信息安全风险模块化层次评估方法研究*)

黄 勤 张月琴 刘益良
(重庆大学自动化学院 重庆 400030)

摘 要 信息系统广泛应用于各行各业,其安全性已经引起人们的密切关注。信息系统风险评估是分析信息系统的安全现状和潜在风险,从而为安全策略的设计实现提供依据和指导的过程,是规划、建设和维护信息系统安全结构的一项重要而且不可缺少的工作。本文根据信息系统功能模块化强的特点,采用系统聚类法建立了信息安全风险模块化层次结构评估模型,将一个完整的信息系统分为"管理模块"、"核心模块"、"分布层模块"、"服务器模块"、"边缘分布模块"、"外网接入模块"以及"外部环境模块"7个模块,并对模块化评估模型聚类方法和评估实施步骤作了详细的介绍。

关键词 风险评估,模块化,层次化

The Research of Risk Evaluation Method of Modularization and Hiberarchy of Information Security

HUANG Qin ZHANG Yue-Qin LIU Yi-Liang
(Automation School, Chongqing University, Chongqing 400030)

Abstract Information system has been used in every walk of life and its security has nearly been noticed. The risk evaluation which can analyze the current status and potential risk of information system provide gist and direction for later security programming, moreover it is an important and indispensable for programming, building and maintaining security framework of information system, so it is indispensable. We use system clustering method to build risk evaluation method of modularization and hiberarchy based on the strong function modularization of information system. It breaks up the system into seven modules: manage module, core module, distribution layer module, sever module, margin distribution module, Internet module and outer circumstance module. In this article, we introduce detailedly the modularization model, the clustering method and the evolution process.

Keywords Risk evaluation, Modularization, Hiberarchy

1 引言

现在关于风险评估的理论研究很多,所采用的分析方法也是多种多样,常见的有故障树法、专家打分法、德尔菲法、层次分析法以及模糊综合评价法。单一的分析方法已不能完成对一个大型信息系统的风险评估了,目前多采用将多种方法相结合的综合方法进行风险评估。在层次分析方法中应用专家打分法确定判断矩阵;在模糊综合评价方法中应用德尔菲法确定评价指标子集;在故障树方法中应用层次分析方法确定评价权值等等。这些方法可以应用到各种信息系统中,且均能比较准确合理地评估出系统的风险系数,但它们也都存在着不足之处。专家打分法主观性较强、层次分析法计算量大而模糊综合评价方法不能得出较细致具体的评价[1]。为弥补以上各自的不足,本文提出模块化综合评价法,将一个大型信息系统分解成若干模块,在反映体系结构各功能模块间的安全关系的同时,又可以让评估人员逐个模块地评估和实施安全性,减小计算量同时得到准确具体的评估结果,提高评估效率[2]。

2 模块化层次风险评估方法

2.1 模块化层次风险评估模型基本思想

所谓模块化,就是为了取得最佳效益,从系统观点出发,研究产品(或系统)的构成形式,用分解和组合的方法,建立模块体系,并运用模块组合成产品(或系统)的全过程[3]。近年来,模块化方法在各行各业都得到了广泛应用,已经成为了一种产品设计工具。且随着模块化思想的延伸,均已提出了一种科学管理的观念和方法,并逐渐成为一种现代企业产品设计、组织设计、和知识管理战略设计的方法论。因此,在风险评估领域中,应用模块化方法进行科学有效的风险评估是又一成功应用。我们在风险评估过程中首先将一个大的、复杂的信息系统分解成几个耦合度很弱的模块:管理模块、分布层模块、服务器模块、核心模块、边缘分布模块、外网接入模块以及外部环境模块。每个独立的模块又可以分解成若干独立的子模块,大幅降低了系统的复杂性,降低评估成本。而且在进行风险评估任务时,对各模块的评估可以并行开展,使模块评估的各方从事自己所擅长的工作,缩短评估时间,提高评估效率。而且模块化评估有利于评估工具的开发和应用。

2.2 模块化层次风险评估模型描述

模块化层次风险评估模型的分布关系如图1所示。

信息系统模块化风险评估可分为内部评估、边缘评估和外部评估。内部评估由内部管理人员、技术人员填写调查问卷,提供数据完成;边缘评估主要由系统边界职责部门完成;外部评估由系统的协作有关人员如网络管理人员、对外工作人员通过填写问卷完成。各评估模块同时展开评估,职责分

