信息安全风险评估之资产评估案例实施[1]

石丹
北京邮电大学计算机科学与技术系，北京 (100876)
E-mail: shidan2006@hotmail.com

摘　要：本文给出了在信息安全风险评估中，如何进行资产评估的方法概述，并着重列举了一个针对电子邮件系统进行资产评估的实例，通过这个案例清晰直观的解析了信息安全风险评估中资产评估的步骤和方法。

关键词：信息安全，风险评估，资产识别，资产评估
中图分类号：TP393

1. 引言

信息安全风险评估过程过程，是对资产、威胁、脆弱性、潜在影响和现有安全措施进行识别、分析和评价，然后综合这些风险要素的评估结果，得出风险的评估结果。

资产是风险的第一评估要素，其他要素的评估都是以资产为前提的。也说就是，威胁评估是针对所关注资产面临的威胁，脆弱性评估是针对所关注资产自身的脆弱性，潜在影响评估是针对所关注资产失效时的负面影响，现有安全措施评估也是针对所关注资产已具备的安全措施。因此，资产评估的正确性和准确性对于后续的各风险要素及其综合评估的导向至关重要。信息安全的资产评估目的是为了明晰评估范围内与信息安全相关的资产清单、资产关系和资产价值。下文将给出一个具体的示例，阐述在信息安全风险评估中，如何进行资产评估。

2. 资产识别方法研究

信息资产作为信息系统的构成元素，分布十分广泛；不同信息资产的功能、重要程度也互不相同。因此需要对信息资产进行合理分类，分析安全需求，确定资产的重要程度。本部分的主要工作是在评估实施方案确定的范围之内，按照评估方案约定的方式，进行如下四项工作[1]。

1. 回顾评估范围之内的业务

回顾这些信息的主要目的是：帮助资产识别小组对其所评估的业务和应用系统有一个大致了解，为后续的资产识别活动准备。

2. 识别信息资产，进行合理分类

针对前一个活动中识别出来的每个主要业务或系统，识别完成业务或保证系统正常运转所必需的资产，并注明资产的类别。资产分类的目的是降低后续分析和赋值活动的工作量。

3. 确定每类信息资产的安全需求

在对资产进行合理分类之后，便可对每个资产类别进行安全需求分析（从机密性、完整性、可用性三个方面进行），而不是对每个资产进行安全需求分析。

4. 为每类资产的重要性赋值

在上述安全需求分析的基础上，按照一定方法，确定资产的价值或重要程度等级。

本课题得到国家高技术研究发展计划（863 计划）项目“面向下一代电信网的安全测试评估技术”（课题编号：2006AA01Z448）的资助。

3. 资产赋值方法研究

对资产进行赋值不仅需要考虑它本身的财物价值，还需要考虑他的损失可能会对业务造成的影响（如导致营业收入的减少或竞争对手得益等）[4] 。更重要的是要考虑资产的安全状况，即资产的机密性、完整性、

可用性等安全属性，对组织信息安全性的影响程度。资产赋值的过程也就是对资产在机密性、完整性和可用性上的要求进行分析，并在此基础上得出综合结果的过程。资产对机密性、完整性和可用性上的要求可由安全属性缺失时造成的影响来表示，这种影响可能造成某些资产的损害以至危及信息系统，还可能导致经济效益、市场份额、组织形象的损失。

3.1 机密性赋值

根据资产在机密性上的不同要求，将其分为 5 个不同的等级，分别对应资产在机密性缺失时对整个组织的影响。表 4 提供了一种机密性赋值的参考。

表 1 资产机密性赋值表[4]

赋值	标识	定 义
5	很高	包含组织最重要的秘密，关系未来发展的前途命运，对组织根本利益有着决定性的影响，如果泄露会造成灾难性的损害
4	高	包含组织的重要秘密，其泄露会使组织的安全和利益遭受严重损害
3	中等	组织的一般性秘密，其泄露会使组织的安全和利益受到损害
2	低	仅能在组织内部或在组织某一部门内部公开的信息，向外扩散有可能对组织的利益造成轻微损害
1	很低	可对社会公开的信息、公用的信息处理设备和系统资源等

3.2 完整性赋值

根据资产在完整性上的不同要求，将其分为 5 个不同的等级，分别对应资产在完整性缺失时对整个组织的影响。表 5 提供了一种完整性赋值的参考。

表 2 资产完整性赋值表[4]

