9.1 信息安全概述

目 录

上一页

下一页

结 束

返 回

9.1.1 信息安全意识

1．建立对信息安全的正确认识

随着信息产业越来越大，网络基础设施越来越深入到社会的各个方面、各个领域，信息技术应用成为我们工作、生活、学习、国家治理和其他各个方面必不可少的关键组件，信息安全的地位日益突出。它不仅是企业、政府的业务能不能持续、稳定地运行的保证，也可成为关系到个人安全的保证，甚至成为关系到我们国家安全的保证。所以信息安全是我们国家信息化战略中一个十分重要的方面。

目 录
上一页
下一页
结 束

9.1.1 信息安全意识

2. 掌握信息安全的基本要素和惯例

信息安全包括四大要素：技术、制度、流程和人。合适的标准、完善的程序、优秀的执行团队，是一个企业单位信息化安全的重要保障。技术只是基础保障，技术不等于全部，很多问题不是装一个防火墙或者一个杀毒软件就能解决的。制定完善的安全制度很重要，而如何执行这个制度更为重要。如下信息安全公式能清楚地描述出他们之间关系：

信息安全＝先进技术＋防患意识＋完美流程＋严格制度＋优秀执行团队＋法律保障

目 录
上一页
下一页
结 束

9.1.1 信息安全意识

3．清楚可能面临的威胁和风险

信息安全所面临的威胁来自于很多方面。这些威胁大致可分为自然威胁和人为威胁。自然威胁指那些来自于自然灾害、恶劣的场地环境、电磁辐射和电磁干扰、网络设备自然老化等的威胁。自然威胁往往带有不可抗拒性，因此这里主要讨论人为威胁。

目 录
上一页
下一页
结 束

9.1.1 信息安全意识

3. 清楚可能面临的威胁和风险

1） 人为攻击

人为攻击是指通过攻击系统的弱点，以便达到破坏、 欺骗、窃取数据等目的，使得网络信息的保密性、完整性、可靠性、可控性、可用性等受到伤害，造成经济上和政治上不可估量的损失。

人为攻击又分为偶然事故和恶意攻击两种。偶然事故虽然没有明显的恶意企图和目的，但它仍会使信息受到严重破坏。恶意攻击是有目的的破坏。

恶意攻击又分为被动攻击和主动攻击两种。

目 录
上一页
下一页
结 束

9.1.1 信息安全意识

3．清楚可能面临的威胁和风险

2）安全缺陷

如果网络信息系统本身没有任何安全缺陷，那么人为攻击者即使本事再大也不会对网络信息安全构成威胁。但是，遗憾的是现在所有的网络信息系统都不可避免地存在着一些安全缺陷。有些安全缺陷可以通过努力加以避免或者改进，但有些安全缺陷是各种折衷必须付出的代价。

目 录
上一页
下一页
结 束

9.1.1 信息安全意识

3. 清楚可能面临的威胁和风险

3）软件漏洞

由于软件程序的复杂性和编程的多样性，在网络信息系统的软件中很容易有意或无意地留下一些不易被发现的安全漏洞。软件漏洞同样会影响网络信息的安全。

一些有代表性的软件安全漏洞

3．清楚可能面临的威胁和风险

4）结构隐患

结构隐患一般指网络拓扑结构的隐患和网络硬件的安全缺陷。网络的拓扑结构本身有可能给网络的安全带来问题。作为网络信息系统的躯体，网络硬件的安全隐患也是网络结构隐患的重要方面。

4. 养成良好的安全习惯

1）良好的密码设置习惯

2）网络和个人计算机安全

3）电子邮件安全

4）打印机和其他媒介安全

5）物理安全

目 录
上一页
下一页
结 束
返 回

9.1.2 网络礼仪与道德

1. 网络道德概念及涉及内容

计算机网络道德是用来约束网络从业人员的言行，指导他们的思想的一整套道德规范。计算机网络道德可涉及到计算机工作人员的思想意识、服务态度、业务钻研、安全意识、待遇得失及其公共道德等方面。