*)本文研究得到重庆市自然科学基金项目(CSTC,2004BB2181)资助。黄 勤 副教授,研究方向为信息安全领域和计算机硬件技术;张月琴 硕士研究生,研究方向为信息安全领域。

割，结果提供专家和专业评估人员完成整个信息系统的综合评估。这样可以保证评估工作的高效率、低风险。

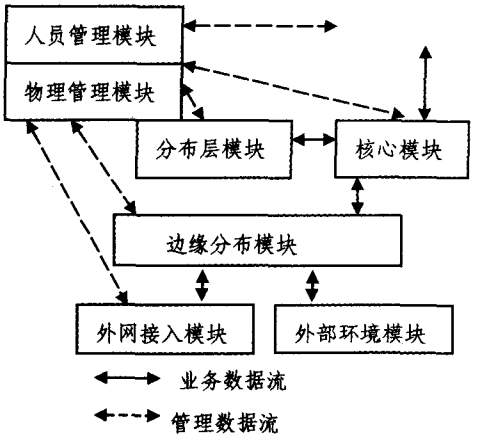

图1 模块化层次风险评估模型

(1)管理模块

管理模块集中了所有制定有关的法律法规、行业标准，不断完善管理制度，加大管理力度来保证企业设备和信息系统的安全的功能。管理安全是系统安全的基础，由于动态多变性往往存在相对较大的风险。评估内容包括安全策略、组织安全、资产的分类和控制、个人安全、物理和环境安全等5个重要方面[3]。

·安全策略(Security policy)的目标是管理层制定一套清晰的策略指导，为信息安全提供管理性的指导和支持。

·组织安全(Organization security)的目标是管理组织内的信息安全；维护组织内被第三方访问的信息处理设备和信息资产的安全；维护信息处理外包给另外一个组织时信息的安全。

·资产的分类和控制(Asset classification and control)的目标是为组织的资产提供适当的保护；确保信息资产得到了适当级别的保护。

·个人安全(Personnel security)的目标是减少人为错误、盗窃、欺诈或设备误用造成的风险；确保用户意识到信息安全的威胁和利害关系，并做好准备在日常工作过程中支持组织的安全策略；把安全事件和故障造成的破坏降低到最低，监控并从事件中汲取教训。

·物理和环境安全(Physical and environmental security)的目标是防止对系统基础设施和信息的非授权访问、破坏和干扰；防止资产损失、被破坏和业务活动的中断；防止对信息和信息处理设备的盗窃和损坏。

(2)核心模块

核心模块包括将信息流尽可能快速地从一个网络路由或者交换至另一网络的各主要功能部分。

核心模块的主要设备是三层交换机，保障交换架构的安全是消除分组窃听威胁的有效手段。核心模块主要评估了系统的开发和维护以及数据库。

·系统的开发和维护(System development and maintenance)的目标是确保将安全融入信息系统的组成部分；防止应用软件系统中用户数据的丢失、改动或误用；保护信息的机密性、源认证和完整性；确保IT支持活动在安全的方式下进行并控制对系统文件的访问；维护应用程序系统软件和信息的安全。

·数据库平台评估对信息系统中重要的数据库和数据运作流程进行了深入分析，对数据库进行了以漏洞扫描为主的远程安全漏洞评估，和以本地安全配置检查为主的本地安全策略评估，完整地分析了数据库平台网络配置、系统漏洞、角色和账号管理、审计措施等各方面的安全问题。

(3)分布层模块

分布层模块主要由提供包括路由、网络服务质量和访问控制的服务等组成。数据流首先经过分布层再传至核心层。目标包括控制对信息的访问；防止未授权用户、未授权的设备对信息系统的访问；防止未授权用户的访问；保护网络服务；防止未授权的计算机访问；防止对信息系统内信息的未授权访问；探测未经授权的活动；确保移动办公和远程工作的安全。

(4)服务器模块

服务器模块包含所有向最终用户和设备提供应用服务的任务。服务器模块主要评估了操作系统以及应用服务器。

·操作系统脆弱性评估，对整个信息系统中的各平台服务器操作系统(如Windows Server 2000、Redhat Linux 9.0、Redhat Linux AS 2.1/3.0、Aix 5.0)进行了远程和本地漏洞扫描，并检查了本地安全的完整性、可靠性和一致性。

