# 一种风险评估和等级防护相结合的信息风险预测系统

任 贝 贝
(上海市网络技术综合应用研究所 上海 200233)

**摘 要** 信息安全问题越来越严重,仅仅依靠单一的产品预防根本无法安全有效地保护公司网络信息系统。对此设计一套应用于公司安全风险等级评估系统。风险评估是按照国家有关标准、规范,从信息系统的完整性、保密性及可用性等因素进行综合分析的过程。它和等级保护相结合成为一种有效的风险分析手段。该系统基于等级测评和风险评估相结合的理论,通过建立信息资产风险库,将信息风险和对应的风险等级建立连接。通过对公司信息进行相应的监测,自动测算出每一个系统的风险概率,并提出相应的风险预防措施。整个软件平台经多次测试结果表明,系统运行达到应有的效果。

**关键词** 风险评估 等级保护测评 信息安全

**中图分类号** TP3 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2019.02.027

## AN INFORMATION RISK PREDICTION SYSTEM COMBINING RISK ASSESSMENT AND LEVEL PROTECTION

Ren Beibei
(*Shanghai Institute for Integrated Application of Network Technology*, *Shanghai 200233*, *China*)

**Abstract** Information security is becoming more and more serious. It is impossible to achieve the safe and effective protection of the company's network information system security by only relying on a single product. To solve this problem, we designed a set of risk assessment system for company safety. In accordance with relevant national standards and norms, risk assessment was an effective means of risk analysis which combined the process of comprehensive analysis from the aspects of integrity, confidentiality and availability of information system with grade protection. The system was based on the theory combining grade assessment with risk assessment. The information risk and corresponding risk levels were connected by establishing information asset risk database. Through the corresponding monitoring of company information, the risk probability of each system could be calculated automatically, and the corresponding risk prevention measures were put forward. The test results show that the system achieves the desired results.

**Keywords** Risk assessment Evaluation of grade protection Information security

## 0 引 言

随着互联网技术的不断发展,网络系统应用于社会的各个方面,但是信息安全问题日益突出,公司紧紧依靠单一的病毒防护软件无法安全有效地保护系统内部信息资产的安全。风险评估技术已广泛应用于信息系统安全风险检测过程中,许多单位已建立完善的风险评估体系,风险评估已成为部分单位信息安全工作的重要措施之一。随着《中华人民共和国网络安全法》的正式实施,国家对实施网络安全等级保护的要求日趋严格,相关主管部门对实施等级保护测评工作也越来越重视。因此,如何保证在等级保护测评中真实地反映信息系统存在的信息安全风险,成为等级保护测评中一个非常迫切的需求[1]。

为了对信息安全进行行之有效的保护,设计了一种基于风险评估和安全等级相结合的网络信息保护平台,整个平台通过建立信息资产风险库,将信息资产进

收稿日期:2018-08-12。任贝贝,高工,主研领域:等级保护测评。

行风险等级划分。通过对网络内的所有信息数据进行检测,及时测算每个系统的风险概率,对风险等级高的系统提出预警和提出改进建议。

# 1 信息系统安全测评理论研究

## 1.1 风险评估

信息安全风险评估是以信息资产为核心,鉴别存在的脆弱性以及可能利用脆弱性的威胁。结合现有的安全措施,分析存在的安全风险,并选择切合实际的安全措施,使安全风险降低到组织可以接受程度的过程。风险评估贯穿于信息系统的管理、操作及维护过程中,评估人员要获得充分的、可靠的、有关的证据[2],以有效完成评估目标。同时,对获取的证据进行合理、准确地分析和解释,以支持评估结果和结论。

