

一种基于层次分析法的大规模信息系统风险评估方法

李晨旻* 张晓梅 李媛
(北京信息安全测评中心 北京 100101)

摘 要 大规模信息系统涉及到的资产种类多、数量多、分布范围广且网络结构复杂,在相关风险评估及等级测评实践中遇到了效率低下、结果不全面、灵活性差等问题。提出一种基于层次分析法的大规模信息系统风险评估方法。该方法结合大规模信息系统的特点,以层次分析法为基础,引入节点分类、风险调整等流程实现了定性与定量相结合的风险评估,有效解决了上述问题,为大规模信息系统的风险评估及等级测评工作提供了方法,同时为提高大规模信息系统等级测评的结果判定的准确性提供了思路。

关键词 大规模信息系统 风险评估 层次分析法 等级测评

中图分类号 TP319 文献标识码 A DOI:10.3969/j.issn.1000-386x.2013.10.087

A LARGE-SCALE INFORMATION SYSTEM SECURITY RISK ASSESSMENT METHOD BASED ON ANALYTIC HIERARCHY PROCESS

Li Chenyang* Zhang Xiaomei Li Yuan
(Beijing Information Security Test and Evaluation Center, Beijing 100101, China)

Abstract The diverse category, large quantity and wide distribution of the assets are what the large-scale information system involved in, its network structure is complex as well, in the practice of related risk assessments and rank evaluation, it encounters the problems of low efficiency, incomprehensive result and poor flexibility, etc. In this paper, we present an AHP-based large-scale information systems risk assessment method. With the characteristics of large-scale information system combined, this method takes analytic hierarchy process as the basis, and introduces the processes including node classification and risk adjustment to have implemented the risk assessment with qualitative and quantitative combination. The method effectively resolves the problems listed above and provides an approach for risk assessments and rank evaluation of large-scale information system. Meanwhile it also provides a thought for improving the accuracy of the results judgement on the rank evaluation of large-scale information system.

Keywords Large-scale information system Risk assessment Analytic hierarchy process (AHP) Rank evaluation

0 引 言

伴随着网络的高速发展,信息系统特别是大规模信息系统被越来越多地应用到各行各业中,而风险评估作为保障信息系统安全的重要手段,也受到人们的广泛关注。风险评估方法一般包含资产识别、威胁识别、脆弱性识别及风险分析等过程,而风险评估方法的选择将直接影响评估结果的准确性。常见的评估方法可分为定性的评估方法、定量的评估方法、定性与定量相结合的评估方法。作为等级测评结果判定的重要方法,风险评估的结果也影响到等级测评结果的准确性。

大规模信息系统涉及到的资产种类多、数量多、分布范围广且网络结构复杂,在相关风险评估及等级测评实践中遇到了效率低下、结果不全面、灵活性差等问题,亟待引入新的风险评估流程和方法。目前,已有一些针对大规模系统的风险评估方法的研究,如文献[1]中提出的动态风险评估方法强调了各要素的量化方法,文献[2]中提出的 HRAM 风险评估模型强调了安全事件的获取技术。然而上述研究成果仍存在评估流程不规范、实施复杂等问题。本文提出了一种基于层次分析法的大规

模信息系统风险评估方法,该方法结合大规模信息系统的特点,以层次分析法(AHP)^[3]为基础,引入节点分类、风险调整等流程实现了定性与定量相结合的风险评估,可为测评机构开展大规模信息系统的风险评估及等级测评提供参考。

1 大规模信息系统风险评估中存在的问题

近年来,业务信息系统朝着大规模、分布式的方向发展,许多大规模信息系统都采用了“骨干节点-分支节点”的方式部署,即核心业务应用主要部署于少量骨干节点,大量分支节点主要用于承载客户端访问等简单功能。与骨干节点相比,分支节点结构往往相对简单,且大量分支节点的网络结构及资产类型基本相同。此类大规模信息系统往往具备以下特点:

