

第 1 章 网络信息安全概述

学习目标

- (1) 掌握网络信息安全的定义和主要威胁。
- (2) 了解网络信息安全的现状和主要影响因素。
- (3) 了解网络信息安全所涉及的主要内容。
- (4) 掌握 PDRR 模型、安全策略设计原则和网络信息安全保障技术。
- (5) 了解网络信息安全标准和网络安全等级保护。
- (6) 了解网络安全法律法规。

1.1 网络信息安全简介

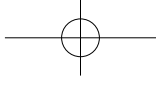
计算机网络是信息社会的基础，已经进入社会的各个角落，经济、文化、军事和社会生活越来越多地依赖计算机网络。然而，开放性的网络在给人们带来巨大便利的同时，其安全性如何保证？因此，计算机网络的安全性成为信息化建设的一个核心问题。

计算机网络中存储、传输和处理的信息多种多样，许多是敏感信息甚至是国家机密，如政府宏观调控决策、商业经济信息、股票证券、科研数据等重要信息。由于网络安全漏洞等原因，可能会造成信息泄露、信息窃取、数据篡改、数据破坏、计算机病毒发作、恶意信息发布等事件，由此造成的经济损失和社会危害难以估量。互联网已经渗透到人们生活的方方面面，没有网络安全，就没有国家安全。在频发的安全事件催化下，网络信息安全已经上升至国家战略高度。

1.1.1 网络信息安全的重要性

尽管网络的重要性已经被广泛认同，但对网络信息安全的忽视仍很普遍，缺乏网络信息安全意识的状况仍然十分严峻。不少企事业单位极为重视网络硬件的投资，但没有意识到网络信息安全的重要性，对网络信息安全的投资较少。这也使目前不少网络信息系统都存在先天性的安全漏洞和安全威胁，有些甚至产生了非常严重的后果。下面是一些重大网络信息安全事件。

1995 年，凯文·米特尼克（Kevin Mitnick）闯入许多计算机网络，偷窃了 2 万个信用卡号，他曾闯入北美空中防务指挥系统，破译了美国著名的太平洋电话公司在南加利福尼亚



亚州通信网络的用户密码,入侵过美国 DEC 等 5 家大公司的网络,造成 8000 万美元的损失。

2002 年,黑客用 DDoS 攻击影响了 13 个根 DNS 中的 8 个,作为整个 Internet 通信路标的关键系统遭到严重的破坏。

2010 年 1 月 12 日,中国最大中文搜索引擎“百度”遭到黑客攻击,长时间无法正常访问。

2013 年 6 月,前中情局(CIA)职员爱德华·斯诺顿曝光美国国家安全局的“棱镜”项目,该项目为秘密项目,过去几年间,美国国家安全局和联邦调查局通过进入微软、谷歌、苹果、雅虎等 9 大网络巨头的服务器,监控美国公民的电子邮件、聊天记录、视频及照片等秘密资料。

2014 年 12 月 25 日,乌云漏洞报告平台报告称,大量 12306 用户数据在互联网疯传,内容包括用户账号、明文密码、身份证号码、手机号码和电子邮箱等。这次事件是黑客首先通过收集互联网某游戏网站以及其他多个网站泄露的用户名和密码信息,然后通过撞库^[1]的方式利用 12306 的安全机制的缺陷来获取这十几万条用户数据。

2015 年 12 月 23 日,乌克兰发生了一次影响很大的安全事件,黑客通过有组织、有预谋的定向网络攻击,致使乌克兰境内近 1/3 的地区持续断电。

2017 年 5 月 12 日,勒索病毒(WannaCry)全面暴发,100 多个国家的数十万用户遭到袭击。此病毒对计算机内的文档、图片、程序等实施高强度的加密锁定,并向用户索取以比特币支付的赎金。

2021 年 5 月 9 日,美国宣布进入国家紧急状态,原因是当地最大燃油管道运营商 Colonial Pipeline 遭勒索软件攻击,被迫关闭向美国东部沿海各州供油的关键燃油网络。

