广西科学院学报
Journal of Guangxi Academy of Sciences
2006,22(4):367～369
Vol. 22,No. 4 November 2006

信息安全风险评估的探讨与实践

Discussion and Practice of Information Security Risk Assessment

陈友初
CHEN You-chu

(广西经济信息中心,广西南宁 530022)
(Guangxi Economic Information Center,Nanning,Guangxi,530022,China)

摘要:分析产生信息安全风险的原因,介绍了信息安全风险评估方法和评估工具,并尝试性地对广西自治区级电子政务网络平台进行安全风险评估。评估结果显示广西自治区级电子政务网络基本处于黄色预警等级,与网络信息系统的现状基本相符。

关键词:信息安全 风险评估 方法 资产 威胁 脆弱性
中图法分类号:TP393.08 **文献标识码**:A **文章编号**:1002-7378(2006)04-0367-03

Abstract: The causes for the information security risks are discussed. The methods and tools which are used to assess information security risk are introduced. The risk of the provincial electronic government affair network of Guangxi is assessed. The result reveals that the risk is at yellow warning,and coincides with the real situation.

Key words: information security,risk assessment,method,threat,asset,vulnerability

随着信息化的深入发展,人们的工作与生活越来越离不开网络与信息系统,网络和信息系统的基础性、全局性作用日益增强,国民经济和社会发展对基础信息网络和重要信息系统的依赖性越来越大,产生的信息安全问题对国家安全的影响日益突出。信息化的风险与风险管理问题已引起各国普遍重视,国外许多国家非常重视信息安全风险评估,美国政府 2002 年颁布联邦信息安全管理法,对信息安全风险评估提出了具体的要求。欧盟国家对信息安全风险评估也提出了具体的部署。我国于 2003 年启动了信息安全风险评估工作,将信息安全风险评估作为一项重要的举措,2004 年国务院信息办开始研究制定信息安全风险评估指南和信息安全风险管理指南两个风险评估的标准。2005 年国务院信息办组织有关省市开展了试点,2006 年由国信办、公安部、安全部等起草了《关于开展信息安全风险评估工作的意见》。本文在分析产生网络信息安全风险的原因的基础上,介绍了信息安全风险的评估方法,并尝试性地对广西自治区级电子政务网络平台进行安全风险评估。

收稿日期:2006-07-21
作者简介:陈友初(1955-),男,广西玉林人,教授级高工,主要从事软件开发、网络设计与建设、网络应用开发等工作。

1 产生网络信息安全风险的原因

保障网络信息的安全已经成为关系信息化能否健康发展的重大问题,要保证网络信息系统的安全、稳定运行,必须要了解网络信息系统产生安全风险的原因,才能有针对性地做好信息安全风险评估,有效地采取措施降低网络信息系统的风险。网络信息系统产生安全风险的主要原因有以下几种:(1)自然灾害。(2)误操作、安全生产事故。(3)病毒以及网络攻击。(4)内部造成的信息、数据的篡改、丢失和泄密。(5)外部造成信息、数据的泄露、篡改和丢失。(6)借助高端技术进行欺诈等。(7)设备、线路故障。

2 信息安全风险评估方法

2.1 评估方法

信息安全风险评估是信息系统安全保障机制建立过程中的一种评价方法,评价结果为信息安全风险管理提供依据。风险评估分析要涉及资产、威胁、

脆弱性等基本要素，资产分为网络、数据、软件、硬件、文档、服务、人员等类，资产的属性是资产价值；威胁是指可能导致对系统危害的潜在起因，威胁的属性是威胁出现的频率；脆弱性是指可能被威胁所利用资产的弱点，脆弱性的属性是资产弱点的严重程度。

信息安全风险评估要确定风险评估的目标、范围和评估方法。风险评估的范围可以是单位全部的信息及与信息系统相关的各类资产、管理机构，也可以是某独立的系统，关键业务流程。

传统的风险评估理论从计算方法区分有定性方法、定量方法和定性与定量结合方法[1]。

2.2 评估工具

风险评估分析工具分为风险评估与管理工具、系统基础平台工具、辅助工具三类。风险评估与管理工具是集成了风险评估各类知识和判据的管理信息系统，以规范风险评估的过程和操作方法；或者是用于收集评估所需要的数据和资料，基于专家经验，对输入输出进行模型分析。系统基础平台风险评估工具主要用于对信息系统的操作系统、数据库系统、网络设备等主要部件的弱点进行分析，如网络扫描器、主机扫描器、数据库扫描器。风险评估辅助工具主要实现对数据的采集、现状分析和趋势分析等，为风险评估各要素的赋值、定级提供依据，如入侵监测系统、安全审计工具、拓扑发现工具、资产信息收集系统，评估指标库、知识库、漏洞库、算法库、模型库等[2]。

3 自治区级电子政务网络平台的安全风险评估实践

风险评估贯穿到信息系统的整个生命周期，在信息系统规划设计阶段、验收阶段和系统运维阶段均需要进行风险评估。

广西互联网经过多年的建设，已经具有一定的规模，建成了自治区级机要专网、自治区级政务内网和广西政务外网3个物理独立的网络平台，分别联接了160、140和130个自治区直属厅局单位，形成了广西电子政务基础网络平台，在这些平台上运行了一批应用系统。为了保证网络系统、应用系统的安全、稳定运行，我们参考国家的有关标准并结合广西互联网的实际情况，开展了网络信息安全风险评估的研究与实践工作。广西互联网已投入运行，属于运维阶段评估。运行维护阶段风险评估的目的是了解和控制网络信息系统运行过程中的安全风险，是保证系统安全的动态措施。评估内容包括对真实运行的网络与信息系统、资产、威胁、脆弱性等各方面。