赋值	标识	定 义
5	很高	完整性价值非常关键，未经授权的修改或破坏会对组织造成重大的或无法接受的影响，对业务冲击重大，并可能造成严重的业务中断，损失难以弥补
4	高	完整性价值较高，未经授权的修改或破坏会对组织造成重大影响，对业务冲击严重，损失较难弥补
3	中等	完整性价值中等，未经授权的修改或破坏会对组织造成影响，对业务冲击明显，但损失可以弥补
2	低	完整性价值较低，未经授权的修改或破坏会对组织造成轻微影响，对业务冲击轻微，损失容易弥补
1	很低	完整性价值非常低，未经授权的修改或破坏会对组织造成影响可以忽略，对业务冲击可以忽略

3.3 可用性赋值

根据资产在可用性上的不同要求，将其分为 5 个不同的等级，分别对应资产在可用性缺失时对整个组织的影响。表 5 提供了一种可用性赋值的参考。

表 3 资产可用性赋值表[4]

赋值	标识	定 义
5	很高	可用性价值非常高，合法使用者对信息及信息系统的可用度达到年度 99.9%以上，或系统不允许中断
4	高	可用性价值非常高，合法使用者对信息及信息系统的可用度达到每天 90%以上，或系统允许中断时间小于 10 分钟
3	中等	可用性价值较高，合法使用者对信息及信息系统的可用度在正常工作时间达到 70%以上，或系统允许中断时间小于 30 分钟。
2	低	可用性价值较低，合法使用者对信息及信息系统的可用度在正常工作时间达到 25%以上，或系统允许中断时间小于 60 分钟
1	很低	可用性价值可以忽略，合法使用者对信息及信息系统的可用度在正常工作时间低于 25%

3.4 资产重要性等级

资产价值应依据资产在机密性、完整性、可用性上的赋值等级，经过综合评定得出。综合评定方法有两种：

1）选择对资产机密性、完整性和可用性最为重要的一个属性的赋值等级作为资产的最终赋值结果。

2）根据资产的机密性、完整性、可用性的不同等级对其赋值进行加权计算得到资产的最终赋值结果。加权方法根据组织的业务特点决定[1] 。

因此，通常资产赋值也可以划分为 5 个等级。评估者可以根据资产赋值的结果，确定重要资产的范围，并围绕重要资产，进行下一步的风险评估。

表 4 资产等级及含意描述[4]

等级	标识	描 述
5	很高	非常重要，其安全属性破坏后可能对组织造成非常严重的损失
4	高	重要，其安全属性破坏后可能对组织造成比较严重的损失
3	中等	比较重要，其安全属性破坏后可能对组织造成中等程度的损失
2	低	不太重要，其安全属性破坏后可能对组织造成较低的损失
1	很低	不重要，其安全属性破坏后可能对组织造成很小的损失，甚至忽略不计

4. 应用举例

本章将按照上面的方法和步骤，对一个电子邮件系统进行资产评估，完成从业务识别到资产识别，最后对资产识别的整个过程。

4.1 网络拓扑结构

该系统为一个电子邮件系统，服务器软件版本为 SendMail 8.9.3，该系统使用电子邮件系统作为信息传递与共享的工具和手段，网络拓扑结构如下图所示

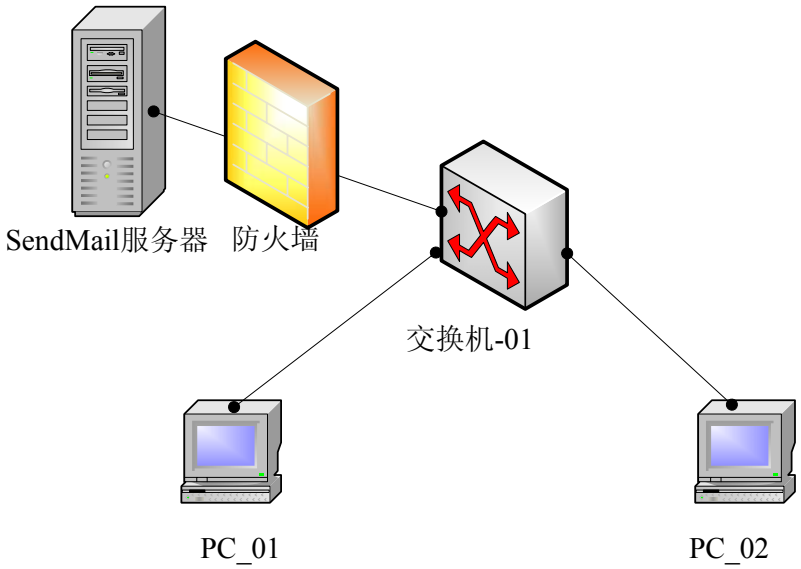

图 1　Mail 系统网络拓扑结构示意图

4.2 业务识别

该系统采用以电子邮件作为统一入口的设计思想，电子邮件信箱作为发文、收文、信息服务、档案管理、会议管理等业务的统一“门户”。因此电子邮件系统作为本系统的通信基础设施，为各种业务提供通用的通信平台。