2022 年 9 月 5 日,国家计算机病毒应急处理中心和 360 公司分别发布了关于某大学遭受美国国家安全局网络攻击的调查报告,美国国家安全局(NSA)下属的特定入侵行动办公室(TAO)使用了四十余种不同的专属网络攻击武器,持续对该大学开展攻击窃密,窃取该校关键网络设备配置、网管数据、运维数据等核心技术数据。

以上仅仅是一些个案。事实上,这样的案例不胜枚举,而且计算机犯罪案件有逐年增加的趋势。美国的一项研究显示,全球互联网每 39s 就发生了一次黑客事件,其中大部分黑客没有固定的目标。

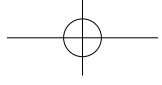
因此,网络系统必须有足够强大的安全体系,无论是局域网还是广域网,无论是单位还是个人,网络信息安全的目标是全方位防范各种威胁以确保网络信息的保密性、完整性和可用性。

1.1.2 网络信息安全的现状

现今 Internet 环境正在发生着一系列的变化,安全问题也出现了相应的变化,主要反映在以下几个方面。

(1) 网络犯罪成为集团化、产业化的趋势。从灰鸽子病毒案例可以看出,木马从制作

[1] 撞库是指黑客利用从某些网站或渠道获取的用户账号和密码,在其他网站上进行登录尝试。这主要是由于目前有相当一部分互联网用户喜欢在不同网站上使用统一的用户名和密码。



到最终盗取用户信息甚至财物，渐渐成为一条产业链。

(2) 无线网络、智能手机成为新的攻击区域及新的攻击重点。随着无线网络的大力推广及 5G 网络使用人群的增多，使用的用户群体也在不断地增加，手机病毒、手机恶意软件呈现快速增长的趋势。

(3) 垃圾邮件依然比较严重。虽然经过这么多年的垃圾邮件整治，垃圾邮件现象得到明显改善。例如，有一些国家有相应的立法来处理垃圾邮件，但是在利益的驱动下，垃圾邮件仍然影响着每个人的邮箱使用。

(4) 漏洞攻击的爆发时间变短。从近几年发生的攻击来看，不难发现漏洞攻击的时间越来越短，系统漏洞、网络漏洞、软件漏洞等被攻击者发现并利用的时间间隔在不断地缩短，很多攻击者都是通过这些漏洞来攻击网络的。

(5) 攻击方的技术水平要求越来越低。现在有很多黑客网站免费提供了许多攻击工具，利用这些工具可以很容易地实施网络攻击。

(6) 拒绝服务攻击 (deny of service, DoS) 更加频繁。由于 DoS 攻击更加隐蔽，难以追踪到攻击者，大多数攻击者采用分布式的攻击方式和跳板攻击方法。这种攻击更具有威胁性，攻击更加难以防范。

(7) 针对浏览器插件的攻击。插件的性能不是由浏览器来决定的，浏览器的漏洞升级并不能解决插件可能存在的漏洞。

(8) 网站攻击，特别是网页被挂木马。大多数用户在打开一个熟悉的网站，如自己信任的网站，但是这个网站被挂木马，在不经意间木马将会安装在自己的计算机中，这是现在网站攻击的主要模式。

(9) 内部用户的攻击。现今企事业单位的内部网与外部网的联系越来越紧密，来自内部用户的威胁也不断地表现出来。来自内部攻击的比例在不断上升，变成内部网络的一个防灾重点。据国家互联网应急中心 (英文简称 CNCERT) 发布的《CNCERT 互联网安全威胁报告—2022 年 6 月》中显示，国家互联网应急中心接收网络安全事件 9971 件，数量排名前 3 位的是安全漏洞类事件 4008 件 (占 40.2%)、恶意程序类事件 3585 件 (占 36.0%) 和网页仿冒类事件 1334 件 (占 13.4%)，如图 1-1 所示。