风险评估过程涉及的关键要素包括资产、脆弱性、威胁、风险、安全措施等[3],各要素之间存在密切的相互联系。风险评估要素关系模型如图 1 所示。

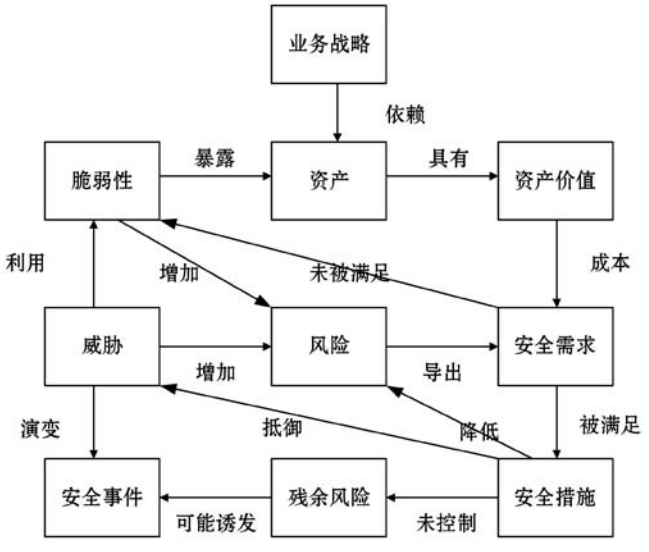


图 1 风险评估要素关系模型

## 1.2 等级保护

等级保护指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护,对信息系统中使用的信息安全产品实行按等级管理[4],对信息系统中发生的信息安全事件分等级响应、处置。它是国家信息安全保障的基本制度、基本策略、基本方法。

根据信息系统重要程度,结合受损害的客体及损害程度确定了等级保护定级原则,共为五个等级:第一级为自主保护级;第二级为指导保护级;第三级为监督保护级;第四级为强制保护级;第五级为专控保护级[5]。

## 1.3 两者关联的必要性

信息系统中包含着大量的公司机密代码,因此成为了大量黑客和病毒的攻击对象。多年实践证明依靠单一的防御手段无法保证在新型攻击来临之时起到有效的防护作用。而且由于一个公司系统业务流程比较复杂,因此系统需要维护的部分各不相同。不同的部分在系统中的作用不同,需要防护的手段和流程都不相同,系统中的每一个部分的维护都需要进行科学化分析[6],因此需要根据不同部分在系统中的作用划分等级。如果对系统中的每个部分按照相同的科学分析方法、相同的资源配置以及同等规格的等级进行风险预防,会对资源造成不必要的浪费,也无法对需要重点保护的系统进行有效的防护。由于在系统的整个生命周期过程中需要不断地对系统进行风险评估,将风险评估和等级防护相结合可以根据系统部件等级以及风险程度对整个系统的防护资源进行综合分配,使得整个系统的防护资源利用得到最大化[7]。因此在等级保护测评中合理、有效地应用风险评估手段,显得尤为重要。

# 2 系统需求和设计

## 2.1 功能需求

根据信息系统评估流程以及公司内信息系统的流程划分,整个信息系统平台功能图如图 2 所示。

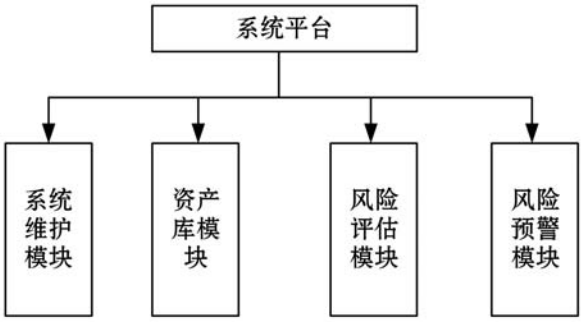


图 2 信息系统平台功能图

系统维护模块主要负责对系统的使用人员进行管理员权限的分配,账号、密码的设置以及系统信息的维护。资产库模块负责对整个系统的单个模块进行数据管理,单条数据的增删改查以及资产库中的数据维护等功能。风险评估模块用来对系统中的子系统的风险等级、风险参数以及网络情况进行检测,并实时展示该子系统的风险评估参数。风险预警模块的作用为当某一个子系统面临高风险的时候会发出警报,并分析风

险原因,展示可能应对的风险处理手段。

### 2.2　性能需求

风险评估软件在开发的过程中需要具备以下两个方面的性能需求。

1）安全性需求:一所公司,尤其是大型公司包含大量的人员信息。人才作为公司无形的资产起着关键的作用,因此需要安全保护。数据库作为系统的一个部分,存储着公司的审计信息等相关财务信息尤其是和用户进行交互的公司。比如旅游网络公司的数据库中包含大量的用户信息以及用户的银行卡信息,一旦泄露出去将会对公司造成无法挽救的损失,因此系统的安全性能一定要好。

2）系统性能需求:为了保证用户的使用感受,需要系统满足用户体验感受最低要求。因此对整个系统提出如下要求:(1) 在响应时间上应保持一定的响应的速度,例如用户对数据进行添加的时候系统应该在 2 s 内进行响应;(2) 提供可视化的界面,使得用户可以对操作系统进行直观、便捷的使用;(3) 查询信息的准确性,整个系统要保证展示在用户面前的每一条信息都是准确的,准确性是一个系统的最低保障需求。

