基于生命周期分析信息安全管理体系

于新辉,张 建,李伟涛
(山东建筑大学 计算机科学与技术学院,山东 济南 250101)

摘 要:信息安全管理正成为当前全球的热门话题,建立健全信息安全管理体系对企业的安全管理工作和企业的发展意义重大。信息技术在加速企业发展的同时,也给企业带来了各种各样的威胁。文中在跟踪现有的信息安全管理实际状况的基础上,分析各项威胁对信息系统造成的影响,并讨论基于生命周期建立一套信息安全管理体系所经历的四个阶段的主要内容及其作用。确保信息的完整性、可用性和保密性,从而保持业务运作的持续性和组织的竞争优势。

关键词:信息安全;生命周期;管理
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2012)03-0237-03

Analysis of Information Security Management System Based on Life Cycle

YU Xin-hui, ZHANG Jian, LI Wei-tao
(College of Computer Science and Technology, Shandong Jianzhu University, Jinan 250101, China)

Abstract: Information security management is becoming a hot topic, it is important to establish a good information security management for the manage work and the development of enterprise. While the information technology could accelerate the development of enterprises, it brings a variety of threats to business. Based on the current state of information security management, analyse the impact on the information system from every threat and discuss the content and function of the four stages to establish information security management system on life cycle. Ensure the integrity, the availability and the confidentiality of information so as to maintain a competitive advantage and business continuity.

Key words: information security; life cycle; management

0 引 言

随着信息技术的迅猛发展,为了确保企业经营战略的实现和满足业务快速发展的需要,越来越多的企业在运行各个环节中运用了信息技术。信息技术确实加速了企业的发展,同时这些企业也面临着来自各个方面的信息安全威胁,包括系统安全漏洞、DDoS(Distributed Denial of Service 分布式拒绝服务)攻击、非法入侵、病毒感染、通信故障等,保护客户和企业自身信息资产的保密性、完整性和可用性对提升服务水平和竞争力具有重要作用,因此建立全面可靠的信息安全管理体系是非常有必要的。

1 信息安全管理现状

随着信息化社会的来临,信息资源对社会发展的重要程度越来越大。从人们日常生活、组织运作到国家管理,信息资源都是必不可少的重要资源,现代社会的生存和发展,都需要各种信息的支持。但是信息在社会中发挥越来越重要的作用的同时,与之而来的信息安全问题也变得日益突出,需要加以安全保护。

目前,许多标准化组织都提出了各自的信息安全管理的体系标准[1,2]和控制模型[3],这些基于业务、技术与管理层面的标准在某些行业得到了很好的应用,并且信息安全管理工作也逐步纳入公司的日程中,但是这项工作目前仍存在不少的问题,信息安全管理现状依旧比较混乱,主要表现为以下几方面[4]:

由于缺乏权威、统一、专门的立法管理机构对国内信息安全管理进行组织、规划、管理和实施协调,导致我国现有的一些信息安全管理没有来自法律的推动力和约束;

在IT系统建设过程中信息安全管理并没有得到充分考虑,导致后期管理工作和安全建设比较被动,同时造成信息安全管理建设与业务的发展及IT的建设不对称;

安全管理缺乏系统管理的思想。被动应付多于主

收稿日期:2011-08-15;**修回日期**:2011-11-17
基金项目:山东省软科学项目(2009RKB216)
作者简介:于新辉(1987-),男,山东德州人,硕士,研究方向为信息安全、风险控制;张 建,教授,研究方向为信息安全、风险控制。

动防御,没有做前期的预防,而是出现问题才去想补救的方法,缺乏科学的、全面的、动态的安全管理方法;

重视安全技术,忽略安全管理。企业多在防火墙、网路、主机及应用系统开发等安全技术上投资,而相应的管理水平、手段没有体现;

在安全管理中不够重视人的因素[5],缺乏懂得管理的信息安全技术人员;

企业安全意识薄弱,因为信息安全管理不仅仅需要 CIO 或 CFO 的参与,企业各层领导和员工的重视与参与也是必不可少的。

2 各项威胁对企业信息安全的影响

企业信息安全有太多的因素需要关心:自然灾害、黑客攻击、计算机病毒以及企业内部信息泄露。2011 年大量信息安全事件中,索尼的数据泄漏是其中备受瞩目的一个,索尼的 PlayStation 网络于 4 月 20 日关闭,同时取证组开始调查索尼数据泄漏的范围。截止到 5 月 2 日,该泄漏事件影响了大约 1 亿人,索尼公司已经花费 1.71 亿美元处理其数据泄漏所带来的后果。一项调查显示,中国内地企业在改善信息安全机制上仍有待努力,从近年安全事件结果看,中国每年大约 98 万美元的财务损失,此外,42% 的中国内地受访企业经历了应用软件、系统和网络的安全事件,信息安全给企业造成了巨大的损失。而目前企业面临的主要威胁有以下几种。

