安全防护基本知识

1.1安全防护基本知识

一、网络空间安全介绍

网络空间Cyberspace已成为领土、领海、领空、太空之外的“第五空间”或人类“第二类生存空间”成为国家主权延申的新疆域

网络空间安全（Cybrespace Security）是指作为信息环境中的一个整体域的网络空间的安全性。保证由独立且相互依存的信息基础设施和网络组成，包括互联网、电信网、计算机系统、嵌入式处理器系统的这一网络空间中方方面面的安全

二、网络安全评估基础

风险评估相关要素

理解资产、威胁、脆弱性、安全风险、安全措施、残余风险等风险评估相关要素及相互关系

风险评估途径与方法

了解基线评估等风险评估途径及自评估、检查评估等风险评估方法

了解基于知识的评估,理解定性评估、定量评估的概念及区别并掌握定呈分析中量化风险的方法。

风险评估相关要素-资产

构成风险评估的资产是建立对组织具有价值的信息或资源，是安全策略保护的对象。

风险评估中资产的价值不是以资产的经济价值来衡量,而是由资产在这三个安全属性上的达成程度或者其安全属性未达成时所造成的影响程度来决定的。

风险评估相关要素-威胁

可能导致对系统或组织危害的不希望事故潜在起因。

威胁可以通过威胁主体、资源、动机、途径等多种属性来描述。引起风险的外因

造成威胁的因素：人为因素和环境因素。

根据威胁的动机：人为因素又可分为恶意和非恶意两种。环境因素包括自然界不可抗的因素和其它物理因素

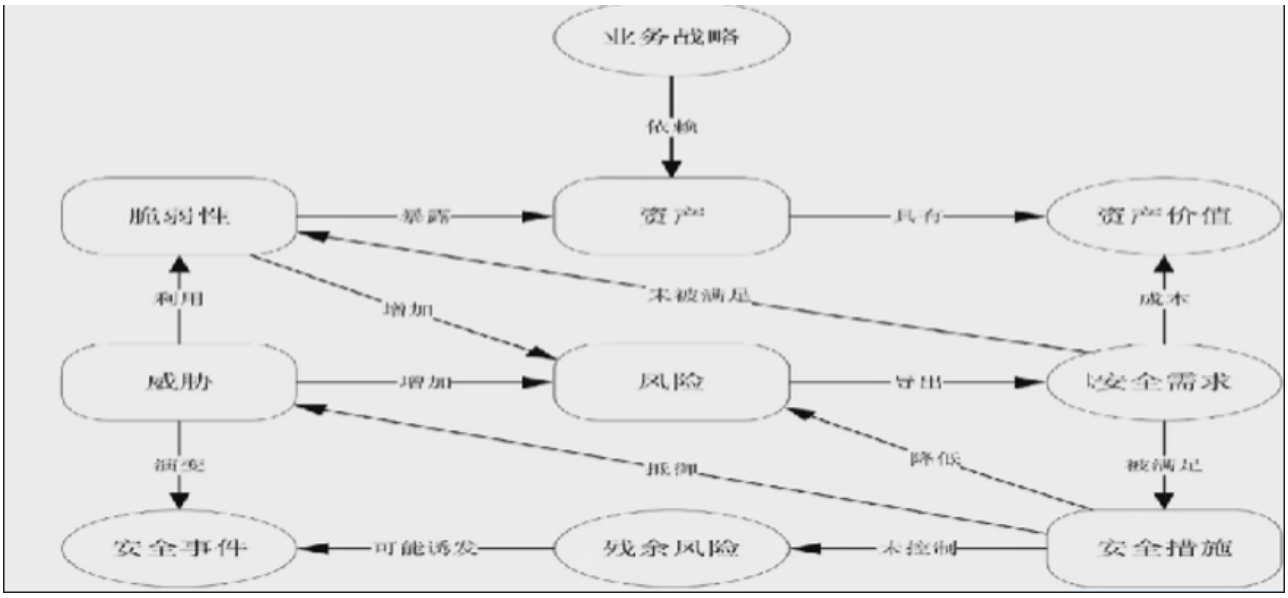
风险评估相关要素-脆弱性

可能被威胁所利用的资产或若干资产的薄弱环节。

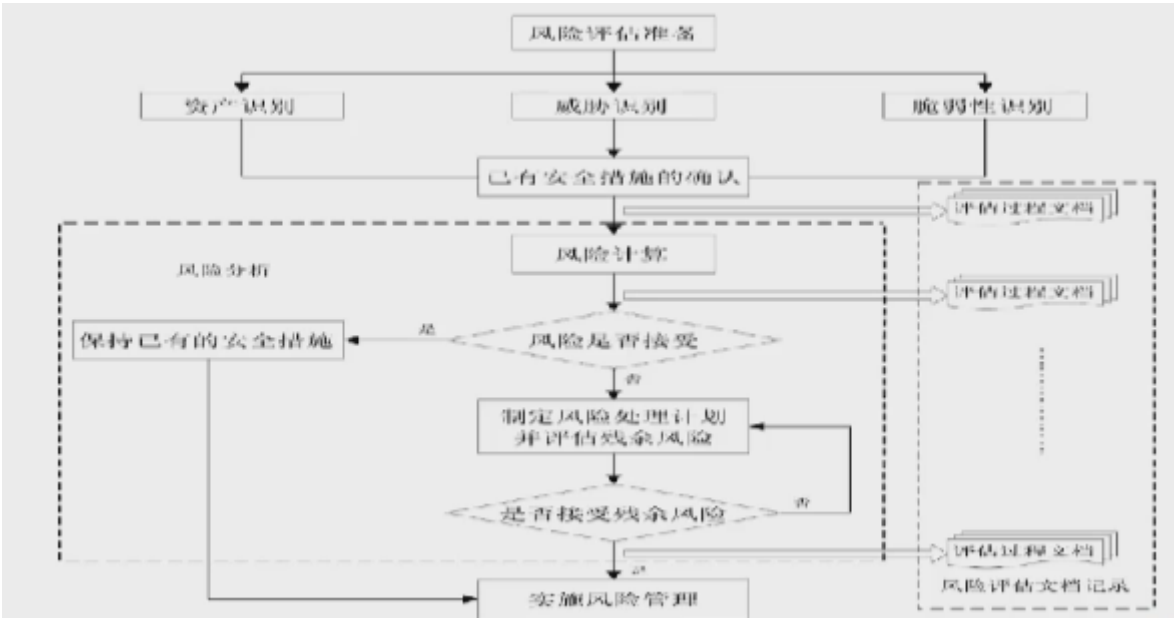