- 1) 涉及的资产数量大、种类多^[4],承载的业务类型复杂;
- 2) 分支节点的同构性强,部署范围广泛^[4],大多仍需进行独立的管理运维;

收稿日期:2012-08-14。李晨旻,工程师,主研领域:安全测评,应用安全,网络安全。张晓梅,助理研究员。李媛,工程师。

3) 系统发生变化的频率相对较高,系统中每个资产和业务的变化都对系统整体造成一定的影响。

大规模信息系统的上述特点,导致在风险评估实践中存在以下问题:

1) 评估工作效率不高。大规模系统资产数量较大且分布广泛,带来了大量的脆弱性采集分析工作,按照传统风险评估方法针对资产或层面逐一进行全面的脆弱性分析和威胁分析效率较低,而分支节点的同构性较强也导致采集分析过程中存在大量重复性工作;

2) 评估结果不全面。传统风险评估方法往往更关注系统整体的风险分析,而忽略各节点的风险分析,导致评估结果无法直接应用于系统各节点的风险管理工作;

3) 评估流程灵活性差。大规模信息系统发生变化的频率较高,往往需要快速评估变化后的系统风险。而传统风险评估方法未对系统发生变化之后的风险调整过程进行明确的规定,无法规范、快速、准确地评估变化对系统整体风险的影响。

针对上述问题,本文提出了一种基于层次分析法的大规模信息系统风险评估方法。

2 基于层次分析法的大规模信息系统风险评估方法

基于层次分析法的大规模信息系统风险评估方法流程如图 1 所示。

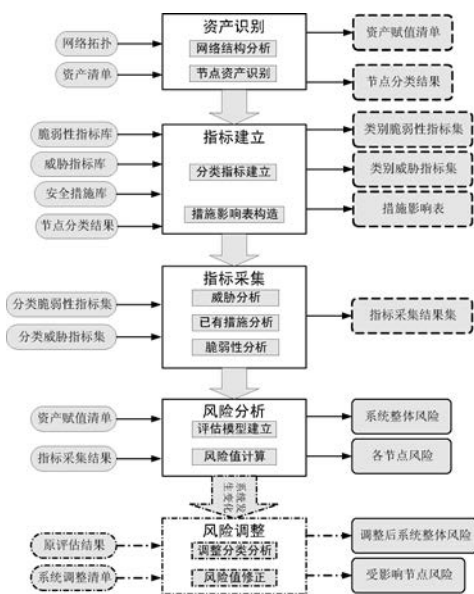


图 1 评估方法流程图

方法实施流程包括资产识别、指标建立、指标采集、风险分析以及当系统发生变化时进行的风险调整。该评估方法首先利用分支节点的同构性特点将节点分类;之后根据每类节点的资产特征按类别建立脆弱性指标集和威胁指标集,以减少脆弱性及威胁分析的工作量,提高评估效率;最后采用层次分析法,构造系统总体-节点-资产层次模型,对系统整体和各节点进行风险分析。当系统发生变化时,则基于原风险评估结果快速准确的进行风险调整。

2.1 资产识别

资产是信息安全风险的主要构成要素之一,资产识别环节的目标是识别处于风险中的资产及其重要性,其结果将作为风

险分析过程的重要输入直接影响结果的准确性^[5]。大规模系统涉及到的资产种类多、数量多、分布范围广,需要对资产进行合理分类并体现出资产之间的关联和层次。资产识别环节包含以下步骤:

(1) 网络结构分析

大规模系统的承载网络多为广域网,资产以分布式方式部署在多个节点中。网络结构分析的目标是通过分析系统拓扑图、设计文档等静态资料,明确系统各节点之间的连接方式、层次关系、业务关联及节点在系统中的重要性,并将网络结构相同、资产类型及数量相近的节点归类。

为了便于计算系统的风险,需要为节点在系统中的重要性等级赋值。这里,节点的重要性定义为节点内的资产和服务遭到破坏后对大规模信息系统整体造成的影响程度,并将节点重要性分为 5 级:5(高)、4(较高)、3(一般)、2(较低)、1(低),用 p_{n_i} 表示节点 n_i 的重要性等级赋值。