目 录
上一页
下一页
结 束

2. 网络的发展对道德的影响

1）淡化了人们的道德意识

2）冲击了现实的道德规范

3）导致道德行为的失范

目 录
上一页
下一页
结 束

3. 网络信息安全对网络道德提出了新的要求

1）要求人们的道德意识更加强烈，道德行为更加自主自觉

2）要求网络道德既要立足于本国，又要面向世界

3）要求网络道德既要着力于当前，又要面向未来

目 录
上一页
下一页
结 束

4. 加强网络道德建设对维护网络信息安全有着积极的作用

1）网络道德可以规范人们的信息行为

2）加强网络道德建设，有利于加快信息安全立法的进程

4）加强网络道德建设，有利于发挥信息安全技术的作用

目 录
上一页
下一页
结 束
返 回

9.1.3 计算机犯罪

所谓计算机犯罪，是指行为人以计算机作为工具或以计算机资产作为攻击对象实施的严重危害社会的行为。由此可见，计算机犯罪包括利用计算机实施的犯罪行为和把计算机资产作为攻击对象的犯罪行为。

目 录
上一页
下一页
结 束

1. 计算机犯罪的特点

1）犯罪智能化

2）犯罪手段隐蔽

3）跨国性

4）犯罪目的多样化

5）犯罪分子低龄化

6）犯罪后果严重

目 录
上一页
下一页
结 束

2. 计算机犯罪的手段

1）制造和传播计算机病毒

2）数据欺骗

3）意大利香肠战术

4）活动天窗

5）清理垃圾

6）数据泄漏

7）电子嗅探器

8）口令破解程序

除了以上作案手段外，还有社交方法，电子欺骗技术，浏览，顺手牵羊和对程序、数据集、系统设备的物理破坏等犯罪手段。

目 录
上一页
下一页
结 束

3. 网络黑客

黑客一词源于英文Hacker，原指热心于计算机技术，水平高超的电脑专家，尤其是程序设计人员。但到了今天，黑客一词已被用于泛指那些专门利用电脑搞破坏或恶作剧的人。目前黑客已成为一个广泛的社会群体，其主要观点是：所有信息都应该免费共享；信息无国界，任何人都可以在任何时间地点获取他认为有必要了解的任何信息；通往计算机的路不止一条；打破计算机集权；反对国家和政府部门对信息的垄断和封锁。黑客的行为会扰乱网络的正常运行，甚至会演变为犯罪。

目 录
上一页
下一页
结 束

黑客行为特征表现形式

1）恶作剧型

2）隐蔽攻击型

3）定时炸弹型

4）制造矛盾型

5）职业杀手型

6）窃密高手型

7）业余爱好型

目 录
上一页
下一页
结 束

9.1.4 常见信息安全技术

目前信息安全技术主要有：密码技术、防火墙技术、虚拟专用网（VPN）技术、病毒与反病毒技术以及其他安全保密技术。

1.密码技术

1）密码技术的基本概念

密码技术是网络信息安全与保密的核心和关键。通过密码技术的变换或编码，可以将机密、敏感的消息变换成难以读懂的乱码型文字，以此达到两个目的：

其一，使不知道如何解密的“黑客”不可能从其截获的乱码中得到任何有意义的信息；

其二，使“黑客”不可能伪造或篡改任何乱码型的信息。

目 录
上一页
下一页
结 束

密码技术

2）单钥加密与双钥加密

传统密码体制所用的加密密钥和解密密钥相同，或从一个可以推出另一个，被称为单钥或对称密码体制。若加密密钥和解密密钥不相同，从一个难以推出另一个，则称为双钥或非对称密码体制。