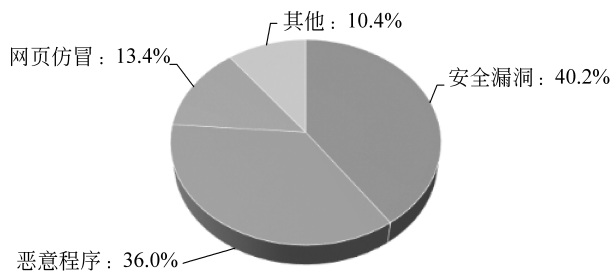
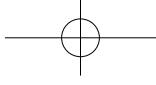


图 1-1 2022 年 6 月网络安全事件数量占比按类型分布

1.1.3 网络信息安全的定义

网络信息安全是陆、海、空、太空之外的第五维国家安全边界。网络信息安全是一个



关系国家主权、安全、社会稳定、民族文化继承和发扬的重要问题，其重要性正随着全球信息化步伐的加快越来越凸显出来。

网络信息安全是指计算机及其网络系统资源和信息资源不受自然和人为有害因素的威胁和危害，即是指计算机、网络系统的硬件和软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，确保系统能连续可靠正常地运行，使网络服务不中断。网络信息安全从其本质上讲就是系统上的信息安全。网络信息安全是一门涉及计算机科学、网络技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性科学。

从广义来说，凡是涉及计算机网络上信息的保密性、完整性、可用性、可控性和不可否认性的相关技术和理论都是计算机网络信息安全的研究领域。

（1）保密性。保密性是指网络信息不被泄露给非授权的用户、实体或过程，即信息只为授权用户使用。即使非授权用户得到信息也无法知晓信息的内容，因而不能使用。

（2）完整性。完整性是指维护信息的一致性，即在信息生成、传输、存储和使用过程中不发生人为或非人为的非授权篡改。

（3）可用性。可用性是指授权用户需要时能不受其他因素的影响，方便地使用所需信息，即当需要时能否存取所需的信息。这一目标是对信息系统的总体可靠性要求。例如，网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

（4）可控性。可控性是指对网络系统中的信息传播及具体内容能够实现有效控制，即网络系统中的任何信息要在一定传输范围和存放空间内可控。

（5）不可否认性。不可否认性是指保障用户无法在事后否认曾经对信息进行的生成、签发、接收等行为，一般通过数字签名来提供不可否认服务。

从网络运行和管理者角度来说，他们希望对本地网络信息的访问、读/写等操作受到保护和控制，避免出现“陷阱门”^[1]、病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。对安全保密部门来说，它们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害及对国家造成巨大损失。从社会教育和意识形态角度来讲，网络上不健康的内容会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

网络信息安全问题应该像每家每户的防火、防盗问题一样，做到防患于未然。网络安全问题十分常见，甚至在不会想到自己也会成为目标的时候，威胁就已经出现了，并且一旦发生，常常令人措手不及，可能会造成极大的损失。

1.1.4 网络信息安全的主要威胁类型

网络系统的安全威胁主要表现在主机可能会受到非法入侵者的攻击，网络中的敏感数据有可能泄露或被修改，从内部网向公网传送的信息可能被他人窃听篡改等。网络信息安全的主要威胁类型如表 1-1 所示。

[1] 陷阱门是在某个系统或某个文件中设置的“机关”，使在提供特定的输入数据时，允许违反安全策略。例如，一个登录处理子系统允许处理一个特定的用户识别码，以绕过通常的口令检查。

