电子政务系统中的安全风险管理

Security Risk Management in the E – Government System

闫　强　舒华英　(北京邮电大学 经济管理学院 100876)
陈　钟　段云所　(北京大学 计算机科学技术系 100871)

摘要:电子政务的开展以信息技术为基础,如何解决电子政务系统的安全问题已成为一个迫在眉睫的课题。本文从安全风险管理的角度出发,论述了电子政务系统面临的风险,介绍了风险评估与风险消除的一般方法。

关键词:电子政务　风险管理　风险评估

1　引言

随着计算机网络技术的成熟和普及,大量政务信息的实时共享和双向交流在技术上已经成为可能。电子政务就是借助电子信息技术而进行的政务活动。其最重要的内涵是运用电子信息技术打破行政机关的组织界限,建构一个电子化的虚拟机关,使得人们可以从各种电子化渠道获取政府的信息及服务;而政府机关内部、政府机关之间及政府与社会各界之间也可以经由各种电子化渠道进行相互沟通。

然而计算机网络在迅速普及的过程中也暴露出许多问题,其中安全问题日益突出,根据 CERT 2002 年初的报告,2001 年该中心接到的计算机安全事故报告的数量达到 52,658 份,软件安全漏洞的数量达到 2,437 种,均比 2000 年翻了一倍还多。

因此,我国在大力开展电子政务的同时,加强安全忧患意识,从技术、管理各个层面强化安全防范措施,就显得尤为重要。

本文从安全风险管理的角度出发,论述了电子政务系统面临的风险,介绍了风险评估与风险消除的一般方法。

2　风险管理

电子政务系统安全风险管理的目的是保证政府组织活动的正常运转,而非仅仅保证其中的 IT 资产的安全。因此风险管理不仅仅是技术人员的任务,也是组织管理者的任务。

风险管理的一个基本前提假设是:信息系统不可能是百分之百的安全[1]。由于任何组织能够用于信息系统安全保护的资源都是有限的,理性的组织管理者必须权衡用于保护其信息系统的各项措施的代价与由此获得的安全收益。将安全风险降低到可以接受的程度是每一个组织采用各种安全措施的目的。实际上,所有安全相关的活动都可以看作是风险管理过程的一部分。风险管理贯穿于整个系统开发生命周期[2],其过程可以分为风险评估及风险消除两个部分。风险管理通过度量风险以及选择经济有效的安全控制来增进系统的安全性。

风险管理过程涉及以下七个要素[1,3]:

(1) 资产(Assets):即要保护的对象是什么?

(2) 威胁(Threats):针对什么威胁来提供保护以及威胁发生的可能性是什么?

(3) 脆弱性(Vulnerability):在安全过程、技术控制、物理控制以及其他控制方面存在哪些可以被威胁源所利用的不足?

(4) 影响(Impacts):威胁发生的直接影响是什么(如信息泄密、被篡改)?

(5) 后果(Consequences):威胁发生的长期影响是什么(如信誉的损失)?

(6) 控制(Controls):保护资产的有效的安全措施是什么?

(7) 风险(Risk):通过实施安全控制,是否将风险降低到了可以接受的水平?

在风险管理过程中并不需要分别对上述七个方面分别进行分析,很多方面可以结合起来同时进行。

3　风险评估

风险评估是确定一个信息系统面临的风险级别的过程,是风险管理的基础。通过风险评估确定系统中的剩余风险,并判断该风险级别是否可以接受或需要实施附加措施来进一步降低风险[2]。风险取决于威胁发生的概率和相应的影响[4]。完整的风险评估过程包括系统特点分析、威胁分析、影响分析及风险级别判断四个阶段[2],如图 1 所示:

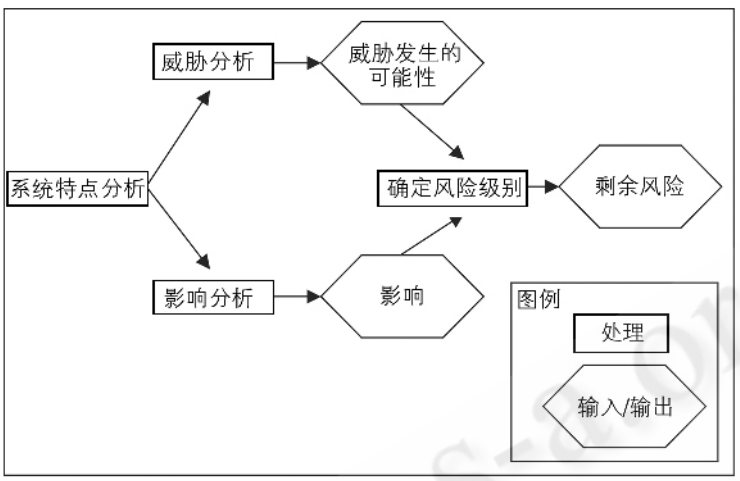

图 1　风险评估过程

3.1　电子政务系统特点分析

在风险评估过程中,系统特点分析的目的是明确风险分析的对象,标识系统边界及其所包含的资源,明确组织的任务以及信息系统在组织中的作用及影响,从而确定风险管理的主要范围,即在什么范围内、以什么样的详细程度来进行风险管理。