脆弱性是资产本身存在的，如果没有被相应的威胁利用，单纯的脆弱性本身不会对资产造成损害。

威胁总是要利用资产的脆弱性才可能造成危害。

风险评估要素之间的关系



风险评估基本过程



风险评估准备

风险评估准备是整个风险评估过程有效性的保证

组织实施风险评估是一种战略性的考虑,其结果将受到组织的业务战略、业务流程、安全需求、系统规模和结构等方面的影响。

风险评估工作

确定风险评估的目标

根据满足组织业务持续发展在安全方面的需要、法律法规的规定等内容，识别现有信息系统及管理上的不足，以及可能造成的风险大小。

确定风险评估的范围

风险评估范围可能是组织全部的信息及与信息处理相关的各类资产、管理机构，也可能是某个独立的信息系统、关键业务流程、与客户知识产权相关的系统或部门等。

组建适当的评估管理与实施团队

风险评估实施团队,由管理层、相关业务骨干、IT技术等人员组成风险评估小组。

评估实施团队应做好评估前的表格、文档、检测工具等各项准备工作．进行风险评估技术培训和保密教育,制定风险评估过程管理相关规定。

进行系统调研

系统调研是确定被评估对象的过程，风险评估小组应进行充分的系统调研,为风险评估依据和方法的选择、评估内容的实施奠定基础。

调研内容至少应包括: 业务战略及管理制度;主要的业务功能和要求;网络结构与网络环境，包括内部连接和外部连接;系统边界;主要的硬件、软件数据和信息;系统和数据的敏感性;支持和使用系统的人员。

系统调研可以采取问卷调查、现场面谈相结合的方式进行。

确定评估依据和方法

根据系统调研结果,确定评估依据和评估方法。

评估依据包括（但不仅限于):现有国际标准、国家标准、行业标准;行业主管机关的业务系统的要求和制度;系统安全保护等级要求;系统互联单位的安全要求;系统本身的实时性或性能要求等