(2) 节点资产识别

对各节点中的资产进行梳理,并结合节点重要性及资产自身在保密性、完整性、可用性方面的安全要求,确定资产在所属节点中的重要性等级赋值。这里,资产的重要性定义为资产遭到破坏后对所属节点造成的影响程度,并将资产重要性等级分为 5 级:5(高)、4(较高)、3(一般)、2(较低)、1(低),用 p_{z_j} 表示资产 z_j 的重要性等级赋值。

资产识别环节可获得节点重要性等级赋值结果、节点分类结果、资产与节点的所属关系以及资产的重要性等级赋值结果。

2.2 指标建立

区别于传统风险评估方法,本评估方法在进行脆弱性分析及威胁分析之前,先基于上一环节中的节点分类结果为每个节点建立脆弱性指标集及威胁指标集^[6],而避免对所有节点的所有资产逐一进行全面的脆弱性和威胁分析,以提高评估效率。指标建立环节包含以下步骤:

(1) 分类指标建立

首先建立包含常见脆弱性的脆弱性指标库及包含常见威胁的威胁指标库。指标库可通过参考专家经验、参考标准等方法建立或采用已有知识库,本方法以《信息安全等级保护基本要求》^[7](GB/T 22239-2008)中的各级基本要求作为脆弱性指标库。

之后依据“资产识别”环节中产生的节点分类结果建立指标集。取节点类别 c_m ,并抽取类别中的 1~2 个节点。根据节点包含资产从指标库中选取适用的脆弱性指标和威胁指标,并对脆弱性严重程度及威胁等级赋值。其中,脆弱性按其严重程度划分为 5 级:5(高)、4(较高)、3(一般)、2(较低)、1(低);威胁综合其发生可能性及破坏程度划分为 5 级:5(严重)、4(较严重)、3(一般)、2(较不严重)、1(不严重)。这里,脆弱性 v 的严重程度等级赋值用 s_v 来表示,威胁 t 的等级赋值用 q_t 来表示。选取的脆弱性指标及其严重性等级赋值、威胁指标及其等级赋值组成节点类别 c_m 的类别脆弱性指标集 V_m 及类别威胁指标集 T_m 。最终得到所有节点类别的脆弱性指标集合及威胁指标集合,分别用 V 和 T 来表示。

(2) 措施影响矩阵构造

已有安全措施能够降低脆弱性为系统带来的安全风险,这里将安全措施的影响定义为安全措施对脆弱性严重程度的影响程度。为了高效地评估这一影响,可在脆弱性分析之前采用如

下方法构造“措施影响表”:

Step1 采用参考专家经验等方式建立包含及时更新补丁、明确的访问控制策略等常见安全措施的“安全措施库”,并对各措施编号;

Step2 结合脆弱性指标库构造如下“措施影响表”,其中 e_{ij} 表示第 i 个防护措施对第 j 条脆弱性严重程度的影响值:

$$\begin{bmatrix} e_{11} & e_{12} & \cdots & e_{1x} \\ e_{21} & \cdots & \cdots & \cdots \\ \cdots & \cdots & e_{ij} & \cdots \\ e_{y1} & \cdots & \cdots & \cdots \end{bmatrix}$$

(1)

其中 $e_{ij} \geq 0$ 且 $e_{ij} < s_j$ 。

针对具体系统进行评估时,可调整矩阵中的值。

2.3 指标采集

指标采集环节将依据各类别的脆弱性指标集合及威胁指标集合进行所有资产的威胁分析、已有措施分析及脆弱性分析,记录确实存在的脆弱性及其关联威胁。采集的方法包括访谈、配置检查、日志分析、工具探测等,这里不再赘述。