4.3 资产识别与分类

对该电子邮件系统风险评估中进行的资产识别的资产，主要分为硬件资产、文档和数据、人员、管理制度等，其中着重针对硬件资产进行风险评估，人员主要分析其安全职责，IT 网络服务和软件结合其设计的硬件资产进行综合评估。下面列出具体各类清单。

硬件资产清表：

表 5　硬件资产清单

资产编号	资产名称	责任人	资产描述
ASSET_01	Mail Server	A	Mail 服务器，软件版本为 SendMail v8.9.3
ASSET_02	Fire Wall_01	B	防火墙，软件版本为 IPTables v1.2.11
ASSET_03	Switch_01	B	骨干交换机
ASSET_04	PC_01	C	用户终端
ASSET_05	PC_02	D	用户终端

文档和数据资产表：

表 6　文档和数据资产清单

资产编号	资产名称	责任人	资产描述
ASSET_06	人员档案	E	机构人员档案数据
ASSET_07	电子文档数据	E	OA 系统中的电子文件

制度资产清单表：

表 7　制度资产清单

资产编号	资产名称	责任人	资产描述
ASSET_08	安全管理制度	E	机房安全管理制度等
ASSET_09	备份制度	E	系统备份制度

人员资产清单表：

表 8　人员资产清单

资产编号	资产名称	责任人	资产描述
ASSET_10	杨肖	A	系统管理员
ASSET_11	石丹	B	网络管理员
ASSET_12	孙悦	B	普通用户
ASSET_13	万黎	D	普通用户
ASSET_14	王玉龙	E	档案和数据管理员，制度实施者

4.4 安全需求分析

对已经识别和分类的资产，按照不同的安全属性，逐一分析资产在机密性、完整性、可用性三个属性上的重要性和保护要求，为对资产 CIA 三性赋值提供基础。

评估方和被评估方都要参与进来，采用座谈会或调查问卷的方式，双方一同分析各个资产类别在其业务或应用系统中的位置以及所发挥的作用，分析每个资产类别在机密性、完整性、可用性等方面的要求。

下面以 ASSET_01 MailServer 为例，列举出它的人工访谈表格：

表 9　资产识别记录表格

资产识别活动信息			
日期	2007-7-2	起止时间	2007-7-4
访谈者	A	访谈对象及说明	系统管理员
地点说明	640		
记录信息			
所属类别	硬件资产		
资产名称	Mail Server	资产编号	ASSET_01
IP 地址	59.64.156.193	物理位置	机房
功能描述	接收和发送电子邮件		
机密性要求	很高		
完整性要求	很高		
可用性要求	很高		
重要程度	很高		
安全控制措施	防火墙		

负责人	A
备注	

4.5 资产赋值

三个属性赋值分为 5 个等级，分别对应了该项信息资产的机密性，完整性和可用性的不同程度的影响，根据资产赋值一节中对三个属性赋值的依据和标准，得到的 CIA 三性等级表如下：

表 10　资产 CIA 三性等级表

资产编号	资产名称	机密性	完整性	可用性
ASSET_01	Mail Server	5	5	5
ASSET_02	Fair Wall_01	5	5	5
ASSET_03	Switch_01	5	5	5
ASSET_04	PC_01	2	2	2
ASSET_05	PC_02	2	2	2
ASSET_06	人员档案	5	5	2
ASSET_07	电子文档数据	5	5	3
ASSET_08	安全管理制度	1	4	4
ASSET_09	备份制度	1	4	4
ASSET_10	A	5	3	2
ASSET_11	B	5	3	2
ASSET_12	C	1	3	2
ASSET_13	D	1	3	2
ASSET_14	E	1	3	2

