试析信息系统安全管理

李忱胁,王汉斌
(太原理工大学,山西 太原 030024)

[摘 要]对信息系统安全构成威胁的因素很多,有灾难、系统安全问题、系统错误与质量问题。意识到信息时代的安全隐患,通过对信息系统安全风险的评估,制定和实施相应的信息系统安全策略,应急响应系统,以应付突发事件的发生,使安全事件产生的影响最小化。

[关键词]信息系统;安全管理;评估
[中图分类号]G931.6 [文献标识码]A [文章编号]1673-9477(2009)01-0021-02

信息时代既带给我们无限商机与方便,也充斥着隐患与危险。越来越多的黑客通过网络肆意侵入企业的计算机,盗取重要资料,或者破坏企业网络,使其陷入瘫痪,造成巨大损失。因此,网络安全越来越重要。企业网络安全的核心是企业信息的安全。具体来说,也就涉及到企业信息系统的安全问题。一套科学、合理、完整、有效的网络信息安全保障体系,就成为网络信息系统设计和建设者们追求的主要目标。

信息安全是整个网络系统安全设计的最终目标,信息系统安全的建立必须以一系列网络安全技术为基础。但信息系统是一个综合的、动态的、多层次之间相结合的复杂系统,只从网络安全技术的角度保证整个信息系统的安全是很困难的,网络信息系统对安全的整体是任何一种单元安全技术都无法解决的。因此对信息系统的安全方案的设计必须以科学的安全体系结构模型为依据,才能保障整个安全体系的完备性、合理性。

一、信息系统安全风险的评估

信息系统安全风险评估是一种对信息系统所面临各类危及信息安全的影响因素进行的综合评判和分析。由于系统存在脆弱性、人为或自然的威胁导致安全事件发生所造成的影响,使信息系统的安全存在风险。信息安全风险评估就是要依据国家有关的信息安全技术标准,对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行科学评价,它要评估信息系统的脆弱性、信息系统面临的威胁以及脆弱性被威胁源利用后产生的实际负面影响,并根据安全事件产生的可能性和负面影响的程度来标识信息系统的安全风险。信息系统安全风险评估也是对信息系统所面临威胁的评估和信息系统脆弱性的评估。

信息系统所面临的威胁主要是指可能对信息系统造成不期望事件的主体,这些威胁主要来自于:

1. 通过网络进入信息系统的行为人。这种威胁是对信息系统基于网络的威胁,是行为人有意或无意的行为。

2. 通过物理方式接近信息系统的行为人。这种威胁是对信息系统的物理威胁,是行为人有意或无意的行为。

3. 系统缺陷造成的威胁。包括硬件缺陷、软件缺陷、相关系统的不可用性,重要基建的不可用性造成的威胁。

4. 病毒和恶意代码的威胁。目前病毒和恶意代码已经成为影响信息系统安全运行的重要因素。

5. 自然灾害的威胁。如洪水、地震或风暴。

信息系统的脆弱性是指信息系统中存在着可以被威胁主体所利用的造成对系统不期望影响的缺陷或弱点,主要有:

1. 技术脆弱性:主要是指信息系统技术方面存在的弱点可以被威胁主体所利用并最终导致对系统产生不良影响。如操作系统存在漏洞,系统中多个不受控外联网络,没有防病毒工具可能被病毒利用导致系统被病毒感染。

2. 组织脆弱性:由于信息系统管理组织的问题,导致信息系统被威胁因素所利用,造成对系统的不良影响。如没有人负责防病毒代码库的更新,对系统中介质的使用没有任何约束,可能被病毒利用导致系统感染。信息系统安全风险评估是信息系统安全保障体系建立过程中的重要评判方法和决策机制,主要有以下作用:

1. 明确信息系统的安全现状。通过评估可以让信息系统的管理组织准确了解自身的网络、各种应用系统以及管理制度规范的安全现状,从而明晰信息系统安全的需求。

2. 确定信息系统的主要安全风险。对信息系统进行信息安全评估并对风险分级,让信息系统的管理组织选择处置措施。

3. 指导信息系统安全技术体系与管理体系的建设。信息系统安全风险评估,有助于信息系统的安全策略及安全解决方案的制定,并指导信息系统安全技术体系与管理体系的建设。

二、信息系统安全策略的制定和实施

通过评估,可以明晰信息系统所面临的安全风险,制定相应的安全策略并组织实施,使由信息系统所面临的风险引发的安全事件的可能性降低到最小。它是信息系统安全工作的一个重要环节,信息系统的安全策略的制定和实施包括:信息系统安全管理策略;信息系统安全运行策略。

