内部的安全威胁可能会更大,因为内部人员了解内部的网络、主机和应用系统的结构;能够知道内部网络和系统管理员的工作规律,甚至自己就是管理员;拥有系统的一定的访问权限,可以轻易地绕过许多访问控制机制;在内部系统进行网络刺探、尝试登录、破解密码等都相对容易。如果内部人员为了报复或销毁某些记录而突然发难,在系统中植入病毒或改变某些程序设置,就有可能造成损失。内部人员的破坏活动也并不局限于破坏计算机系统,还包括越权处理公务、窃取国家机密数据等。

2.4　法律方面

黑客攻击、病毒入侵等网络犯罪的日益增多与网络信息安全法制不健全和对网络犯罪的惩治不力密不可分。一方面,我国已经出台了一系列与网络信息安全有关的法律法规,例如:《计算机软件保护条例》(1992 年)、《中华人民共和国计算机信息系统安全保护条例》(1994 年)、《警察法》(1995 年)、《公安部关于对国际联网的计算机信息系统进行备案工作的通知》(1996 年)、《中华人民共和国信息网络国际

联网管理暂行规定》(1997 年)、《计算机信息网络国际联网安全保护管理办法》(1997 年)、《商用密码管理条例》(1999 年)、《计算机信息系统国际联网保密管理规定》(2002 年)等。此外,1997 年 3 月颁布的新《刑法》第 285 条、第 286 条、第 287 条,对非法侵入计算机信息系统罪、破坏计算机信息系统罪,以及利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家机密等犯罪行为,作出了规定。尽管这些法律法规的出台和实施对于我国网络信息的安全起到相当积极的作用,但仍难以适应网络发展的需要,信息安全立法还存在相当多的盲区。

另一方面,已颁布实施的法律法规不仅规定了出入口制度和市场准入制度,确定了网络信息安全管理机构,阐明了安全责任,而且明确了法律责任,对于危害网络信息安全的个人和单位,规定了经济处罚、行政处罚和刑事处罚等三大类型。但是由于网络犯罪的隐蔽性和高科技性,给侦破和审理带来了极大困难,再加上其他原因,导致执法部门的打击力度有限,在法律的执行上还有不到位之处,一些违法情况及当事人还未得到及时处理和制裁。

3 电子政务信息安全的防范策略

3.1 强化电子政务环境下公务员的信息安全意识

所谓的信息安全意识,是指公务员对电子政务中信息安全问题主要表现与危害以及保证政府信息安全的意义的正确认识,发现电子政务中影响信息安全的现象和行为的敏锐性,维护电子政务信息安全的主动性[11]。强化公务员的信息安全意识就是要让公务员认识到电子政务信息安全是电子政务正常而高效运转的基础,是保障国家信息安全甚至国家安全的重要前提,从而牢固树立信息安全第一的思想。我国各级政府部门要利用多种途径对公务员进行电子政务信息安全方面的教育。一是通过大众传播媒介,增强公务员信息安全意识,普及信息安全知识。二是积极组织各种专题讲座和培训班,培养信息安全人才,并确保防范手段和技术措施的先进性和主动性。三是要积极开展安全策略研究,明确安全责任,增强公务员的责任心。

3.2 建立电子政务信息安全管理机构

首先,政府部门要严格按照《中华人民共和国计算机信息系统安全保护条例》和《计算机信息网络安全保护管理办法》的规定,在国家安全部,国家保密局,国务院有关部门及各省、市、自治区公安厅(局),地(市)、县(市)公安局负责计算机网络信息系统安全保护的行政管理下,建立本单位、本部门、本系统的组织领导管理机构,明确领导及工作人员责任,制定管理岗位责任制及有关措施,严格内部安全管理机制,并对破坏电子政务信息安全的事件进行调查和处理,确保网络信息的安全[12]。

其次,要完善"网上警察"队伍建设,加大监视和打击网络犯罪活动的力度。我国于 1983 年成立了公安部计算机管理和监察局,1985 年全国人大通过了《警察法》,其目的就是"监督计算机信息系统安全保护工作"。1998 年又成立了公安部公共信息网络安全监察局,并逐步形成了一支"网上警察"。当前,公安部门的首要任务是吸纳高级信息安全人才充实到网上警察队伍,提高网上警察的快速反应能力、侦察与追踪水平等。

3.3 完善我国信息安全基础设施

当前迫切需要建立的国家信息安全基础设施包括:国际出入口监控中心、安全产品评测认证中心、病毒检测和防治中心、关键网络系统灾难恢复中心、系统攻击和反攻击中心、电子保密标签监管中心、网络安全紧急处置中心、电子交易证书授权中心、密钥恢复监管中心、公钥基础设施与监管中心、信息战防御研究中心等[13]。

