

全国信息技术人才培养工程指定培训教材

信息安全理论与实用技术丛书

信息安全管理的指南

信息产业部电子教育中心 组 编

戴宗坤 主 编

罗万伯 胡 勇 吴少华 副主编

重庆大学出版社

内 容 简 介

本书从信息安全有关的法律法规,行政、技术和工程管理等精辟地阐述了信息安全管理理论、方法和工程实践,包括从信息安全角度识别信息系统及资源的方法和分类原则,识别并针对信息系统资源的脆弱性、威胁、影响等因素进行风险管理的过程,识别与对抗风险的理论与方法,以及从资源分析、风险分析与评估、安全需求分析到安全保护策略和措施选择的工程实践和实务操作等。

本书是“全国信息技术人才培养工程教材”之一,适于用作与信息技术和信息安全相关专业本科生、研究生的教材,也是相关专业从业人员值得优选的参考书。

图书在版编目(CIP)数据

信息安全管理指南/戴宗坤主编. —重庆:重庆大学出版社,2008.3

(信息安全理论与实用技术丛书)

ISBN 978-7-5624-4348-3

I. 信... II. 戴... III. 信息系统—安全管理—指南
IV. TP309-62

中国版本图书馆 CIP 数据核字(2008)第 002487 号

全国信息技术人才培养工程指定培训教材

信息安全理论与实用技术丛书

信息安全管理指南

信息产业部电子教育中心 组 编

戴宗坤 主 编

责任编辑:李长惠 吴达周 孔 霁 版式设计:王 勇 王海琼

责任校对:秦巴达 责任印制:赵 晟

*

重庆大学出版社出版发行

出版人:张鸽盛

社址:重庆市沙坪坝正街 174 号重庆大学(A 区)内

邮编:400030

电话:(023) 65102378 65105781

传真:(023) 65103686 65105565

网址:<http://www.cqup.com.cn>

邮箱:fxk@cqup.com.cn (市场营销部)

全国新华书店经销

自贡新华印刷厂印刷

*

开本:787×1092 1/16 印张:14.25 字数:287 千

2008 年 3 月第 1 版 2008 年 3 月第 1 次印刷

印数:1—3 000

ISBN 978-7-5624-4348-3 定价:25.00 元

本书如有印刷、装订等质量问题,本社负责调换

版权所有,请勿擅自翻印和用本书

制作各类出版物及配套用书,违者必究

前 言

本书是作者在 2004 年承担由国务院信息化工作办公室下达的“信息安全管理指南”研究项目的基础上,结合与同事们十多年来在信息安全管理方面的理论研究成果和工程实践经验,并经过多次修改最后形成。虽然作者尽了极大努力,并力求在书稿中体现中国特色和国家对信息安全的方针政策,但由于水平所限,书中仍可能存在需要精雕细刻甚至需要刀劈斧砍的地方;更由于信息安全管理理论和方法研究在国内还处于探索阶段,因此本书中如有与他人观点和管理实践不一致的地方,那应该是可以在学术上争鸣的见仁见智的事情了;再则,作者和同事们虽然尽了极大努力,但毕竟是迄今为止所做的事情,这种努力还会继续下去。总之,现在呈现给读者朋友的这本书,是我们多年辛勤劳动的结果,希望对读者朋友有所帮助。

作者和同事们在信息安全理论与方法研究方面已经投入了大量的资源和精力,出于职业良心和教学、科研的需要,我们先后将研究成果和经验心得以译著、专著和工具书的形式向社会毫无保留地奉献了。其中,于 2000 年 4 月由机械工业出版社出版了《防火墙与因特网安全》(译);于 2000 年 9 月由金城出版社出版了《信息系统安全》、《信息系统安全工程学》和《VPN 与网络安全》;于 2003 年 3 月由电子工业出版社出版了《英汉网络信息安全辞典》,同时出版了《信息系统安全》、《信息系统安全工程学》和《VPN 与网络安全》的修订版;于 2005 年 5 月由重庆大学出版社出版了《信息安全应用基础》、《信息安全实用技术》和《信息安全法律法规与管理》,本书正好与这三本书构成一个完整体系,这也是作者与重庆大学出版社友好合作的完美体现。

本书涉及与信息安全有关的法律法规,行政、技术和工程管理的方方面面,既有信息安全管理理论与方法论的介绍;也有从信息安全管理角度识别信息系统及资源的方法和分类原则,以及识别信息系统资产的脆弱性、威胁、影响进而进行风险管理的过程描述;还有从信息安全管理角度识别风险、对抗风险的理论和方法的论述,以及进行基于风险管理的从资源分析、风险分析与评估、安全需求分析,到安全保护策略和措施选择的工程实践方法和实务操作的详细描述。从事信息系统的安全规划、设计、建设和保护,以及从事技术开发、信息安全咨询服务和产品生产的人们,都可以从本书中找到他们在其他地方找不到的东西;同时本书也可作为与信息技术和信息安全专业有关的研究生、本科生或培养高级专业技术人才时的教材或参考书。

参加本书编写的有戴宗坤、罗万伯、胡勇和吴少华等人。其中,戴宗坤负责全书的内容规划和设计,并主写第1、2章;罗万伯负责全书结构设计并主写第3、4章;胡勇起草“本书涉及的术语和定义”以及主写第5、6章;吴少华主写第7章以及附录。全书由戴宗坤和罗万伯审校,参加本书资料收集和整理的还有陈超、朱爱华等。

本书的编撰得到国务院信息化工作办公室王渝次司长和赵泽良副司长的热情鼓励和直接指导,在此表示衷心感谢。

戴宗坤
2007年夏

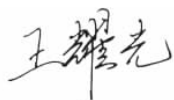
“全国信息技术人才培养工程教材”丛书序

当今世界,随着信息技术在经济社会各领域不断深化的应用,信息技术对生产力以至于人类文明发展的巨大作用越来越明显。党的“十六大”提出要“坚持以信息化带动工业化,以工业化促进信息化”,“优先发展信息产业,在经济和社会领域广泛应用信息技术”,明确了我国经济发展的道路,赋予了信息产业新的历史使命。近年来,日新月异的信息技术呈现出新的发展趋势,各类信息技术加快了相互融合和渗透的步伐,信息技术与其他技术的结合更加紧密,信息技术应用的深度、广度和专业化程度不断提高。

我国的信息产业作为国民经济的支柱产业正处于有利的国际、国内形势中,电子信息产业的规模总量已进入世界大国行列。但是我们也清楚地认识到,与国际先进水平相比,我们在产业结构、核心技术、管理水平、综合效益、普及程度等方面,还存在较大差距,缺乏创新能力与核心竞争力,“大”而不强。国际国内形势的发展,要求信息产业不仅要做大,而且要做强,要从制造大国向制造强国转变,这是信息产业今后的重点工作。要实现这一转变,人才是基础。机遇难得,人才更难得,要抓住本世纪头二十年的重要战略机遇期,加快信息产业发展,关键在于培养和使用好人才资源。《中共中央、国务院关于进一步加强对人才工作的决定》指出,人才问题是关系党和国家事业发展的关键问题,人才资源已成为最重要的战略资源,人才在综合国力竞争中越来越具有决定性意义。

为抓住机遇,迎接挑战,实施人才强业战略,信息产业部启动了“全国信息技术人才培养工程”。该项工程旨在通过政府政策引导,充分发挥全行业 and 全社会教育培训资源的作用,建立规范的信息技术教育培训体系、科学的培训课程体系、严谨的信息技术人才评测服务体系,培养造就大批行业急需的、知识技能结构合理的高素质信息技术应用型人才,以促进信息产业持续快速协调健康发展。

由各方专家依据信息产业对技术人才素质与能力的需求,在充分吸取国内外先进信息技术培训课程优点的基础上,信息产业部电子教育中心精心组织编写了信息技术系列培训教材。这些教材注重提升信息技术人才分析问题和解决问题的能力,对各层次信息技术人才的培养工作具有现实的指导意义。我谨向参与本系列教材规划、组织、编写的同志们致以诚挚的感谢,并希望该系列教材在全国信息技术人才培养工作中发挥有益的作用。



王耀先
二〇〇四年四月十日

全国信息技术人才培养工程教材 编委会

- 主 任** 王耀光 (信息产业部人事司 副司长)
- 副主任** 柳纯录 (中国电子信息产业发展研究院 总工程师)
华平澜 (中国软件行业协会 副会长)
- 委 员** (以姓氏笔画为序)
- 张 刚 (天津大学信息学院 教授)
- 陈 平 (西安电子科技大学软件学院 教授)
- 沈林兴 (信息产业部电子教育中心 高级工程师)
- 柏家球 (天津大学信息学院 教授)
- 杨 成 (河北大学计算机学院 副教授)
- 张长安 (航天科工集团 研究员)
- 张 宜 (北京邮电设计院 高级工程师)
- 张鸽盛 (重庆大学出版社 编审)
- 袁 方 (河北大学计算机学院 副教授)
- 曹文君 (上海复旦大学软件学院 教授)
- 温 涛 (东软信息技术学院 教授)
- 蒋建春 (中国科学院信息安全技术工程研究中心 博士)
- 程仁洪 (南开大学 教授)

通讯地址:北京 4356 信箱教育中心

<http://www.ceiaec.org/>

本书涉及的基本术语和定义

信息技术 (Information Technology, IT) 获取、加工、存储、变换、显示和传输文字、数值、图像与视频、音频和言语信息,以及提供这些服务的方法与设备的总称。这一术语有时与自动电子处理设备的含义很难严格区分。

信息技术安全, IT 安全 (IT Security) 与定义、获得以及维持信息技术系统及其组件机密性、完整性、可用性、可确认性、抗抵赖性和可靠性等有关的所有技术方面。

信息技术安全策略, IT 安全策略 (IT Security Policy) 对一个组织的信息系统包括敏感信息在内的所有资产实施管理、保护以及分配控制措施的规则和指令(集)。

信息安全 (Information Security) 提供信息和信息系统的机密性、完整性、可用性、可确认性和抗抵赖性,从而使信息和信息系统免遭未授权的访问、使用、泄露、干预、修改、重放和破坏,并保证使用和操作信息以及信息系统的任何实体的身份不被假冒或欺骗,实体的来源与行为可被唯一跟踪和不可抵赖。其中,机密性指对信息和信息系统的访问和泄露只限于被授权者的特性,包括任何形式的个人隐私和专用权信息;完整性指信息和信息系统不受到任何形式的未授权修改和重放的特性,并且还包括信息和信息系统的来源真实性;可用性指信息和信息系统能及时、可靠地为授权者提供访问和使用,以及能在面对各种攻击或出现差错和故障的情况下继续提供实质性服务,并且能够及时地恢复正常服务的特性;可确认性指实体的行为被唯一跟踪到该实体的特性;抗抵赖性指对信息和信息系统进行使用和操作的行为及其内容不能在事后予以否认的特性。

国家(信息)安全系统 (National Security System) 由某一(国家)机构,或机构的合约方,或机构所信任的其他组织所使用或运行的(包括任何通信系统在内

的)信息系统。这些信息系统或者涉及(国家)情(谍)报活动、国计民生和社会稳定;或者涉及与国家安全有关的密码活动、军事力量的指挥与控制或者作为武器与武器系统组成部分的装备,以及直接实现军事或情(谍)报业务的关键信息等的功能、操作和使用;或者在国家法律、法规和政策限制下已被授权保护其中的信息。

资产(Asset) 信息系统中对一个组织具有价值的任何东西和事物(包括硬件的或软件的、有形的或无形的、货币化的或非货币化的,等等)。

机密性(Confidentiality) 对信息和信息系统的访问和泄露只限于被授权者的特性,包括任何形式的个人隐私和专用权信息。

数据完整性(Data Integrity) 信息(数据)不受到任何形式的未经授权修改和重放的特性,并且还包括保证信息来源的真实性。

完整性(Integrity) 对数据完整性概念的合理延伸,指信息和信息系统不受到任何形式的未经授权修改和重放的特性,并且还包括保证信息和信息系统来源的真实性。

可用性(Availability) 信息和信息系统能及时、可靠地为授权者提供访问和使用的服务能力,以及能在面对各种攻击或出现差错和故障的情况下继续提供实质性服务,并且能够及时地恢复正常服务的特性。

可确认性(Accountability) 又称可审查性,或可追查性,一种保证某一实体的行为可被唯一跟踪到该实体的特性。

真实性(Authenticity) 保证一个实体或资源的身份及来源就是所声称的那个实体或资源的身份和来源的特性。真实性往往通过对用户、进程、系统和信息的鉴别来实现。

抗抵赖性(Non-repudiation) 对否认和抵赖曾经使用和操作过信息或信息系统的行为或内容进行对抗的特性。

脆弱性(Vulnerability) 一个或一组信息和系统资产的弱点或缺陷,这些弱点或缺陷可能导致在系统安全规程、系统设计、系统实现、内部控制和运行等方面被威胁者开发利用或直接遭到破坏。

威胁(Threat) 旨在限制、阻止、破坏信息系统业务,或降低服务能力,或降低系统或设备能力有效性,或泄漏和窃取信息和系统资产等的潜在力量、能力和战略目标的总和,主要包括对信息和系统的机密性、完整性、可用性、可确认性和抗抵赖性等造成危害的可能性和危害程度的所有因素。

影响(Impact) 不期望的事件所引起的后果,包括有形的和无形的,货币化的和非货币化的。

风险(Risk) 给定的威胁利用某一或某组(信息系统)资产的脆弱性对一个组织造成损失的可能性(概率),以及损失后的后果的总和。

风险分析(Risk Analysis) 识别风险的时间和空间分布及其强度(或等级)的过程。

风险管理(Risk Management) 识别、确定、控制、降低、消除或转移影响系统资产安全性的不定因素的总过程,包括风险分析、绩效分析、安全保护措施的选择、实现与测试、安全评估,以及所有的与安全有关的监管活动。

残留风险 (Residual Risk) 信息系统在采取保护措施后仍未消除的风险。

安全措施 (Safeguard) 安全措施也称安全保护措施,是控制、降低、消除或转移风险的实践、程序和机制。

基线控制 (Baseline Control) 一个(行业)系统或组织的信息系统从安全保障工程角度所建立的安全保护措施的最小集。

组织 (Organization) 一个机构管理下的具有共同利益和共同安全属性的业务单位或部门的总称。例如,一个企业,一个机关,或一个法人单位,在本书中都是组织,有时也称为团体或共同体。

目 录

1 信息安全概述	1
1.1 信息安全的总体要求和基本原则	2
1.1.1 总体要求	2
1.1.2 基本原则	2
1.2 信息安全管理范围	3
1.2.1 信息基础设施	3
1.2.2 信息安全基础设施	3
1.2.3 基础通信网络	4
1.2.4 广播电视传输网	5
1.2.5 信息系统	5
1.3 安全管理在信息安全保障中的地位和作用	6
2 信息安全管理与组织机构	7
2.1 信息安全管理的基本问题	8
2.1.1 信息系统生命期安全管理问题	8
2.1.2 信息安全中的分级保护问题	9
2.1.3 信息安全管理的基本内容	20
2.2 信息安全管理的指导原则	20
2.2.1 策略原则	20
2.2.2 工程原则	21
2.3 安全过程管理与 OSI 安全管理的关系	23
2.3.1 安全管理过程	23

2.3.2	OSI 管理	24
2.3.3	OSI 安全管理	25
2.4	信息安全管理组织机构	27
2.4.1	行政管理机构	28
2.4.2	信息安全服务与技术管理机构	28
3	信息安全管理要素与管理模型	31
3.1	概述	32
3.1.1	信息安全管理活动	32
3.1.2	安全目标、方针和策略	32
3.2	与安全管理相关的要素	33
3.2.1	资产	33
3.2.2	脆弱性	34
3.2.3	威胁	34
3.2.4	影响	35
3.2.5	风险	35
3.2.6	残留风险	35
3.2.7	安全措施	36
3.2.8	约束	36
3.3	管理模型	37
3.3.1	安全要素关系模型	37
3.3.2	风险管理关系模型	38
3.3.3	基于过程的信息安全管理模型	40
3.3.4	PDCA 模型	43
4	信息系统生命周期的安全管理	47
4.1	安排和规划	48
4.1.1	组织的信息安全策略	49
4.1.2	信息安全的组织	50
4.1.3	风险分析方法	52
4.2	管理的技術方法	57
4.2.1	信息安全的目標、方針和策略	57
4.2.2	組合風險分析法	61
4.3	安全措施的选择与实施	70
4.3.1	基础性评估	72
4.3.2	安全措施	74
4.3.3	根据信息系统类型选择基线安全措施	83

4.3.4	根据安全重点和威胁选择安全措施	86
4.3.5	根据详细风险评估选择安全措施	100
4.3.6	安全措施的实施	102
4.3.7	安全意识	103
4.4	后续活动	104
4.4.1	维护安全措施	104
4.4.2	安全遵从性	105
4.4.3	监控	105
4.4.4	事件处理	106
5	管理要求与人员安全	107
5.1	概述	108
5.2	信息安全策略	109
5.2.1	信息安全策略文档	109
5.2.2	评审与评估	109
5.3	组织对安全的管理	110
5.3.1	信息安全管理的基础结构	110
5.3.2	第三方访问的安全问题	112
5.3.3	委外管理	113
5.4	人员安全	114
5.4.1	岗位定义和资源分配的安全	114
5.4.2	用户培训	115
5.4.3	对安全事件和故障的响应	116
5.5	符合性要求	118
5.5.1	符合法律要求	118
5.5.2	符合安全策略和技术标准	121
5.5.3	系统审计方面的考虑	122
6	资产分类与物理安全管理	123
6.1	资产分类与管理	124
6.1.1	资产分类与责任落实	124
6.1.2	信息分类与标记	124
6.2	物理和环境安全	125
6.2.1	安全区域	125
6.2.2	设备安全	127
6.2.3	日常性控制措施	129

7 运行安全管理	131
7.1 网络安全管理	132
7.1.1 概述	132
7.1.2 任务	132
7.1.3 识别和分析	133
7.2 通信和操作管理	144
7.2.1 操作程序和责任	144
7.2.2 系统规划和验收	146
7.2.3 脆弱性和补丁	147
7.2.4 防范恶意软件	148
7.2.5 内务处理	149
7.2.6 网络管理	150
7.2.7 介质处理和安全	150
7.2.8 信息和软件的交换	152
7.3 访问控制	162
7.3.1 访问控制的策略	162
7.3.2 用户访问管理	162
7.3.3 用户职责	164
7.3.4 网络访问控制	165
7.3.5 操作系统访问控制	167
7.3.6 应用系统访问控制	170
7.3.7 监控系统访问与使用	171
7.3.8 移动计算和远程工作	172
7.4 系统开发和维护	174
7.4.1 系统的安全需求	174
7.4.2 应用系统中的安全	175
7.4.3 加密控制	176
7.4.4 与工程有关的系统文件安全	178
7.4.5 开发和支持进程的安全	179
7.5 业务持续性管理	181
7.5.1 业务持续性管理	182
7.5.2 业务持续性和影响的分析	182
7.5.3 制订和实施持续性计划	182
7.5.4 业务持续性计划框架	182
7.5.5 测试、维护和再评估业务持续性计划	183

附录	185
附录 1 信息安全管理检查列表	186
附录 2 信息安全应知应会培训参考材料	187
2.1 信息安全 ABC	187
2.2 信息安全知识主题和概念	190
附录 3 信息安全常见缩略语	197
参考文献	206

1

信息安全概述



1.1 信息安全的总体要求和基本原则

1.1.1 总体要求

信息安全保障工作的总体要求是:坚持积极防御、综合防范的方针,全面提高信息安全防护能力,重点保障基础信息网络和重要信息系统安全,创建安全健康的网络环境,保障和促进信息化发展,保护公众利益,维护国家安全。

积极防御就是要坚持用发展的思路辩证地认识 and 解决信息安全问题,在对信息安全风险进行充分分析和评估的基础上,构造安全防护与安全监管结合的保护体系,加强预警、应急处理和灾难备份。综合防范就是从预防、监控、应急处理、对抗和打击犯罪等环节,从法律、管理、技术、人员等方面采用多层次的、立体的、全面的防护措施,充分发挥国家、社会、组织和个人的作用,全社会共同构筑国家信息安全保障体系。

1.1.2 基本原则

信息安全保障工作的基本原则是:立足国情,以我为主,坚持管理与技术并重;正确处理安全与发展的关系,以安全促发展,在发展中求安全;统筹规划,突出重点,强化基础性工作;明确国家、企业、个人的责任和义务,充分发挥各个方面在信息安全保障工作中的积极性。

增强国家综合实力,促进经济社会的跨越式发展是信息化的根本目的,信息安全保障则是信息化发展的必要前提和保证。将信息安全绝对化或脱离发展过程中的现实而盲目追求信息安全是有害的;同样,只强调信息化应用,忽视信息安全则是另一个极端的错误。必须坚持以安全促发展,在发展中求安全的辩证思想原则。同样,信息安全中的技术与管理也是辩证统一的。在强调信息安全保障工作中的高技术对抗特点时,必须十分重视管理的作用。科学的管理不但贯穿信息安全保障的过程,而且是将信息安全技术转化为保证能力的必要条件。

基于目前我国信息安全主要设备和核心技术尚受制于人的现实,我们必须充分发挥政治、制度优势,强化信息安全意识和责任心,坚持以我为主、管理与技术并重的方针。这样做,不但能有效解决信息安全中技术与管理的互补性问题,同时也是降低信息安全成本的可行办法。坚持从本地、本单位的实际出发,根据信息化发展的不同阶段和不同的安全保护目标,统筹规划,保证重点,客观分析信息安全与信息化应用的适应性。综合平衡安全风险和安全成本,是信息安全保障中始终要遵循的原则。

1.2 信息安全管理的管理范围

1.2.1 信息基础设施

1) 全球信息基础设施

信息基础设施 (Information Infrastructure) 是有线和无线通信网络、计算机网络、广播网络、网络互连设备、外围设备、数据库、动力保障和环境设备的集合, 它可以建立在国家或本地的广大地域、空域和海域上。

理论上, 全球信息基础设施不被单个机构所控制或归其所有。它的“所有权”分布于公司、学术单位、政府实体以及个人。因特网就是一个全球信息基础设施的实例, 也是全球通信网络平台。大多数对内对外通信的网络都是在这个全球信息基础设施基础上建立起来的虚拟网、专用网、广域网以及定制的网络。

2) 国家信息基础设施

国家信息基础设施 (National Information Infrastructure) 是一个国家用来处理其 (政府或商业的) 业务的信息基础设施。

3) 区域信息基础设施

区域信息基础设施 (Local Information Infrastructure) 是指一个地区、行业或组织为处理其业务所建设和使用的信息基础设施。

4) 网络边界

网络边界指某个组织位于自己的和他人的物理网络系统交界位置的一个区域, 这个区域往往由一台或一组设备体现, 这些设备处理不同级别的信息。与因特网相连的局域网或私有网, 其物理边界就在互连网络设备处, 而逻辑边界则与不同级别的信息相关。

1.2.2 信息安全基础设施

信息安全基础设施主要包括 CA (Certification Authority, 证书机构), KMI (Key Management Infrastructure, 密钥管理基础设施) 和 PMI (Privilege Management Infrastructure, 权限管理基础设施) 等各类与公开密钥有关的基础设施, 其主要作用是使用基于数字证书的网络信任体系提供支撑性基础服务。这些基础设施分别在国家统一规划和技术标准指导下, 按行业、系统、业务类别, 以树形结构, 从上 (根) 至下分层进行部署, 将

全国大一统网络按层次分类划分为众多的虚拟网络,并按信息级别和使用权限对各类信息资源进行安全有序的访问与操作使用。

1) CA

CA (Certification Authority, 证书机构) 是一种用于网络环境中支持身份鉴别与认证、完整性和机密性保护以及不可抵赖性的基础设施,其基本元素是数字证书。数字证书上有持有者的身份标识、权限属性、密钥信息等基本数据,是网络信任体系用户的身份证。

2) KMI

KMI (Key Management Infrastructure, 密钥管理基础设施) 用于为鉴别和加密提供密钥管理,并且提供密钥恢复服务以及存取用户证书的目录。

KMI 不直接满足用户的安全需求,而是提供被其他安全设备和技术使用的模块和接口参数。KMI 的主要运行过程包括:登记授权使用 KMI 的个体;接受个体的密钥申请;生成对称或非对称密钥;根据用户个性化参数和非对称密钥生成证书;密钥的安全分发;密钥的跟踪审计;泄密处理,例如删除已泄露的密钥。

由此可知,KMI 可提供 4 个方面的业务:

- ①对称密钥的产生和分发。
- ②支持非对称密码以及相应的证书管理。
- ③提供目录服务。
- ④对 KMI 自身的管理。

随着 PKI 技术在电子政务系统建设过程中的不断完善和发展,对密钥管理的需求必将不断增长和强化。

3) PMI

PMI (Privilege Management Infrastructure, 权限管理基础设施) 是信息安全基础设施中的另一个重要组成部分,其主要用途是向用户和应用程序提供权限管理服务,负责向应用系统提供与应用相关的权限管理服务,提供用户身份到应用权限的映射功能,提供与实际应用处理模式对应的、与具体应用系统开发和管理无关的授权和访问控制机制,可以简化具体应用系统的开发和维护。

PMI 作为信息安全基础设施之一,为用户指定权限属性信息,例如特权、能力和角色等,并采用 X.509 协议所规定的格式使用证书。PMI 通过应用服务中使用用户权限管理支持访问控制服务。

1.2.3 基础通信网络

我国基础通信网络担负着为国家信息化提供互连互通的网络平台服务以及为与

国际联网提供高速信道服务的重任,目前比较有影响的基础通信网络有:

- 中国科技网(CSTNET)。
- 中国公用计算机互联网(CHINANET)。
- 中国教育和科研计算机网(CERNET)。
- 中国联通互联网(UNINET)。
- 中国铁通互联网(网通控股)(CRNET)。
- 宽带中国 CHINA169 网(网通集团)。
- 中国国际经济贸易互联网(CIETNET)。
- 中国移动互联网(CMNET)。
- 中国长城互联网(CGWNET)。
- 中国卫星集团互联网(CSNET)。

国家对基础通信网络的安全管理要求是:在网络交换的链路层和物理层为国家大一统网络的安全有序和健康运行提供公共平台服务。为此,对基础通信网络的基本安全要求是:有防止和对抗网络病毒传播与大规模拒绝服务攻击的能力。

1.2.4 广播电视传输网

各级政府或政府授权的机构利用有线、无线和卫星系统构成的广播电视传输网络,担负着以语音、图像和数据为表现形式的公共传媒载体的重任,为社会提供公共信息和社会控制信息服务。

国家对广播电视传输网的安全管理要求是:对传输信道和媒体的控制,以及防止和对抗系统外的势力对传输信道和媒体的侵占、插入、篡改和干扰,确保传输网络正常运行。

1.2.5 信息系统

1) 国家重要信息系统

国家重要信息系统指关系国家安全、国计民生、经济命脉、社会稳定等方面的数据相对集中的规模较大的信息系统,其中包括受国家委托或需要受控管理的军事工业企业或研究单位的信息系统。这些系统通常由政府或其委托的机构负责建立、运行和维护。

2) 电子政务系统

电子政务系统指各级政务机关为实现办公自动化、网络化、信息化而建立、运行和维护的公文流转和业务信息系统。这些系统辅助政府实现:

- ①增强提供给公众、其他部门和其他政府实体的信息和服务进行访问和交付的

能力。

②改进政府管理工作和提升政府形象,包括增强影响力、提高效率和服务质量,或加速改革进程。

3) 电子商务系统

电子商务系统指利用互联网络平台开展商务活动的金融、物资流通和各类交易的信息系统。

4) 企事业信息系统

企事业信息系统指各类企业和事业单位利用互连网络平台/技术所建立起来的集内部办公业务和生产、管理资源,以及与社会交互为一体的综合信息系统。

5) 其他信息系统

利用互联网络平台为社会和个人提供除上述信息系统服务功能以外的信息化服务系统,例如网吧、咨询服务等。

1.3 安全管理在信息安全保障中的地位和作用

安全管理和安全技术是构造信息安全保障体系的两大组成部分,两者具有同等重要的地位和作用。安全技术需要安全管理来规划、设计、实施、调整和维护,安全技术的效能需要安全管理予以激活和提升;安全管理需要借助安全技术实现系统化、智能化和科学化。安全管理和安全技术互为支持和补充,在一定条件下,两者可以互相转化。安全管理和安全技术的最佳搭配可以提高安全保障体系的功效或绩效比,降低安全成本。

2

信息安全管理与组织机构



2.1 信息安全管理的基本问题

2.1.1 信息系统生命期安全管理问题

1) 信息系统生命周期的几个阶段

安全管理贯穿于各个阶段:

- ①开发(Development):包括需求分析、系统设计、组件设计和集成。
- ②制造(Manufacturing):包括试制和批量生产。
- ③验证(Verification):包括对设计的论证、试验、审查和分析(包括仿真),非正式的演示,全面的开发测试和评估,以及产品验收测试。
- ④部署(Deployment):包括对系统及其组件的配备、分布和放置。
- ⑤运行(Operation):包括对系统及其组件的操作,以及系统的运转。
- ⑥支持和培训(Support and Training):包括对系统及其组件的维护,对操作、使用等的了解和指导。
- ⑦处置(Disposal):包括报废处理。

2) 安全管理在信息系统整个生命期的各个阶段中的实施内容

- ①制订策略:利用安全服务为组织提供管理、保护和分配信息系统资源的准则和指令。
- ②资产分类保护:帮助组织识别资产类别并进行适当的保护。
- ③人事监管:减少人为错误、盗窃、欺诈或设施误用所产生的风险。
- ④物理和环境安全:防止未经授权访问、损坏和干扰通信媒体和机房(及其附属建筑设施)以及信息泄漏。
- ⑤通信和运营管理:确保信息处理设施的正确和安全运营。
- ⑥访问控制:按照策略控制对信息的访问。
- ⑦系统开发和维护:确保将安全服务功能构建到信息系统中。
- ⑧业务连续性管理:制止中断业务的活动以及保护关键的业务过程不受大的故障或灾害影响,并具有灾难备份和快速恢复能力。
- ⑨遵从:保持与信息安全有关的法律、法规、政策或合同规定的一致性并承担责任。

2.1.2 信息安全中的分级保护问题

1) 信息系统安全保护目标

信息系统安全的保护目标与所属组织的安全利益是完全一致的,具体体现为对信息的保护和系统的保护。信息保护是使所属组织有直接使用价值(用于交换服务或共享目的)的信息和系统运行中有关(用于系统管理和运行控制目的)的信息的机密性、完整性、可用性和可控性不受到非授权的改变和破坏。系统保护则是使所属组织用于维持运行和履行职能的信息技术系统的可靠性、完整性和可用性不受到非授权的改变和破坏。系统保护的功能有两个,一是为信息保护提供支持,二是对信息技术系统本身进行保护。

2) 信息系统分级保护

对信息和信息系统进行分级保护是体现统筹规划、积极防范、突出重点的信息安全保护原则的重大措施。最有效和科学的方法是在维护安全、健康、有序的网络运行环境的同时,以分级分类的方式确保信息和信息系统安全既符合政策规范,又满足实际需求。其基本思想和方法如下:

(1) 敏感信息系统保护等级的划分原则

- ①组织级别与保护等级的关系:组织的行政级别越高,保护等级越高。
- ②敏感程度与保护等级的关系:信息系统及其信息的敏感程度越高,保护等级越高。
- ③敏感信息量与保护等级的关系:相对集中的敏感信息量越大,保护等级越高。
- ④履行职能与保护等级的关系:职能与国家安全、国计民生、社会稳定的关系越大,保护等级越高。

在遵循以上原则时,要对信息系统中个别信息和组件的保护等级与整个系统的保护等级加以适当区分,不因对个别信息和组件的高等级保护要求而提高整个系统其他信息和组件的保护等级。

(2) 非敏感信息系统保护等级的划分原则

- ①社会影响面与保护等级的关系:社会影响面越广,保护等级越高。
- ②危害程度与保护等级的关系:造成的社会危害性越大,保护等级越高。
- ③资源价值与保护等级的关系:资源价值越大,保护等级越高。
- ④资源利用效率与保护等级的关系:资源利用效率越高,保护等级越高。
- ⑤资源密集度与保护等级的关系:资源集中度越高,保护等级越高。

3) 信息系统保护等级的技术标准

敏感信息系统和非敏感信息系统的保护等级及其评估的技术标准在 GB 17859—1999《计算机信息系统安全保护等级划分准则》和 GB/T 18336—2001《信息技术 安全技术 信息技术安全性评估准则》等国内外的基本技术框架内制订。对一个组织的信息系统,可按物理/逻辑方法划分为两个或两个以上保护等级子系统。

(1) 计算机信息系统的安全保护等级

GB 17859—1999《计算机信息系统安全保护等级划分准则》是我国计算机信息系统安全保护等级系列标准的基础,是进行计算机信息系统安全等级保护制度建设的基础性依据,也是信息安全评估和管理的重要基础。这个标准虽然并不具备技术上的可操作性,但其基本准则却是我国多类信息系统划分保护等级和确定等级保护措施的指导原则和策略根据。此标准将计算机信息系统安全保护从低到高划分为 5 个等级,即用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。高级别安全要求是低级别要求的超集。计算机信息系统安全保护能力随着安全保护等级的增高逐渐增强。

在该标准中,一个重要的概念是可信计算基(TCB)。TCB 是一种实现安全策略的机制,包括硬件、固件和软件。它们根据安全策略来处理主体(系统管理员、安全管理员、用户等)对客体(进程、文件、记录、设备等)的访问。TCB 还具有抗篡改的能力和易于分析与测试的结构。TCB 主要体现该标准中的隔离和访问控制两大基本特征,各安全等级之间的差异在于 TCB 的构造不同以及它所具有的安全保护能力不同。

①第 1 级:用户自主保护级

本级的计算机信息系统可信计算基通过隔离用户与数据,使用户具备自主安全保护的能力。它具有多种形式的控制能力,对用户实施访问控制,即为用户提供可行的手段,保护用户和用户组信息,避免其他用户对数据的非法读写与破坏。

本级实施的是自主访问控制,即通过可信计算基定义系统中的用户和命名用户对命名客体的访问,并允许用户以自己的身份或用户组的身份指定并控制对客体的访问。这意味着系统用户或用户组可以通过可信计算基自主地定义主体对客体的访问权限。

从用户的角度来看,用户自主保护级的责任只有一个,即为用户提供身份鉴别。在系统初始化时,可信计算基首先要求用户标识自己的身份(如口令),然后使用身份鉴别数据来鉴别用户的身份,并实施对客体的自主访问控制,避免“非法”用户对数据的读写或破坏。

在数据完整性方面,可信计算基通过自主完整性策略,阻止非授权用户修改或破坏敏感信息。

②第2级:系统审计保护级

与用户自主保护级相比,本级的计算机信息系统可信计算基实施了粒度(粗细程度,如IP地址比IP段粒度细,IP地址加端口号比IP地址粒度细。粒度越细,控制越精确)更细的自主访问控制。它通过登录规程、审计安全性相关事件和隔离资源等措施,使用户对自己的行为负责。

本级实施的是自主访问控制和客体的安全重用。在自主访问控制方面,可信计算基实施的自主访问控制粒度是单个用户,并控制访问权限的扩散,即没有访问权的用户只允许由授权用户指定其对客体的访问权。在客体的安全重用方面,在客体被初始指定或分配给一个主体之前,或在客体再分配之前,必须撤消该客体所含信息的授权;当一个主体获得一个客体的访问权时,原主体的活动所产生的任何信息,对当前主体而言是不可获得的。

从用户的角度来看,系统审计保护级的功能有两个:身份鉴别和安全审计。身份鉴别方面,本级比用户自主保护级增加两点:

- 为用户提供唯一标识,确保用户对自己的行为负责。
- 为支持安全审计功能,具有将身份标识与用户所有可审计的行为相关联的能力。

安全审计方面,可信计算基能够创建、维护对其所保护客体的访问审计记录,还授权主体提供审计记录接口,以便记录那些主体认为需要审计的事件,并且只有授权用户才能访问审计记录。另外,本级还支持系统安全管理员可以根据主体身份有选择地审计任何一个用户的行为。

在数据完整性方面,可信计算基应提供并发控制机制,以确保多个主体对同一客体的正确访问。

③第3级:安全标记保护级

本级的计算机信息系统可信计算基具有系统审计保护级的所有功能。此外,还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述,具有准确地标记输出信息的能力,消除通过测试发现的错误。

本级的主要特征是可信计算基实施强制访问控制。强制访问控制就是可信计算基以敏感标记为主体和客体指定其安全等级。安全等级是一个2维组,第1维是分类等级(如秘密、机密、绝密等),第2维是范畴(如适用范围等)。由可信计算基控制的主体和客体,只有当满足一定条件时,主体才能读/写一个客体,即只有当主体分类等级的级别高于客体分类等级的级别、主体范畴包含客体范畴时,主体才能读一个客体;只有当主体分类等级的级别低于或等于客体分类等级的级别、主体范畴包含于客体范畴时,主体才能写一个客体。

敏感标记是实施强制访问控制的基础,因此系统应明确规定需要标记的客体(如文件、记录、目录、日志等),应明确定义标记的粒度(如文件级、字段级等),并必须使其

主要数据结构具有敏感标记。另外,本级可信计算基应维护与每个主体及其控制下的存储对象相关的敏感标记,敏感标记应准确地表示相关主体或客体的安全级别。

从用户的角度来看,系统仍呈现身份鉴别和审计两大功能。本级可信计算基除了具有第2级的功能外,还有如下能力:

- 确定用户的访问权和授权访问的数据。
- 接受数据的安全级别,维护与每个主体及其控制下的存储对象相关的敏感标记。
- 维护标记的完整性。
- 维护并审计标记信息的输出,并与相关联的信息进行匹配。
- 确保以该用户的名义而创建的那些在可信计算基外部的主体和授权,授其访问权和授权的控制。

在数据完整性方面,可信计算基还应提供定义、验证完整性约束条件的功能,以维护客体 and 敏感标记的完整性。

④第4级:结构化保护级

本级的计算机信息系统可信计算基建立在一个明确定义的形式化安全策略模型之上,它要求将第3级系统中的自主访问控制和强制访问控制扩展到所有主体与客体。此外,还要考虑隐蔽通道。本级的计算机信息系统可信计算基必须结构化为关键保护元素和非关键保护元素。计算机信息系统可信计算基的接口也必须明确定义,使其设计与实现能经受更充分的测试和更完整的复审。本级还增强了鉴别机制、支持系统管理员和操作员的可确认性。提供可信设施管理,增强了配置管理控制,确保系统具有相当的抗渗透能力。

本级的主要特征有:

- 可信计算基基于一个明确定义的形式化安全保护策略。
- 将第3级实施的(自主和强制)访问控制扩展到所有主体和客体。即在自主访问控制方面,可信计算基应维护由可信计算基外部主体直接或间接访问的所有资源的敏感标记;在强制访问控制方面,可信计算基应对所有可被其外部主体直接或间接访问的资源实施强制访问控制,应为这些主体和客体指定敏感标记。
- 针对隐蔽信道,将可信计算基构造成为关键保护元素和非关键保护元素。
- 可信计算基具有合理定义的接口,使其能够经受严格测试和复查。
- 通过提供可信路径来增强鉴别机制。
- 支持系统管理员和操作员的可确认性,提供可信实施管理,增强严格的配置管理控制。

在审计方面,当发生安全事件时,可信计算基还能够检测事件的发生、记录审计条目、通知系统管理员、标识并审计可能利用隐蔽信道的事件。

在隐蔽信道分析方面,系统开发者应彻底搜索隐蔽信道,并确定信道的最大带宽,

这样才能确定有关使用隐蔽信道的安全性。

⑤第5级:访问验证保护级

本级的计算机信息系统可信计算基满足基准监控器(Reference Monitor)需求。基准监控器仲裁主体对客体的全部访问。基准监控器本身具备抗篡改性,且必须足够小,能够分析和测试。为了满足基准监控器需求,计算机信息系统可信计算基在其构造时,排除那些对实施安全策略来说并非必要的代码;在设计和实现时,从系统工程角度将其复杂性降低到最小程度。支持安全管理员可确认性;扩充审计机制,当发生与安全相关的事件时发出信号;提供系统恢复机制。系统具有很高的抗渗透能力。

本级与第4级相比,主要区别在以下4个方面:

- 在可信计算基的构造方面,具有基准监控器。所谓基准监控器,是监控主体和客体之间授权访问关系的部件,仲裁主体对客体的全部访问。基准监控器必须是抗篡改的,并且是可分析和测试的。
- 在自主访问控制方面,因为有基准监控器,所以访问控制能够为每个客体指定用户和用户组,并规定他们对客体的访问模式。
- 在审计方面,在基准监控器的支持下,可信计算基扩展了审计能力。本级的审计机制能够监控可审计安全事件的发生和积累,当积累超过规定的门限值,能够立即向系统管理员发出报警;并且,如果这些与安全相关的事件继续发生,能以最小的代价终止它们。
- 在系统的可信恢复方面,可信计算基提供了一组过程和相应的机制,保证系统失效或中断后,可以进行不损害任何安全保护性能的恢复。

(2)基于通用准则的安全等级

在《信息技术 安全技术 信息技术安全性评估准则》(GB/T 18336—2001,等同ISO/IEC 15408:1999)中定义了7个递增的安全评估保证级(EAL, Evaluation Assurance Level),这种递增靠替换成同一保证子类中的一个更高级别的保证组件(即增加严格性、范围或深度)和添加另外一个保证子类的保证组件(例如,添加新的要求)来实现。

评估保证级是由GB/T 18336—2001第3部分中保证组件构成的包,该包代表了CC(Common Criteria,通用准则)预先定义的保证尺度上的某个位置。一个保证级是评估保证要求的一个基线集合。每一评估保证级定义一套一致的保证要求,合起来,评估保证级构成一个预定义CC保证级尺度。

评估保证级并不用于直接对信息和系统的等级保护,而是用于对信息和系统的保护有效性进行评估和验收,包括对保护措施(或保证组件)的功能和效能进行等级评估、测试和验证。

①评估保证级1(EAL1)——功能测试:

- 适用对象:TOE(Target of Evaluation,评估对象)在有一定信任,安全威胁不严重的环境或者能单独保证对人员或信息的保护方面有足够重视的情况。

- 评估内容: EAL1 为用户提供了 TOE 的一个评估, 包括依据一个规范的独立性测试和对所提供的指导性文档的检查。EAL1 通过利用功能和接口的规范以及指导性文档, 对安全功能进行分析以提供一种基础级别的保证, 以理解安全行为。这种分析需要 TOE 安全功能的独立性测试支持。预计在没有 TOE 开发者的帮助下, 一个 EAL1 评估也能成功地进行而且所需费用最少。在这个级别上的一个评估应当提供这样的证据, 即 TOE 的功能与其文档在形式上是一致的, 并且对已标识的威胁提供了有效的保护。

和未经评估的 IT 产品或系统相比, 本 EAL 提供了有意义的保证的增强。

② 评估保证级 2 (EAL2)——结构测试:

在交付设计信息和测试结果时, EAL2 需要开发者的合作, 但不应要求开发方付出过多的费用或时间。

- 适用对象: 在缺乏现成可用的完整的开发记录时, 开发者或使用者需要一种低到中等级别的独立保证的安全性。当保护的是老系统或者与开发者的交流受到限制时, 会出现这种情况。

- 评估内容: EAL2 通过利用功能和接口的规范、指导性文档和 TOE 的高层设计, 对安全功能进行分析来提供保证, 以理解安全行为。这种分析由 TOE 安全功能的独立性测试、开发者基于功能规范进行测试得到的证据、对开发者测试结果的选择性独立确认、功能强度分析、开发者搜索明显的脆弱性 (如公开的脆弱性) 的证据等因素来提供支持。EAL2 通过评估和分析的结果、TOE 的配置表和安全交付程序的证据来提供保证。

本 EAL 在 EAL1 基础上有意义地增加了保证。这是通过要求开发者测试, 以及在 EAL1 基础上增加脆弱性分析和基于更详细的 TOE 规范的独立性测试来实现的。

③ 评估保证级 3 (EAL3)——系统地测试和检查:

EAL3 可使一个尽职尽责的开发者在设计阶段从正确的安全工程中获得最大限度的保证, 而不需要对现有的合理的开发实践做大规模的改变。

- 适用对象: 开发者或使用者需要一个中等级别的独立保证的安全性, 以及在没有再次进行真正的工程实践的情况下, 要求对 TOE 及其开发过程进行彻底调查。

- 评估内容: EAL3 通过利用功能和接口的规范、指导性文档和 TOE 的高层设计, 对安全功能进行分析来提供保证, 以理解安全行为。这种分析由 TOE 安全功能的独立性测试、开发者基于功能规范和高层设计进行测试得到的证据、对开发者测试结果的选择性独立确认、功能强度分析、开发者搜索明显的脆弱性 (如公开的脆弱性) 的证据等因素来提供支持。EAL3 还通过使用开发环境控制措施、TOE 的配置管理和安全交付程序的证据来提供保证。

本 EAL 在 EAL2 的基础上增加了保证, 这是通过要求更完备的安全功能测试范围, 以及要求一些提供 TOE 在开发过程中不会被篡改的可信性的机制或程序来实

现的。

④评估保证级 4 (EAL4)——系统地设计、测试和复查：

EAL4 可使开发者从正确的安全工程中获得最大限度的保证,这种安全工程基于良好的商业开发实践。这种实践虽然很严格,但并不需要大量专业知识、技巧和其他资源。在经济合理的条件下,对一个已经存在的生产线进行翻新时,EAL4 是所能达到的最高级别。

- 适用对象:开发者或使用者对传统的商品化的 TOE 需要一个中等到高等级别的独立保证的安全性和准备负担额外的安全专用工程费用。

- 评估内容:EAL4 通过利用功能规范和完备的接口规范、指导性文档、TOE 的高层设计和低层设计、实现的子集,对安全功能进行分析来提供保证,以理解安全行为。也可通过 TOE 安全策略的一个非形式化模型来额外地获得保证。这种分析由 TOE 安全功能的独立性测试、开发者基于功能规范和高层设计进行测试得到的证据、对开发者测试结果的选择性独立确认、功能强度分析、开发者搜索脆弱性的证据,以及对抵御低等攻击潜力的穿透性攻击者的能力进行论证的独立脆弱性分析等因素来提供支持。EAL4 还通过使用开发环境控制措施、包括自动化在内的额外的 TOE 配置管理以及安全交付程序的证据来提供保证。

本 EAL 在 EAL3 基础上增加了保证,这是通过要求更多的设计描述、实现的子集,以及提供 TOE 在开发或交付过程中不会被篡改的可信性的改进机制或程序来实现的。

⑤评估保证级 5 (EAL5)——半形式化设计和测试：

EAL5 可使一个开发者从安全工程中获得最大限度的保证,这种安全工程基于严格的商业开发实践,是靠应用专业安全技术来支持的。设计和开发这样的 TOE 需要有达到 EAL5 保证的决心。相对于没有应用专业技术的严格开发而言,由 EAL5 要求引起的额外开销也许不会很大。

- 适用对象:开发者和使用者在有计划的开发中需要一个高级别的独立的安全性保证,以及在没有由专业安全技术引起不合理开销的条件下,需要一种严格的开发手段。

- 评估内容:EAL5 通过利用功能规范和完备的接口规范、指导性文档、TOE 的高层和低层设计以及所有的实现,对安全功能进行分析来提供保证,以理解安全行为。也可以通过 TOE 安全策略的形式化模型、功能规范和高层设计的半形式化表示,以及它们之间对应性的半形式化论证等方式额外地获得保证。此外还需要一个模块化的 TOE 设计。这种分析由 TOE 安全功能的独立性测试,开发者基于功能规范、高层设计和低层设计进行测试得到的证据,对开发者测试结果的选择性独立确认,功能强度分析,开发者搜索脆弱性的证据,以及对抵御中等攻击潜力的穿透性攻击者的能力进行论证的独立脆弱性分析等因素来提供支持。这种分析也包括对开发者的隐蔽信道分析的确认。EAL5 还通过使用开发环境控制措施、包括自动化在内的全面的 TOE 配置

管理以及安全交付程序的证据来提供保证。

本 EAL 在 EAL4 的基础上增加了保证,这是通过要求半形式化的设计描述、整个实现、更结构化(因而更具有可分析性)的体系,隐蔽信道分析,以及提供 TOE 在开发过程中不会被篡改的可信性的改进机制或程序来实现的。

⑥评估保证级 6(EAL6)——半形式化验证的设计和测试:

EAL6 可使开发者通过把安全工程技术应用于严格的开发环境,而获得高度的保证,以便生产一个昂贵的 TOE 来对抗重大的风险,保护高价值的资产。

- 适用对象:应用于高风险环境下的安全 TOE 的开发,在这里受保护的资源值得花费额外的开销。

- 评估内容:EAL6 通过利用功能规范和完备的接口规范、指导性文档、TOE 的高层和低层设计,以及实现的结构化表示,对安全功能进行分析来提供保证,以理解安全行为。还通过 TOE 安全策略的形式化模型、功能规范、高层设计和低层设计的半形式化表示,以及它们之间对应性的半形式化论证等方式额外地获得保证。此外还需要一个模块化和分层的 TOE 设计。这种分析由 TOE 安全功能的独立性测试,开发者基于功能规范、高层设计和低层设计进行测试得到的证据,对开发者测试结果的选择性独立确认,功能强度分析,开发者搜索脆弱性的证据,以及对抵御高等攻击潜力的穿透性攻击者的能力进行论证的独立脆弱性分析等因素来提供支持。这种分析也包括对开发者的系统化隐蔽信道分析的确认。EAL6 也通过使用结构化的开发流程、开发环境控制措施、包括完全自动化在内的全面的 TOE 配置管理以及安全交付程序的证据等来提供保证。

本 EAL 在 EAL5 的基础上增加了保证,这是通过要求更全面的分析,实现的结构化表示,更体系化的结构(如分层),更全面的独立脆弱性分析,系统化隐蔽信道识别,以及改进了的配置管理和开发环境控制等来实现的。

⑦评估保证级 7(EAL7)——形式化验证的设计和测试:

- 适用对象:EAL7 适用于安全 TOE 的开发,该 TOE 将应用在风险非常高的地方或有高价值资产、值得更高开销的地方。EAL7 的实际应用目前只局限于一些 TOE,这些 TOE 非常关注能经受广泛的形式化分析的安全功能。

- 评估内容:EAL7 通过利用功能规范和完备的接口规范、指导性文档、TOE 的高层和低层设计以及实现的结构化表示,对安全功能进行分析来提供保证,以理解安全行为。也可通过 TOE 安全策略的形式化模型,功能规范和高层设计的形式化表示,低层设计的半形式化表示,以及它们之间对应性的适当的形式化和半形式化论证等方式获得额外保证。此外还需要一个模块化的、分层的且简单的 TOE 设计。这种分析由 TOE 安全功能的独立性测试,开发者基于功能规范、高层设计、低层设计和实现表示进行测试得到的证据,对开发者测试结果的全部独立确认,功能强度分析,开发者搜索脆弱性的证据,以及对抵御高等攻击潜力的穿透性攻击者的能力进行论证的独立脆弱性

分析等因素来提供支持。这种分析也包括对开发者的系统化隐蔽信道分析的确证。EAL7 也通过使用结构化的开发流程、开发环境控制措施、包括完全自动化在内的全面的 TOE 配置管理以及安全交付程序的证据等来提供保证。

本 EAL 在 EAL6 的基础上增加了保证,这是通过要求利用形式化表示和对应性的形式化进行更全面的分析,以及更全面的测试来实现的。

(3) 几种安全等级标准的映射关系

表 2.1 给出了几种安全等级标准的映射关系。

表 2.1 几种安全等级标准的映射关系

CC	GB/T 7859	TCSEC	FC	CTCPEC	ITSEC
EAL1	—	—	—	—	—
EAL2	第 1 级	C1	—	—	E1
EAL3	第 2 级	C2	T - 1	T - 1	E2
EAL4	第 3 级	B1	T - 2	T - 2	E3
—	—	—	T - 3	T - 3	—
—	—	—	T - 4	—	—
EAL5	第 4 级	B2	T - 5	T - 4	E4
EAL6	第 5 级	B3	T - 6	T - 5	E5
EAL7	—	A1	T - 7	T - 6	E6
—	—	—	—	T - 7	—

CC——Common Criteria:通用准则;

TCSEC——Trusted Computer System Evaluation Criteria:可信计算机系统评估准则,美国于 1985 年提出,2000 年 12 月停止使用;

FC——Federal Criteria:美国联邦准则;

CTCPEC——Canada Trusted Computer Product Evaluation Criteria:加拿大可信计算机评估准则;

ITSEC——Information Technology Security Evaluation Criteria:信息技术安全评估准则,欧洲。

4) 信息安全等级保护管理办法

公安部、国家保密局、国家密码管理局、国务院信息化工作办公室于 2007 年 6 月 27 日联合发布《信息安全等级保护管理办法》,用于规范信息安全等级保护管理,提高信息安全保障能力和水平,维护国家安全、社会稳定和公共利益,保障和促进信息化建设。

(1) 总原则

- 国家通过制定统一的信息安全等级保护管理规范和技术标准,组织公民、法人和其他组织对信息系统分等级实行安全保护,对等级保护工作的实施进行监督、管理。
- 公安机关负责信息安全等级保护工作的监督、检查、指导。国家保密工作部门负责等级保护工作中有关保密工作的监督、检查、指导。国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导。涉及其他职能部门管辖范围的事项,由有关职能部门依照国家法律法规的规定进行管理。国务院信息化工作办公室及地方信息化领导小组办公室负责等级保护工作的部门间协调。
- 信息系统主管部门应当依照《信息安全等级保护管理办法》及相关标准规范,督促、检查、指导本行业、本部门或者本地区信息系统运营、使用单位的信息安全等级保护工作。
- 信息系统的运营、使用单位应当依照《信息安全等级保护管理办法》及其相关标准规范,履行信息安全等级保护的义务和责任。

(2) 定级保护

国家信息安全等级保护坚持自主定级、自主保护的原则。

信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度,信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

信息系统的安全保护等级分为五级:

- 第1级 信息系统受到破坏后,会对公民、法人和其他组织的合法权益造成损害,但不损害国家安全、社会秩序和公共利益。
- 第2级 信息系统受到破坏后,会对公民、法人和其他组织的合法权益产生严重损害,或者对社会秩序和公共利益造成损害,但不损害国家安全。
- 第3级 信息系统受到破坏后,会对社会秩序和公共利益造成严重损害,或者对国家安全造成损害。
- 第4级 信息系统受到破坏后,会对社会秩序和公共利益造成特别严重损害,或者对国家安全造成严重损害。
- 第5级 信息系统受到破坏后,会对国家安全造成特别严重损害。

