文章编号:1001 - 9081(2008)08 - 1920 - 04

信息系统安全风险评估技术分析

杨晓明[1], 罗衡峰[1], 范成瑜[2],陈明军[2],周世杰[2],张 利[3]
(1.信息产业部 电子第五研究所,广州 510610; 2.电子科技大学 计算机科学与工程学院,成都 610054;
3. 中国信息安全产品测评认证中心,北京 100089)
(lhf@ ceprei. biz)

摘 要:信息系统安全的风险评估是建立信息系统安全体系的基础和前提。在对国内外现有的信息安全风险评估方法与技术进行归纳和较系统的介绍的基础上,指出了目前信息安全风险评估需要解决的问题,对未来信息系统安全风险评估的发展前景进行了分析。

关键词:信息系统;信息安全;风险评估
中图分类号: TP309 **文献标志码**:A

Analysis of risk evaluation techniques on information system security

YANG Xiao-ming[1], LUO Heng-feng[1], FAN Cheng-yu[2], CHEN Ming-jun[2], ZHOU Shi-jie[2], ZHANG Li[3]
(1. *The Fifth Research Institute of Ministry of Information Industry, Guangzhou Guangdong* 510610, *China*;
2. *School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu Sichuan* 610054, *China*;
3. *China Information Technology Security Certification Center, Beijing* 100089, *China*;)

Abstract: The risk evaluation on information system security is the basis and precondition of the security mechanism of information system. This paper introduced the present evaluation techniques in detail and then summarized these techniques according to different characteristics. After that, we analyzed the problems existing in risk evaluation on information system security and future prospect.

Key words: information system; information security; risk evaluation

0 引言

在现代社会,以信息技术为基础的信息产业已经成为世界经济的重要支柱产业,信息产业的发达程度已成为一个国家的综合国力和国际竞争力强弱的重要标志。与此同时,网络与信息系统自身存在的缺陷、脆弱性以及面临的威胁,使信息系统的运行客观上存在潜在的风险,阻碍了信息产业的发展[1]。因此,如何保证信息系统和网络安全有效地运行,成为当前亟待解决的问题。在经历大量实践之后,人们认识到信息系统的安全是一个非常复杂问题,任何单一层次上的安全措施都不可能提供真正的全方位的安全[2]。我们必须从风险分析入手,获得信息系统的安全状态,对信息系统受到的威胁进行客观科学的分析和评估,才能为信息系统的安全保护提供坚实的基础。本文对目前国际和国内流行的信息安全风险评估的基本原理、相关标准进行了研究,并对风险评估的基本方法进行了分类和比较。

1 风险分析原理

所谓信息安全风险评估,是从风险管理角度,运用定性、定量的科学分析方法和手段,系统地分析信息和信息系统等资产所面临的人为的和自然的威胁,以及威胁事件一旦发生可能遭受的危害程度,有针对性地提出抵御威胁的安全等级防护对策和整改措施,从而最大限度地减少经济损失和负面影响[2]。它的基本要素包括:要保护的信息资产、信息资产的脆弱性、信息资产面临的威胁、存在的可能风险、安全防护措施等。其中,每个要素有各自的属性。资产的属性是资产价值;威胁的属性可以是威胁主体、影响对象、出现频率、动机等;脆弱性的属性是资产弱点的严重程度。风险评估围绕着这些基本要素展开,通过分析信息资产的脆弱性来确定威胁可能利用哪些弱点来破坏其安全性。

基本的风险分析原理[3]如下。

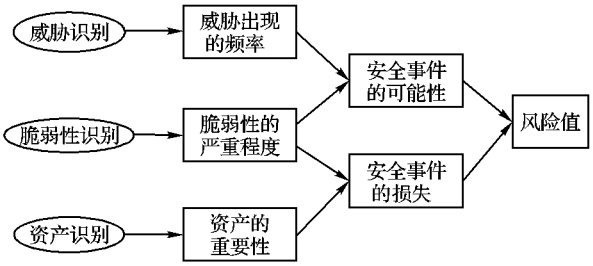

图1 风险分析示意图

如图1所示,风险分析主要内容为:

1)对资产进行识别,并对资产的重要性进行赋值;

2)对威胁进行识别,描述威胁的属性,并对威胁出现的频率赋值;

收稿日期:2008 - 05 - 16;**修回日期**:2008 - 06 - 16。

作者简介:杨晓明(1974 -),男,湖北宜昌人,高级工程师,硕士,主要研究方向:信息安全; 罗衡峰(1978 -),男,湖南邵阳人,工程师,硕士,主要研究方向:信息安全; 范成瑜(1981 -),男,重庆人,硕士研究生,主要研究方向:信息安全; 陈明军(1982 -),男,四川隆昌人,硕士研究生,主要研究方向:信息安全; 周世杰(1970 -),男,四川荣县人,副教授,博士,主要研究方向:分布式计算、网络安全; 张利(1972 -),男,湖北黄石人,博士,主要研究方向:信息安全。

3)对资产的脆弱性进行识别,并对具体资产的脆弱性的严重程度赋值;

4)根据威胁和脆弱性的识别结果判断安全事件发生的可能性;

5)根据脆弱性的严重程度及安全事件所作用资产的重要性计算安全事件的损失;

6)根据安全事件发生的可能性以及安全事件的损失,计算安全事件一旦发生对组织产生的影响,即风险值。

2　评估标准分析

通过依据某个标准的风险评估或者得到该标准的评估认证,不但可为信息系统提供可靠的安全服务,而且可以树立单位的信息安全形象,提高单位的综合竞争力。现在,世界各国根据自己的研究进展和实际情况,相继发布了一系列有关安全评估的准则和标准。目前,国际上适用较广泛的标准有:

1)CC 标准。

信息技术安全评估公共标准(Common Criteria of Information Technical Security Evaluation,CCITSE),简称 CC,是美国、加拿大及欧洲四国(共 6 国 7 个组织)经协商签署同意的,是国际标准化组织统一现有多种准则的结果,它是目前最全面的评估准则。CC 2.0 版于 1999 年成为国际标准 ISO/IEC 15408,我国于 2001 年等同采用为 GB/T 18336。

CC 是面向所有 IT 行业的,但不包括对信息安全管理和物理安全方面的评测。它侧重于对系统和产品的技术指标的评估标准。

2)BS 7799(ISO/IEC 17799)。

BS 7799 标准是由英国标准协会(BSI)制定的信息安全管理标准,是国际上具有代表性的信息安全管理体系标准,标准包括两部分:BS7799-1:1999《信息安全管理实施细则》,BS7799-2:2002《信息安全管理体系规范》。其中 BS7799-1:1999 于 2000 年 12 月通过国际标准化组织(ISO)认可,正式成为国际标准,即 ISO/IEC17799:2000[4];BS7799-2:2002 已更新并在 2005 年 10 月正式发布为 ISO/IEC 27001:2005。

BS7799 是侧重于管理理念的最好体现。在对信息系统日常管理方面,BS7799 涵盖了安全管理涉及的方方面面,提供了一个可持续提高的信息安全管理环境,但在安全技术方面不如 CC 分析得系统、透彻。