·应用服务器平台评估，通过源代码黑盒测试、应用渗透测试、远程漏洞扫描、开发文档和安全策略分析等多种措施，针对各类应用服务进行了准确的脆弱性调查，比较完整地分析和提取了应用系统中可能存在的安全弱点。

(5)边缘分布模块

边缘分布模块是企业信息系统的第一层防护的集合，也是从接入网发送到企业内网的所有信息流的最后一道防线。目标是确保信息处理设备正确、安全的运行；将系统故障的风险降到最低；保护软件和信息的完整性；维护信息处理和通信服务的完整性和可用性；确保网络中信息的安全和基础支撑设施的安全；控制并从物理上保护介质以防止资产损坏和业务活动的中断；防止组织间进行信息交换时信息的丢失、被修改和误用。

(6)外网接入模块

大多数企业网虽然都是专网，但是不可避免要和外网连接。这里所说的外网包括其它企业网和互联网。通过对网络设备的远程漏洞扫描、网络管理措施分析、系统网络架构分析、本地安全策略分析等多层次的手段，全方位地分析了整个信息系统中的网络基础设施和网络架构安全性，审计了网络方面的主动和被动安全弱点。

(7)外部环境模块

一个信息系统是依附于某个产业或部门，所以存在很多的关系网络以及竞争对手，对自己用户以及对手的充分了解可以有效减小系统的威胁，提高评估的针对性。

3 模块之间的相互关系

采用模块化设计，并非简单地将信息系统分解成各个孤立的模块，模块间存在着紧密的联系，且每个模块的评估结果也直接影响到其它模块的评估。

管理模块是整个信息安全体系的核心，位于其它所有模块的最顶层。信息安全体系的建立，应该首先建立管理模块的安全结构。管理模块相对于其它模块而言具有很大的独立性，它是建立其它模块安全结构的基础和前提。

核心模块、服务器模块和分布层模块构成信息系统的内

部网络。这三个模块主要评估来自企业网内部的安全威胁。分布层模块提供了针对内部发起攻击的第一道防线，核心模块的主要目标是转发数据流，其安全性主要依赖于核心模块交换设备本身的安全设置以及分布层模块的安全防护，服务器模块往往会成为内部攻击的主要目标，安全性除了自身的安全措施和分布层模块的安全防护外，严格的安全管理是极为重要的。

边缘分布模块是连接企业内网和外部接入网的桥梁和纽带。边缘分布模块在外部接入网安全措施的基础上，为企业内网提供附加的安全功能。

外部接入网为企业内网提供了第一道安全防线，它可以防范大部分来自外网的安全威胁。外部接入网为外网接人企业网提供统一的接入平台。

模块化的设计将复杂的大型网络划分为几个相对简单的模块，以模块为基本单位构筑整个网络的风险评估结构。使用模块化的风险评估有两个主要优势：首先，它很容易实现单个模块的评估，同时量化了模块与模块间的评估关系，从而在整个企业信息系统中形成分层次的纵深安全体系。其次，它可使设计者进行逐个模块的评估和实施安全，而非试图在一个阶段就完成整个体系结构。

4 基于聚类分析的模块划分方法

聚类分析的基本思想是：认为我们所研究的对象中各单位之间存在着程度不同的相似性(亲疏关系)。于是，根据众多单位的多个观测指标，找出能够度量各单位之间相似程度的统计量，以其作为划分类型的依据，把一些相似程度较大的单位聚合为一类，把另外一些彼此相似程度较大的单位聚合为另一类，关系密切的聚合到一个小的分类单位，关系疏远的聚合到一个大的分类单位，当所有单位都聚合完毕后，再将不同的类型一一划分出来，形成一个由小到大的分类系统。最后再把整个分类系统画成一张图，用它把所有的单位间的亲疏关系表示出来。这是聚类中使用最多且最基本的一种方法，称为系统聚类法。此外，聚类法还包括动态聚类法、图论聚类法、模糊聚类法和有序聚类法，等等。本文中模块的划分方法就是基于系统聚类法的。