表 1-1 网络信息安全的主要威胁类型

威胁类型	含 义
网络窃听	网络中传输的敏感信息被窃听
窃取资源	窃取系统重要的软件、硬件、信息和资料等资源
讹传信息	攻击者获得某些信息后，发送给他人
伪造信息	攻击者将伪造的信息发送给他人
篡改发送	攻击者对合法用户之间的通信信息篡改后，发送给他人
非授权访问	某一资源被某个非授权的人或以非授权的方式使用
截获 / 修改	网络系统传输中数据被截获、删除、修改、替换或破坏
拒绝服务攻击	攻击者以某种方式使系统响应减慢甚至瘫痪，使网络难以正常服务
行为否认	通信实体否认已经发生的行为
旁路控制	攻击者发掘系统的安全缺陷或安全性上的脆弱之处获得非授权的权利或特权
人为疏忽	已授权人为了利益或由于粗心将信息泄露给未授权人
信息泄露	信息被泄露或暴露给非授权用户
物理破坏	通过计算机及其网络或部件进行破坏，或绕过物理控制非法访问
病毒木马	利用计算机病毒或木马等恶意软件进行破坏或恶意控制他人系统
服务欺骗	欺骗合法用户或系统，骗取他人信任以便谋取私利
设置陷阱	设置陷阱系统或部件，骗取特定数据以违反安全策略
资源耗尽	故意超负荷使用某一资源，导致其他用户服务中断
消息重发	重发某次截获的备份合法数据，达到信任并非法侵权目的
冒名顶替	假冒他人或系统用户进行活动
媒体废弃物	利用媒体废弃物得到可利用信息，以便非法使用
信息战	为国家或集团利益，通过信息战进行网络破坏或恐怖袭击

1.1.5 影响网络信息安全的主要因素

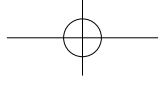
影响网络信息安全的因素有很多，归纳起来主要有以下一些因素。

(1) 开放性的网络环境。网络特点正如一句非常经典的话所描述的：“Internet 的美妙之处在于你和每个人都能互相连接，Internet 的可怕之处在于每个人都能和你互相连接。”

Internet 是一个开放性的网络，是跨越国界的，这意味着网络的攻击不仅来自本地网络的用户，也可以来自 Internet 上的任何一台机器。Internet 是一个虚拟的世界，无法得知联机的另一端是谁。在这个虚拟的世界里，已经超越了国界，某些法律也受到了挑战，因此网络信息安全面临的是一个国际化的挑战。

网络建立初期只考虑方便性、开放性，并没有考虑总体安全构架，任何一个人或者团体都可以接入，因而网络所面临的破坏和攻击可能是多方面的。例如，可能是对物理传输线路的攻击，可能是对操作系统漏洞的攻击，可能是对网络通信协议的攻击，也可能是对硬件的攻击等。网络信息安全已成为信息时代人类共同面临的挑战。

(2) 操作系统的漏洞。漏洞是可以在攻击过程中利用的弱点，它可以是软件、硬件、程序缺陷、功能设计或者配置不当等造成的。黑客或入侵者会研究分析这些漏洞，加以利



用而获得侵入和破坏的机会。

网络连接离不开网络操作系统，操作系统可能存在各种漏洞，有很多网络攻击的方法都是从寻找操作系统的漏洞开始的。

① 系统模型本身的漏洞。这是系统设计初期就存在的，无法通过修改操作系统程序的源代码来修补。

② 操作系统程序的源代码存在漏洞。操作系统也是一个计算机程序，任何一个程序都可能存在漏洞，操作系统也不例外。例如，冲击波病毒针对的是 Windows 操作系统的 RPC 缓冲区溢出漏洞。

③ 操作系统程序配置不当。许多操作系统的默认配置的安全性较差，进行安全配置比较复杂并且需要一定的安全知识，许多用户并没有这方面的能力，如果没有正确配置这些安全功能，会造成一些系统的安全缺陷。

(3) TCP/IP 的缺陷。一方面，该协议数据流采用明码传输，且传输过程无法控制，这就为他人截取、窃听信息提供了机会；另一方面，该协议在设计时采用协议簇的基本体系结构，IP 地址作为网络节点的唯一标识，不是固定的且不需要身份认证。因此攻击者就有了可乘之机，他们可以通过修改或冒充他人的 IP 地址进行信息的拦截、窃取和篡改等。