我们采用以定性为主，定性和定量相结合的评估方法。我们进行风险评估的做法是，首先确定风险评估的目标和范围，按资产的重要性进行分类，建立网络信息系统风险评估的评价体系，确定风险评估的指标，然后定期对网络系统进行风险评估，根据评估结果及时解决发现的安全问题，使风险降低到可以控制的程度。

根据产生安全风险的原因和与安全密切相关的资产情况，评价指标分为机房环境安全、网络安全、系统安全、应用安全和安全管理5类共34项指标，每项指标值为0～12分，每个指标计算或评估出分值，34项指标的分值累计即为总分。安全风险评估的各项具体指标如表1所示。

表1 广西自治区级电子政务网络平台安全风险评估指标

序号	指标名称
1.	机房环境安全
(1)	防火、防盗、防雷击措施
(2)	温度、湿度、烟尘
(3)	UPS电源满足设备需求情况
2.	网络安全
(1)	网络结构合理性
(2)	网络主干线路故障情况
(3)	用户报修网络故障情况
(4)	机房网络设备故障情况
(5)	外部网络设备故障情况
(6)	机房网络设备故障情况
(7)	外部网络设备故障情况
(8)	主干核心交换机冗余
(9)	主干汇聚交换机冗余
(10)	网络线路冗余
(11)	出口路由器设备冗余
(12)	国际互联网出口稳定性
(13)	隔离与访问控制措施
(14)	入侵检测技与漏洞扫描系统
3.	系统安全
(1)	服务器病毒防护
(2)	系统漏洞
(3)	网络操作系统安全配置
4.	应用安全
(1)	服务器安全配置程度
(2)	用户访问记录
(3)	服务器设备备份
(4)	网站数据备份情况
(5)	网络运行数据备份
(6)	服务器管理情况
(7)	网站信息内容安全
(8)	网站、应用系统安全
5.	安全管理
(1)	内部员工网络安全培训次数
(2)	安全保障制度完善程度
(3)	制度执行效果满意度
(4)	内部协作程度
(5)	网络运维人员解决问题能力
(6)	中心领导监督重视程度

根据全部指标的总分,结合重要的关键指标的值将整个系统的安全分为 4 个等级:

(1)绿色安全:总分 367 分以上,网络信息系统安全系数高,风险小。

(2)黄色预警:总分 306～366 分,网络信息系统安全存在隐患,需要对存在的问题进行改善。

(3)橙色预警:总分 245～305 分,网络信息系统安全存在隐患较多,需要尽快解决存在的问题。

(4)红色预警:总分 244 分以下,网络信息系统安全存在严重问题,安全风险较大,必须及时解决才能保证系统的安全稳定运行。

从我们 2006 年 1～6 月的网络信息系统安全风险评估实践看,风险评估结果基本处于黄色预警等级,与网络信息系统的现状基本相符。通过风险评估,进一步完善安全组织和安全管理制度,完善了各种安全技术防护体系,对提高网络信息系统的安全性、稳定性,保证系统的正常运行起到了良好的作用。

4 结束语

我国信息系统风险评估工作刚刚起步,我们也仅进行了有益的探讨与实践,风险评估的规范化、评估模型和评估方法还需要深入研究,风险评估工具和风险评估经验还比较少,我们将按照国家有关风险评估标准进一步完善风险评估指标体系、评估方法和评估手段,收集风险评估需要的各种数据,建立符合实际情况的风险评估指标库、模型库和知识库,提高风险评估水平,保障网络系统的安全、稳定运行。

参考文献:

[1] 宁家骏. 利用风险评估完善信息安全风险管理体系[J]. 信息网络安全,2005,5(5):43-45.

[2] 国家信息化办工作公室. 信息安全风险评估指南:送审稿[S]. 2006.

(责任编辑:韦廷宗)

(上接第 363 页)

3 结束语

本文在分析垃圾文件形成的基础上,提出了 4 种清除垃圾文件的方法,通过这 4 种方法来清理磁盘后,不但净化了系统,而且提高了系统的运行效率。但由于软件更新速度的加快,这些方法不可能全面,而且还有很多垃圾文件是使用者本身形成的。所以我们在注意清理垃圾文件的同时,还要形成把自己生成的文件保存到非系统盘的习惯。只有这样,才能最大限度地保证系统的清洁,提高计算机的运行效率。

参考文献:

[1] 翁元祥. 自制 DOS 下的垃圾收集器[J]. 电脑知识,1998(12):14.

[2] 周绍安. 找回被 Windows ME 系统下垃圾文件浪费的硬盘空间[J]. 微机发展,2001(6):36-38.

[3] 潘凤. 删除系统目录下的"怪"文件[J]. 科技情报与经济,2004,14(5):201.

[4] 张卒. 让"最近文件"一次消失[J]. 软件世界,2005(3):60.

[5] 邵国辉. 自力更生清理"垃圾文件"[J]. 电脑爱好者,2002(6):59.

[6] 张幼真. 让"垃圾文件"无处可藏[J]. 微电脑世界,2002(20):100-103.

[7] ABC. 剿匪大行动——全歼 Windows 另类垃圾[J]. 电脑爱好者,2004(16):55-61.

[8] 佚名. 去其糟粕取其精华——玩转垃圾清理术[J]. 电脑爱好者,2006(5):42-43.

[9] 宗剑钊. 火眼金睛识"垃圾"[J]. 电脑知识与技术,2006(16):26.

[10] 郭萍,肖四发,印德彬. Windows XP 超级技巧 1000 例[M]. 北京:电子工业出版社,2006.

[11] 阿飒. 巧用批处理删除垃圾文件[J]. 电脑校园,2003(6):30.

(责任编辑:韦廷宗)