工作秘密：可口可乐配方

工控有层级但定级时要整体定级

大数据 没办

原则上 大数据不低于三级

作业：

某款公司的安全产品

容灾备份

双备份 热备份 容备份

验收：安全功能 资料等一堆

第三级及以上需要测评的相关费用

整改要素：

身份差别和自主访问控制 都有

强制访问控制 三四级有要求

安全审计 二三四级有要求

完整性与保密性 都有

边界防护 二（非授权内联外）三（非授权外联内）四有要求

资源控制 二三四

入侵防范和恶意代码防范 都有

网络安全包括物理安全

1.0检查

2.0核查

可信验证 沈昌祥

CVE-XXXX

SOC

CERT 中国的安全问题集合

安全域：信息的交互，边界的划分：允许访问，但是需要有限制

等级保护基本要求：狭义的等保

设计要求：包括技术类管理类产品类 细化

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

先看通用再看具体

GB/T 25070-22019 信息安全技术 网络安全等级保护安全设计技术要求

考试不考这些标准

2.0 宽和严

管的东西多了，标准严格了

Eg：不允许开后门

一个中心，三重防御

可信技术 可信运算等

第三级以上的网络应当再境内实施技术维护，不得境外远程技术维护。

（只能境内维护，境外维护后果自负

云上贵州

三级以上系统出事儿了要告诉公安

APT：高级可持续性攻击

系统划分方法：管理机构、业务特点、分析物理位置的差异

跨省要统一审核

4.20

测试人员签字

公安局备案

工具测试：扫描探测、渗透测试、协议分析

目的：获得系统的漏洞、了解访问的情况

流程：收集目标系统信息->规划工具测试接入点->制定《工具测试作业指导书》->现场测试->结果整理分析

收集目标信息：

网络设备、安全设备、主机设备、目标系统网络拓扑结构等相关信息

规划工具测试接入点：

可以确定的是不确定性

相关原则：由低级别系统向高级别系统探测、同一系统同等重要程度功能区域要探测、较低重要程度向较高重要程度的区域进行探测

现场测试：

在相应的约束下

众多交接过程需要沟通、备份、预案等，报告上要签字balabala

核心数据区：猛地一笔 要当心

网络设备列表，最后需要写一个版本号，因为相应的漏洞不一样

Web等级二级、城域网等级三级，核心数据库最NB

IP地址给被测单位看一眼确认能不能用

1. 检查
2. 核查！=检查

2.0 访谈

4.25

威胁-外因&脆弱性-内因

相辅相成

组织&资产

组织-受害者

资产-需要进行相关的评估

评估风险->规避、转嫁、降低风险->将风险控制在可承受的范围内

风险评估&等级保护（计算题）

（前者快要被后者吸收了，一种技术/方法啥的）

等级保护中高级别的信息系统不一定就有高级别的安全风险

等保：只考虑是什么东西，威胁可能多，风险等级不一定，因为他可能有很多的防护手段

风险要素及属性的关系 听着蛮重要的

业务战略的实现对资产有依赖性，依赖程度越高，风险越小

残余风险：安全措施不当/无效 主动放弃不去控制

资产分类&资产赋值

数据、软件、硬件、服务、人员、其他

资产赋值：半定性半定量 三个安全属性赋值 综合分析 归一性 五级分级制

风险评估不适合作为研究方向

可用性

CPS：信息物理系统

威胁识别：重点识别&&全面识别

重点识别：重心突出，结构分明，同质性

全面识别：在调整和变化阶段，安全等级高的系统

植树、剪枝、统计

威胁树：思维导图

进行相关的分析，辅助，不能纯用

资产赋值：自定义：评估人员和被评估人员一起决定

但是威胁不行

自定义（主观的东西），它定义（客观的东西）

不能按照频率去进行威胁赋值

思想：保持开放的态度，这节课相关领域都是不断变化开放的

4.27

白皮书啥的官方给威胁

用威胁发生的频率定义威胁的大小（其实不合理然并卵）

软环境（管理体系，人员、制度）&硬环境（物理环境 温度湿度等）

人机合一

脆弱性 绝对-相对 技术-管理

数字孪生技术

各种预警

风险评估==风险分析

风险管理包含风险分析

计算：

可能性L+损失F=风险值R

风险值=R(L(T,V),F(Ia,Va))

T:威胁出现的频率 V:脆弱性

Ia:资产价值 Va:严重程度

R要根据ATV都进行计算，但是在不同系统中赋值的意义是不一样的

相乘的关系就行，具体怎么乘不管

算子：考试会给

取上界/下界：柔化处理

L（T,V）=sqrt（2\*3）向上取整=3

F（Ia,Va）=sqrt（5\*3）向上取整=4

R（ATV）=R(L,F)=sqrt（3\*4）向上取整=4

5.1

1.0与2.0的比较

2.0新增 通信传输 可信验证 沈昌祥NB 垃圾邮件防范

通信传输：完整性和保密性

通信设备

可信：国产密码 可信根是否被更改

网络边界 组织机构与internet、合作伙伴、内网、电信专用网、电话网、无线网等

测评：测评指标、测评对象、测评实施 不建议压力测试

3级以上系统才会有检测硬件冗余 主要是因为太烧钱了

主备/双活(俩都在干活不需要时间等待)

拓扑图

拓扑扫描工具

应用安全

2.0安全计算环境 安全通信网络

自主访问控制 强制访问控制

可信计算

老三样：防火墙、杀病毒、入侵检测 被动免疫，无法在发生之前进行防御

利用可信计算技术实现主动免疫——沈昌祥

底层基础芯片可信->终端平台可信->

Arm trust zone

现场检查（核查）

测试

Scada

电网！=电厂

应急响应流程（前期有相应的计划/规划）

信息通报-上报-披露-写报告

横向通报：组织内进行通报（同单位内进行通报/组织外如下游客户等通报

重要的——实时跟踪

不重要的——留档

定级还挺重要的

如何启动，启动几级的“应急响应启动令”

划重点

等保2.0

工具测试 报告 核查 访谈 访谈的注意事项 写测评的报告 网络测评包括哪些内容 看书 如何做测评+新的书上没有的

网络 1.0/2.0 主机安全测试评估 2.0没有主机 叫做计算环境 可信

风险识别与评估 是什么 等级保护和风险评估的关系 风险评估具体的特性 资产识别balabala如何识别如何赋值 威胁识别 分类方法 软环境威胁硬环境威胁 脆弱性需要注意的事情

哪些脆弱性 如何赋值

计算风险值 计算题 风险控制原则是什么

应急响应 是什么 三个环节 流程 业务影响的两层含义 恢复的目标是那两点 如何确定xpo和xpo 基本要素 流程 没了