信息系统运营、使用单位依据《信息安全等级保护管理办法》和相关技术标准对信息系统进行保护,国家有关信息安全监管部門对其信息安全等级保护工作进行监督管理。其中:

第1级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。

第2级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行指导。

第3级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行监督、检查。

第4级信息系统运营、使用单位应当依据国家有关管理规范、技术标准和业务专门需求进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行强制监督、检查。

第5级信息系统运营、使用单位应当依据国家管理规范、技术标准和业务特殊安全需求进行保护。国家指定专门部门对该级信息系统信息安全等级保护工作进行专门监督、检查。

(3) 等级保护的实施与管理

不同安全保护等级的信息系统,有不同的实施和管理要求,涉及确定安全保护等级,评审与审批,备案及备案管理,信息系统安全建设或者改建,评测,安全监督、检查、指导,查处各种违规违法行为和泄密事件等。对于第2级以上的系统,有严格规定。

(4) 信息安全等级保护的密码管理

国家密码管理部门对信息安全等级保护的密码实行分类分级管理。

(5) 法律责任

第3级以上信息系统运营、使用单位违反《信息安全等级保护管理办法》规定,有下列行为之一的,由公安机关、国家保密工作部门和国家密码工作管理部门按照职责分工责令其限期改正;逾期不改正的,给予警告,并向其上级主管部门通报情况,建议对其直接负责的主管人员和其他直接责任人员予以处理,并及时反馈处理结果:

- (一)未按本办法规定备案、审批的;
- (二)未按本办法规定落实安全管理制度、措施的;
- (三)未按本办法规定开展系统安全状态检查的;
- (四)未按本办法规定开展系统安全技术测评的;
- (五)接到整改通知后,拒不整改的;
- (六)未按本办法规定选择使用信息安全产品和测评机构的;
- (七)未按本办法规定如实提供有关文件和证明材料的;
- (八)违反保密管理规定的;
- (九)违反密码管理规定的;
- (十)违反本办法其他规定的。

违反前款规定,造成严重损害的,由相关部门依照有关法律、法律予以处理。

信息安全监管部门及其工作人员在履行监督管理职责中,玩忽职守、滥用职权、徇私舞弊的,依法给予行政处分;构成犯罪的,依法追究刑事责任。

2.1.3 信息安全管理的基本内容

信息系统的安全管理涉及与信息系统的有关的安全管理以及信息系统的管理的安全两个方面。这两方面的管理又分为技术性管理和法律性管理两类。其中技术性管理以 OSI 安全机制和安全服务的管理以及对物理环境的技术监控为主,法律性管理以法律法规遵从性管理为主。信息安全管理本身并不完成正常的业务应用通信,但却是支持与控制这些通信的安全所必需的。

由信息系统的行政管理部门依照法律并结合本单位安全实际需要而强加给信息系统的策略可以是各种各样的,信息安全管理活动必须支持这些策略。受同一个机构管理并执行同一个安全策略的多个实体构成的集合有时称为“安全域”。安全域以及它们的相互作用是一个值得进一步研究的重要领域。

信息系统的管理的安全包括信息系统所有管理服务协议的安全以及信息系统的管理信息的通信安全,它们是信息系统安全的重要部分。这一类安全管理将借助对信息系统安全服务与机制做适当的选取,以确保信息系统的管理协议与信息获得足够的保护。

在信息安全管理的技术性管理中,为了强化安全策略的协调性和安全组件之间的互操作性,设计了一个极为重要的基本概念,即用于存储和交换开放系统所需的与安全有关的全部信息的安全管理信息库(SMIB)。SMIB 是一个分布式信息库。在实际中,SMIB 的某些部分可以与 MIB 结合成一体,也可以分开。SMIB 有多种实现办法,例如数据表、文件以及嵌入到实开放系统软件或硬件中的数据或规则。

安全管理协议以及传送这些管理信息的通信信道,可能遭受攻击。所以应特别对安全管理协议及其协议数据加以保护,其保护的强度通常不低于为业务应用通信提供的安全保护的强度。

安全管理可以使用 SMIB 信息在不同系统的行政管理机构之间交换与安全有关的信息。在某些情况下,与安全有关的信息可经由非自动信息通信通道传递,局部系统的管理者也可采用非标准化方法来修改 SMIB。在另外一些情况下,可能希望通过自动信息通信通道在两个安全管理机构之间传递信息。在获得安全管理者授权后,该安全管理将使用这些通信信息来修改 SMIB。修改 SMIB,必须先得到安全管理者的授权。

2.2 信息安全管理指导原则

2.2.1 策略原则

信息安全管理的基本原则为:

(1) 以安全保发展,在发展中求安全

信息安全的目的是通过保护信息系统内有价值的资产,比如数据、硬件、软件和环

境等以实现信息系统的健康、有序和稳定运行,促进社会、经济、政治和文化的发展。没有安全保证的信息化,以及牺牲信息化发展来换取安全,是两种必须摒弃的错误做法。科学的安全发展观是在安全意识上全面提高对信息安全保障认识的同时,采用渐进的适度安全策略来保证和推进信息化的发展,并通过信息化的发展为信息安全保障体系的逐步完善提供充足的人力、财力和物力支持。

(2) 受保护资源的价值与保护成本平衡

信息安全的成本和效益比应该在货币和非货币两个层面上进行评估,以保证将成本控制在预期的范围内。

(3) 明确国家、企业和个人对信息安全的职责和可确认性

应该明确表述与信息系统相关的所有者、管理者、经营者、供应商以及使用者应该承担的安全职责和可确认性。

(4) 信息安全需要积极防御和综合防范

信息安全需要综合治理的方法,坚持保护与监管相结合、技术措施与管理并重的方针,综合治理方法将延伸到信息系统的整个生命期。

(5) 定期评估信息系统的残留风险

信息系统及其运行环境是动态变化的,一劳永逸的信息系统安全解决方案是不存在的。因此必须定期评估信息系统的残留风险,并依此调整安全策略。

(6) 综合考虑社会因素对信息安全的制约

信息安全受到很多社会因素的制约,比如国家法律、社会文化和社会影响等。安全措施的选择和实现还应该综合考虑法律框架下信息系统所有者与使用者、所有者和社会各方面之间的利益平衡。

(7) 信息安全管理体现以人为本

信息系统安全管理要体现人性化、社会公平和交换平等的价值观念。

2.2.2 工程原则

为了指导信息安全工程的组织和实施,信息安全工程应遵循 6 类基本原则,即基本保证、适度安全、实用和标准化、保护层次化和系统化、降低复杂度和安全设计结构化。这些原则简单明了,可应用于信息系统的安全规划、设计、开发、运行、维护管理和报废处理等多个环节。

(1) 基本保证

- ① 信息系统安全工程设计前应制订符合本系统实际的安全目标和策略。
- ② 将安全作为整个系统设计不可分割的部分。
- ③ 识别信息及信息系统资产,以此作为风险分析和安全需求分析的对象。

- ④划分安全域。
- ⑤确保开发者受过软件安全开发的良好训练。
- ⑥确保信息系统用户的职业道德和安全意识的持续培训。

(2) 适度安全

- ①通过对抗、规避、降低和转移风险等方式将风险降低到可接受的水平,不追求绝对或过度安全的目标。
- ②安全的标志之一是系统可控。
- ③在减小风险、增加成本开销和降低某些操作有效性之间进行折中,避免盲目地追求绝对安全目标。
- ④采用剪裁方式选择系统安全措施,以满足组织的安全目标。
- ⑤保护信源到信宿全程的机密性、完整性和可用性。
- ⑥在必要时自主开发非卖品以满足某些特殊的安全需求,将残留风险保持在可接受水平。
- ⑦预测并对抗、规避、降低和转移各种可能的风险。

(3) 实用和标准化

- ①尽可能采用开放的标准化技术或协议,增强可移植性和互操作性。
- ②使用便于交流的公共语言进行安全需求的开发。
- ③设计的新技术安全机制或措施,要确保系统平稳过渡,并保证局部采用的新技术不会引起系统的全局性调整,或引发新的脆弱点。
- ④尽量简化操作,以减少误操作带来新的风险。

(4) 保护层次化和系统化

- ①识别并预测普遍性故障和脆弱性。
- ②实现分层的安全保护(确保没有遗留的脆弱点)。
- ③设计和运行的信息系统对入侵和攻击应具有必要的检测、响应和恢复能力。
- ④提供对信息系统各个组成部分的体系性保障,使信息系统面对预期的威胁具有持续阻止、对抗和恢复能力。
- ⑤容忍可以接受的风险,拒绝绝对安全的策略。
- ⑥将公共可访问资源与关键业务资源进行物理/逻辑隔离。
- ⑦采用物理或逻辑方法将信息系统的局域网络与公共基础设施相分离。
- ⑧设计并实现审计机制,以检测非授权和越权使用系统资源,并支持事故调查和责任确认。
- ⑨开发意外事故处置或灾难恢复规程,并组织学习和演练。

(5) 降低复杂度

- ①安全机制或措施力求简单实用。

- ②尽量减少可信系统的要素。
- ③实现访问的最小特权控制。
- ④消除不必要的安全机制或安全服务冗余。
- ⑤“开机—处理—关机”全程安全控制。

(6) 安全设计结构化

- ①通过对物理的/逻辑的安全措施进行合理组合实现系统安全设计的优化。
- ②所配置的安全措施或安全服务可作用于多个域。
- ③对用户和进程使用鉴别技术,以确保在域内和跨域间的访问权控制。
- ④对实体进行标识以确保责任的可追究性。

2.3 安全过程管理与 OSI 安全管理的关系

2.3.1 安全管理过程

政府、企事业和商业组织在开放互连的网络环境下通过合理地使用信息来指导和处理他们的业务活动。信息系统资源的机密性、完整性、可用性、不可抵赖性、可确认性、真实性和可靠性等特性的缺失会对组织造成有害影响。因此,需要保护信息系统资源和管理信息系统的安全。

信息系统安全管理是一个过程,用来实现和维持信息系统及其资源适当等级的机密性、完整性、可用性、不可抵赖性、可确认性、真实性和可靠性。信息系统安全管理包括分析系统资产,分析风险,分析安全需求,制定满足这些需求的计划,执行这些计划,并维持和管理安全设备的安全。信息系统安全管理行为主要包括:

- ①决定组织的信息系统安全目标、方针和策略。
- ②分析组织内信息系统资产存在的安全脆弱性。
- ③分析组织内信息系统资产面临的安全威胁。
- ④评估对组织不利的影响。
- ⑤分析信息系统的风险。
- ⑥通过对抗、降低、转移和规避等方法处理风险。
- ⑦确定组织的信息系统安全需求。
- ⑧通过选择适当的保护措施减少风险。
- ⑨识别存在的残留风险。
- ⑩为了使组织内的信息系统及其资源处于有效保护之下,需要监视安全措施的实现和运行。
- ⑪开发和实施可提高安全意识的计划。
- ⑫对安全事件进行检测和响应。

⑬系统备份和灾难恢复计划与实施。

2.3.2 OSI 管理

OSI 管理包括故障管理、计账管理、配置管理、性能管理和安全管理等功能,这些管理功能对在 OSI 环境中进行通信的资源进行监视、控制和协调。

(1)故障管理

故障管理包括对 OSI 环境中的异常操作故障进行检测、隔离和纠正。故障导致开放系统不能实现运行目标。这些故障可能是持续性的,也可能是暂时的。故障在开放系统运行中作为特殊事件(比如差错)处理。故障检测提供识别故障的能力。故障管理实现下列功能:

- ①维护和检查故障日志。
- ②接收和处理故障检测报告。
- ③识别和跟踪故障。
- ④实施一系列诊断性测试。
- ⑤隔离故障点或故障区域。
- ⑥纠正故障行为。

(2)计账管理

计账管理是对使用 OSI 环境中资源的费用进行建账,识别使用这些资源的成本和使用情况。计账管理包括下列功能:

- ①通知用户所产生的成本和所耗费的资源。
- ②设置账单,使账目表和资源的使用情况相关联。
- ③使成本与被请求的多种资源相一致,进而获得给定的通信目标。

(3)配置管理

配置管理识别、操作和控制开放互连系统,从开放互连系统收集数据和为其提供数据。其目的是为初始化和系统启动提供持续性运行和终止连接服务做准备。配置管理包括下列功能:

- ①对控制开放互连系统的路由操作进行参数设置。
- ②将被管理目标和目标集与其名字相关联。
- ③对被管理目标进行初始化。
- ④按需收集开放互连系统的目前状况信息。
- ⑤获得开放互连系统条件发生重大变更的信息。
- ⑥变更开放互连系统的配置情况。

(4)性能管理

性能管理激活 OSI 环境中资源的行为以及通信活动的效力。性能管理的功能

包括:

- ①收集统计信息。
- ②维护和检查关于系统状态的历史记录。
- ③在自动和人工条件下判断系统性能。
- ④为处理性能管理活动变更系统运行模式。

(5) 安全管理

安全管理的目的是支持和维持使用安全策略,其功能有:

- ①创建、修改、删除及控制安全服务和机制。
- ②发布安全相关信息。
- ③报告安全相关事故。

2.3.3 OSI 安全管理

OSI 安全管理包含与 OSI 有关的安全管理和 OSI 管理的安全。OSI 安全管理本身不是正常的业务应用通信,但却为支持与控制这些通信的安全所必需。

OSI 安全管理涉及 OSI 安全服务的管理与安全机制的管理。这种管理要求给这些安全服务与机制分配管理信息,并收集与这些服务和机制的运行有关的信息。例如,密钥分配、设置行政管理强加的安全参数、报告正常的与异常的安全事件(审计跟踪),以及安全服务的激活与停止。安全管理并不保证在调用特定安全服务协议中(例如连接请求的参数中)传递与安全有关的信息。这些信息的安全由安全服务来提供。

由分布式开放系统的行政管理强加的安全策略可以是各种各样的,OSI 安全管理应该支持这些策略。

OSI 安全管理活动可分为 4 类:系统安全管理、安全服务管理、安全机制管理和 OSI 管理本身的安全管理。这几类安全管理执行的关键功能如下:

(1) 系统安全管理

系统安全管理的典型活动包括:

- ①总体安全策略的管理,包括策略一致性的修改与维护。
- ②与别的 OSI 管理功能的相互作用。
- ③与安全服务管理和安全机制管理的交互作用。
- ④事件处理管理。例如,远程报告那些违反系统安全的明显企图,以及对用来触发事件报告的阈值的修改。
- ⑤安全审计管理,包括:
 - 选择将被记录和被远程收集的事件。
 - 授予或取消对所选事件进行审计跟踪日志记录的能力。
 - 审计记录的远程收集。
 - 准备安全审计报告。

⑥安全恢复管理,包括:

- 维护那些用来对明确的或可疑的安全事件作出反应的规则。
- 远程报告明显的系统安全违规行为或事件,并予以响应。
- 安全管理者之间的交互。

(2)安全服务管理

安全服务管理涉及对具体安全服务功能的管理。下列行为是在管理具体安全服务功能时可能执行的典型活动。

①为该种安全服务分配一个或多个安全保护的目标。

②指定与维护规则(存在可选情况时),用以选取为提供所需的安全服务而使用的特定的安全机制。

③对那些需要事先取得管理层同意的安全服务,可用安全机制进行协调(本地的与远程的)。

④通过适当的安全机制管理功能调用特定的安全机制。例如,用来提供行政管理强加的安全服务。

⑤与别的安全服务管理功能和安全机制管理功能的交互。

(3)安全机制管理

安全机制管理涉及的是对具体安全机制的管理。下列行为是典型的安全机制管理功能。

①密钥管理,包括:

- 周期性地产生与所要求的安全级别相当的合适密钥。
- 根据访问控制的要求,决定每个密钥应该复制给哪些实体。
- 用可靠办法使这些密钥对实开放系统中的实体实例是可用的,或将这些密钥分配给它们。

应该强调的是,某些密钥管理功能将在 OSI 环境之外执行,其中包括用可靠手段对密钥进行物理的分配。

工作密钥的选取也可以通过访问密钥分配中心来完成,或事先通过管理协议分配。

②加密管理,包括:

- 与密钥管理的交互作用。
- 建立密码参数。
- 密码同步。

密码机制就是使用密码管理和采用共同方式来调用密码算法。

可使用密码算法寄存器或在实体间协商,以便调用相同的加密算法。

③数字签名管理,包括:

- 与密钥管理的交互作用。

- 建立密码参数与密码算法。
- 在通信实体与可能的第三方之间使用协议。

一般说来,数字签名管理与加密管理类似。

④访问控制管理。访问控制管理可涉及安全参数(包括口令)的分配,或对访问控制表或权力表进行修改;也可能涉及在通信实体与其他提供访问控制服务的实体之间使用协议。

⑤数据完整性管理,包括:

- 与密钥管理的交互作用。
- 建立密码参数与密码算法。
- 在通信的实体间使用协议。

当对数据完整性使用密码技术时,数据完整性管理与加密管理相类似。

⑥鉴别管理。鉴别管理可以包括把说明信息、口令或密钥分配给请求执行鉴别的实体;也可以包括在通信的实体与其他提供鉴别服务的实体之间使用协议。

⑦通信业务填充管理。通信业务填充管理包括维护那些用作通信业务填充的规则,例如:

- 预定的数据率。
- 指定随机数据率。
- 指定报文特性,例如长度。
- 可能按日期、时间或日历来改变这些规定。

⑧路由选择控制管理。路由选择控制管理涉及确定那些按特定准则被认为是安全可靠或可信任的链路或子网络。

⑨公证管理,包括:

- 分配有关公证的信息。
- 在公证方与通信的实体之间使用协议。
- 公证方之间的交互。

(4) OSI 管理的安全

OSI 管理的安全包括所有 OSI 管理功能的安全以及 OSI 管理信息的通信安全,它们是 OSI 安全的重要部分。这一类安全管理,将借助于对 OSI 安全服务与机制做适当的选取,以确保 OSI 管理协议与信息获得足够的保护。例如,在管理信息库的管理实体之间的通信一般将要求进行某种形式的保护。

2.4 信息安全管理的组织机构

信息安全管理的组织机构大致可以分为两大类,一类是行政管理、协调类型的机构,另一类是技术服务、应急响应和技术支持类型的管理机构。

2.4.1 行政管理机构

①国家信息化领导小组:综合协调涉及各个领域的信息化和信息安全工作;组织协调计算机网络与信息安全管理方面的重大问题。

②国家网络与信息安全工作协调小组:综合协调国家信息安全保障工作。

③国务院信息化工作办公室:负责日常工作。

④国家密码管理委员会:负责密码管理工作。

⑤国家保密部门:负责涉密网络和信息系统的管理。

⑥国家安全部:负责计算机网络信息安全管理中涉及国家安全的事项。

⑦公安部:负责维护网络公共秩序和打击计算机网络犯罪。

⑧信息产业部:负责计算机网络信息安全产业管理工作。

⑨教育部:负责信息安全学科体系、专业和培训机构建设,信息安全学历和非学历人才培养。

⑩国家认证认可委员会:负责规划和协调全国信息安全产品和服务类型测试、评估和认证工作。

国家有关主管部门明确分工、加强配合,在各自的职责范围内发挥作用。

2.4.2 信息安全服务与技术管理机构

(1)国家技术标准体系

国家技术标准体系是我国信息安全技术,特别是发展和完善自主知识产权技术的重要法则,从国家意志层面规范信息安全体系结构、技术要素和交流语言的通用法则。国家技术标准体系的管理机构是国家质量监督检验检疫总局,它负责组织起草并颁布与信息安全有关的国家标准。在此基础上,国家和政府有关部门进一步制定符合中国国情的法规和技术细则。

(2)安全测评与认证体系

国家信息安全测评与认证体系,包括对密码与非密码、涉密与非涉密的涉及机密性、完整性和可用性的各类产品及系统,以及计算机病毒防范、查杀产品和系统的安全适用性和安全等级的符合度进行测试和认证。这些测试和认证工作,在国家认证和认可委员会的统一协调下,由国家或政府指定或授权的测试、评估和认证机构承担。

(3)应急响应体系

应急响应体系是我国信息安全应急响应处理和技术支持的工作体系。应急响应体系保证国家基础网络设施和重要信息系统在网络恐怖活动或公共网络突发事件影响下的生存能力和快速恢复能力。国家信息安全应急响应体系包括:

①国家信息安全应急处理协调委员会及其专职办公室,负责组织制定应急处理的

方针、政策、法规和标准,培育和保持一支应急处理网络突发事件和网络恐怖活动的队伍,协调国家各安全主管部门提高信息安全应急处理能力,组织采取国家信息安全重大应急行动。

②国家信息安全应急处理支援中心和国家应急信息交换中心,以及各行业与地区的对口应急机构,其职能包括:应急信息汇集和交换、应急资源管理、保护目标的信息安全档案管理、入侵检测与系统恢复、跟踪与取证、计算机病毒防治、安全预警信息分析与发布、信息安全情报协商与上报。

③国家信息安全应急处理的法律性文件和技术标准,如国家应急处理管理条例、应急服务组织的认证管理条例、国家应急响应等级标准、保护目标的安全等级标准、应急处理指标体系等。

(4) 计算机病毒防治与服务体系

国家设立计算机病毒应急处理中心,开展计算机病毒防治与服务,包括:发现、收集、解剖和分析计算机病毒;提交病毒疫情分析报告;发布计算机病毒疫情;为受计算机病毒攻击破坏的计算机用户提供后援服务;培训计算机病毒防治的工作人员等。

(5) 安全咨询服务

安全咨询服务指在规划、设计、实施、运行和维护信息系统的整个生命期,提供对系统的风险分析和安全需求分析、安全设计、安全检测、安全评估,以及技术培训和技术支持等项业务,以保障系统的可信性、可靠性、可用性、可控性和可核查性。

我国重要的安全服务单位有:

- 中国国家 CERT(计算机应急响应机构)。
- 国家计算机病毒应急处理中心。
- 中国互联网络信息中心。

3

信息安全管理要素与管理模型



3.1 概 述

3.1.1 信息安全管理活动

- ①决定组织的信息系统安全目标、方针和策略。
- ②识别和分配组织内的角色和责任。
- ③风险管理,包括识别和评估以下各项:
 - 被保护资源的分布及其价值。
 - 被保护资源的脆弱性。
 - 被保护资源的潜在威胁。
 - 对组织的不利影响。
 - 风险及其强度(值)。
 - 安全需求,即通过降低、转移和规避风险等方法对抗风险的需求。
 - 残留风险以及可接受风险值。
 - 适当的安全保护措施。
 - 约束条件,包括法律法规、技术规范、社会文化和意识形态、企业文化、外部物理和人文的环境,等等。
- ④监管,包括:
 - 决定安全事件的检测和响应机制。
 - 控制组织的信息系统安全态势。
- ⑤配置管理,包括:
 - 选取和配置组织的信息系统的安全措施。
 - 配置安全设备和重要资源的默认系统参数。
- ⑥变更管理。
- ⑦制订安全事件处理计划和灾难恢复计划。
- ⑧规划和开发提高安全意识的计划并开展训练。
- ⑨其他活动,包括:
 - 系统维护。
 - 安全审计。
 - 过程监理。

3.1.2 安全目标、方针和策略

一个组织的安全目标、方针和策略是有效管理组织内信息安全的基础。它们支持组织的活动并且保证安全措施间的一致性。安全目标表述的是信息系统安全要达到

的目的,安全方针是达到这些安全目标的方法和途径,安全策略则是达到目标所采取的规则和措施。

目标、方针和策略的确定可以从组织的领导层到操作层分层次地进行。它们应该反映组织的行政管理强加给信息系统的安全要求,并且考虑各种来自组织内外的约束,如国家法律法规、技术规范、社会文化及意识形态、组织的企业文化等,保证在各个层次上和各个层次之间的一致性。还应该根据定期的安全性评审(如风险分析,安全评估)结果以及业务目标的变化进行更新。

一个组织的安全策略主要由该组织的安全规则和指令组成。这些安全策略必须反映更广泛的组织策略,包括每个人的权力、合法的要求及各种技术标准。

一个信息系统的安全策略必须使包含在组织的安全策略之中的安全规则和适用于该组织信息系统安全的指令相一致。

信息系统的安全目标、方针和策略用安全术语(通常用一种自然的或社会化的语言)来表达,但也可能需要使用某些数学语言以更为形式化的方式来表达。这些表达的内容应该涉及下列关于信息系统及其资源的属性:

- 机密性。
- 完整性。
- 可用性。
- 抗抵赖性。
- 可确认(审查)性。
- 真实性。
- 可靠性。

安全目标、方针和策略将为组织的信息系统建立安全的等级,可接受风险的阈值(等级水平),以及组织的安全需求。

3.2 与安全管理相关的要素

3.2.1 资 产

安全保护的對象是信息系统资产,包括:

- 物理资产,如计算机硬件、通信设施、建筑物、机房设施等。
- 信息/数据,如文档、数据库等。
- 软件,如操作系统、通信协议和应用程序等。
- 生产产品或提供服务的能力。
- 人,包括管理人员和用户。

- 无形资产,如组织的信誉和形象。

识别资产并评估资产的价值是风险分析与评估的前提之一。在很多情况下,需要将资产进行编组或分类。

应该考虑资产的属性,包括资产的价值/敏感度,以及固有的安全特性。面临特定威胁的脆弱性将影响资产的保护需求。系统运行的环境、文化背景和法律体系也可能对资产及其属性产生影响,如在有些环境下,个人信息的保护显得非常重要,而在另一些环境下个人信息可能就不需要保护。环境、文化和法律变化对国际性组织及在跨国间使用的信息系统的安全影响可能很大。

3.2.2 脆弱性

与资产相关的脆弱性包括在物理布局、组织、过程、员工、管理、行政、硬件、软件或信息中的弱点或缺陷。这些弱点或缺陷可能被威胁利用而损害信息系统或业务目标。脆弱性本身并不产生损害,但脆弱性是威胁对资产造成损害的条件和途径。例如,缺乏访问控制机制将可能导致入侵事件并使资产丢失或损毁。需要考虑由不同原因(例如自然的或人为的)产生的脆弱性,除非资产本身有所改变使脆弱性降低或消失,否则脆弱性将一直存在。在一个具体系统或组织里不是所有的脆弱性都将受到威胁的利用。脆弱性如果存在对应的威胁,则必须立即找出脆弱性的存在或表现形式,并采取措​​施加以改善。由于环境可能动态地变化,因此应该监视所有的脆弱性,以便识别那些已经暴露给旧威胁或新威胁的脆弱性。

脆弱性分析是对那些可以被已知的和潜在的威胁利用的弱点进行评测,这种分析必须考虑环境和现有的安全措施。

脆弱性的评测结果可以用高、中和低来表示其严重程度的差异,也可以用更多的等级来更细化地表示其严重程度的差异。

3.2.3 威胁

资产面临着各种各样的威胁。威胁具有潜在破坏力,导致不良后果或对系统和组织及其资产造成损害。这些损害来源于对(正在被信息系统或服务处理的)信息的直接或间接攻击,如对信息的未经授权泄漏、修改、讹用以及使之不可用或者丢失。威胁利用资产存在的脆弱性损害资产。威胁可以是自然的或人为造成的,可以是偶然的或蓄意的。偶然的和蓄意的威胁都需要被识别出来,并对其危害等级和可能性做出评估。

表 3.1 是一些常见的威胁(形式)。

表 3.1 常见威胁示例

人为因素		环境因素
蓄意的	偶然的	
偷听、信息修改、系统劫持、恶意代码、偷窃、武力攻击等	错误和遗漏、文件删除、不正确的路由、物理事故等	地震、雷电、洪灾、火灾等

3.2.4 影 响

影响是一个有害的事件所造成的后果。事件由蓄意的或偶然的原因引起,对资产造成损害。事件的直接结果可能是破坏某些资产,毁坏信息系统,以及丧失机密性、完整性、可用性、抗抵赖性、可确认性、真实性和可靠性等。可能的间接影响包括资产流失、市场份额丢失或公司形象损坏。对影响的评估需要在有害事件的后果与阻止这些有害事件所耗费用之间进行权衡。有害事件发生的频度也是评估影响的重要因素。特别是在单个事件引起的危害较低、但多个事件所累积的危害很大时,需要考虑事件的发生频度。对影响的评估是风险评估和安全措施选择的重要基础性工作。

有很多方法可用来对影响进行定性和定量的度量,例如:

- 财务成本核算。
- 对其严重程度设定一个经验标度,如 1 ~ 10,或进行数值化表示。
- 使用表示影响程度的预定义形容词来度量影响程度,如低、中、高。

3.2.5 风 险

风险主要通过分析和评估威胁利用资产的脆弱性对组织的信息系统造成危害的成功可能性及危害的后果来度量。

一个威胁或多个威胁可以利用一个或多个脆弱性,一般并无固定的对应关系。风险用两种因素的组合来刻画:有害事件发生的可能性及其产生的影响。资产、威胁、脆弱性和安全保护等方面的任何变动都可能对风险产生巨大的影响。及早地检测以弄清楚环境或系统的变动就能增加识别风险的机会,以便采取合适行动减少风险。

3.2.6 残留风险

通常,通过安全措施的配置,风险可以被消除、降低或转移。一般来说,如要减少更多的风险,就需要更多的开销。实际上,信息系统通常都会存在残留风险,但这必须对信息系统业务是可以容忍的。因此信息系统安全的方法并不在于追求零风险,而在于获得适度的安全等级,或将风险降低到可接受程度。判断现有的安全措施是否充分,依据就是残留风险是否可以接受。

管理层应该能够意识到所有残留风险可能带来的影响以及发生某些事件的可能性。是否接受残留风险是由具有一定职位的负责人决定的,该负责人将承担由于有害事件发生而造成后果的责任,而当系统不能接受这种等级的残留风险时,他应该授权实施附加的安全措施或调整安全策略。

3.2.7 安全措施

安全措施是一系列技术和管理的实践、过程或者机制,用来减少脆弱性,对抗威胁,限制有害事件的发生和影响,检测有害事件和促进恢复活动。有效的安全保护通常需要结合使用多种不同的安全措施,为资产提供足够充分的一层或多层安全。

安全措施对于信息系统安全保障的作用和功能在于:

- 防范不期望事件或行为的发生。
- 威慑蓄意或敌意的入侵、攻击和破坏企图。
- 检测入侵和攻击行为、事件并发出告警和预警。
- 限制不期望事件的扩大和不良影响。
- 修正/校正已有安全措施使之满足安全需求。
- 恢复设备或系统的正常运行能力。
- 监视信息系统关键业务设施的安全运行态势。
- 增强与信息系统有关的多个层次人员的安全意识。

选择合适的措施对于正确地实现安全解决方案是极为重要的。

3.2.8 约束

约束通常由组织的管理者根据国家法律和系统具体情况设定,并且受组织的运行环境影响。常见的约束有:

- 组织的结构与机构。
- 业务运行流程。
- 业务计划及执行。
- 环境。
- 员工素质。
- 时间段或周期。
- 法律规定及强制度。
- 技术先进性与成熟度。
- 文化/社会背景及和谐程度。

当选择并实现安全措施的时候应考虑如下因素:定期复核现有的或新的约束,并识别约束发生的变化。约束可能随着时间、地理位置、社会环境和组织文化的变化而变化。组织运行的环境和企业文化将对一些安全要素,特别是对资产的脆弱性和威胁

和安全措施产生影响。

3.3 管理模型

信息安全管理有多种模型,各种模型都是从不同角度构建的,都有各自的优劣,但各种模型所提出的概念,都有利于对信息安全管理的原理和实践进行理解。归纳起来有以下几种模型:

- 安全要素关系模型。
- 风险管理关系模型。
- 基于过程的信息安全管理模型。
- PDCA (Plan-Do-Check-Act) 模型。

上述概念模型和组织的业务目标一起可形成一个组织的信息安全目标、方针和策略。信息安全的目标就是保证组织能够安全地运行,并且将风险控制在可以接受的程度。任何安全措施都不是万能的,即不是对任何风险都是完全有效的,因此需要规划和实施意外事件后的恢复计划以及构建可将损坏程度限制在一定范围的安全体系。

3.3.1 安全要素关系模型

信息系统安全是一个能从不同方面来观察和研究的多维问题。为了确定和实现一个全局的、一致的信息安全方针和策略,一个组织应该考虑与之相关的所有方面的问题。图 3.1 说明了资产可能受到大量潜在威胁的情况。一般来说,这些威胁的集合总是随时间变化的,并且只有部分是已知的。

这一模型表示的含义为:

- 环境,包含约束和威胁,它们是不不断变化的并且只有部分是已知的。
- 应予保护的组织的资产。
- 这些资产存在的脆弱性。
- 为保护资产和降低风险所选择的安全措施。
- 缓解风险的安全措施。
- 组织可接受的残留风险。

如图 3.1 所示,一些安全措施(S)可以在减轻与多种威胁(T)/多种脆弱性(V)相关联的风险(R)中起作用。有时需要几种安全措施才能保证残留风险(RR)是可接受的。在风险是可接受的情况下,即使出现预期威胁,也无必要采取额外安全措施。另外,一些情况下可以存在某种脆弱性,但没有已知的威胁利用它。可以实施一些安全措施来监视威胁环境,以确保没有威胁能利用该脆弱性。约束(C)影响安全措施的选择。

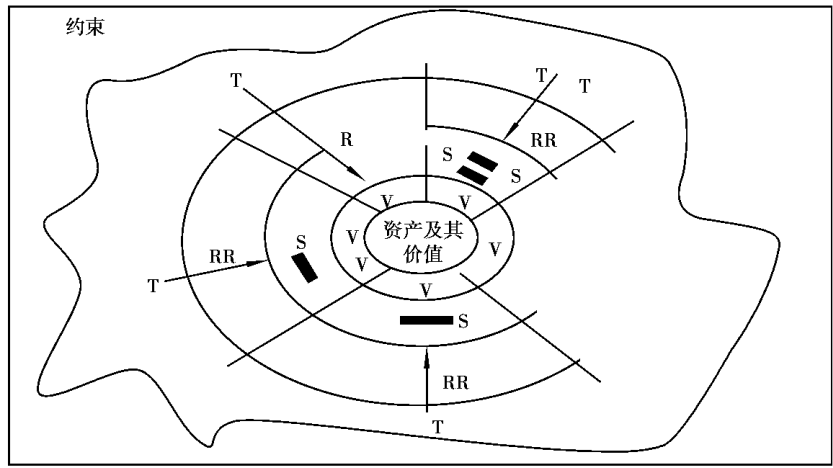


图 3.1 安全要素之间的关系

R—风险;RR—残留风险;S—安全措施;T—威胁;V—脆弱性

3.3.2 风险管理关系模型

图 3.2 阐述了与风险相关的安全要素之间的关系。为了简单清晰起见,该图只表示了主要关系。

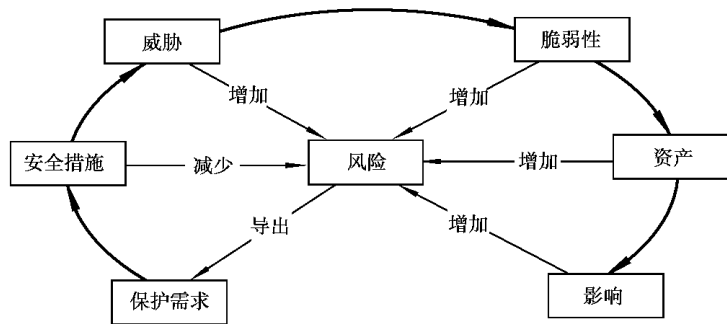


图 3.2 风险管理关系模型

信息系统的资产,如硬件、软件、通信服务,尤其是信息体等对组织业务的运行非常重要。这些对组织有价值的资产,可能存在风险,如信息的未授权泄漏、修改、抵赖,信息或服务的不可用或丧失。对这些风险,首先要识别出资产真实的价值,然后要考虑哪些威胁可能会造成影响,以及它们的影响有多大,还要考虑有哪些脆弱性可能会被这些威胁利用来造成影响。根据资产的价值、脆弱性的严重程度,以及威胁的等级确定出风险大小。对风险的识别和度量能够导出整个保护需求,保护需求通过安全措施的实现来满足。多重实现的安全措施可以对抗威胁并减少风险。

图 3.3、图 3.4 和图 3.5 分别说明了保护需求、脆弱性、影响和资产之间的逻辑关系。

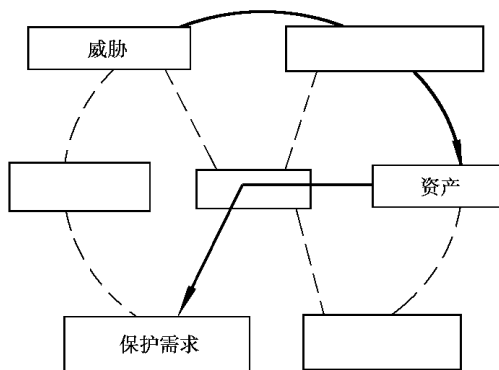


图 3.3 威胁视图

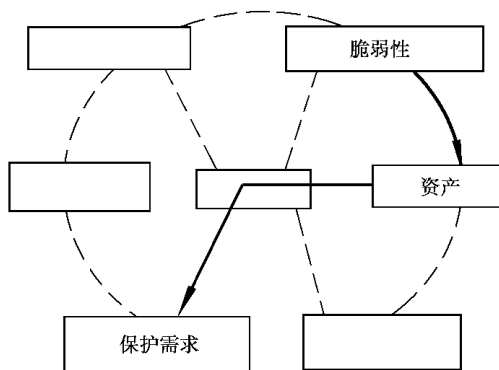


图 3.4 脆弱性视图

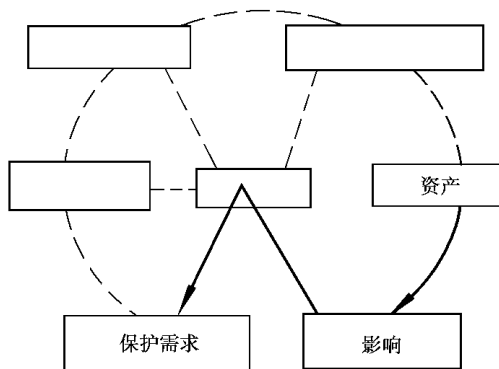


图 3.5 影响视图

3.3.3 基于过程的信息安全管理模型

信息安全管理是一个由许多子过程组成的不间断过程。其中一些过程,如配置管理和变更管理,可以用来控制安全以外的其他过程。经验表明,风险管理过程及其风险分析子过程在信息安全管理中极其有用。图 3.6 说明了信息安全管理中的几个方面,包括风险管理、风险分析、变动管理和配置管理等。

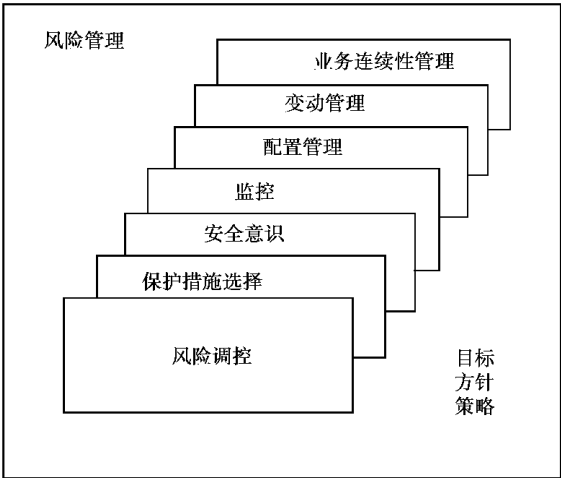


图 3.6 信息安全的组件模型

(1) 风险管理

风险管理是一个基于可接受的成本,对影响信息系统安全的风险进行识别、控制、最小化或消除的过程。风险管理根据评估的风险对保护收益和保护成本进行比较,从而导出与组织的信息安全策略和业务目标相一致的信息系统安全方针和实现策略。需要综合考虑不同类型的安全措施及配置这些措施所花费的代价和从保护中获得的收益的平衡关系。安全措施的选择同风险有关。可接受的残留风险的等级是风险评估的基准。重要的是,在识别和实现安全措施时所耗费的最小成本和组织所拥有的资产之间取得平衡是保证所有系统都得到适度的保护的前提。

风险管理是一种渐进的活动。对于新系统或者计划阶段中的系统来说,风险管理应该贯穿到设计和开发过程中。对于已经存在的系统,应该适时引入风险管理。而当计划对系统进行重大变更时,风险管理应该成为这一变更计划的一部分。风险管理应该考虑一个组织中的所有系统,而不应该孤立地应用到某一个系统,同时应注意到安全措施本身也可能包含脆弱性,进而可能导致新的风险。因此,选择安全措施必须小心,做到减少现存风险的同时不引进新风险。

(2) 风险分析

风险分析是对那些需要被控制或被接受的风险进行识别。信息系统的风险分析涉及对资产价值、脆弱性和威胁的分析。风险是通过资产的机密性、完整性、可用性、可靠性、真实性、抗抵赖性及可确认性的可能损坏进行识别和分析的。

(3) 责任分配与确认

责任分配与确认是风险管理中的一种有效措施,它明白无误地将责任进行分配并确定责任者。责任需要被分配给信息系统的资产所有者、管理者、供应商和使用者,并能在需要时予以确认。因此,资产的所有权和相关的安全责任,加上对安全行为的审计,可以落实并追究安全事件的责任,以此增强相关人员的安全意识,并对恶意行为构成威慑,对信息系统的有效安全来说非常重要。

(4) 监 控

监控是安全措施实施本身所需要的,它能确保安全功能正常发挥作用,并在安全设备运行期间,当环境改变后,仍能维持所设计的效能。系统日志的自动收集和分析,是帮助系统性能达到预期效果的有效工具。这些工具也可以用来检测有害事件,它们的使用可以对某些潜在威胁起到威慑的作用。

需要定期验证安全措施是否有效。通过监控和安全效能符合性的检测可以实现安全措施如期望的那样正常发挥功效。很多安全措施会产生输出,例如日志、报警信息等。通过检查这些输出可以发现安全事件和分析潜在的安全事件。系统审计功能可以在安全方面提供有用信息,并能提供监控所需的输入信息。

(5) 安全意识

安全意识是确保信息系统安全所需的基本要素。组织中有关人员缺乏安全意识和恶劣的陈规陋习会在相当大的程度上降低安全措施的有效性或者引发风险。一个组织中的个体通常被认为是信息安全链中的薄弱环节之一。为确保组织中每个人都有足够的安全意识,非常有必要建立和维持有效的安全意识规程和加强训练。这个规程的主要目的是向组织的雇员、合作伙伴、供应商阐明:

- 安全目标、安全方针和策略。
- 与他们相关的角色和责任的安全需求。
- 从职业道德和行政、技术法规上需要养成的良好习惯和必须遵从的行为规范。

此外,此规程还应规范雇员、合作伙伴和供应商在安全体系中承担的安全责任和义务。

应使组织内从高层管理人员到负责日常活动的每个人知晓并实施安全意识规程。通常需要针对组织中不同部门的人、不同的角色以及负不同责任的人,开发和提交不同的安全意识教育材料。一个比较合理的综合安全意识规程是分阶段开发和提交的。每个阶段都以以前的经验为基础,从安全的概念开始,到如何解决执行与监控安全的

责任问题。

组织内的安全意识规程可以包括各种各样的活动,其中一个活动是安全意识材料的开发和发布。另一个活动是举办训练课程,对所有员工有针对性地进行合适的安全实践培训。此外,训练课程还应提供若干特定安全专题方面的具有专业水准的教育。一般来说,在业务培训计划中加入安全意识知识是行之有效的。对于安全意识规程的开发,需要考虑以下几个问题:

- 需求分析。
- 安全意识规程的内容。
- 规程的提交。
- 对规程执行情况的监控。

(6)配置管理

配置管理或控制是启动并维持系统配置的过程,这一过程能够以正式或非正式的方式完成。配置管理的基本安全目标是确保及时得到更新的系统配置文件,以及以降低安全措施效能和组织的整体安全的方式对已批准的系统变更进行管理。

(7)变更管理

变更管理是另外一种过程,当一个信息系统发生变更时用来帮助识别新的安全需求。信息系统及其运营环境经常发生变化,这些变化或者是由新的信息系统特性和服务所导致,或是因为发现新的脆弱性和威胁。信息系统的变更包括:

- 新的程序。
- 新的特性。
- 软件升级。
- 硬件更换。
- 新增加用户,包括外部组或匿名组。
- 增加子网和与外部网络互连。

当信息系统发生变动或者计划变动信息系统时,重要的是要确定这些变动会对系统的安全带来什么影响。如果系统拥有配置控制中心或者其他组织机构来管理系统的技术变动,那么应指定信息系统安全官员并赋予相应的职责,以便对这些变动是否会影响系统的安全以及会有什么影响做出判断。在某些情况下,需要对变动可能降低系统安全的理由进行分析。这时往往需要评估安全性降低的程度,并基于所有有关的事实做出管理决策。换句话说,改变一个系统需要适时地考虑对安全的影响。对于涉及购买新的硬件、软件或服务的重大改变,需要分析以确定新的安全需求。另一方面,许多变动只造成小的系统性能变化,不需要像大变动那样做深入的分析。然而不管系统变动或大或小,都需要进行风险评估,确定保护的收益与保护的平衡。

(8)业务持续性管理

业务持续性管理是不断发展和维持业务的管理过程。业务持续性管理为确保业

务的连续运营而提供进程和资源的持续可用性。业务持续性管理包括应急计划和灾难恢复。

①应急计划是当(包括信息系统)运行和支持能力降低或不可用时如何维持基本运行业务的保证。这些计划应该涉及各种可能的情况,包括:

- 规定各种业务中断的时间长度,预估不同类型设施的损失。
- 估计的房产及其附属建筑物的总损失。
- 恢复到损坏发生前的状态。

②灾难恢复计划描述怎样恢复运行受有害事件影响的信息系统。包括:

- 制订灾难的识别准则。
- 激活恢复计划的职责。
- 各种恢复活动的职责。
- 恢复活动的过程描述。
- 测试恢复计划是否有效的职责。

(9) 风险调控

风险调控过程贯穿于安全工程的整个生命周期,图 3.7 说明风险调控的各个环节及其调控流程。

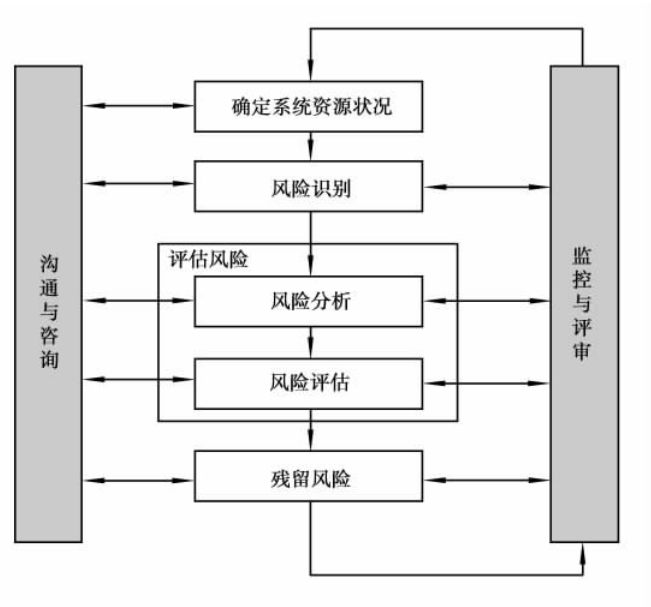


图 3.7 风险调控过程概览

3.3.4 PDCA 模型

PDCA(规划—实施—检测—改进)模型如图 3.8 所示,其中 ISMS(Information Se-

curity Management System)表示信息安全管理体制。

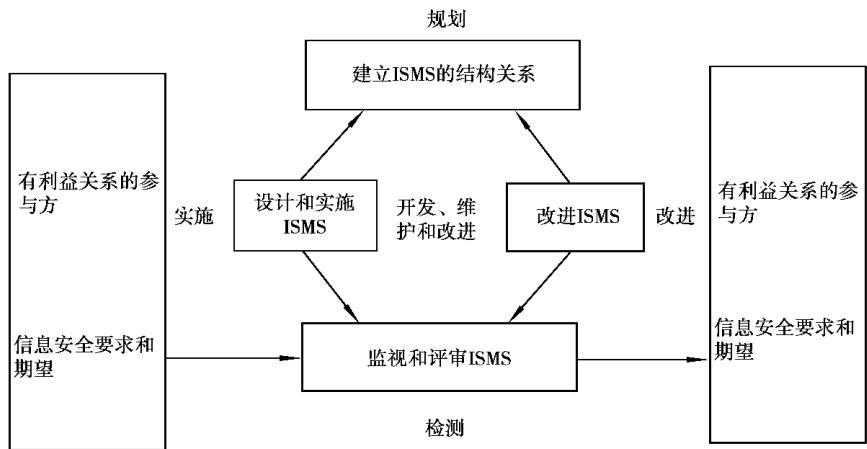


图 3.8 PDCA 过程模型

(1)各模块功能

现对过程模型中的各模块分别描述如下：

- ①规划(Plan):建立 ISMS 的结构关系。建立与信息安全相关的安全目标、安全方针、安全策略、安全过程和安全规程;提交与组织的整体目标和方针相一致的文档。
- ②实施(Do):设计和实现。对过程管理程序进行设计和实现。
- ③检测(Check):监控和审核。根据安全目标、方针、策略和运行实践来量度和评估过程管理的性能并把结果报告给决策者。
- ④改进(Act):进一步改善过程管理的性能。

(2)建立信息安全管理体制的步骤

如表 3.2 所示,建立一个信息安全管理体制(ISMS)有 6 个步骤。

- ①第 1 步:制订信息安全管理策略。考虑所有信息资产以及它们对组织的价值,然后设置一个可以用来识别信息重要程度以及理由的策略。从实践的观点来看,只有那些具有重要价值的信息才需要得到关注。
- ②第 2 步:确定管理的范围。排除低价值的信息,确定整个组织所关心的信息种类或信息体。这种情况下,需要考虑所有的信息系统资源和它的外部接口资源以及通信电子表格、文件柜、电话交流、公共关系等范围之内的信息。或者将注意力集中在特定的面向用户的系统资源上。

表 3.2 建立信息安全管理体系的步骤

步 骤	管理活动内容	关键因素或结果
第 1 步	制订信息安全管理策略	
第 2 步	确定管理的范围	信息资产
第 3 步	风险评估	脆弱性、威胁、影响
第 4 步	风险管理	组织的风险管理方法
第 5 步	选择安全措施	控制设备和控件;附加的控件
第 6 步	可用性的说明	

③第 3 步:风险评估。判断资产损失的风险。要考虑影响风险的方方面面,极端情况还要考虑技术的复杂性、开发新技术及其业务压力,以及工业间谍活动和信息战等方面对风险评估的影响。

④第 4 步:风险管理。决定如何管理风险,包括对技术、人员、管理程序和物理方面的因素以及保险契约等的风险管理。风险一旦发生,需要想办法抑制或减小危害,更需要一个有效的可持续计划。

⑤第 5 步:选择安全措施。按安全需求选择安全措施,例如选择合适的管理风险的方法。

⑥第 6 步:可用性的说明。需要证实所选择的所有安全措施的足够性并证明它们的正当性,以及说明没有被选中的安全措施是与本项不相关的。

4

信息系统生命周期的安全管理



本章从两个方面介绍信息系统生命周期的安全管理：一是安排和规划信息安全，二是信息安全管理技术。

安排和规划信息安全，描述信息安全的管理和计划方面，涉及与组织信息系统有关的管理人员及其职责，例如，负责监督信息系统设计、部署、实施、测试或操作的管理员，或对信息系统实际使用负责的管理员及其职责。

信息安全管理技术描述在一项工程的生命期里与管理有关的活动（例如规划、设计、部署、实施、测试或操作等）所用的安全技术。

4.1 安排和规划

本部分涉及信息安全的各种安排和规划活动的内容，它关系到信息系统的规划、建设、运行、维护过程中管理者的职责，同时也关系到那些对信息系统的实际应用活动负责的管理者。总之，这一部分的内容对一个组织的信息系统中有管理职责的人都有用。

政府和商业机构在很大程度上依赖信息系统来指导和完成业务活动并与公众、社会实现交互。信息和服务的机密性、完整性、可用性、可审计性、真实性和可靠性的丢失，会给组织带来不利影响，因此迫切需要保护信息系统的信息和提高相应的安全管理水平。在开放系统互连网络环境下的信息系统，由于组织内外的网络是互相连通的，这种信息保护更为重要。

信息安全管理是一个获得机密性、完整性、可用性、可审计性、真实性和可靠性，并将其维持在一个合适的水平的过程。信息安全管理的内容包括：

- 决定组织的信息安全目标、方针和策略。
- 决定组织的信息安全需求。
- 识别和分析组织内需要保护的信息系统资产及其脆弱性和安全威胁。
- 识别和分析安全风险。
- 选择合适的安全措施。
- 监控组织内用于有效保护信息和服务的安全措施的实施和运行状况。
- 开发和实施安全意识教育工程。
- 检测突发事件并做出反应。

为了履行对信息系统的管理责任，安全必须作为组织的管理计划中不可缺少的组成部分，分布于组织的各个功能过程中。因此，在这里并不注重拓宽管理的一般含义，而更侧重于安全方面的管理与一般管理的联系。

图 4.1 从安排和规划的角度描绘了安全管理过程的主要阶段和活动。

组织的信息安全保护的出发点是保护业务目标的实现，然而为了实现这一目标就需要制订信息安全策略。因此，安全策略只有作为组织结构的一部分，其既定的安全

目标才能得以实现。

图 4.1 所描述的安全管理过程大致分为 5 个部分：组织的信息安全策略、信息安全组织因素、风险管理、实施以及后续活动（维护、监控、检查、培训、评审等）。

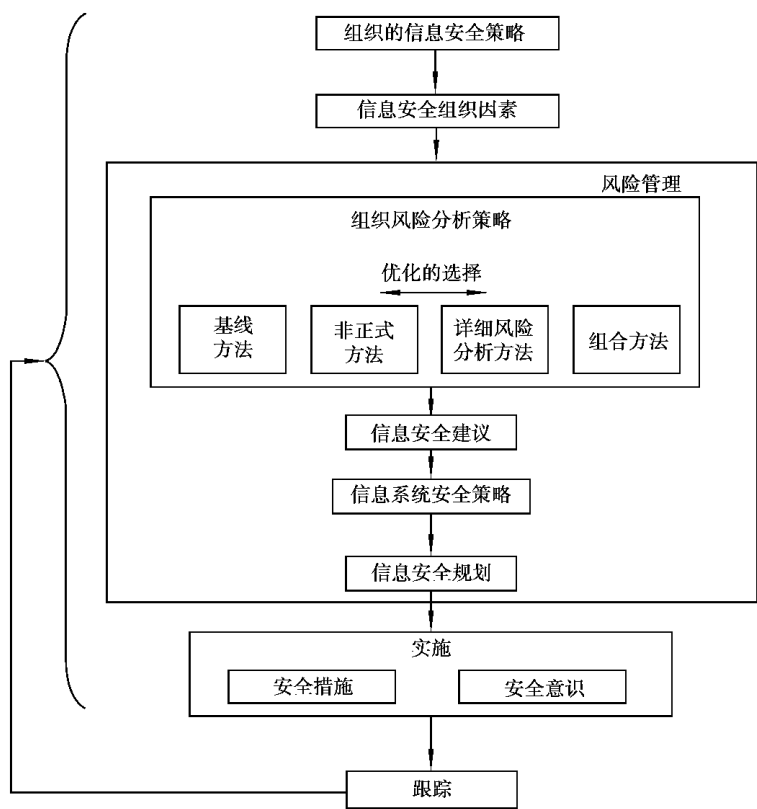


图 4.1 安全管理过程

4.1.1 组织的信息安全策略

(1) 管理委员会

一个组织的管理委员会是信息安全最高决策机构，信息安全策略需要得到他们的正式批准，并且要为其建立文档。组织的信息安全策略应服从组织的安全策略。

(2) 策略关系

作为阐述组织信息系统安全策略的基础，组织的安全策略一般应该包括组织的技术和管理策略。信息系统安全策略的陈述应该使用简明的、有说服力的语句来阐明安全的重要性，特别是当安全必须依从于某个具体策略的时候尤其如此。一般来说，组织的安全策略、信息技术策略和业务策略等是组织的信息安全策略的基础，而组织的

