《信息安全培训》
-段方

教授 北京大学博士后

1 概述

1.1 信息安全的概念及范围

1.1.1 概述

1.1.2 信息系统潜在威胁

被动攻击

主动攻击

黑客攻击手法

1.1.3 信息安全技术概览

1.1.4 信息安全注重体系安全

防

护

检测

响应

恢复

1.2 信息安全等级分类

1.2.1 分级的概念

1.2.2 分级保护涉及的标准

1.2.3 职责和角色

1.2.4 企业信息等级选择依据

1.3 信息安全的层级界定

1.3.1 网络层

1.3.2 硬件层

1.3.3 操作系统层

1.3.4 应用层

1.3.5 数据层

1.4 信息安全的**“**维度 **”**

1.4.1 硬件故障

1.4.2 人为过失

1.4.3 软件失误

1.4.4 电脑病毒

1.4.5 自然灾害等

1.5 信息安全的现状

1.5.1 中国国家层面的法律、法规等

1.5.2 美国 **NSA** 等安全保障体系

1.5.3 一些黑客攻击案例

1.6 客户隐私保护

1.6.1 客户隐私的界定

1.6.2 客户隐私保护的内容

1.6.3 客户隐私的国际情况

欧洲的 **GDPR** 说起

1.6.4 【思考】不同企业客户隐私的界定

1.7 常见问题的防范

1.7.1 培养良好习惯

1.7.2 电脑病毒的防护

1.7.3 浏览器的防护

1.7.4 操作系统的安全防护

1.7.5 网络层面的防护等

1.8 【案例】信息安全防护的具体案例

2 客户隐私保护

2.1 客户隐私的定义

2.1.1 隐私的历史由来

2.1.2 中国对隐私的界定

2.1.3 客户隐私的信息有哪些？

2.1.4 【案例】隐私泄露引发的悲剧

2.2 法律上客户隐私的界定

2.2.1 私人信息

2.2.2 个人私事

2.2.3 私人领域等

2.2.4 隐私的特点

2.3 企业对客户隐私的规避

2.3.1 规避的合同

2.3.2 规避的司法案例

2.4 企业如何保护客户隐私

2.4.1 哪些系统有客户隐私？

2.4.2 隐私保护的原则

2.4.3 隐私保护的技术方法

2.4.4 隐私保护的管理方法

2.5 【案例】附件——**APP** 如何进行安全防护

2.6 【思考】防不胜防的隐私泄露——透明倒逼的“ 善良 ”

3 信息网络安全

3.1 网络安全攻击的概述

3.1.1 概述

3.1.2 中外黑客的历史等

3.1.3 网络攻击的思路

3.2 网络攻击的方法及原理

3.2.1 端口攻击

3.2.2 获取口令

3.2.3 放置木马

3.2.4 网络钓鱼

3.2.5 DDOS 攻击等

3.3 网络攻击的类型举例

3.3.1 特洛伊木马

3.3.2 后门攻击

3.3.3 病毒攻击

3.3.4 拒绝服务攻击

3.4 网络防御技术

3.4.1 防火墙技术

3.4.2 入侵监测系统

3.4.3 密码学

3.4.4 网络安全态势感知

3.4.5 病毒监测技术

3.4.6 蜜罐技术

3.5 【案例】附件——网络安全介绍

4 数据加密方法

4.1 加密算法概述

4.1.1 概

述 凯撒密

码

摩斯密码

BASE64 编码

4.1.2 算法的分类

对称加密

非对称加密

4.1.3 算法的特点评估

4.1.4 HTTPS 工作原理

4.2 加密算法的选择和评估

4.2.1 选择的原则

4.2.2 如何评估和对比

4.3 加密算法的原理

5.1 层层防御的技术理念

5.1.1 从敏感数据角度的层层防御

5.1.2 从数据出来环节的层层防御

5.1.3 从数据生命周期的层层防御

5.2 数据访问策略

5.2.1 隐私数据策略管理

5.2.2 告警策略管理

5.3 “ 三分技术、七分管理 **”**

5.3.1 安全管理的重要性

5.3.2 安全管理的内容和范围

5.3.3 技术围绕管理需求

5.4 与网络安全的关系

5.4.1 层次不同

5.4.2 解决网络突破后的数据安全问题

5.5 数据导出管理与监控

5.5.1 数据水印技术

6.2 金库管理模式

6.2.1 何为金库模式？

6.2.2 金库模式的要点

6.2.3 金库模式的意义

6.3 管理规章制度设计

6.3.1 设计哪些规章制度

6.3.2 规章制度的设计原则

6.3.3 规章制度的设计分类

6.4 访问日志管理

6.4.1 大数据的日志如何管理

6.4.2 日志的价值分析

6.4.3 日志的分析应用

6.5 安全实时告警

6.5.1 如何进行实时监控

6.5.2 监控规则的实时计算

6.5.3 告警信息的实时传送