3)ISO/IEC TR 13335[5]。

在各国研究的基础上,国际标准化组织在 1996 年开始制定《IT 信息安全管理指南》(ISO/IEC TR 13335),它由 5 个部分组成,目前分别是:ISO/IEC 2nd PDTR 13335-1:2002(revision)《信息技术 安全技术 信息安全管理指南 第 1 部分:信息安全管理和计划的概念和模型》;ISO/IEC WD 13335-2:2001《信息技术 安全技术 信息安全管理指南 第 2 部分:信息安全管理和计划》;ISO/IEC 1st WD 13335-3:2002《信息技术 安全技术 信息安全管理指南 第 3 部分:信息安全管理技术》;ISO/IEC TR 13335-4:1999《信息技术 安全技术 信息安全管理指南 第 4 部分:安全措施的选择》;ISO/IEC DTR 13335-5:2000《信息技术 安全技术 信息安全管理指南 第 5 部分:网络安全管理指南》。此标准的主要目的是要给出如何有效地实施 IT 安全管理的建议和指南。用户完全可以参照这个标准制定自己的安全管理计划和实施步骤。相比 BS 7799/ISO17799,它对安全管理的过程描述得更加细致。我们在选择风险控制措施时,可以参考此标准的相关内容。

4)OCTAVE 2.0[6]。

OCTAVE 全称 Operationally Critical Threat, Asset, and Vulnerability Evaluation,是一种信息安全风险管理方式。包括面向大型组织的 OCTAVE 方法和面向小型组织的 OCTAVE-S 方法两种具体方法。实际使用时,一个组织可能需要混合使用上述两种方法,或与 OCTAVE 完全不同的评估方式混合。

5)国家标准。

我国国家标准《计算机信息系统安全保护等级划分准则》(CB17859)[7]于 1999 年 9 月正式批准发布,该准则将计算机信息系统安全分为五级:用户自主保护级、系统审核保护级、安全标记保护级、结构化保护级和访问验证保护级。《信息安全风险评估规范》[3]等一批信息安全的新标准于 2007 年 11 月正式批准发布,用于指导和规范针对组织的信息系统及其管理的信息安全风险评估工作。

3　评估方法分析

评估方法的选择直接影响到评估过程中的每个环节,甚至可以左右最终的评估结果,所以需要根据系统的具体情况,选择合适的风险评估方法。

现有的风险评估方法有很多种,可大致分为定量的风险评估方法、定性的风险评估方法和综合的风险评估方法三大类。

3.1　定量的评估方法

定量评估方法的思想是,对构成风险的各个要素和潜在损失的水平赋以数值或货币的金额,当度量风险的所有要素(资产价值、威胁可能性、弱点利用程度、安全措施的效率和成本等)都被赋值,风险评估的整个过程和结果就可以进行量化[8]。

定量的评估方法的优点是用直观的数据来表述评估的结果,看起来一目了然,而且比较客观,定量分析方法的采用,可以使研究结果更科学,更严密,更深刻。它的缺点是,常常为了量化,使本来比较复杂的事物简单化、模糊化了,有的风险因素被量化以后还可能被误解和曲解。

以下是一些常用的定量评估方法:

1)模糊综合评判法。

模糊综合评判法是根据模糊数学中的模糊变换原理和最大隶属度原则,考虑与被评事物相关的各个因素,从而所做出的综合评价。该种评估方法的着眼点是所考虑的各个相关因素。

2)BP 神经网络。

BP 神经网络是通过对所要解决的问题的知识存储以及对样本的学习训练,不断改变网络的连接权值以及连接结构,从而使网络的输出接近期望的输出的方法。这种方法的本质是对神经网络中的可变权值的动态调整。

3)灰色系统。

灰色系统将一切随机变量看作在一定范围内的灰色量，将随机过程看作是在一定范围内变化的与时间有关的灰色过程。对灰色量的处理不是从统计规律的角度通过大样本量进行研究，而是用数据处理的方法将杂乱的原始数据整理成规律性较强的生成数列再做研究。

3.2 定性的评估方法

定性的评估方法是目前采用最为广泛的一类方法。它主要依据研究者的知识、经验、历史教训、政策走向及特殊变例等非量化资料对系统风险状况做出判断的过程。它主要以与调查对象的深入访谈做出个案记录为基本资料，然后通过一个理论推导演绎的分析框架，对资料进行编码整理，在此基础上做出调查结论。