3.4 倾力扶持国有信息安全产业的发展

自主的信息产业或信息产品国产化是保证电子政务信息安全的根本。信息安全技术、产品受制于他国是对国家安全利益的极大威胁。国家应对国有信息安全产业的发展予以充分的政策和财政支持。当前,应在以下 3 种技术上求得突破:一是能逐步改善信息安全状况、带有普遍性的关键技术,如密码技术、鉴别技术、病毒防御技术、入侵检测技术等;二是创新性强、可发挥杠杆作用的突破性技术,如网络侦察技术、信息监测技术、风险管理技术、测试评估技术和 TEMPEST 技术等;三是能形成"撒手锏"的战略性技术,如操作系统、密码专用芯片和安全处理器等。还要狠抓技术及系统的综合集成,以确保电子政务信息系统的安全可靠。令人可喜的是,2002 年 8 月 19 日由我国自主开发的高性能通用芯片"龙芯 1"运行成功,这是我国信息安全产业发展史上具有里程碑意义的事件。

3.5 健全法律,严格执法

(下转第 73 页)

成英文并与外国出版商联合出版一种中国图书馆学与信息科学期刊,并同时在网上出版发行其电子版。(5)鉴于 ISI 在选刊过程中也受理机构、专家推荐或刊物自荐期刊,中国图书馆学会、中国情报学会可主动与 ISI 联系,向 ISI 推荐我国图书馆学、情报学刊物,主动征询意见,加强与 ISI 的沟通;目前办刊质量高的刊物如《中国图书馆学报》、《图书情报工作》、《情报学报》等可向 ISI 自荐其刊物,以供选用。(6)加强对外发行力度,可考虑组织若干家期刊社联合寻求国外代理发行商,以扩大期刊的国外发行量,提高国际显示度,扩大影响。

但愿中国图书馆学、情报学界树立走向世界的信心,努力创造条件,把握机遇,为中国更多社会科学期刊走向世界先行一步,带个好头,为加强中国社会科学与国外的学术交流,提高中国社会科学的国际学术地位和影响作出新的贡献。

参考文献

1 金碧辉,汪寿阳. SCI 期刊等级区域的划分及其中国论文的分布. 科研管理,1999,20(2)
2 赵基明主编. SCI 收录期刊信息大全. 北京:中央文献出版社,2000
3 师昌绪,田中卓等. 科学引文索引(SCI) ——国际上评定科研成果的一种方法. 科学通报,1997,42(8)
4 邹承鲁. 中国科技期刊的国际化. 科学时报,1998-05-18
5 张广学,王春光. 为我国学术期刊早日实现国际化而奋斗. 中国科技期刊研究,1999,10(4)
6 任胜利,王宝庆等. 中国科技期刊及论文在 SCI 中的国际地位分析及对策. 科学通报,1997(21)
7 汪寿阳,金碧辉. SCI、SSCI 与管理科学期刊. 管理科学学报,2000,3(4)
8 马费成. CSSCI 与社会科学评价. 南京大学学报,2000,37(4)
9 http://www.isinet.com/isi/journals/index.html
10 http://www.jcrweb.com
11 Jin BH, Wang B. Chinese science citation database: Its construction and application. SCIENTOMETRICS, 1999, 45(2)
12 乔文明,索大武. 利用 CSSCI 从引文分析角度对我国图书馆学情报学期刊进行综合评价. 图书情报工作,2002(11)
13 http://www.las.ac.cn

赵基明 武汉大学图书馆副研究馆员。通讯地址:湖北省武汉市。邮编 430072。
(来稿时间:2002-12-25)

(上接第 51 页)

法律是保障电子政务信息安全的最有力手段,发达国家已经在政府信息安全立法方面积累了成功经验,如美国的《情报自由法》和《阳光下的政府法》、英国的《官方信息保护法》、俄罗斯的《联邦信息、信息化和信息保护法》等。我国立法部门应加快立法进程,吸取和借鉴国外网络信息安全立法的先进经验,尽快制定和颁布个人隐私保护法、数据库振兴法、信息网络安全性法规、预防和打击计算机犯罪法规、数字签名认证法、电子凭证(票据)法、网上知识产权法等,以完善我国的网络信息安全法律体系,使电子政务信息安全管理走上法制化轨道。另外,执法部门还要进一步严格执法,提高执法水平,确保各项法律法规落到实处。对于各种违法犯罪情况要严加追究,绝不姑息,对于各种隐患要及时加以预防和制止。

参考文献

1 黄志澄. 电子政务的内涵及发展. 中国信息导报,2002(4)
2 杨义先,林晓东,邢育森. 信息安全综论. 电信科学,1997(12)
3,5,7, 冯杰,李会欣. 我国电子政府安全运行分析. 新视野,2002(5)
4,8 崔丽,沈昌祥. 国家安全概念:对信息系统的安全应从“两弹一星”的高度去认识. 中国青年报,1999-06-18
6 尹秀莲,于跃武. 电子政务与网络信息安全. 内蒙古科技与经济,2002(2)
9,10 汤志伟. 电子政府的信息网络安全及防范对策. 电子科技大学学报(社科版),2002(1)
11 娄策群. 保障电子政府信息安全的政策选择. 情报科学,2002(5)
12 杨海平. 网络信息安全研究. 情报科学,2000(10)
13 蒋坡. 国际信息政策法律比较. 北京:法律出版社,2001

王欢喜 武汉大学信息管理学院 2001 级硕士研究生。通讯地址:武汉大学信息管理学院。邮编 430072。
(来稿时间:2002-11-11)