信息系统安全策略则是下属部门信息安全策略的基础,以此类推。无论一个组织采用什么样的组织结构和使用什么格式的文档,重要的是保持策略有关信息之间的一致性。

(3)组织的信息安全策略要素

信息安全策略至少应包括以下要素:

- 信息安全需求(比如机密性、完整性、可用性、可审计性、真实性和可靠性需求,尤其是要尊重资产所有者安全需求的意愿)。
- 组织的基本结构和责任分配。
- 将安全特性综合到系统生命周期的获取过程中。
- 指令和规程。
- 信息安全分级定义。
- 员工选聘、上岗、下岗、解聘或辞退规范(对在岗员工,尤其是维护人员、系统管理员和主要业务岗位操作人员特别需要加强管理)。
- 安全意识有关的职业道德和业务素质的培训和实施。
- 法律的和管理责任。
- 外购外包管理。
- 风险管理方针。
- 应急和恢复计划。
- 安全事件处理规范和实施计划。

4.1.2 信息安全的组织

1)角色和责任

信息安全与每一个信息工程和系统以及组织内信息系统的所有管理者和使用者都有关。责任的指定和划分,应该保证高效完成所有的业务。不管组织的规模、结构和管理体系,也无论实现信息安全目标的方式,都应配备下面的角色:信息安全管理委员会,用于解决跨技术学科的协调问题及通过行政指令和技术规范;信息安全官员,一个组织内信息安全各个方面的组织者和指挥者(实际上是组织内部所有信息安全方面的权威)。

应该对信息安全管理委员会和信息安全官员两类角色进行良好定义和责任划分,并且保持其在信息系统中的适当地位,以确保在执行团体的信息安全策略时有充分的人力、资金、资源及权威性。

(1)信息安全管理委员会

该委员会应包括这样的一些人士,他们具有识别安全需求、确定安全策略、解释安全策略、草拟安全规程、评审安全有效性以及指导信息安全官员等所必需的知识

能。这样一种委员会充当的角色是：

- 向信息系统管理机构提供关于战略安全规划方面的建议。
- 正式形成支持信息系统战略的本组织的信息安全策略,并获得信息系统管理机构的正式批准。
- 将本组织的信息安全策略转换成为信息安全执行项目。
- 监督信息安全活动的执行。
- 评审组织的信息安全策略的有效性。
- 提高信息安全意识和技能水平。
- 对规划过程和信息安全活动的实现中所需要的资源(人力、财力、知识等)提出建议。

为使信息安全管理委员会具有效力,委员会应该包括具备安全和信息系统技术知识背景的成员,以及典型的信息系统供应商和使用者代表,因为开发一个实用的组织的信息安全策略需要这些领域的知识和技能。

(2)信息安全官员

由于信息安全的责任较为分散,可能存在一种风险,即最后可能没有人对整个系统或子系统的安全负责任(没有人对全局、局部安全负责)。为了避免此问题,应将责任分解后指定给具体的人。建议设立这样一个专门的岗位,选择一个具有安全和技术背景的人作为信息安全官员。信息安全官员的活动应成为一个组织内信息安全各个方面的核心。其主要职责是:

- 从细节上管理信息安全活动的实施。
- 适时向信息安全管理委员会和组织的安全主管官员报告安全状况。
- 牵头事件调查并起草处理意见。
- 管理全组织范围的信息安全意识项目。
- 为信息系统工程和系统管理员以及下属部门的信息安全官员分派有关的安全事项。

2)主动支持

有效的信息安全需要得到各个层次管理人员的支持,这些支持包括:

- 理解组织的全局业务需求。
- 理解组织内的信息安全需求。
- 采用示范方式推动信息安全。
- 无保留地陈述信息安全需求。
- 愿意将资源分配给信息安全需求。
- 最高领导层清楚地意识到信息安全的含义、范围和程度。

应该信息安全的目标把通告给整个组织的每一个雇员或者合同人,让他们都清楚

知道自己的角色和职责,以及他们对信息安全的作用及他们受委托应实现的目标。

3) 协调一致

应对所有的开发、维护以及运行活动进行协调,确保将安全保护贯穿到信息和信息系统的整个生命期。组织方面的结构必须适应与信息安全有关的协调活动,这就需要得到与规范和标准相一致的各个管理层次的支持。这些规范和标准用于解决跨技术学科的协调问题,可能是行政性的和技术性的,包括国际的、国家的、行业的、地方的、区域性的以及组织自己的,需要根据组织的信息安全的需求进行选择和应用。

使用规范的好处包括:

- 系统可获得综合性的完整的安全。
- 可获得系统间的互操作性。
- 可获得系统内各部分在安全和效率之间的平衡。
- 可获得可移植性。
- 系统缩放时具有经济可行性。
- 利于组织间的业务交互和信息资源共享。

4.1.3 风险分析方法

1) 风险分析策略

任何组织的安全需求都与其业务运行的规模、方式及其环境和文化紧密相关。风险分析策略的选择也与这些因素有关。

有时候,一个组织可能决定暂不或暂缓执行某些安全措施,这种情况只能出现在该组织的信息安全策略已获得高层审核并通过之后。在做出这样的决定之后,要意识到风险可能产生的不利影响,以及突发事件导致的可能后果。只有在慎重考虑可能出现的种种不利影响之后,才能做出不保护或者缓保护某些资产的决定。

在开始风险分析活动前,一个组织应该以文档说明方式确定风险分析的方针并商定选择风险分析方法的办法和准则。风险分析方针应保证选择的方法适合信息系统的运行环境,并且把安全努力集中到真正需要的地方。下面给出的选择,描述了4种不同的分析方法。各种选择的基本区别是风险分析的深度和细微程度。对所有的信息系统都做详细风险分析会造成太大花费,另一方面对重要风险只给予一般的注意也是不合适的,所以需要在各种选择间进行平衡。

这4种基本选择是:

①选择1:不考虑系统面临的危险,对所有的系统使用同样的基线方法,并接受那些也许并不合适的安全风险。

②选择2:使用非正规方法进行风险分析。

③选择3:使用正规方法进行详细风险分析。

④选择4:起初用一种高等级风险分析方法将暴露在高风险下并对业务起决定性作用的信息系统或子系统识别出来,继而对该样的信息系统进行详细风险分析,并对其余系统采用基线法。

上述4种选择分别对应于:基线法、非正式法、详细风险分析法和组合法。

如果一个组织决定在安全方面不实施或者推迟实施安全保护措施,那么管理部门应该清楚这个决定可能产生的后果。一个组织如不遵从法律和法规约束,那么这个组织必须承担由此造成的影响。对大多数组织来说这种做法是不可取的。

(1)基线法

如果一个组织的信息系统只有低等级的安全需求,这种情况宜选择基线法来反映信息系统需要的大多数保护,这可能是费用效率比最佳的策略。多数组织总是面对一些敏感数据需要遵从法律和法规的要求而进行最低等级保护。但是当一个组织各个系统的业务敏感度、规模和复杂性不同时,将一种普遍的标准应用到所有系统则是不合逻辑的,也不能获得合理的成本效益比。

基线法是选择一套安全措施使所有系统都取得某一基线水平的保护。在基线文档和实施规范中应有很多关于安全措施的建议。在对基本需求进行评审之后,这些具有普遍性的安全措施可以在国内外的其他标准及建议中选用。

基线法的优点是:

①对每个保护措施实现的风险分析和管理所需要的资源数量最小,选择保护措施时耗费的时间和工作量最少。

②基线保护措施是一种可提供高效费比的解决方法。如果组织的大量系统都在普通环境下运行,很多系统都可以简便地采用基线方法。

基线法的缺点是:

①如果基线水平设置得太高,那么整个信息系统的安全等级和保护成本可能会太高。

②如果基线水平设置得太低,那么信息系统中某些部分的安全等级可能无法获得满足,从而导致更高等级的风险。

③在对与安全相关的变更进行管理时,可能出现困难。例如,如果一个系统升级了,就很难评估初始的基线保护措施是否足够。

(2)非正式法

这种方法是对信息系统中所有部分采用一种非正式的但却实用的风险分析。它不是基于结构化的方法,而是利用个人的经验和知识。当内部安全专家不在现场时,组织外的安全顾问们也可以进行类似分析。

非正式法的优点是:进行这种非正式的系统风险分析不需要学习更多的技能,而且比详细的风险分析来得快。所以这种方式适用于小企业单位的信息系统,比较经济

实惠。

非正式法的缺点是：

- ①由于分析没有采用结构的方法,所以可能漏掉一些风险及风险区域。
- ②保护措施只是基于已被识别的脆弱性来配置的,而没有考虑到是否存在进一步利用这些脆弱性的威胁。
- ③由于采用非正式的方法,分析结果可能受审核人员主观因素和个人偏好的影响。
- ④很难证明根据这种风险评估方法所采用的保护措施是否合理和充分。
- ⑤由于在安全措施选择上缺乏调整余地,所以在安全措施上的费用也很难调整。
- ⑥在不进行重新审核的情况下,如果系统的变更与安全相关,很难对这些变更进行管理。

基于以上的缺点,这种选择对很多组织的风险分析并不是一个有效的方法。

(3)详细风险分析法

这种方法包括资产的识别、对资产脆弱性和威胁等级的系统性分析等。这种风险评估方法通过识别资产的风险、通过管理将风险降低到可接受的程度,从而支持安全措施的识别、挑选和选定。详细的风险分析是一个非常耗费资源的过程,因此需要认真确定边界并给予持续的关注。

详细风险分析法的优点是：

- ①对每个系统而言,都有量身定制的安全等级保护措施满足其安全需求。
- ②对与安全相关的变动的管理可以从详细风险分析中获益。

详细风险分析法的缺点是:要得到较好的结果,需要付出相当多的时间、努力和费用,并且要求分析人员具有专门的知识。因此,对所有的信息系统都使用详细风险分析是不明智的。

(4)组合法

这种方法首先使用高等级的风险分析方法将那些对业务运营来说有较高风险强度或重要的系统识别出来。基于这些识别出来的结果,将系统分为两类,一类是需要使用详细风险分析法使其达到合适的保护,另一类则是只用基线法保护就足够了。这就是分类保护的基本思想。

组合法综合了基线法和详细风险分析法,它在安全保护和成本开销之间维持一个平衡,既节约资源,又达到既定的保护要求。

组合法的优点是：

- ①可以建立一个安全工程策略图,协助做出进一步更优的规划。
- ②将资源和资金用在最需要的地方,对风险最大的地方做出预案。

组合法的缺点是：

- ①如果高等级风险分析导致不准确的结果,则某些需要详细风险分析的系统可

能会被漏掉而导致无法预测的后果。

②对从事风险分析的人员的专业知识要求高。

在多数情况下,这是最有效的风险分析方法,大多数组织都可采用。

2) 信息安全建议

无论采用上面介绍的哪一种风险分析方法,都应提供能将安全风险降到一个可接受等级的建议。这些建议应该包括下列各项,并应获得管理层的批准:

- 决定风险可接受等级的准则。
- 使风险降到可接受水平所需选择的安全措施。
- 安全措施的实施好处,以及通过这些安全措施而降低的风险程度。
- 所有的安全措施都实施后,是否接受仍然存在的残留风险。

(1) 安全措施的选择

有几种类型的安全措施可供选择:

①预防、监视、检测、减少有害事件。预防措施可以包括阻止有害行为以及增强安全意识的活动。

②从有害事件中恢复。

安全措施应用的主要区域包括:

- 硬件(备份)。
- 软件(电子签名、日志、反病毒工具)。
- 连接与通信(防火墙、数据加密)。
- 物理环境(电磁屏蔽、标记、门禁)。
- 员工(安全意识、雇佣的起止程序及在岗考核)。
- 管理(授权、硬件处置、许可证控制)。

安全措施一般应协调发挥作用而不是相互独立地运行。选择安全措施时必须考虑到它们的相互关联。在选择安全措施时,严防可能存在安全间隙或空白。这些间隙绕过已有的安全措施留下漏洞,存在意外威胁对资产造成破坏的可能性。

对新系统或有重大变动的现有系统而言,安全措施的选择可以包括安全体系结构的设计。安全体系结构是整个信息系统体系结构的一部分。它描述安全需求,以及信息安全系统与安全措施的合乎逻辑的安排与布局。它考虑安全措施的技术方面,同时也涉及非技术因素。

所有的安全措施都需要有管理来保证其有效运行,很多安全措施的维护需要行政的强力支持。在选择安全措施的过程中这些因素必须予以考虑。

重要的是,安全措施的实施必须发挥预期效能并且避免带来不适当的用户及日常管理开销。如果安全措施的实施导致用户和管理过程的重大变动,那么它们的实施就应该和安全意识活动项目、变更管理、管理配置等过程综合起来考虑。

(2)可接受的风险

在实施选定的安全措施后,系统仍然存在残留风险。这是因为一个系统不必也不可能做到绝对安全或零风险,因此会有意或无意地留下一些未予保护的地方(比如,假定风险很低,或相对于要保护的资产的价值来说,被推荐的安全措施成本太高)。

残留风险的处理过程的第一步,是复审所选安全措施以及识别和评估所有残留风险。接下来是将残留风险分为两类:可被组织接受的和不可接受的。不可接受的风险不能被容忍,因此应该考虑额外的安全措施以限制其带来的影响和后果。

3)信息系统安全策略

信息系统安全策略由用来保护系统和服务的规则和指令组成。这些策略保证信息系统和服务达到足够的安全等级要求。

在制定信息系统的安全策略时,要着重考虑的是:

①定义信息系统及其边界。

②定义系统所要实现的业务目标,因为它们可能影响系统的安全策略以及安全措施的选择与实施。

③下述原因引起的对业务不利的潜在的定量影响(例如直接或间接的经济损失)以及定性影响(例如声誉损失、生命损失和个人隐私暴露):

- 服务和资产(包括信息)的不可用、抵赖或破坏。
- 非授权修改信息和软件。
- 非授权暴露或泄漏信息。

④信息系统的投资能力和规模。

⑤脆弱性分析,包括可使信息系统受到已知威胁攻击的薄弱环节。

⑥对信息系统及被处理的信息的重大威胁。

⑦安全措施需求。

⑧信息安全的成本,比如保护信息资产所需的开销(信息安全的开销实际上是信息系统所有者开销的一部分)。

⑨与供应商、外包商(例如计算中心、个人计算机提供商等)的关系以及选择供应商、外包商的原则。

信息安全需要一个规划方法,它在安全策略的制订中起重要作用。因此应该保证安全从一开始就被规划和设计到体系中。在大多数的情形下,将安全放在最后来规划不但会增加安全开销,更为严重的是这种规划根本不可能满足安全需求,并可能存在致命缺陷。

4)信息安全规划

信息安全规划是一系列文档,定义实现一个信息系统安全策略时应采取的协同活

动。这个规划应该包含在小的、中等的和大的范围内采取的主要活动,以投资、运行成本、工作量等表示的成本,以及实施时间表。具体包括:

- ①总的安全体系结构和设计。
- ②确定与被评估风险相关、通过管理使其保持和生效的安全措施。
- ③对安全措施的实际置信度(包括效率)进行评估。
- ④在给定系统或应用的环境中对残留风险进行总体评估。
- ⑤为实施安全措施制订详细工作计划,包括优先级、预算、时间表。
- ⑥工程控制行为,包括资源委托和责任分配及确定进度报告程序。
- ⑦信息系统的职员和终端用户的安全意识教育及技能培训。
- ⑧确定开发安全操作及管理过程中的需求。

为确认上述各项事宜,在规划中需要定义条件和行为以及对规划本身的修改原则。

4.2 管理的技术方法

信息安全管理包括安全需求分析,满足这些需求的安全设计、设计的实现,以及对已实现的安全进行维护和管理。这个过程在建立组织的信息系统安全目标和开发组织的信息安全策略时就开始了。

信息安全管理过程的一个重要部分是风险评估,以及风险如何被降到可接受的水平。在风险评估的同时,为了达到该目的每个信息系统都要配置合适的安全措施。

信息安全管理包括维护、安全遵从性检查、变更管理、监控和事故处理等各种后续活动。图 4.2 列出了信息安全管理技术所涉及的各个部分。

4.2.1 信息安全的目标、方针和策略

目标(要实现什么)、方针(如何达到目标)和策略(为达到目标需遵循的规则)可以在一个组织的每个层次和每个业务单位或部门定义。为了达到高效的信息安全,有必要针对组织的每个层次和业务部门的实际需求确立不同的目标、方针和策略。重要的是使多层次和业务部门的这些文档之间保持一致性,因为许多安全措施可能是共同的。

建立组织的信息系统安全目标之后,应开发信息系统安全方针,为组织的信息系统安全策略的开发打下基础。为了确保风险管理过程的结果的合适和有效性,科学地开发组织的信息系统安全策略至关重要。这需要整个组织在管理方面的协同和支持。组织的信息安全策略必须使组织的安全策略和组织的业务策略保持一致。有了一致性,组织的安全策略才能对信息安全策略实施时所需的系统资源提供有效帮助,并且能确保在各种不同的系统环境里保持一致的安全方法。

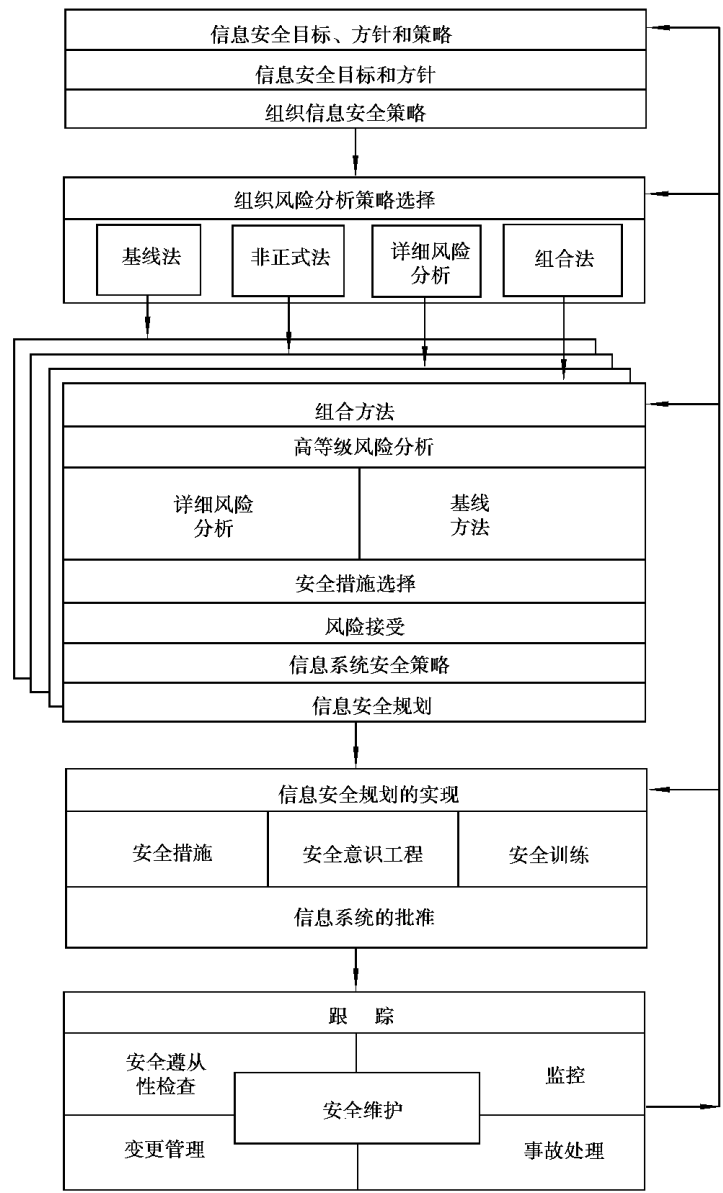


图 4.2 信息安全管理技术

必要时可为每个或某些信息子系统开发独立的和专门的安全策略。

(1) 安全目标和方针

作为信息安全管理过程的第一步,应考虑的问题是“多大的风险水平对这个组织是可接受的”。正确的可接受的风险水平和合适的安全保护等级,是安全管理成功的

关键。所需的安全等级是由组织的信息系统安全目标决定的。为了评估这些安全目标,应该考虑信息系统及其资产对于这个组织的价值。评估一个组织对信息系统的依赖程度必须考虑的因素有:

- ①识别出没有信息系统的支持就不能开展的业务。
- ②识别出只能在信息系统帮助下才能完成的任务。
- ③识别出组织中必须依赖于信息系统所处理的信息的准确性、完整性或可用性。
- ④识别出需要保护的那些被处理的机密或敏感信息。
- ⑤评估对组织有害的不期望事件可能造成的后果。

解决这些问题可以帮助建立一个组织的安全目标。例如,如果一个业务的一些重要或很重要的部分依赖于准确的或最新的信息,那么这个组织的一个安全目标就是要确保信息在系统中处理时的完整性和实时性。而且,在评估安全目标的时候要考虑重要的业务目标和它们与安全的关系。

信息系统安全方针用一般术语来简述一个组织如何实现它的信息安全目标。方针将依赖于安全目标的数量、类型和重要性,以及是哪个部门或业务认为应该在整个组织内统一提出来,这些内容可能很具体,也可能很宽泛。

作为具体安全方针的一个例子,假设一个组织因为其业务的性质,需要所有的系统都维持一个高等级的可用性目标。在这种情况下,安全方针所提出的可能就是直接通过全组织范围安装杀毒软件来维持系统业务的连续可用性。

为了说明安全方针的广泛意义,假设一个组织的业务是出售信息服务,可以在一个更宽泛的范围内有一个信息安全目标,向潜在的顾客证明其系统的安全性。那么安全方针所提出的可以是所有的系统都要被共同信任的第三方来证实确实是安全的。

具体的或宽泛的安全方针可以包括:

- 在整个组织范围内采用的风险分析方针和方法。
- 系统的信息安全策略需求。
- 系统的安全操作规程需求。
- 整个组织范围的信息敏感度分类方案。
- 在连接到其他组织前,需要满足和检查的连接安全条件需求。
- 能被普遍应用的事故处理方案。

(2) 安全策略

一个组织的信息安全策略应在组织的信息安全目标和方针基础上产生。建立和维护信息安全策略,需要保持与组织的业务、安全策略、信息策略以及法律法规的一致性。

如前所述,影响组织信息安全策略的一个重要因素是组织在多大程度上依赖于它使用的信息系统。组织对信息系统的依赖程度越大,就需要越多的安全来保证业务目标的实现。在制订组织的信息系统安全策略的时候,还应充分考虑组织的文化、环境

和机构的特点,因为它们会影响实现安全的途径,例如,一些安全措施可能很容易在一种环境下被接受,但在另一环境中完全不被接受。

在开发组织的信息安全策略时,以下职能部门的代表应该参加:

- 审计。
- 财务。
- 信息系统(技术人员和用户)。
- 公共事务/基本设施(例如负责建筑、供电和空调的人员)。
- 人事部门。
- 安全。
- 业务高级管理层。

组织的信息安全策略的详细程度根据安全目标和一个组织为实现这些目标而采取的方针决定。

组织的信息安全策略至少要描述:

- 适用范围和目的。
- 考虑了法律、法规和业务目标的安全。
- 用机密性、完整性、可用性、可确认性、真实性和可靠性来表示的信息安全需求。
- 覆盖组织和个人的责任和权限的管理。
- 组织所采取的风险管理准则。
- 能够用来确定安全措施实施优先级的准则。
- 组织要求的安全等级和残留风险的接受准则。
- 访问控制的一般准则(对建筑、房间、系统、信息的逻辑控制和物理控制)。
- 组织内的安全意识教育和训练安排。
- 检查和维护安全的规程。
- 一般员工的安全管理规程。
- 把策略传达到所有有关人员的规程。
- 策略应在何种情况下进行复审。
- 对策略的更改进行控制的准则。

在对组织的信息安全策略进行描述时,应考虑:

- 组织范围内的安全模型。
- 使用的标准和规程。
- 安全措施实现步骤。
- 后续活动,包括安全遵从性检查、安全措施的监控、安全事故的处理和信息系统的

使用监控。

- 何时何地雇佣组织外的安全顾问。

以前的风险分析、管理评审、安全遵从性检查和安全事故的结果很可能会影响组

织的信息安全策略。因而,以前定义的方针或策略需要重新评审和调整。

为了保证与安全有关的方法得到支持,组织的信息安全策略应获得高层管理部门批准。组织应指派一个人来负责组织的信息安全策略,并保证这个策略反映了组织的需求和实际状况。这个人通常是组织的信息安全官员,由此负责有关的后续活动,包括安全遵从性检查的评审,事故和安全脆弱性的处理,以及根据这些活动的结果可能需要对组织信息安全策略进行变更或调整。

基于组织的信息安全策略,应该为所有管理人员和员工编写有关指令。这可能需要每个员工在文件上签名,承诺其在组织内的安全责任。进一步,应该开发和实施一个安全意识工程和训练活动的计划。

4.2.2 组合风险分析法

组合风险分析法首先使用高等级的风险分析方法识别出那些对业务运营来说重要的或有较高风险强度的系统。每种情况下都需要识别出信息系统的业务价值和它所暴露的脆弱性和面临的威胁。对组织的业务很重要/暴露于高风险中的信息系统,应该优先进行详细风险分析。对其他系统,则可选择基线方法。

下面进一步介绍组合风险分析法的一些基本原则。

1) 高等级风险分析

首先,有必要进行初始的高等级风险分析,以便识别每一个信息系统更适合采用哪一种方法(基线法或详细风险分析法)。这种高等级风险分析方法考虑信息系统及其处理的信息所具有的业务价值,以及从组织的业务角度看所面临的风险。可以通过以下考虑来确定适合信息系统的方法:

①使用该信息系统要达到的业务目标。

②组织的业务依赖该信息系统的程度,也就是组织认为对它的生存或有效的业务运作很必要的那些功能是不是依赖这个系统,或者依赖于这个系统所处理信息的准确性、机密性、完整性、可用性、可确认性、真实性、实时性和可靠性。

③开发、维护或替换这个系统所要求的投资水平,以及该信息系统的资产价值。

这些经评估后,很容易做出决定。如果一个系统的安全目标对该组织的业务运作很重要,或如果系统的置换费用高,或如果资产价值处于高风险,那么这个系统就需要进行详细的风险分析。

一个普遍适用的法则是:如果信息系统缺乏安全,可能对一个组织及其业务过程或它的资产造成重大危害或破坏,就需要详细风险分析来识别风险。在其他的情况下,应用基线法即可提供适当的保护。

2) 基线法

基线保护的方法是建立若干等级的最少数量的安全措施用以保护一个组织的所

有或一些信息系统。使用这种方法,有可能在组织范围内采用同一等级的基线保护,而额外地使用详细风险分析评估以便保护组织中处于高风险的信息系统,或者对业务至关重要的系统。基线法的使用减少了组织在执行风险分析评估时所需的投资。

可以通过使用安全措施目录来建立合适的基线保护,每个目录推荐一组保护信息系统的保护措施以对抗最常见的威胁。可以调整基线安全的等级来适应组织的需要,而不需要对脆弱性、威胁和风险进行详细评估。在确认安全措施已经部署到位后,还要与基线安全措施目录中列出的那些安全措施作一个比较,判断哪些安全措施还没有部署到位,以及哪些安全措施还需要调整等。

基线安全措施目录会详细说明需要用到的安全措施,或者会给出一组安全建议,说明对于所考虑的系统来说哪些安全措施是合适的。

基线安全措施目录可以从以下地方获得:

- 国际和国内的标准化组织。
- 工业部门标准或建议。
- 其他同类组织。

当然,一个组织可以通过建立相应的典型环境和业务目标来形成它自己的基线。

3) 详细风险分析

一个信息系统的详细风险分析包括识别相关的风险和评估它们的重要性。这是通过识别不期望事件对业务的潜在不利影响以及不期望事件发生的可能性来完成的。不期望事件对组织的业务、人或者其他价值实体有负面影响。一个不期望事件的不良影响是在有风险的情况下,所有可能与资产价值相关的损失的综合体现。发生的可能性依赖于资产对潜在攻击者的吸引力,以及脆弱性被开发利用的难易程度。风险分析的结果决定安全措施的识别和选择,以使可识别风险降到可接受的水平。

详细风险分析包括对图 4.3 中每一步的深入评审。选择正确的防护措施是风险管理过程的一部分。这些防护措施要求在信息系统安全策略和相关的信息安全规划中以文档的形式给出。有很多事件和外在影响,可能影响系统的安全需求,使得需要重新考虑部分或全部安全分析。这些影响可能有:系统最近的重要变更,已经计划的变更,或需要处理的事件的结果。

一旦系统的详细风险分析第一次完成后,评审的结果,包括资产及其价值、脆弱性、威胁和风险等级以及安全措施的确认等,都要保存下来(例如存到数据库)。

有很多方法用来完成详细风险分析,包括从基于检查列表的方法到基于结构分析的技术。基于自动的(计算机辅助的)或手动的风险分析产品也可以使用。不管组织使用何种分析方法或产品,都应该解决下面要讨论的题目,并都要合乎组织的文化和社会背景。

(1) 评审边界的建立

在确定信息系统资产之前,需要定义评审边界。这一边界的准确定义可以避免不

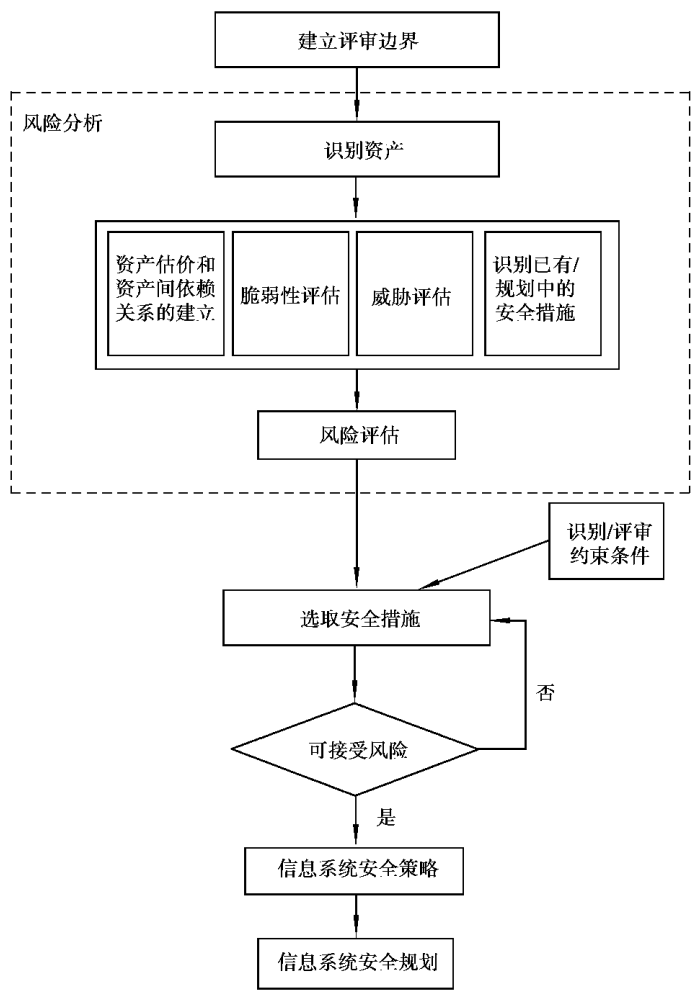


图 4.3 含有详细风险分析的风险管理

必要的工作并提高风险评估的质量。定义边界时应当包括：

- 信息资源,如硬件、软件、信息。
- 人,如员工、分包者、其他外部人员。
- 环境,如建筑、机房和运行场所。
- 活动(操作)。

(2) 资产的识别

资产是一个系统的有价值的组件或组成部分,一个组织为系统评定价值并且对它进行保护。对资产进行识别时,要记住信息系统不光是由硬件和软件组成的,还包括设计、建设和使用信息系统的人以及运行环境。资产类型包括：

- 信息/数据,如包含支付流程的各种数据、产品的信息等。
- 硬件,如计算机、打印机等。
- 软件,包括操作系统、文字处理程序、为特定目的开发的程序等。
- 通信设备,如交换设备、电话、铜电缆、光纤等。
- 固件,如软盘、只读存储器光碟、可编程只读存储器和移动存储器等。
- 文档,如合同、技术资料等。
- 资金。
- 产品。
- 服务,如信息服务、计算资源。
- 服务中的秘密和信任,如支付服务过程和方法等。
- 环境。
- 员工。
- 组织形象。

评审边界内的所有资产都必须进行标识。处于一个评审边界之外的任何资产,要被分到另一个评审边界中以保证不漏掉。

(3) 资产估价和资产间依赖关系的建立

列出受评审的信息系统的所有资产后,应该给这些资产确定价值。这些价值代表了资产对一个组织业务的重要性。基于组织的业务需要,资产的识别和估价是风险分析中的重要环节。

资产的所有者和使用者应为资产估价提供依据。风险分析人员将列出资产(表)。他们应该从组织内那些参与业务计划、财务、信息系统建设和其他相关活动中的人中寻求帮助,以便为每一个资产确定价值。价值应与获得和维护这些资产的费用有关,还应与由于机密性、完整性、可用性、可确认性、真实性和可靠性的丧失而造成的潜在的业务负面影响有关。每个被识别的资产对组织都有价值。然而并不存在一种直接的或简单的方法对所有的资产确定经济上的价值。因此有必要使用组织的非经济的术语,例如质量上的术语,来表述那些具有重要价值的资产。否则,将很难识别所需保护等级以及组织为保护这些资产应投入资源的数量。这样一个估价尺度可以是低、中和高等级,或者,更具体一些地表述为:可忽略的一低一中一高一很高。

还可以有其他的确定资产价值的更详细的度量方法。不管采用什么度量方法,以下情况所导致的可能影响必须在这个估价中予以考虑:

- 违反法律/法规。
- 业务性能的损失。
- 信誉损失/名誉的负面影响。
- 与个人信息相关的机密性损坏。
- 个人安全受到的危害。

- 法律实施中的负面影响。
- 商业机密性的破坏。
- 公共秩序的破坏。
- 资金损失。
- 业务活动的中断。
- 环境安全的破坏。

组织还需要考虑其他对业务较为重要的技术性标准。组织还要定义自己的风险等级(如“低”或“高”)。举例来讲,一定数量的资金损失对一个小公司来讲可能是致命的,但对一个大型公司来讲也许并不重要甚至可以忽略不计。

在这一阶段需要强调的是,估价的方法不仅允许进行定量的计算,而且在定量计算不可能或不合逻辑时必须进行定性的评估(例如,生命丧失的潜在损失、公司信誉损失),并对所用的评估尺度给出解释。

某一资产对其他资产的依赖性也需要识别。因为这有可能影响到资产的价值。例如,在整个处理过程中都必须保持数据的机密性,那么数据处理程序所需的安全性与被处理数据的机密性的价值就直接相关;如果一个业务过程依赖于一个程序产生的特定数据的完整性,该程序输入的数据就应该有适度可靠性。又如,信息的完整性依赖于存储和处理此信息的硬件和软件系统的安全性。进一步说,硬件也要依赖于电力供应,以及可能还有空调等环境条件。因此,有关依赖关系的分析将对特定脆弱性和相关威胁的识别有帮助。它还有助于将资产的真实价值(通过依赖关系)分配给该资产,并进一步确保一个合适的保护水平。

依赖于其他资产的资产所具有的价值可用以下几种方式修正:

①如果那些依赖于它的资产(如数据)的价值低于或等于此资产(如软件)的价值,则此资产的价值保持不变。

②如果那些依赖于它的资产(如数据)的价值较高,则要根据依赖的程度以及其他资产本身的价值来增加此资产(如软件)的价值。

一个组织的某些资产可能被某个资产重复使用或被多个资产共用,例如软件程序副本或者办公室所用的相同型号的PC机,在进行资产评估时都要考虑到这些事实。一方面,这些副本之类的东西很容易被忽略,所以要特别关注以识别所有的东西;另一方面,它们可降低可用性。

这一步的最后输出是一个资产及其价值的列表,其中价值与泄漏(机密性保护)、修改(完整性保护)、不可用和破坏(可用性保护)以及替换成本等相关。

(4)脆弱性评估

脆弱性评估是识别物理环境、组织、规程、人事、管理、行政、硬件、软件或通信设备等中的弱点或缺陷。这些弱点或缺陷可能会被威胁源利用而导致对资产和业务的危害。脆弱性的存在本身并不造成损害,必须要存在能利用它的威胁才可能造成损害。

没有相关威胁存在的脆弱性暂不需要实施安全保护措施,但是需要识别和监视可能出现的变化。应该注意,一个未被正确实施或功能不正确的安全措施,或不正确使用的安全措施,自身就是一种脆弱性。

脆弱性可能与资产的特性或属性有关,可能因资产的利用方式与在购买或制造时所期望的那种方式不同而产生。例如,一个 EEPROM(电可擦除可编程只读存储器)的特性之一就是上面存储的信息可以被擦除和替换。这是一个 EEPROM 的设计准则。然而,这个特性也意味着可能对存储在 EEPROM 上的信息进行未授权的修改或破坏。这可能是一个脆弱性。

此项评估识别可以被威胁利用的脆弱性,并评估弱点或缺陷的可能的等级,也就是被利用的容易程度。脆弱性评估的输入应该从资产的所有者和使用者、设备专家以及硬件和软件方面的专家处获得。脆弱性的例子是:

- 未受保护的连接(例如因特网)。
- 未受训练的用户。
- 错误选择和使用口令,以及口令字长度过短等。
- 不适当的访问控制(逻辑的/物理的)。
- 没有信息或软件的备份。
- 位于易遭受洪水的地区。

重要的是评估脆弱性的严重程度,换句话说它们是它们被威胁利用的容易程度。脆弱性评估要针对每个可以在特定情况下利用它的威胁来进行。如,一个系统可能存在对冒用用户身份和滥用资源的威胁的脆弱性。因为缺少用户鉴别,冒用用户身份的脆弱性会很高。另一方面,缺少用户鉴别对滥用资源(即不合理地使用资源)的脆弱性却会低,因为即使缺少用户鉴别,资源被滥用的方式也是有限的。

这一步的结果应该是一个列表,包含脆弱性及其被利用的容易程度(例如用高、中 and 低来表示)的评估。

(5)威胁评估

威胁具有危害信息系统及其资产的可能性。如果威胁发生,它能够以一定方式影响信息系统,导致意外事件发生和产生负面影响。威胁可能是自然或人为发生的,可能是偶然的或蓄意的。对偶然和蓄意两种威胁的源都应该识别,它们发生的可能性应受到评估。关键是不要忽略有关的威胁,因为这可能导致信息系统安全的丧失或产生脆弱性。

威胁评估的输入应该从以下方面获得:资产的所有者和使用者,人事部门员工,设施规划和信息技术专家,以及负责保护组织的人等。其他组织如法人机构和国家政府机构也可以提供帮助,例如通过提供威胁统计资料。一般的潜在威胁目录和其他威胁目录对实行威胁评估是有帮助的。

一些最普遍的威胁的表现形式示例:

- 错误和失职。
- 欺诈和偷窃。
- 员工蓄意破坏。
- 物理和基础设施支持的缺失。
- 恶意的黑客行为(例如,伪装、入侵等)。
- 恶意代码(例如,病毒程序和木马等)。
- 工业或国家间谍活动。

在使用威胁目录或此前的威胁分析结果时,应该意识到威胁是在不断变化的,特别是当业务环境或信息系统变化时。

在确认了威胁源(威胁行为的主体)和威胁目标(受到该威胁影响的资产,威胁行为的客体)后,有必要评估威胁的可能性。评估时应该考虑到:

①威胁出现的频度(根据经验、统计资料等),持续的时间等。

②动机,被发觉的潜在能力,攻击者可利用的资源,以及信息系统资产对攻击者和威胁源的吸引力和脆弱性程度。

③偶然的威胁源的地理性因素(如靠近化学或石油工厂),极端天气出现的可能性,以及能引起人类错误和设备故障的各种因素。

根据对评估精度的需要,可能需要把资产分布到系统的部件中,并且将威胁与部件关联起来。例如,一个物理资产可能开始时是“中央数据服务器”,但当这些服务器被确认处于不同的地理位置时,会被分为“中央数据服务器1”和“中央数据服务器2”。类似地,一个软件资产刚开始可能是一个“应用软件”整体,但是后来分为两个或更多的“应用软件”实例。一个关于数据资产的例子,可以是在开始时被定为“犯罪记录”,但是后来分成“犯罪记录文本”和“犯罪记录图像”。

威胁评估完成时,将会有有一个列表,包含已识别的威胁,将受它们影响的资产或资产组,以及以某种评估尺度(比如高、中或低)表示的威胁出现的可能性量度。

(6) 现有或计划中的安全措施的认识

紧接着风险分析评审后识别的安全措施是对已有或已规划的安全措施的补充。重要的是,这一阶段要将这些已有和已规划的安全措施识别出来,这就可以避免不必要的努力或花费,例如避免安全措施的重叠。已有或已规划的安全措施也可能被鉴定为不合适,若是这样,应该检查是否去掉这样的安全措施,或者用另一个更合适的安全措施替换,或者继续部署(例如,因为费用的原因)。

另外,为了确定在风险分析评审后选择的安全措施是否与现有或计划的安全措施兼容,即被选的安全措施与存在的安全措施不能相互妨碍,也需要进行核查。

在识别现有安全措施时,应进行检查,以确保这些安全措施运行正常。

这一步的结果是现有或已规划的安全措施及其实现和使用状况的列表。

(7) 风险评估

这一步的目的是识别和评估信息系统及其资产的风险,以便识别、选择和调整安全措施。风险包括处于危险中的资产的价值,能被识别的威胁利用脆弱性的容易程度,导致业务潜在负面影响的威胁出现的可能性,以及任何已有或规划中的可以降低风险的安全措施相互妨碍或工作异常等。有不同的方法可将这些因素联系起来。例如,将分配给资产的价值、脆弱性和威胁组合起来以得到一个度量风险的值。

不管采用什么方法去评估风险值,这一步的结果应该是一个已度量风险的列表,包括信息系统的泄露、修改、不可用性以及破坏等每一种因素所造成的风险。更进一步,风险度量可以帮助在选择安全措施时确认处理风险的优先顺序。所用的风险评估方法应该是可复核和可跟踪的。

4) 安全措施的选择

应确认和选择合适的和被证明是正当的安全措施,以把被评估的风险降到可接受的水平。已有的和计划中的安全措施,信息系统安全建筑和各种类型的约束条件都应被考虑,帮助进行适当的选择。关于安全措施选择技术的详细介绍,见第 4.3 节“安全措施的选择与实施”。

5) 风险接受

所选择的安全措施的实施可以降低已有风险,但总是会有残留风险——没有系统可以做到绝对安全。对一个组织来说,这些残留风险可分类为“可接受的”或“不可接受的”。这种分类可通过评审与那些风险关联的潜在的负面业务影响来完成。显然,对残留风险需要更进一步地考虑其是否可容忍。管理层的决策就是要决定,这些风险在其他约束(如费用,或不可能简单预防,诸如飞机撞到建筑物或地震等,但从这些事件中恢复的计划还是可以做的)发生时是否仍然是可以被接受的,或者是否需要选择额外的或可能昂贵的安全措施来减少这些不可接受的风险。

6) 安全策略

信息系统需要制定包括风险评估的安全策略。该信息系统的安全策略应与组织的安全策略保持一致。这些安全策略应在比组织的信息安全策略更低的层次上对问题进行描述。信息系统安全策略在对该系统的风险分析评估和安全措施的识别的结果基础上制定,并为满足安全目标而选择一套安全措施。这些安全措施保证此系统获得适当水平的保护。

信息系统安全策略应基于以下信息,并且包含为使系统达到适当安全等级保护水平所必须的安全措施(包括规程)要求。信息系统安全策略和所有的相关文档应涉及:

- ①信息系统的定义,其部件和边界的描述(这个描述应围绕组成系统的所有硬件、

软件、人员、环境和活动展开)。

②信息系统业务目标说明。这会对此系统的信息安全策略、风险分析方法以及安全措施的选择和实施优先权产生影响。

③对系统安全目标的识别。

④组织对信息系统的依赖程度,用组织的系统因其遭到损失或破坏而受危害的程度和范围,以及此信息系统要实现的任务以及被处理的信息来表示。

⑤信息技术的投资水平,用开发、维护和替换信息系统的费用和资本,以及运行和替换零部件、子系统或整个系统所需的费用来表示。

⑥信息系统选择的风险分析方法。

⑦组织要保护的信息系统的资产。这些资产的估价,用资产遭破坏对组织产生的后果来表示(信息的价值应按照信息的泄露、修改、不可用性和破坏造成的业务负面影响来衡量)。信息系统资产的脆弱性,包括对可被威胁利用的固有弱点的描述。

⑧信息系统及所处理的信息面临的威胁,包括资产脆弱性和威胁间的关系,这些威胁发生的可能性。

⑨信息系统的安全风险,诸如脆弱性被利用的容易程度、威胁发生的可能性、对组织的业务的潜在负面影响。

⑩已确认的保护该信息系统的安全措施列表。

⑪估计的信息安全的费用。

7) 信息安全规划

信息安全规划是一种协调性文件,定义实施一个信息系统所需要的安全措施的行动。该规划应包含上面描述的评审的结果,在短期、中期和长期要采取的用来获得和维持适当安全保护水平的行动、费用以及实现计划(进度安排)表。对每个系统来说都应包含:

①安全目标,用机密性、完整性、可用性、可确认性、真实性和可靠性来表示。

②为该信息系统确定的风险分析方法(基线法、详细风险分析法或组合法等)。

③现有的以及计划中的安全措施列表,包括它们效力的判断和需要的安全措施升级。这个列表应包括:

- 被选安全措施的实现和现有安全措施的升级的优先级顺序,以及这些安全措施在实践中如何工作。

- 对这些安全措施的安装和运行费用的评估。

④被挑选出来、待实现的安全措施列表。

⑤对识别出来的安全措施的实现是否达到期望值以及残留风险是否可接受进行评估。

⑥对这些安全措施的实施和后续活动的人力资源的评估。

⑦实施这些安全措施の詳細工作计划,包含优先级顺序和优先级顺序有关的实现计划表、需要的预算、责任。

⑧保证安全措施效力所需的对信息系统员工和终端用户的安全意识和训练规程。

⑨关于在需要的地方实施安全措施的批准过程表。

⑩后续规程的进度表。

此外,信息安全规划应描述对安全措施的正确实施过程进行控制的设施,例如:

①对进展情况的报告规程的定义。

②用来识别可能出现的困难的规程。

③使上面列出的各点生效的规程,包括在需要时对规划的单个部分或规划本身进行修改的规程。

这一步骤的结果应该是为每一个系统生成一个详细的信息安全规划,这个规划依据信息系统安全策略,综合考虑了上述评估的结果。应该保证根据信息系统风险分析结果导出的安全措施优先级,以及在规划中描述的如何实现这些安全措施和如何达到合适的安全保护水平等及时地得以实现。本规划还应包含维持这个安全保护水平的后续进度表。

4.3 安全措施的选择与实施

信息系统必要的安全措施应该根据信息安全规划予以实施。常规性信息安全意识则是安全措施发挥效力的重要因素。也就是说,安全措施的实施和安全意识工程,应该平行运行。

为了选择适当的安全措施,不管对风险是否需要进行分析,都有必要进行基本评估。评估对象包括:

- 信息系统的类型(单机,还是网络)。
- 信息系统的位置和周围环境条件。
- 已经部署的/计划中的安全措施。
- 评估工作是否提供了足够的可用于选择“基线”安全措施的信息。

有两种主要的方式可以辅助选择信息系统的安全措施:基线法和详细风险分析法(见图4.4)。

实施详细风险分析法可以对风险状况有一个全面、深入的认识。当风险状况成了影响安全措施选择的重要因素时就要在详细的风险分析基础上选择安全措施。这样可以避免保护过度或欠保护。但这项工作需要大量的时间、努力和专业知识,所以它只适于处于高风险状态下的信息系统或子系统。而对于低风险下的信息系统,简单一些的方法就可以了。

“基线”安全模式起码要达到组织对各种信息系统安全要求的最低标准。通过实

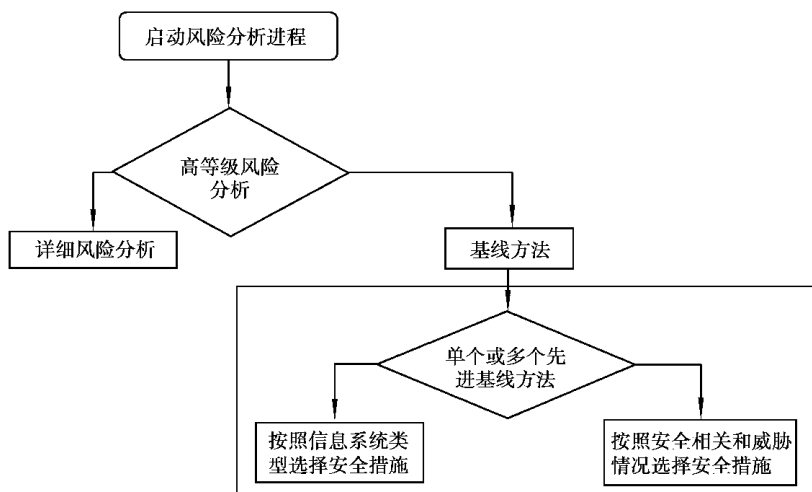


图 4.4 安全措施的选择方法

施“基线”安全措施(即一系列最基本的安全措施)可以达到“基线”安全标准。

使用基线法可有两种不同的处理办法：

- ①根据信息系统的安全类型和特征选择安全措施。
- ②按照安全保护重点和威胁情况选择安全措施。

图 4.5 给出了根据信息系统类型或根据安全保护重点和威胁选择安全措施的过程,可以看作是对图 4.4 的补充。

采用“基线”方式评估风险后,选择安全措施时必须考虑可以利用的资源、安全保护重点以及所涉及的信息系统的类型和特点。如果一个组织不想在安全措施的选择上花费大量的时间和精力,则可使用无需进行更深入评估的“基线”方式。如果组织的业务运作以中等程度依赖于信息系统或服务/信息系统所处理的信息比较敏感,那么就需要更多的安全措施。在这种情况下,为了使所选择的安全措施有效地保护信息系统,最好是对信息的重要性及可能的隐患进行详细的分析。如果组织的业务运行在很大程度上依赖于信息系统或服务/信息系统所处理的信息非常敏感,那么风险就会比较高,这就需要详细风险分析,只有这样才能确定出适当的安全措施。

下列情况需要通过详细的风险分析来确定出具体的安全措施：

- ①信息系统的类型在 4.3 节的评估对象中找不到。
- ②在 4.3 节中所提供的解决方案不能满足业务或安全需要。
- ③考虑到潜在的高风险或信息系统对业务的重大作用而有必要进行更详细的评估。

需要注意的是更详细的风险分析对于“基线”安全措施的应用也是有帮助的。

组织必须做的一个决定是：只单纯地使用“基线”方法,还是把“基线”方法作为更广泛范围内的风险分析战略的一部分。在做此决定时,需要注意的是前者的安全效果很可能要低于后者。如果考虑到安全措施选择过程中的低成本、资源的低耗费以及对信

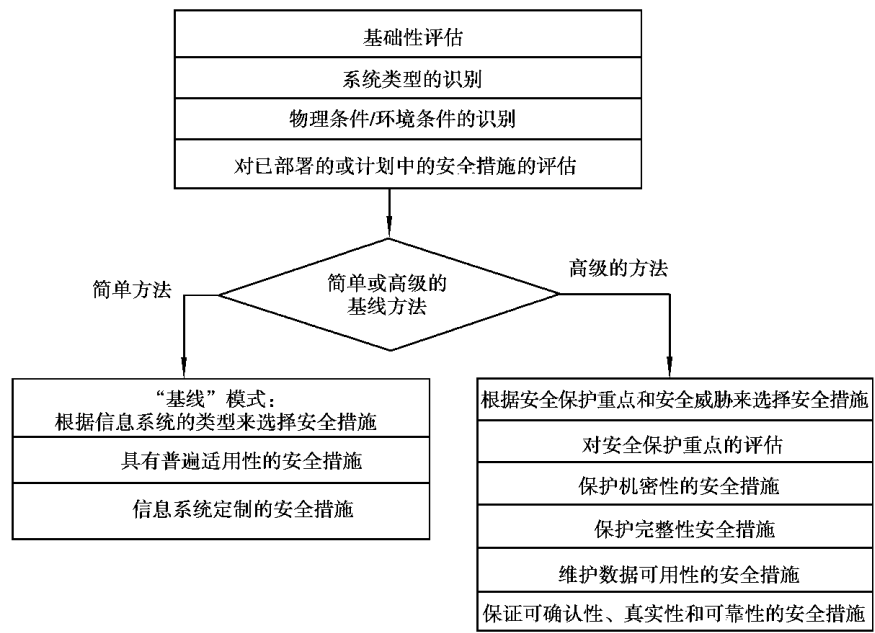


图 4.5 根据信息系统类型或安全保护重点和威胁选择安全措施

息系统安全的低标准,在一些安全要求不高的小型网络中使用“基线”模式也可能是非常可行的。

如果一个组织决定要在其整个组织中或部分组织部门中应用“基线”安全模式,那么需要决定组织的哪些部门可以使用相同的“基线”,以及这种“基线”应该达到什么安全目标。绝大多数情况下,使用“基线”安全仅能保证最低的安全标准,当涉及中等和高风险时,还要实施另外的安全措施。“基线”只代表平均的安全水平,因此,可以根据风险分析的结果对“基线”保护水平进行合理的调整。