### 2.3　总体架构及流程

本系统采用 ASP. NET 技术,浏览器使用任意浏览器,考虑到各个浏览器之间的差异,以 IE 浏览器为标准,操作系统为 Windows 操作系统,使用 IIS 作为前端服务器,选择 SQL 作为后台数据库,前端界面使用 HTML 语言进行编写[8]。整个系统的架构如图 3 所示。

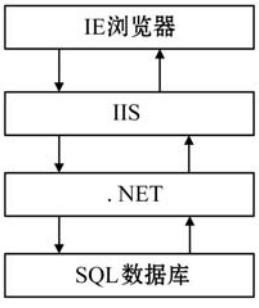


图 3　系统架构

整个系统按照使用顺序进行流程解析,系统使用流程图如图 4 所示。

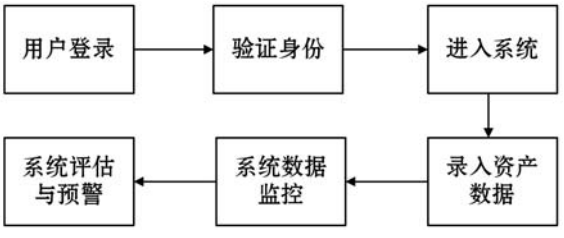


图 4　系统使用流程图

从图 4 可知,在系统使用过程中用户首先要输入账号、密码进行身份验证,身份验证通过才可以向系统资产名单中对信息资产进行增删改查[9]。系统数据在录入的过程中要选择对应的等级,同时系统会对资产数据库中的资产进行数据监测和风险评估,并对高风险资产进行预警以及应对方法提示。

## 3　系统研究与实践

### 3.1　维护模块

系统维护模块是整个系统的权限管理中心,也可以称为系统的主界面。整个系统的层次设计结构如图 5 所示。

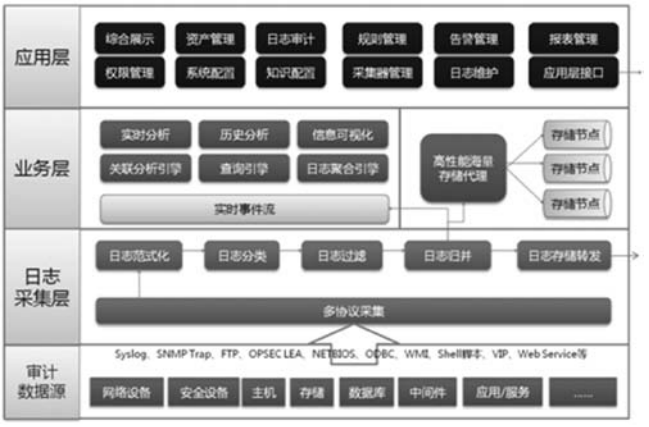


图 5　系统层次设计架构图

如图 5 所示,整个系统平台划分为应用层、业务层、日志采集层和审计数据源层 4 个部分。应用层主要负责界面展示、规则管理(权限管理等)、资产报表管理等。业务层负责根据风险评估和等级防护原则对资产进行分析和管理。日志采集层负责对日志信息进行管理,并且负责将实时采集到的系统信息状况进行日志记录。审计数据源层负责数据的存储、数据管理等。系统维护模块界面图如图 6 所示。