单钥密码的优点是加、解密速度快。缺点是随着网络规模的扩大，密钥的管理成为一个难点；无法解决消息确认问题；缺乏自动检测密钥泄露的能力。

目 录
上一页
下一页
结 束

双钥加密

双钥体制的特点是密钥一个是可以公开的，可以像电话号码一样进行注册公布；另一个则是秘密的，因此双钥体制又称作公钥体制。由于双钥密码体制仅需保密解密密钥，所以双钥密码不存在密钥管理问题。双钥密码还有一个优点是可以拥有数字签名等新功能。双钥密码的缺点是算法一般比较复杂，加、解密速度慢。

目 录
上一页
下一页
结 束

密码技术

3）著名密码算法简介

数据加密标准（DES）是迄今为止世界上最为广泛使用和流行的一种分组密码算法。它的产生被认为是20世纪70年代信息加密技术发展史上的两大里程碑之一。DES是一种单钥密码算法，是一种典型的按分组方式工作的密码。其他的分组密码算法还有IDEA密码算法、LOKI算法等。

最著名的公钥密码体制是RSA算法。RSA算法是一种用数论构造的、也是迄今为止理论上最为成熟完善的一种公钥密码体制，该体制已得到广泛的应用。它的安全性基于“大数分解和素性检测”这一已知的著名数论难题基础。著名的公钥密码算法还有Elgamal公钥体制等。

目 录
上一页
下一页
结 束

2. 防火墙技术

当构筑和使用木质结构房屋的时候，为防止火灾的发生和蔓延，人们将坚固的石块堆砌在房屋周围作为屏障，这种防护构筑物被称为防火墙。在今日的电子信息世界里，人们借助了这个概念，使用防火墙来保护计算机网络免受非授权人员的骚扰与黑客的入侵，不过这些防火墙是由先进的计算机系统构成的。

目 录
上一页
下一页
结 束

3. 虚拟专用网（VPN）技术

虚拟专用网是虚拟私有网络（**Virtual Private Network**）的简称，它被定义为通过一个公用网络（通常是因特网）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。虚拟专用网是对企业内部网的扩展。

目前，能够用于构建**VPN**的公共网络包括**Internet**和服务提供商（**ISP**）所提供的**DDN**专线（**Digital Data Network Leased Line**）、帧中继（**Frame Relay**）、**ATM**等，构建在这些公共网络上的**VPN**将给企业提供集安全性、可靠性和可管理性于一身的私有专用网络。

目 录
上一页
下一页
结 束

4．病毒与反病毒技术

计算机病毒自20世纪80年代中后期开始广泛传播，其危害由来已久。计算机病毒具有自我复制能力，它能影响计算机软件、硬件的正常运行，破坏数据的正确性与完整性，造成计算机或计算机网络瘫痪，给人们的经济和社会生活造成巨大的损失并且呈上升的趋势。

计算机病毒的危害不言而喻，人类面临这一世界性的公害采取了许多行之有效的措施，如加强教育和立法，从产生病毒的源头上杜绝病毒；加强反病毒技术的研究，从技术上解决病毒传播和发作。

目 录
上一页
下一页
结 束

5. 其他安全与保密技术

1）实体及硬件安全技术

实体及硬件安全是指保护计算机设备、设施（含网络）以及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故（包括电磁污染等）破坏的措施和过程。实体安全是整个计算机系统安全的前提，如果实体安全得不到保证，则整个系统就失去了正常工作的基本环境。另外，在计算机系统的故障现象中，硬件的故障也占到了很大的比例。正确分析故障原因，快速排除故障，可以避免不必要的故障检测工作，使系统得以正常运行。

目 录
上一页
下一页
结 束

2）数据库安全技术

数据库系统作为信息的聚集体，是计算机信息系统的核心部件，其安全性至关重要，关系到企业兴衰、国家安全。因此，如何有效地保证数据库系统的安全，实现数据的保密性、完整性和有效性，已经成为业界人士探索研究的重要课题之一。

目 录
上一页
下一页
结 束