据组织机构自身的业务特点、信息系统特点，选择适当的风险分析方法并加以明确，如定性风险分析、定量风险分析，或是半定量风险分析。

根据评估依据，应考虑评估的目的、范围、时间、效果、人员素质等因素来选择具体的风险计算方法，并依据业务实施对系统安全运行的需求,确定相关的判断依据，使之能够与组织环境和安全要求相适应。

制定风险评估方案

风险评估方案的目的是为后面的风险评估实施活动提供一个总体计划.用于指导实施方开展后续工作。

风险评估方案的内容包括：

团队组织:包括评估团队成员，组织结构、角色、责任等内容;

工作计划:风险评估各阶段的工作计划，包括工作内容、工作形式、工作成果等内容;

时间进度安排:项目实施的时间进度安排。

获得最高管理者对风险评估工作的支持

上述所有内容确定后，应形成较为完整的风险评估实施方案．得到组织最管理者的支持、批准;

对管理层和技术人员进行传达,在组织范围就风险评估相关内容进行培训,以明确有关人员在风俭评估中的任务。

资产识别

资产分类、分级、形态及资产价值评估

资产分类

数据、软件、硬件、服务、人员、其他（（GB/T 20984《信息安全风险评估规范》））

资产形态

有形资产、无形资产

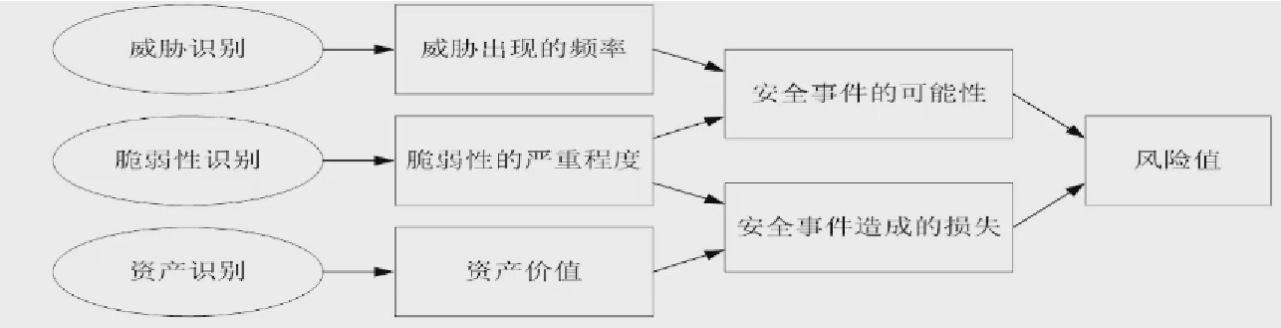
资产分级

保密性分级、完整性分级、可用性分级

资产重要性分级

风险分析

GB/T 20984-2007《信息安全风险评估规范》给出信息安全风险分析思路



风险值=R(A,T,V)=R(l(T,V),F(la,va))