(4) 人为因素。在计算机使用过程中，使用者的安全意识缺乏、安全管理措施不到位等，通常是网络信息安全的一个重大隐患。例如，隐秘性文件未设密码，操作口令被泄露，重要文件的丢失等，都会给黑客提供攻击的机会。对于系统漏洞的不及时修补以及不及时防病毒，都可能会给网络信息安全带来影响。

1.2 网络信息安全涉及的内容

网络信息安全是一门交叉学科，除了涉及数学、通信、计算机等自然科学领域外，还涉及法律、心理学等社会科学领域，是一个涉及多领域的复杂系统。

2019 年颁布的国家标准《信息安全技术 网络安全等级保护基本要求》(GB/T 22239—2019)(等保 2.0)的内容包括安全通用要求和安全扩展要求，其主要内容如表 1-2 所示。

表 1-2 《信息安全技术 网络安全等级保护基本要求》的主要内容

要求类型	详细内容	
安全通用要求	技术部分	物理和环境安全
		网络和通信安全
		设备和计算安全
		应用和数据安全
	管理部分	安全策略和管理制度
		安全管理机构和人员
		安全建设管理
		安全运维管理
安全扩展要求	云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求、工业控制系统安全扩展要求	

1.2.1 物理和环境安全

(1) 物理安全。物理安全也称实体安全,是指保护计算机网络设备、设施及其他媒体,免遭地震、水灾、火灾等环境事故,以及人为操作失误、错误或者各种计算机犯罪行为导致的破坏。保证计算机信息系统各种设备的物理安全,是整个计算机信息系统安全的前提。

物理安全包括以下两个方面。

① 设备安全:主要包括设备的防盗、防毁(接地保护)、防电磁信息辐射泄露、防止线路截获、抗电磁干扰及电源保护等。

② 物理访问控制安全:建立访问控制机制,控制并限制所有对信息系统的计算、存储和通信系统设施的物理访问。

(2) 环境安全。为了确保计算机处理设施能正确、连续地运行,要考虑及防范火灾、电力供应中断、爆炸物、化学品等,还要考虑环境的温度和湿度是否适宜,必须建立环境状况监控机制,以监控可能影响信息处理设施的环境状况。

1.2.2 网络和通信安全

信息系统网络建设以维护用户网络活动的保密性、网络数据传输的完整性和应用系统的可用性为基本目标。

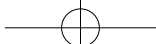
依据国家标准《信息安全技术 网络安全等级保护基本要求》(GB/T 22239—2019),在网络和通信安全部分,网络和通信安全强调对网络整体的安全保护,确定了新的控制点为网络架构、通信传输、边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计和集中管控,如表 1-3 所示。

表 1-3 网络和通信安全的组成

网络和通信安全子项	含 义
网络架构	设计安全的拓扑、链路备份、IP 划分等
通信传输	设置防火墙等安全设备、数据加密(VPN 等)
边界防护	对内部用户非授权连接到外部网络的行为进行限制或检查,限制无线网络的使用等
访问控制	访问控制功能的设备包括网闸、防火墙、路由器和三层路由交换机等
入侵防范	入侵检测系统等
恶意代码防范	在关键网络节点处对恶意代码进行检测和防护
垃圾邮件防范	在关键网络节点处对垃圾邮件进行检测和防护
安全审计	各系统配置日志,提供审计机制
集中管控	集中监测、集中审计和集中管理

1.2.3 设备和计算安全

设备和计算安全通常指网络设备、安全设备、服务器设备、终端设备等节点设备自



身的安全保护能力，一般通过启用操作系统、数据库、防护软件的相关安全配置和策略来实现。

设备和计算安全的最终目标是，对节点设备启用防护设施和安全配置，通过集中统一监控管理，提供访问控制、入侵检测和病毒防护、漏洞管理、安全审计等功能，使系统关键资源和敏感数据得到保护，确保数据处理和系统运行时的保密性、完整性和可用性，并在发生安全事件后能快速定位，有效回溯，减少损失。

