信息资源管理第 8 节课官方笔记

目录

一、教材节构图

第六章信息资源管理的标准与法规

6.1 信息资源安全管理内涵

信息资源安全问题呈现形式：实体破坏，黑客攻击，违法行为，病毒入侵

信息资源安全管理：是指针对普遍存在的信息资源安全问题，人们利用各种技术方法和组织手段，所进行的有计划的管理活动。

本质上，信息资源安全管理问题是指信息可用性和权属受到威胁。

信息安全技术关注问题

1、可用性：保护合法用户对信息的使用不会被不正当地拒绝。

2、保密性也称私密性：保证机密信息不被窃取，或窃取者不能了解信息的真实含义。

3、认证性也称真实性：对信息的来源进行判断（身份认证），能对伪造来源的信息予以鉴别。

4、一致性也称完整性：保证信息是一致或完整的，即信息在生成利用全过程中，内容不被非法用户篡改（信息内容认证）。

信息资源安全管理的主要任务

1、采取技术和管理措施，保证信息资源可用，即让信息和信息系统在任何时候可被合法用户使用。

2、采用数据加密技术，使信息在其处理过程（存储或传递）中，内容不被非法者获得。

3、建立有效的责任机制，防止用户否认其行为。

4、建立可审查的机制，实现责任追究性。

1、银行、电信、能源等涉及面广、影响重大的要害部门，面临信息资源安全问题重大，需要采取高等级的安全管理措施和手段。

2、银行：应对突发灾难的最有效办法，是迅速建立并不断完善金融机构的灾难备份和恢复系统。

6.2 信息资源安全的系统管理

6.2.1 信息系统安全模型

OSI 七层模型：

6.2.2 行为规范管理

信息系统安全的行为规范管理包括国家和社会组织两个层面。

国家，制定信息安全法规体系；社会组织，制定信息资源安全管理策略。

制定安全策略的步骤：理解组织业务特征，建立安全管理组织机制，确定信息资源安全的整体目标，确定安全策略的范围，安全策略评估，安全策略实施。

信息资源安全策略从宏观的角度反映了组织整体上的安全思想与观念，一般由组织的高层负责制定。

安全策略制定要兼顾内容上的可理解性、技术上的可实现性和实际操作的可执行性，它应该是简明的、原则的、可审核的、可行的、文档化的、动态的。

6.2.3 实体安全管理

实体安全主要涉及信息系统的硬件及其运行环境，其安全与否对网络、软件、数据等的安全有着重要的影响。针对：场地环境，硬件，介质等做好防护策略。

场地环境安全：包括机房场地安全，如远离易燃易爆易腐蚀的地点；空气调节系统安全，如温度保持 20℃；防火管理，配备烟火报警装置等。

硬件安全：包括硬件设备的档案管理、防电磁干扰、防电磁泄漏、电源安全：一般电功率要超过所有设备负载的 125%。

介质安全：重要数据要加密保存、分门别类存放介质，保证不被破坏。

6.2.4 网络安全管理

一个典型的通过互联网实现的 Web 应用涉及的网络资源包括：

主机系统：各类提供网络服务的计算机系统，也称服务器。

终端系统：各类服务请求的计算机系统，也称客户机。

网络互连设备：包括网线和接口；集线器、交换机、路由器以及网关、网桥系统等。

网络安全措施和技术包括：网络分段，防火墙，VPN（虚拟专用网），入侵检测，病毒防治。

网络分段与 VLAN（虚拟局域网）

网络分段通常被认为是控制广播风暴的一种基本手段。其指导思想就是将非法用户与网络资源相互隔离。

网络分段的好处包括：过滤通信量；扩大了网络范围；提高可靠性；减少了网络嗅觉器监听范围。

网络分段包括：物理分段和逻辑分段。

VLAN（虚拟局域网）技术是一种常用的逻辑分段方法。

防火墙技术

部署防火墙的系统必须确保通过防火墙与系统外部的网络连接。

VPN （虚拟专用网）

VPN 被定义为是通过公共网络建立的专用网络。优点是：经济；结构灵活、管理方便；安全

入侵检测

入侵检测是一种主动安全保护技术。它在不影响网络性能的前提下，对网络进行检测，从计算机网络的若干关键点收集信息，通过分析这些信息，发现异常并判断识别是否为恶意攻击。