与定量评估比较，定性评估操作起来相对容易，它没有定量评估那样繁多的计算负担，还可以挖掘出一些蕴藏很深的思想，使评估的结论更全面、更深刻，但它的主观性很强，要求评估者具备一定的经验和能力，其分析的结果也很难统一。常用的评估方法有专家评价法、历史比较法、事故树分析法、因果分析法和逻辑分析法等。

其中，最常用的专家评价法是一种吸收具有丰富现场经验的专家参与，根据事物的过去、现在以及未来的发展趋势，进行积极的创造性思维活动，对事物的未来进行分析、预测的方法。它包括两种形式：一种是专家审议法，根据一定的规则，组织相关专家进行积极的创造性活动，对具体问题通过具体讨论，集思广益。第二种是专家质疑法，即由专家对提出的设想或方案进行质疑。

3.3 综合的评估方法

通过比较定性和定量的评估方法（表 1），我们不难发现两者各有其优缺点。

表 1 方法优缺点对比

方法类别	优点	缺点
定性方法	定性分析基于主观，分析的准确性较好；计算量小；操作简单，可以利用专家的知识	易受主观影响，分析精确度不够；分析者需要具备一定的经验和能力；评估对象多为小系统；结果难以统一
定量方法	定量分析基于客观，精确性好；分析的结果较为直观，容易理解	分析的准确性可能较差；需要大量的统计数据；操作复杂，计算量较大；被量化后的风险因素可能被误解

在实际的系统风险评估过程中，需要考虑的因素很多，有些评估要素是可以用量化的形式来表达，而对有些要素的量化又是很困难甚至是不可能的。所以，我们不能将定性分析和定量分析两种方法简单的割裂开来，而是应该将这两种方法综合起来，采用综合的评估方法。在不容易获得准确数据的情况下采用定性分析方法分析，在定性分析的基础上使用定量方法进行计算以减少其主观性。

最典型的综合评估方法是层次分析法（Analytic Hierarchy Process，AHP）。如图 2 所示，其思想是根据所要分析的问题的性质和达到的总体目标，将问题分解为不同的组成要素，并按照因素间的相互关联、影响以及隶属关系将因素按不同的层次聚集组合，形成一个层次的分析结构模型，并最终把系统分析归结为最底层相对于最高层的相对重要性权值的确定或相对优劣次序的排序问题。

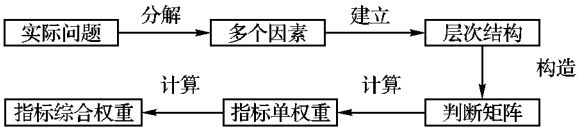

图 2 AHP 法的分析流程

这一方法的核心是将决策者的经验判断给予量化，从而为决策者提供定量形式的决策依据。使用 AHP 方法进行风险评估的基本步骤[1]如下：

1）系统分解，建立层次结构模型：基于分解法的思想，进行对象的系统分解，构造层次模型。如下图所示，它的基本层次有三类：目标层、准则层和方案层，目的是基于系统基本特征建立系统的评估指标体系。其中的准则层可以由若干个层次组成，包括所需考虑的准则、子准则。

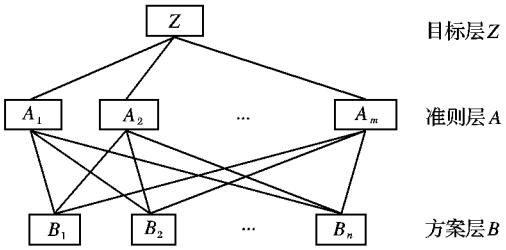

图 3 层次结构模型

2）构造判断矩阵：判断矩阵是将层次结构模型中同一层次的要素相对于上层的某个因素，根据重要程度相互间进行成对比较而形成的矩阵。在对评估指标的相对重要程度进行测量时，根据心理学家提出的“人区分信息等级的极限能力为 7 ±2”的研究结论，一般引入九分位的相对重要的比例标度。假定 A 层中元素 A_k 与下层元素 $C_1, C_2, \cdots, C_m$ 有联系，那么构造的判断矩阵形式如下：

$$\boldsymbol{C} = \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1m} \\ C_{21} & C_{22} & \cdots & C_{2m} \\ \vdots & \vdots & & \vdots \\ C_{m1} & C_{m2} & \cdots & C_{mm} \end{bmatrix}$$