“基线”安全方式的优点之一是,如果它被应用于一组信息系统,那么整个组织的安全水平可以决定某部分的安全水平。在这些情况下,对组织或部门的“基线”目录进行编制、完善和归档通常是非常方便的。

4.3.1 基础性评估

在选择安全措施的过程中,总是需要一些信息系统的类型和特征的知识(例如,是单机 PC,还是连接到内部或外部网络的 PC),因为这些对于安全措施的选择有着重大的影响。此外,对建筑物、房间等基础设施的了解也是非常必要的。另一个对安全措施的选择有重要影响的因素是对现有的/计划中的安全措施进行评估。

(1) 信息系统类型的识别

为了对现有或计划中的信息系统进行评估,要把所涉及的信息系统与下列组件进

行比较,从而把该系统的组件识别出来。这些组件包括:

- 独立的工作站。
- 连接到一个网络的工作站(不共享资源)/终端设备。
- 连接到一个网络的服务器或连接到一个网络且共享资源的工作站/终端设备。

(2) 物理条件/环境条件的评估

对环境的评估包括:识别支持现有的/计划中的信息系统的基础设施以及现有的/计划中的安全措施。因为安全措施应该与物理环境相适应,这些工作对安全措施的选择是否成功至关重要。在考虑基础设施时,可以通过回答下列问题来进行。另外,还应该认真考虑组织机构的环境及需要考虑的所有特殊情况。

① 周边环境和建筑物,包括:

- 建筑物的位置是有围栏的单独场所,还是在车水马龙的大街上。
- 建筑物是独占还是共同占有。
- 如果是共同占有,那么其他占有者是谁。
- 敏感/关键的区域在什么位置。

② 对访问的控制,包括:

- 谁有权进入建筑物。
- 在适当的位置是否安装了物理访问控制系统。
- 建筑物结构的牢固程度如何。
- 门、窗户等设施的牢固程度如何,对它们采取了何种保护措施。
- 建筑物是否有保卫,如果有,是每天 24 小时全天候有保卫,还是仅仅在工作时间有保卫。
- 建筑物或放有关键装备的房间是否配备了报警器。

③ 到位的安全措施,包括:

- 对放有信息系统相关设备的房间采取了哪些保护措施。
- 是否配备了失火检测、警报和灭火设施,配备在什么地方。
- 是否配备了水/液体的泄漏检测装置、泄漏警报装置和排泄设施,配备在什么地方。
- 是否有不间断电源(UPS)、水管装置、通风和空调(对温度和湿度进行控制)之类的支撑工具。

通过回答这些问题,就容易识别出在物理保护区域里已存在的安全措施。例如,当考察建筑物的门时,能够同时确认门锁以及其他物理访问控制。

(3) 对现有或计划中安全措施的评估

在搞清信息系统的组件及其物理/环境条件后,应对其他所有已到位或计划中的安全措施进行确认。这对于避免重复选择已存在的或者计划中的安全措施是非常必要的,而且,如果知道已实现的或计划中的安全措施,这对进一步选择安全措施、并将

它们组合起来发挥作用也是有帮助的。在选择安全措施时,同时应考虑现行安全措施与新选择的安全措施的兼容性。一个安全措施可能与别的安全措施发生冲突,或者不能顺利地运行和对系统提供保护。

为了对现有或计划中的安全措施进行确认,下列活动是有帮助的:

①查阅有关安全措施信息(例如信息系统安全规划或概念设计)的文件。如果安全流程的文档齐全,那么文件中应该列有所有现有或者计划的安全措施及它们的实现状况。

②到负责人员(如信息系统安全官员、基建或运营经理)和使用人员那里去查对信息系统的哪些安全措施真正得到了实现。

③在建筑物里观察各项安全措施,把已经实现的安全措施与应该在此实现的安全措施进行比较,以便确定是否存在应该实现但还没有实现的安全措施。进一步检查已实现的安全措施是否运行得正确、有效。

④如果发现现有安全措施超出了当前的需要,应考虑去掉多余的安全措施。如果要去掉多余的安全措施,那么要考虑安全保护效果是否满足安全目标的需要。因为安全措施是相互影响的,去掉多余的安全措施可能降低整体的安全性。另外,保留某些安全措施有时可能会比去掉它们从信息系统维护的整体上看更省钱。当安全措施维护费用很高时,去掉它们则会更经济。

4.3.2 安全措施

这一节将对用来提高安全性的安全措施做一般性的介绍。在这些安全措施中,一部分是机制,另一部分可以看成是应被执行的规程。需要注意的是,对安全措施进行阐述时,并没有考虑选择方式。有一些安全措施可以使用任何方式进行选择,而有的则应该或只能通过详细风险分析方式来选择。

为了便于描述各种类型的安全措施,这里引入了安全措施类别的概念。以下先对安全措施分类以及各分类对应的安全措施进行简单描述。

1) 组织性的和物理的安全措施

下面介绍组织性的和物理的安全措施。

(1) 信息安全管理策略

此类安全措施包含所有用来处理信息系统安全管理、活动规划、责任分配以及开展所有其他相关活动的安全措施。这些安全措施在于使整个组织保持合适的、一致的安全等级。下面列出了此范围内的安全措施:

①组织的信息安全策略。应该编写含有规则、指令、惯例的书面文件,用来描述在组织内部应怎样管理资产、保护资产以及资产的分布情况。在信息系统安全策略文件中,应指明哪些地方需要指导,以及为何对其进行指导。

②信息系统安全策略。对于每一个信息系统,应该制订出信息系统安全策略,描述组织已有的或有必要实现的安全措施,还要概括现有或计划中的安全措施所要保护的安全重点/对抗的威胁。

③信息安全管理。应该以适合本组织的方式使信息安全管理正规化,并使安全管理工作在组织内保持协调。例如成立信息安全委员会、任命信息安全官员使其对每个信息系统的安全负责。

④责任的分配。组织内各层次的信息安全责任应该明确地写入文件,并根据组织的信息安全策略和信息系统安全策略明确地分配责任。

⑤信息安全的组织问题。所有能支持信息安全的业务流程(如采购、与其他组织进行的合作)都应以安全的方式进行组织,以对信息安全提供组织性支持。

⑥资产确认和评估。应对组织的全部资产以及与信息系统相关的资产进行识别,并评估各种资产对业务的价值。

⑦信息系统的验收。对信息系统的验收应该在信息安全策略的指导下进行。验收过程就是要检查所实现的安全措施是否能提供适当的保护等级水平。它应该考虑信息系统中已经存在的和可能扩展的通信及业务需求。

(2) 遵从性检查

必须确保安全措施遵从相关的法律、法规、政策和安全策略。因为任何法律法规、政策或安全策略要发挥作用,需要信息系统的使用人员遵从并与它们保持一致。这一方面的安全措施如下:

①遵从信息安全策略。应定期检查是否所有用户都遵从信息安全策略。同时还要检查所有的信息系统的安全措施是否都与信息安全策略中列出的相关的安全措施和技术标准完全一致。

②遵从法律和法规。对遵从情况的检查应包括确保信息系统遵从所在国的法律和法规,如数据保护和隐私权、软件的复制、组织档案保护、对信息系统或加密技术的滥用等方面的相关立法等。信息安全策略必须保证将这种遵从写入法律要求条款中,并确保每一信息系统的安全措施在实现时是满足这些法律要求的。

(3) 事件处理

组织中的每个人都应该意识到及时报告安全事件的必要性。为此,组织应该制订相应的报告制度。事件处理包括:

①事件报告。每一位员工应该认识到及时报告安全事件的责任。也可以通过某些工具对事件进行识别和报告。为了更有效地处理事件,组织应制订汇报制度和联络人。

②安全漏洞或缺陷报告。如果使用人员发现了任何的安全漏洞或缺陷,他们应当尽快报告给负责人员。

③软件故障报告。如果使用人员发现了任何的软件故障,他们应当尽快报告给负责人员。

④事件管理。应该制订管理流程,以支持对事件的防护、检测、汇报和适当的应对。应收集、评价有关事件的信息,以防止事件的再次发生或减小再次发生所造成的损失。

(4)人 员

此方面的安全措施是要减少由于人员操作失误和违反安全规定(故意或无意)所造成的安全风险。这方面的安全措施如下:

①针对终身职员和临时职员的安全措施。所有的职员都应该知道他们在系统安全上的作用和责任。职员应该遵守的与安全有关的规程都应在文件中明确声明。在雇用前应对职员进行审查,如果有必要还要签订保密协议。

②针对临时工的安全措施。应对临时工(如清洁工等)及所有参观考察者进行控制。在临时工获得接触(物理意义上或逻辑意义上的)信息系统设施的资格之前,应该让其签订保密协议。

③安全意识和培训。所有使用、开发、维护及对信息系统设施有访问权的人员都应阅读定期的安全简报和材料。应该教育并保证工作人员知道他们掌握的信息对业务的重要性,以及与重要性相伴随的信息的脆弱性、潜在威胁和风险,以使他们理解安全措施必要性。另外,还应对使用人员进行培训,以让他们正确地使用信息设备,避免错误。对于信息安全官员、信息安全管理员等关键人员,则有必要进行更深入和更专业的安全培训。

④严明纪律。所有雇员都应该知道(有意和无意)违反组织范围内的具体的信息安全策略及其他明确写明了的安全协议的后果。

(5)操作方面

这方面的安全措施是用以维持信息设备及相关系统安全、正确和可靠运行的程序。通过组织程序的执行就可以实现大多数安全措施。操作上的安全措施与其他安全措施,如管理性和技术性的安全措施,配合使用是非常有必要的。这方面的安全措施如下:

①配置和变动管理。配置管理识别、操作和控制开放系统,从开放系统收集数据和为其提供数据。变动管理就是随时掌握对信息系统所做的改动。配置和变动管理的基本安全目标就是保证对信息系统所做的变动不至于降低安全措施的可利用性和安全措施所保证的整体安全性。变动管理有助于在信息系统被改动后,识别出新的安全措施。

②容量管理。容量管理就是要防止因容量不足所造成的故障。在估计信息系统应具有容量时,应考虑对未来容量的要求和当前要求的变化趋势。

③编制文档。与信息系统配置和操作有关的一切内容都应编制成文档,以保证连续性和一致性。信息系统安全也应在信息系统安全策略、安全操作规程及业务连续性战略规划和制订中形成文档。文档应该及时形成并归档,并且查找方便。

④维护。为了保证信息系统持续的可靠性、可用性和整体性,应该对其中的设备进行正确地维护。要在维护合同中写明维护人员必须遵循的安全要求。维护工作应根据供应商的合同进行,并且必须由获得授权的人员进行维护。

⑤对与安全有关的变动进行监控。应对脆弱性、威胁、影响、风险的特征及其变动情况进行监控。既要对现有的方面进行监控,又要对新出现的方面进行监控,还要对信息系统所处的环境进行监控。

⑥审计跟踪和日志。应利用服务器的(例如,审计操作记录和分析工具)、网络的(例如,防火墙或路由器的审计模块)和应用程序的(例如,发送信息或交易处理等应用程序的审计功能)的审计和日志能力,来跟踪安全事件的详细情况。这包括对未经授权或错误事件进行辨认的详细资料,还有表面看起来是正常事件的详细资料(可留作以后分析用)。对操作记录和日志的审计应定期进行,以发现未经授权的操作并采取纠正措施。另外,还应对日志中的重复性事件进行分析,这些重复性事件可能表明系统的脆弱性和威胁,它们可能是由设备(或程序)缺陷或不适当的安全措施所导致。另外,这样的分析还可以从表面上不相关的事件中找出一些模式,这些式可以对未经授权进行操作的人员的身份进行确认。

⑦安全测试。为了保证信息系统设备和所有的相关软件能正确使用,必须进行安全性测试。安全性测试应包括在信息系统安全策略和测试方案中,并且要制订相应的测试标准以检验是否达到了要求的安全等级。

⑧介质控制。介质控制包含了为磁带、磁盘、USB 存储器、光碟(光盘)、输入输出装置及其他介质提供物理保护和环境保护的大量安全措施。这包括做标记、日志记录、完整性验证、物理使用权保护、传输和安全配置等。

⑨信息的彻底删除。如果已存入存储装置的机密信息不再使用,就应将其销毁。应该保证含有机密信息的文件已被抹掉并进行了物理性覆盖,或者已被毁掉。因为计算机中的删除功能并不能保证做到以上要求,因此需要经过负责人员的同意,为使用人员提供能使他们彻底删除信息的工具。

⑩职能的分割。为了把滥用特权的风险和可能性降至最低,要对必要的职能和关键性任务进行分割。那些可能绕过或超越安全措施和审计的任务和职能,以及可能使雇员获得过多操作条件的任务和职能,必须进行分割。

⑪正确使用软件。要保证不对有版权控制的软件进行复制,并严格遵守专有软件的许可协议。当对软件进行改动时要保证能保持软件的完整性(软件变动控制仅针对软件,而配置和变动管理是针对整个系统及其环境的)。应制订能对所有变动进行管理并保持信息系统安全等级的软件变动控制程序。这包括对变动的授权制度、中期解决方案的安全考虑和最终解决方案的安全审计。

(6)业务连续性计划

为了使业务,特别是关键业务流程,免于遭受重大故障或能力丧失所带来的影响,

或把损害降至最低,必须制订有效的业务连续性(包括意外事件的应对措施和失效恢复)策略和方案。包括下列安全措施:

①意外事件处理策略。应在确定出因脆弱性、调整和毁坏对业务可能造成潜在负面影响的基础上,制订意外事件处理策略(包括意外事件的应对措施和失效恢复),并形成正式文档。

②业务连续性计划。在业务连续性策略的基础上制订业务连续性计划(包括处理意外事件和失效恢复的方案),并形成正式文档。

③业务连续性计划的测试和更新。在业务连续性计划被认可之前,应彻底地测试连续性计划以保证它在系统的生命期中能够真正起作用。应该保证所有相关人员都理解这些计划。业务连续性计划必须进行定期更新。业务连续性策略也应在必要的时候进行更新。

④备份。所有重要的文件、业务数据、系统程序和文档都必须进行备份。备份频度要依照信息的重要性和业务连续性计划的规定而定,使其与信息的重要性和业务连续性计划相适应。应对备份内容进行安全的异地和远距离的保存。为了保证可靠性,还要定期地检查恢复情况。

(7)物理安全

这方面的安全措施是进行物理保护,物理保护形式可以是规程性的,也可以是技术性的。它们应结合对环境的识别来考虑。下列措施可应用于建筑物、安全区域、计算机房和办公场地等。对安全措施的选择要根据所涉及建筑物中的具体部分而定。这方面的安全措施如下:

①环境保护。对建筑物的物理保护包括栅栏、门禁控制、坚固的墙壁、门和窗户。应通过对物理访问权限的控制和门卫等来防止未经许可的人员进入安全区。像服务器及其配套软件和数据库这些对业务非常关键的信息系统设施,设置安全区是有必要的。进入安全区的权限应给尽量少的有限的人员,并在日志里进行详细记录。全部诊断和控制装备都应安全放置,对其使用也要进行严格控制。

②防火。应对设备及其周围环境采取措施,以防止火势从建筑物内的其他地方或从邻近的其他建筑物蔓延过来。在放有信息系统设备的房间和地区的附近,应把发生火灾的可能性降至最低。自己要防止放有关键设备的房间和地区有火灾发生,也要防止可能在附近发生而危及这些房间和地区的火灾。安全措施应该包括烟火检测装置、火警装置和灭火装置。在选择灭火装置时还应注意,不能让水和其他灭火材料损害信息系统。

③防水/防液体。关键设备不能放在有可能发生严重液体泄露的地方。在有严重液体泄露威胁的地点要采取适当的保护。

④对自然灾害的预防。对关键设备和放有关键设备的建筑物应采取防雷措施。可以通过避开可能发生自然灾害的区域来预防其他自然灾害。

⑤防盗。为了进行有效的资产控制,所有的设备都应具有独有的可辨认特征,并对所有的设备编制财产详细目录。保卫和传达室人员应对在未经授权的情况下离开房间、区域或建筑物的设备及介质进行检查。对存于便携式介质(如软盘、移动存储设备)上的敏感信息和专有软件,应进行适当保护以防止丢失或被盗。

⑥电源和空调。如果有必要,应防止信息系统设备出现断电或电力不足。应使用与信息系统设备相配的电源。如果有必要,还应配备不间断电源。信息系统的运行场所必须保持合适的湿度与温度。

⑦电缆保护。应防止电源线和传输数据的通信电缆被截断、损伤和负压过重。对电缆应采取物理安全措施,以防止有意或无意的损伤。要根据其用途来选择电缆的材料和布线方式。在规划时如果能考虑到将来的需要,那就会省很多麻烦。在有必要和可能的情况下,要防止电缆被搭接和串接。

2) 信息系统特有的安全措施

(1) 识别和鉴别

识别是将某一用户从一群用户中区别出来的过程。鉴别是对用户所声称身份的真实性进行确定。以下是如何完成识别与鉴别的例子。

①通过使用人员所知道的信息进行的识别与鉴别。口令是用于鉴别的最典型的形式。对口令的分配及定期改动应有控制。如果是由用户自己来选择口令,那么他们应该熟悉编制和使用口令的基本常识。可以通过软件来进行这项工作,比如可以对一些常用口令或字符进行限制使用。如果有必要,应对口令进行复制、安全保存,这样当使用人员不在或忘记口令时,也可以获得合法的访问。另外,通过用户所知道的信息进行识别与鉴别时,也可以使用密码方法和鉴别协议(Cryptographic Means and Authentication Protocols)。这种方式也可用于远程识别与鉴别。

②通过用户持有的东西进行的识别与鉴别。用于识别与鉴别的东西可以是具有存储功能的卡 and 智能卡。具有存储功能的卡最常见的应用就是信用卡背面的磁条信息。

③通过用户自身的特性(生物特性)所进行的识别与鉴别。生物鉴别技术利用每个人所特有的特征或特性对其身份进行鉴别,如指纹、手掌形状、视网膜、声音和手书等。相关的特征信息可以安全地存储在智能卡或系统上。

(2) 逻辑访问控制和审计

实施这方面安全措施的作用是:限制对信息、计算机、网络、应用程序、文件和程序的使用权限;对错误和用户所做操作的详细情况进行记录,并对其进行分析。这样做的目的是以适当的方式查出安全漏洞,并对其进行处理。

加强使用权控制的常用手段是把识别与鉴别所用的详细信息与访问控制列表相捆绑,访问控制列表说明了对于特定的用户能使用哪种文件、哪种资源以及以何种方

式使用等。这方面的安全措施如下：

①访问控制策略。对于每个用户或每组用户,应该明确说明访问控制策略。这些策略应该根据业务要求(如可用性、生产效率)来授权访问,并实现访问的最小授权机制。对访问权限的分配应该考虑组织获得安全的方式(开放式或限制式)和文化特点,以在满足业务需要的同时又能让用户接受。

②用户对计算机的访问。应对计算机的访问进行控制,以防止未经授权的使用。对每个已获授权的用户的身分进行确认和核实是必要的。密码技术或其他识别与鉴别方法有助于对计算机访问的控制。

③用户对数据、信息服务和应用软件的访问。应控制计算机或网络中的数据和服务在未经批准的情况下被使用。利用适当的识别与鉴别体系、网络服务间适当的接口和能够确保仅得到批准后才能使用信息服务的网络配置,就能达到以上目的。为了防止未经授权使用应用软件,可以根据用户的业务职能来决定是否授权访问,这种方法叫基于任务的访问控制。

④对访问控制进行检查和更新。对授权用户的访问控制要进行定期的检查。如果现有的访问控制已不能满足安全或业务需要,就要进行更新。对优先访问应进行更频繁的检查,以防止权力被滥用。如果访问已不再有必要时,应及时收回访问授权。

⑤审计。信息系统完成的所有工作都应该记录到日志,并对日志进行定期的检查,这包括对系统成功和不成功的登录、所使用的数据记录、所使用的系统功能等。另外,错误也应该被记录下来,并进行定期检查。对这些数据的使用应遵从有关数据保护和隐私保护的法律法规。例如,这些数据仅能在有限的时期内保存,并且仅能用来查找安全违规问题。

(3)防范恶意代码

恶意代码可以通过外部接口(例如软盘、移动存储设备、网络访问等)引入系统。如果不采取适当的安全措施,那么可能只有在恶意代码发作并造成损害后,才能发现它。恶意代码可能会破坏安全措施(例如获取并泄漏密码),使信息悄悄地被泄漏,或信息自动改动、系统丧失完整性、信息被破坏以及系统资源被未授权使用等。

恶意代码有下列表现类型:

- 病毒。
- 蠕虫。
- 特洛伊木马(程序)。

携带恶意代码的媒介有:

- 可执行软件。
- 数据文件(包括可执行的宏指令,例如字处理文件或电子表格)。
- 网页上的活动内容。

传播恶意代码的途径有:

- 软盘复制。
- 其他便携式介质传播。
- 电子邮件。
- 网络传播。
- 文件或网页内容下载。

通过以下措施可以有效防范恶意代码侵入：

①扫描。专门的扫描软件和完整性检查(工具)能有针对性地检测出相应的恶意代码,并能将其杀灭。扫描装置能以脱机或在线的方式工作。扫描装置在线运行能提供主动的保护,即在信息系统感染恶意代码但未被破坏之前就能识别甚至是删除恶意代码。扫描装置对单机、工作站、文件服务器、电子邮件服务器和防火墙是有效的。不过,应该让用户和管理员知道:由于新的恶意代码出现变种形式,扫描装置并不能保证在新的恶意代码出现时就能将其识别并予以杀灭。

②完整性检测。在很多时候,必须采取其他形式的安全措施,以扩大由扫描装置所提供的安全成果。例如,可以使用检查统计(工具)来检查程序是否被改动。完整性检测(工具)也是防护恶意代码的技术性安全措施之一。这种技术仅能用于不保存属性信息的数据文件和程序。

③移动存储介质的传递控制。如果不对移动存储介质(特别是软盘和USB盘)的传递进行控制,就会使信息系统遭受恶意代码攻击的风险加大。通过以下方式可以对存储介质的传递进行有效控制:

- 使用专用软件传递信息。
- 从规程上保证并强化传递过程的安全(参照④)。

④规程方面的安全措施。应为用户和管理员制订指导方针,包括能使系统被恶意代码攻击的可能性降至最低的活动规程和操作规定。这些指导方针应包括游戏和其他可执行软件的安装、各种互联网服务的使用和各种文件的输入等的规定。必要的时候,要对源代码或可执行代码进行单独检查。在执行恶意代码防范规程和操作规定之前,应先进行安全意识的培训和训练。

(4) 网络管理

这些内容包括对网络的规划、操作和管理。对网络进行正确的配置和管理是减少风险的有效手段。网络管理的安全措施如下:

①操作性规程。为了保证对网络进行正确、安全的操作,有必要确定相应的操作性程序和责任。这包括把操作性程序形成正式文档,并制订针对安全事件的应对程序。

②系统规划。为了保证运行可靠和足够的网络容量,有必要进行更深入的规划、准备和监控(包括安装统计软件)。应为新系统制订认可标准,并且应该对变动进行控制和管理。

③网络配置。恰当的网络配置对保证可靠的运行是非常关键的。这包括对所有服务器进行标准化的配置和高质量的、非常关键的文件编制工作。此外,必须保证用于特殊目的的服务器不用于其他目的(例如,在防火墙上不应执行其他检测任务),还要保证防范故障的措施到位。

④网络分离。为了把发生滥用的风险和可能性降至最低,应该使处理关键业务及信息的业务区域在逻辑上/物理上保持相互分离。另外,应该把开发性设施与操作性设施分开。

⑤网络监控。应该利用网络监控(工具)来识别出现在网络配置中的缺陷。网络监控器既要考虑由系统负荷所引起的变化,又要有助于识别出攻击者的身份。

⑥入侵检测。应该能检测出试图非法或越权访问系统或网络的登录以及未经许可的成功访问,这样可以使组织能以适当、有效的方式做出反应。

(5)加密技术

加密技术是一种变换数据的数学方法。在信息安全中加密技术有多种用途,例如,加密技术有助于数据的机密性和完整性、抗抵赖保护以及使识别与鉴别方法更加有效。在应用加密技术时,应注意遵守相关的法律和法规。使用加密技术的几种保护形式如下:

①维护数据机密性。当存储或传输的信息机密性要求高时,要考虑对信息进行加密存储或传输等安全措施,以保证存储或传输的安全性。在使用加密安全措施时,应考虑:

- 有关政府对密码技术使用和管理的法律和法规。
- 密钥管理必须克服的困难。
- 加密机制与所需要的保护强度之间的适应性。

②维护数据完整性。当存储或传输的信息完整性要求高时,应考虑利用散列算法、数字签名/其他完整性安全措施来保护存储或传输的信息。有些完整性安全措施(如 MAC,即消息鉴别码)针对有意或无意的改动、信息的添加或删除提供防护。数字签名安全措施不仅能为消息的完整性提供类似的防护,而且具有加强抗抵赖的性能。使用数字签名或其他完整性安全措施时,应考虑:

- 相关政府法律和法规约束。
- 相关的重要公共基础设施。
- 密钥管理必须克服的困难。

③抗抵赖。加密技术(例如使用数字签名技术)能对消息发送、传输、提交、交付和收到确认等的一致性进行验证,对通信和交易的一致性进行验证。

④数据真实性。当数据的真实性非常重要时,可以使用数字签名来验证数据的合法性。当数据是由来自第三方的参照数据组成时,或当群组实体都依靠参照数据时,尤其有必要使用数字签名。另外,数字签名还能验证数据是否是从特定人员那里发

来的。

⑤密钥管理。密钥管理包括了那些需要对密码机制进行管理和支持的技术、组织和规程等方面的内容。密钥管理的目标是实现对密钥及相关信息的安全管理。密钥管理包括密钥材料的产生、注册、建立、分发、安装、存储、存档、更换、注销和销毁。合理的设计密钥管理体系是非常重要的,这样能减少密钥失效和被未授权访问的风险。密钥管理规程取决于运用的运算法则、密钥的用途和安全策略。

4.3.3 根据信息系统类型选择基线安全措施

有两种方法可用于信息系统保护。一种方法是,将一种组织类别的安全措施在适当条件下应用于所有信息系统。由于它们的普遍可应用性,这些类别的安全措施总是可以考虑采用的。并且,因为它们是通过组织性结构和规程引入的,所以很多安全措施的执行成本并不高。有关这些安全措施的选择将在本节1)中进行讨论。

另一种方法是,对安全措施的选择要考虑信息系统的类型和特点。有关这些安全措施的选择将在本节2)中进行讨论。

当然,对于一个信息系统来说,可能有一个或多个安全措施类别或具体的安全措施对其并不适用。例如,如果对信息的接收或发送不需要保密,或完整性可以通过其他方法进行检验,那就没有必要使用密码技术。另有一些类别的安全措施,只有在获得进一步的风险分析评审信息后才能进行更恰当的选择。

在识别出对所涉及的信息系统都适用的所有安全措施类别后,利用前面介绍的方法,可以获得关于这些安全措施类别和具体安全措施的进一步信息。在对所选择的安全措施付诸实施前,应仔细地与现有或计划中的安全措施进行对照。

要对安全措施进行进一步选择,必须进行更详细的适用性分析。如果这些安全措施是根据不同的准则选择出来的,则应该对最后准备实现的一套安全措施进行仔细的搭配。在考察多个信息系统后,应考虑是否在全组织范围内建立“基线”安全模式。

在选择安全措施时,另一种无需进行详细分析的情况是使用针对具体应用领域的专用的“基线”模式。例如,有电信领域、医疗保健领域、银行业领域及其他领域的“基线”安全模式手册。在使用这些手册时,可以把现有或计划中的安全措施与手册上推荐的安全措施进行对照。在最终决定要执行哪些安全措施之前,再仔细考虑安全需要和安全保护重点。

1) 可普遍应用的安全措施

可普遍应用的安全措施类别如下:

- 信息安全管理策略。
- 遵从性检查。
- 事件处理。

- 人员。
- 操作方面。
- 业务连续性计划。
- 物理安全。

这些类别的信息安全措施是成功进行安全管理的基础,其重要性任何时候都不能低估。这些安全措施与下面要介绍的技术性更强的安全措施之间的协调也是非常重要的。一个组织决定要在这些方面做多少,取决于它的安全要求和保护重点以及可利用的资源情况。

当然,许多其他种类的安全措施在很多情况下也是可应用的,但它们的具体实施方式往往是依具体情况而定(例如,为网络提供访问控制的安全措施不同于为单机提供访问控制的安全措施)。当从可普遍应用的安全措施类别中选择某些安全措施时,应该考虑组织的规模及其安全需求。例如,一个小规模组织没有必要也没有相应的人手来建立信息安全委员会,但是却必须有履行相应职能的人员。因此,在应用时,应对安全措施的实现方式和程度进行适当的调整。

2) 具体的安全措施

除了可普遍应用的安全措施外,还应根据信息系统的类型和实际情况对具体的安全措施进行选择。表 4. 1 给出了怎样开始对具体信息系统的安全措施进行选择的例子。“√”代表正常情况下应实施的安全措施;“(√)”代表在某些情况下有必要实施的安全措施;“—”代表不需要采取安全措施。对安全措施的选择过程并没有到此结束,还要进一步考虑对安全措施的描述,如果有必要,还应从有关的参照资料中获取进一步的信息。

表 4.1 特定安全措施的选择

	独立的工作站	联网的工作站(不共享资源的客户机)	联网的服务器或联网且共享资源的工作站
识别与鉴别			
通过用户所知道的信息进行的识别与鉴别	√	√	√
通过用户持有的东西进行的识别与鉴别	√	√	√
通过用户自身的特性进行的识别与鉴别	(√)	(√)	(√)

续表

	独立的工作站	联网的工作站(不共享资源的客户机)	联网的服务器或联网且共享资源的工作站
权限控制和审计			
使用权限控制策略	—	—	√
用户对计算机的使用权	√	√	√
用户对数据、服务器和应用软件的使用权	√	√	√
检查和更新使用权	—	—	√
审计日志	√	√	√
防范恶意代码			
扫描装置	√	√	√
完整性检测(工具)	√	√	√
移动存储介质的传递控制	√	√	√
规程方面的安全措施	√	√	√
网络管理			
操作性规程	—	—	√
系统规划	—	—	√
网络配置	—	—	√
网络分离	—	—	√
网络监控	—	—	√
入侵检测	—	—	√
密码技术			
维护数据机密性	(√)	(√)	(√)
维护数据完整性	(√)	(√)	(√)
抗抵赖	—	(√)	(√)
数据真实性	(√)	(√)	(√)
密钥管理	(√)	(√)	(√)

4.3.4 根据安全重点和威胁选择安全措施

根据安全重点和威胁来选择安全措施时,应以如下方式进行:

①首先是要识别并评估安全重点以及对机密性、完整性、可用性、可确认性、真实性和可靠性的要求。所选安全措施的力度和数量应与所确定的安全重点的保护要求保持一致。

②其次,针对每一个安全重点,列出威胁,然后针对每一个威胁,提出对应的安全措施建议。这样,才可能满足具体的安全需求,并能对真正需要的地方进行保护。

1) 评估安全重点

为了有效地选择出适当的安全措施,有必要了解信息系统所支持的业务运营的安全重点。通过识别出安全重点,以及导致这些重点出现安全问题的相关的威胁后,就能正确地选择安全措施。如果评估结果表明需要高强度的保护,为了获得适当的保护,就应使用第 4.3.5 节所推荐的方法,即根据详细评估选择安全措施。安全重点包括:

- 机密性。
- 完整性。
- 可用性。
- 可确认性。
- 真实性。
- 可靠性。

评估对象应包括:信息系统自身、由信息系统存储或处理的信息、由信息系统完成的业务。信息系统的不同部分,或由信息系统存储和处理的信息的不同部分,可能对应于不同的安全重点。把安全重点与资产直接联系起来是非常重要的,因为这会直接影响到所选择安全措施的恰当性。

通过分析由于安全方面的失误或漏洞给业务造成损失的严重性(是严重损失、较小损失还是不会造成损失),就可以对安全重点做出评估。例如,如果一个组织机构的投标信息在信息系统上进行处理时被未经授权暴露,那么可能会使竞争对手开出更低的价格投标,这就可能给该组织造成巨大损失。相反,如果公开性的信息在信息系统上进行处理,那么未授权的泄漏不会给公司造成任何损失。由于不同资产的安全重点也不同,所以评估工作就应根据资产的种类有针对性、有区别地进行。当对安全重点有充分的了解后,可以依据相同或相似的业务要求对资产进行分组概括。

如果信息系统处理多种类型的信息,那么就应根据信息的种类分别对待。对信息系统进行的保护应该保证对所有种类的信息都是足够的。这时,如果某些信息需要较高的安全,那么应对整个系统适当加大保护。当只有很少的信息涉及较高的安全要求

时,可考虑把这些信息移到别的信息系统上去,避免由于保护个别信息而提高整个系统的保护力度。当然,前提是这样做不会导致业务流程的冲突。

当可能发生的机密性、完整性、可用性、可确认性、真实性或可靠性等的丧失只会造成无关紧要的损失时,第4.3.2节所描述的安全措施就能为所涉及信息系统提供足够的保护。如果经确认会造成严重损失,就应考虑是否选择除第4.3.2节至第4.3.5节以外的安全措施。

(1) 丧失机密性

资产机密性的(有意或无意)丧失会导致:

- 失去公众的信任/损害公共形象/暴露内部秘密。
- 法律责任(包括由违反与数据保护有关的法律所引起的问题)。
- 对组织政策的负面影响。
- 人身安全受到威胁。
- 经济损失。

根据对以上问题的具体回答,应该知道丧失机密性会造成的损失严重性,是严重、一般还是无关紧要。然后对分析结果进行编档。

(2) 丧失完整性

资产完整性的(有意或无意)丧失会导致:

- 错误决策。
- 欺骗行为。
- 业务职能的混乱。
- 失去公众的信任/损害公共形象。
- 经济损失。
- 法律责任(包括由违反与数据保护有关的法律所引起的问题)。

根据对以上问题的具体回答,应该知道丧失完整性会造成的损失严重性,是严重、一般还是无关紧要。然后对分析结果进行编档。

(3) 丧失可用性

考虑应用软件可用性或信息可用性的(有意或无意)丧失及其将引发的一系列事件会造成的损失。也就是说,如果某些业务被中断,会造成什么后果。例如,关键应用程序或信息可用性的丧失可能会导致:

- 错误决策。
- 无法执行关键任务。
- 失去公众的信任/损害公共形象/引发各种纠纷。
- 经济损失。
- 法律责任(包括由违反与数据保护有关的法律所引起的,以及因违反合同的最

后期限规定所引起的责任)。

- 巨大的恢复成本。

应该注意的是,丧失可用性所造成的损失可能会因可用性丧失时间的不同而不同。所以应考虑在不同时段内可用性的丧失会带来的各种损失,并评估每个时段中丧失可用性可能造成损失的严重性。

根据对以上问题的具体回答,应该知道丧失可用性会造成的损失的严重性,是严重、一般还是无关紧要。然后对分析结果进行编档。

(4)丧失可确认性

考虑系统用户和其行为代表的主体(如软件)的可确认性的丧失会造成什么损失。丧失可确认性会导致:

- 用户对系统进行操纵。
- 欺骗行为。
- 商业间谍。
- 无法跟踪的操作。
- 错误的控告。
- 法律责任(包括违反与数据保护有关的法律所引起的责任)。

根据对以上问题的具体回答,应该知道丧失可确认性会造成的损失的严重性,是严重、一般还是无关紧要。然后对分析结果进行编档。

(5)丧失真实性

考虑数据和消息真实性的丧失会造成的损失,不管这些数据和消息是人还是系统使用。在分布式系统中,这项工作尤其重要。在分布式系统中,一个决策要传给一个很广的群体,或这个决策作为参照信息使用时,数据和消息的真实性就非常重要。丧失真实性会导致:

- 欺骗行为。
- 对无效数据进行处理导出误导性的结果。
- 外部人员对系统进行操纵。
- 商业间谍。
- 错误的控告。
- 法律责任(包括违反与数据保护有关的法律引起的责任)。

根据对以上问题的具体回答,应该知道丧失真实性会造成的损失的严重性,是严重、一般还是无关紧要。然后对分析结果进行编档。

(6)丧失可靠性

考虑系统可靠性的丧失会造成的损失。对功能和性能可靠性的考虑同样重要。丧失可靠性会导致:

- 错误的输出。
- 市场份额的丢失。
- 工作人员积极性被挫伤。
- 业务停滞或中断。
- 客户信心的丧失。
- 法律责任(包括违反与数据保护有关的法律引起的责任)。

根据对以上问题的具体回答,应该知道丧失可靠性会造成的损失严重性,是严重、一般还是无关紧要。然后对分析结果进行编档。

2) 机密性威胁和安全措施

本节列举可能会危及机密性的威胁和相应的安全措施。

(1) 窃 听

未经授权访问敏感信息的手段之一就是窃听,例如通过窃听网络通信或电话通话。相应的安全措施如下:

①物理性的安全措施。通过对房间、墙壁、建筑物或传输线路等采取安全措施,会使窃听行为无法进行或很难进行。另外一种方式是加干扰。对于电话来讲,合理的布线对防窃听有一定的帮助。

②敏感信息安全策略。对敏感信息应严格约定在何时、何地、以何种方式进行交换。

③数据机密性保护。另外一种防窃听的手段是在交换消息前对其进行加密。

(2) 电磁辐射

窃听或侦听者可利用电磁辐射来获取在信息系统上进行处理或传输的信息。防电磁辐射的安全措施如下:

①物理性的安全措施。通过对房间、墙壁进行涂层处理,或采用经过金属屏蔽的电缆和低辐射光缆,可以阻止电磁辐射泄漏。

②数据机密性保护。对需要传输的数据进行加密处理,这种安全措施仅适用于经过处理的信息,而不是那些正进行处理的、显示出来的或打印出来的信息。

③使用低辐射的信息设备。经过防辐射处理措施的设备可以满足此要求。

(3) 恶意代码

恶意代码会通过捕获和猜测口令导致机密性的丧失。相应的安全措施如下:

①恶意代码防范措施。见“信息系统特有的安全措施”第4.3.2节2)中的(3)。

②事件处理。及时报告异常事件能限制由恶意代码攻击所造成的损失。

(4) 冒充用户身份

冒充用户身份是系统的鉴别功能失效所引起的。当通过这种冒充可访问敏感信

息时,会最终导致机密性的丧失。相应的安全措施如下:

①识别与鉴别。可以根据人所记住的信息、所持有的东西或内在固有的特性来实现识别与鉴别。如果组合使用这三种识别与鉴别方式,会加大冒充的难度。

②访问控制和审计。访问控制虽然不能区分合法使用者和未授权冒充使用者,但是访问控制机制确实能降低冒充使用所造成的影响。对审计日志的分析能识别出未经许可的访问活动。

③恶意代码防范措施。考虑到恶意代码是捕获口令的手段之一,应该有专门防范此种(恶意代码)软件的安全措施。

④网络管理。另外一种未授权访问的方法是在通信(如电子邮件)中冒充用户。可以采取用于网络安全管理的有关安全措施。

⑤数据机密性保护。如果由于种种原因,无法采取以上安全措施时,或以上措施还不够时,可以进一步使用敏感数据的存储加密来加强保护,使得非法获得者无法理解消息所表达的意义。

(5)消息的错误路由

消息的错误路由指故意或意外地将消息引导到错误的传输方向。如果错误路由允许非授权访问消息,则会导致机密性的丧失。相应的安全措施如下:

①网络管理。确保路由表不被未授权修改。

②数据机密性保护。为了防止因消息的错误路由所导致的未授权访问,可对消息进行加密。

(6)软件故障

如果软件发生故障,或者软件故障会引发操作方面的漏洞,就会危及业务运行。安全处理措施如下:

①事件处理。如果用户发现任何软件功能异常,应当尽快报告给负责人员或同时予以适当处理。

②操作方面。应在软件使用前对其安全性能进行测试,以保证软件能正常运行;应对软件变动进行控制,以防止在软件更新或其他形式的变动时引发问题。

(7)防 盗

如果信息系统组件上存有能被偷盗者访问的敏感信息,那么被盗会造成机密性丢失和资产丢失。相应的安全措施如下:

①物理安全措施。通过物理保护,对放有信息设备和信息的建筑物、区域和房间的访问进行控制,或采取更具体的防盗措施。

②人员。人员方面的安全措施(包括控制外来人员、签订保密协议)应到位。

③数据机密性防护。如果存有敏感信息的信息设备(如笔记本电脑)有被盗的可能性,那么应采取数据加密存储措施。

④介质控制。对任何含有重要信息的介质都应进行保护并附加适当防盗措施。

(8) 对未授权使用计算机、数据、服务和应用程序的防范

对计算机、数据、服务和应用程序的未授权使用,都可能导致计算机、数据、服务和应用程序的未授权访问,进而会危及信息的机密性和造成资产丢失。安全措施包括身份识别和鉴别、对逻辑访问权的控制和审计,对网络进行分割管理。

①识别和鉴别。适当的安全措施辅以逻辑访问控制可增强防范未授权访问。

②访问控制和审计。采用访问控制机制,对审计日志的检查和发现未经授权的操作。

③网络分割。网络分割可增加未授权访问的难度。

④物理访问控制。除逻辑访问控制外,还可附加物理访问控制措施。

⑤存储介质控制。当重要敏感信息保存在介质上时,采取介质控制措施以避免未授权访问。

⑥数据机密性保护。如果由于某些原因致使上述安全措施不能或不足以发挥作用,也可采用加密方式来提供保护。

(9) 对存储介质的未授权访问

如果介质上存有机密性信息,那么对存储介质的未授权访问及使用会危及机密性。相应的安全措施如下:

①操作方面。介质控制能为介质提供物理保护和可确认性;经过确认的删除能确保没有人能从已被删除过的介质上获得机密信息。应该特别注意那些可移动的介质的保管、使用和销毁,比如,软盘、USB 盘、备份磁带和备份纸张等。

②物理安全。对房间的适当保护和使用安全设备能防止未经许可的访问。

③数据机密性保护。可通过对信息进行加密来对介质上的敏感信息提供进一步的保护。为保证加密信息的无故障使用,一个有效的密钥管理系统是有必要的。

3) 完整性威胁和安全措施

本节列举可能危及数据完整性的威胁及相应的防范措施。

(1) 存储介质的变质

存储介质的变质会危及存储于其上的信息的完整性。如果该信息的完整性比较重要,应采取以下安全措施:

①存储介质控制。充分的存储介质控制包括完整性检测,通过完整性检测可以探知存储的文件是否遭到损坏。

②备份。所有重要的文件、业务数据都应该进行备份。如果注意到数据的完整性已被破坏,则备份可用来恢复文件。

③数据完整性保护。加密保护方式可用来增强保护存储数据的完整性。

(2) 维护方面的错误

如果维护工作未能定期进行,或在维护过程中存在错误操作,就会危及相关信息的完整性。在此种情况下保护完整性的安全措施有:

①维护。正确的维护是避免出现错误操作的最好办法,包括文档化的和经过验证的维护程序及对工作适当的监督。

②备份。如果维护方面的错误已经发生,备份可用来恢复遭损坏的信息。

③数据完整性保护。某些加密保护方法可用来增强保护存储数据的完整性。

(3) 恶意代码

恶意代码能破坏系统相关功能,最终会导致多种形式的安全性能损坏(比如说,通过恶意代码进行未授权访问系统的人对数据或文件进行破坏,或恶意代码直接对数据或文件进行破坏)。相应的安全措施如下:

①恶意代码防范措施。见“信息系统特有的安全措施”第4.3.2节2)中的(3)。

②事件处理。及时报告所有的事件有助于把恶意代码所造成的损害控制在一定范围内。入侵检测可以察觉出试图访问系统或网络的登录。

(4) 冒充用户身份

冒充用户身份能破坏系统的鉴别功能及其相关功能。当假冒人员把信息修改或破坏信息时,会导致完整性破坏。总之,当通过冒充用户身份获得访问权限和修改信息时,就会导致信息的完整性问题。防范此类威胁的安全措施如下:

①识别与鉴别。可以根据用户知道的信息、所持有的东西或内在固有的特性来实现识别与鉴别。如果组合使用这三种识别与鉴别方式,会加大冒充的难度。

②逻辑性访问控制和审计。访问控制机制能降低冒充使用系统资源所造成的影响。对审计日志的分析能识别出未经许可的活动。

③恶意代码的防范。考虑到窃取口令的方式之一就是利用恶意代码来捕捉口令,从而实现假冒合法用户的目的,所以应采取针对此类恶意软件的防范措施(在第4.3.2节2)中有相关介绍)。

④网络管理。另外一种未授权访问的方法是在通信(如电子邮件)中冒充用户。可通过网络安全的有关安全措施阻止这类非法访问。

⑤数据完整性保护。如果由于某些原因致使上述安全措施不能或不足以发挥作用,也可采用某些加密方法(如数字签名)来提供保护。

(5) 消息的错误路由

错误路由也可能导致完整性的丧失,例如消息有可能被修改后传送到原定的地址。相应的安全措施如下:

①网络管理。针对错误路由的防护措施是确保路由表不被非授权修改,以及路由信息的真实可靠。

②数据完整性保护。为了防止因消息的错误路由所导致的未授权更改数据,可采用散列函数和数字签名方法对信息进行处理。

(6)抗抵赖

当消息收发的确认和不可否认特性非常重要时,应当采取“抗抵赖”安全措施。

(7)软件故障

软件故障可以破坏用该软件处理的数据或信息的完整性。防范此类威胁的安全措施如下:

①报告软件故障。及时报告软件故障能限制由此引起的损失。

②操作方面。应对安全性能进行测试,以保证软件的正常运行;应对软件变动进行控制,以防止软件更新时或其他形式的变动时所引发的安全问题。

③备份。备份可用来恢复那些因软件故障而损坏的数据。

④数据完整性保护。某些加密方法可用来保护信息的完整性。

(8)供应故障(电源、空调)

供应故障会影响系统配件的完整性。例如,供应故障会导致硬件故障或存储介质故障。针对供应故障的安全措施如下:

①电源和空调。应在必要的地方对电力供应和空调采取安全措施以避免由供应故障所导致的问题,比如采用电力过载和欠压保护的安全措施。

②备份。应对所有重要文件和业务数据等进行备份。如果文件或其他信息因供应故障丢失,备份文件将可以用来恢复。

(9)技术故障

技术故障,如在一个网络里的故障,会破坏那些在网络上保存或处理的信息的完整性。相应的安全措施如下:

①操作方面。配置管理、变动管理以及容量管理可用来预防信息系统故障。编档和维护可用来确保信息系统的无故障运行。

②网络管理。应通过制订操作程序、进行系统规划和适当的网络配置将技术故障发生的可能性降至最低。

③电源和空调。应在必要的地方对电力供应和空调采取安全措施以避免由技术故障所导致的安全问题,比如采用电力过载或欠压保护的安全措施。

④备份。备份可用来恢复被损坏的技术信息。

(10)传输错误

传输错误会危及信息的完整性。安全措施如下:

①线缆。精心设计和铺设线缆可以避免传输错误。

②网络管理。应当正确操作和维护网络设备以避免传输故障引起传输数据出错。

③数据完整性保护。通信协议中的检验和循环冗余码可用来防范意外的传输错

误。在恶意攻击的情况下,可采用加密方式保护数据的完整性。

(11)对未授权使用计算机、数据、服务和应用软件的防范

对计算机、数据、服务和应用软件的未授权使用,可能导致计算机、数据、服务和应用软件的未授权破坏,进而危及信息的完整性。安全措施包括身份识别和鉴别、对逻辑访问的控制和审计以及对网络进行分割管理。

①识别与鉴别。适当的识别与鉴别安全措施辅以逻辑访问控制可增强防范未授权访问。

②访问控制和审计。采用访问控制机制,检查和分析审计日志可发现未经授权的操作。

③网络分割。网络分割可增加未授权访问的难度。

④物理访问控制。除逻辑访问控制外,还可采用物理访问控制措施。

⑤存储介质控制。当重要敏感信息保存在介质上时,就应采取介质控制措施以避免未授权访问。

⑥数据完整性保护。某些加密方法可用来保护正在存储或传送的信息的完整性。

(12)对未授权程序和数据的使用的防范

未授权使用程序和数据可导致对信息的修改,或可能将程序和信息中含有的恶意代码引入系统或网络中,危及在系统中保存或运行的数据和信息的完整性。防范措施如下:

①安全意识培训。所有人员应意识到他们不应在系统上使用任何未经信息系统安全管理者授权的软件和数据。

②备份。备份可恢复已丢失或被损坏的信息。

③识别与鉴别。适当的识别与鉴别安全措施辅以逻辑访问控制可增强防范未授权访问。

④逻辑访问控制和审计。对访问进行控制,保证只有获得授权的人员才能使用软件对信息进行处理和删除。检查和分析审计日志可发现未授权使用程序和数据的行为。

⑤对恶意代码的防范。所有程序和数据在使用前都应进行恶意代码检查。

(13)对存储介质的未授权访问

对存储介质的未授权访问及使用会危及完整性,还可能导致对存储在介质上的信息的未授权销毁。相应的安全措施如下:

①操作方面。介质控制能为介质提供物理保护和可确认性,以防止未授权访问介质上的信息。应该特别注意那些可移动的介质的保管、使用和销毁,比如软盘、USB盘、备份磁带和备份纸张等。

②物理安全。对房间的适当保护和使用访问控制设备能防止未经许可的访问。

③数据完整性。加密方法可用来保护存储介质上信息的完整性。

(14) 用户过失

用户过失能破坏信息的完整性。相应的安全措施如下：

①安全意识培训。应对所有用户进行培训以防止在处理信息过程中出现操作失误和过失。这需要对用户就特定操作而定义的规程(操作性规程或安全规程)进行培训。

②备份。备份能恢复那些因用户过失而被破坏的信息。

4) 维护数据可用性的安全措施

可能危及可用性的威胁和相应的安全措施如下。

(1) 毁坏性攻击

毁坏性攻击能毁坏数据或使信息系统(或组件)瘫痪。防范此类威胁的安全措施如下：

①纪律约束。所有的员工都应意识到如果他们毁坏信息、系统或组件(无论是故意的还是无意的)会带来的严重后果。

②存储介质控制。所有的存储介质都应通过适当的物理保护手段和可确认性措施来防止非授权用户的访问和使用。

③备份。所有重要的文件、业务数据都应该制作备份。如果文件或其他信息丢失了,备份可用来恢复文件。

④介质保护。物理访问控制可用来避免非授权访问,从而把因遭非授权访问而损坏信息设备和信息的可能性降至最低。

⑤识别与鉴别。适当的识别与鉴别安全措施辅以逻辑访问控制可增强防范未授权访问和使用介质。

⑥逻辑访问控制和审计。对逻辑访问进行控制,保证只有获得授权的人员才能使用软件对信息进行处理和删除。检查和分析审计日志可发现未授权访问或操作行为。

(2) 存储介质的变质

存储介质的变质会危及存储于其上信息的可用性。若可用性很重要,则应当采用下述安全措施：

①存储介质控制。在信息的可用性丧失之前,定期测试检测存储介质的变质。存储介质应当妥善保存在合适的环境中,以防外界影响引起存储介质的变质。

②备份。所有重要的文件、业务数据都应该制作备份。如果文件或其他信息丢失或损坏了,则备份可用来恢复文件和数据。

(3) 通信设备及服务方面的故障

通信设备及服务故障会危及其传输的信息的可用性。可根据引起通信设备和服

务故障的不同原因,采取相应的安全措施:

①冗余与备份。信息交换设备的适当的冗余能降低超载发生的可能性。根据最大可接受的停工时间,也可用备用设备来满足运行需要。在任何时候,配置数据都应进行备份,以应紧急之需。

②网络管理。包括更多、更详细的防范通信设备或服务故障的网络安全措施。

③布线。精心设计和铺设线缆可以预防对线缆的损坏。若线缆有被破坏的迹象,应当进行检查。

④抗抵赖。当消息收发的证明和不可否认特性非常重要时,应当采取“抗抵赖”安全措施。

(4)火患与水患

火患和水患能破坏信息设备和信息的可用性。防火、防水的安全措施如下:

①物理保护。对所有放置信息设备和介质(存有重要信息)的建筑物和房间都应采取防火、防水措施。

②业务连续性方案。为了使业务运营免于火、水引起的灾难性损坏,应制订并实施业务连续性方案,并对所有重要信息进行备份。

(5)维护方面的错误

如果维护工作未能定期进行,或在维护过程中犯错误,相关设备和信息的可用性就会受到威胁。在此种情况下保护完整性的安全措施有:

①维护。正确的维护是避免维护错误的最好办法。

②备份。如果发生维护错误,备份可以恢复丢失的信息。

(6)恶意代码

恶意代码能破坏系统的鉴别功能及其相关功能,最终会导致可用性失效(比如说,通过恶意代码而获得未经授权访问系统的人对数据或文件进行破坏,或恶意代码直接对数据或文件进行破坏)。相应的安全措施如下:

①恶意代码防护措施。见“信息系统特有的安全措施”第4.3.2节2)中的(3)。

②事件处理。对所有事件的及时反应有助于把恶意代码所造成的损害控制在一定范围内。对入侵的检测可以察觉出试图进入系统或网络的登录情况。

(7)冒充用户身份

冒充用户身份能破坏系统的鉴别功能及其相关功能。当假冒人员把信息修改或破坏信息时,会最终导致信息的不可用。相应的安全措施如下:

①识别与鉴别。可以根据人知道的信息、所持有的东西或内在固有的特性来实现识别与鉴别。组合使用这三种识别与鉴别方式,会加大冒充的难度。

②逻辑性访问控制和审计。访问控制机制能降低冒充使用所造成的影响。对审计日志的分析能识别出未经许可的访问和操作活动。

③防护恶意代码。考虑到窃取口令的方式之一就是利用恶意代码来捕捉口令,所以采取针对此类恶意软件的防护措施(参见第4.3.2节2)中的介绍)。

④网络管理。另外一种未经授权访问的方法是在通信(如电子邮件)中冒充用户。对此可以使用有关网络管理的安全措施。

⑤数据的备份。数据备份虽然不能防止对用户身份的冒充,但能恢复因冒充操作引起的数据损坏。

(8)消息的错误路由

错误路由也能够导致消息丧失可用性。相应的安全措施如下:

①网络管理。针对错误路由的防护措施是确保路由表不被修改,以及路由信息的来源真实可靠。

②抗抵赖。如果需要收发消息证明和不可否认特性非常重要时,那么就需使用“抗抵赖”的措施。

(9)对资源的滥用

对资源的滥用能导致信息的不可用。相应的安全措施如下:

①人员。每个员工都应意识到滥用资源可能引起的后果和自己应承担的责任;如果有必要应进行纪律处理。

②操作方面。应对系统的使用情况进行监控,以查出未经许可的活动;应对任务进行分割,以使滥用职权的可能性降至最低。

③识别与鉴别。适当的识别与鉴别安全措施与逻辑访问控制结合使用,可以增强防止未经许可的使用。

④逻辑访问控制和审计。对各种资源进行逻辑访问控制。对审计日志的分析能查出未经许可的操作活动。

⑤网络管理。应通过适当的网络配置和权限分割把网络资源被滥用的可能性降至最低。

(10)自然灾害

为了防止自然灾害对信息和设施造成损害,应采取以下安全措施:

①自然灾害防护。针对自然灾害,应对建筑物进行符合有关政策要求的保护。

②业务连续性方案。应制订业务连续性方案,并进行严格测试,还应应对重要信息、设施和资源进行备份。

(11)软件故障

软件故障能破坏相关软件中数据和信息的可用性。维护可用性的安全措施如下:

①报告软件故障。及时报告软件故障能限制软件故障所造成的损失。

②操作方面。应对安全性能进行测试,以保证软件的正常运行;应对软件变动进行控制,以防止软件更新时或其他形式的变动时所引发的不可用问题。

③备份。应进行备份,例如,将以前生成的数据保存下来可用来恢复功能不正常的软件处理过的那些数据。

(12) 供应故障(电源、空调)

供应故障会影响可用性。例如,供应故障会导致硬件故障、存储介质故障。针对供应故障的安全措施如下:

①电源和空调。应在必要的地方对电力供应和空调采取安全措施以避免由供应故障所导致的不可用问题,比如采用电力过载或欠压保护的安全措施。

②备份。应对所有重要文件和业务数据等进行备份。如果文件或其他信息因供应故障丢失,备份文件可以用来恢复数据。

(13) 技术故障

技术故障,如网络里的故障,会破坏那些在网络上保存或处理的信息的可用性。有关安全措施如下:

①操作方面。配置管理、变动管理以及容量管理可用来预防信息系统故障导致的不可用问题。编档和维护可用来确保信息系统的无故障运行。

②网络管理。应通过制订操作程序、进行系统规划和适当的网络配置将发生技术故障的可能性降至最低。

③业务连续性方案。为了避免因技术故障导致的灾难性后果,应制订业务连续性方案,重要的信息、设施和资源应有备份。

(14) 防盗

偷盗行为会危及信息的可用性和信息设备安全。相应安全措施如下:

①物理安全措施。通过设备和介质保护,对放有信息设备和信息的建筑物、区域和房间的访问进行控制,或采取具体防盗措施。

②人员。人员方面的安全措施(包括控制外部人员、签定保密协议)应到位,以避免偷盗。

③介质控制。对任何含有重要信息的介质都应进行保护以防盗。

(15) 负荷超载保护

设备负荷超载会危及信息的可用性。安全措施如下:

①冗余与备份。信息交换设备的适当的冗余能降低超载发生的可能性。根据最大可接受的停工时间限制,也可采用备用设备来满足运行需要。在任何时候,配置数据都应进行备份,以应紧急之需。

②网络管理。适当的网络配置、管理措施和使用适当的信息交换设备可以避免超载。

(16) 传输错误

传输错误会危及信息的可用性。安全措施如下:

①线缆。精心设计和铺设线缆可以避免传输错误,如超载所引发的数据错误。

②网络管理。网络管理虽然不能避免传输错误的发生,但可以在传输错误发生时识别症结所在,并发出警报,以及时采取补救措施。

(17)对未授权使用计算机、数据、服务和应用软件的防范

对计算机、数据、服务和应用软件的未授权使用可能导致计算机、数据、服务和应用软件被未授权破坏,进而危及信息的可用性。安全措施包括身份识别和鉴别、对逻辑访问的控制和审计,还有对网络进行分割管理。

①识别和鉴别。适当的识别和鉴别安全措施辅以逻辑访问控制可增强防范未授权访问。

②逻辑访问控制和审计。采用访问控制机制,对逻辑访问进行控制,对审计日志的检查和发现未经授权的操作。

③网络分割。网络分割可增加未授权访问的难度。

④物理访问控制。除逻辑访问控制外,还可采用物理访问控制。

⑤存储介质控制。当重要敏感信息保存在介质上时,就应采取介质控制措施以避免未授权访问和操作。

(18)防止使用未授权的程序和数据

使用未授权的程序和数据(如游戏,不明外来软件)会危及在系统中保存或处理的数据信息的可用性,如删除信息或带入恶意代码。防范措施如下:

①安全意识培训。所有人员应意识到他们不应在系统上使用任何未经信息系统安全管理者授权的软件。

②备份。备份可恢复已丢失或被损坏的信息、设施及其配置资源。

③识别和鉴别。适当的识别和鉴别安全措施辅以逻辑访问控制可增强防范未授权访问。

④逻辑访问控制和审计。对逻辑访问进行控制,保证只有获得授权的人员才能使用软件对信息进行处理和删除。检查和分析审计日志可发现未授权访问和操作行为。

⑤对恶意代码的防范:所有程序和数据在使用前都应进行恶意代码检测。

(19)对存储介质的未授权访问

对存储介质的未授权访问及使用会导致对存储在介质上的信息的未授权修改甚至销毁,危及可用性。相应的安全措施如下:

①操作方面。介质控制能为介质提供物理保护和可确认性,以防止未授权访问存于介质上的信息。应该特别注意那些可移动的介质的保管、使用和销毁,比如软盘、USB 盘、备份磁带和备份纸张等。

②物理安全。对房间的适当保护和使用访问控制设备能防止未经许可的访问。

(20)用户过失

用户过失能破坏信息的可用性。相应的安全措施如下:

①安全意识培训。应对所有用户进行培训以防止在处理信息过程中出现过失。这需要对用户就特定操作而定义的规程(操作规程或安全规程)进行培训。

②备份。备份能恢复那些因用户过失而被破坏的信息。

5)保证可确认性、真实性和可靠性的安全措施

在不同领域内,可确认性、真实性和可靠性所指的内容是不一样的。相应地,应在不同的领域实施不同的安全措施。因此,本节仅给出一般性指导。

(1)可确认性

有些威胁可能无法追查某些操作的具体执行人员。对于这些威胁一定要仔细考虑。此类威胁的例子有:共享账号导致缺乏对操作的追溯能力,冒充用户身份,软件故障,对计算机、数据、设施及应用软件的未授权访问,对身份的低鉴别能力。为了维护可确认性,应认真考虑这些威胁。

有两种可供选择的可确认性方法。一种是对负责具体操作的人员的身份进行确认。审计日志能帮助做到这一点。另一种是同一信息系统内用户之间的可确认性。使用抗抵赖功能、知识分割和双向鉴别能做到这一点。

许多安全措施可以加强或帮助加强可确认性。这方面的安全措施从安全策略、安全意识和逻辑访问控制及审计,到一次性口令、介质控制,都可以应用。信息所有权策略的实施是保证可确认性的前提条件。在选择具体安全措施时应考虑可确认性的具体用途。

(2)真实性

有些威胁使用户、系统或处理进程不能确定某一个客体到底是什么或从哪里来,降低真实性。例如不加控制的数据更改、不对数据来源进行核对以及没有对原始数据进行维护。

许多安全措施可以加强或帮助加强真实性。这方面的安全措施从使用有标记的参考数据、逻辑访问控制及审计,到使用数字签名,都可以应用。

(3)可靠性

能导致系统不正常运行的威胁会降低可靠性。这种威胁的例子有不稳定的系统性能和不可靠的供应商。可靠性的丧失会导致糟糕的客户服务或使客户失去信心。

许多安全措施可以加强或帮助加强可靠性。这方面的安全措施从业务连续性计划、物理结构中的冗余、系统维护,到确认与验证、逻辑访问控制及审计,都可以应用。在选择具体安全措施时应考虑可靠性的具体用途。

4.3.5 根据详细风险评估选择安全措施

根据详细风险评估来选择安全措施时,所遵循的原则与上一节相同。详细风险分

析能考虑到信息系统及其资产的具体要求和环境。与上一节的不同点在于评估过程中的工作量和细微程度。

我们已经在前面介绍了组织范围内的几种主要风险分析策略,包括:

- 所有的信息系统都使用“基线”法。
- 所有的信息系统都使用详细风险分析法。
- 使用“组合法”,即对所有的信息系统先进行高等级风险分析,然后在低风险的信息系统应用“基线”法,高风险的信息系统应使用详细风险分析法。

下面介绍安全措施的选择原则。如果决定对所有信息系统使用详细风险分析以确定出安全措施,那么关于如何选择安全措施和如何使用详细风险分析结果的内容可以从这些选择原则中找到。

安全措施选择涉及的内容有四方面,即脆弱性、威胁、影响和风险本身。当决定是降低或消除某个风险还是接受某个风险时,需要考虑风险本身的处理方法(降低风险的例子:买保险;消除风险的例子:把敏感信息移到另一台计算机上)。决定风险的因素(即脆弱性、威胁和影响)是安全措施要解决的主要对象。安全措施对这些因素的解决形式如下:

①脆弱性。安全措施能够消除脆弱性,或降低其脆弱程度(例如,当一个与外部网络相连的内部网络十分脆弱,易于遭受未经授权访问攻击,安装合适的防火墙将使这种连接的脆弱性降低,而断开连接则会完全消除此脆弱性)。

②威胁。安全措施能降低威胁发生的可能性,或在遭受恶意攻击时,通过增大攻击所需的技术复杂程度来阻止威胁的发生或降低发生的概率。

③影响。安全措施能减少或避免影响(例如,如果负面影响是信息可用性的丧失,那么,复制这些信息并安全地保存在其他地方,再加上有一个业务连续性方案可随时执行,就能降低或消除负面影响)。有好的审计跟踪记录、分析和报警设施能够及早地检测出事件,并减少负面业务影响。

即使是同一个安全措施,以不同的方式和在不同的地方使用,那么实施效果的差别也是非常大的。在很多情况下,一个威胁可利用多个脆弱性。因此,如果一项措施是被用来阻止这种威胁的发生,可能会同时涉及好几个脆弱性。反过来也是这样,即弱化或消除一个脆弱性的安全措施可能会阻止或减小多个威胁。在选择安全措施时,要尽可能考虑这些关系所带来的好处。所有附带的好处也应该整理成文档,以便使我们对某项安全措施所能满足的安全要求有一个全面的认识。

一般来讲,安全措施能提供以下一种或多种类型的保护:预防、检测、监控、阻碍、减缓、恢复、纠正以及安全意识。至于哪一种是最好的,这取决于具体环境及每种安全措施要达到的目的。在很多情况下,一项安全措施会提供多种保护及附加好处。只要有可能,应尽量选择能提供多种好处的安全措施。

在涉及以上各种保护时,要考虑安全的适度平衡问题。如果过于强调一种类型的

安全措施,那么整体的安全性可能得不到保障。例如,如果实现一种主要具有阻碍威胁的功能的安全措施而没有足够的检测安全措施与其配套,那么在阻碍威胁的功能失效时就不能及时识别出来,则系统的整体安全性仍将是低效的。

在实施所建议的安全措施前,应将其与现行的安全措施做一个比较评估,首先应考虑能否通过对现行安全措施的扩展或升级来达到所要求的安全。因为与引入全新的安全措施相比,这样做的成本会低得多。

在选择安全措施的时候,要对实施安全措施的成本与资产的价值、安全措施所带来的收益进行权衡。有时安全措施的实施和维持成本要比安全措施本身的成本高得多,因此在选择安全措施时,应考虑实施后的维持能力。

一些技术上的约束条件,如对性能的要求、可管理性(操作方面的支持要求)和兼容性问题等,可能会限制使用某些安全措施。在这种情况下,系统管理者应与安全管理者协调工作以确定出最佳的解决方案。有时一项安全措施会降低系统的性能,这又需要系统管理者与安全管理者一同确定出解决方案,此解决方案应在保证足够安全性的同时,使系统具有必要的性能。

隐私保护及法律等方面可能要求一些特定的安全措施,因此要定义保证这些法律性要求的“基线”安全要素。

4.3.6 安全措施的实施

为了实施安全措施,信息安全计划中描述的所有的必要步骤都应执行。负责这个计划的人(一般是信息系统安全官员),应保证遵照信息安全规划中的优先顺序和进度计划表执行。

为保证连续性和一致性,安全措施的文档应是信息安全文档的一个重要组成部分,也应该是组织的安全文档的一部分。信息安全文档是一系列文档,包括安全规划、业务连续性计划、风险分析文档以及安全策略和规程等。它应该设计成能满足领导、用户、系统管理员、维护人员和那些参与配置和变更管理的人员的需要。它必须是通用的和足够详细的,以帮助消除安全过失和疏忽所造成的影响,也提供保证安全操作正确和有效地执行的信息。很多文档,特别是关于脆弱性、威胁和风险的文档,可能是敏感的并应妥善保护起来防止未被授权的泄露。因此,绝大多数组织都需要非常小心地处理这些文档,并且可能需要一种“可信的”的分发规程。如果采用这种规程,也应以一种方式将这些规程文档化,包括描述安全措施的敏感信息如何被存储、访问和使用。此外,这个规程应确认谁负责决定被保护的信息如何存储以及谁可以访问和使用它。在分发规程的设计中,安全措施信息的可访问性应考虑到一些特别的因素,例如在灾难或其他不可预见的事件等情况下,由于时间的紧迫性,需要尽快找到和使用灾难恢复计划。最后,对安全措施文档进行严格的配置控制也是需要的,以保证不会作出未被授权的更改而造成降低安全措施的效率。

一旦信息安全规划完成,安全措施一定要付诸实施,安全遵从性也要进行检查和测试。进行安全遵从性检查检测的目的是检查安全措施是否被正确地实施,它们是否被有效地使用和恰当地测试。安全测试可作为这个检测的一部分来进行。安全测试应按照安全测试计划进行,测试计划描述了测试方法、进度表和环境。如果渗透测试被风险评估证明有效,则可以使用渗透测试。必须撰写详细的安全测试过程,并使用标准测试报告。其目的是以某种方式来执行渗透测试,这种方式保证信息安全的需求得到满足,风险被降低。

在已经制订信息安全规划之后,实施则是信息系统安全官员的责任。在实施过程中应考虑下列情况:

- 将安全措施的开销维持在批准的范围内。
- 按照信息安全规划的要求正确实施安全措施。
- 按照信息安全规划的要求操作和管理安全措施。

大多技术上的安全措施都需要操作方面的及行政管理的规程的补充和支持,绝不能单纯地依赖技术措施。

安全措施的实施同样需要安全意识的培训。需要特别参加安全培训的有:

- 开发信息系统的负责人。
- 操作信息系统的负责人。
- 信息工程及系统安全官员。
- 安全管理(比如访问控制)的相关负责人。

当信息安全规划完成后,应正式地批准实施在信息安全规划中规定的安全措施。当这些安全措施得到批准并实施后,就应该授权运行该信息系统或提供服务。

信息系统和服务的任何重大变更都应该进行重新评审、重新测试并重新获得批准。

4.3.7 安全意识

组织内从管理者到用户的所有层次,都应该贯彻执行安全意识活动计划。特别注意的是,没有用户层员工的接受和参与,安全意识活动计划不可能得到成功。用户需要理解安全意识活动计划成功执行的重要性。

安全意识活动计划应该大力宣传组织的信息安全策略,并且确保完全理解安全指南以及各种正确的行为。另外,安全意识活动计划应该包含系统安全规划的目标。该活动计划至少应包括下列内容:

- 信息分类。
- 用户和组织应知的安全事件的含义。
- 组织的信息安全策略所包含的目标、对组织信息安全策略的解释、风险管理策略、用来指导和理解风险与安全措施的方针和策略。

- 待实施的信息安全计划以及待检测的安全措施。
- 信息保护的基本需求。
- 资产所有者或管理者的责任、作业描述和规程。
- 需要报告和调查各种破坏及企图攻击等事件和行为。
- 以未经授权方式和越权方式行事的后果(包括纪律处置)。
- 更改、配置管理。

有效的安全意识活动计划有各种形式,比如宣传手册、海报、电视、新闻报道、实际练习、专题讨论会、研究班、演讲等。重要的是安全意识活动计划的实施应该考虑社会、文化、心理学和法律等方面的问题。

安全意识应该关注组织中的每一个人,并且应该影响人们的行为规范,引导并提高全体人员的责任感。提高每个职员的安全意识是各层次负责人的工作之一。因此,他们必须制订实施安全意识活动计划的策略。在大型组织中,信息安全意识教育的责任属于组织的信息安全官员。

安全意识教育应该定期重复进行,既可以更新原有雇员的安全知识,又可以使新人了解这方面的情况。此外,每一位新雇员、每一位履行新岗位职责者以及新升迁者都应该受到安全意识的再教育,以了解自己新的责任。将信息安全方面的知识融合到其他培训课程中,是安全意识教育的有效方法。需要强调的是,安全意识活动计划是一个持续和长期的过程。

4.4 后续活动

后续活动在信息安全中是至关重要的,但是很容易被忽略。已实施的安全措施只有通过在实际业务运行中的检验才能知道其有效性。必须保证这些安全措施是被正确地使用的,并且任何安全事件和更改都要检测到并进行处理。后续活动的主要目的是保证安全措施像设计的那样在发挥作用。经过一段时间后,任何服务或机制的性能都可能有恶化的趋势。后续活动力图发现这种恶化并启动矫正行动。这是维持保护信息系统所需的安全水平的唯一方法。下面描述的活动计划构成一个有效的后续活动的基础。信息安全管理是一个不断进行的过程,在实施了安全措施和安全计划后仍然要继续。

4.4.1 维护安全措施

安全措施的维护,包括行政管理,是一个组织的安全活动计划的基本组成部分。它是各层次管理的共同责任,它确保:

- 使用组织的资源维护安全措施。
- 定期检查,保证安全措施的性能满足期望值。

- 修改参数以反映变化或增减。
- 重新初始化种子值或计数器值等。
- 发现新的需求时升级安全措施(例如升级到新版本)。
- 明确维护安全措施的责任。
- 信息系统软、硬件的修改和升级不应该改变已有安全措施的性能。
- 推行新技术不应该导致新的脆弱性和威胁。

当上述维护活动完成时,已有的安全措施将会持续发挥作用,不利影响也会尽量避免。

4.4.2 安全遵从性

与安全审计和安全评审类似,安全遵从性是保证信息系统安全计划一致性和连续性的非常重要的活动。

为了保证合适的安全等级,极为关键的是使已实施的安全措施遵从和继续遵从信息工程或系统安全规划。在所有信息工程和系统中,遵从性在下列过程中是必需的:

- 在设计和开发时。
- 在系统运行的生命期内。
- 在更换和处置时。

安全遵从性检测可以由现有的外部或内部人员(例如审计员)来完成,并且主要基于使用与该信息工程或系统相关的检测列表。

应该很好规划安全遵从性检测,并将其与其他规划的活动整合在一起。

现场检测特别有助于判断职员和使用者是否遵从具体的安全措施及规程。检测应该用来保证安全措施是实施了的、正确实施的、正确使用的、部署的地方是正确的以及经过测试的。如果发现某些安全措施没有遵从安全一致性,应该制订更正行动计划并付诸行动,更正的结果还应通过评审。

4.4.3 监 控

监控是信息系统安全周期的一个关键部分。如能正确进行,可以对下述问题提供清晰的管理意见:

- 同设置的目标和最后底线比较,取得了什么效果。
- 取得的效果是否令人满意,以及特定的主动权是否发挥作用。

所有关于资产、脆弱性、威胁和安全措施的改变都会对风险产生潜在的重要影响,及早对系统变更进行检测,可以阻止潜在的风险演变为真实的风险。

很多安全产品都可产生一系列与安全相关事件的日志。对这些日志,经过定期的审核并尽可能使用统计技术进行分析,可以及早检测到变更的趋势和不利事件的发生。监控活动也应包括向相关信息安全官员报告的规程以及对标准的基础性管理的

规程。

4.4.4 事件处理

发生安全事件是不可避免的。要针对每个事件所造成的损害开展调研。事件处理过程能对正常信息系统运行的偶然或故意破坏做出反应。因此,应该开发出事件处理报告和调查方案,并使之适合整个组织的信息系统和服务。信息安全事件调查的基本目标是:

- 以一种有效的方式对事件做出反应。
- 从事件中吸取经验教训以防止类似事件的再发生。

对已决定的安全计划的活动进行预先定义,将使组织在合理的时间内做出反应。消息处理计划必须包括以年月日时的顺序记录所有事件和活动,这将有助于事件的确定。这是达到下一个目标的先决条件,用来减少在未来改进安全措施时的风险。当分析被记录的事件时,应注意下列问题:

- 何时发生了何事。
- 职员是否已按计划行事。
- 职员们是否可及时使用需要的信息。
- 同类事件再发生时职员们应采取的动作。

对这些问题的回答将有助于理解和处理事件。

5

管理要求与人员安全



5.1 概 述

(1)信息安全的任务

信息安全的任务包括：

- 评估安全风险。
- 确定安全需求。
- 选择并实施安全控制措施。

(2)信息安全的内容

信息安全的内容包括：

- 制订安全策略。
- 建立安全机构。
- 对资产分类并进行控制。
- 人员安全。
- 物理和环境安全。
- 通信和操作。
- 访问控制。
- 系统开发和维护。
- 业务持续性管理。
- 遵从性检查。

(3)信息安全起始点

一些安全保护措施可作为实现信息安全的起始点。

(4)安全保护对象

从法律角度,对一个组织具有重大意义的安全保护对象包括：

- 知识产权。
- 组织的各类信息。
- 提供服务的数据和个人信息。

(5)控制措施

作为信息安全通用实施方法的控制措施包括：

- 信息安全策略文档。
- 信息安全责任划分与分配。
- 信息安全意识教育与培训。
- 安全事件汇报。
- 可持续运营管理。

(6) 保护成功的关键因素

经验表明,一个组织能否成功地实现信息安全,以下因素是至关重要的:

- 反映组织业务目标的安全目标、方针和策略。
- 与组织的文化相一致的实施安全的方法。
- 管理层明显的支持和承诺。
- 正确识别组织中需要保护的资源及其价值。
- 正确理解安全需求、风险评估和风险管理。
- 向所有的管理员和雇员灌输安全理念。
- 向所有的员工和签约方发布关于信息安全策略与标准的指南,以及解释本组织的信息安全策略与标准。
- 提供适当的培训和教育。
- 一个综合的、平衡的评估体系,用于评估信息安全管理性能以及反馈改进建议。

5.2 信息安全策略

管理者应该制订一套清晰的策略指导方针,并通过在组织内发布和维护信息安全策略,表明对信息安全的支持与承诺,达到为信息安全提供管理指导和支持的目的。

5.2.1 信息安全策略文档

信息安全策略文档应得到管理层批准,并以适当的方式发布、传达到所有员工。该文档应该陈述管理者的承诺,并阐明本组织管理信息安全的方法。信息安全策略至少应该包括以下几个部分:

- ① 定义信息安全总体目标、方针和策略,以及安全作为一种保障措施为实现信息共享所起的重要作用。
- ② 陈述管理层的决心、支持的信息安全目标和原则。
- ③ 对组织有重大安全意义的安全策略、原则、标准和遵从性要求做简要说明,例如遵从法规和合同的要求;安全教育的要求;对计算机病毒和其他恶意软件的防范和检测;业务持续性管理;违反安全策略的后果。
- ④ 定义信息安全管理的一般和具体责任,包括报告安全事件。
- ⑤ 与其他支持安全策略的文档的关系,例如,特定信息系统的更详细的安全策略和规程,或用户应该遵守的安全规则。

5.2.2 评审与评估

信息安全管理策略应有专人负责维护并按照既定的评审程序进行评审。此过程应确保任何可能影响风险评估的原始依据的变化,如重大的安全事件、新的脆弱性、组

织的基础结构或技术基础设施的变化都会得到相应的评审。同时,应对以下各项进行有计划的、定期的评审:

- ①策略的有效性,可通过记录在案的安全事件的性质、数量和所造成的影响来论证。
- ②对业务效率进行控制的成本和影响。
- ③技术变化所起的作用。

5.3 组织对安全的管理

应建立管理框架来启动和控制组织内实施的信息安全,达到在组织内对信息安全有效管理的目的。

5.3.1 信息安全管理的基础结构

应该建立适当的、具有管理权的信息安全管理委员会来批准信息安全策略,分配安全职责并协调组织内部信息安全的实施。如有必要,应在组织内建立信息安全咨询专家小组并使其发挥作用。应建立与外部信息安全专家的联系,以跟上行业发展趋势,跟踪安全标准和评估方法,并在处理安全事件时提供适当的联络渠道。另外,应鼓励多学科综合的信息安全方法,例如管理者、用户、行政人员、应用软件设计人员、审计人员和保安人员以及行业(如保险和风险管理领域)专家之间的协作。

(1) 信息安全管理委员会

信息安全管理委员会应该承担的典型职责主要有:

- 评审和批准信息安全策略和总体职责。
- 监视面临重大威胁时信息资产暴露所发生的重大变化。
- 评审和监视信息安全事件。
- 批准加强信息安全的重大行动。

应有一名信息安全管理员负责与安全有关的所有活动。

(2) 信息安全的协作问题

在较大的组织内部,有必要成立由各相关部门的管理代表组成的跨部门的信息安全协调委员会,以共同实施信息安全的控制措施。它的主要功能有:

- 协调组织内关于信息安全的各部门的具体分工和责任。
- 协调信息安全方面的具体方法和步骤,如风险评估、资产分类。
- 协调和支持全组织范围的信息安全行动,如安全意识培训活动计划。
- 确保信息安全问题是信息规划过程的一部分。
- 评估新系统或服务在信息安全控制方面的充分程度,并协调其实现过程。
- 评审信息安全事件。

- 提高全组织对信息安全的支持程度。

(3) 信息安全责任分配

应该明确定义保护各种资产和实施具体的安全措施过程的职责。

应该用信息安全策略来指导组织内部信息安全任务和责任的分配。必要时,应针对具体的地点、系统和服务对此策略做更详细的补充。清晰定义出各项有形资产和信息资产以及安全程序管理和使用方承担的责任。

在大多数组织中,应任命一名信息安全管理员来负责信息安全工作的开展和实施,并支持控制措施的标识工作。分配资源和实施控制措施的责任则一般由各部门管理者承担。通常的做法是为每项信息资产指定专人来负责日常的安全工作。

信息资产的负责人可以把安全职责委托相关部门的管理员或服务供应商。但是,信息资产负责人对资产的安全负有最终的责任,并应有权认定责任人是否恰当地履行了职责。

对各个管理者所负责的安全领域进行描述,特别应进行以下工作:

- 对和各个系统相关的各种资产和安全过程应给予标识和明确的定义。
- 各项资产或安全过程的管理者责任应经过审批,并以文件的形式详细记录。
- 授权级别应清晰定义并记录在案。

(4) 信息处理设施的授权程序

在对新的信息处理设施建立管理授权程序时,应考虑以下措施:

- 新设施应有适当的用户管理审批制度,对用户的使用目的和使用权限进行授权,同时应得到负责维护本地信息系统安全环境的管理者的批准,以确保符合所有相关的安全策略和要求。

- 如有必要,应检查硬件和软件,以确保与其他的系统部件兼容(注:对于有些连接,履行审批手续也是必需的)。

- 使用个人信息处理设施处理业务信息,以及部署必要的控制措施时都应获得授权。

- 在工作场所使用个人信息处理设施可能导致新的脆弱性,因此应经过评估和授权。

上述控制措施在联网的环境中尤为重要。

(5) 信息安全专家意见

许多组织可能需要信息安全专家的意见,这最好由组织内富有经验的信息安全顾问来提供。建议组织或单位专门指定一个人来协调组织中对信息安全的认识和实践以尽量达成共识,并帮助做出安全决策。同时他们还应与组织外部合适的安全顾问保持联系,以获得自身经验之外的专家建议。

信息安全顾问或类似的联络人员的任务是使用他们自己的和外部的建议,为信息

安全的所有方面提供咨询。他们对安全威胁的评估质量和对控制措施的建议水平决定了组织的信息安全的有效性。为使安全建议最大限度地发挥作用,他们应有权接触组织管理层的各方面。

若怀疑信息系统出现安全事件或破坏,应尽早地咨询信息安全顾问或相应的外部专家,以获得专业性指导,并对资源进行调查。尽管多数的内部安全调查通常是在管理层的控制下进行的,但仍可以邀请安全顾问给出建议,以加强领导或指导调查。

(6)组织间的合作

组织应和执法机关、管理机构、信息服务提供机构以及电信营运部门保持适当的联系。同样也应积极参与信息安全组织和行业论坛的活动。

信息安全管理信息的交换应该加以限制,以确保组织的秘密信息不会泄漏到未经授权的人员手中。

(7)信息安全的独立审计

审计工作应该独立进行,并具有可行性和有效性,以确保组织的做法能够客观地反映安全策略。

审计工作应由组织内部的审计职能部门、独立经理人或精通此种审计工作的第三方机构来实施,这些信息安全的审计人员具有相应的技能和经验。

5.3.2 第三方访问的安全问题

应该控制第三方对组织内部的信息处理设施的访问,以确保第三方访问本组织的信息处理设施时信息资产的安全性。

若业务上需要第三方的访问,应对此做出风险评估以便确定访问可能带来的安全后果和对访问进行的控制需求,控制措施应经双方同意,并在合同中进行明确定义。

第三方访问可能涉及与第三方有关的其他参与者,授予第三方访问权的合同应该涵盖允许的其他的合法参与者的名称以及他们的访问条件等内容。

在考虑信息的外包处理时,第三方访问的安全管理可以作为签订此类合同的必要条款。

(1)识别第三方访问的风险

需要考虑的访问和资源类型有:

- 物理访问,如访问办公室、计算机房、文件柜等。
- 逻辑访问,如访问组织的数据库、信息系统等。

在业务上有与第三方接触的需求时,需进行风险评估,以确定具体的控制措施的需求。还要考虑访问类型、信息的价值、第三方访问的控制措施和访问给组织信息的安全可能带来的后果。

按照合同规定可以在现场滞留一段时间的第三方,也有可能带来安全隐患。

(2)与第三方签约时的安全要求

涉及第三方访问本组织信息处理设备时应签订正式的合同,该合同应包括或涉及安全要求,以保证遵守本组织的安全策略和安全标准。合同应确保本组织和第三方之间没有理解上的分歧。组织应确保供应商的可信性和可靠性。合同中应该考虑如下条款:

- 信息安全的总体策略。
- 资产保护方面,包括保护组织资产(包括信息和软件在内)的过程、确定资产是否受到危害(如数据的丢失和篡改等)的确认方法、确保在合同截止时或合同执行期间的某一个双方同意的时间,以及归还或销毁信息的控制措施、完整性和可用性、对复制和泄漏信息的限制。
- 对每一可用服务的描述。
- 服务的等级和服务的不可接受等级。
- 人员调整的规定。
- 协约方各自的责任。
- 法律方面的责任,如数据保护法规,当合同涉及其他国家的组织,还应考虑不同国家法律体系的区别。
- 知识产权和版权转让以及合作成果保护。
- 访问控制协议,包括所允许的控制方法,对独特的标识符如用户 ID、口令等的控制和使用;用户访问和权限的授予过程;要求有一份名单记录被授权使用可用服务的用户,以及他们的使用权限。
- 可验证的性能的定义、监视和汇报。
- 监视和撤销用户行为的权力。
- 审计合同责任,或是委任第三方来执行审计的权力。
- 建立解决问题的流程,在适当情况下,还要考虑应急安排。
- 软件、硬件安装和维护责任。
- 清晰的报告结构和双方认同的报告形式。
- 详细、清晰的变更管理的流程。
- 确保控制措施得以实施所需的物理保护控制和机制。
- 对用户和管理者在方法、流程和安全方面的培训。
- 确保防范恶意软件的控制措施。
- 报告、通知和调查安全事件和安全损失的安排。
- 第三方和连带承包商的牵连问题。

5.3.3 委外管理

当把信息处理的责任委托给其他组织时,要确保委外信息的安全性。

委外安排时,应该在签订的合同中表明信息系统、网络/桌面环境方面的风险、安

全控制和流程。

如果组织将其全部或部分信息系统、网络或桌面环境的管理和控制任务委托给其他组织,委外的安全要求应在合同中加以规定并要征得双方同意。

5.4 人员安全

5.4.1 岗位定义和资源分配的安全

应该在新员工聘用阶段就提出安全责任问题并将其包括在聘用合同条款中,在员工的雇佣期间进行培训和监督,从而降低人为错误的风险,如盗窃、诈骗或滥用设备或信息。

可能时应该对新员工进行充分的筛选,尤其是对从事敏感工作的员工;所有雇员以及信息处理设施的第三方用户(例如产品供应商、信息安全咨询服务商和工程队伍等)都应该签署保密协议。

(1) 岗位责任中的安全

对安全角色和责任形成文件。这些角色和责任既应该包括实现或保持安全策略的一般责任,又应该包括保护特定资产或执行特定安全过程或活动的具体责任。

(2) 人员选拔及方针

对长期雇佣员工的考核检查应该在招聘时进行。这应该包括以下措施:

- 审查能力、人品推荐材料。
- 检查应聘者所学课程简表。
- 对应聘者声称的学术或专业资格的确认。
- 个人身份检查(护照或类似证件)。

无论是员工的初次任命还是提升,当该员工具有访问信息处理设备的机会,特别是这些设备处理敏感信息,如财务信息或高度机密的信息时,组织应该附加信用度审查。对于处在有相当权力位置的人员,这种审查应该定期重复进行。

对于承包方和临时员工应该执行类似的筛选程序。若这些人员是由代理机构推荐的,则在与代理机构签订的合同中应该明确规定该代理机构的推荐责任;如果代理机构没有完成筛选工作或者组织对筛选结果怀疑或不满意,必须补充筛选或中止推荐的沟通过程。

管理层应该对有权访问敏感系统的新员工和缺乏经验的在岗员工的监督工作进行评价,每一名员工的工作都应该定期经过一个更高层职员的监督和指导。

管理者应该意识到员工的个人环境可以影响他们的工作。个人或收入问题、行为或生活方式的改变、重复的缺勤以及压力或抑郁等可能导致员工欺诈、偷窃、错误或其他安全隐患,应该据此充分考虑这类员工接触的信息的保护问题。

(3) 保密协议

保密或不泄密协议用于向协议双方告知信息是机密的或秘密的,以及为保守秘密必须遵守的行为规范和应承担的义务。雇员通常应该签署此类协议作为他们受雇的先决条件。

应该要求临时员工和第三方用户在被授予信息处理设备访问权之前签署保密协议。

在雇佣条款或合同条款发生变化时,特别是员工要离开组织或合同到期时,应该对保密协议的执行情况进行评审。

(4) 雇佣期限和条件

雇佣期限和条件应该阐明雇员对信息安全的责任。必要时,在雇佣结束后,这些责任应该延续一定的时间,包括如果雇员无视安全要求时必须承担的责任。

雇员的法律责任和权利,如涉及版权法或数据保护法,应该阐明并将其包括在雇佣条款和条件中,还应该包括对雇主数据分类和管理的责任,在合同需要的地方,雇佣期限和条件应该说明这些责任应延伸到组织范围以外和正常工作时间以外,例如在家里工作时。

5.4.2 用户培训

应对用户进行安全管理规程和正确使用信息处理设备的培训,以尽量降低可能的安全风险,确保用户意识到对信息安全的威胁和危害关系,并具有在日常工作过程中支持安全策略的能力。

组织中所有员工以及相关的第三方用户,应该接受适当的信息安全教育和培训,以适应组织的策略和管理规程的变化。这包括安全要求、法律责任和业务控制措施,还包括在被授权访问信息或服务之前正确使用信息处理设备的培训,如登录程序、软件包使用。

(1) 培训模型

培训模型如图 5.1 所示。

(2) 安全意识教育和培训

安全意识教育与培训是员工培训教育中的重要组成部分,这种教育与培训将改变个人和组织对安全的认识 and 态度,使他们认识到安全的重要性和安全失败所导致的不良后果。安全意识教育与培训这一过程对所有雇员都是必需的。

信息安全意识教育与培训必须考虑到人们的接受能力,循序渐进,逐步强化。如果只考虑刺激方式,起初能够引起人们的注意,但重复使用,学习者就会有选择性地忽略某些刺激。因此,意识培养必须是不断发展的、具有创造性的和有新意的,以吸引学习者的注意力,将那些条款式的规范和操作行为变为潜意识或习惯性行为。这一过程

称为同化。通过该过程,把新的经验融合在个人的习惯模式中。

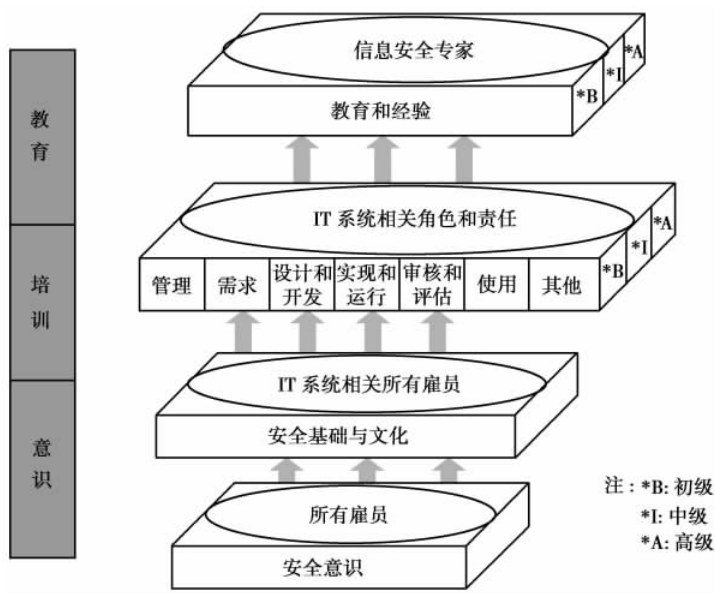


图 5.1 培训模型

总之,安全意识是要雇员建立对计算机系统脆弱性和威胁的敏感性,以及认识到需要保护数据、信息和对它们进行处理的方法。信息安全意识计划的基本价值是使人们通过改变组织文化的态度为培训准备条件。因为安全失败对每个人都会造成潜在的不利后果。因此,信息安全是每个人的工作。

培训的目的是使受训者获得相关的和所需的安全技能,这也是信息安全之外的功能性专业(例如,管理,系统设计和开发、部署、审计等)的从业者所必备的能力。

教育则将所有安全技能和各种功能性专业的能力整合成为一个公共的知识体系,通过多学科的概念、问题和原则(技术上的和社会性的)等的学习和互相渗透、融合,努力培养出具有远见的信息技术安全专家和专业人才。

(3) 在职安全教育

所有在职在岗的各个层次的员工应针对实际工作需要,不断地接受管理、技术和安全意识方面的培训教育。

有关培训和教育的知识要点参见附录 2 “信息安全应知应会培训参考材料”。

5.4.3 对安全事件和故障的响应

影响安全的事件应该尽快通过适当的管理渠道报告给有关人员和机构,尽量减少安全事件和故障造成的损失,监视此类事件并吸取教训。

应使所有雇员和签约人知道可能影响组织资产安全的不同种类事件的各种报告

程序。应该要求他们以最快的速度把看到的或怀疑的事件报告给指定的联络人。组织应该建立正式的惩罚条款以处理破坏安全的员工。为妥当地处理事件,有必要在事件发生后尽快收集证据。

(1) 报告安全事件

安全事件应该尽快通过适当的管理渠道报告给有关人员。

应该建立正式的报告程序,同时建立事件响应程序,阐明接到事件报告后应采取的行动。应该使所有员工和签约方知道报告安全事件的程序,并应该要求他们按要求报告此类事件。应该在事件被处理结束后,执行适当的反馈程序,以确保对事件报告的响应。

(2) 报告安全脆弱点

应该要求提供信息服务的用户记录并报告任何察觉的或怀疑的系统或服务的安全脆弱点或对它们的威胁预测,用户应该尽快把这些问题向管理层或直接向服务供应商反映。应该告知用户,在任何情况下,他们都不应该擅自对一个被察觉和怀疑的弱点进行验证,这是为了保护他们自己,因为测试脆弱点可能被认为是滥用系统或可能对系统造成致命损害。

(3) 报告软件故障

建立报告软件故障的规程,应该考虑以下步骤:

- 记录故障问题的征兆和显示在屏幕上的信息。
- 如果可能,计算机应被隔离,并停止对其使用,应该立即对与使用软件有关的行为产生警觉,如果需要检测设备,应在重新启用前将其与组织的所有网络断开,存储在软盘或硬盘上的信息不应该传送给其他计算机。
- 该事件应该立即报告给信息安全管理者。

除非被授权,用户不应该试图删除可疑的软件,应该由经过适当培训并有经验的员工在授权状态下执行修复或恢复工作。

(4) 从事件中学习

应该有适当的机制使事件和故障的种类、数量和损失被量化并受到监控。这类信息可用于识别事件是初次发生还是再发生,是偶然发生还是条件性发生,是有重大影响的事件还是故障。

(5) 惩罚程序

对违反组织安全策略和规程的雇员应该有正式的惩罚程序。这样一个程序对可能无视安全策略的雇员能够起到威慑作用。另外,应该保证正确、公正地处理被怀疑严重或连续破坏安全的雇员。

5.5 符合性要求

5.5.1 符合法律要求

对信息系统的设计、操作、使用和管理需要符合法律、法规和合同的有关要求,避免触犯任何刑事、民事法律、法规或违反合同约定的责任。

1) 识别可适用的法律

与一个信息系统相关的法律、法规和合同的要求应该进行明确界定并予以文档化。为满足这些要求而采取的具体的控制措施和个人责任也应该进行类似的界定并予以文档化。

2) 知识产权

(1) 版权

在使用与知识产权如版权、设计权、商标权相关的资料时,应确保符合法律规定。侵犯版权的行为可能导致民事甚至刑事诉讼。

法律、法规和合同的要求可能对私有资料的复制进行了限制。在某些情况下,法律、法规可能规定只有组织自己开发的,或者取得了许可证的开发者提供给组织的资料,才能使用。

(2) 专利权

专利软件产品通常在许可协议下使用,将产品的使用限制在特定的计算机上,并且要求复制只能用于备份。应当考虑下面的控制措施:

- 发布一个遵守软件版权的政策,保证软件和信息产品的合法使用。
- 制订获得正版软件产品的流程。
- 提高保护软件版权和获取策略的认识,提请注意:如果违反规定将受到惩罚。
- 保有对拥有软件许可权、母盘和手册等权利的证据。
- 对任何产品使用者的数量不得超过限制。
- 确保只有授权的软件和取得许可证的产品才能安装。
- 制订维护许可证环境的策略。
- 制订处理和传递软件给他人的策略方针。
- 遵守从公共网络取得软件 and 信息的条款和条件。

3) 保护组织记录

组织的重要记录应该保护以防止丢失、毁坏和篡改。像支持基本的业务活动一

样,记录的信息也需要得到安全保管。典型的例子是一些被作为证据的记录,可用于证明组织的运营是遵守法律法规的,或者在发生民事、刑事诉讼时呈堂供证,或者供股东、合作伙伴和审计人员确认组织的经营状况。记录信息的保存时间符合国家法律法规规定。

记录应该被划分为不同种类,如财务记录、数据库记录、交易日志、审计日志和操作规程等。每一种记录都应详细规定保存期限和存储介质的种类,如纸、缩微胶片、磁介质、光介质。任何与加密或数字签名相关的密钥应该安全的保存并在需要时对经授权的人可以利用。

应考虑用于存储记录的介质的变质问题。

一旦选定数据存储介质,处理规程应确保在整个保存期间对数据具有访问能力(存储介质和存储格式的可读性),防止由于技术变化造成数据不可读。

选择的数据存储系统,应保证存储的数据能够以一种法庭可接受的方式进行检索。

数据存储和处理系统应该明确标志记录的类型和内容,以及法律法规所要求的保存期限。在保存期届满后,如果组织不需要这些记录,应该恰当地销毁这些数据。

为了履行这些责任,下面的步骤应该在组织内采用:

- 公布保留、存储、处理和处置记录与信息的指导原则。
- 确认重要的记录数据种类和它们应该保存的时间。
- 维护关键信息资源的存储介质。
- 实施恰当的控制措施保护重要的记录数据和信息,防止丢失、损坏和篡改。

4) 数据保护和个人信息隐私

国家制定法律对个人数据的处理和传送进行保护。这类保护措施可能对收集、处理和传播个人信息设置限制,并且对将个人信息从一个国家传递到另一个国家设置限制。

遵守数据保护法需要适当的管理机构和控制。通常,最好的做法是任命一个数据保护专员,针对管理者、使用者和服务供应商的个人责任和应该遵守的特定流程提供指导。为了维护个人数据,并且确保受到相关法律的保护,信息所有者有责任将相关注意事项告诉数据保护专员。

5) 防止滥用信息处理设备

组织的信息处理设备是为了实现业务目标而提供的。管理层应该对信息处理设备的使用进行授权。在没有得到管理层的同意时,任何出于非业务或非经授权目的的使用,都应该被视为不适当地使用设备。如果这类活动通过监控或者其他途径被确认,应该引起管理者的注意,并考虑对此进行适当的惩罚。

使用监控措施的合法性因国家法律规定而有所区别,并且可能要求事先通知职员或者得到他们的同意。在实施监控措施前,应该听取法律建议。

许多国家已经制定出或者正在制定防止计算机或信息处理设备被滥用的法律。出于未经授权的目的使用计算机有可能成为犯罪行为。使所有的用户意识到他们允许访问的范围是基本的安全要求。应该告诉组织的职员以及第三方用户,除非经过授权,否则一切访问都是禁止的。

应该在计算机屏幕上显示登录警告信息,指出将进入的系统是需要授权的,否则是不允许访问的。用户必须确认屏幕上的信息并做出恰当地表明已获授权的响应才能继续该登录过程。

6) 加密控制规则

国家应该通过法律、规章或其他措施控制使用加密设施。这类控制包括:

- 实现加密功能的硬件和软件的进口/出口许可制度。
- 按设计增加了加密功能的软件和硬件的进口/出口许可制度。
- 对由于提供内容机密性需要而使用硬件或软件加密的信息,国家要求依法实现强制性或自由决定的访问方法。

应该寻求法律建议来确保遵守国家法律。在加密信息和加密设施转移到另一个国家之前,同样应该符合出入国的法律限制。

7) 证据收集

(1) 证据规则

收集证据对一个人或组织的行为的性质判定是必要的。如果这种行为是一个内部惩罚事件,所需证据的充分性将通过内部程序描述。

一旦一个人或组织的行为涉及法律,无论是民法或刑法,所提供的证据应该符合相关法律或者该案件受理法院规定的规则。一般来讲,这些规则包括:

- 证据的可信性,即能否在法庭上使用。
- 证据的证明力,即证据的质量和完备性。
- 适当的证据,证明在该待恢复的证据被系统存储和处理期间正确和一致地执行了。

(2) 证据的可信性

为了保证证据的可信性,组织应该确保用于采集证据的产品是遵从已公布的采信证据产品的标准或操作规范的。

(3) 证据的质量和完备性

为了保证证据的质量和完备性,需要严格的证据跟踪。一般来讲,这种跟踪的严

格性在下面的条件下成立：

- 对于纸质文档来说,原始版本文档应该被安全保管并且记录证据发现者、发现的地点、发现的时间,以及证据发现过程的见证人,所有的调查都应该确保原始版本文档没有被篡改。

- 对于存储于计算机介质上的信息来说,应该将任何可移动介质,例如硬盘上的或者存储器中的信息进行复制以确保其可用性,在复制过程中的所有活动的日志应该保存并且此过程应该能证明,介质的复制以及该日志应安全保管。

在一个事件的证据刚发现时,并不一定表明是否将有诉讼活动。因此,在意识到事件的严重性之前,存在着必要证据被意外毁坏的危险。建议让律师和警察介入任何可能的法律程序活动并且对所需的证据有效性提供建议。

5.5.2 符合安全策略和技术标准

信息系统的安全性应该定期检查,确保系统符合组织的安全策略和技术标准。

这些检查的执行应该符合安全策略,并且对技术平台和信息系统的检查应该依从安全实施的标准。

(1)符合安全策略

管理者应该确保在他们责任领域内的所有安全规程得到正确实施。另外,组织内的所有领域应该进行定期检查以确保符合安全策略和技术标准。检查对象包括：

- 信息系统。
- 系统供应商。
- 信息和信息资产的所有人。
- 用户。
- 管理人员。

信息系统的所有人员都应该支持经常性的检查,目的在于确定系统是否符合适当的安全策略、技术标准和有关的安全需求。

(2)技术标准符合性审查

应定期地检查信息系统是否符合安全实施标准。技术标准符合性检查涉及对操作系统的检验,以确保正确地实施软件和硬件控制。这种类型的符合性检查要求有专家的技术支持。检查工作应由有经验的系统工程师手工进行;如果必要的话,可采用适当的软件工具支持,这些软件可以生成由技术专家事后进行解释的技术报告。

符合性检查还包括诸如渗透测试等,此种测试可以邀请专家独立进行。符合性检查对于发现系统的脆弱性和检查控制措施的有效性是很有用的。检查程序应该小心演练,以免渗透测试危害到系统的安全性或意外地引起其他的脆弱点。

任何技术标准符合性检查都只能由有能力的、业经授权的专业人员进行。

5.5.3 系统审计方面的考虑

在系统审计时,应采取控制措施保护操作系统和审计工具,目的是减少对系统审计过程的干扰。

为保护审计工具的完整性和防止对其误用,需要适当的安全措施。

(1)对系统审计进行控制

应该仔细规划和协商审计需求以及涉及在操作系统上检查的活动,尽量减小中断业务流程的风险。为此应该遵守以下各项:

- 审计需求应得到适当的管理层的同意。
- 审计的范围应得到控制。
- 审计工作一般应局限于对软件和数据只读的访问。
- 必要的地方允许对系统文件进行隔离复制,复制件在审查工作完成之后应该删除或销毁。
- 对执行审计所需的信息系统资源应该进行明确的标识并保持其可用性。
- 审查过程中的特殊的或额外的处理需求应进行标识和经过同意。
- 应监督和记录所有的访问活动,以生成跟踪信息。
- 审计所涉及的流程、需求和责任都应文档化。

(2)对系统审计工具的保护

对系统审计工具的访问,如软件或数据文件,都应给予控制以防止任何可能的误用和危害。这些工具应与开发工具和操作系统隔离保管,不应保留在磁带库或用户区内,否则应给予适当等级的附加保护。

6

资产分类与物理安全管理



6.1 资产分类与管理

6.1.1 资产分类与责任落实

应该对所有重要的信息资产予以识别并指定负责人。资产责任有助于维持对组织资产的适当保护。

应该为所有重要资产指定负责人,并分配其保持适当控制措施的责任。实施控制措施的职责应由指定的资产所有人或管理者承担,也可以委托人承担。

应该编制并保持与每一个信息系统相关的重要资产的清单。编制资产清单的过程是风险评估的基础和依据。应该清晰地识别每项资产、资产拥有权、经同意和记录为文件的安全等级,以及资产现在的位置(当试图从丢失和损坏状态恢复时可以用到这一状态参数)。

与信息系统相关的资产包括:

- 信息资产,包括数据库和数据文档、系统文件、用户手册、培训资料、操作和支持程序、持续性计划、备用系统安排以及供访问的信息等。
- 软件资产,包括应用软件、系统软件、开发工具和实用程序等。
- 有形资产,包括计算机设备(处理器、监视器、笔记本电脑、移动存储器、调制解调器),通信设备(路由器、数字程控交换机、传真机、应答机),磁介质(磁盘和软盘),其他设备(电源、空调设备等),家具和住所等。
- 无形资产,包括计算和通信服务、服务能力、版权、品牌和形象等。

6.1.2 信息分类与标记

信息有不同程度的敏感性和重要性,一些信息可能需要额外级别的保护和特殊处理。应该对信息进行分类以指明保护要求、优先级顺序和保护等级,确保信息资产受到适当级别的保护。

应该根据信息价值和信息的安全属性遭损坏后的影响程度来定义适当的保护等级,并考虑特殊信息处理设施对安全的要求。

(1) 分类准则

信息分类和相应的保护控制措施应该考虑共享或限制信息的业务要求,以及与这些要求相关的业务影响,如对信息未经授权的访问或损坏可能造成的后果。

分类原则应该预见并顾及到这样一个事实,即任何特定信息的分类都不是一成不变的,而是可以根据某些预定的方针进行修改。

应该考虑分类的数量及其所带来的益处。

(2)信息的标记和处理

根据所采用的分类方案,为信息的标记和处理定义合适的规程。这些规程必须覆盖以物理或电子形式存在的信息资产。对每一信息类别,均应定义处理规程,包含下列信息处理活动:

- 信息的复制。
- 信息的存储。
- 以普通邮件、传真和电子邮件传递信息。
- 以口头方式传送信息(如移动电话、语音邮件、答录机)。
- 销毁。

敏感或重要的信息应该采用适当的分类标记,该标记应该反映分类准则。标记的项目包括打印报告、屏幕显示、记录信息的介质(磁带、磁盘、光碟、盒式磁带),以及信息的敏感度级别、信息宿主、共享范围等的定义。

6.2 物理和环境安全

6.2.1 安全区域

关键或敏感的业务信息处理设备应该放置在安全区域,有规定的安全防护带、适当的安全屏蔽和入口控制保护,这些设备应该受到物理保护,防止未授权的访问、破坏和干扰。

所提供的保护应该与识别出的风险相当。建议采用清空桌面和清除屏幕显示的策略以降低对文件、介质和信息处理设备的未经授权的访问或破坏的风险。

(1)物理安全防护带

物理保护可以通过在业务场所和信息处理设备周围设置若干屏障,使用安全防护带来保护放置信息处理设备的区域。每个屏障形成一个安全防护带,每个防护带都能增强整体防护。安全防护带是构成屏障的某些东西,如墙、卡控门或有人值守的接待台等。每个屏障的位置和强度依评估出的风险而定。

应该考虑下述原则和控制措施:

- 应该明确规定安全防护带的边界、构成形式。
- 放置信息处理设备的建筑物或场所的防护带在物理上应该是固定的(例如,在防护带或安全区域不应该有能够轻易闯入的缺口),场所的外墙应该是坚固的建筑物,所有的外门应该受到适当的保护,防止未经授权的访问。这些防护设施应置有控制机制、栅栏、警铃、锁等。
- 应该设置有人值守的接待区或其他隔离控制方法对场所或建筑物实施访问的物理控制,对场所和建筑物的访问应该仅限于被授权的人员。