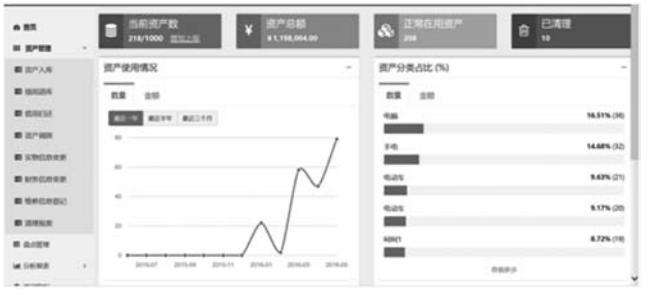

图 6　系统维护模块界面图

### 3.2　资产风险库模块

资产风险库模块主要负责对公司内所有的固定资产和非固定资产信息进行录入、删除等功能。资产风险路模块信息界面如图 7 所示。

图 7 资产风险路模块信息界面图

从图 7 可以看出,资产信息的主要录入内容包括物品名称、物品使用者、物品的存放地址等信息,并且可以通过物品编号和物品状态等多种信息对资产进行查询。

### 3.3 单个系统分支监控模块

单个系统分支监控模块主要对整个系统中的层级进行划分。比如公司内包含的财务网络系统可以作为单个模块来检测。整个系统的模块划分结构如图 8 所示。

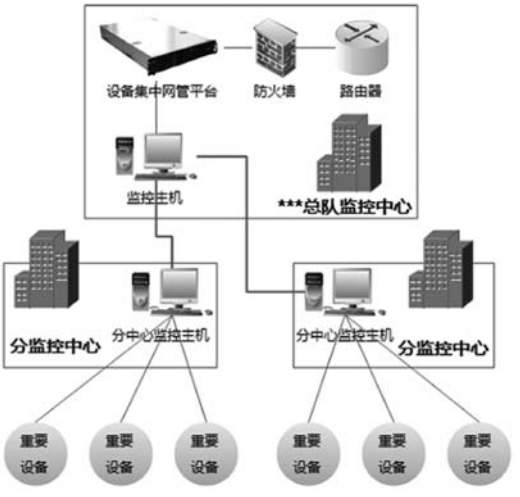


图 8 系统单个模块划分架构图

从图 8 可以看出,整个公司按照层级划分,总队监控系统包含监控主机、设备网管平台等对公司的各个部门进行监控。分监控中心将各个部门的重要设备信息通过分中心监控主机回传给总队监控中心,实现了整个系统平台对一个大公司内部所有的信息模块进行监控。每一个重要设备就是信息模块监控的一个分支,总队监控中心可以统一对单个系统分支的任意模块监控信息进行查阅。

### 3.4 风险评估预报及建议模块

风险评估模块主要负责将单个模块的风险评估情况进行输出和展示。按照等级防护原则对高风险的系统进行预警,预警情况划分为五个等级:自主保护级系统风险高于 85% 进行预警;指导保护级系统风险高于 75% 进行预警;监督保护级系统风险高于 65% 进行预警;强制保护级系统风险高于 50% 进行预警;专控保护级系统风险高于 35% 进行预警,并通过后台数据库进行连接展示可能解决该风险问题的手段。

## 4 结 语

本文为了提高公司信息系统风险抗击能力,对抗现代互联网层出不穷的系统攻击,设计了一种基于风险评估和等级防护相结合的风险等级防护系统。整个系统对公司内所有资产进行录入管理,通过对公司内信息网络的监测,根据设备等级进行资产风险评估。现有系统会对有风险的资产进行预警并提出相关的建议,后期可将系统内容进行扩展使得系统可以对常规风险进行自动化处理。

## 参 考 文 献

[1] 邱意民. 风险评估在安全等级保护测评中的应用[C]//电力通信管理暨智能电网通信技术论坛. 2013.

[2] 袁静, 毕马宁, 江雷,等. 谈风险评估方法在等级测评中的进一步运用[C]//全国信息安全等级保护技术大会. 2014.

[3] 黄洪. 信息系统安全评估方法和技术研究[D]. 成都:四川大学, 2005.

[4] 周英. 信息系统风险评估中几点关键技术的研究[D]. 青岛:中国海洋大学, 2008.

[5] 文伟平, 郭荣华, 孟正,等. 信息安全风险评估关键技术研究与实现[J]. 信息网络安全, 2015(2):7-14.

[6] 刘莹. 基于知识库的信息安全风险评估技术研究与软件实现[D]. 济南:山东轻工业学院, 2009.

[7] 韩权印. 基于 BS7799 的信息安全风险评估研究与设计[D]. 西安:西安电子科技大学, 2005.

[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.

[9] 覃萍. 信息安全风险评估技术与应用[D]. 北京:北京邮电大学, 2007.

(上接第 84 页)

[11] 罗明, 施云飞. 体绘制中传递函数的研究[J]. 信息通信, 2018(3): 11-12.

[12] Kruger J, Westermann R. Acceleration techniques for GPU-based volume rendering[C]//Proceedings of the 14th IEEE Visualization 2003(VIS'03). IEEE Computer Society,2003: 38.

[13] Peng T, Cao J. Time slicing and arbitrary horizon extraction algorithm and implementation of 3D SEGY seismic data volume[C]//IEEE Fifth International Conference on Bio-Inspired Computing: Theories and Applications. IEEE, 2010: 981-984.