对电子政务系统来说,其主要包括三个组成部分:一是政府部门内部的电子化和网络化办公系统;二是政府部门之间通过计算机网络而进行的信息共享和实时通信;三是政府部门通过网络与民众之间进行的双向信息交流。

3.2　威胁分析

威胁是威胁源无意触发或有意利用系统脆弱性的潜能。正是由于系统存在各种各样的脆弱性,威胁源才构成了系统的风险。因此在风险分析过程中必须对威胁源及脆弱性进行标识和描述。

威胁源是任何可能对系统造成危害的环境或事件,包括人、自然以及环境等多种因素。系统面临的自然威胁与其地理位置有关,而来自人的威胁可能是无意的,也可能是故意的。标识系统面临的威胁时可以采用头脑风暴法(brainstorming)、德尔菲法(Delphi)、幕景分析法(Scenarios Analysis)等。表 1 列出了一些可能的威胁源[5]:

对来自人的威胁,其可能的动机如表 2:

关于脆弱性的信息可以通过场地调查、人员调查、网络扫描、穿透测试、系统及组织的相关文档分析以及其他公开的脆弱性信息源等途径获得。在脆弱性分析阶段,如果系统还处于设计阶段,则分析的重点主要在系统的安全策略、规程及安全需求的定义。如果系统已经得到实施,则分析内容还要包括设计文档等更详细的信息。如果系统处于运行阶段,则还要进一步分析系统的安全功能、安全控制的实际效果。

表 1　可能的威胁源

威胁	可能的来源
敌意的威胁	恐怖分子
	对本组织不满、心理不平衡的人
	犯罪分子
	与外敌勾结的内部人员
	黑客
非敌意的威胁	系统使用者的误操作
	系统管理者、维护者的误操作
自然威胁	地震
	火山爆发
	飓风
	洪水
	雷电
	冰雹

表 2　可能的动机

动机
获取机密或敏感数据的访问权
跟踪或监视目标系统的运行
扰乱目标的运行
窃取钱物或服务
非授权使用资源(如计算机资源、网络资源)
技术挑战
好奇

威胁分析的最终目的是确定总体的风险概率。影响风险概率的因素包括威胁源的动机、能力、系统脆弱性的性质以及有关安全措施的效力。确定风险概率是一个主观性很强的过程,关于自然威胁可能存在一定的历史数据,这些数据可以辅助分析自然威胁发生的概率,而对信息系统来说,来自人员的、技术性的、操作性的威胁往往缺乏历史信息,对这类威胁的概率的估计可以采用类比的方法,但实际上往往取决于分析者的经验。

一种简单的方法是将风险概率描述为高、中、低,如表 3:

表 3　风险概率的定义

概率	描述
高	威胁源具有很高的动机及能力,安全措施缺乏效力。
中	威胁源具有一定的动机和能力,但安全措施具有效力;或者威胁源不具备动机;或者威胁源不具备明显的能力。
低	威胁源缺乏动机和能力,安全措施能够有效阻止脆弱性被攻击。

3.3 影响分析

风险评估的下一个过程是确定威胁对组织的影响程度。威胁对组织的影响可以从以下五个安全目标的损失或降级来描述:完整性(integrity)、可用性(availability)、机密性(confidentiality)、责任性(accountability)以及保证(assurance)。下面对这五个方面的损失进行描述。

(1) 完整性损失。当系统或数据受到未授权的修改时,无论这种修改是故意的还是无意的,我们都说系统的完整性受到了损失。完整性损失和可用性损失的后果有一定的相似之处。如果完整性的损失未被及时发现,则继续使用被篡改的数据会导致进一步的损失。另外,对系统完整性的破坏可能只是破坏系统可用性、机密性的第一步,同时也会降低系统的保证。

(2) 可用性损失。系统可用性的损失会对组织的业务造成影响,系统在功能、操作性能方面的损失会导致组织在公众中的信誉降低,或导致生产时间的延迟,而且,非授权用户对资源的占用也会导致信心、责任等诸多方面的损失。

(3) 机密性损失。机密性是指保护数据不被非授权地泄露。机密性损失的影响大到危及国家安全,小到使组织陷入窘境。

(4) 责任性的损失。责任性在这里是指对非法用户行为进行跟踪的能力。责任性对抗抵赖、威慑、错误隔离、入侵检测和预防、事后恢复及法律责任追究提供支持,而责任性的损失将影响到这些功能。责任性的损失往往伴随着对完整性、机密性或可用性的破坏。

(5) 保证的损失。保证是相信上述 4 个安全目标(完整性、可用性、机密性及责任性)得到满足的基础。保证的损失意味着系统缺乏足够的保护措施来防止用户的疏忽、软件的错误以及有意的穿透及旁路。

有些影响可以定量描述,如收入的损失、系统修正、恢复的成本等,有些无形的影响则适宜于使用高、中、低等定性的描述[6]。文献[2]给出了四种定性描述,如表 4 所示:

表 4　影响程度的定义

影响	描述
严重影响	威胁导致数据或系统其他资产的不可用、被篡改、泄密、被破坏或导致系统服务能力的损失,对国家造成灾难性影响,可能导致人员伤亡。
高度影响	威胁导致数据或系统其他资产的不可用、被篡改、泄密、被破坏或导致系统服务能力的损失,导致组织功能明显退化,可能伤及人员。
中度影响	威胁导致数据或系统其他资产的不可用、被篡改、泄密、被破坏或导致系统服务能力的损失,这些损失可恢复,对组织功能产生短期重大影响,但不伤及人员。
低度影响	威胁导致数据或系统其他资产的不可用、被篡改、泄密、被破坏或导致系统服务能力的降级,对组织功能不产生严重影响,也不会伤及人员。

3.4 确定风险级别

正如前面所说,风险取决于威胁发生的概率及相应的影响。表 5 根据威胁发生的可能性和相应后果对整体风险等级进行了判断:

4 风险消除

在风险消除阶段,根据风险分析阶段的结果,对已标识的风险采用相应的措施,将风险程度降低到组织

可以接受的水平,同时保持对系统其他功能的影响最低。消除所有的风险是不可行也是不可能的,因此,风险消除的目的是采用适合于系统环境及组织任务的经济、可行的安全控制措施。

表 5 风险等级判断

影响	威胁发生的可能性		
	高	中	低
严重影响	严重	高	中
高度影响	高	中	低
中度影响	中	中	低
低度影响	低	低	低

为了消除风险,可以综合采用下面三种方法:

预防:通过消除系统脆弱性、缺陷及其被利用的可能行,排除系统威胁;

限制:实施一定的安全控制,将威胁的影响限制在一定范围内;

检测与响应:采取入侵检测措施以及响应行动来消除不利影响。

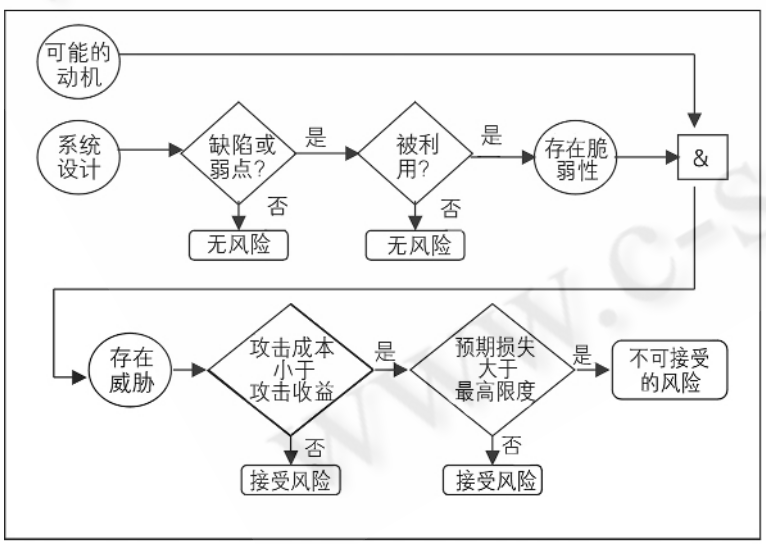

图 2 风险消除过程说明

在选择技术的或管理的解决措施时,应考虑系统及组织的目标,对那些可能造成严重影响的威胁应优先采取解决措施。图 2 说明了消除风险的几种途径:

风险消除过程可以概括如下:降低缺陷产生的可能性;降低脆弱性被利用的概率;增加攻击者成功实施攻击的代价;限制脆弱性存在和威胁发生的范围,降低损失。

5 总结

电子政务的开展以信息技术为基础,如何解决电子政务系统的安全问题已成为一个迫在眉睫的课题。本文从安全风险管理的角度出发,论述了电子政务系统面临的风险,介绍了风险评估与风险消除的一般方法。在信息技术不断发展的今天,要确保电子政务系统的安全运行,加强风险管理不失为一种有效的途径。

参考文献

1 National Institute of Standards and Technology, Technology Administration, U. S. Department of Commerce. An Introduction to Computer Security: The NIST Handbook. Draft, June 1994.

2 U. S. Department of Commerce, National Institute of Standards and Technology, Technology Administration. Risk Management Guide: Recommendations of the National Institute of Standards and Technology. Draft, June 2001.

3 Federal Information Processing Standards Publication 191. Specifications for Guideline for The Analysis Local Area Network Security. November 1994.

4 R. J. Staker. Use of Bayesian Belief Network in the Analysis of Information System Network Risk. In Proceedings of Information, Decision and Control, IDC 99. 1999, 145 – 150.

5 National Security Agency Information Assurance Solutions Technical Directors. Information Assurance Technical Framework, Release 3.0. September 2000.

6 S. P. Bennett, M. P. Kailay. An Application of Qualitative Risk Analysis to Computer Security for the Commercial Sector. In Proceedings of Eighth Annual of Computer Security Applications Conference. 1992, 64 – 73.