式中，C_{ij} 表示对于 A_k 而言，C_i 相对 C_j 的重要程度赋值。赋值可由决策者直接提供，或是由分析者通过某种技术咨询而得，但一般由熟悉问题的专家独立给出。

3）指标单权重系数的计算：计算的中心问题是求解判断矩阵的最大特征根及其对应的特征向量；通过判断矩阵及矩阵运算的数学方法，确定对于上一层次的某个元素而言，本层次中与其相关元素的相对权重值。比如，根据 m 个元素 $C_1, C_2, \cdots, C_m$ 对于元素 A_k 的判断矩阵 $\boldsymbol{C}$，求它们对于元素 A_k 的相对权重向量 $\boldsymbol{W} = \{w_1, w_2, \cdots, w_m\}^{\mathrm{T}}$。在实际应用中，多采用近似算法计算，即：

$$w_i = \sqrt[m]{\prod_{j=1}^{m} \boldsymbol{C}_{ij}}, \quad (i,j = 1,2,\cdots,m)$$

在求得相对权重向量后，为了保证应用层次分析法得到的结论合理，还需要对构造的判断矩阵进行一致性检验。这时，需要利用一致性指标 $CI = \dfrac{\lambda_{\max} - m}{m - 1}$ 做一致性检验，当 CI 值越大，判断矩阵的不一致程度越严重。若检验通过，特征向

量(归一化后)即为权向量;若不通过,需要重新构造成对比较矩阵。

4)计算指标综合权重:指标综合权重是指方案层中所有元素对目标层的权重,它的每一个分量表示相应方案在目标中所占的份额或比重。已知准则层对目标层的权重 $W1$ 及方案层对准则层的权重 $W2$,则方案层对目标层的综合权重向量的计算公式为 $W = W1 \times W2$。综合权重也必须进行一致性检验验证,判断是否满足 $CR < 0.1$ ($CR = CI/RI$)。若上述条件满足,则认为综合权重计算结果具有满意的一致性。

4　风险评估工具分析

对国家政府部门和大中型企业的基础网络和重要信息系统进行风险评估,是一项极其复杂、耗时的工作。依靠自动化的工具,可以让技术人员从大量简单重复的劳动中解放出来,专注于困难复杂的分析工作中去,有利于提高评估工作的质量和效率。目前,常见的风险评估的工具可大致分为风险评估辅助工具、系统软件评估工具、安全管理评价系统三类[3]。

4.1　安全管理评价系统

安全管理评价系统根据一定的安全管理模型,基于专家经验,对输入输出进行模型分析。此类工具主要从安全管理方面入手,评估资产所面临的威胁。评估的方式可以通过问卷的方式、也可以通过结构化的推理过程,建立模型、输入相关信息,得出评估结论。通常这种系统在对信息安全风险进行评估后都会有针对性地提出风险管理措施。这种风险评估工具通常建立在一定的算法之上,或通过建立专家系统,利用专家经验进行风险分析,给出专家结论。

常用的安全管理评价系统包括 CC Toolbox、COBRA、ASSET、RiskWatch 等,这些系统的相关情况如表 2 所示。

表 2　安全管理评价系统比较

工具	国家公司	成熟度	功能	标准
Asseet-1	美国 NIST	NIST 发布	依据美国 NIST SP 800-26 进行 IT 安全自动化自我评估	NIST SP 800-26
CC Toolbox	美国 NIAP	NIAP 发布	依据 CC 进行信息安全自动化评估	CC
COBRA	美国 C&A System Security Ltd	成熟产品	主要依据 ISO 17799 进行风险评估	主要依据 ISO 17799
RiskWatch	美国 RiskWatch 公司	成熟产品	综合各类相关标准进行风险评估和风险管理	各类信息安全相关标准