系统聚类分析法的实施步骤可分为以下 7 步：

(1)选择据以分类的 p 个基本指标(或数量标志)。本文中选用了影响信息系统风险高低的三个重要指标，即资产价值(X_1)、威胁系数(X_2)，脆弱性(X_3)，并在此基础上搜集相关的数据资料。

(2)根据重要性程度确定各指标的权数。

(3)对原始数据进行标准化的处理，即数据的无量纲化的处理。本文中采用了标准极差化法，即：

$$z_{ik}=\frac{X_{ik}-\overline{X}_k}{S_k}$$

其中：$\overline{X}_k$ 表示指标平均值，S_k 表示指标标准差，得标准化矩阵：

$$Z=\begin{bmatrix}Z_1^T\\Z_2^T\\\vdots\\Z_n^T\end{bmatrix}=\begin{bmatrix}z_{11}&z_{12}&\cdots&z_{1p}\\z_{21}&z_{22}&\cdots&z_{2p}\\\cdots&\cdots&\cdots&\cdots\\z_{n1}&z_{n2}&\cdots&z_{np}\end{bmatrix}$$

(4)求标准化矩阵 Z 的相关矩阵，也即各资产的相关矩阵。

$$R=[r_{ij}]_{p\times p}=\frac{Z^TZ}{n-1}$$

式中 $r_{ij}=(\sum_{k=1}^{n}z_{ki}z_{kj})/(n-1)$，$j=1,2,\cdots,p$

(5)计算各资产间在 p 维空间的距离 d_{ij}，以反映资产间的亲疏程度。在聚类分析中，常用的距离计算公式有多种，可通过采用加权欧式距离，即第 i 项资产和第 j 项资产的空间距离为：

$$d_{ij}=\sqrt{\sum_{k=1}^{m}f_k(z_{ik}-z_{jk})^2}$$

其中 f_k 表示各指标权数，z_{ik} 表示第 i 项资产的第 k 个指标值，可以计算出 n 项资产相互间的距离。

(6)聚类。用于聚类的方法很多，这里主要应用系统聚类法。由于在聚合过程中需要比较各个类间的距离，因此还要对类间距离加以定义。日前，对类与类之间距离的定义有很多，我们选用常用的最短距离法。依此方法，类与类之间的距离，取决于这两类中相距最近的两项资产之间的距离。最短距离法的计算步骤是：先计算出各资产间的距离 d_{ij}，然后，从这些距离中选出距离最短的资产对，将这两个资产合并为一类，接着选出距离次短的，并将挑选结果按下列规则处理：①若该资产对在已有的类中没有出现过，则将其合并为一个新类。②若该资产对分别属于已有的两类，则把这两类合并为一类。③若该资产对中的某一资产在已分好的类中出现过，则将另一个资产也并入该类中。④若该资产对都在已分好的同一类中，则在原类不动。依照上述规则反复挑选、合并，直至将所有的资产归并成一类为止。

(7)确定分类结果。在这一步中最终确定划分的类数，即模块数，以及各资产的类别归属。按照上面介绍方法将分类结果与原始数据结合起来，便可以对各模块风险高低作出判断，可以根据实际需要将其划分成需要的模块数。再根据每个模块中的评估主体来确定所分得的模块属于上述七个主要模块中的某个模块。

总结及其改进 本文对基于层次化结构的风险评估模型的设计方案进行了具体而细致的研究，从而总结出在信息系统中建立模块化层次分析模型具有如下优点：(1)评估效率高。各评估模块可并行评估，评估的各方从事自己所擅长的工作，缩短评估时间，提高评估效率。(2)调试灵活方便。用户可以任意安排、调用、增删和连接模块，在某些算法的系数中考虑了可使模型更加简化或更加精确的选择项。这样在对一个实际信息系统进行建模时，可根据计算机资源的拥有量选择不同的系数，满足不同的建模要求。并可对某些模型进行在线修改调试提供多种维护和监视手段。

参 考 文 献

1 Aagedal J O, den Braber F, Dimitrakos T, et al. Model-based Risk Assessment to Improve Enterprise Security:[0-7695-1656-4/02]. IEEE, 2002

2 周国威. 模块化设计构筑大型企业网络的安全体系. 信息安全与通信保密，2005,11

3 任韶清. 模块化方法与企业模块化合作研究:[北京航空航天大学硕士学位论文]. 2001