系统存在的所有脆弱性及其关联威胁将构成指标采集结果的集合 U ,一条指标采集结果将包含节点、资产、脆弱性、威胁及关联的已有安全措施的信息。于是,如果节点 n_i 中部署的资产 z_j 存在脆弱性 v ,可能被威胁 t 利用,与已有安全措施集合 M (如无相应措施则记为0)相关,该条指标采集结果 u_k 可表示为:

$$u_k = (i, j, v, t, M)$$

(2)

2.4 风险分析

资产识别、指标建立及指标采集环节完成后,需要采用适合的方法分析集合 U 中的每一条指标采集结果为相关节点及系统整体带来的风险。这里,采用层次分析法^[2,3,8]逐步计算和分析指标采集结果、资产、节点及系统整体的风险值。

(1) 评估模型建立

资产识别环节中对资产、节点及系统的关系进行了分析,可建立如下的层次分析模型:



图2 风险评估层次分析模型

可以看出,采用该模型可以获得各资产、节点及系统的总体风险。

(2) 风险值计算

下面依次计算单个指标采集结果、单个资产、单个节点以及系统总体的风险值。

Step1 计算单个指标采集结果的风险值

单个指标采集结果 u_k 的风险与结果中的脆弱性 v 、关联的威胁 t 及已有安全措施 m 均相关。如前文所述,已有安全措施可降低相关脆弱性为系统带来的风险,这里定义脆弱性实际严重程度等级赋值以量化安全措施带来的影响,脆弱性 v 的实际严重程度等级赋值 s_v^* 可表示为:

$$s_v^* = s_v - \text{Max}(e_{1v}, e_{2v}, \cdots, e_{mv})$$

(3)

其中, s_v 表示脆弱性 v 的严重程度等级赋值; $\text{Max}(e_{1v}, e_{2v}, \cdots, e_{mv})$ 为与其关联的措施集合 M 中各安全措施对脆弱性 v 的影响

值中的最大值,可通过查询措施影响表得到,如无相应措施则为值0。

于是,单个采集结果 u_k 的风险 r_{u_k} 表示为:

$$r_{u_k} = s_v^* \times q_t = [s_v - \text{Max}(e_{1v}, e_{2v}, \cdots, e_{mv})] \times q_t$$

(4)

其中, q_t 表示脆弱性关联的威胁 t 的威胁等级赋值。

Step2 计算单个资产的风险值

按照层次分析模型,单个资产的风险值由与其相关的各指标采集结果的风险值决定。简单起见,这里假设各指标采集结果的风险相互独立且对所属资产风险值的影响程度相同,于是是一个与 $|U|$ 个指标采集结果相关的资产 z_j 的风险值用所有相关指标采集结果风险值的算术平均值来表示:

$$r_{z_j} = \frac{\sum_{k=1}^{|U|} r_{u_k}}{|U|}$$

(5)

Step3 单个节点的风险值

以此类推,单个节点的风险值由节点中的所有资产的风险值决定。由3.1节的描述可知,资产 z_j 在所属节点中的重要程度由其重要性等级赋值 p_{z_j} 来表示,可以用该值表示资产风险值对所属节点风险的影响程度。于是,一个包含 Z 个资产的节点 n_i 的风险用所有相关资产风险的加权平均值来表示:

$$r_{n_i} = \frac{\sum_{j=1}^Z p_{z_j} \cdot r_{z_j}}{\sum_{j=1}^Z p_{z_j}}$$

(6)

Step4 系统总体风险值

同理,系统总体风险值由所有节点的风险值决定,包含 N 个节点的系统的总体风险值 r_s 用所有节点风险值的加权平均值来表示:

$$r_s = \frac{\sum_{i=1}^N p_{n_i} \cdot r_{n_i}}{\sum_{i=1}^N p_{n_i}}$$

(7)

至此完成系统安全风险的分析。系统总体风险值、节点风险值及资产风险值的取值范围相同,可通过比较风险值的大小来比较大规模系统各组成部分的风险高低。

在等级测评实践中,也可对标准符合性检测结果进行上述风险分析,以风险分析结果作为结果判定的依据,提高等级测评结果判定的准确性。

2.5 风险调整

当大规模信息系统发生变化时,可通过“风险调整”环节评估各种变化对系统安全风险造成的影响。

按照系统发生变化的对象和范围,这里分三种情况调整系统的安全风险值:

(1) 增加节点或资产

当系统中新增节点或资产时,需针对新增部分进行资产识别、指标建立及指标采集,综合原有各级风险值及新增指标采集结果,计算新增指标采集结果、资产及受影响节点的风险值,最终重新计算系统总体风险。

(2) 减少节点或资产

当系统中的节点或资产减少时,在重新计算受影响节点的风险值时去除相应资产的风险值、或在计算系统总体风险时去除相应节点的风险值即可。

(3) 调整防护措施

防护措施调整是指在不改变现有资产的情况下进行的系统调整,例如数据库升级方式变更等。此类调整往往是针对风险评估后发现的脆弱性进行整改,可能降低风险评估中发现的脆弱性带来的风险。可采用以下步骤评估调整措施的影响:

① 查找措施影响表及原系统的指标采集结果集合,确认与调整措施相关的脆弱性,将措施添加至关联的指标采集结果中;

② 重复 3.4 节 Step 1,重新计算相关采集结果的风险;

③ 所有调整措施相关的指标采集结果风险值计算完成后,重新计算受影响资产、受影响节点及系统总体的风险值。

3 结 语

针对大规模信息系统风险评估及等级测评实践中存在的效率低、结果不全面、灵活性差等问题,本文提出了一种基于层次分析的大规模信息系统风险评估方法,该方法具有以下特点:

1) 利用大规模信息系统节点的同构性特点进行分类评估,减少了重复的工作量,提高了评估效率;

2) 建立了层次分析模型,风险评估后获得系统总体风险的同时,可获得各节点、各资产的风险以及相互影响关系,便于后期进行风险管理;

3) 增加了风险调整环节,规范了系统发生变化后进行局部重新评估的过程,便于高效、准确地评估系统变化对安全风险的影响。

因此,基于层次分析的大规模信息系统风险评估方法具有较好的可操作性,为大规模信息系统的风险评估及等级测评工作提供了方法,同时为提高大规模信息系统等级测评的结果判定的准确性提供了思路。

参 考 文 献

[1] 赵阳,范红,等. 面向等级保护的大规模网络动态风险评估方法研究[J]. 信息安全,2007(8):19-21.

[2] 郑兆娜. 基于大规模网络的安全风险评估研究[D]. 济南:济南大学,2011.

[3] Satty T L. The Analytic Hierarchy Process[M]. NewYork, USA: McGraw-Hill Companies,1980.

[4] 金瀚,李为. 大型等级测评项目实施探讨[J]. 信息安全,2011(增刊):35-37.

[5] 向宏,傅鹏,詹榜华. 信息安全测评与风险评估[M]. 北京:电子工业出版社,2009.

[6] 杨继华. 信息安全风险评估模型及方法研究[D]. 西安:西安电子科技大学,2007.

[7] GB/T 22239-2008. 信息安全技术信息系统安全等级保护基本要求[S].

[8] 陈秀真,郑庆华,等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报,2006(4):885-897.

(上接第 228 页)

两种情况仿真输出数据对比,如表 5 所示。

表 5 输出数据对比表

截取时间点	L—A 未实施引导策略疏散人数	L—A 实施引导策略疏散人数
1 分 00 秒	150	180

截取时间点	L—A 未实施引导策略疏散人数	L—A 实施引导策略疏散人数
2 分 00 秒	456	572
3 分 30 秒	680	750
疏散总时间(1750 人)	9 分 14 秒	8 分 34 秒

2.4 结果分析与对策

仿真中通过引入 Lead-Agent 角色研究应急疏散人群中有引导和组织角色时对疏散的影响。通过上述仿真和数据分析发现:

1) 地铁站内部 L-A 引导,使大家行动更为一致和有序,能够改善疏散的效果,提高疏散效率。通过两次仿真中同一时间点截图对比,发现当 L-A 实施引导策略时,人群聚集度更大,落后于整体的 Agent 的数目减少。说明人群在 L-A 的正确引导和语言激励下,能快速找到疏散路径,同时缓解恐慌情绪、增加成功疏散的信心,于是对整个疏散效果有正面的影响。

2) 疏散中的连续疏散状态一般发生在中间阶段,离散状态呈现在地铁内疏散行动的初始阶段和最后阶段。这两个阶段是寻求缩短疏散时间的目标阶段。

3) 疏散开始到接近尾声,地铁车站的两侧的楼梯处和四个出口处的狭小区域出现了人群滞留的现象,这种现象一直持续到疏散基本完成。楼梯和出口的位置、数量和有效宽度的地铁站内防火设计是需要考虑的点。

4) 地铁站内疏散的总时间取决于站内人群中恐慌者的反应和行动速度。如果这部分恐慌者能够在一定程度上减短反应时间,增加行动力,可大大减短疏散时间。

3 结 语

本文构建了多 Agent 系统交互的地铁内人员应急疏散的模型,弥补了其他研究成果只关注疏散中个体的心理反应和行为特征的片面性,建立 L-A、O-A、A-A 三个角色,强调了疏散中群体的作用,并对角色提供的信息引导和协调对疏散效果的影响进行仿真和分析。本文的研究能够为建筑物内尤其是客运站等场所的人员应急疏散及相关领域的研究提供一定的参考价值,并在应急疏散实践中具有指导意义。

参 考 文 献

[1] Dirk Helbing, Peter Molnar. Social force model for pedestrian dynamics[J]. Physical Review E,1995,51(5):4282-4286.

[2] Dirk Helbing,Illes J Farkas, Tamas Vicsek. Simulating dynamical features of escape panic[J]. Nature (S0028-0836),2000,407(28):487-490.

[3] Khatib O. Real-time obstacle avoidance for manipulators and mobile robots[J]. International Journal of Robotics Research,1986,5(1):90-98.


[4] 方正,卢兆明. 建筑物避难疏散的网格模型[J]. 中国安全科学学报,2001,11(4):10-13.

[5] 崔喜红,李强,陈晋,等. 基于多智能体技术的公共场所人员疏散模型研究[J]. 系统仿真学报,2008,20(4):1006-1010,1023.

[6] 黄希发,等. 基于 Agent 技术的人员疏散微观仿真模型研究[J]. 系统仿真学报,2009,21(15):4568-4582.

[7] 徐高. 基于智能体技术的人员疏散仿真模型[J]. 西南交通大学学报,2003,38(3):301-304.

一种基于层次分析法的大规模信息系统风险评估方法

作者: [李晨昶](#), [张晓梅](#), [李媛](#), [Li Chenyang](#), [Zhang Xiaomei](#), [Li Yuan](#)
作者单位: [北京信息安全测评中心](#) 北京 100101
刊名: [计算机应用与软件](#) 
英文刊名: [Computer Applications and Software](#)
年, 卷(期): 2013(10)

参考文献(8条)

1. [赵阳;范红](#) [面向等级保护的大规模网络动态风险评估方法研究](#)[期刊论文]-[信息安全](#) 2007(08)
2. [郑兆娜](#) [基于大规模网络的安全风险评估研究](#) 2011
3. [Satty T L](#) [The Analytic Hierarchy Process](#) 1980
4. [金瀚;李为](#) [大型等级测评项目实施探讨](#) 2011(增刊)
5. [向宏;傅鹏;詹榜华](#) [信息安全测评与风险评估](#) 2009
6. [杨继华](#) [信息安全风险评估模型及方法研究](#)[学位论文] 2007
7. [信息安全技术信息系统安全等级保护基本要求](#)
8. [陈秀真;郑庆华](#) [层次化网络安全威胁态势量化评估方法](#)[期刊论文]-[软件学报](#) 2006(04)

本文链接: http://d.g.wanfangdata.com.cn/Periodical_jsjyyrj201310088.aspx