4.2　系统软件评估工具

系统软件评估工具主要用于对一些信息系统的部件(如操作系统、数据库系统、网络设备等)的漏洞进行分析,包括脆弱点扫描工具和渗透性测试工具。

脆弱点扫描工具也称为安全扫描器或漏洞扫描仪,用于识别网络、操作系统、数据库系统的安全漏洞。通常情况下,这些工具能够发现软件和硬件中已知的安全漏洞,以决定系统是否易受已知攻击的影响,并且寻找系统脆弱点。

渗透性测试工具是根据漏洞扫描工具扫描的结果,进行模拟黑客测试,判断是否这些漏洞能够被他人利用。其主要目的是检测已发现的漏洞是否真正会给系统或网络环境带来威胁。这种工具可以是针对某个漏洞攻击的软件,也可以是一些脚本文件。通常,渗透性工具与漏洞扫描工具都是一起使用的。

比较常用的系统软件评估工具包括 ISS Internet Scanner、Nessus、SAINT 等。我们在进行评估工作时,可以针对被评估对象的运行环境对上述工具进行选择,比如:ISS 工具只用于 Windows 主机扫描,而 Nessus 和 SAINT 则适合于 Unix 环境的网络扫描。

4.3　风险评估辅助工具

科学的风险评估需要大量的实践数据和经验数据的支持,因此历史数据和技术数据的积累是风险评估科学性和预见性的基础。为了收集评估所需要的数据、资料和监控某些网络行为的日志系统,评估人员常采用风险评估辅助工具收集评估所需要的数据和资料,帮助完成现状分析和趋势分析。

最常见的风险评估辅助工具是入侵监测系统(IDS),它可以帮助检测各种攻击试探和误操作;同时也可以作为一个警报器,提醒管理员发生的安全状况。

5　结语

风险评估是信息安全建设的基础和前提,它从风险管理的角度,运用科学的方法和手段,系统地分析网络与信息系统所面临的威胁及存在的脆弱性,并为防范和化解信息安全风险,保障网络和信息安全提供科学依据。目前,风险评估正处于发展阶段,仍然存在各种问题。比如,评估过程的主观性是影响评估结果的一个相当重要而又是最难解决的方面;安全评估体系所应包括的相应组织架构、业务、标准和技术体系还不完善;没有统一的评估标准,由于各种标准的侧重点不同,导致评估结果没有可比性,甚至会出现较大的差异。

随着信息化的不断深入,信息安全越来越成为关系到国民经济的每一方面的重大问题。作为信息系统安全工程重要组成部分,风险评估得到了极大重视。因此,研究一套科学的、先进的、可行的信息安全风险评估方法,对于我国的信息化建设及信息安全的发展具有重要的理论与实践意义。

参考文献:

[1] 冯登国,张阳,张玉清. 信息安全风险评估综述[J]. 通信学报,2004,25(7):10-18.

[2] 吴亚非,李新友,禄凯. 信息安全风险评估[M]. 北京:清华大学出版社,2007.

[3] GBT20984-2007. 信息安全技术信息安全风险评估规范[S]. 国家质量监督检验检疫局,2007.

[4] ISO/IEC 17799:2000. Information technology-code of practice for information security management[S]. ISO,2000.

[5] ISO/IEC TR 13335. Guidelines for the Management of IT Security (GMITS)[R]. 1996.

[6] ALBERTS C, DOROFEE A, STEVENS J, *et al*. Introduction to the OCTAVE approach [EB/OL]. [2007-08-23]. http://www.cert.org/octave/approach_intro.pdf.

[7] GB17859-1999. 计算机信息系统安全保护等级划分准则[S]. 国家质量技术监督局. 北京:中国标准出版社,1999.

[8] 朱方洲. 基于 BS7799 的信息系统安全风险评估研究[D]. 合肥:合肥工业大学, 2007.