2.1 自然灾害

由于近年来自然灾害的多发,给计算机系统造成了一些不可挽回的破坏而引发了许多信息安全问题,但相对于其他因素来说,自然灾害对信息安全的威胁算最小的,并且自然灾害的威胁只可尽量减小而不可避免。

2.2 黑客与病毒

随着计算机技术的发展,黑客的破坏力也日益扩大化,黑客傻瓜式工具的大量出现和黑客组织的形成导致的直接后果就是黑客技术的普及,网络上随便搜索一下,就能找到一大堆黑客技术交流网站。这些黑客站点提供黑客工具、公布系统漏洞、公开传授黑客技术、进行黑客教学,甚至还有黑客组织通过论坛形式相互交流黑客技术经验、协调黑客行动等。黑客事件的剧增、黑客组织规模的扩大、黑客站点的大量涌现,说明了黑客技术开始普及,同时黑客攻击对于信息安全的威胁也越来越大。仅在美国,黑客攻击每年造成的经济损失就超过 100 亿美元,可想而知,对于安全刚起步的中国破坏的影响程度有多大了。

而计算机病毒(恶意软件)的使用是黑客攻击常用的手段之一,计算机病毒的传播不仅可以破坏计算机信息系统,还可以盗取各种秘密信息,严重危害着当今社会的信息安全。根据安全供营商 McAfee(迈克菲)新发布的数据显示,2010 年前半年是 McAfee 进行恶意软件保护更新的最活跃的六个月,在第二季度报告中,恶意软件数目达到了最高,发现了一千多万个新的恶意软件,而第一季度发现的恶意软件数只有一百万。如果企业对自己的信息进行严密的监控,恶意软件可能会悄悄地潜伏进企业核心计算机,直到几周或几个月后才发现企业的信息已经被盗走了,企业的损失将是无法估量的。

2.3 移动设备的漏洞

据 3M 委托进行的《2010 年可视数据泄漏风险评估研究》报告指出,多于 70% 的公司仍然没有制定明确的政策来控制员工在公共场所工作时可以使用哪些设备连接网络。而经常出差的员工需要通过公司外部设备能够随时随地的通过 Internet 接入公司的网络,从而对公司的信息安全提出了一系列的挑战,员工的笔记本电脑和 U 盘需要使用 2 种以上的安全控制手段来实现综合加密,同时企业需要部署和强制执行严格的移动办公安全策略。

另外,硬件技术的发展使得移动介质有能力将海量数据存储到一个便携设备中,并且这些移动设备时常被带出公司。所以 IT 安全策略应当要求任何通过 USB 接口移动的数据或使用类似方式来建立连接的介质都必须在加密的基础上进行。而且这些介质类型绝不可以被用来做任何数据的单独拷贝,特别是重要任务或者企业机密,并严格限制它们用于临时性的数据传输。

2.4 对科技过于依赖

许多领导认为装好了顶级杀毒软件或者最新的防火墙,他们的系统安全就有保障了。但实际上,如果防火墙没有正确配置,防病毒软件也没有进行更新和升级,有跟没有是一样。

在特定环境下正确设置防火墙需要很高的技巧。它不是一项设置完就可以丢到脑后的工作,它要比安装杀病毒软件清除恶意软件复杂得多。防火墙需要经常调整以满足最新的要求,当一个新的端口扫描攻击出现时,必须在几周内阻断会受其影响的那些端口,了解最容易被攻击的 10 个端口,把计算机安全组织 SANS 的网页加入收藏夹。对于防病毒程序,不仅仅要及时升级,还必须要留意最新的弥补反病毒软件自身缺陷的补丁。

反间谍软件要比反病毒软件简单得多,所以很少需要打补丁。尽管如此,它们也要和反病毒软件一样要注意经常下载最新的数据库文件。最后,如果忽视安全检测程序发出的报告,所有的安全装置都会失去

意义。

2.5 内部威胁

前面所谈论的威胁和危险均来自于外部网络,但正如许多企业所了解的那样,最难以防范的安全威胁来自于组织内部[6]。

将公司的整个内部网络按域划分,实现部门级别的权限管理。每个部门内的每个员工在文件服务器上都有互相独立的存储空间。但是如果部门内的员工可以读、更改、删除另一个业务员在文件服务器中文件夹里面的资料,那么威胁同样存在。所以访问权限的设置应该体现实际的安全需求:部门之间禁止互相访问,同时对访问权限加以严格控制,每个访问者进行的操作及其操作对象都应该记录下来。

