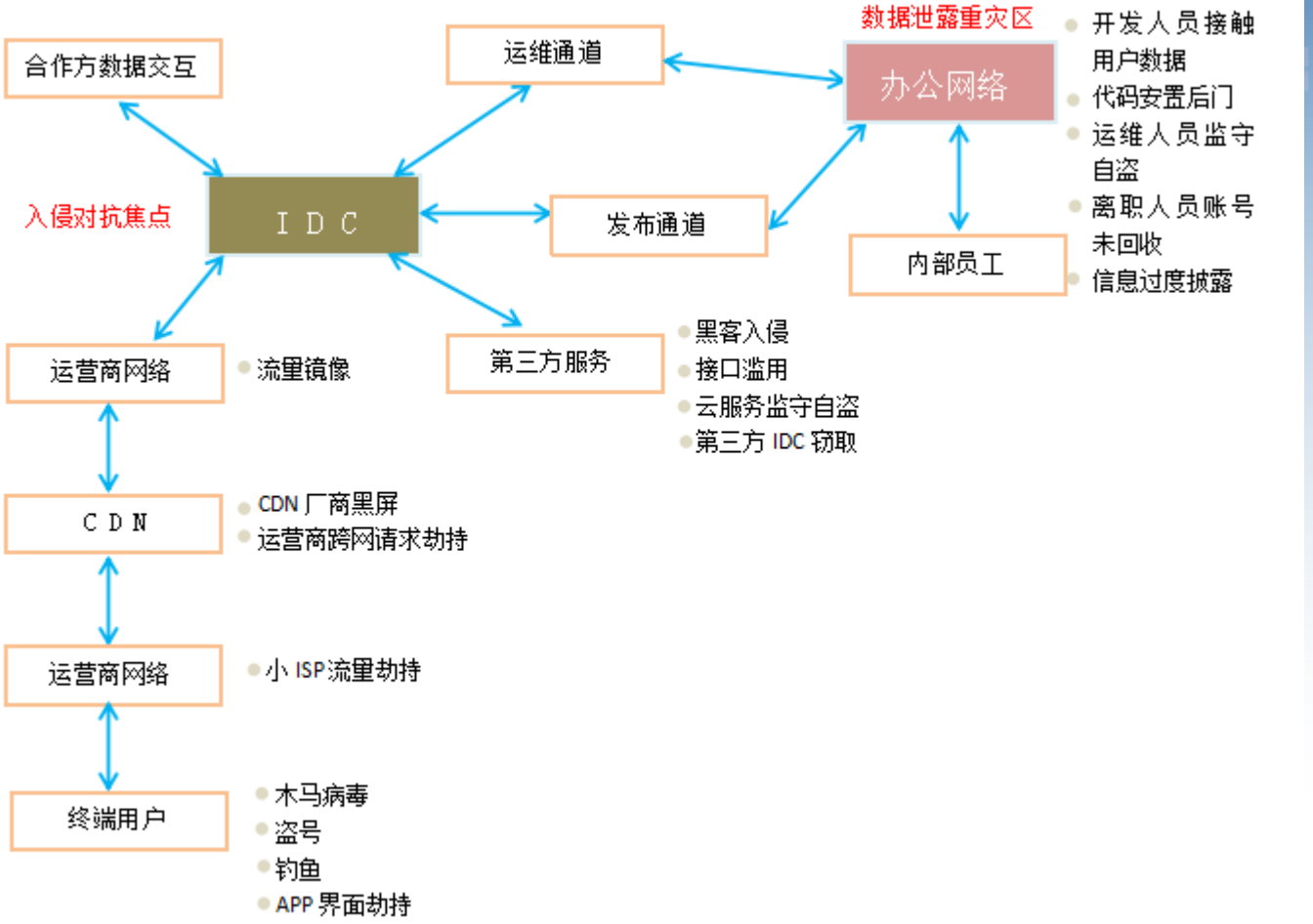
OWASP

Open Web Application Security Project

浅谈企业信息安全建设规划


合作方数据交互
运维通道
数据泄露重灾区
办公网络
开发人员接触用户数据
代码安置后门
运维人员监守自盗
离职人员账号未回收
信息过度披露
入侵对抗焦点
IDC
发布通道
内部员工
运营商网络
流量镜像
第三方服务
黑客入侵
接口滥用
云服务监守自盗
第三方 IDC 窃取
CDN
CDN 厂商黑屏
运营商跨网请求劫持
运营商网络
小 ISP 流量劫持
终端用户
木马病毒
盗号
钓鱼
APP 界面劫持

OWASP

Open Web Application Security Project

图上所标注的威胁，基本涵盖了一家互联网公司所面临的所有威胁。但是对于不同企业、不同规模的企业而言，需要的安全能力和需求是完全不一样的。

企业的安全建设是由多方面组成，其主要工作包括防范威胁发生，以及采取风险降低的措施，因此安全工作开展涉及多方面的内容。

OWASP
Open Web Application Security Project

数据安全管理	应急检测与保障	安全体系设计与维护	网络架构安全管理
数据安全管理策略 敏感数据防护措施分析 数据备份及有效性分析	信息安全事件发现、通知、溯源及跟踪 安全舆情及威胁收集与管理 敏感数据防护措施分析 安全事件应急预案制定与维护	信息安全制度体系的设计、维护及发布 新型安全理念的评估及可行性落地 信息安全技术有效性测量与风险量化评估 信息安全培训	网络架构安全需求设计 安全域划分 边界防护 防火墙、waf、入侵防御系统等 堡垒机
终端安全管理	**应用安全管理**	**主机安全管理**	**网络安全管理**
维护终端安全管理策略优化及维护 终端病毒防护、补丁分发及软件管理 办公上网行为管理及员工办公合规管理	漏洞扫描、渗透测试、代码审计、安全评估 信息数据保护管理 日志、流量收集分析，安全威胁监测	漏洞扫描、渗透测试、安全评估 主机日志收集及安全威胁监测 主机监测/防护体系的维护及管理	漏洞扫描、安全评估、网络架构安全分析 网络防护体系的优化、搭建以及运维管理 网络链路维护及访问控制策略