资产价值应依据资产在机密性、完整性和可用性上的赋值等级，经过综合评定得出，根据本系统的业务特点，采取相乘法决定资产的价值，计算公式如下，其中：v 表示资产价值，x 表示机密性，y 表示完整性，z 表示可用性。$v=\sqrt{z*\sqrt{x*y}}$

根据给计算公式可以计算出资产的价值，得到本系统资产的价值清单如下。

表 11 资产价值表

资产编号	资产名称	机密性	完整性	可用性	资产价值
ASSET_01	Mail Server	5	5	5	5
ASSET_02	Fair Wall_01	5	5	5	5
ASSET_03	Switch_01	5	5	5	5
ASSET_04	PC_01	2	2	2	2
ASSET_05	PC_02	2	2	2	2
ASSET_06	人员档案	5	5	2	3.2
ASSET_07	电子文档数据	5	5	3	3.9
ASSET_08	安全管理制度	1	4	4	2.8

ASSET_09	备份制度	1	4	4	2.8
ASSET_10	A	5	3	2	2.8
ASSET_10	B	5	3	2	2.8
ASSET_12	C	1	3	2	2.4
ASSET_13	D	1	3	2	2.4
ASSET_14	E	1	3	2	2.8

为与上述安全属性的赋值相对应，根据最终赋值将资产划分为 5 级。

表 12 资产重要性程度判断准则

资产价值	资产等级	资产等级值	描述
4.2＜x≤5	很高	5	非常重要，其安全属性破坏后可能对组织造成非常严重的损失
3.4 ＜ x≤4.2	高	4	重要，其安全属性破坏后可能对组织造成比较严重的损失
2.6 ＜ x≤3.4	中等	3	比较重要，其安全属性破坏后可能对组织造成中等程度的损失
1.8 ＜ x≤2.6	低	2	不太重要，其安全属性破坏后可能对组织造成较低的损失
1＜x≤1.8	很低	1	不重要，其安全属性破坏后可能对组织造成很小的损失，甚至忽略不计

根据表 8 中对资产等级的规定，可以通过资产价值得到资产的等级。本系统的资产等级如表 9 所示。

表 13 资产价值表

资产编号	资产名称	资产价值	资产等级	资产等级值
ASSET_01	Mail Server	5	很高	5
ASSET_02	Fair Wall_01	5	很高	5
ASSET_03	Switch_01	5	很高	5
ASSET_04	PC_01	2	低	2
ASSET_05	PC_02	2	低	2
ASSET_06	人员档案	3.2	中	3
ASSET_07	电子文档数据	3.9	高	4
ASSET_08	安全管理制度	2.8	中	3
ASSET_19	备份制度	2.8	中	3
ASSET_10	A	2.8	中	3
ASSET_11	B	2.8	中	3
ASSET_12	C	2.4	低	2
ASSET_13	D	2.4	低	2
ASSET_14	E	2.8	中	3

5. 结论

在风险评估中需要对资产的价值进行识别，因为价值不同将导致风险值不同。风险评估中资产的价值不是以资产的经济价值来衡量，而是以资产的机密性、完整性和可用性等安全属性为基础进行衡量。资产在机密性、完整性、可用性三个属性上的要求不同则资产的最终价值也不同。

在资产赋值的过程中，需要解决的关键的问题是对资产的赋值，本文档中采取分别对资产的三个维度进行的赋值方法，最后算出权值。资产识别范围的划定以及资产赋值的准确与否直接影响着风险评估最终结果的准确程度，在信息安全风险评估中起着举足轻重的作用。

参考文献

[1] 吴亚非，李新友，禄凯，《信息安全风险评估》[M]，清华大学出版社 2007 年 4
[2] 范红 冯登国，《信息安全风险评估实施教程》[M]，清华大学出版社，2006 年 5 月
[3] 中华人民共和国国家标准，《计算机信息系统安全保护等级划分准则（GB17859--1999）》[S]，1999 年
[4] 国务院信息化工作办公室，《信息安全风险评估规范》[S]，[2006]9 号文

Research of Valuation of Assets in Analysis of Information System

Dan Shi
Computer Science & Technology Beijing University of Posts & Telecommunications，Beijing (100876)

Abstract

This paper simply introduced the normal methods of identifying the assets and valuation of assets. It is helpful to risk analysis of information system. There are two parts in the body of the paper: the common introduce of how to do the assets analysis. The second part use a case to follow the method that we have mentioned in the first part.

Keywords：Information System，Risk Analysis，Identification of Assets，Valuation of Assets