3 基于生命周期分析信息安全管理体系

为了保障企业的信息安全,就需要建立可靠的信息安全管理体系。而技术是不断发展的,并且机构的业务也经常会发生变化,因此为保障信息安全所使用的管理制度和技术措施也必须发生相应的调整和变化。现在关于信息安全建设已经达成一个共识:它是一个动态的、整体的、持续性的过程,企业不仅要进行安全建设,而且要根据技术的发展和业务的变更不断地进行评估,并在此基础上对已有的安全措施和设施进行调整、完善[7]。

根据对目前信息安全管理体系的调查研究,一般信息安全建设和管理的生命周期分为四个阶段:调研策划,风险评估,设计实施,运行改进。因此,将企业的业务特点与信息安全建设管理的生命周期[8]中的每个环节紧密结合起来,才能构建适合企业的信息安全管理体系。

3.1 调研策划

对企业所处的环境进行调研[9]是建设信息安全管理体系必不可少的工作,它是策划的依据。在这部分工作中,需要深入调查分析企业所处的国内外宏观环境、行业环境、企业所具有的优势与劣势、面临的发展机遇与威胁等。同时分析企业战略目标,理解企业发展战略在产业结构、核心竞争力、产品结构、组织结构、市场和企业文化等方面的定位。在此基础上,通过分析明确上述各要素与信息技术特点之间的潜在关系,从而确定信息技术应用的驱动因素,使信息安全管理与企业战略目标实现融合。

由于安全是相对的,安全技术也是不断发展进步的,因此企业应有一个合理和明确的安全要求使得公司有章可循,而且这些要求最终要体现在安全策略当中。衡量一个信息安全策略的首要标准就是现实可行性。因此信息安全策略与现实业务状态的关系是:信息安全策略既要符合现实的业务状态,又要能满足未来一段时间的业务发展要求。因此,企业根据自己的安全要求和实际情况,合理地制定安全策略是信息安全管理建设的基础。

3.2 风险评估

根据有关信息安全技术与管理标准,对企业内以信息资产进行资产识别,其中信息资产包括:信息、人员、软件和硬件以及系统的运行状况与安全措施。

针对各个资产,对其进行重要性评估时,将考虑资产在失去机密性、完整性和可用性等安全属性对企业造成的危害,并评估该信息资产所面临的威胁[10]及其发生安全事件的可能性,并结合如果发生安全事件后所涉及的各方面损失来判断安全事件可能对企业造成的影响。简而言之,就是风险计算[11],计算公式如下:

风险级别(R) = 资产重要性(V) × 风险发生可能性(L)

目前,实际工作中常使用的风险评估途径包括基线评估、详细评估和组合评估三种[12]。而在风险评估过程中又有许多操作方法,如基于知识的分析方法、基于模型的分析方法、定性分析和定量分析等。无论采用哪种途径和操作方法,共同的目的都是得到三个最主要的分析结果:资产保护等级分类、安全事件防护等级分类以及目前安全水平与企业安全需求间的差距。

3.3 设计实施

在完成风险评估后,要在第一阶段制定的安全策略的指导下,并根据风险评估的结果设计详细的信息安全保护实施方案[8]。

首先,从整体和全局的角度规划和建立一个合理的信息安全管理框架。从企业信息系统本身出发,对企业信息安全的不同层面进行整体安全分析,根据企业业务特征、组织形式、信息资产状况和技术条件,建立信息资产清单,进行安全需求分析和需要的安全控制级别[9],从而提出相应的安全解决方案。

安全解决方案的提出过程就是编写一套信息安全管理体系文件,应包含以下文档:安全方针文档、适用范围文档、风险评估文档、实施与控制文档、适用性声明文档等。这些文件的编写是建立信息安全管理体系的重要基础,也是一个企业实现风险控制和持续改进管理体系必不可少的依据。

3.4 运行改进

企业应按照编制的信息安全管理体系文件要求进行审核和批准并发布实施后,至此信息安全管理体系进入运行阶段。在此期间,企业应充分发挥管理体系本身的各项功能,及时找出管理体系中存在的问题,并采取纠正措施,按照更改要求对管理体系加以更改,以

(下转第244页)

3 结束语

RBAC 模型通过将用户和角色相联系，降低了授权管理的复杂性，解决了具有大量用户和权限分配的系统中管理复杂性问题[12]。但是由于该模型对角色的依赖性过大，限制了系统访问授权管理的灵活性和可变更性。因此，文中提出了一种改进的基于角色的通用性权限管理模型——RUP 模型。该模型在继承了 RBAC 优点的基础上着重强调了通用性和授权灵活的特点。最后，基于 RUP 模型设计并实现了一个通用的权限管理平台，该平台相较于以往的通用权限管理平台，具有管理粒度细化（即将系统资源分为功能和范围两部分，可以分别进行管理控制）、分级授权和权限制约的特点，使其能更广泛地满足各种业务系统复杂、多变的应用需求。

参考文献：

[1] 蒋 永，蒋玉明，彭思达. 基于工作流用户权限管理模型的研究与设计[J]. 计算机技术与发展，2009，19(1)：161-164.