- 如有必要,物理屏障应从地板延伸到天花板,以防止未经授权的访问和因诸如火灾和水灾引起的环境污染。
- 安全防护带的所有防火门应具备报警功能。

(2)物理进入控制措施

安全区应该通过适当的进入控制措施保护,以确保只有经授权的人员能够进入。应考虑以下的控制措施:

- 对安全区的访问者应该被监视或经批准,同时记录他们进入和离开的日期和时间。他们应该仅被允许访问指定的、经授权的场所和目标,并发给他们关于安全区域要求和应急程序的说明。
- 对敏感信息和信息处理设备的访问应受到控制并仅限于获得授权者。鉴别控制措施,如带个人身份标识的扫描卡,对所有访问进行身份鉴别和授权。应该对所有访问的审计日志进行安全保护。
- 应该要求所有员工配戴某种明显的身份标志,并鼓励员工对没有陪伴的陌生人和没有配戴明显身份标志的人进行盘问。
- 对安全区的访问权应该定期评审并更新。

(3)保护办公室、计算机房和设备的安全

安全区可能是上锁的办公室或物理安全防护带中的若干房间,这些房间可能存放有上了锁的柜子和保险箱。安全区的选择和设计应该考虑在火灾、水灾、爆炸、暴乱和其他形式的自然或人为灾害发生时的应对措施和疏散通道,遵从相关的卫生、安全法规和标准,以及应对来自相邻场所的安全威胁,如来自其他区域的水泄漏或火蔓延。

应该考虑以下控制措施:

- 关键设备的放置场所应该避免被公众访问。
- 建筑物不要过分显眼,并尽可能少地对外公布其用途,建筑物内外不放置可表明存在信息处理活动的明显标志。
- 辅助功能和设备,如影印机、传真机应该妥当地放置在安全区,以避免可能危害信息安全的访问。
- 房间在无人看管时门窗应该关闭上锁,必要的地方应该考虑对窗户,特别是地面层窗户的外部保护或掩护。
- 应该在所有的外门和可以出入的窗户按专业标准安装防盗系统并定期测试,无人区应该时刻保持警戒状态。
- 由组织管理的信息处理设备应该和第三方管理的信息处理设备加以物理隔离。
- 显示敏感信息处理设备位置的目录和内部电话本不应被公众获取。
- 危险或易燃物品应该保存在与安全区有安全距离的地方,大宗消耗材料如文具等一般不必存放在安全区内。
- 备用设备和备份介质的放置应该与原设备和介质保持安全距离,以避免因灾害

蔓延造成毁坏。

(4) 在安全区内工作

对在安全区内工作的员工和第三方人员以及发生在安全区的第三方活动,需要额外的控制措施和指导原则来加强安全区域的安全性。应该考虑以下控制措施:

- 员工只有在有必要的时候才应该知道安全区的存在或其内的活动。
- 在安全区内应该避免无人值守的活动。
- 空闲的安全区应该关门上锁并定期检查。
- 第三方服务支持人员只有在必要时才应该被允许有限制地访问安全区或敏感信息处理设备,这种访问应该经过授权并接受监督。在安全防护带内具有不同安全要求的区域之间需要设置控制访问的额外屏障和防护带。
- 只有经授权,才允许使用照相、录像、录音或其他记录设备。

(5) 隔离交接区

交接区应予以控制,必要时,与信息处理设备隔离,以避免未经授权的访问。此类区域的安全要求应该由评估出的风险决定,可考虑以下控制措施:

- 从建筑物外对接货区的访问应限于经确认和授权的人。
- 应将接货区设计成送货员能够卸货但却无法访问建筑物安全防护区。
- 当接待区的内门打开时,外门应该是安全的。
- 进入的物品在从接货区转移到使用地点之前应该接受检查,以防止潜在的危險。
- 如有必要,进入的物品应在入口处登记。

6.2.2 设备安全

应该在物理上保护设备免受安全威胁和环境危害,并考虑设备的放置和布局,以降低对数据未经授权访问的风险以及防止丢失或损坏。

(1) 设备放置和保护

合理放置或保护设备应该考虑以下控制措施:

- 放置设备的工作区应避免不必要的参观访问。
- 敏感数据的信息处理和存储设备应该妥善放置。
- 需要特殊保护的设备或物品应隔离放置,以降低总体保护等级。
- 尽量规避潜在威胁的风险,包括偷窃、火灾、爆炸、烟雾、用水(或供水)故障、灰尘、震动、化学反应、电源干扰、电磁辐射。
- 禁止在信息处理设备附近饮食和吸烟等行为。
- 对于可能对信息管理设备的运行有负面影响的环境条件应该进行监控。
- 考虑在工业环境下设备的特殊保护方法(如加键盘保护膜等)。

- 考虑发生在临近区域的灾害的影响,如临近建筑物着火、天花板漏水、低于地平面的地面渗水或临街爆炸。

(2) 供电设施安全

应该保护供电设施以防电源中断和其他与电有关的异常情况,根据设备制造商的说明提供合适的电力。

实现不间断供电的可选措施包括:

- 多条线路供电。
- 配备不间断电源(UPS)。
- 配备备用发电机。
- 配备电源净化装置。

在支持关键业务运行的设备上,推荐使用不间断电源(UPS),以保证设备的正常关机或持续运转。UPS 设备应该定期检查,以确保其有足够的电量,并按照制造商的建议进行测试。还应该包括在 UPS 失效时所采取的应急行动。

在长时间停电的环境中,应该考虑备用发电机。发电机应该按照制造商的说明定期测试,并保证有足够的燃料供应,以确保发电机能长时间的工作。

另外,紧急电源开关应位于设备室的紧急出口附近,以便在紧急情况下迅速切断电源。在电源发生故障时,应该提供应急照明。应该对所有建筑物采用雷电防护,并在所有外部通信线路上安装雷电防护过滤器。

(3) 电缆安全

应该保护传送数据或支持信息服务的电源和通信电缆,防止窃听或损坏。应该考虑以下控制措施:

- 如有可能,接入信息处理设备的电源和通信线路应该铺设在地下管网内,或者采取其他安全保护措施避免暴露。
- 应该保护通信电缆以防止搭线窃听或破坏,例如,通过使用电缆屏蔽管道和避免电缆通过公共区域。
- 电力电缆应该与通信电缆隔离,并保持安全距离,以防干扰。
- 对于敏感或关键系统,需要考虑附加的控制措施包括在监控点和端点处安装坚固的管道以及给房间或柜子上锁、使用可替换的路由选择或传输介质、使用光纤电缆、扫描监视未经授权而连接在电缆上的设备。

(4) 设备维护

正确地维护设备以确保其持续的可用性和完整性,应该考虑以下控制措施:

- 设备应该按照供应商推荐的服务周期和规定进行维护。
- 只有经授权的维护人员才能修理和保养设备。
- 应该对所有可疑的和确认的故障以及所有预防和纠正措施进行完整记录。

- 在将设备送到组织外维护时,应选择定点授权单位,并采取适当的控制措施。

(5) 场所外设备的安全

信息处理的设备运行在组织场所外必须经管理层授权批准。考虑到设备在组织外运行的风险,所提供的保护应该等同于组织内相同用途的设备。应该考虑以下指导原则:

- 从组织带出的设备和介质不应留在无可靠人员看管的公共场所,旅行途中移动设备应该随身携带并加以适当掩饰。
- 应该始终遵守生产商对设备保护的规定,如设备不暴露于强电磁场等。
- 对用于家庭工作的设备的控制应该通过风险评估,并采取合适的措施,如文件柜上锁、清空桌面以及控制对计算机的访问等。

损坏、被盗和窃听的安全风险在不同地点差别很大,应该考虑适合不同环境的恰当的控制措施。

(6) 设备的安全处置或再启用

草率地处置或再启用设备可能泄漏信息。存储敏感信息的存储设备应该从物理上销毁或安全地重写,而不是使用一般的删除功能。

带存储介质(如固定硬盘)的所有信息处理设备处置前应该仔细检查,以确保任何敏感数据和授权软件在处置前已被清除或重写。被损坏的存有敏感数据的存储设备,需要经过风险评估后决定其是否应该销毁、修理或丢弃。

6.2.3 日常性控制措施

日常性的控制措施应该到位,以尽量减少所保护信息和信息处理设备损失或损坏。

(1) 清空桌面和清屏

组织应考虑对文件及便携式的存储介质采取桌面清空策略,防止遗留在桌面;对信息处理设备采取清屏策略,以降低在正常工作时间以外信息未经授权的访问、丢失和损坏的风险。此策略应考虑信息安全等级、相应的风险和组织文化方面等因素。

留在桌面上的信息存储介质也有可能被诸如火灾、水灾或爆炸等灾害损坏或销毁。

日常性控制措施有:

- 适当情况下,文件和计算机介质处在不同状态时,特别是在工作时间外,应存放在适当的上锁柜子/其他形式的安全设备中。
- 敏感或关键业务信息,在不使用时,尤其是办公室无人看管时应妥善存放(最好存放在防火保险柜或密码文件柜中)。
- 个人计算机、计算机终端和打印机,在无人看管时不应处于登录状态,不用时应

采用锁键盘或其他的控制措施加以保护。

- 收发信件的场所、无人看管的传真机和电传机应该加以保护和监视。
- 下班后应将复印机上锁(或者以其他方式防止未经授权的使用)。
- 敏感或机密信息打印完后,应该立即从打印机存储区中将其清除。

(2)资产的搬移

设备、信息或软件未经授权不应带离原场所;有必要带离时,设备应先行注销并在带回时再注册。应建立抽查制度,以检查财产的非经授权移动。

7

运行安全管理



7.1 网络安全管理

7.1.1 概 述

本部分描述的是一个过程,这个过程是识别和分析与通信相关的、建立网络安全需求必须考虑的因素,为可能的安全措施提供指南。本部分为在网络和通信方面对信息安全管理负责的人提供指导原则,支持与通信相关因素的识别和分析。这些因素在确立网络安全需求中是必须考虑的。

7.1.2 任 务

为了识别与网络相关的安全需求和安全措施,需要完成以下任务:

- ①根据组织的信息系统安全策略,评审网络连接的一般安全需求。
- ②评审与网络连接相关的网络体系结构和应用,以便提供必要的背景知识来指导后续的子任务。
- ③识别应该考虑的网络连接类型。
- ④评审联网特性以及与之关联的信任关系。
- ⑤在可能从风险分析和管理的评审结果中得到帮助的地方,确定相关的安全风险类型,包括对通过连接进行传送的信息的业务价值,以及通过这些连接以非授权的方式可访问的其他信息。
- ⑥在网络连接的基础上,识别出安全风险类型、安全需求和合适的安全措施等。
- ⑦建立文档并复核安全体系结构的备选方案。
- ⑧使用识别出来的安全措施的参考标准以及取得共识的安全体系结构等,为详细的安全措施选择、设计、实施和维护而分配任务。

图 7.1 解释了这样一个全过程,它识别和分析了与通信相关的确定网络安全需求必须考虑的因素,并且提供关于潜在的安全措施区域的标示。

需要指出的是,在图 7.1 中,实线代表过程的主要步骤,虚线代表这些地方需要确定安全风险的类型,可以通过安全风险分析和管理的评审结果帮助解决。

此外,在图 7.1 所示过程中,某些步骤特别是“评审组织的信息安全策略”和“评审网络体系结构和应用”,需要再次调查前面步骤的结果以保证一致性。例如:

- ①在确定安全风险的类型后,也许需要评审组织的信息安全策略;因为有些事很可能会发生了但却没有包括在那个策略的层次结构中。
- ②在识别可能的安全措施区域时,应该考虑组织的信息安全策略,例如,该策略可能规定,不管风险如何,某个特殊的安全措施必须在组织里实施。
- ③在审核安全体系结构的备选方案时,为了保证兼容性就必须考虑网络的体系结构和应用。

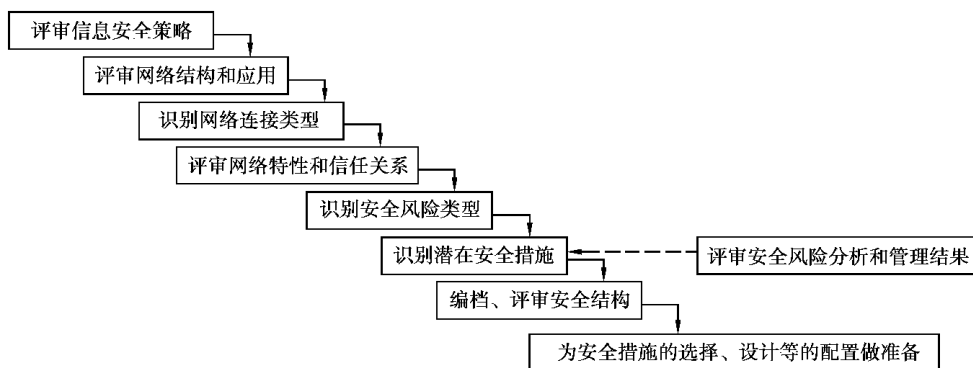


图 7.1 网络安全管理过程

7.1.3 识别和分析

7

1) 评审组织的信息安全策略需求

组织的信息安全策略应该包括关于机密性、完整性、可用性、抗抵赖性、可确认性、真实性和可靠性的要求的陈述,对威胁进行分类,以及安全措施需求等,这些都与网络连接直接相关。

比如,可以这样表述一个策略:

- 主要关注哪些类型信息或服务的可用性。
- 不允许拨号电话线路的连接。
- 所有通向 Internet 的连接都必须经过安全网关。
- 必须使用哪一种特定类型的安全网关。
- 没有数字签名的任何付款指令都是无效的。

在确定网络连接中安全风险类型和识别潜在安全措施区域时,必须考虑怎样表述这些问题和需求。如果有安全需求,就要将这些需求记录在潜在安全措施区域的列表草案中,并且反映在安全体系结构中。

2) 评审网络体系结构和应用

(1) 概述

接下来的几个步骤是确认可能的安全措施区域,即识别:

- 将要使用的网络连接的类型。
- 联网特性及其信任关系。
- 安全风险的类型。

事实上,安全措施区域列表的开发以及其后为一个特定连接的安全而进行的相关

设计,应该在已有或规划中的网络体系结构和应用背景下完成。

通过在尽可能早的阶段中弄清这些问题,识别相关安全需求的标识标准、识别可能的安全措施区域以及细化安全体系结构等过程,将更加有效地获得更好的安全解决方案。

另一方面,如果一个可接受的安全方案不能从当前实际的体系结构中获得,那么在尽可能早的阶段中考虑网络体系结构和应用方面的问题也能保证有时间复审和修改它们。

在网络体系结构和应用中需要考虑的问题包括:

- 网络的类型。
- 网络协议。
- 网络应用。

(2) 网络的类型

依据网络覆盖的区域,网络体系结构可划分为 3 类:

- 局域网(LAN),用于在本地将系统互连起来。
- 城域网(MAN),用于在一个大都市范围或一个综合业务地域内将系统互连起来。
- 广域网(WAN),用于比城域网范围更大的区域以至覆盖全球范围将系统互连起来。

按网络传输技术进行分类,网络可分为两类:广播式网络(Broadcast Networks)与点对点式网络(Point-to-Point Networks)。

按是否存在连接线,网络可分为两类:有线网络(Wired Networks)和无线网络(Wireless Networks)。

(3) 网络协议

不同的协议具有不同的安全特性,因此需要特别考虑。如:

①共享介质协议主要用于 LAN 中(有时也用在 MAN 中)并在互连的系统或用户之间提供机制来管制所使用的共享的介质。

②路由选择协议用于在 MAN 和 WAN 中通过不同节点传送信息时定义传送路径。信息对在此路径上的所有系统都是物理上可访问的,并且路径是可以改变的。

协议可用于不同的网络拓扑中,比如总线型、环型和星型等,包括通过有线或无线技术实现的网络,这些网络拓扑可能对网络安全都有影响。

(4) 网络应用

需要考虑网络应用类型与安全的关系,这些类型包括:

- 基于应用的终端仿真。
- 基于应用的存储、转发和假脱机处理系统。

- 客户/服务器应用。

(5)其他考虑

当审查网络体系结构和应用时,还应该考虑存在于组织内部的连接以及“外部”与组织发生的网络连接。由于协议冲突或合同要求,组织已存在的连接也许会限制或阻止新的连接。“外部”进入组织或从组织出去的网络连接将会引起额外的脆弱点,从而导致更高的风险,因此需要采用额外的安全措施。

3)网络连接的类型识别

一个组织可能希望利用的网络连接类型有多种,有些可以通过专用网络来实现,有些可以通过公共网络(任何组织或个人都可以访问)实现。而且,这些连接可以提供各种各样的服务,如电子邮件、电子数据交换(EDI)等,并且还可能使用因特网(Internet)和组建内联网(Intranet)、外联网(Extranet)网络结构提供更广泛的服务。每一种网络类型的连接可能有不同的脆弱性,从而有相应的安全风险,因而需要一系列不同的安全措施。

表 7.1 给出网络连接的一种分类方式。

表 7.1 网络连接的类型

序号	网络连接类型	描 述
1	组织内在同一个控制区域内的连接	在一个控制区域内将同一组织内的不同部分互连起来,如单独控制的大厦或局域网
2	将同一组织内地理位置分开的不同部分的连接	通过广域网将一个组织的区域分部/区域分部与总部互连起来。在这种类型的网络连接中,绝大多数或所有的用户都能通过该网络访问组织的信息系统,但并不是组织内的所有用户都有权力访问所有的应用和信息,即每个用户只能根据所授予的权限进行访问 组织可使用一种访问类型进行远程维护,这种类型的用户和连接需要更高的授权
3	组织的站点与远离组织的个人工作站点的连接	雇员在家里或者其他远程站点通过网络与组织相连,使用移动数据终端或者建立远程连接来访问组织的信息系统。这种类型的网络连接,用户在自己的系统中被授予为系统用户
4	关系密切的不同组织间相互连接,即由于合同或其他法律绑定关系,或者由于商业共同利益,例如银行业和保险业的连接	在两个或更多的组织间的互连,由于业务需要而利用组织间的电子交易(比如,由银行传送的电子资金)。这种网络连接和本表第 2 种类型类似,不同的是这种方式中互连的站点属于两个或更多个组织,而且这种连接并不提供对每个参与组织的应用的访问

续表

序号	网络连接类型	描 述
5	一个组织与其他组织的连接	<p>访问其他组织的远程数据库(比如通过服务供应商)类型的网络连接中,所有用户包括那些连接起来的组织,由外部组织(其信息可提供访问)单独预授权。然而,虽然所有的用户都被预授权,但却无法阻止那些潜在的、不想为享受了服务而付款的用户</p> <p>这些连接还能访问在组织内的一些系统上的应用程序,这些系统存储、处理组织的信息,而这些信息可以提供给外面的用户。在这种情况下,应该知道这些用户是来自外部的,并且授权给他们</p> <p>别的组织可使用一种访问类型进行远程维护,这需要为这种类型的用户和连接分配更高的权限</p>
6	与公共域连接	<p>能够由组织的用户启动,访问公共数据库、Web 站点/电子邮件设施(例如通过因特网)。此处启动、访问的目的是为了信息检索、从组织的个人或站点发送或接收信息等,而他们并不需要得到组织的特别的预授权。在这种类型的连接中,组织的用户可能为组织的目的(甚至个人目的)使用这些设施。因此,组织可能对这些传送的信息只有极少的控制(如果说还有控制的话)或不予控制</p> <p>对组织的设施进行的访问能够被外部用户启动(通过因特网)。在这种连接类型中,组织并不对来自外部个人的访问单独特别地预授权</p>

4) 联网特性和相关信任关系评审

(1) 网络特性

应该审查已有或计划中的网络的特性。重要的是识别网络属于哪种类型以及网络所传输的数据的类型:

- 公共网络,即任何人都可访问的网络。
- 专有网络,即一个由自己组建或租用的线路组成的网络,因此认为它比公网更安全。
- 数据网络,即主要用于传送数据,并使用数据传输协议。
- 语音网络,即主要用于电话,但也能传送数据。
- 语音和数据两者都能传送的网络。

- 其他数据网络,如数据包网络或电路交换网络。
- 有时还需要确定网络连接是永久性的还是临时性的。

(2)信任关系

一旦确认了已有的或计划中的网络的特性,以及至少知道是通过公网还是专网建立的,接下来就应该确认相关的信任关系。

首先应该用表 7.2 所示的简单的阵列关系将网络连接与可适用的信任环境关联起来。

表 7.2 信任环境描述

信任环境	描 述
低	未知的用户团体的网络
中	熟知的用户团体的网络,并且同在关系密切的业务团体中(多于一个组织)
高	熟知的用户团体的网络,并且只在一个关系密切的组织内

其次,相关的信任环境(从低、中到高)应该与可适用的网络特性(公网或专网)和包含的网络连接类型相关联,可以使用表 7.3 所示的阵列关系来完成建立信任关系(表 7.3 中使用的序号为表 7.1 的网络连接类型序号)。

表 7.3 信任关系识别

网络连接类型	信任环境		
	低	中	高
公网	6	4	2
		5	3
私网		4	1
		5	2
			3

从表 7.3 能为每一相关的信任关系确定其参考类别。所有可能的类别如表 7.4 所示。

表 7.4 信任关系归类

信任关系类别	描 述
低/公网	低信任,使用公众网络
中/公网	中信任,使用公众网络
高/公网	高信任,使用公众网络

续表

信任关系类别	描 述
低/私网	低信任,使用专有网络
中/私网	中信任,使用专有网络
高/私网	高信任,使用专有网络

5) 识别安全风险的类型

必须意识到各种网络连接技术会产生额外的安全风险。本节中提到的风险类型与下述概念有关:对信息的非授权访问、未授权发送信息、引入恶意代码、否认接收或发送,以及拒绝连接服务。这样,一个组织要面对的安全风险将与失去下列特性相关:

- 信息的机密性。
- 信息的完整性。
- 信息和服务的可用性。
- 抗抵赖性。
- 交易的可确认性。
- 信息的真实性。
- 信息的可靠性。

不是所有可能的安全风险都会出现在每个地方或每个组织。但是,需要识别与本组织相关的安全风险,以便识别潜在的安全措施区域(包括其后的安全措施选择、设计、实施和维护)。

需要说明的是,用户越多,越需要更多的控制。这有两方面的原因:第一,需要很多控制来保护主机信息设施,包括用于识别和鉴别,以及逻辑访问控制的设施;第二,即使是被信任的用户,由于常常可以访问重要/关键的信息/功能,这需要额外的安全措施。

6) 识别恰当的潜在安全措施区域

本节介绍与潜在的安全措施区域识别有关的问题。需要指出的是有大量的安全措施与信息系统相关,不管这些系统是否和网络连接,都可以使用第4章第3节“安全措施的选择与实施”中介绍的技术来选择安全措施。此处的讨论假定将安全措施部署到组织的与网络连接的系统。

识别出来的潜在安全措施区域需要在相关的网络体系结构和应用中得到全面评审,作为以后进行详细的安全措施选择、设计、执行和维护等的基础。

(1) 安全服务管理

对任何网络来说,一个很关键的安全需求是得到安全服务管理活动的支持,这些

管理活动将启动和控制安全的实施以及安全运营,以保证一个组织所有信息系统的安全。对于网络连接方面,管理活动应包括:定义与网络连接安全相关的所有责任,并指派一个全面负责的安全官员;已文档化的信息安全策略,以及配套的已文档化的安全技术体系结构;已文档化的安全运行规程;进行安全遵从性检查,以保证安全维持在要求的保护水平上;已文档化的、待建立的连接在允许连接之前要遵循的安全条件;已文档化的用于网络服务的用户的安全条件;安全事件解决方案;已文档化的并经过测试的业务连续性/灾难恢复计划。

①安全运行规程:为了支持系统的安全策略,应开发和维护安全运行规程的文档,它们应包括和安全相关的日常运行规程的细节,以及谁使用谁负责和谁管理谁负责的规程细节。

②安全遵从性检查:对网络连接而言,安全遵从性检查应该按照一个全面的检查列表进行检查,此列表包含的安全措施来源于下述文档:

- 系统的安全策略。
- 相关的安全运行规程。
- 技术性的安全体系结构。
- 安全网关服务的访问(安全)策略。
- 业务连续性计划。
- 相关地方的连接安全条件。

③连接的安全条件:除非连接的安全条件已具备并用合同形式予以约束,组织才不会受到与网络连接的另—终端相关联的风险的影响。例如,在 B 组织能通过一个网络连接到 A 组织的系统之前,A 组织可能需要 B 组织保证它要连接进来的系统维持一定的安全等级。通过这种方式,A 能够确保 B 以一种可接受的方式在管理它的风险。这种情况下,A 应该提供一种连接的安全条件的文档,详细说明在 B 的终端应有的安全措施,并由 B 来实施,双方再以组织的形式签署一个对其起约束作用以及安全将得到维护的声明。A 将保留对 B 进行安全遵从性检查的权利。

还有一种情况,组织间相互协商一种“连接的安全条件”文档,这个文档记录各方的义务和责任,包括相互的遵从性检查。

④用于网络服务的用户的、文档化的安全条件:应给被授权在远程工作的用户发布一个“网络服务用户的安全条件”的文档,用以描述用户对与网络相关的硬件、软件和数据应承担的责任,以及它的安全性。

⑤事件处理:在存在网络连接的地方,容易发生有害事件,对业务引起严重的负面影响。此外,由于用网络连接到其他组织,有害事件还可能引起法律纠纷。为此,一个有网络连接的组织需要拥有良好文档化并供实施的事件处理方案,以及将相关的基础设施配置到位,以便在意外事件发生后能够很快做出反应,将负面影响减至最低,同时吸取教训防止类似事件再次发生。

(2) 识别和鉴别

①远程登录:来自工作在组织的网络站点之外的被授权的人员(例如远程的维护工程师,或者其他组织的人员,或者本单位的外出人员等)可以通过拨号连接、因特网连接或其他组织的专线实现共享访问的远程登录。这些连接是由内部系统或合同伙伴使用公共网络在需要时建立的。每一种类型的远程登录都要求额外的、与该连接类型相适应的安全措施。安全措施的一些例子如:

- 不能允许使用远程访问的账户直接访问系统和网络应用软件,除非提供附加的账号验证和身份鉴别,以及必要时进行端对端的加密。

- 对那些与电子邮件软件以及存储在 PC 机和便携式计算机内、被组织的人员在办公室之外使用的目录数据等相关联的信息进行保护。

②增强鉴别:使用用户身份标识或口令是一种简单的鉴别用户身份的方法,但是标识或口令可能被泄漏或被猜出来。当一个未被授权者极有可能访问被保护的重要的系统时,则需要使用一些更加安全的方式来增强鉴别用户身份。增强鉴别的例子如:

- 使用其他的识别方式来支持用户鉴别,比如远程验证的令牌、智能卡和磁条卡(例如通过连接在 PC 上的阅读器读出),手持式一次性密钥生成设备,回拨调制解调器,以及基于生物特征的鉴别设施等。

- 使用呼叫者线路验证技术。

- 在不用时断开通过调制解调器进行的连接,只有当呼叫者身份得到核实后才连接。

③远程网络体系的识别:对那些从外部发起访问的系统所进行的鉴别可以通过对该系统(和其位置/访问点)的验证而得到增强。应该认识到,不同的网络体系结构能够提供不同的识别能力。因此,组织可通过选择一个恰当的网络体系结构来增强鉴别。被选网络体系结构的所有安全措施的效果都应考虑。

④安全的一次性登录:安全的一次性登录通过减少用户不得不记忆的多个口令,从而能减少口令被窃或丢失的风险。然而,要注意的是,一次性登录系统故障所产生的后果也是严重的。因此,需要比标准的识别和鉴别机制更强的机制,必要时可能要考虑从安全一次性登录机制中将高权限(系统级)识别与鉴别的功能卸掉。

(3) 审计跟踪

通过检测、调查和报告安全意外事件以保持网络安全的有效性极为重要。应该将有关失败与成功事件的审计跟踪信息完全记录下来,以便能够通过复审找出可疑事件和真实事件等。不过,应认识到,记录大量的与审计相关的信息会使分析的工作量大且非常困难,可能会影响正常工作,因此应仔细考虑哪些信息是真正需要记录的。

对网络连接而言,以下几种类型事件的审计是很重要的:

- 失败的远程登录尝试及其日期和时间。
- 失败的重新鉴别(或令牌的再使用)事件。
- 安全网关通信流异常变化。
- 远程尝试访问的审计跟踪信息。
- 系统管理的安全告警(例如 IP 地址重复,承载电路中断等)。

审计跟踪涉及对敏感信息或有关企图通过网络连接攻击该系统的信息的日志审计和跟踪。此外,拥有审计跟踪信息可以为在有争议的事件中提供证明,特别在保证完整性和抗抵赖时将极为有用。所以,所有的审计跟踪信息都应该得到合适的保护。

(4)入侵检测

随着网络连接的增加,入侵者通过下列方法将会更容易进入系统:

- 找到多种途径渗透进一个组织的信息系统和网络。
- 伪装成初始访问点。
- 通过网络访问并进入内部的信息系统。

更为严重的是,入侵者变得越来越有经验,并拥有更多的先进技术(工具),更先进的入侵技术和工具能轻易地在因特网或者公开的印刷品中得到其需要的信息。入侵检测与好的识别和鉴别、逻辑访问控制以及计账和审计等安全措施的实施一起,可以对抗或降低入侵和穿透系统的风险。入侵检测提供了预测入侵、实时识别入侵以及产生合适警告等的能力;还能在本地收集有关入侵的信息,继而分析和加固信息系统,以及分析一个组织正常的信息系统特性/使用模式。

(5)防护恶意代码

恶意代码有可能通过网络连接进入用户的网络和主机环境。恶意代码在破坏发生之前一般不易被发觉,如果不采用合适的安全措施,恶意代码甚至可能损坏安全措施(使设备功能失效)、泄露信息、改变信息、毁坏信息/非授权地使用系统资源。

一些恶意代码可被特殊的扫描软件检测到并加以清除。恶意代码扫描器可与防火墙、文件服务、邮件服务器以及工作站集成使用。重要的是,为了能检测新出现的恶意代码,必须及时升级扫描软件。当然,用户和管理者必须意识到,不能完全依赖扫描来发现所有的恶意代码(或者某种特殊类型的所有恶意代码),因为新的恶意代码会不断出现。一般来说,需要使用其他形式的安全措施来增强扫描软件所提供的保护。

网络连接系统的用户和管理者应该注意到当通过外部连接与外部组织进行业务合作时,可能将恶意软件引入进来,因此安全管理策略应该强调对连接过程和操作中可能出现的这种不期望事件的处理预案,以最小化引发恶意代码的可能性。

用户和管理者应该特别小心地对与网络连接相关的系统和应用进行配置,禁止环境中不必要的功能(如 PC 机通过配置禁止宏默认,或在执行宏前需要得到用户的确认)。

(6) 网络安全管理

任何网络的管理都应该以一种安全的方式进行,保证为管理网络的安全提供真正的支持。这应该考虑通过不同的可用安全服务以及与安全服务有关的网络协议来完成。无论是虚拟的或物理的远程诊断口都应加以控制或保护,以防止未授权访问。

(7) 安全网关

恰当的安全网关部署将会保护组织的内部系统以及根据文档化的安全网关服务的访问策略,安全地管理和控制其上通过的通信流。

一个安全网关应该实现:

- 逻辑地隔离网络。
- 为逻辑网络之间传递的信息提供约束和分析功能。
- 作为组织的一种控制点,控制对该组织的网络的访问,以及从该组织的网络发起的对外访问。
- 提供一个对逻辑网络进行访问的可控的和可管理的单入口点。
- 强制执行组织的关于网络连接的安全策略。
- 通过一个单点进行登录。

对每一个安全网关都应该开发并实施一个独立的服务访问(安全)策略的文档,以保证每个这样的连接只允许授权信息流通过。必须能够根据通信协议和其他细节信息来定义允许的连接。为了保证只有合法的用户才能从通信连接中获得访问权,这个策略文档必须详细地定义和记录施加到每个安全网关的输入和输入流上的约束和规则,以及其管理和配置参数。

对于所有的安全网关,都应该全面使用适当的识别与鉴别、逻辑访问控制和审计设施。此外,还应该经常检查未经允许的软件/数据,一旦发现问题,应该根据组织的安全事件分析和解决方案做出事件报告。

需要强调的是,只有在经过检查证实所选的安全网关满足组织的要求,以及所有由这样的连接所引起的风险都能够被安全地管理之后,才允许连接到一个网络。应确保没有任何可能旁路与此安全网关的连接。

(8) 网络上的数据机密性

在机密性保护非常重要的地方,应考虑使用加密设施来对通过网络连接传输的信息进行加密。使用加密安全措施时应考虑到:

- 相关的政府法律法规(特别是当网络连接跨越几个国家或地区的地方)。
- 相关的公开密钥基础设施和密钥管理需求。
- 加密机制对这种类型的网络连接的适用性,以及所需保护强度是否足够。

(9) 网络上的数据完整性

在完整性保护非常重要的地方,应考虑使用数字签名/信息完整性的安全措施来

保护通过网络连接的信息。

使用数字签名/信息完整性安全措施时应该考虑：

- 相关的政府法律或法规(特别是网络连接跨越几个国家或地区的地方)。
- 相关的公开密钥基础设施及密钥管理需求。
- 待采用的机制对这种类型的网络连接的适用性,以及所需保护强度是否足够。

(10) 抗抵赖性

有些场合要求确保信息的真实来源,以及收发信息行为和内容的不可否认特性,并提供实际证明。有这些要求的地方应该考虑下面的安全措施:

- 能对信息提交提供确认的通信协议。
- 需要发起者地址或标识符的应用协议,以提供和检查此信息的存在。
- 能检查发送者和接收者真实身份的网关。
- 能对来自网络的交付行为提供确认的协议。
- 能对交付内容提供确认的协议。

在那些需要证明信息的传输或收发以免产生纠纷的地方,可以通过使用标准的数字签名方法来提供进一步的保证。为此应该考虑:

- 使用可信第三方如证书机构以及被关联的公钥基础设施所支持的抗抵赖机制(数字签名,时间戳等)。
- 用能防止修改日志的机制记录并保存登录消息。
- 保护秘密/私有(签名)密钥不被未授权使用的机制。
- 获取解决争端所需的证书或密钥,保证它们在要求时间内(可能比关联的密钥材料的保护周期更长)的可用性和完整性。

(11) 虚拟专用网

虚拟专用网(VPN)是一类私有或专用网络,它在公共网络的基础设施上使用技术方法加以实现。

在 VPN 中,可选用密码技术来实现机密性和完整性安全功能和服务,特别是在公众网(如因特网)上构造 VPN 时。

对所有的私有网络,重要的是在所有连接到 VPN 的系统(网络或终端)上实施合适的安全措施,比如,保证只有得到授权的网络、终端或系统才能与 VPN 连接。

VPN 可以应用于下列几种情况:

- 使用移动设备或不在现场的雇员实施对组织的远程访问。
- 将一个组织分布在不同地理位置的局域网连接起来,包括冗余连接以实现一个全备份的基础设施。
- 为其他组织/业务伙伴建立起组织的网络的连接。

(12) 业务连续性/灾难恢复

重要的是将能在适当的时间内提供各部分业务的恢复功能的安全措施部署到位,

以保证业务在灾害事件后可持续进行。业务连续性/灾难恢复计划是一个整体,包括开发适当的业务连续性/灾难恢复策略及相关计划,并进行测试。

7.2 通信和操作管理

7.2.1 操作程序和责任

应该建立所有信息处理设备管理和操作的责任和规程,包括制定适当的操作指南和事件响应程序,确保对信息处理设备正确和安全的操作。

必要时应实施责任划分,以降低疏忽或故意滥用系统的风险。

(1) 操作程序文档化

安全策略确定的操作程序应该文档化并加以维护。

文档化的操作程序应该规定每项工作的详细操作指导,包括:

- 信息的加工和处理流程。
- 日程要求,包括和其他系统的依存关系,最早的工作开始时间和最晚的工作完成时间。
- 执行过程中出现的错误或其他意外情况的处理原则,包括对系统功能使用的限制。
- 在发生意外操作或技术困难时的支持策略。
- 特殊输出处理的指导,诸如特殊文具的使用或保密输出的管理,包括失败作业输出的安全处理程序。
- 在系统失效时使用的系统重启和恢复程序。
- 与信息处理和通信设备有关的系统日常管理活动也应准备文档化的程序,如计算机启动和关机程序、备份、设备维护、计算机房和信息处理的管理和安全保护。

(2) 操作的变更控制

对信息处理设备和系统的变更必须进行控制。可行的情况下,应把操作和应用的变更控制程序整合起来。特别应考虑以下控制措施:

- 重大变更的识别和记录。
- 评估此类变更的潜在影响。
- 更改建议的审批程序。
- 将变更细节通知给所有相关人员。
- 确定中止和恢复不成功变更的责任的程序。

(3) 事件管理流程

应建立事件管理责任和流程来确保对安全事件快速、有效和有序的响应。应考虑

以下的控制措施：

①对下列潜在的安全事件类型建立响应程序：

- 信息系统故障和服务丧失。
- 拒绝服务。
- 业务数据不完整或不准确所导致的错误。
- 机密性破坏。

②除正常的应急计划(为尽快地恢复系统或服务而设计),程序还应包括：

- 分析和识别事件原因。
- 如有必要需设计和实施补救措施以防止事件的复发。
- 收集审计信息和类似证据。
- 与受到事件影响的人或恢复工作涉及的人沟通。
- 向有关当局汇报情况。

③如果有必要,收集并安全地保管审计线索和类似的证据,以用于：

- 内部问题分析。
- 作为可能违反合同和违反法规要求或引起的民事或刑事诉讼(如由于滥用计算机或违反数据保护法)相关的证据。
- 与软件和服务供应商商谈赔偿问题。

④对安全破坏的恢复工作以及系统故障的纠正工作,应进行正规和严谨的控制。

此程序应确保：

- 仅允许经明确标识和授权的员工访问运行中的系统和数据。
- 详细记录所采取的所有应急行动。
- 应急行动应报告给管理层并按规程进行审批。
- 及时对控制措施和业务系统完整性进行确认。

(4) 职责分离

职责分离是降低意外或故意滥用系统的风险的一种方法。为减少未经授权的修改或滥用信息或服务的机会,适当分开管理或执行的职责或责任是非常必要的。

小型组织可能发现这种控制方法难以实现,但是只要需要并可行,这一原则就应该以适当方式(包括简化措施)予以坚持。如难以对职责进行分离,应考虑相应的控制措施,如行为监视、审计跟踪和管理监督。这种情况下,保持安全审计的独立性显得格外重要。

要特别提防在独立责任领域内出现的诈骗或监守自盗行为。

(5) 开发和操作设备的分离

对开发、测试和操作设备的职责进行分离对实现任务非常重要。应该制定并文档化软件从开发转入操作状态的管理规则。

开发和测试行为不得由同一个(组)人来执行,也不得在同一台(组)设备中运行。

类似地,开发和操作也不得由同一个(组)人来执行。

当开发和测试人员有权访问操作系统和其他信息时,就有可能引入未经授权和未经测试的程序代码或改变操作数据。在某些系统中,这种能力可能被滥用来进行欺诈,或引入未经测试或恶意的代码。未经测试的或恶意的代码能引起严重的操作问题,给操作的信息的机密性造成威胁。

如果开发和测试活动共享相同的计算环境,可能造成软件和信息意外改变。因此为降低意外改变或未经授权的访问操作软件和业务数据的风险,隔离开发、测试和操作设备是值得的。应该考虑如下的控制措施:

- 开发和操作软件应该运行在不同的计算机处理器上,或是在不同的域中或目录下。
- 开发和测试活动应该分离。
- 编译程序、编辑程序和其他的软件系统在不需要时不得擅自通过操作系统访问。
- 对操作系统和测试系统应使用不同的登录程序,以降低操作风险,应该鼓励用户对这些系统使用不同的口令,操作菜单应显示适当的识别信息。
- 只有获得操作系统特权口令的开发人员才有权获得操作所需的口令,控制措施应确保口令在使用后被更改。

(6)外部设备管理

由外部合同方管理信息处理设备可能引起潜在的安全性问题,如数据在承包商一方被泄密、修改、损失或遗失的可能性。应该提前识别这些风险,与合同方商定适当的控制措施,并将义务与责任写入合同。

应该提出的特殊问题有:

- 识别保留在外部设备中的敏感或关键的应用软件。
- 获得业务应用软件所有人的授权。
- 提供可持续业务计划。
- 需要详细说明的安全标准和衡量符合性的程序。
- 有效监督所有相关安全活动的具体责任分配和程序。
- 报告和处理安全事件的责任和程序。

7.2.2 系统规划和验收

需要事先规划和准备以确保系统有足够的容量和资源可用,达到将系统失效的风险降到最低的目的。

对未来容量需求做出预测,以降低系统超载的风险。

建立新系统的操作要求,在验收和使用前进行文档化并加以测试。

(1) 容量规划

应监控所需的容量并预测未来的容量需求,确保有足够的处理能力和存储能力。容量规划应当考虑新业务和系统的需求,以及组织在信息处理方面当前和未来的趋势。

管理者应使用此类信息来识别和避免可能对系统安全或用户服务造成威胁的潜在瓶颈,并设计适当的补救措施。

(2) 系统的验收

制订新信息系统以及系统升级和新版本的验收标准,并在验收前对系统进行适当的测试。管理者应确保新系统的验收要求和标准被清晰地定义、文档化和测试。考虑以下控制措施:

- 性能和计算机容量的要求。
- 从故障中恢复和重启程序及应急计划。
- 准备和测试日常的操作程序以达到规定的标准。
- 实施业经同意的安全控制措施。
- 有效的指南规程。
- 业务持续性安排。
- 新信息系统的安装不会给现有信息系统带来负面影响的论证资料,特别是在处理量高峰时间,如月末。
- 已经考虑了新信息系统对组织的整体安全产生的影响的论证资料。
- 操作和使用新信息系统的培训。

对于主要的新的开发工作,应该在开发过程的所有阶段咨询操作人员和用户,以确保所提出的系统设计方案的操作效能。应该实施适当的测试来确认所有的接收标准已被满足。

7.2.3 脆弱性和补丁

补丁程序对维持信息系统在操作上的可用性、机密性和完整性是必不可少的。然而,信息技术专业人员最常见的错误是没有或不及时为操作系统和应用软件安装补丁。新补丁程序可能不断发布,及时跟上所有新补丁是连有经验的系统管理员都感到困难的事情。

脆弱性是软件中的缺陷或弱点,它可能被恶意实体利用从而在一台计算机上获得比被授权更多的访问和权限。并不是所有的脆弱性都可用补丁程序来修补,因此,系统管理员不但必须意识到脆弱性和相应的补丁,还要通过其他方法(如防火墙、路由控制表等)来减轻那些无相应补丁程序的脆弱性。

为了帮助处理日益增多的补丁程序,建议组织开发一个补丁、脆弱性策略并采用系统的、文档化的规程来处理补丁。该文档为完成目标提供准则和方法,可能的措施

之一是建立一个补丁和脆弱性处理组(PVG, patch and vulnerability group),由他们在组织内识别和分发补丁。PVG 职责包括:

- 建立一个组织的软件和软件清单。
- 识别新近发现的脆弱性和安全补丁。
- 优先考虑补丁程序的应用。
- 建立补丁库。
- 测试补丁的功能性和安全性。
- 为本地管理员分发脆弱性信息和补丁程序。
- 通过网络安装补丁后再进行主机脆弱性扫描。
- 培训系统管理员使用脆弱性数据库。
- 在适当的时候自动部署补丁。
- 在适当的时候应用程序自动更新补丁程序。

即使组织建立了 PVG,系统管理员为 PVG 控制下的系统安装补丁的责任丝毫不可减少。每个系统管理员需要:

- 应用已被 PVG 识别的补丁。
- 在特定的目标系统中测试补丁。
- 测试与软件有关的没有被 PVG 监控的补丁和脆弱性。

7.2.4 防范恶意软件

需要有预防措施来检测和防止恶意软件的引入或渗透。

软件和信息处理设备易受引入或渗入的恶意软件的攻击,恶意软件包括计算机病毒、网络蠕虫、特洛伊木马以及逻辑炸弹等。用户应该意识到未经授权或恶意软件的危害,在需要的地方,管理人员应该采取特殊的控制措施来检测和防止此类恶意软件的引入或渗入,特别是有必要采取预防措施来检测和防止个人计算机上的计算机病毒。

防范恶意软件必须强调安全意识,实施适当的系统访问控制和变更管理控制。考虑如下的恶意软件控制措施:

- 遵守软件许可协议并禁止使用未经授权的软件。
- 防范从外部网络或通过外部网络或从任何其他介质上取得文件和软件而引入恶意软件的风险,为此应制定相应的安全措施。
- 安装和定期更新防病毒检测和修复软件,对计算机和存储介质进行扫描。
- 定期检查支持关键业务过程的系统的软件和数据内容,对出现的任何未经批准的文件或未经授权的修改应进行正式的调查。
- 对于存储介质上来源不明或来源未经授权的文件,或者从不可靠的网络上收到的文件,在使用之前应进行病毒检查。

- 对任何电子邮件的附件和下载内容,在使用之前应进行恶意软件检查。此类检查可在不同地点进行,如电子邮件服务器、桌面计算机或在进入组织的网络入口。

- 定义病毒防范的管理程序和责任,加强用户培训,及时报告病毒并从病毒攻击中恢复。

- 用于病毒攻击后恢复工作的持续业务计划,包括所有必须的数据和软件的备份以及对攻击后的恢复安排。

- 建立验证和所有恶意软件相关的信息的程序,确保警告公告信息的准确性和可用性。管理者应确保资料来源是可靠的,如有声望的杂志、可信赖的网站或防毒软件供应商,以区分出恶作剧和真正的病毒。员工应该知道如何识别恶作剧并在收到恶作剧信息时进行适当处理。

这些控制措施对于支持大多数工作站、个人终端和网络服务器的防范工作是有效的。

7.2.5 内容处理

应建立常规程序以实施备份策略、备份数据和演练备份资料的及时恢复,对操作事件和失效进行日志记录,并在条件许可时监控设备环境,保持信息处理和通信服务的完整性和可用性。

(1) 信息备份

重要的业务信息和软件应该定期备份。应该提供足够的备份设备以确保所有重要的业务信息和软件能够在发生灾难或介质故障后迅速恢复。不同系统的备份安排应该定期进行测试,以确保可以满足业务持续性计划的要求。应考虑如下的控制措施:

- 备份的系统恢复所需的最小信息集、准确和完整的备份情况的记录以及文档化的恢复流程都应该保存在足够远的地点,以避免由于主场所发生灾害所带来的备份信息丢失或损失,对重要的业务应用程序的备份信息至少应该保留法定的时间。

- 对备份信息的物理和环境的保护级别应和主场所保护的标准相一致,对主场所的介质所实施的控制措施适用于备份的场所。

- 如有必要,对备份介质进行定期的测试,以确保需要时可用于紧急恢复。

- 备份流程应定期进行检查和测试,以确保其有效性,并确保恢复工作可以在规定的时间内完成。

- 决定重要业务信息的保留期,对需要永久保存的文档进行复制。

(2) 操作者日志

应该保留操作人员行为日志,日志应包括:

- 系统启动和关机时间。

- 系统错误和所采取的修正行为。

- 对数据文件和计算机输出的处理情况。
- 登录人员的名字。

对操作人员日志应按操作流程进行定期的、独立的检查。

(3) 差错记录

对差错应该进行报告并采取修正行动。应该记录用户所报告的信息处理中和通信系统中的差错。对如何处理报告的差错应有明确的规范：

- 检查差错记录,以保证差错被圆满解决。
- 检查对差错进行修正的记录,以确保没有危害到控制措施,并且所采取的修正行动是经过授权的。

7.2.6 网络管理

确保对网络中信息和支持性的基础设施进行保护。对跨组织边界的网络的安全管理需要格外注意。对于通过公共网络的敏感信息要有额外的保护和控制措施。

由网络管理员实施网络控制,确保网络中数据的安全,并防止网络服务受到未授权的访问。特别需要考虑如下控制措施：

- 条件许可时,将网络操作和计算机操作的责任予以分离。
- 建立对远程设备(包括用户区的设备)的管理责任和流程。
- 如有必要,应建立特殊的控制措施来确保通过公共网络的数据的机密性和完整性,并保护与网络相连接的系统,还需要特殊的控制措施来维护网络服务和所连接的计算机的可用性。
- 管理行为要紧密协作,以优化对业务所提供的服务,并确保对信息处理基础设施的控制措施得以始终保持。

7.2.7 介质处理和安全

对介质应加以管理和提供基于物理措施的保护。应建立合适的操作流程来保护文档、计算机介质(磁带、软盘、盒式磁带、USB 盘、光盘等)、输入/输出数据和系统文件免受损坏、盗用和未授权的访问。

(1) 可移动的计算机介质的管理

应有规程来管理可移动的计算机介质,如磁带、软盘、盒式磁带、USB 盘和光盘。应考虑如下的控制措施：

- 对从组织中换下来的可再用介质上的数据和信息,如不再需要,应实现不可恢复的删除。
 - 对从组织中换下来的任何介质都应妥善保存,并实行审核跟踪。
 - 所有的介质应该按照制造商的使用指南保存在安全的环境中。
- 所有的规程和处理行为的授权都要有清晰的记录。

(2)介质的处置

介质作废后,应当按规程对其进行安全处理。因此,应当建立规范的介质安全处理流程,将泄露信息风险降至最低。应当考虑下面的控制措施:

①对载有敏感信息的介质应加以安全妥善的保存或采用安全的方式加以处置,如焚烧或粉碎,或在清空数据后供本组织的其他机构使用。

②下面指明了可能需要安全处置的物品:

- 书面文件。
- 录音或其他形式的记录。
- 复写纸。
- 输出报告。
- 一次性打印色带。
- 磁带。
- 可移动的磁盘或磁带。
- 光学存储介质。
- 程序列表。
- 测试数据。
- 系统文档。

③把所有的介质收集起来集中进行安全处理,比试图分离出敏感的介质进行单独处理可能更加容易。

④应当注意选择一个有足够控制措施和经验的适当的收购商——专门对文件、设备和介质进行收购和处理服务的机构。

⑤对敏感物品的处理要进行记录,以便日后进行复核。

将大量介质积聚在一起等候集中处理时,应当特别注意所谓的“积聚效应”,即大量未分类信息积聚在一起可能比少量单个信息更敏感。

(3)信息处理的流程

应当建立信息处理和存储流程,以便保护这些信息免于未授权的泄露或误用。制订必要的流程并按照其分类对文件、计算机系统、网络、移动计算、移动通信、文本、邮件、语音邮件、一般语音通信、多媒体、邮政服务及设施、传真机和其他敏感物品等的使用进行管理。应当考虑下面的管理控制措施:

- 对所有介质进行标记。
- 对访问进行限制以识别未授权的人员。
- 保留数据合法收件人的正式记录。
- 确保输入数据的完整性和处理过程的正确完成,并对输出进行有效确认。
- 对等待输出的数据采取与其敏感性相对应的保护。
- 把介质存放在符合制造商规定的环境中。

- 尽量减少数据的分发。
- 对所有的数据副本进行清晰标记,以引起合法接收人员的注意。
- 定期对分发清单和合法收件人名单进行复查。

(4) 系统文档的安全

系统文档可能载有系列敏感信息,如对应应用程序、流程、数据结构、授权过程的描述。应当考虑下面的控制措施以保护系统文档免受未授权的访问:

- 系统文档应当安全地保存。
- 要尽量减少系统文档的访问量,对其访问要经过管理者的授权。
- 保留在公共网络上的或通过公共网络提供的系统文档应当加以适当的保护。

7.2.8 信息和软件的交换

在组织之间交换的信息应该防止丢失、修改或误用。应当控制在组织之间交换信息和软件,并使交换符合相关的法规。建立流程和标准来保护传输中的信息。应当注意到与电子数据交换有关的安全隐患以及控制措施的需求。

1) 信息和软件交换协议

在组织之间进行信息和软件的交换(通过电子的或人工的方式)必须订立协议,这些协议可能是规范的,必要时还要订立包括由第三方保存软件的协议。关于安全交换的协议应当考虑:

- 对传输、发送和接收进行控制的管理权责。
- 通知发件人和收件人,以及传输、发送和接收的流程。
- 包装和传输的最低技术要求的标准。
- 信使的身份证明标准。
- 丢失数据的责任。
- 对敏感或关键的信息使用协商一致的标记系统,确保标记的含义易于理解,使信息得到适当的保护。
- 信息和软件所属权及数据保护的责任,软件版权的合法性和类似考虑。
- 用于记录和读写信息和软件的技术标准。
- 保护敏感信息所要求的任何特殊的控制措施,例如加密保护。

2) 传输中媒体的安全

应当采用下列控制措施来保护两地传递过程中的安全:

- 使用可靠传递方式或信使并核查信使身份。
- 应当有充分的包装,以保护内容免受传输过程中可能发生的物理损坏。
- 在必要的地方,应当采用特殊的控制措施,以保护敏感信息免受未授权的泄露

或修改,可采用的控制措施包括使用上锁的或加封条的包装箱、人工传递、防拆包装(可显示被拆封的痕迹)、在特殊的情况下将发送的信息分割成若干份并通过不同的路线传递、信息内容使用数字签名和加密技术保护。

3) 电子政务的安全

所谓电子政务指的是政府使用基于 Web 技术的因特网和其他信息技术的结合,实现对办公业务和各类电子信息(数据)进行自动处理和交换的过程,达到增强政府提供给公众、社会和其他政府实体的信息和服务的访问和交付;或改进政府工作,促进政府职能转变,提升政府形象,包括影响力、效率、服务质量或改革。

(1) 电子政务安全体系框架

电子政务安全体系框架包括安全策略、安全法规、安全管理、安全标准、安全服务、安全技术与产品、安全基础设施七个方面,如图 7.2 所示。

安全策略明确了为保障电子政务安全,必须实行“国家推动、社会参与、保障发展、全局治理、积极防御、适度安全”的方针。

安全法规是涉及信息保密与信息公开、数字签名与电子文档、隐私权保护等的一系列法律性文件。

安全管理是对电子政务安全所涉及的分工、配合以及对安全生命周期进行监控的相应规范。

安全标准是对与电子政务有关的 PKI、KMI、PMI、信息安全产品接口、涉密内容密级分级与标签等的管理与技术的标准。

安全服务包括电子政务系统的脆弱点分析、威胁分析、风险分析、安全需求分析、系统安全设计和系统安全评测等。

安全技术与产品指适用于电子政务安全保障的技术与产品,其中涉及信息安全的核心技术与产品必须自主研发。

信息安全基础设施是对涉及电子政务安全保障基础的 PKI、PMI、KMI、灾难恢复基础设施、应急响应体系、安全产品测评与认证体系、计算机病毒防治与服务体系等国家信息安全基础设施的统筹规划。

