第七章

1.1信息安全管理概述

信息安全管理( Information Security Management,ISM),是管理者为实现信息安全目标(如信息资产的CIA等特性、业务运行的持续性)而进行计划、组织、指挥、协调和控制的一系列活动。它的管理对象是组织的信息及相关资产,包括信息、人员、软件等,同时还包括信息安全目标、信息安全组织架构、信息安全策略规则等。管理的目的是保障组织的业务正常运转。

组织的活动能够反映组织的业务目标。

组织所有级别的管理者能够给予信息安全实质性的、可见的支持和承诺。

组织的管理者对信息安全需求、信息安全风险、风险评估及风险管理有正确深入的理解。

向所有管理者、员工和其他相关方提供有效的信息安全宣传以提升信息安全意识。

向所有管理者、员工和其他相关方分发、宣贯实行信息安全方针、策略和标准。使全员都对组织的信息安全方针、策略、标准的要求有深入的理解,是成功实施信息安全管理的重要基础。

管理者为信息安全建设提供足够的资金。这是信息安全管理成功实施的必要保障。

建立有效的信息安全事件管理过程。

建立有效的信息安全测量体系。

2信息安全风险管理

信息系统不可能达到绝对安全,但可以通过安全风险(以下简称"风险”)控制来实现符合个人或单位目标的一定程度的安全。信息安全管理的核心思想是风险管理,关键在于如何控制、化解和规避风险。风险管理是信息安全管理的基本方法,通过对单位信息资产实施一定的安全管理措施来保障信息的保密性、完整性和可用性。

2.1信息安全风险

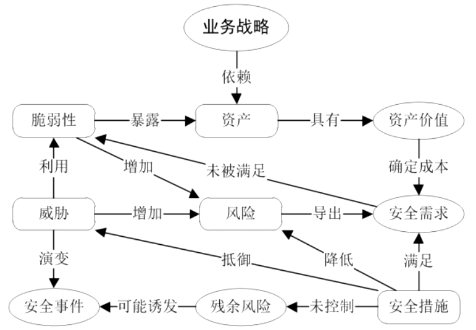
风险是一种潜在的、负面的东西,处于未发生的状态,它是指遭受损害或损失的可能性。因此,风险一方面客观存在,另一方面其发生的时间具有不确定性,风险一旦发生,将会产生损失。风险强调的是损害的潜在可能性,而不是事实上的损害,风险是不能消除殆尽的。

威胁

脆弱性

影响

资产



2.2风险管理

风险管理是信息安全管理的基本方法,通过对组织信息资产实施一定的安全管理措施来保障信息的保密性、完整性和可用性。风险管理是组织机构识别、评估风险并采取相关活动,将风险降低到一个可接受级别的过程。它是单位管理活动的一部分,其管理的主要对象就是风险。以风险为驱动的信息安全管理,其核心就是通过识别风险、选择对策、消减风险

按照GB/z24364-2009《信息安全风险管理指南》,信息安全风险管理有四个基本步骤:

背景建立

风险评估

风险处理

批准监督

风险管理是一个动态发展、不断循环的过程,一次风险管理完成后,因为新的变化引起新的风险,或者因为业务本身的要求,都需要进入新轮风险管理周期。

以体系化的方式实施信息安全管理,才能实现并保持一定的信息安全水平。

3信息安全时间与应急响应

3.1信息安全事件

信息安全事件,是指由于自然或者人为以及软硬件本身缺陷或故障的原因,对信息系统造成危害,或在信息系统内发生对社会造成负面影响的事件。至今尚没有仼何一种信息安全策略或防护措施,能够对信息及信息系统提供绝对的保护,以完全避免信息安全事件的发生。对信息安全事件进行有效管理和响应,最小化事件所造成的损失和负面影响,是组织信息安全战略的一部分。应急响应是信息安全事件管理的重要内容。

信息安全事件可以是故意、过失或非人为原因引起的,可以分为有害程序事件、网络攻击事件、信息破坏事件、信怠内容安全事件、设备设施故障、灾害性事件和其他信息安全事件等7个基本分类。通常,对信息安全事件的分级主要考虑三个要素:信息系统的重要程度、系统损失和社会影响。