安全管理策略规定了针对信息系统的组织管理和技术管理的安全保护策略,包括:1. 信息系统组织策略。它包括人事安全管理制度,操作安全管理制度,场地与设施管理制度,设备安全管理制度,网络维护安全管理制度,操作系统、数据库安全管理制度,计算机网络安全管理制度,应用软件安全管理制度,技术文档、资料安全管理制度,口令安全管理制度,应急管理制度。2. 安全贯彻策略。它主要指为整个信息系统制定统一的安全策略。包括安全策略宣传贯彻体系、安全策略评审与评估体系,整个信息系统安全策略的一致

[收稿日期]2008-11-25
[作者简介]李忱胁(1982-),男,山西长治人,硕士生,研究方向:管理信息系统。

性检查等。3.人员安全策略。包括定义工作职责中的安全责任,建立人员资质审查策略,与重要员工签署保密协议,建立定期的信息安全教育和培训体系,建立安全事故报告制度,建立安全弱点报告制度,建立软件故障报告制度,建立安全事件分析总结制度,建立违规处罚制度。4.物理和环境安全策略。包括建立基本的物理安全边界,在重要的信息处理设备进出口处设置保安设施,对所有信息设备采取物理保护措施,保障电力供应,保护传输电缆,设备定期维护,保障离开安全区域的设备安全,建立设备报废或再启用安全流程。

信息系统访问控制策略包括有:强口令设置管理;身份认证管理;访问外网控制;用户身份及权限及时更新;网络边界安全策略;网络入侵检测。

网络系统安全策略包括线路冗余,网络设备冗余,服务器的高可用性。

计算机系统平台安全策略包括计算机防病毒体系的建立、信息系统的审计、主机入侵检测和系统加固。

除此之外,还有信息资源管理与安全监控。负责整个信息系统的日常运行维护、资源管理、设备报废、设备登记、软硬件设备接入、网络故障排除、网络流量统计分析、安全设备及安全事件分析处理等。对重要的服务器和重要的客户机进行安全加固,对网络设备及安全设备统一进行安全配置。(1)定期安全评估。(2)备份与恢复。(3)病毒、漏洞管理。

三、信息系统安全事件的应急响应

任何信息安全系统都不可能保障信息系统的绝对安全,因此,必须建立信息系统的应急响应系统,以应付突发事件的发生,使安全事件产生的影响最小化。

应急响应体系包括应急组织机构的建立,突发事件的定位,风险控制,限制损害事故的后果,应急预案的确立并经过演练后加以执行,以确保在所要求的时间期限内恢复业务处理,减少事件的影响,减低系统的风险。

信息系统的管理组织应针对各自的信息系统的实际情况制定安全应急处理预案,明确应急指挥机构,明确信息安全事件的严重程度和类别以及应急处理流程等内容,编制具体应急方案。

应急响应系统应能处理各种应急事件,对应对信息系统的管理人员进行相关的培训,使应急响应系统发挥应有的作用。应急响应系统应跟踪国内外安全事故的发展趋势,使其能够处理新型安全事件的发生。应急响应系统也要制定相应的方案,做到有备无患。

[参考文献]

[1]刘亚力.信息系统安全保障工程模型的设计与实施[J].湖南科技学院学报,2006,(05):55.
[2]胡晓梅.科学传播与网络[J].河北工程大学学报(社会科学版),2008,(1):85.

[责任编辑:陶爱新]

Analysis of information system security management

Li Chen - xi, WANG Han - bin
(Taiyuan University of Technology, Taiyuan 030024, China)

Abstract: Information system could be affected by many factors, such as system security, systemmistake and quality problem. Potential danger in the information age shall be identified and correspondingstrategies and emergency response system for information system security should be made and carried outto deal with the emergency and minimize the potential danger.

Key words: information system; security management; assessment

(上接第12页)

The study on durative development current situation of High - level sport teamsin Hebei province colleges and universities and the countermeasures

WANG Suo - gui, YAN Gui - fang
(Hebei University of Engineering, Handan 056038, China)

Abstract: Based on the investigation and analysis of the current situation of high - level sport teams involved in eight colleges and universities in Hebei province, this article gave the existent mostly problem and advanced some countermeasures and suggestions, which possibly provided theory direction and practice base for durative development of high - level sport teams in colleges and universities.

Key words: colleges and universities; high - level sport team; current situation; countermeasures