(2) 电子政务的安全管理

①安全域的划分与管理。电子政务安全域的基本概念是“以信息密级划分的网络空间”。按照这个概念,电子政务可以划分为 3 个大的安全域,即涉密域(全称为“涉及国家秘密域”)、非涉密域(全称为“非涉及国家秘密域”)和公共服务域,如图 7.3 所示。

涉及国家秘密的网络空间称为涉密域。涉密域是电子政务中安全保密级别最高的安全域,是电子政务安全体系中确保的重点。对涉密域的基本安全保护要求是与其他域的物理隔离以及域内涉密信息的分级处理。隔离的措施可以采用硬件(具有电子

开关功能和单向传输控制能力)方式,其极端方式是不与其他域发生物理连接。要将需要实行物理隔离才足以保护其边界安全的网络空间压缩至最小。涉密域的边界以国家秘密等级划分为依据而不以业务(工作)部门为依据确定。

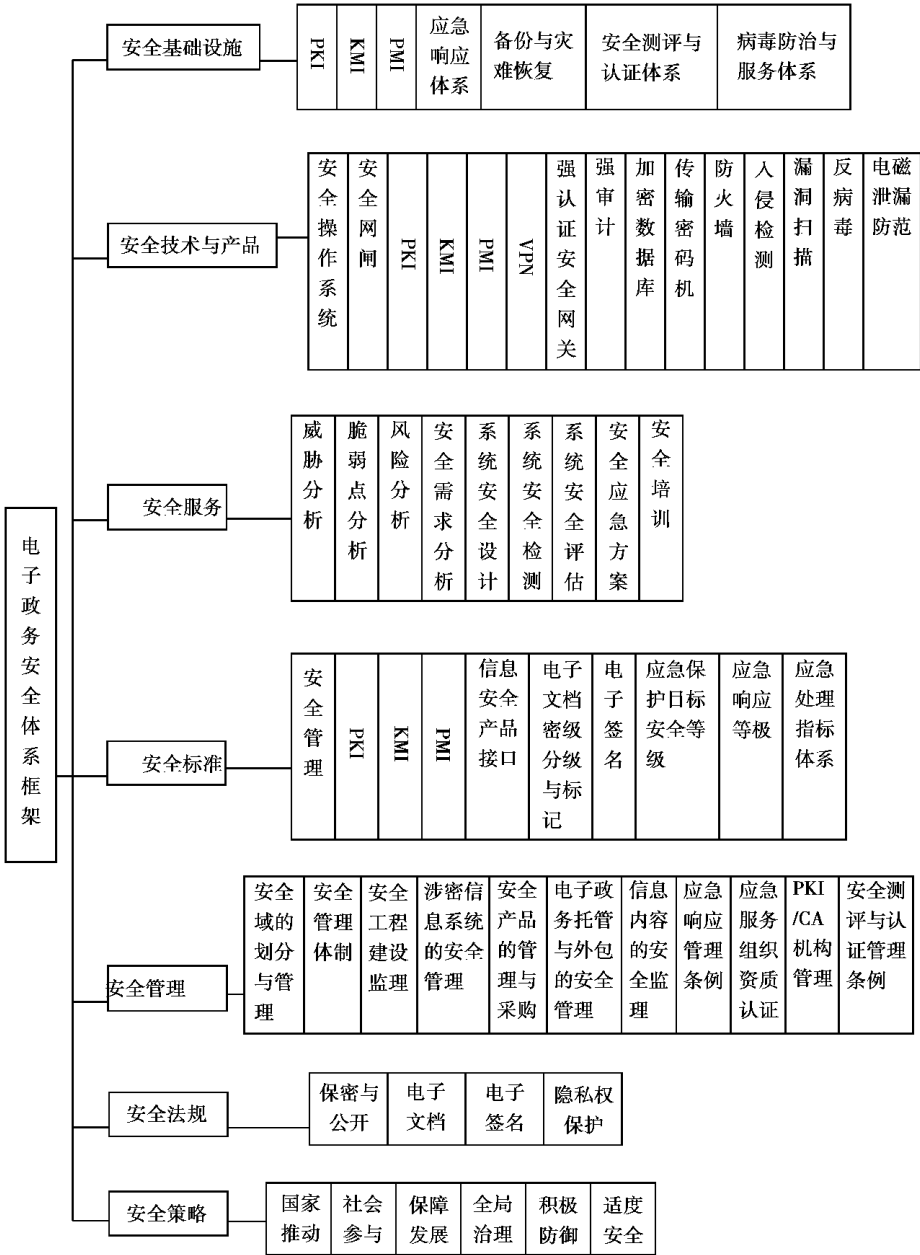


图 7.2 电子政务安全体系框架

不涉及国家秘密,但涉及本单位、本部门或本系统工作秘密或敏感信息的网络空间,称为非涉密域。非涉密域需要采用适度的安全措施,如可以通过适当隔离手段(例如防火墙、VPN 设备和代理服务等)与公共网络相连,或通过公共网络构建内联网来保证工作秘密或敏感信息的安全。

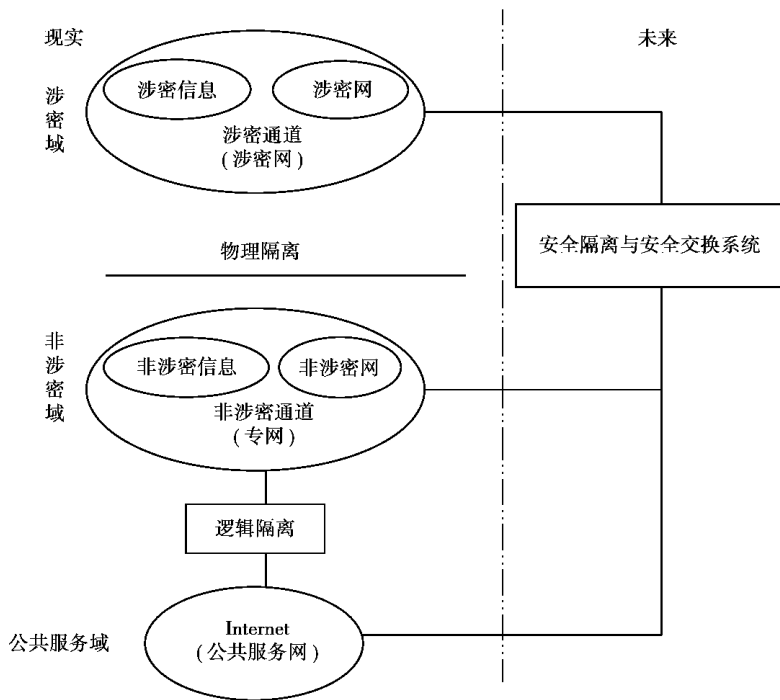


图 7.3 网络空间

不涉及国家秘密、工作秘密或敏感信息,但涉及机关或部门之间以及与社会、公众进行信息交换、共享的网络空间,称为公共服务域。这个域没有明确的物理边界。公共服务域依托在公共网络上,可以采用的安全措施大多集中在身份鉴别、访问控制和权限管理等方面。

电子政务的安全建设应与网络建设同步进行,已建成运行的电子政务系统应考虑逐渐过渡到有适度安全保障的合理体系。为此,可以考虑:

- 各部门目前已建成的电子政务网保留使用,但需依据上述三个安全域的划分进行整改。
- 各部门的涉密网通过涉密通道连接,形成国家电子政务涉密专网。
- 各部门的非涉密网通过非涉密通道连接,形成国家电子政务非涉密专网。
- 各部门通过 Internet 建立公共服务网,提供公共服务。

②安全管理体制。电子政务信息安全管理组织体系包括国家信息化领导小组及其办公室和国家有关主管部门。

国家信息化领导小组综合协调涉及各个领域的信息化和信息安全工作,组织协调计算机网络与信息安全管理方面的重大问题。国务院信息化工作办公室是国家信息化领导小组的办事机构,具体承担领导小组的日常工作,包括组织起草推进国家信息化建设和计算机网络与信息安全管理工作中的法规、标准及相关政策,以及负责组织和协调全国计算机、网络信息安全管理工作的。

国家有关主管部门明确分工,加强配合,在各自的职责范围内发挥作用。各政府机构遵守并执行国家主管部门制定的信息安全管理法规、标准,确保政府机构内部电子政务信息安全管理程序化、制度化。

③安全工程建设监理:电子政务安全工程建设监理机构负责监督电子政务安全工程的建设,并制定相关管理规定。

④涉密信息系统的管理:按照国家有关保密法规、标准和规范对涉密信息系统实施安全管理。

⑤安全产品的管理与采购:

- 国家有关主管部门负责制定信息安全产品的管理与采购政策。
- 涉及密码技术的安全保密产品必须获得国家密码主管部门的批准。
- 涉密网络安全保密产品原则上使用通过国家主管部门指定的测评机构检测的国产产品。

⑥电子政务托管与外包的安全约束规则:

- 电子政务系统的托管。电子政务中,涉密系统不能进行托管,非涉密系统和面向公共服务的系统应按照相关条例执行托管。

- 电子政务系统的工程外包。电子政务系统工程外包应遵从有关的管理规定,电子政务中涉密信息系统的工程承包单位必须具有国家保密主管机关颁发的涉密系统集成资质证书,非涉密信息系统的工程承包单位必须具有信息产业部颁发的系统集成相应的资质证书,具有涉密系统集成资质证书的承包单位可以承包非涉密系统的建设。

⑦信息内容的安全监管:电子政务中信息内容的安全监管目的是防止通过网络泄密以及反动、黄色信息在网络上出现。应强化信息内容安全监管的手段,建立相应机构,制订有关规定。

4) 电子商务的安全

(1) 控制措施

电子商务很容易受到大量来自网络的威胁或攻击,从而导致欺诈、合同纠纷和信息的泄露或修改。应当采取控制措施来保护电子商务免受类似的威胁。对于电子商务的安全应当包括下面的控制措施:

- 使用鉴别服务,鉴别客户和交易人的身份。

- 对制订价格、交易内容和签署关键交易文件的人授予操作权限,并以适当方式告知交易伙伴。

- 关键文件的发送、接收及合同必须在保证机密性、完整性和真实性的环境下完成。

- 确保报价清单的完整性和敏感的折扣信息的机密性。

- 采取措施确保订单、支付和交货地址的细节及接收确认方面的完整性和机密性。

- 对客户提交的支付信息进行审查。

- 采取抗抵赖服务,防范支付过程中的欺诈或抵赖行为。

- 加强对交易过程的监管和审计。

贸易伙伴间的电子商务安排应当由文档化的协议来支持,该协议使双方都对议定的贸易条款作出承诺,包括授权的细节。同时也有必要与信息服务和网络增值业务供应商签订其他的协议。

公共交易系统应当向客户公开其交易条款及规定。

应当考虑用于电子商务的计算机终端对于网上攻击的对抗能力和应急恢复能力。

(2) 可信第三方的管理

① 可信第三方(TTP)

电子商务安全需求可通过端对端的双方信任方案得以满足,但是在很多情况下直接实现端对端信任方案是有困难的,特别是对涉及大量的商业关系的时候,这就需要由第三方服务供应商提供信任解决方案。这样可以保证在一个更广泛的电子商务基础设施上提供更多的信任和安全。

可信第三方可以提供的服务包括:

- 加密或数字签名技术所使用的密钥管理服务。

- 鉴别和认证服务。

- 时间戳服务。

- 电子公证与仲裁服务。

- 目录服务。

- 抗抵赖服务。

TTP 可以提供上述所有这些服务或其中的一部分。TTP 的服务功能可被用于提供类似的支持服务,例如,证书服务供应商(CSP)可使用 TTP 的部分功能支持使用数字签名的服务。通常,CSP 提供与公钥证书相关的服务,这些公钥证书用于数字签名机制。

② 数字签名

很多标准和技术可用于数字签名。世界上的许多国家已经或者将要通过立法来界定这些技术的合法性和商业上的可接受性。数字签名背后的思想是非常简单和直

接的。通常一个用户拥有两个密钥:私密密钥和公开密钥。私密密钥被密钥所有者保护,以防非授权访问。公开密钥对所有需要使用它的用户是公开的(事实上,它在一个广泛分布并具有访问通道的目录媒体中公布)。私密密钥用来签名一个电子文档,例如,一个电子付款指令、电子合同或服务协议或其他任何可以合法绑定的文档。假定该密钥保持其私密性并且只能由其所有者掌握,那么文档就只能被所有者签名。收到文档的个人可以通过公钥来证实该签名。私密所有者的签名信息和已签名的文档相联系,这是一种安全的电子签名而非传统的手写签名,因此是支持电子商务的强大商业工具。

和所有的密码技术一样,密钥的管理对使用签名技术提供安全保障主关重要。这种情况下,需要管理私钥和公钥,以及管理调用公钥证书相关的事项。

③使用和管理可信第三方服务

技术规范“ISO/IEC TR 14516:2002 信息技术—安全技术—使用和管理可信第三方服务的指南”为 TTP 服务管理提供了技术指导。该技术规范是 ISO 与 ITU-T 联合开发的,相同的文本发布在 ITU-T 和 Rec. X842 中。

ISO/IEC TR 14516 面向系统管理员、开发人员、TTP 操作人员和企业使用者,帮助他们选择满足特定业务需求的 TTP,也有助于他们理解管理所包含的内容,使用这些服务和建立 TTP 安全策略。该技术报告包括管理、交互技术和服务方面的内容,以及如何识别 TTP 服务,包括时间戳、抗抵赖、密钥管理、证书管理和电子公证。这些主要服务中的每一个都由几个服务要素构成,逻辑地关联在一起。这就要求第三方供应商需要知道面临的风险以及如何通过实施合适的管理和技术,达到风险的最优管理。这方面的重要控制是建立信息安全策略,反映维护 TTP 处理的任何敏感信息的机密性,保护它处理的任何关键信息的完整性,以及它的服务、系统和信息对那些授权访问的人的可用性。

5) 电子邮件的安全

电子邮件(E-mail)是目前通过因特网(或其他计算机网络)交换信息的最大众化的网络应用系统之一。电子邮件系统可分为两个主要构件:邮件服务器,它们是交付、转发和存储邮件的主机;客户机,它们与用户相连,允许用户进行读、写、发送和存储邮件信息。

邮件服务器是最容易被攻击者瞄准的目标之一。因为计算和网络化技术支持邮件的普遍应用,它也就为攻击者开发攻击方式提供了广泛的学习和演练环境。因此,邮件服务器、邮件客户机和支持它们的网络基础设施必须得到保护。

邮件安全问题的例子如下:

- 邮件服务器应用程序中的缺陷可能被利用来攻击网络。
- 拒绝服务攻击(DoS)可以直接针对邮件服务器或支持它的网络基础设施,以拒

绝或阻碍用户有效使用邮件服务器。

- 邮件服务器上的敏感信息可能被未授权个体获得或以未授权方式改变。
- 在邮件服务器和客户机之间未加密地传送敏感信息可能被拦截,例如,所有大众邮件通信标准系统设定发送用户名、口令和 E-mail 净信息本身(未加密)。
- 电子邮件中的信息在发送者和接收者之间的某一点可能被改变。
- 恶意实体可能在组织的计算机网络的其他地方,通过对邮件服务器的成功攻击,获得对资源的未授权访问,例如,一旦邮件服务器被泄漏,攻击者就能够检索到用户的口令,这可能使攻击者获得访问组织网络内其他主机的权限。
- 恶意实体对一个邮件服务器主机的成功攻击进而利用邮件服务器继续攻击外部组织,这样就隐藏了入侵者的身份,并可能使组织对危害负责。
- 错误配置可能允许恶意实体使用组织的邮件服务器发送基于邮件的广告。
- 病毒和其他类型的恶意代码能够通过电子邮件传播。
- 用户可能通过 E-mail 发送不合适的、专有的或其他敏感信息,这可能泄漏秘密或引起法律诉讼。
- 垃圾邮件。

下列主要措施可用来维护邮件服务器的安全:

(1) 为邮件服务器制订安全计划

安全考虑应该从初始计划阶段开始。当组织开发和使用一个详细的、设计完整的开发计划时,需要考虑以下因素:

- 人员需求类型(如系统和邮件服务器管理员、网络管理员、信息系统安全官员)。
- 被指定人员必备的技能 and 培训。
- 个人和集体的素质要求。

(2) 组织需要执行适当的安全管理作业和控制

当操作和维护邮件服务器时,为保证邮件服务器和支持邮件服务器的网络基础设施的安全,需要:

- 组织范围的信息系统安全策略。
- 配置/改变控制和管理。
- 风险评估和管理。
- 满足信息系统安全策略的标准化软件配置。
- 安全意识教育和培训。
- 突发事件的处置和灾难恢复计划。
- 证书和信任。

(3) 邮件服务器操作系统的配置和管理要满足组织的安全需求

使邮件服务器安全的第一步是要保证运行于系统底层的操作系统安全。邮件服

务器通常运行在通用操作系统上,默认的硬件和软件配置一般由销售商指定。销售商一般只关注设施的功能和易使用性,并不关注各个组织的具体安全需求。每个邮件服务器管理员必须重新配置服务器以反映组织的安全需求以及当需求变化时的再配置。保证操作系统的安全通常包括以下考虑:

- 安装补丁和升级操作系统。
- 删除或禁止不必要的服务、应用和脚本内容。
- 配置操作系统用户鉴别功能。
- 配置资源控制措施。
- 对邮件系统进行安全测试。

(4) 实施加密技术以保护用户鉴别和邮件数据

大多数标准邮件协议对未加密用户的鉴别和使用明文发送邮件数据是默认的。明文发送数据使攻击者很容易窃取用户的账号或拦截和改变未加密的邮件。大多数组织需要要求用户的鉴别会话内容进行加密,现在很多标准和专有的邮件协议支持对用户鉴别的会话进行加密。

加密电子邮件要求用户的计算机和组织的网络基础设施额外消耗很大的运算和传输资源,同时还要考虑加入病毒扫描和邮件内容过滤,这就需要从管理上对安全和效率进行折中考虑。然而,对很多组织而言,邮件加密的好处将远远超出为此所付出的代价。

(5) 保护网络安全设施以保护邮件服务器

网络安全设施(如防火墙、路由器、入侵检测系统),对邮件服务器的安全保护起着重要作用。在大多数配置中,网络安全设施将是因特网和邮件服务器之间的第一道防御。

(6) 维护邮件服务器的安全

维护邮件服务器的安全是一个不间断的过程。因此,在日常维护的基础上,对邮件服务器进行安全管理是邮件服务器安全的一个重要方面。维护邮件服务器的安全通常包括以下措施:

- 配置、保护和分析记录文件。
- 经常性地备份数据。
- 避免受到恶意代码(如病毒、蠕虫、特洛伊木马等)的伤害。
- 定期检测服务器脆弱性并及时安装补丁。
- 监控与审计。

(7) 电子邮件内容过滤

内容过滤是根据一定的特征词(汇)对邮件内容进行某种判断而决定是否接收或发送,它并不对恶意代码进行过滤。通常内容过滤和病毒扫描在同一服务器中进行。

一般来说,定义的过滤规则是根据过滤结果,要求服务器转发、隔离、放弃、清除或删除任何数据。

6) 公用系统的安全

应当注意保护以电子形式发布的信息的完整性,防止对其进行未授权的修改而造成对组织声誉的损害。在公用系统上的信息,如通过因特网的网络服务器发布的信息,必须合乎其所在地区或所从事交易的地区的法律要求。在公开信息之前,应当有一个正式的审核与授权流程。

应当采取适当的机制对公用系统上的软件、数据或其他要求高度完整性的信息加以保护,例如通过数字签名的信息。对那些允许直接输入信息的系统,要加以严格的控制,做到:

- 信息的获取符合任何数据保护法规的要求。
- 输入发布系统并由发布系统处理的信息应得到完整、准确和及时的处理。
- 在数据采集的过程中和存储的时候,敏感的信息应得到保护。
- 访问发布系统时不允许对与其相连接的网络进行额外访问。

7) 其他形式信息交换中的完整性和真实性

应当有适当的流程和控制措施,对通过声音、传真和视频通信设备等进行的信息交换加以保护。由于缺乏安全意识和必要的安全措施,使用这些设备的策略或流程可能导致信息的泄露,例如,在公共场合使用移动电话、语音答录机时会被偷听;对拨号语音邮件系统的未授权访问或使用传真机设备会偶然地将传真错发给别人等。

应当制订一个清晰的策略文件,规定职员在使用语音、传真和视频通信设备时应遵守的流程,这包括:

①提醒职员在打电话时采取适当安全措施,如不暴露敏感信息以避免信息被下列人员偷听或截获:

- 职员周围的人,特别是使用手机的时候。
- 通过并线或其他搭线窃听方式接触电话机或电话线的人,以及使用手机时利用扫描接收器进行监听的人。
- 在受话端的人。

②提醒职员不得在公共场所、开放的办公室或墙壁较薄的房间内谈论保密话题。

③不得在语音答录机上留言,因为这些设备可被非法人员盗听,或由于拨号错误而被录制到不正确的地方。

④提醒职员关于使用传真机所可能导致的问题,即:

- 传真机内存信息被未授权访问。
- 有意无意地对传真机的程序进行修改导致传真发送到别的指定的号码上。

- 由于错误拨号或错误使用传真机内存的号码而把传真内容发送到错误的号码上。

7.3 访问控制

对信息和业务流的访问应从业务需求层面开始进行控制。

7.3.1 访问控制的策略

应对访问控制的需求进行定义并形成文档。每一个用户或用户组的访问控制规则和访问权限都应在访问控制策略文件中明确说明。对用户和服务提供商的访问控制必须根据业务需求进行配置。

访问控制策略应考虑：

- 不同业务应用的安全需求。
- 识别所有和业务应用相关的信息。
- 信息传播和访问授权策略,如信息的安全等级和分类的需求。
- 不同系统和网络之间的访问控制和信息分类策略的一致性。
- 对于被访问的数据和服务进行保护的有关法规和合同条款。
- 在分布式和网络化的环境中利用可用连接类型进行访问的权限管理。

为详细说明访问控制规则,可进一步考虑以下各项：

- 区分必须执行的规则与可选的或有条件才执行的规则。
- 所建立的规则应以“未经明确允许的都是禁止的”默认禁止原则为控制决策,而不是以“未经明确禁止的都是允许的”默认允许原则进行控制。
- 信息标记的变化,包括由信息处理设备自动引起的或是由用户自行决定引起的变化。
- 由信息系统自动引起和管理人员引起的用户许可权的变化。
- 需要管理人员的批准或其他形式的许可才能颁布的规则。

7.3.2 用户访问管理

应有正式的规程来控制对信息系统和服务的访问权分配,以防止对信息系统的未授权访问。该规程应该涵盖用户访问活动期的各个阶段,包括从新用户的注册,到最后不再需要访问信息系统和服务时的注销。在需要分配专有的访问权限或允许用户越过系统控制进行访问的情况下,应给予特别的管理。

(1) 用户注册

应有正式的用户注册和注销规程对多用户信息系统和服务的访问进行授权,控制对多用户信息服务的访问。这一规程应包括：

- 用户使用唯一的用户身份标识符,将用户和其行为联系起来,并使用户为其行为负责,只有在适合于群(组)工作方式的地方,才允许使用组身份标识符。

- 对用户使用信息系统或服务是否获得了系统所有者的授权进行检查,管理人员对访问权限实行个别审批也是适当的。

- 检查所授予的访问权限与业务目标是否一致,并且是否和组织安全策略相一致,访问权限不可危害职责的划分原则。

- 向用户颁发其访问权限的书面说明。

- 要求用户签署一个表明他们已理解访问条件的声明书。

- 确保只有在授权流程完成之后,服务供应商才可以提供服务。

- 保留一份记录所有注册使用该服务的用户的正式名单。

- 对于工作岗位变动或离开组织的用户,应立即取消现有的访问权。

- 定期检查和取消冗余的用户身份标识符和账号。

- 确保冗余的用户身份标识符不分配给其他用户。

应在员工合同和服务合同中包括一些条款,对越权访问等违规行为必须承担的责任进行详细规定。

(2) 特权管理

应对特权(多用户信息系统的功能和设施允许用户超越系统或应用的控制)的分配和使用进行限制和控制。对系统特权的不恰当使用是系统发生故障、造成安全事件的主要原因之一。

多用户系统应该具备由正式的授权过程所控制的特权分配。可考虑如下的步骤:

- 对和系统产品操作相关联的特权,如操作系统、数据库管理系统和每个应用软件的操作特权,以及需要进行特权分配的用户类别都要进行识别。

- 应该在需要的时候才给用户分配特权并只分配最小的特权。也就是说,只在他们需要的时候才分配一个恰好能完成其角色功能的最小特权。

- 应保留授权流程和已分配的特权的记录,在授权过程完成之前,不得授予新的特权。

- 系统例行测试应避免对用户授予特权。

(3) 用户口令管理

口令是证实访问信息系统或服务的用户身份的常用方法,它的分配需要由正式的管理规程来控制。其步骤应是:

- 需要用户签订一份声明,确保个人口令的机密性和组口令只限于组成员之中(这可以包含在雇佣条款和条件中)。

- 在需要用户保留他们自己的口令的情况下,确保向他们提供的口令是安全的和临时性的,用户忘记口令时由系统管理员在通过对用户身份进行鉴别后提供临时口令。

- 需要在安全模式下提供临时口令,避免使用第三方或未受保护(明文)的电子邮件传递口令信息,用户需要对收到的口令进行确认。

存储在计算机内的口令必须以某种形式进行相当的保护。其他用于标识用户身份的技术,比如指纹、签名和硬件标记(如芯片卡),都可用于标识和识别用户的身份,其功能相当于用户口令,但强于口令。

(4) 用户访问权的检查

为了对数据和信息服务的访问进行有效控制,管理人员应该定期地对用户访问权执行检查工作:

- 对用户访问权限定期进行检查(建议6个月为一周期),并在变更后进行检查。
- 特殊访问权的批准更要经常地进行审查,建议3个月为一个周期。
- 定期检查特权分配的情况,以确保分配的特权不被窃取。

7.3.3 用户职责

防止未授权用户访问是有效安全的基本条件。要求用户必须意识到在维护有效访问控制中的责任,特别是有关用户口令的使用和用户设备的安全保护。

(1) 口令的使用

口令提供了确认用户身份的一种方法,从而确认对信息处理设备的访问权。建议所有的用户做到:

- ① 保护口令的机密性,不以任何形式将口令泄露给其他人。
- ② 避免将口令信息记录在纸上和信息处理设备上。
- ③ 如有迹象表明系统或口令受到危害,则应立即更改口令。

- ④ 选择字符足够长的高质量口令,并尽量做到:

- 便于记忆。
- 不要使用与个人有关的信息作为口令,如名字、电话号码和生日信息等。
- 不要采用连续是同一字符或全是数字或全字符群的口令。

- ⑤ 定期或基于访问次数更改口令,特权账号的口令更要频繁更换,避免重新使用或循环使用口令。

- ⑥ 第一次登录时即更换系统管理员为用户设置的个人口令。

- ⑦ 不要把口令包含在任何自动登录的程序中,例如保存在宏或功能键中。

- ⑧ 不要共享个人口令。

如果用户需要访问多项服务或平台,则建议用户对所有服务使用唯一的高质量口令,这样做可能比使用多个质量不高的口令更好一些。

(2) 无人值守设备管理

对无人值守的设备必须有周密的保护。在用户区所安装的设备,如工作站或文件

服务器,当长时间无人值守时,针对未授权访问需要有特殊的保护措施,要使用户和承包商意识到保护无人值守设备的安全要求和流程,以及他们在实施这种保护时的责任。建议用户做到:

- 除非有适当的锁定机制(如屏保口令)保护,设备使用完后应终止活动的进程并予以关闭。
- 进程结束之后,应从主机上注销并退出系统(不仅仅是关闭个人计算机终端)。
- 通过键盘锁或类似办法避免对个人计算机或终端的未授权使用,如口令保护。

7.3.4 网络访问控制

保护网络服务,控制对内部网络和外部网络服务的访问。为了确保访问网络和网络服务的用户不会危害到这些网络服务的安全性,要确保:

- 在组织内部网络和其他组织的网络以及公共网络之间有合适的接口。
- 对用户和设备有适当的鉴别机制。
- 控制用户对信息服务的访问。

(1)使用网络服务策略

和网络服务的不安全连接将会影响到整个组织。用户只可以直接或间接访问已经明确授权访问的服务。这种控制对于连接到敏感的或关键性的业务应用软件或连接到高风险区(如在组织安全管理和控制之外的公共或外部区域)的用户特别重要。

应制订有关使用网络和网络服务的策略,其中包括:

- 允许用户访问的网络和网络服务。
- 对可以访问不同用户的网络和网络服务的内部或外部授权规程。
- 确保对网络连接和网络服务的管理控制与规程。

该策略要和业务访问控制策略保持一致。

(2)强制访问路径

应控制从用户终端到计算机服务的通信路径。网络设计的基本出发点是允许最大范围的资源共享和路由的灵活性,但这种特点也给未经授权的访问业务应用软件和使用信息设备提供了机会。对用户终端和允许它们访问的计算机服务之间的路径进行控制,是减小访问风险的有效方法之一。

强制控制路径的目的是防止用户在用户终端和其已被授权的服务之间的路径以外选择路径,这需要在路径的不同节点上实施一系列的控制措施。其原理是通过事先选定的路径来限制在网络中每个节点上的路由选项。

(3)外部接入的用户鉴别

用户从外部接入网络可能对业务信息进行未授权的访问,如拨号方式的访问。因此,远程用户的连接访问必须经过身份鉴别。鉴别方法有不同的类型,通过风险评估

来决定鉴别方法的选择原则。

对远程用户的鉴别可以使用(如基于加密技术的)硬件令牌或质询/响应协议来实现。专用线路或网络用户地址检验设备也可以用来提供对连接源地址的鉴别。

对回拨过程进行控制,如使用回拨调制解调器,可以防止对组织信息处理设备的未授权和不需要的访问。这种控制措施可以识别企图在远程站点和组织的网络之间建立连接的用户。在使用此类控制措施时,组织不得使用含有呼叫转接的网络服务,必须禁止使用呼叫转接功能,以避免由此带来的隐患。回拨过程必须保证在组织一方可以中断连接,否则,远程用户可以保持线路的持续开放,而在第二次回拨时不必进行回拨鉴别,否则是很危险的。对于这种可能性,回拨过程和控制措施要进行彻底的测试。

(4)节点鉴别

自动连接到远程计算机的功能为业务应用的未授权访问提供了途径,因此对远程计算机的连接要进行鉴别。如果连接所用的是组织安全管理控制之外的网络,对其鉴别则尤为重要。节点鉴别可以作为验证连接到安全的、共享的计算机设备的远程用户群的可选方法。

(5)远程诊断端口保护

对诊断端口的访问必须严格控制。很多计算机和通信系统都配备有维修工程师所用的拨号远程诊断设备,如果不加以保护和控制,这些诊断端口则提供了未授权且权限很高的访问的途径。因此,应有适当的安全机制来进行保护,如使用键锁和严格的管理规程,以确保只有计算机服务管理人员和要求访问的软硬件支持人员在得到授权后才可以访问这些端口。

(6)网络的隔离

由于所建立的业务合作关系需要信息处理或网络设备的互连或共享,网络正日益扩展到组织的传统边界之外。这种扩展增加了对现有使用网络的信息系统的未授权访问的风险,其中有一些网络由于本身的敏感性或重要性,需要对来自其他网络用户的入侵进行防范。

控制大型网络安全的一种方法就是把网络划分成若干逻辑网络域,如组织内部的网络域和外部网络域。每一个网络域对所定义的安全边界进行保护,可通过在相连的两个网络之间安装安全网关来控制其间的访问和信息流。安全网关要经过配置,以过滤两个区域之间的通信流和根据组织的访问控制策略阻塞未授权访问。这种网关的一个典型例子就是防火墙,特别需要的场合可采用网络物理隔离设备一类的设备在物理层进行隔离。

将网络隔离成子网域的准则是根据访问控制策略和访问需求,并适当考虑成本和由于隔离对网络路由或网关技术性能的影响来制定的。

(7) 网络连接控制

对于共享的网络,特别是跨越了组织边界的网络的访问控制策略,要求包括有限制用户连接容量的控制措施。这种控制措施的实施是通过网关预先定义的路由表或路由规则来过滤通信。所实行的限制措施应基于业务应用的访问策略和需求,因此要进行维护和更新。

应施加限制措施的应用例子有:

- 电子邮件。
- 单向文件传输。
- 双向文件传输。
- 交互式的访问。
- 与时间或日期相关的网络连接。

(8) 网间的路由控制

共享的网络特别是扩展到组织边界之外的网络,需要路由控制措施来确保计算机的互连和信息流不会违背业务应用的访问控制策略。对和第三方(非本组织)用户共享的网络,这种控制措施是必须的。

路由控制应基于明确的源地址和目的地址检查机制。网络地址转换对于网络隔离和防止路由从一个组织的网络扩展到另一个组织的网络是一种很有效的机制。该功能可在软件和硬件上实现。实施时应意识到所采用机制的控制强度。

(9) 网络服务的安全问题

可用的大范围的公共网络和专用网络的服务,其中有一些提供了增值服务。网络服务具有独特、复杂的特点,使用网络提供服务的组织必须提供一个对所使用服务的安全规则的清晰描述。

7.3.5 操作系统访问控制

应对使用操作系统的权限进行限制从而实现对计算机资源的访问控制,以防止对计算机的未授权访问。这些措施应该做到:

- 识别和验证身份,如有必要,对每个授权用户的终端或地点也进行识别和验证。
- 记录成功的和失败的系统访问。
- 提供适当的鉴别方法,如果使用口令管理系统,应确保使用高质量的口令。
- 一般情况下,限制用户的访问次数。
- 其他的访问控制方法,例如质询/响应也可采用。

(1) 自动终端标识

对到特定站点和到移动设备的连接进行鉴别时应考虑自动的终端标识。如果会话只能由特定的站点或计算机终端发起,就能够使用这种自动终端标识技术。放在终

端内或连接到终端上的标识符可用于指示此特定的终端是否允许发起或接收特定的业务。需要对终端实施物理保护,以维护终端标识符的安全。

(2) 终端登录流程

对信息服务的访问只有通过安全的登录流程才是允许的。计算机系统的登录流程应设计成尽量减小未授权访问的可能性。因此,登录流程应尽量少地泄漏系统信息,以避免为未授权用户提供不必要的信息。一个好的登录流程应该是:

- ①不显示系统或应用的鉴别设备,直到登录流程成功完成。
- ②显示一般通知信息,提示用户该计算机只接受已经授权的用户访问。
- ③在登录过程中,不提供帮助未授权用户的信息。
- ④在完成所有的登录输入数据时,才对登录信息的有效性进行证实。当发生错误时,系统不提示数据出错的位置和值。
- ⑤限制所允许的不成功登录企图次数(建议为3次),并考虑:
 - 记录不成功的登录尝试。
 - 在进一步的登录尝试之前,应强制一个时间延迟,或是拒绝没有特定授权的进一步尝试。
 - 必要时断开数据链路连接。
- ⑥对登录流程限制最大和最小时间,如果超时,系统则终止登录过程。
- ⑦在成功的登录流程完成之后,记录如下信息:
 - 上次成功登录的日期和时间。
 - 从上一次成功登录以来不成功的登录尝试的详细情况。

(3) 用户识别和鉴别

所有的用户,包括技术支持人员,如操作人员、网络管理人员、系统程序员和数据库管理人员,都应有为本人使用的唯一的用户标识,以对用户行为进行跟踪。用户标识符不应显示特权级别用户的任何线索,如管理员、超级用户。

在有明显共同利益的例外情况下,对用户群或特定的作业可以共享一个用户标识符。管理部门对此种情况要以文件形式审批。为了维持对责任的审查,可能需要有额外的控制措施。

不同的鉴别流程可用来验证用户所声称的身份。口令则是在只有用户知道的基础上,用于识别和鉴别的最常用的方法。使用加密技术和鉴别协议同样可以证实用户身份。

用户拥有的记忆标记或智能卡一类的实物,以及利用个人的特征和属性的生物学鉴别技术都可用于识别和鉴别用户身份。组合使用安全连接技术将使鉴别更强。

(4) 口令管理系统

口令是用来证实用户访问计算机信息系统服务的权力标志的常用方法之一。口

令管理系统应该提供有效的、交互的功能,以确保口令的质量(见第 7.3.3 节中“口令的使用”)。

一些应用要求有独立的权力机构来分配用户口令。大多数个人终端特别是未连入网络中的计算机,口令的选择和维护都是由用户来进行的。

好的口令管理系统应该是:

- 使用个人口令,以维持责任分割原则。
- 适当的情况下,允许用户选择和更换自己的口令,并包括一个允许在选择和更换口令过程中输入出错的确认流程。
- 选择高质量口令。
- 用户定期更换口令。
- 用户选择口令时,强制第一次登录时即更改系统的默认口令或临时口令。
- 保留一份以前的用户口令记录,如前 12 个月的记录,以防止重用。
- 输入口令时屏幕上不要显示口令字符(值)。
- 将口令文件和应用系统数据分开保存。
- 使用单向加密算法加密存储口令。
- 在软件安装后,改变厂商的默认口令。

(5) 系统工具的使用

多数的计算机安装过程都有一套或多套可以超越系统和应用程序控制的系统工具软件,限制和控制其使用是很重要的。应考虑以下的控制措施:

- 对系统工具实施鉴别流程。
- 将系统工具和应用软件隔离开。
- 将对系统工具的使用限制在尽可能少的可信任的授权用户。
- 对系统工具的特殊使用进行授权。
- 限制系统工具的可用期限,如授权变动的持续时间期限。
- 记录对系统工具的使用。
- 定义和记录系统工具的授权级别。
- 拆除所有不必要的基于软件的工具和系统软件。

(6) 保护用户的强制告警措施

对可能成为强制控制对象的用户应考虑有强制告警措施。是否提供这种告警措施应根据风险的评估结果决定,对强制告警措施的响应根据已经定义的责任和流程进行。

(7) 终端超时

处于高风险区的待用终端,如处于组织安全管理之外的公共的或外部的区域,或提供高风险服务的待用终端,在所规定的无操作状态之后的一定时限后应该关机,以

防止未授权人员的访问。在规定的无操作时间之后,应该自动清掉终端的屏幕,终止应用软件和网络的会话。超时处理应能反映区域和终端用户的安全风险。

可以为一些个人计算机提供终端超时处理的功能及措施,可以清屏和防止未授权访问,但不一定中断应用软件和网络会话。

(8)连接时间限制

限制连接时间可以对高风险的应用提供额外的安全保护,对终端连接到计算机服务所允许的时间进行限制可以降低未授权访问的机会。对于敏感的计算机应用,应该考虑这样的控制措施。特别是高风险区的终端,如处于组织安全管理之外的公共的或外部的区域,更应给予考虑。这种限制措施的例子有:

- 采用预定的时隙,如批文件传输期,或有规则时间的交互式会话期间。
- 如果没有超时或延时的操作,将连接时间限制在正常的处理时间内。

7.3.6 应用系统访问控制

在应用系统内应采用安全设施限制访问,以防止对信息系统内部的信息未授权访问。

对软件和信息逻辑访问应该限制在授权用户中。应用系统应该是:

- 依照定义的业务访问控制策略,控制用户对信息和应用系统功能的访问。
- 对所有可能超越系统或应用控制的工具和操作系统软件进行控制,防止未授权访问或滥用。
- 不危害共享信息资源的安全特性。
- 只有信息所有者、其他获得授权的个人或规定的用户群才能够访问应用系统。

(1)信息访问控制

应该依照规定的访问控制策略,基于不同业务应用的需求,对应用系统用户(包括支持人员)提供访问信息和应用系统功能的权利。为支持对访问的限制需求,应考虑应用下述控制措施:

- 为控制对应用系统功能的访问提供菜单式操作。
- 通过对用户文档进行适当的编辑,限制用户了解没有被授权访问的信息或应用系统的功能。
- 控制用户对信息的访问权,如读、写、删除和执行。
- 确保处理敏感信息的应用系统的输出只包含与使用有关的信息,并只能发送到授权的终端和站点,同时需要对这些输出进行周期性的检查,以确保删除冗余信息。

(2)敏感系统隔离

敏感系统可能要求有专用的(经隔离的)计算环境保护。这就意味着该应用系统应在专用的计算机上运行,只应和可信的应用系统共享资源。应实现下述事项:

- 应由应用系统的所有者对应用系统的敏感性级别进行明确定义,并文档化。
- 在共享的环境中运行敏感应用系统时,应由该敏感应用系统的所有者对与其共享资源的其他应用系统进行安全验证和认可。

7.3.7 监控系统访问与使用

应该对系统进行监控,以发现违背访问控制策略的操作事件和行为,并记录被监控事件,以便于在发生安全事件后提供证据。

系统监控还能对采用的控制措施的有效性进行验证,并证实与访问策略的一致性。

(1) 事件日志

应建立记录意外事件和其他与安全相关事件的审计日志,并按规定保留一段时间,以协助事后的调查工作。审计日志应包括:

- 用户身份标识符。
- 登录和退出系统的日期和时间。
- 终端的身份和位置标识信息。
- 成功的和被拒绝的系统访问尝试的记录。
- 成功的和被拒绝的对数据和其他资源的访问尝试的记录。

可靠的审计日志应作为档案策略的一部分,作为收集的证据并存档以供调阅和分析。

(2) 监控系统的使用

应建立监控信息处理设备使用情况的流程,确保用户只进行被明确授权的操作。不同设备所需的监控级别应根据风险评估来确定。应该进行监控的有:

① 授权访问,包括如下的细节:

- 用户 ID(身份标识符)。
- 关键事件发生的日期和时间。
- 事件类型。
- 被访问的文件、使用的程序和设施。

② 所有的特权操作,如:

- 使用系统管理员账号。
- 系统启动和停止。
- 输入输出设备的连接与断开。

③ 未授权的访问尝试,如:

- 失败的尝试。
- 对网关和防火墙访问策略的违背和通告。
- 入侵监测系统的报警。

④系统告警或故障,如:

- 控制台告警或消息。
- 系统登录异常。
- 网络管理警报告警。

应经常检查监控行为的结果。检查的频繁程度由所涉及的风险来决定。检查因素包括:

- 应用进程的关键程度。
- 涉及信息的价值、敏感性或重要程度。
- 系统被侵袭和误用的历史记录。
- 系统互连的广度(特别是公众网)。

日志审查包括了解系统所面临的威胁和威胁发生的形式。

系统日志通常包括大量的信息,其中很多和安全监控无关。为帮助辨认出对安全监控目的有意义的事件,应考虑将消息进行适当分类并自动地复制到第二层次的日志中,或使用适当的记录设施或工具来执行文件审查工作。

分配日志审查责任时,应考虑在执行审查工作的人员和被监督人员之间进行角色划分。

(3)时钟同步

正确设置计算机信息系统时钟,以确保审计日志的准确性。准确的审计日志是调查所需要的,它是法律事件或违规事件的证据。不准确的审计日志会妨碍调查和破坏这些证据的可信性。

在计算机或通信设备有能力运行网络时钟协议的情况下,时钟应被设置成公认的标准,如世界协调时间(UCT)或当地标准时间。有些时钟会随时间出现漂移偏差,应有流程来检查和矫正一切明显的偏差。

7.3.8 移动计算和远程工作

移动计算和远程连接设施的主管或代管部门(以下简称代理)应该意识到维护一个安全的远程接入网或无线网络是一个连续的过程,它比其他网络和系统需要更多的管理和维护。此外,当使用无线网络连接技术时,更加频繁的评估风险和测试、评估系统安全控制是很重要的,目的是确保使用移动计算和远程连接设施时信息的安全。

维护一个安全的无线网络和相关的设施需要相当大的工作量、资源并涉及以下步骤:

- 对无线网络拓扑的完全理解。
- 为投入运行的无线的和手提式的设施设置标签。
- 经常备份数据。
- 执行无线网络的周期性安全测试和评估。

- 执行持续性的安全保密检查以实施监控和跟踪。
- 应用补丁和安全增强技术维护无线网安全。
- 跟踪无线网络产业技术,提高安全特性的标准和采用新的产品。
- 为防止新的脆弱性和威胁,不断更新无线网络的监控技术。

当前很多的通信协议和商业产品未提供适当的保护,因此代理的操作出现一些不可接受的风险。在部署无线技术之前,代理必须主动应对这些风险以保护其支持必要操作的能力。此外,很多组织在管理无线技术方面还不完善,包括对厂商默认配置或入口控制点等都没有提供合适的安全保护控制,也没有开发和使用适合无线环境的安全机制(例如有线和无线系统之间的防火墙、阻断不需要的服务/端口、使用加密技术等)。在大多数情况下,大部分风险是可以减小的,但减小这些风险要求适当地考虑技术方案和成本代价之间的平衡。

(1) 移动计算

当使用移动计算设备时,如笔记本电脑、掌上电脑和移动电话,必须确保业务信息不被泄漏,应重视使用移动计算设备而带来的风险并制订适当的保护策略,特别是这种使用在未受保护的环境中时。这些保护策略应包括对物理保护、访问控制、加密技术、备份和病毒防护的需求。策略还应包括移动设备连到网络上的安全规则和建议,以及在公共场所使用此类设备的管理原则。

在公共场所、会议室和组织边界之外的其他未受保护的地区使用移动计算设备时,应采用加密技术等对这些设备存储和处理的信息进行保密,避免未经授权访问或泄漏。

同样重要的是,当这些设备在公共场所使用时,应避免未经授权人员的窥视;应有防范恶意软件的流程并定期更新;应快速方便地备份信息,并对这些备份信息给予充足的保护,以防止备份信息的盗用、丢失和损坏。

对于连接到网络上的移动设备,不管是用于办公还是跨过公网远程访问业务信息,都需经过鉴别,并有适当的访问控制机制。

对移动计算设备在办公或运输途中应强调物理保护,以防止被盗或遗忘在汽车等交通工具、旅馆房间、会议中心和会议室里。携带重要的、敏感的或关键性的业务信息的设备必须专人照管,如有可能,应进行物理锁定,或使用特殊的掩护方法来保护设备。

对进行移动计算的员工必须进行培训,提高他们对这种工作方式所引起的额外风险意识,实施控制措施的意识。

(2) 远程接入

远程接入是利用网络通信技术,使员工在组织之外的异地或远程接入本地网络并访问组织内的信息资源。对远程接入站点要给予适当的保护,防止诸如设备和信息的盗用,非授权的信息泄露,对组织内部系统的未授权的远程访问,或对设备的滥用等。

重要的是,管理人员对远程接入的计算设备要进行授权和控制。

组织应考虑制订一种策略、流程 and 标准来控制远程计算和访问活动。只有遵循组织的安全策略进行合适的安全保护和控制,组织才可以授权进行远程接入和访问。采取安全保护和控制措施时应考虑以下因素:

- 远程接入站点应当考虑到其建筑物和当地环境的物理安全。
- 远程工作环境满足技术要求(标准)。
- 通信安全需求应当考虑通过通信连接访问或传播的信息的敏感性,以及组织内部系统的敏感性。
- 其他可能使用到设备的人员,如家属和朋友对信息或资源的未授权访问的威胁。

远程接入的保护和控制措施有:

- 对远程接入的设备和存储工具必须经过审查。
- 规定允许的远程运行业务或操作时间,以及远程工作人员授权访问的内部系统和服务。
- 规定合适的通信设备和安全远程访问的方法。
- 远程站点物理安全。
- 家属和来访者访问设备和信息的规则和指南。
- 软件、硬件支持和维护的规范。
- 备份和业务持续性流程。
- 审计和安全监控。
- 远程接入结束时,撤销授权访问并释放所占用的设备。

7.4 系统开发和维护

7.4.1 系统的安全需求

信息系统包括基础设施、业务应用软件和为用户开发的应用软件。支持应用或服务的业务过程的设计和实施对安全至关重要。在开发信息系统之前,应当识别和确定安全需求。

所有的安全需求,应当在项目需求分析阶段被识别出来并论证其合理性,然后文档化,作为信息系统整体文档资料的一部分。

对于新系统的业务需求或现有系统的业务扩展或变更,应当说明控制措施的需求,将这些需求并入信息系统的自动控制措施,以及支持人工控制措施的方法。

安全需求和控制措施应当反映所涉及的信息资产的价值,以及可能由故障或安全的缺失而导致的潜在业务损失。分析安全需求和识别控制措施是风险管理的重要内

容之一。

在设计时就引入安全控制措施的,其实施和维护的费用要比在实施中或实施后再引入安全措施低得多。

7.4.2 应用系统中的安全

业务应用系统中应当设计有适当的控制措施和审计记录或活动日志,包括书面的操作使用规程,其中有对输入数据、内部处理流程和输出数据的确认。目的是防止丢失、修改或误用应用系统中的用户数据。

对于处理或影响敏感的、有价值的或重要的组织资产的系统,应当根据安全需求和风险评估来确定,是否需要额外的控制措施。

(1) 输入数据的确认

输入应用系统的数据应当确保它是正确的和适当的。为此应当考虑下列的控制措施:

①通过重复输入或其他输入检查方法以检测下列错误:

- 数值长度超过规定的位数。
- 数据字段中的无效字符。
- 丢失的或不完整的数据。
- 超出数据量的上下极限。
- 未授权的或不一致的控制数据。

②定期检查关键字段或数据文件的内容,以确定其有效性和完整性。

③检查所复制的输入文档是否有任何未授权的变更(对输入文档的任何变更都应当经过授权)。

④用于响应输入错误的规程。

⑤用于测试输入数据合理性的规程。

⑥定义在数据输入过程中所涉及的所有人员的责任。

(2) 内部处理的控制

已正确输入的数据可能由于内部处理错误或故意的行为而被破坏。应用软件的设计应当确保将导致数据完整性丧失的处理故障的风险降至最低。要考虑的特殊风险区域包括:

- 在应用程序中设置增加与删除功能以实施对数据的合法合理变更。
- 防止程序以错误的顺序运行或在故障修复前继续运行。
- 使用维护程序从故障中恢复以确保对数据的正确处理。

所要求的检查和控制措施将取决于应用的性质以及数据被破坏对业务的影响,其检查实例可能包括:

- 会话或批处理控制措施。

- 对系统生成的数据的确认。
- 检查中央计算机和远程计算机之间的下载或上传数据或软件的完整性。
- 将记录和文件集中起来统一进行散列处理。
- 检查应用程序是否在正确的时间运行。
- 检查应用程序是否按正确的顺序运行,在出现故障时终止运行,并在问题解决后才继续运行。

(3)消息鉴别

消息鉴别是一种用于检测对传输的电子消息的未授权变更或破坏的技术。它可以通过支持物理消息鉴别的装置或软件算法的硬件或软件来实现。

对于有安全需求的应用软件,应当考虑采用消息鉴别技术保护消息内容的完整性,例如对非常重要的电子资金划拨,或其他类似的电子数据的交换进行完整性检测。进行安全风险评估可以帮助决定是否需要消息鉴别。

消息鉴别并不是设计用来保护消息的内容免受未授权的暴露。加密技术在保护消息不受未授权暴露的同时还可以用来实现消息鉴别。

(4)输出数据的确认

对从应用系统中输出的数据应进行确认处理。对输出数据的确认包括:

- 进行合理性检查以测试输出的数据是否合理。
- 进行一致性的控制计算以确保对所有数据的处理方法是一致的。
- 为信息处理系统提供的信息是准确的、完全的和分类正确的。
- 用于输出数据合法性测试的规程。
- 定义数据输出过程中所涉及的所有人员的责任。

7.4.3 加密控制

用其他的控制措施不足以保护面临泄露或暴露的信息时,应当使用加密系统和技术来保护信息的机密性、真实性或完整性。

(1)使用加密控制措施的策略

决定加密的解决方案是在评估风险后选择控制措施的过程的一部分。首先进行风险评估并决定对信息保护的等级。根据风险评估结果所决定的加密控制措施是否适当,应当应用哪种类型的控制措施以及用于何种目的和业务过程,需要进行综合考虑。

一个组织应当制订一个保护信息而使用加密控制措施的策略。为了实现保护利益最大化,将使用加密控制措施的风险最小化,以及避免加密措施被不适当地或不正确地使用,在制订这种策略的时候,应当考虑如下方面:

- 整个组织针对使用加密控制措施的管理方法,包括总的原则,在这种原则的指

导下,应当对哪些信息进行保护。

- 密钥管理的方法,包括在密钥丢失、泄漏或破坏的情况下,对加密信息恢复的处理方法。

- 角色和责任。
- 策略的实施。
- 密钥的管理。
- 如何决定合适的加密保护等级。
- 所采纳的标准以及对于哪种业务过程使用哪种解决方案。

(2) 加密

加密是一种密码变换技术,它可以用于保护信息的机密性。应当考虑将其用于敏感的或重要信息的保护,切不可滥用。

应当根据风险评估,并考虑采用的加密算法的类型和质量,以及根据保护等级确定适当的密钥长度。

当实现组织的加密策略时,应当考虑世界不同国家和地区对于使用加密技术可能采取的限制规则,以及加密信息跨国界流动的法律性和技术性问题。另外,应当考虑对加密技术和设备进出口的法律控制措施。

确定适当的保护等级应当征求专家的建议,选择的产品必须提供所要求的保护能力以及保证密钥管理是安全的。执行加密措施必须遵循密码技术的法律限制。

(3) 数字签名

数字签名提供一种保护电子文档真实性和完整性的方法。可以在电子业务中验证谁签署了一份电子文档,并检查所签署的文档内容是否被修改过。

数字签名适用于电子化处理的任何形式的文档,例如,签署电子支付凭证、资金的划拨、合同和协议等。可以通过使用公钥密码技术来实现数字签名,这种加密技术以一对唯一相关的密钥为基础,其中的一个密钥(私钥)用来生成签名,而另一个(公钥)用来验证该签名。

应当注意保护私钥的秘密性,因为任何有权访问该密钥的人都能够签署文档,例如支票、合同,从而伪造该密钥持有人的签名。另外,需要通过使用公钥的鉴别来保护公钥的完整性。

需要考虑所使用的签名算法的类型和质量以及所使用的密钥的长度。用于数字签名的密钥应当区别于用于加密的密钥。

当使用数字签名时,应当考虑法律限制,相应的法律条款描述了数字签名在什么条件下才具有法律约束力,因此,在应用中,了解数字签名的法律地位是很重要的。

(4) 抗抵赖服务

抗抵赖服务用于解决关于一个事件或行为出现或未出现的争端,例如,涉及在电

子合同或支票上的数字签名的争端。抗抵赖服务能够帮助建立证据以证明一种特定的事件或行为是否确实发生以及发生的内容,例如,否认使用电子邮件发送过信息以及发送的内容。抗抵赖服务是以数字签名技术为支撑的。

(5) 密钥管理

密钥管理是加密技术有效使用的必要条件。密钥的任何泄漏或丢失都可能导致信息的机密性、真实性/完整性的损害。应当有适当的管理系统来支持组织对秘密密钥技术和公钥技术的使用。