[2] 欧阳星明，张华哲. 大型网络 MIS 系统中基于角色的权限管理[J]. 计算机工程与应用，2000，36(4)：138-140.

[3] 曹 晟，杨 浩，孟庆春. 基于 PMI 的系统访问安全管理研究与设计[J]. 计算机工程，2007，33(24)：141-143.

[4] Snyder L. Formal Models of Capability-based Protection Systems[J]. IEEE Transactions on Computers，1981，30(3)：172-181.

[5] 赵志明，江 楠，王力斌. J2EE 平台下权限管理的研究与实现[J]. 郑州轻工业学院学报（自然科学版），2009，24(3)：9-12.

[6] Sandhu R，Coyne E J. Role-based access control models[J]. IEEE Computer，1996，29(2)：38-47.

[7] Abrams M D，Eggers K W，La Padula L J. A generalized framework for access control：an information description[C]// Proceedings of the 13th National Computer Security Conference. [s. l.]：[s. n.]，1990：135-143.

[8] 戴祝英，左禾兴. 基于角色的访问控制模型分析与系统实现[J]. 计算机应用研究，2004(9)：173-175.

[9] 李 仲，杨宗凯，刘 威. 一种基于 RBAC 的实现动态权限管理的方法[J]. 计算机技术与发展，2006，16(10)：1-4.

[10] 沈海波，洪 帆. 访问控制模型研究综述[J]. 计算机应用研究，2005(6)：9-11.

[11] 顾丽娜，郭 炎，宋焱森. 一种通用权限管理系统的设计研究[J]. 科技咨询导报，2007(28)：116-116.

[12] 季小明，汪家常. 基于. NET 动态用户权限管理模型的设计与实现[J]. 计算机技术与发展，2006，16(10)：202-204.

（上接第 239 页）

达到持续完善信息安全管理体系的目的。

信息安全管理体系的建立与实施，能从根本上强化员工的安全意识，规范信息安全行为，可以有效的降低和避免企业的信息资产安全风险，增强了企业的竞争优势。而且管理体系是在动态的技术环境中进行的，以预防为主的方式使企业以最低的成本支出达到可接受的信息安全水平。因此，建立完整的信息安全管理体系是为企业发展提供可靠的保障。

4 结束语

企业应以战略目标为指导，以风险管理为核心，以技术手段为支撑，严格按照以上四个阶段构建一套完善的信息安全管理体系，保障企业信息资产的安全。

参考文献：

[1] ISO/IEC27001：2005. Information Technology- Security Techniques - Information Security Management Systems - Requirements[S]. Geneva：International Organization for Standardization，2005.

[2] ISO/IEC27006：2007. Information Technology-Security Techniques-Requirement for Bodies Providing Audit and Certification of Information Security Management Systems[S]. Geneva：International Organization for Standardization，2007.

[3] 奇 峰. COBIT 在企业信息安全管理中的应用实践[J]. 计算机应用与软件，2009(10)：282-285.

[4] 孙 强，陈 伟，王东红. 信息安全管理：全球最佳实务与实施指南[M]. 北京：清华大学出版社，2004.

[5] Saint-Germain R. Information Security Management Best Practice Based on ISO/IEC 17799[J]. Information Manage Journal，2005(7-8)：60-66.

[6] 赵昌伦，武 波. 基于. NET 的军队计算机网络信息安全对策[J]. 计算机技术与发展，2009，19(1)：150-153.

[7] 万 东，曹木恒. 基于 ISO27001 的 IDC 信息安全管理体系[J]. 信息安全与通信保密，2009(1)：75-77.

[8] 李 力. 信息安全建设和管理的生命周期[J]. 信息安全，2006(9)：54-56.

[9] 黄 松，夏洪亚，谈利群. 基于模糊综合的信息安全风险评估[J]. 计算机技术与发展，2010，20(1)：189-192.

[10] 黄水清，朱晓欢. 基于 ISO27001 的数字图书馆信息资产风险评估[J]. 图书情报工作，2006(11)：79-82.

[11] 罗 佳，杨世平. 基于熵权系数法的信息安全模糊风险评估[J]. 计算机技术与发展，2009，19(10)：177-180.

[12] 杨晓明，罗衡峰，范成瑜，等. 信息系统安全风险评估技术分析[J]. 计算机应用，2008(8)：1920-1923.