广西科学院学报
Journal of Guangxi Academy of Sciences
2006,22(4):364～366
Vol. 22,No. 4 November 2006

一种面向业务的信息安全风险评估方法*

A Risk Assessment Method for the Security of Applied Systems

詹 锋
ZHAN Feng

(广西大学计算机与电子信息学院,广西南宁 530004)
(School of Computer, Electronics and Information, Guangxi University, Nanning, Guangxi, 530004, China)

摘要:根据信息安全风险评估理论提出一种面向业务的风险评估方法。该方法明确将各类业务系统作为整体安全对象进行风险评估,并应用"故障树"方法对业务系统进行风险建模和风险计算。该方法是一种行之有效,易于操作的安全评估方法。

关键词:信息安全风险评估 故障树方法
中图法分类号:TP309.1 **文献标识码**:A **文章编号**:1002-7378(2006)04-0364-03

Abstract: A risk evaluation method for applied systems in security is presented in terms of risk assessment knowledge of information systems. In this method, any applied system is considered as a whole object in security to be assessed. The "Fault tree analysis" is used to setup a risk model and to do risk calculation. The method is applied to concrete project of security evaluation. The result reveals that it is effective and easy in operation.

Key words: information security, security evaluation, Fault Tree analysis

随着社会和各行业信息化进程的加快,信息安全建设越来越受到重视。由于信息系统的安全性可以通过风险的大小来度量,目前的主流信息安全解决方案都以风险管理为核心。作为风险管理的起点,安全风险评估对于了解安全现状,明确安全目标,制定安全对策都具有至关重要的意义。本文在介绍风险评估相关知识的基础上,借鉴"故障树"的自顶向下分析方法,并结合信息安全评估工作经验,提出一种面向业务的风险评估方法,并对其实际运用效果进行了介绍。

1 安全风险评估概述

1.1 风险评估过程

开展信息安全风险评估需要理论的指导。风险评估理论主要包括风险计算模型、风险评估方法等等。其中风险计算模型描述了形成风险的各个要素,是风险评估的基本理论依据。在国内外的风险评估参考标准[1～4]和实际工作中,以"资产—威胁—脆弱性"(Asset-Threat-Vulnerability)为核心的风险计算模型被广泛推荐和采用,这一模型如图1所示,从左至右的有向线段表示了计算各类信息资产风险值的过程。

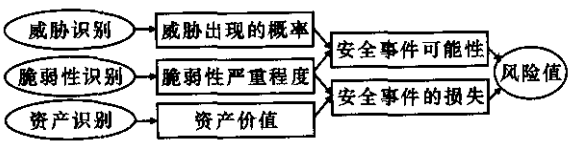

图1 通用风险计算模型示意

图1所示的风险模型显示风险评估要解决的主要问题是根据信息资产的价值、资产所受威胁以及资产自身的脆弱性来计算资产风险值。根据"资产—威胁—脆弱性"风险计算模型,可以得出风险评估的主要过程为:(1)根据评估范围和系统目标、系统特性确立评估对象;(2)通过调查获取各类风险要素,

收稿日期:2006-07-17
作者简介:詹 锋(1979-),男,硕士,广西武鸣人,助教,主要从事信息安全研究。
*广西留学回国人员科学基金项目(桂科回0342001)和广西科技攻关项目(桂科攻0385001)联合资助。

计算被评估对象的风险值。不同的安全风险评估实践大多遵循上述过程。

1.2　安全风险评估分析法

不同的安全风险评估方法在评估的具体实施手段和风险的计算方面各有不同。从实施手段来区分,有基于树的技术[5,6],动态系统的技术[7]等等。从计算方法来区分,有定性的方法、定量的方法和半定量的方法。以上的各种方法各有特色,但需要根据不同的系统灵活运用。故障树分析法 FTA(Fault Tree Analysis)[5,8]是一种自顶向下的风险分析法,最初来自工业设计分析领域,目前主要用于分析大型复杂系统,被公认为是对系统可靠性及安全性进行分析的有效方法。

2　面向业务的风险评估方法

2.1　面向业务的风险评估过程

面向业务风险评估的实施过程如图 2 所示。

图 2　面向业务的风险评估实施过程

2.2　业务对象分类

面向业务风险评估方法将各类业务系统直接作为安全评估对象,通过开展各类调查对业务系统风险做出评价。

在大型信息系统中,业务系统数量多,评估涉及范围广、难度大,而且不同业务系统的各个安全性要素互相覆盖,各自评估将导致评估工作内容的冗余和重复。比如信息系统所在地点的环境安全因素就对所有业务系统产生类似的影响。因此,有必要根据业务特点划分相应的业务类别,在评估过程中对某一类别中有代表性的业务进行重点评估。根据实际经验,业务系统的分类应该咨询业务专家,并充分考虑业务特点如数据安全要求、业务实时性要求、对整个系统的服务范围和影响力等因素。大多数信息系统可以按表 1 所示划分为四大类别(这里由于未涉及具体业务系统,故表中的信息并不完整,实际评估工作中的业务分类应该根据实际情况进一步细化)。

在进行了分类之后,可以根据业务专家经验从每一类别的系统中选取最重要的一两个系统进行重点评估,而对其余系统进行常规评估,达到"重点突出,兼顾全局"的目的。

表 1　业务分类示例

业务类别	业务及业务数据特点	安全要求
生产应用业务类	与核心业务运行有直接联系	业务实时性和可用性要求很高
财务营销业务类	处理机密的内部业务和机密数据	业务数据的机密性要求很高
管理信息业务类	办公自动化等管理信息业务	业务的可用性要求较高
对外开放业务类	直接对外部用户提供服务	有完整性和可用性要求