对秘密密钥技术而言,两个或更多的当事方共享相同的密钥,并且该密钥既可用于加密信息,也可用于解密经过加密的信息。显然,这种密钥是对称的。该密钥必须被秘密地保存,因为任何有权访问该密钥的人都能够解密用该密钥加密的所有信息,或引入非法的信息。

对公钥技术而言,每一个使用者都有一对密钥,包括一个公钥(可以透露给任何人)和一个私钥(必须秘密地保存)。公钥技术可以用于加密和生成数字签名。这种密钥是不对称的。

应当保护所有的密钥,防止修改和破坏,需要保护秘密密钥和私钥,防止未授权的泄露。加密技术也可以用于保护密钥,而物理保护方法则可以保护产生、存储密钥和将密钥存档的设备。

为了减少密钥泄漏的可能性,密钥应当规定有效期和失效期。时间段的长短应当取决于加密的控制措施适用的环境以及已识别到的风险。

除了对秘密密钥和私钥进行安全管理之外,也应当考虑对公钥的保护。

与加密服务的供应商(如与一个证书机构)所签订的服务协议或合同的内容,应当包括责任、服务的可靠性和对服务提供的相应时间。

7.4.4 与工程有关的系统文件安全

应当控制对某些系统文件的访问,确保以一种安全的方式实施信息技术项目和工程支持活动。

维护这些系统文件的完整性应当由用户功能或应用系统或软件所从属的开发组负责。

(1) 操作系统软件的控制

应当对操作系统软件的操作进行控制。为了最大限度降低操作系统损坏的风险,应当考虑下列的控制措施:

- 对操作系统程序库的更新只能根据适当的管理授权并由指定的程序库管理员进行。
- 如有必要,操作系统只保留执行代码。
- 在证实测试成功和用户接收之前,以及相应的程序资源库被更新之前,在操作

系统上不应运行可执行代码。

- 应保留所有操作系统程序库的更新检查的审计日志。
- 应当保留更新或升级前的软件版本作为临时应变的恢复措施。

对运行中操作系统上的由销售商供应的软件的维护,必须保持在供应商所要求的级别上。对升级到新版本的任何决定都应当考虑该版本的安全性,例如,新的安全功能的引入或影响该版本的安全问题的数量和严重性。如果软件的修补能够有助于消除或减少安全的弱点,那么就应当进行应用程序的修补。

在必要的时候,经管理层的批准,出于支持的目的才给予供应商在物理或逻辑上的访问权,同时应当监控并记录供应商的维修或访问活动。

(2) 系统测试数据的保护

测试数据应当受到保护和控制。系统接受测试通常要求尽可能接近于实际操作数据的大量测试数据。应当避免使用含有个人信息的操作数据库,并使用下列控制措施保护操作数据:

- 适用于应用系统的访问控制过程也应当适用于操作系统测试。
- 操作信息每次被复制到一个测试应用系统的时候都应当有单独的授权。
- 测试完成后,应当立即将操作信息从测试应用系统中清除。
- 应当记录操作信息的复制和使用情况,以供审计跟踪。

(3) 对程序资源库的访问控制

为了减少计算机程序被破坏的可能性,应对程序资源库的访问有严格控制。

- 程序资源库不应保存在操作系统中。
- 为每一种应用指定程序库管理员。
- 信息技术支持人员不应当具有对程序资源库不受限制的访问权。
- 开发或维护中的程序不应保存在程序资源库中。
- 程序资源库的更新和向程序员发布的程序应由指定的程序库管理员根据信息技术支持者对应用的授权来完成。
- 程序清单应保存在一个安全的环境中。
- 应保存对程序资源库访问的所有日志记录。
- 对程序资源库的维护和复制应当依从严格的变更控制流程。

7.4.5 开发和支持进程的安全

应当严格控制项目的开发环境和支持环境,维护应用系统软件开发的信息安全。

负责应用系统的管理人员应当负责项目开发或支持环境的安全。他们应当对系统更改进行审核,以确定没有危害系统或操作环境的安全问题。

(1) 变更控制流程

为了将信息系统的损坏减至最小,应当对变更的实施进行严格的控制。应当加强

变更控制流程的规范性,确保安全和控制流程不被损害。从事技术支持的程序员只能访问他们的工作所必需的那些系统部分,并应当获得对于任何变更的正式的协议。对应用程序的变更可能要求操作环境同时变更。在可能时,都应当整合应用程序和操作系统变更控制流程。这个过程应当包括:

- 保留一个协商一致的授权级别的记录。
- 确保变更是由授权的用户提交的。
- 检查控制措施和整合变更流程,以确保它们不会因变更受到损害。
- 识别所有需要修改的计算机软件、信息、数据库实体和硬件。
- 在变更开始之前,获得对详细变更建议的正式批准。
- 确保授权的用户在任何实施之前接受变更。
- 确保变更过程中业务受到的损失最小化。
- 确保在完成每次变更时建立更新的系统文档,并将旧文档存档或销毁。
- 保持对所有软件更新的版本控制。
- 保持对所有变更请求的审计跟踪。
- 确保对操作文档和用户操作流程的必要和同步的变更。
- 确保变更的实施不干扰所涉及的业务过程。

许多组织维护了一个用户与开发和生产环境相隔离的测试新软件的环境。这就提供了可以对新软件进行控制的方法,并允许对用于测试目的的操作信息进行额外的保护。

(2)对操作系统变更的技术检查

有必要定期变更操作系统,例如安装新版本或补丁程序。当变更出现的时候,应当检查和测试应用系统,以确保对于操作或安全没有负面的影响。这个过程应当包括:

- 检查应用控制措施和整合变更流程,以确保它们没有受到操作系统变更的损害。
- 确保年度支持计划和预算涵盖了由操作系统变更所导致的检查和系统测试所需的人力和财力资源。
- 确保及时提供操作系统变更通知,以便在实施之前进行现状检查。
- 确保对业务持续性计划进行适当的同步变更。

(3)对软件包变更的限制

一般不鼓励对软件包的修改,因为销售商所提供的软件包应当是尽可能不修改就能够使用。确需修改软件包时,应当考虑如下几点:

- 软件包内置的控制措施和程序调用过程被损害的风险。
- 是否应当获得销售商的同意。
- 从厂商那里获得作为标准程序更新所要求的变更的可能性。

- 组织由于软件的变更而对将来的维护责任所造成的影响。

如果认为有必要变更,则应保留原始软件。所有的变更应经过充分的测试并形成文档,以便在必要时可以作为原版软件的升级版本。

(4) 隐蔽信道和木马程序代码

隐蔽信道可以通过某些间接的和模糊的途径泄露信息。它可以通过改变计算机系统的安全和不安全部件访问的参数,或通过将信息嵌入信息流中而被激活。特洛伊代码被设计成以一种未被授权且不易被发现的不是程序接受者或用户所要求的方式对系统进行操作。隐蔽信道和木马程序代码不是疏忽或偶然出现的,而是一个故意行为。在那些担心隐蔽信道或木马程序代码的地方,应当考虑如下措施:

- 从信誉好的供应商处购买正版软件。
- 购买源代码程序以便验证。
- 使用评估过的产品。
- 在进行操作使用前,检查所有的源代码。
- 代码一旦被安装,就需要控制对代码的访问和修改。
- 使用可靠的职员操作关键的系统。

(5) 外包的软件开发

软件开发外包时,应当考虑如下措施:

- 确认代码的所有权和知识产权。
- 审查外包开发商的资质条件和开发进度的精确度。
- 对开发质量进行控制。
- 用契约方式对代码质量提出明确要求。
- 在安装之前进行测试以检测木马程序代码和软件缺陷。

7.5 业务持续性管理

为了维持业务持续性,应通过预防和灾难恢复控制措施相结合的模式将灾难和安全事件引起的业务中断和系统破坏减少到可以接受的程度,保护关键的业务过程免受故障或灾难的影响。

应当分析灾难、安全事件和服务丢失的后果,制订和实施突发事件应急计划,以确保业务过程可以在预期的时间期限内恢复。该计划应受到维护并予以实施,使之成为整个管理过程的组成部分。

业务持续性管理还应当包括识别和减少风险、限制破坏事件的后果,以及确保主要操作及时恢复的各种控制措施。

7.5.1 业务持续性管理

应当有一个适当的管理过程用于开发和维护整个组织的业务持续性。应当将下列业务持续性管理的关键要素组合在一起：

- 在分析和评估风险发生的可能性及其影响的基础上,理解组织的重要业务和应用系统所面临的风险。
- 识别业务中断对组织可能产生的影响,找到处理较小事件和威胁组织生存的严重事件的解决办法。
- 考虑购买适当的保险,并将其纳入业务持续性管理的组成部分。
- 将与组织的发展策略保持一致的业务持续性策略规范化和文档化。
- 定期测试和更新处于适当阶段的计划和过程。
- 确保业务持续性的管理并入组织的管理过程和管理结构,协调业务持续性管理过程的责任应当在组织(如信息安全管理委员会)内以适当级别进行分配。

7.5.2 业务持续性和影响的分析

从识别可能引起业务过程中断的事件开始,如设备故障、洪灾和火灾等事件开始,随后进行风险评估,以确定业务中断造成的影响(根据破坏的规模和恢复的时间)。进行这两项活动时,都应有业务资源和过程管理的所有者的普遍参与。

应当根据风险评估的结果,制订一个策略计划,以决定业务持续性的总体处理方法。计划制订后应当得到管理层的认可。

7.5.3 制订和实施持续性计划

应当制订计划,以便在关键的业务过程中断或出现故障之后的期望时间范围内,维护或恢复业务运营。业务持续性计划管理过程应当考虑如下几点：

- 识别并一致同意所有的责任和应急流程。
- 实施应急流程,以便在期望的时间范围内恢复业务。
- 将拟定的流程和过程文档化。
- 在拟定的包括危机管理的应急流程和管理过程中对职员进行培训教育。
- 测试和更新计划。

计划的处理应当集中于组织的业务目标,例如,在一个可以接受的时间范围内,恢复对客户的特定服务。

7.5.4 业务持续性计划框架

维护一个独立的业务持续性计划框架,可以保证所有计划的一致性,以及测试和维护的优先顺序。每一个业务持续性计划都应当明确规定执行的条件,以及执行每一

部分计划的负责人,当新的需要出现时,应当修正已建立的应急流程,例如,疏散计划或任何转移安排。

业务持续性计划框架应当考虑如下几点:

- 启动计划的条件,描述每一个计划启动之前所应遵照的规程。
- 应急流程,描述在事件发生后应采取的行动,包括公共关系管理的安排以及与适当的公共权威机构,如与公安局、消防队和当地政府等的有效联络。
- 转移流程,描述将必要的业务活动或支持服务转移到预备的临时位置,并在要求的范围内,使业务过程恢复要采取的行动。
- 恢复流程,描述恢复到正常的业务运营要采取的一系列行动。
- 维护时间表,规定如何和何时测试该计划以及维护该计划的过程。
- 意识教育和培训活动,使有关人员理解确保该业务持续性计划得以有效实施的过程和规范。
- 个人职责,描述执行各部分计划的负责人,应当按照要求指定候选人。

每一个计划都应当有一个特定的负责人。应急流程、转移计划和恢复计划都应当在适当的业务资源或有关的业务过程的负责人的责任范围之内。对于技术服务的安排,诸如信息处理和通信设施等的技术支持,通常应当是服务供应商的责任。

7.5.5 测试、维护和再评估业务持续性计划

(1) 测试计划

业务持续性计划在测试的时候可能失败,这常常是由于不正确的条件假定、疏忽或人员变动所造成的。应当定期测试,以确保它们是最新的和有效的。应急恢复小组的所有成员以及其他有关的职员应参与和理解测试计划。

业务持续性计划测试时间表应指明如何及何时测试计划的每一个要素。建议经常测试计划的各部分,使用多种技术对计划的实际运行提供保证。这些包括:

- 对不同方案的桌面测试,通过使用业务中断实例来探讨业务恢复的安排。
- 模拟演练(尤指培训事故或紧急情况之下担任管理职责的人员)。
- 技术恢复测试,确保信息系统能够有效地恢复。
- 在备用的站点测试恢复流程,在远离主站点进行恢复操作时,同时进行业务处理。
- 测试供应商的设备和服务,确保外部所提供的服务和产品符合合同的承诺。
- 完整的演练,测试组织、职员、设备、设施和过程是否能够应付中断。

(2) 维护和再评估业务持续性计划

通过定期的评审和更新来维护业务持续性计划,是确保业务持续性计划有效性的方法。对于没有反映在业务持续性计划中的业务安排应当在该计划的适当的更新中进行维护。变更控制过程应当定期检查整个计划。更新计划的管理包括新设备、操作

信息安全管理指南

系统的升级以及下列的变动：

- 人员。
- 地址或电话号码。
- 业务策略。
- 位置、设施和资源。
- 法规。
- 承包商、供应商和主要客户。
- 工序(增加一些新的或取消一些旧的)。
- 风险(含运行和财务方面的风险)。

附 录



附录 1 信息安全管理检查列表

(只给出示例式样)

参考点		检查范围、目的和提问		检查结果	
检查项	依据标准	条 款	提 问	发现问题	结 论
1.1.1	5.2.1	信息安全策略文档			

附录2 信息安全应知应会培训参考材料

2.1 信息安全 ABC

2.1.1 基本术语

A (Assets, 资产) 信息系统中对一个组织具有价值的任何东西和事物(包括硬件的或软件的、有形的或无形的、货币化的或非货币化的,等等)。

B (Backup, 备份) 信息系统中在出现系统故障或数据丢失、损坏和不可用时,用来恢复系统或数据原样的复制品。

C (Countermeasures and Controls, 对策和控制) 应对安全事件发生后的方针和策略,以及相应的管理和技术措施。

D (Designed Accreditation Authority, 指定的认可机构) 授权系统运行的机构。

E (Ethics, 道德) 依靠信念、教育、社会舆论和传统习惯等,对人与人和人和社会之间的关系进行规范和调整的准则的集合。

F (Firewalls, 防火墙) 用于隔离网络并实施基于访问策略的控制的设备或设施。

G (Goals, 目标) 信息系统或信息数据的机密性、完整性和可用性(CIA)。

H (Hackers/Crackers, 黑客/骇客) 利用信息系统或组件的缺陷或漏洞对信息系统或组件实施渗透、入侵和攻击的群体。

I (Individual Accountability/Responsibility, 行为的可确认性/责任) 对每个操作行为的来源进行追溯并确定行为者身份的能力。

J (Job Description/Job Function, 作业描述/作业职能) 用于定义个人在组织内的角色。

K (Keys to Incident Prevention, 防范事件的关键) 安全意识、遵从性和安全知识。

L (Laws and Regulations, 法律法规) 建立基本控制/安全目标必须遵循的法制性规范集。

M (Model Framework, 培训模型框架) 与角色和责任相关的培训需求、策略、规划、方案和流程的轮廓。

N (Need to Know, 应知) 为培训和学习制订的理论知识和方法的基本要求集。

O (Ownership, 所有权) 资产的拥有权限。

P (Policies and Procedures, 策略和规程) 需要完成某一目标的方法和途径,以及实现这一策略的符合逻辑的规则集。

Q (Quality Assurance/Quality Control, 质量保证/质量控制) 保证过程一致性和完整性等的一系列规范和措施。

R (Risk Management, 风险管理) 综合平衡不利影响和安全措施成本的管理和技术活动。

S (Security Training, 安全培训) 对安全应知应会知识进行灌输和训练。

T (Threats, 威胁) 利用信息系统或组件的缺陷或漏洞进行未经授权活动的主观因素和能力。

U (Unique Identifiers, 唯一标识符) 标明身份的不与任何第三方实体属性参数相同的数字或符号集合。

V (Vulnerabilities, 脆弱性) 可被威胁利用的系统或组件的缺陷或漏洞。

W (Waste, Fraud, and Abuse, 浪费, 欺骗和滥用) 对系统造成威胁的三种最基本影响方式。

X (Expect the unexpected, 未雨绸缪) 对可能发生的事件进行预测分析, 并对不期望事件采取预案措施。

Y (You, 你) 在谈及安全问题时, 与谈论主体形成会话体系的基本要素。

Z (Zone/Compartmentalization, 区域/分区) 利用物理和逻辑方法将一个结构完整的区域分离成两个(或以上)的具有某种相同属性特征的层次化或类别化的更小一些的区域。

2.1.2 信息安全基本术语详解

资产 (Assets) 资产是指具有一定价值、需要保护的东西。资产的价值可能是可以用货币值衡量的, 也可能是不能用货币值衡量的; 可能是有形的, 也可能是无形的。例如, 计算机软硬件可以直接标价, 也可以按照获取或代替该资产所需成本来换算。然而, 数据则可以用币值衡量(取得数据所需费用), 也可能是不可用币值(使公众对数据的精确性失去信任)衡量的, 或二者兼备; 又如, 信息系统的基础设施(如设备、电缆等)是具有物理形态的资产, 而一个组织的信誉、形象则是无形的资产。

备份 (Backup) 对基本数据/进程的动态数据进行备份在任何信息系统运行环境中都是关键的安全措施之一。备份的概念包括创建和试验从灾难中恢复及可持续性运营规划计划, 以及准备数据文件的备份并把它存放在远离危险的地方。

对策和控制 (Countermeasures and Controls) 应对措施、控制和安全措施通常在安全领域被交替应用。它们涉及使用规程和技术来阻止安全事件的发生, 检测正在发生或已经发生的事故, 以及提供对安全事故做出反应或从中恢复的能力。安全措施可能是用户的口令, 关键文件的备份计划, 能将具体的行为与个人关联起来的审计跟踪, 或其他任何一种技术或规程上的手段。

指定的认可机构 (Designated Accreditation Authority) 负责分配资源和授权系统运行的实体或人。资源可能被分配用于解决信息安全问题或其他需要的问题。对于特定信息系统来说, 具有这样权限的实体为指定的认可机构、审批机构、授权者、推荐者或组织所特有的其他实体。这种具有分配资源权限的实体在做出决定时同样应负责平衡风险和成本以及接受残留风险。认可机构在做出这些决定时, 一般需要证书机构 (CA) 的帮助, 以便提供当前安全环境中足够的技术评估, 以及为解决缺陷和不足提供建议。

道德规范 (Ethics) 行为规则的集合。它是个人或社会活动经验的产物, 是一个基础性的为大多数人所公认的共识, 在做决定时用来判断对与错。遗憾的是, 在当今开放互连网络环境下, 道德规范是会因环境而变化的(如个人对是与非的定义依赖特定的情况而变化)。例如, 某人可能认为闯入别人的房间是错误的, 但却不认为动用别人的计算机系统是错误的。

防火墙和职责分离 (Firewalls and Separation of Duties) 防火墙和职责分离是两个不同的概念, 但却具有相似的功能结构和互补的目的: 防火墙是一种技术安全措施, 它提供活动、系统或系统部件之间的分离, 以便将安全事故或缺陷予以抑制, 且对其他活动或系统没有影响(如实施将局域网与因特网的隔离); 职责分离同样提供分离和隔离, 但它的目的是保证没有一个独立个体(单独行动)可以穿透应用系统。在这两种情况里, 程序上的和技术上的安全措施用来加强基础安全策略, 那么高风险的活动就会通过风险活动的分离而得到控制, 以及单个人不可能穿透整个应用系统。

目标 (Goals) 信息安全活动计划的目标可以用三个词来概括: 机密性, 即数据必须保护以防未

授权泄密;完整性,信息系统不允许进程和数据的未经授权改变;可用性,必须保证提供对信息系统的授权访问的服务水平和能力。

黑客/骇客(Hackers/Crackers) 术语“黑客”是一个杜撰的词汇,最初指这样的群体,他们关注于学习一切所能得到的关于信息技术的知识,特别是那些为此而“忘我”或“废寝忘食”的人。“骇客”则是指任何使用先进的网络或因特网知识危害网络安全的个人。通常,传统的黑客侵入信息系统,出于学术上的目的(如学习和演练),由此造成的危害或破坏性结果都是无意的。而骇客是具有主观意识,受某种利益和动机驱使而去危害信息系统安全的个人。通常报纸对黑客/骇客行为的报道很多,而且不加以区分。而实际上更多的安全事件是由授权用户的无意行为造成的,后者往往造成更大的破坏和损失。

行为的可确认性(可追究性)/职责(Individual Accountability/Responsibility) 维护网络和信息系统的运行秩序的一个基本原则就是个人必须对他们的行为负责。如果不遵从和执行这一原则,就不可能成功地对那些有意损害或破坏系统的人提出公诉,或要求那些责任人由于自己的行为造成非期望结果而必须接受安全意识和技术培训。个人责任的概念产生很多安全措施的需求,例如用户标识符、审计跟踪和访问权限规范等。

作业描述/作业职能(Job Description/Job Function) 为了向个人提供作业所必须的培训,为了配备适当的安全措施加强个人责任的确认性,就必须知道每一个人授权执行的功能(如他们在组织中的角色)的情况。有时,这些活动通过正式的或书面描述的作业说明来完成。其他情况下,这类评估基于对所执行职能的分析。

防范事故的关键(Keys to Incident Prevention) 很多信息安全事故是可以避免的,条件是每个人在他们的日常活动中牢记以下三个基本概念:安全意识,个人应该意识到他们用于作业的资产的价值以及相关威胁和脆弱性的本质;遵从,个人必须遵守已建立的安全措施(如磁盘扫描、改变口令、实施备份)和法律性依据;操作常识。

法律法规(Laws and Regulations) 国家已经制定了很多的法律,这些法律为信息安全建立了基本的策略架构,并根据与信息系统应用出现的规则和指导方针的变化而不断扩充。

培训模型框架(Model Framework) (信息安全培训)模型框架描述了与组织内工作职能和角色有关的个人培训需求。该模型框架还包括组织的培训策略、规划、方案和流程的轮廓。

应知(Need to Know) 需要了解的东西涉及两个方面:首先,完成作业所需访问的信息及访问规程;第二,为适应作业的变更需要继续学习的东西。在第一种情况里,对信息和进程的访问仅限于要求完成作业的个人。这种方法将未经授权活动的可能性最小化,而要求个人对与信息系统的使用或维护相关联的威胁和脆弱性的本质进行最大程度的理解。在第二种情况里,要求个人对快速发展的技术特征有必要了解,以便更好地认识信息系统的脆弱性。

所有权(Ownership) 对信息系统或资产的安全职责必须指定到单个的、可辨别的实体以及实体中的个体,为安全事故以及授权访问和使用这些系统资产的责任提供确认性。个人职责和权限的概念通常被称为所有权或管理权。资产(特指数据)所有权通常被保留,甚至是当资产迁移到其他组织时也需保留这种所有权。例如,通过内部税务服务系统使被中央和各省(市、自治区)税务部门所共享的税收数据必须按照内部法规进行保密。

策略和规程(Policies and Procedures) 信息安全措施力图达到特定的控制目标。这些目标被安全策略控制,并按照每个信息系统的实际要求进行设计。规程定义了技术和流程上的安全措施,规程的执行能加强特定的策略。信息安全规程可能在安全计划中编档。

质量保证/质量控制(Quality Assurance/Quality Control) 质量保证和质量控制是用于保证安全措施的一致性和完整性的两个过程。具体地说,这些过程在保证安全策略在全作业负荷和运营条件下,按照规定流程执行是不可缺少的。

风险管理(Risk Management) 风险管理是这样的一个进程,即将脆弱性、威胁和来自安全事故的潜在影响与实施安全措施的成本进行综合平衡。风险管理的目的是保证所有的信息资产得到正当的保护,避免浪费、欺骗、滥用和破坏运营。随着潜在威胁范围增大或可用资源减少,风险管理的重要性愈显突出。

安全培训(Security Training) 安全培训是将大量信息安全相关知识传授给那些使用、维护或管理信息系统的人的过程的总称。一个经过良好培训的职员通常可以弥补技术和过程方面安全措施的缺陷、提高安全技术和安全设备的保护效能。安全培训已被证明会使在任何技术和程序方面的信息安全措施的投资得到最大收益。

威胁(Threats) 威胁是指将导致资源消耗、欺骗、滥用或破坏运营等对信息系统造成影响的(有意或无意的)行为或企图。威胁总是存在的,威胁发生的频度不能被控制。因此,信息安全措施必须被设计成能够阻止或最小化任何针对信息系统的威胁。

唯一标识符(Unique Identifiers) 唯一标识符是指一个代码或一组代码,它们是机构确认个人身份的依据。安全措施必须到位,以保证标识符仅被已指定的个人使用。

脆弱性(Vulnerabilities) 脆弱性是信息系统及组件,以及运行环境中的缺陷和漏洞。威胁可能利用脆弱性给信息系统带来不利影响。安全措施用于减轻或消除脆弱性。

浪费、欺骗和滥用(Waste, Fraud, and Abuse) 浪费、欺骗和滥用是对信息系统及组件潜在的负面影响形式,它们可能由于有意或无意实施不当行为或企图而造成。浪费、欺骗和滥用被明确地认为是安全策略中必须解决的潜在影响。

未雨绸缪(Expect the unexpected) 信息安全措施的功能是对抗未预期或不期望的行为。这些行为(个人行为或外部力量行为)可以有很多形式,并且可以在任何时间发生。因此,安全措施应该足够灵活并有效力,从而对任何偏离预先定义的行为做出确认并启动预案反应。

你(You) 每个人将对自己的行为及相关的信息系统或相关的数据负有责任,并且保持可确认性。每个人的积极性/不作为可以加强或减弱信息安全环境的安全性。比如,你可以通过定期更换口令加强信息安全,也可以从不更换口令而减弱其安全性。

区域/分隔区(Zone/Compartmentalization) 区域和分隔区指将一个环境分隔成若干独立的安全环境的应用。在应用受到损害之前破坏安全的一个地方可能致使两个或多个地方出现故障。这种方法可以应用于与信息系统关联的物理和逻辑环境中对区域之间的关联进行分析。

2.2 信息安全知识主题和概念

2.2.1 法律法规

国家和政府层面的或组织自己制定的有关信息安全的法律、规则、策略、指南、标准和规程是管理和保护信息系统及其资源的强制性要求。

- 国家法律法规
- 国家标准和指南
- 法律和责任问题

- 组织策略、指南、标准和规程
- 组织的活动计划
- 特定的法律问题
- 特定应用系统中的法律问题

2.2.2 信息安全活动计划

一个用于建立、实施和维护信息安全活动的计划应保证组织的信息系统,包括在得到普遍支持的系统和主要应用中采集、处理、传输、存储或发布的所有组织信息,有足够的信息安全。

- (1)组织范围内的信息安全活动计划。
- (2)系统级别的信息安全活动计划。
- (3)信息安全活动计划的要素。
- (4)角色、责任和可确认性:

- 高层管理者
- 组织范围内的信息安全管理
- 活动计划和项目管理员
- 系统/应用所有者
- 信息所有者/托管者
- 信息系统安全管理
- 签约人/合作伙伴
- 相关安全活动计划管理者
- 用户

2.2.3 系统环境

与信息系统运行相关的环境,包括硬件、软件、固件、通信能力、保障能力及其物理环境。

- 信息系统体系结构
- 硬件类型
- 操作系统软件
- 应用软件
- 通信要求
- 设施规划
- 处理流程
- 相关脆弱性
- 相关威胁

2.2.4 系统互连

一个系统和另一个或其他多个系统或网络之间的通信或互连需求,包括在支持多组织的或公共活动计划中的共享处理能力及传递数据和信息的需求。

- 通信类型

信息安全管理指南

- 网络体系结构
- 电子邮件
- 电子业务(商务,政务,农务.....)
 - 业务数据传送
 - 业务数据交换
 - 数字签名
 - 电子签名
- 访问控制(例如,防火墙、代理服务器、专用网关)
- 监控
- 密码技术

2.2.5 信息共享

组织之间信息共享的需求和应用,支持多个内部或外部组织、团体和公共活动计划的信息共享。

- 通信类型
- 网络体系结构
- 电子邮件
- 电子业务(商务,政务,农务.....)
 - 电子业务传送
 - 业务数据交换
 - 数字签名
 - 电子签名
- 访问控制(比如,防火墙、代理服务器、专用网关)
- 监视
- 密码技术
- 数据所有权
- 保护记录数据存储介质

2.2.6 敏感性

信息技术环境包括系统、数据和应用的工作环境,必须受到单独的和整体的检查。所有的信息系统和应用需要一定类别的保护,以保证机密性、完整性和可用性。保护类型和强度通过对所处理信息的敏感度、紧急程度的评估,系统与组织的关系,以及该系统组件的经济价值等因素决定。

- 机密性
- 完整性
- 可用性
- 紧急性
- 聚合

2.2.7 风险管理

信息系统和资源的风险评估过程,作为风险管理的一部分,通过分析其脆弱性和威胁,选择合适

的成本效能换算的控制方法,达到将风险维持在可以接受的水平,从而判断系统安全是否充分。

- 资产评估
- 脆弱性
- 威胁
- 风险
- 不确定性分析
- 风险分析
- 风险评估
- 风险缓解
- 可行性评估
- 资产的适当和充分保护
- 费效比
- 应用业务的安全审计/评审
- 系统的安全审计/评审
- 内部控制审计

2.2.8 管理控制

管理控制指管理系统的开发、维护和使用等的过程控制行为,包括具体的系统策略、过程、行为准则、个人角色和责任、身份可确认性和安全决策。

(1)系统/应用责任:

- 项目和功能管理者
- 所有者
- 托管者
- 签约者
- 相关安全项目管理员
- 信息系统安全管理员
- 用户

(2)系统/应用策略和过程。

(3)标准的执行过程。

(4)个人安全:

- 背景调查
- 岗位敏感度
- 分离/分隔责任

(5)系统规则操作行为:

- 分配和限制系统权限
- 连接其他系统和网络的规则
- 知识产权/版权问题
- 在家进行远程访问/工作问题
- 官方和非官方的系统使用

信息安全管理指南

- 身份可确认性

(6)对违规的约束和惩罚。

2.2.9 操作控制

用来保护运营系统和应用的日常规程和机制。操作控制影响系统和应用环境。

(1)物理和环境保护：

- 物理安全
- 环境控制
- 自然威胁
- 设施管理
- 防火
- 电力/能源供应
- 后勤保障
- 物理访问控制
- 入侵检测/报警
- 维护
- 供水和排水
- 移动和便携式系统的物理环境

(2)生产、输入输出控制：

- 文档标记、处理、运送、存储
- 介质标记、处理、运送、存储
- 敏感材料的处置
- 剩磁的清理和清除

(3)应对意外事故：

- 备份
- 意外事故/灾难恢复计划的开发
- 意外事故/灾难恢复计划的测试
- 签订意外事故服务条约
- 签订灾难恢复服务条约
- 加入保险/自我保险

(4)审计和差错检测：

- 系统日志和记录
- 与标准行为的偏差

(5)硬件和系统软件维护控制。

(6)应用程序的维护控制。

(7)编制文档。

2.2.10 意识、培训和教育控制

(1) 安全意识活动计划是通过培训来改变组织中每个人对信息安全的态度,使其认识到安全的重要性以及安全事故所产生的不利后果。

(2) 培训的目的是教人以技能,以便他们能高效安全地完成自己的工作。

(3) 教育的目标是培养安全专家,着重于开发能力和视野的专业训练,以便完成复杂的、多种学科的信息安全活动。

2.2.11 技术控制

技术控制包括硬件和软件的控制,用以提供对信息系统或应用的自动保护。技术控制运行在技术系统和应用中。

(1) 用户身份鉴别:

- 口令
- 令牌
- 生物统计学技术
- 单点登录

(2) 授权和访问控制:

- 逻辑访问控制
- 基于角色的访问
- 系统/应用的访问权限管理

(3) 完整性/合法性控制:

- 安全规约和需求的遵从性
- 恶意程序/病毒的防护、检测和清除
- 鉴别消息
- 例行的调解过程

(4) 审计跟踪机制:

- 事务监视
- 事务重建

(5) 机密性控制:

- 密码技术
- 访问控制
- 环境的物理控制

(6) 事故响应:

- 欺骗、浪费或滥用
- 黑客和未授权用户行为
- 事故报告
- 事故调查
- 法律诉讼

(7) 公共访问控制:

信息安全管理指南

- 访问控制策略
- 应知应会
- 隐私保护

(8)控制目标:

- 保护的资源
- 保护的需求

附录3 信息安全常见缩略语

AAA	Authentication, Authorization and Accountability	鉴别、权限和可确认性
ACI	Access Control Information	访问控制信息
ACL	Access Control List	访问控制表
ACM	Association for Computing Machinery	[美]计算机协会(联盟)
ACSE	Association Control Service Element	关联控制服务元素
ADC	ADF Combination	ADF 组合
ADF	Access Control Decision Function	访问控制判决功能
ADI	Access Control Decision Information	访问控制判决信息
AEC	AEF Combination	AEF 组合
AEF	Access Control Enforcement Function	访问控制执行功能
AES	Advanced Encryption Standard	高级加密标准
AH	Authentication Header	鉴别头
AI	Authentication Information	鉴别信息
ANSI	American National Standard Institute	美国国家标准协会
API	Application Program Interface	应用程序接口
APP	[NIST]Application Portability Profile	[(美)国家标准和技术研究所]
		应用可移植性轮廓
ARP	Address Resolution Protocol	地址解析协议
ASN.1	Abstract Syntax Notation One	抽象语法表示法 1
A-S/SPEC	Type A-System/Segment Specification	A 型系统/段规范
ASR	Alternative System Review	备选系统评审
ATM	Asynchronous Transfer Mode	异步传送模式
AUP	Acceptable Use Policy	可接受使用策略
B-ISDN	Broadband-ISDN	宽带 ISDN
BP	Base Practices	基本实施
B/SA	Browser/Server-Application	浏览器/服务器应用
B-SPEC	Type B-Development Specification	B 型开发规范
C&A	Certification and Accreditation	认证与认可
CA	Certificate Authority	证书机构
CAALS	Computer Aided Acquisition and Logistics Support	计算机辅助获取和后勤支持
CALS	Continuous Acquisition Life-cycle Support	连续获取生命期支持
CAN	Campus Area Network	社区网,校园网
CC	Common Criteria	通用准则
CCB	Configuration Control Board	配置控制委员会
CCP	Compression Control Protocol	压缩控制协议
CCTL	Common Criteria Test Lab	通用准则测试实验室

信息安全管理指南

CDR	Critical Design Review	关键设计评审
CDRL	Contract Data Requirement List	合同数据需求列表
CHAP	Challenge Handshake Authentication Protocol	质询握手鉴别协议
CI	Configuration Item	配置项
CIA	Center Intelligence Agency	[美]中央情报局
CIITAC	Computer Investigate and Infrastructure Threat Assessment Center	[美]计算机调查与设施威胁评估中心
CLID	Client ID	客户 ID
CM	Configuration Management	配置管理
CMIS/CMIP	Common Management Information Service/Common Management Information Protocol	公共管理信息服务/公共管理信息协议
CMISE	Common Management Information Service Element	公共管理信息服务元素
CMM	Capability Maturity Model	能力成熟度模型
CMOL	Common Management Information Protocol Over Logical Link Layer	逻辑链路层上的公共管理信息协议
CMOS	Complementary Metal Oxide Semiconductor	互补金属氧化物半导体
CMOT	Common Management Information Protocol Over TCP/IP	运行在 TCP/IP 上的公共管理信息协议
CNNIC	China National Network Information Center	中国互联网络信息中心
COEA	Cost and Operational Effectiveness Analysis	成本和运行有效性分析
COMPUSEC	Computer Security	计算机安全
CONOP	Concept of Operation	(客户的)操作概念
COS	Class Of Service	服务类型
COTS	Commercial-Off-The-Shell	商业现货
CSCI	Computer Software Configuration Item	计算机软件配置项
CSMACD	Carrier-Sense Multiple Access with Collision Detection	带冲突检测的载波监听多址存取
C-SPEC	Type C-Product Specification	C 型产品规范
CWBS	Contract Work Breakdown Structure	合同工作细目分类结构
DAA	Designated Approving Authority	指定批准机构
DARPA	Defense Advanced Research Project Agency	[美]国防高级研究规划署
DBMS	Database Management System	数据库管理系统
DCA	Defense Communication Agent	[美]国防通信署
DDN	Digital Data Network	数字数据网
DES	Data Encryption Standard	[美]数据加密标准
DESE	DES Encryption	(微软)加密(协议)
DGSA	DoD Goal Security Architecture	[美]国防部目标安全体系结构
DH	Diffie-Hellman	Diffie-Hellman(公开密码算法)
DID	Data Item Description	数据项描述

附 录

DISA	Defense Information Systems Agency	[美]国防信息系统局
DISA CISS	DISA Center for Information Systems Security	[美]国防信息系统局信息安全中心
DISA CISS/A&E	The Architecture and Engineering Division of DISA CISS	[美]国防信息系统局信息安全中心体系结构和工程分部
DNS	Domain Name System	域名系统
DoD	Department of Defense	[美]国防部
DOI	Domain of Interpretation	解释域
DS	Digital Signature	数字签名
DSSS	Direct Sequence Spread Spectrum	直序扩展频谱技术
DT&E	Development Test and Evaluation	开发测试和评估
DTE	Data Terminal Equipment	数据终端设备
DTS	Data Tracking Sheet	数据跟踪表[单]
EAL	Evaluation Assurance Level	评估保证级
ECP	Encryption Control Protocol	加密控制协议
EDI	Electronic Data Interchange	电子数据交换
E-mail	Electronic Mail	电子函件
ESP	Encapsulation Security Payload	封装安全载荷
ESR	Evaluation Summarization Report	评估总结报告
ETR	Evaluation Technology Report	评估技术报告
FBI	Federal Bureau of Investigation	[美]国家联邦调查局
FCA	Functional Configuration Audit	功能配置审计
FDDI	Fiber Distributed Data Interface	分布式光纤数据接口
FDMA	Frequency Division Multiple Access	频分多址访问(存取)
FHSS	Frequency Hopped Spread Spectrum	跳频扩展频谱技术
FIPS	Federal Information Processing Standard	[美]联邦信息处理标准
FR	Frame Relay	帧中继
FRAD	Frame Relay Assemble/Dissemble	帧中继装/拆(设备)
FSRS	General Functional Security Requirement Specification for a Telecommunications System	远程通信系统一般功能安全需求规范
FTP	File Transfer Protocol	文件传送协议
GIIC	Global Information Infrastructure Committee	全球信息基础设施委员会
GMITS	Guidelines for the Management of IT Security	IT 安全管理指南
GOTS	Government-Off-The-Shelf	政府现货
GP	Generic Practices	通用实施
GRE	Generic Routing Encapsulation	通用路由封装
HCI	Hiding Confidentiality Information	隐藏机密性(的)信息
HDLC	High-level Data Link Control	高级数据链路控制

信息安全管理指南

HGW	Home Gateway	总部网关
IANA	Internet Assigned Number Authority	因特网编号分配机构
IATF	Information Assurance Technical Framework	信息保障技术框架
IC	Smart Card	IC 卡, 灵通卡
ICAM	Integrated Computer and Manufacturing	集成计算机和制造
ICMP	Internet Control Message Protocol	互联网控制消息协议, 因特网控制消息协议
ICV	Integrity Check Value	完整性校验值
ID	Identification	标识
IEEE	Institute of Electrical and Electronic Engineers	[美]电气和电子工程师学会
IETF	Internet Engineering Task Force	因特网工程任务组
IFIP	International for Information Process	国际信息处理联合会
IKE	Internet Key Exchange	因特网密钥交换(协议)
ILS	Integrated Logistics Support	一体化的后勤支持, 综合 的后勤支持
INFOSEC	Information System Security	信息系统安全
InterNIC	Internet Network Information Center	因特网信息中心
IOC	Initial Operational Capability	初始运行能力, 初始操作能力
IP	Internet Protocol	互联网协议
IPCP	IP Control Protocol	IP 控制协议
IPOA	IP Over ATM	通过 ATM 的 IP
IPsec	IP Security	IP(层)安全(协议)
IPSEC	IP Security	互联网(层)安全(协议)
ISA	Industry Standard Architecture	工业标准体系结构
ISAKMP	Internet Security Association and Key Management Protocol	因特网安全关联和密钥 管理协议
ISDN	Integrated Services Digital Network	综合业务数字网
ISMS	Information Security Management System	信息安全管理体制
ISO	International Standard Organization	国际标准化组织
ISP	Internet Service Provider	因特网服务供应商
ISSE	Information System Security Engineering	信息系统安全工程
IT	Information Technology	信息技术
ITSEC	Information Technology Security Evaluation Criteria	信息技术安全评估准则
IV&V	Independent Verification and Validation	独立验证和证实
KDC	Key Distribution Center	密钥分发中心
KMI	Key Management Infrastructure	密钥管理基础设施
KTC	Key Translation Center	密钥转移中心
L2F	Layer 2 Forwarding Protocol	层 2 转发协议
L2TP	Layer 2 Tunneling Protocol	层 2 隧道协议

附 录

LAC	L2TPAccess Concentrator	L2TP 访问集中器
LAN	Local Area Network	局域网
LAP-D	Link Access Protocol-D	数字信道链路接入协议
LCIE	Life-Cycle INFORSEC Engineer	生命期信息系统安全工程
LCP	Link Control Protocol	链路控制协议
LDAP	Lightweight Directory Access Protocol	轻型名录访问协议简单 名录访问协议
LLC	Logical Link Control	逻辑链路控制
LMMP	LAN Man Management Protocol	局域网个人管理协议
LNS	L2TP Network Server	L2TP 网络服务器
LPP	Light-weight Presentation Protocol	轻型表达协议
MAC	Medium Access Control	介质访问控制
MAC	Mandatory Access Control	强制访问控制
MAC	Message Authentication Code	消息鉴别码
MAN	Metropolitan Area Network	城域网
MDII	Modification Detection Integrity Information	变换检测完整性信息
MIB	Management Information Base	管理信息库
MIC	Message Integrity Code	消息完整性编码
MID	Multiplexing ID	复用 ID
MIL-STD	Military Standard	[美]军方标准
MISSI	Multilevel Information Systems Security Initiative	多级信息系统安全倡议
MK	Master Key	主密钥
MNS	Mission (Capability) Needs Statement	任务(能力)要求说明
MP	Multi-link Protocol	多链接协议
MPOA	Multiprotocol over ATM	通过 ATM(实现)多协议传输
MPPE	Microsoft Point to Point Encryption	(微软)点到点加密(协议)
MTBF	Mean Time Between Failures	平均无故障时间
MTU	Maximum Transport Unit	最大传输单元
MVLAN	Main VLAN	主虚拟局域网
NAS	Network Access Server	网络访问服务器
NAT	Network Address Translation	网络地址转换
NCP	Network Control Protocol	网络控制协议
NCSA	National Computer Security Association	[美]国家计算机安全协会
NCSC	National Computer Security Center	[美]国家计算机安全中心
NDI	Non-Developmental Item	非开发项目
NIAP	National Information Assurance Partner	[美]国家信息保证伙伴
NII	National Information Infrastructure	国家信息基础设施
NIPC	National Infrastructure Protection Center	[美]国家设施保护中心
N-ISDN	Narrow-ISDN	窄带 ISDN

信息安全管理指南

NIST	National Institute of Standards and Technology	[美]国家标准和技术研究所
NOS	Network Operating System	网络操作系统
NR-TTP	Non-repudiation-TTP	抗抵赖可信第三方
NSA	National Security Agency	[美]国家安全局
NSF	National Science Foundation	[美]国家科学基金(会)
NSTISSC	National Security Telecommunications and Information Systems Security Committee	[美]国家安全远程通信 和信息系统安全委员会
NSTISSI	National Security Telecommunications and Information Systems Security Instruction	[美]国家安全远程通信 和信息系统安全训令
OA	Office Automation	办公自动化
OAN	Operation Area Network	操作域网,运行域网
ODP	Open Distributed Processing	开放分布式处理
OID	Object identifier	对象标识符
OPM	Office of the Personal Management	人事管理办公室
ORD	Operational Requirements Document	运行需求文档,操作需求文档
OSA	Open Systems Architecture	开放系统体系结构
OSI	Open System Interconnection	开放系统互连
OSI/RM	OSI Reference Model	OSI 参考模型
OSIE	OSI Environments	开放系统互连环境
OT&E	Operational Test and Evaluation	操作测试与评价,运行测试与评价
P3I	Pre-Planned Product Improvement	预计划的产品改进
PA	Process Area	过程区
PAC	PPTP Access Concentrator	PPTP 访问集中器
PAD	Packet Assembler/Disassembler	分组装/拆(设备)
PC	Personal Computer	个人计算机
PCA	Physical Configuration Audit	物理配置审计
PCCIP	The President's Commission on Critical Infrastructure Protection	[美]总统关键设施 保护委员会
PCM	Pulse Code Modulation	脉冲编码调制
PDCA	Plan, Do, Check and Act	规划、实施、检查和改进 (模型),PDCA 模型
PDR	Preliminary Design Review	初级设计评审
PDU	Protocol Data Unit	协议数据单元
PIN	Personal Identification Number	个人标识号,个人身份号
PKI	Public Key Infrastructure	公开密钥基础设施
PM	Program Manager	程序管理员
PMI	Privilege Management Infrastructure	授权/权限管理基础设施
PMO	Program Management Office	项目管理办公室
PMP	Program Management Plan	项目管理计划

PNS	PPTP Network Server	PPTP 网络服务器
POP	Point of Presence	(现场)接入点
POSIX	Portable Operating System Interface for Computer Environments	计算机环境可移植操作系统接口
PP	Protection Profile	保护轮廓
PPP	Point To Point Protocol	点到点协议
PPTP	Point To Point Tunneling Protocol	点到点隧道协议
PSTN	Public Switched Telephone Network	公共交换式电话网
PSV/D-3	Portable Secure Voice/Data III	可移植安全语音/数据 III
PVC	Permanent Virtual Circuit	永久虚电路
PVC	Permanent Virtual Connection	永久虚连接
PVG	Patch and Vulnerability Group	补丁和脆弱性[处理]组
PWBS	Program Work Breakdown Structure	项目工作分类结构
QoS	Quality of Service	服务质量
RAA	(Security) Risk Acceptance Authority	(安全)风险验收[权力]机构
RADIUS	Remote Authentication Dial-In User Service	远程鉴别拨入用户服务
RBAC	Role-Based Access Control	基于角色的访问控制
RCI	Revealing Confidentiality Information	显现机密性[的]信息
RFP	Request for Proposal	请求建议
ROSE	Remote Operations Service Element	远程操作服务元素
RPC	Remote Procedure Call	远程过程调用
RSA	Ronald Rivest, Adi Shamir, Leonard Adleman	Rivest-Shamir-Adleman [加密算法]
RSA	Rivest-Shamir-Adleman	RSA(算法)
RVTM	Requirements Verification Traceability Matrix	需求验证可追踪性模板
SA	Security Association	安全关联,安全联盟
SA	System Acquisition	系统获取
SAID	SA Identifier	SA 标识符
SAPI	Security Application Program Interface	安全应用程序接口
SDA	Security Domain Authority	安全域机构
SDNS	Secure Data Network System	安全数据网系统
SDU	Service Data Unit	服务数据单元
SE	System Engineer	系统工程
SE-CMM	Systems Engineering Capability Maturity Model	系统工程能力成熟度模型
SEDS	System Engineering Detailed Schedule	系统工程详细进度表
SEMP	System Engineering Management Plan	系统工程管理计划
SEMS	System Engineering Main Schedule	系统工程主进度表
SF	Security Function	安全功能
SFA	Security Fault Analysis	安全故障分析

信息安全管理指南

SFP	Security Function Policy	安全功能策略
SFR	System Functional Review	系统功能评审
SI	Security Information	安全信息
SH	Shielded Integrity Information	屏蔽的完整性信息
SKIP	Simple Key-management for Internet Protocol	简单互联网密钥管理协议
SLIP	Serial Line Interface Protocol	串行线接口协议
SMIB	Security Management Information Base	安全管理信息库
SNA	System Network Architecture	系统网络体系结构
SNMP	Simple Network Management Protocol	简单网络管理协议
SOF	Strength of Function	功能强度
SOW	Statement of Work	工作说明,工作陈述
SP	Service Provider	服务供应商
SPD	Security Policy Database	安全策略数据库
SPI	Security Parameter Index	安全参数索引
SPO	System Program Office	系统项目办公室
SQL	Structured Query Language	结构化查询语言
SRM	Security Risk Management	安全风险管理的
SRR	System Requirement Review	系统需求评审
SSAM	Systems Security Engineering Capability Maturity Model (SSE-CMM) Appraisal Method	系统安全工程能力成熟度模型评估方法
SSE	Systems Security Engineering	系统安全工程
SSE-CMM	Systems Security Engineering Capability Maturity Model	系统安全工程能力成熟度模型
SSR	Software Specification Review	软件规范评审
ST	Security Target	安全目标
STAR	System Threat Assessment Report	系统威胁评估报告
STDM	Statistical Time Division Multiplexing	统计时分复用(技术)
STM	Synchronous Transfer Mode	同步传输模式
SVC	Switched Virtual Circuit	交换式虚电路
SVC	Switched Virtual Connection	交换式虚连接
SVR	Security Verification Review	安全验证评审
TAFIM	Technical Architecture Framework for Information Management	信息管理的技术体系结构框架
TCB	Trusted Computing Base	可信计算基
TCP	Transmission Control Protocol	传输控制协议
TCSEC	Trusted Computer System Evaluation Criteria	可信计算机系统评估准则
TDMA	Time Division Multiple Access	时分多址访问
TECNET	Test and Evaluation Community Network	测试与评价社团(共同体)网
TEMP	Test and Evaluation Master Plan	测试与评价主计划

附 录

TEMPEST	Transient ElectroMagnetic Pulse Emanation Standard, Telecommunications Electronics Material Protected from Emanating Spurious Transmissions	瞬态电磁脉冲辐射[标准], 防电磁泄露[技术]
TNG	Trusted Network Guideline	可信网络指南
TOE	Total Operating Expense	总操作(运行)费用
TOE	Target of Evaluation	评估对象
TPM	Technical Performance Measurement	技术性能测量
TRR	Test Ready Review	测试准备就绪评审
TSC	TSF Scope of control	评估对象安全功能控制范围, TSF 控制范围
TSDM	Trusted Software Development Methodology	可信软件开发方法学
TSF	TOE Security Function	评估对象安全功能, TOE 安全功能
TSFI	TSF Interface	评估对象安全功能接口,TSF 接口
TSP	TOE Security Policy	评估对象安全策略, TOE 安全策略
TSP	Telecommunication Service Provider	通信服务供应商
TTL	Time To Live	存活时间
TTP	Trusted Third Party	可信第三方
TVP	Time Variant Parameter	时间变量参数
UDP	User Datagram Protocol	用户数据报协议
UII	Unshielded Integrity Information	去屏蔽的完整性信息
UNI	User Network Interface	用户网络接口
V&V	Verification & Validation	验证与证实
VCC	Virtual Circuit Connection	虚拟电路连接
VLAN	Virtual Local Area Network	虚拟局域网
VPN	Virtual Private Network	虚拟专(用)网
WAN	Wide Area Network	广域网
WBS	Work Breakdown Structure	工作明细结构
WWW	World Wide Web	万维网
xDSL	All Digital Subscribe Lines	全部数字用户线

参考文献

- [1] 国家信息化领导小组. 国家信息化领导小组关于加强信息安全保障工作的意见[Z]. 2003-7-9.
- [2] 公安部,国家保密局,国家密码管理委员会办公室,国务院信息化工作办公室. 关于信息安全等级保护工作的实施意见[Z]. 2004.
- [3] 戴宗坤,罗万伯,等. 信息系统安全[M]. 北京:电子工业出版社,2002.
- [4] 罗万伯,刘嘉勇,戴宗坤,等. 信息安全法律道德规范与管理[M]. 重庆:重庆大学出版社,2005.
- [5] ISO/IEC 13335-1:2004. Information technology-Security techniques-Management of information and communications technology security-Part 1: Concepts and models for information and communications technology security management[S].
- [6] ISO/IEC 13335-2. Information technology-Guidelines for the management of IT Security-Part2: Managing and planning IT Security (2nd WD) [S].
- [7] ISO/IEC TR 13335-3:1998. Information technology-Guidelines for the management of IT Security-Part 3: Techniques for the management of IT Security[S].
- [8] ISO/IEC TR 13335-4:2000. Information technology-Guidelines for the management of IT Security-Part 4: Selection of safeguards[S].
- [9] ISO/IEC TR 13335-5:2001. Information technology-Guidelines for the management of IT Security-Part 5: Management guidance on network security[S].
- [10] ISO/TR 13569:2005. Financial services-Information security guidelines[S].
- [11] ISO/IEC 15408-1:2005. Information technology-Security techniques-Evaluation criteria for IT security-Part 1: Introduction and general model[S].
- [12] ISO/IEC 15408-2:2005. Information technology-Security techniques-Evaluation criteria for IT security-Part 2: Security functional requirements[S].
- [13] ISO/IEC 15408-3:2005. Information technology-Security techniques-Evaluation criteria for IT security-Part 3: Security assurance requirements[S].
- [14] ISO/IEC TR 15443-1: 2005. Information technology-Security techniques-A framework for IT security assurance-Part 1: Overview and framework[S].
- [15] ISO/IEC TR 15443-2: 2005. Information technology-Security techniques-A framework for IT security assurance-Part 2: Assurance methods[S].
- [16] ISO/IEC 17799:2005. Information technology-Security techniques-Code of practice for information security management[S].
- [17] ISO/IEC 18028-2:2006. Information technology-Security techniques-IT network

- security-Part 2: Network security architecture[S].
- [18] ISO/IEC 18028-3:2005. Information technology-Security techniques-IT network security-Part 3: Securing communications between networks using security gateways[S].
- [19] ISO/IEC 18028-4:2005. Information technology-Security techniques-IT network security-Part 4: Securing remote access[S].
- [20] ISO/IEC TR 18044:2004. Information technology-Security techniques-Information security incident management[S].
- [21] ISO/IEC TR 19791:2006. Information technology-Security techniques-Security assessment of operational systems[S].
- [22] ISO/IEC 27001:2005. Information technology-Security techniques-Information security management systems-Requirements[S].
- [23] GB/T 9387.2-1995. 信息处理系统 开放系统互连 基本参考模型 第2部分: 安全体系结构(idt ISO 7498-2)[S].
- [24] GB/T 9387.4-1995. 信息处理系统 开放系统互连 基本参考模型 第4部分: 安全管理框架(idt ISO 7498-4)[S].
- [25] GB/T 17142-1997. 系统管理综述(Systems Management Overview)(idt ISO/IEC 10040 (CCITT X.701))[S].
- [26] GB 17859-1999. 计算机信息系统安全保护等级划分准则[S].
- [27] ISO/IEC TR 14516:2002. Information technology-Security techniques-Guidelines for the use and management of Trusted Third Party[S].