病毒防治

网络病毒防治，主要从客户机或工作站、主机和防火墙等层面，对寄宿病毒的计算机系统及其网络进行预防和治理，包括扫描、过滤、清除等。

6.2.5 软件安全管理

软件安全问题：信息资产受到威胁；软件应用的安全问题

1、信息资产受到威胁：从管理手段看，软件安全管理既依赖于道德、法律（知识产权等）

和实体保护（防盗）等非技术手段，也可以通过一些技术手段达到安全管理的目的。

软件资产的安全管理措施：软件备份安全管理和软件代码安全管理。

磁盘或光盘备份的软件：软件指纹，软件加密；

安装使用的软件：软件狗，电子锁，时间炸弹；

2、软件应用安全问题：软件分为系统软件和应用软件两类；恶意程序。

1983 年，美国国防部国家计算机中心提出的“可信计算机系统评审标准”（TCSEC），堪称信息系统安全史上里程碑式的工作。

四类八级：

1、D：非安全保护类。如 MS-DOS

2、C：自主型保护类。

C1：如早期 UNIX

C2：如 Windows2000，UNIX

3、B：强制型安全保护类

B1； B2； B3

4、A：验证型保护类

A1；超 A1

我国 1999 年公布的《计算机信息系统安全保护等级划分准则》，规定了计算机系统安全保护能力的五个等级：

第一级：用户自主保护级

第二级：系统审计保护级

第三级：安全标记保护级

第四级：结构化保护级

第五级：访问验证保护级

操作系统安全：

最小特权：为了使无意的或恶意的攻击所造成的损失达到最低程度，每个用户和程序必须尽可能地使用最小特权。

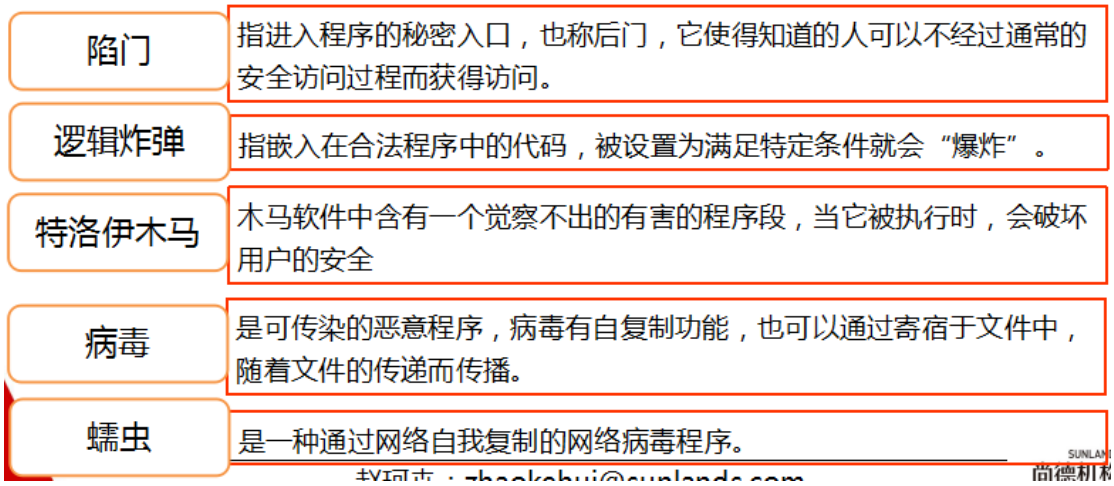
硬件系统：内存保护、进程控制、输入/输出控制

软件系统：身份识别与鉴别、访问控制、最小特权管理、安全审计

恶意程序：是指未经授权在用户不知道的情况下，进入用户计算机系统中，影响系统正常工作，甚至危害或破坏系统的计算机程序。具有破坏性，非法性，隐蔽性。

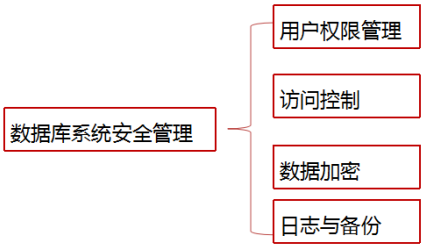
恶意程序的防治包括防护和治理两方面，应该采取管理和技术相结合的方法。

常见的恶意程序：



6.2.6 数据安全管理

数据安全管理：是信息系统安全最根本的落脚点，其他层面的安全管理也是为数据安全目的而服务的。数据安全管理主要解决数据(信息)的可用性、机密性、认证性和一致性等问题。



数据库管理系统的用户权限管理

数据库模式修改权限：索引权限，资源权限，修改权限，撤销权限。

数据操作权限：读权限，插入权限，修改权限，删除权限。

数据库管理员可以利用 GRANT<权限表> ON<数据库元素>TO<用户表><WITH option>语句进行授权。

数据加密技术

数据加密本质是一种数据变换，将数据变为不可识别（不可读）的内容，一般人不可利用。许多访问控制技术（口令信息的加密、文件访问控制）、通信网络信道加密（如 VPN 等）、真实性认证等都用到了加密技术。

日志与备份

数据库的日志文件用来记录数据库每一次更新活动。

三、配套练习题

1、信息资源安全主要关注信息在开发利用过程中面临的（ABCD）。多选题 1307

A:可用性问题 B:机密性问题 C:真实性问题 D:完整性问题 E:可行性问题

2、保密性可以保证信息不被窃取，或者窃取者不能（A）。单选题 1304

A:了解信息的真实含义 B:破坏信息 C:使用信息 D:传送信息

3、应对银行突发灾难的最有效办法，是迅速建立并不断完善金融机构（ A）。单选题 1304

A:灾难备份和恢复系统 B:信息系统 C:认证系统 D:交易系统

5、信息资源安全问题呈现形式有（ABCE）。多选题 1304

A:实体破坏 B:黑客攻击 C:违法行为 D:网上购物 E:病毒侵入