2.3　采用故障树方法分析和计算风险

在确立了评估对象也就是具体的业务系统之后,面向业务的安全风险评估方法引入了故障树方法,采用自顶向下的方式分解该业务系统可能出现的风险或故障,从而实现定性或定量的风险评估。

2.3.1　故障树分析

故障树分析过程如下:(1)故障树建模。首先将系统重大风险事件如系统完全失效作为树顶,称为"顶事件",然后按照演绎分析原则,从顶事件逐级向下分析各事件的直接原因事件,称为"基本事件",并根据事件间逻辑关系,用逻辑门符合连接上下事件,直至所要求的分析深度,最终形成逻辑关系图即故障树。(2)简化故障树,求出全部最小割集。所谓割集是风险树的若干"底事件",即故障树的叶子节点的集合,如果这些事件都发生,则顶事件发生。若在某个割集中将所含的底事件任意去掉一个,余下的底事件构不成割集,即不能使顶事件发生,则这样的割集成为最小割集。

根据故障树分析原理,在选定了某一业务系统作为评估对象后,就可以展开具体的调查评估工作,包括专家访谈、填写问卷、人工调查、工具扫描等等,从顶事件也就是重大风险开始逐级向下分析"资产—威胁—脆弱性"等各类风险要素作为中间事件或者底事件,当完成一颗故障树也就完成了一个业务系统的全部或部分风险要素的评估。

2.3.2　风险分析

在对故障树建模并求出最小割集之后,可以用选择定性或定量的方法对故障树进行风险分析,故障树的定性分析指的是通过求出的全部最小割集得到顶事件的全部故障模式,例如某些失效事件的可能方式以及各类风险的排序。定性分析常用来发现系统中最薄弱也就是风险最大的环节或部位,指导安全加固和强化。

故障树的定量分析指的是在已知"底事件"发生概率的情况下,通过逻辑关系得到"顶事件",即所分

析的重大风险事件的发生概率。定量分析的计算方法如下：

先设底事件 X_i 对应的失效概率为 $q_i(i=1,2,\cdots,n)$，n 为底事件个数，则最小割集的失效概率为：$P(m)=P(x_1\cap x_2\cap\cdots\cap X_m)=\prod_{i=1}^{m}q_i$，其中 m 为最小割集的阶数(即该割集所含底事件数目)。那么顶事件发生的概率为：$P(top)=P(y_1\cup y_2\cup\cdots\cup y_k)$，其中 Y_i 为最小割集，k 为最小割集的个数。

评估实践中往往采用定性分析和定量分析相结合的做法，对于需要重点评估的业务系统为了对风险值做更精确的估计可以采用定量分析。

以上是面向业务的风险评估方法采用故障树建模和风险计算方法对单个业务系统的风险评估过程，对整个信息系统的评估，可以采用类似的方式，先对每个业务进行风险值计算，再对整个系统进行故障树建模和计算，得出信息系统的整体风险值。

3 面向业务风险评估方法的特点和应用效果

3.1 特点

面向业务的风险评估方法具有以下的特点：(1)在确立评估对象时，明确以系统中的各类业务系统为单位，并通过业务对象分类以实现重点评估与常规评估相结合，提高评估效率；(2)在评估业务系统的风险时，将主要风险自顶向下分解形成“故障树”，同时加入针对该业务系统调查所获得的风险要素，最后倒推得出该业务系统风险值。

3.2 应用效果

面向业务风险评估方法在广西电网信息系统安全评估等项目中得到了实际应用，取得了较好的效果。实践证明，该方法有以下优点：(1)各类业务系统直接对应评估对象，比按部门或按网络分区划分评估对象更合理；(2)基于故障树的分析方法由于采用自顶向下分解问题的方式开展业务调查，利于不熟悉安全评估的业务专家配合安全评估工作；(3)割集分析法能够根据不同需要进行定性或定量的风险分析，较为灵活。

面向业务风险评估方法是一种行之有效，易于操作的安全评估方法。

4 结束语

本文根据安全评估理论中的经典模型，结合安全评估经验，提出了一种面向业务的风险评估方法，其特点在于将业务系统作为整体安全对象进行评估，并用故障树方法对业务系统风险模式进行建模和风险值分析。在实践运用中也证明了该方法的有效性，当然，本方法也存在一些问题，比如大型系统的故障树逻辑关系复杂，难以理解；在定量分析中某些底事件的发生概率难以确定等等。下一步将针对这些问题主要考虑分析方法的优化以及研究实现用于辅助该方法的自动评估工具系统。

参考文献：

[1] National Computer Security Center. Trusted network interpretation of the trusted computer system evaluation criteria[S]. NCSC-TG-005. 1987-07-31.

[2] ISO/IEC 15408-1:2005 Information technology-Security techniques-Evaluation criteria for IT security-Part 1:Introduction and general model[S].

[3] ISO/IEC 15408-2:2005 Information technology-Security techniques-Evaluation criteria for IT security-Part 2:Security functional requirements[S].

[4] ISO/IEC 15408-3:2005 Information technology-Security techniques-Evaluation criteria for IT security-Part 3:Security assurance requirements[S].

[5] GEYMAYR, J A B Ebecken, N F F. Fault-tree analysis: a knowledge-engineering approach[J]. IEEE Transactions on Reliability, 1995, 44(1):37-45.

[6] KENARANGUI R. Event-tree analysis by fuzzy probability[J]. IEEE Trans on Reliability, 1991, 40(1): 120-124.

[7] LEE W S, GROSH D L, TILLMAN F A. Fault tree analysis, methods, and applications-A review[J]. IEEE Transactions on Reliability, 1985, 34:33, 194-203.

[8] 范红，冯登国. 信息安全风险评估方法与应用[M]. 北京：清华大学出版社，2006：52-62.

(责任编辑：韦廷宗)