通常,对信息安全事件的分级主要考虑三个要素信息系统的重要程度、系统损失和社会影响。

信息系统的重要程度

系统损失

社会影响

3.2信息安全应急响应

信息安全应急响应,是指一个组织为了应对各种安全意外事件的发生所采取的防范措施,既包括预防性措施,也包括事件发生后的应对措施。实践证明现实中难以发现和抵御所有威胁,安全事件具有突发性、复杂性,所以需要建立信息系统安全事件的快速响应机制。应急响应工作的主要任务是做好预先防范,安全事件发生后,尽快做出正确反应,及时阻止事件的继续发展,并减少损失,使系统恢复正常运行,同时采取追踪攻击者及必要的法律行动。

应急响应的作用主要表现在两个方面

未雨绸缪

亡羊补牢

应急响应组织是专门处理安全事件的组织。常用的名字是:

计算机网络安全事件应急组

计算机安全事件响应组( Computer Security Incident ResponseTeam, CSIRT)

信息安全事件响应组( Information Security Incident ResponseTeam, ISIRT

事件响应组( Incident esponse Team,IRT

通常,应急响应组织由管理、业务、技术和行政后勤等人员组成。

组织建立的内部应急响应组织应与外部的国内外应急响应组织、相关管理部门、设备设施及服务提供商(如电力供应、通信服务等)、利益相关方和新闻媒体等保持联系和协作,以确保在发生信息安全事件时能及时通报准确情况并获得支持。

国家计算机网络应急技术处理协调中心( Nationa| ComputerNetwork Emergency Response Technical Team/CoordinationCenter of China, cn-cert/CC)

国家计算机病毒应急处理中心

国家计算机网络入侵防范中心

3.3信息安全应急管理过程

应急响应方法和过程并不是唯一的,通常可以将应急响应管理过程分为如下6个阶段

准备

检测

遏制

根除

恢复

跟踪总结

4灾难备份

随着信息技术的发展和信息化的不断深入,特别是数据集中和业务集中以及由此产生的对信息系统越来越强的依赖性,导致信息系统相关事件对组织业务运营的影响越来越严重,从而使信息系统灾难备份和恢复越来越成为组织需要迫切解决的问题之一。对组织而言,信息系统失效无疑是一场灾难。在这种情况下,组织的业务无法正常运作,甚至可能陷入完全瘫痪。然而,有许多因素威胁着信息系统的正常运转,大到自然灾害(地震、洪水、飓风、火灾等),小到失窃、断电乃至操作员不经意的失误,都会影响系统的正常运转甚至造成整个系统完全瘫痪。所以,由信息系统瘫痪造成的影响往往十分惊人。

4.1灾难备份概述

GB/T20988-2007《信息系统灾难恢复规范》定义,灾难是指由于人为或自然的原因,造成信息系统运行严重故障或瘫痪,使信息系统支持的业务功能停顿或服务水平不可接受,通常导致信息系统需要切换到备用场地运行的突发事件。典型的灾难事件包括自然灾难,如火灾、洪水、地震、飓风、龙卷风和台风等还有技术风险,如设备故障、软件错误、通讯网络中断和电力故障等;人为因素往往也会酿成大祸,如操作员错误、破坏、植入有害代码和恐怖袭击等。

灾难备份（是灾难回复的基础）

灾难恢复

灾难恢复领域中,常使用如下两个业务参数表示灾难恢复系统的能力

恢复时间目标

恢复点目标

4.2灾难备份方法

灾难备份是指通过技术和管理手段,对信息系统和数据进行备份,以便灾难发生后信息系统及数据能够及时恢复,系统业务连续性得以保持。实施灾难备份前,应当根据信息系统的业务需求等实际情况,选择合适的备份策略

本地备份和异地灾备

数据级灾备和系统级灾备

完全备份和不完全备份

在实际工作中,根据不同业务对数据备份的时间窗口和灾难恢复的要求,结合备份软、硬件的实际情况,可以综合使用这三种备份方式,制定特定的备份策略,一种常用的策略设置方法如下。

执行完全备份

经常进行增量备份

定期执行差异备份