R表示安全风险计算函数　　la表示安全事件所作用的资产价值

A表示资产　　Va表示脆弱性严重程度

T表示威胁　　L表示威胁利用资产的脆弱性导致安全事件的可能性

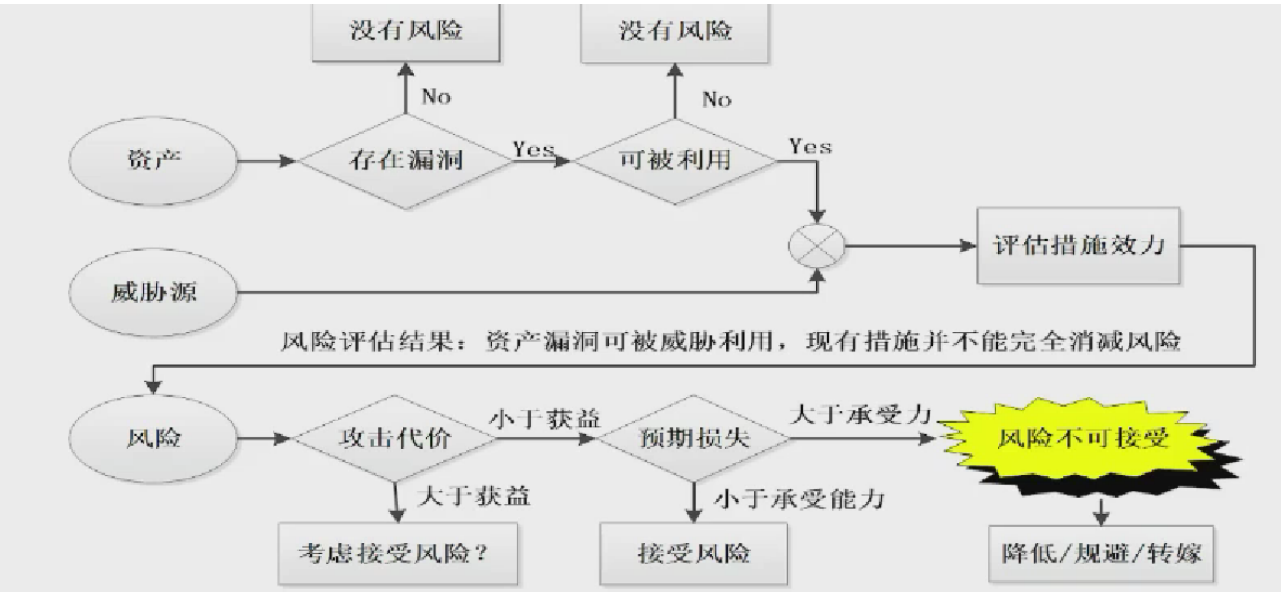
V表示脆弱性　　F表示安全事件发生后造成的损失

风险处理

对不可接受的风险应根据导致该风险的脆弱性制定风险处理计划

管理措施

技术措施



残余风险评估

实施安全措施后对措施有效性进行再评估

在对于不可接受的风险选择适当安全措施后，为确保安全措施的有效性，可进行再评估，以判断实施安全措施后的残余风险是否已经降低到可接受的水平。

某些风险可能在选择了适当的安全措施后，残余风险的结果仍处于不可接受的风险范围内，应考虑是否接受此风险或进一步增加相应的安全措施

三、网络安全攻防描述

概念

网络安全实战攻防演习（以下简称“攻防演习")是以获取目标系统的最高控制权为目标，由多领域安全专家组成攻击队，在保障业务系统安全的前提下，采用"不限攻击路径，不限制攻击手段"的攻击方式．而形成的"有组织"的网络攻击行为。

攻防演习通常是在真实环境下对参演单位日标系统进行可控、可审计的网络安全实战攻击，通过攻防演习检验参演单位的安全防护和应急处置能力，提高网络安全的综合防控能力。

HW行动

HW行动""指的是每年一次由公安部主导的面向国家重要信息系统和关键信息基础设施的网络安全实战演习，通过实战网络攻击的形式检验我国关键信息基础设施安全防护和应急处置能力。每次持续时间大约2~4周。采取红蓝对抗的形式,红队负责攻击、蓝队负责防御。

HW行动覆盖范围

2016年，仅公安部、民航局、国家电网三个事业单位参与“护网2016”行动。

2017年，部分政府部门加入“护网2017”行动，组织演练模拟门户网站、重要信息系统遭受攻击破坏等真实场景。

2018年，部分国有企事业单位及其它重点单位加入“护网2018"行动,组织演练模拟对相关网站和信息系统展开攻击。

2019年，工信、安全、武警、交通、铁路、民航、能源、新闻广电、电信运营商等单位都加入到"护网2019"行动中。

2020年，公有云、物联网相关企业也加入进来。

HW工作阶段

准备阶段

- 确定防守组织及团队
- 明确责任矩阵
- 资产梳理
- 网络拓扑图
- 确定互联网暴露面
- 防守方资料准备

自查整改阶段

- 网络安全检查

主机安全检查

应用系统安全检查

运维终端安全检查

日志审计

备份有效性检查

安全意识培训

安全整改加固

攻防演习阶段

演习启动会

授权及备份

攻击演习（渗透测试、社工、DDOS.....）

防守演习（设备状态检测、蜜罐）

演习总结

正式防护

安全设备监控

部署蜜罐

安全事件处理

日志分析

态势分析

总结优化

设备状态汇总总结

人员投入总结

事件处理总结

整体总结优化