1.2.4 应用和数据安全

应用安全，顾名思义就是保障应用程序使用过程和结果的安全。

现在针对应用系统的攻击很多，因为应用系统安全的实现比较困难，主要原因有两个：一是对应用安全缺乏认识；二是应用系统过于灵活。网络安全、系统安全和数据安全的技术实现有很多固定的规则，应用安全则不同，客户的应用往往都是独一无二的。

数据安全主要包括两个方面：一方面是数据本身的安全，主要是采用现代密码算法对数据进行主动保护，如数据保密性、数据完整性等；另一方面是数据存储的安全，主要是采用现代信息存储手段对数据进行主动防护，如通过磁盘阵列、数据备份、异地容灾等手段保证数据的安全。

应用和数据安全的组成如表 1-4 所示。

表 1-4 应用和数据安全的组成

应用和数据安全子项	含 义	应用和数据安全子项	含 义
应用安全	应用系统平台安全	数据安全	数据保密性
	应用软件安全		数据完整性
			数据备份和恢复

1.2.5 管理安全

安全是一个整体，完整的安全解决方案不仅包括物理安全、网络安全、系统安全和应用安全等技术手段，还需要以人为核心的策略和管理支持。网络信息安全至关重要的往往不是技术手段，而是对人的管理。无论采用了多么先进的技术设备，只要管理安全上有漏洞，那么这个系统的安全就没有保障。在网络管理安全中，专家们一致认为是“30% 的技术，70% 的管理”。

同时，网络信息安全不是一个目标，而是一个过程，而且是一个动态的过程。这是因为制约安全的因素都是动态变化的，必须通过一个动态的过程来保证安全。例如，Windows 操作系统经常发布安全漏洞，在没有发现系统漏洞之前，大家可能认为自己的系统是安全的，实际上系统已经处于威胁之中了，所以要及时地更新补丁。

安全是相对的，没有绝对的安全，需要根据客户的实际情况，在实用和安全之间找一个平衡点。

从总体来看,网络信息安全涉及网络系统的多个层次和多个方面,同时,也是一个动态变化的过程。网络信息安全实际上是一个系统工程,既涉及对外部攻击的有效防范,又包括制定完善的内部安全保障制度;既涉及防病毒攻击,又涵盖实时检测、防黑客攻击等内容。因此,网络信息安全解决方案不应仅提供对于某种安全隐患的防范能力,还应涵盖对于各种可能造成网络信息安全问题隐患的整体防范能力;同时,还应该是一种动态的解决方案,能够随着网络信息安全需求的增加而不断改进和完善。

1.3 网络信息安全防护

1.3.1 PDRR 模型

事实上,安全是一种意识,一个过程,而不仅是某种技术。进入 21 世纪后,网络信息安全的理念发生了巨大的变化,从不惜一切代价把入侵者阻挡在系统之外的防御思想,开始转变为防护—检测—响应—恢复相结合的思想,出现了 PDRR (protect/detect/react/restore, 防护/检测/响应/恢复) 等网络信息安全模型,如图 1-2 所示。PDRR 倡导一种综合的安全解决方法,由防护、检测、响应、恢复这 4 个部分构成一个动态的信息安全周期。

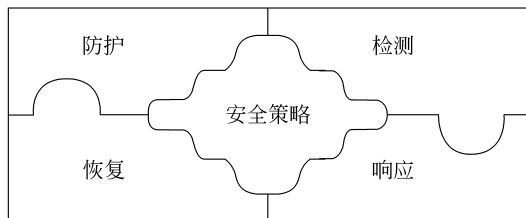
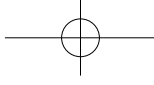


图 1-2 PDRR 网络信息安全模型

安全策略的每一部分包括一组相应的安全措施来实现一定的安全功能。安全策略的第一部分是防护,根据系统已知的所有安全问题做出防护措施,例如,打补丁、访问控制和数据加密等。安全策略的第二部分是检测,攻击者如果穿过了防护系统,检测系统就会检测出入侵者的相关信息,一旦检测出入侵事件发生,响应系统就开始采用相应的安全措施,如断开网络连接等。安全策略的最后一部分是系统恢复,在入侵事件发生后,把系统恢复到原来的状态。每次发生入侵事件,防护系统都要更新,保证相同类型的入侵事件不能再次发生,所以整个安全策略包括防护、检测、响应和恢复,这 4 个方面组成了一个信息安全周期,使信息的安全得到全方位的保障。

1.3.2 安全策略设计原则

网络信息安全策略规定了一系列的安全防范措施,从宏观和微观两方面保障网络的安全。在全面了解组织的网络信息安全现状以后,网络信息安全策略设计者应遵循一定的原



则和方法，在理论知识的指导下制定出科学可靠的网络信息安全策略。虽然网络的具体应用环境不同，但在制定安全策略时应遵循一些总的原则。

（1）适应性原则。安全策略是在一定条件下采取的安全措施，必须是和网络的实际应用环境相结合的。通常，在一种情况下实施的安全策略到另一环境下就未必适合，因此安全策略的制定应充分考虑当前环境的实际需求。

（2）木桶原则。木桶原则即“木桶的最大容积取决于最短的那块木板”，是指对信息进行均衡、全面的保护。充分、全面、完整地对系统的安全漏洞和安全威胁进行分析，评估和检测（包括模拟攻击）是设计信息安全系统的必要前提条件。安全机制和安全服务设计的首要目的是防止最常用的攻击手段，根本目的是提高整个系统“最低点”的安全性能。

（3）动态性原则。安全策略是在一定时期采取的安全措施。由于网络动态性的特点，用户不断增加，网络规模不断扩大，网络技术本身的发展变化也很快，各种漏洞和隐患不断发现，而安全措施是防范性的、持续不断的，所以制定的安全措施必须能随着网络性能以及安全需求的变化而变化，应容易修改和升级。

（4）系统性原则。网络信息安全管理是一个系统化的工作，必须考虑到整个网络的方方面面。也就是在制定安全策略时，应全面考虑网络上各类用户、各种设备、软件、数据以及各种情况，有计划、有准备地采取相应的策略。任何一点疏漏都会造成整个网络信息安全性的降低。

（5）需求、代价、风险平衡分析原则。对任何一个网络而言，绝对的安全是不可能达到的，也是不必要的。应从网络的实际需求出发，对网络面临的威胁及可能承担的风险进行定性与定量相结合的分析，在需求、代价和风险间寻求一个平衡点，在此基础上制定规范和措施，确定系统的安全策略。

（6）一致性原则。一致性原则主要是指网络信息安全问题应与整个网络的工作周期（或生命周期）同时存在，制定的安全体系结构必须与网络信息安全需求相一致，在网络系统设计及实施计划、网络验证、验收、运行等网络生命周期的各个阶段，都要制定相应的安全策略。

（7）最小授权原则。从网络信息安全的角度考虑问题，打开的服务越多，可能出现的安全漏洞就会越多。最小授权原则指的是网络中账号设置、服务配置、主机间信任关系配置等应该为网络正常运行所需的最小限度。关闭网络信息安全策略中没有定义的网络服务并将用户的权限配置为策略定义的最低限度、及时删除不必要的账号等措施可以将系统的危险性大大降低。在没有明确的安全策略的网络环境中，网络信息安全管理通过简单关闭不必要或者不了解的网络服务、删除主机信任关系、及时删除不必要的账号等手段也可以将入侵危险降低一半以上。

（8）整体性原则。要求在发生被攻击、破坏事件的情况下，必须尽可能地快速恢复信息系统的服务，减少损失。因此，信息安全系统应该包括安全防护机制、安全检测机制和安全恢复机制。

（9）技术与管理相结合原则。安全体系是一个复杂的系统工程，涉及人、技术、操作等各方面要素，单靠技术或管理都不可能实现。因此，必须将各种安全技术与运行管理机制、人员思想教育与技术培训、安全规章制度建设相结合。