OWASP

Open Web Application Security Project

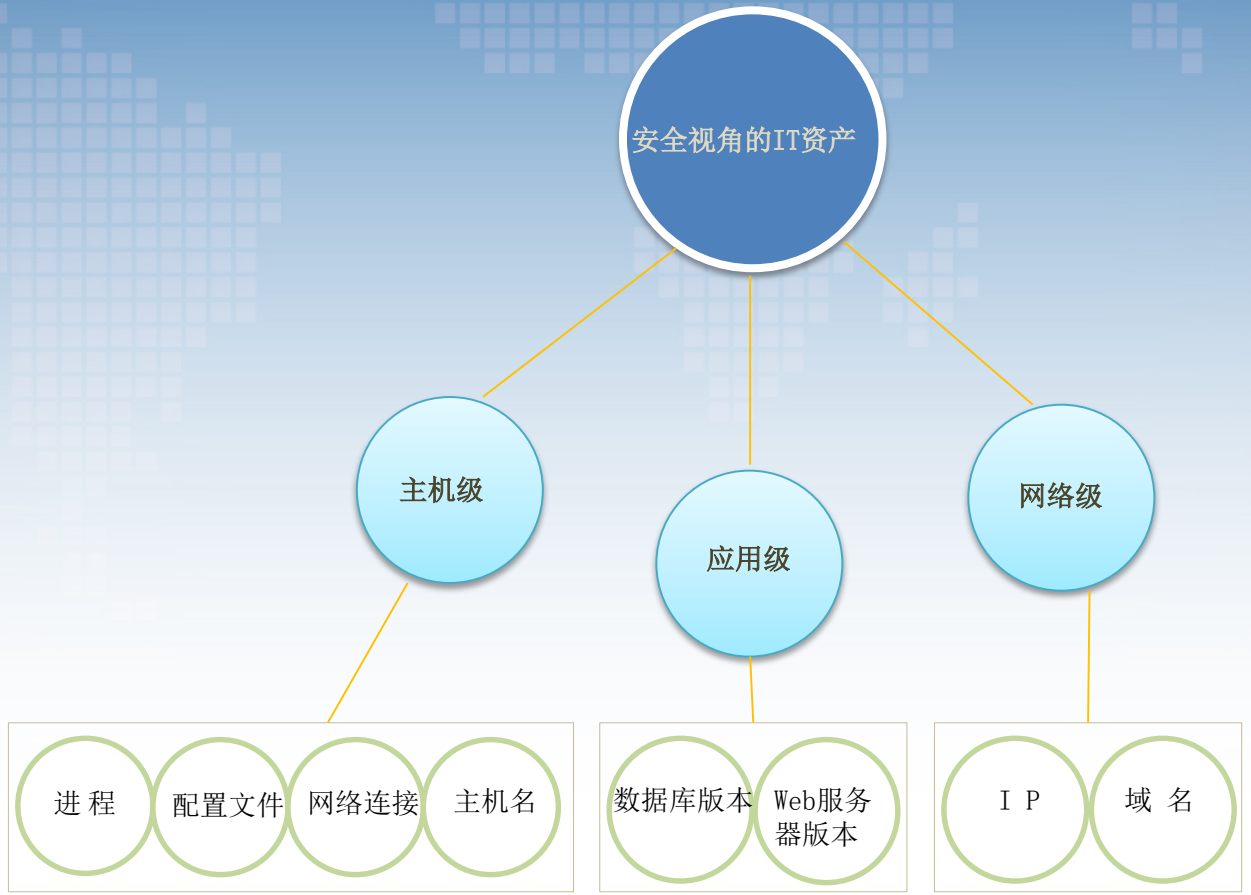
阶段规划实施

OWASP

Open Web Application Security Project

安全建设采用分期建设，主要是根据工作开展的紧迫性和易操作性进行分期规划。

在规划实施前，会先进行安全现状了解，主要是通过对网络、主机、终端、应用系统、数据等进行访谈和抽查，通过对资产信息的收集，然后分析其中所存在的安全问题。


安全视角的IT资产
主机级
应用级
网络级
进 程
配置文件
网络连接
主机名
数据库版本
Web服务器版本
I P
域 名

OWASP
Open Web Application Security Project

信息安全建设主要任务

信息安全建设中进行安全技术检查以及行业安全预警跟踪，尽量及时发现安全脆弱性并加固指导，为后期安全建设提供指导依据。

工作开展计划先防范风险属性由外向内，影响严重程度由高向低进行时间安排。

序号	项目	内容
1	终端安全管理	针对终端分类、访问控制、终端安全使用等运维管理，落实终端安全管理要求。
2	网络架构安全	评估网络架构安全，设计网络架构安全需求落实计算环境安全、区域边界安全、通信网络安全以及安全管理中心的设计要求，选择符合相应要求的安全产品，进行信息系统安全保护环境的产品解决方案。
3	渗透测试	安全专家利用安全工具并结合经验运用各种攻击技术对指定目标进行非破坏性质的模拟黑客攻击和深入的安全测试，发现信息系统隐藏的安全弱点。
4	安全评估与加固	通过对主机操作、网络设备、数据库、应用程序的安全检查发掘安全缺陷和配置错误，并对其中发现的安全问题进行加固指导。
5	专项安全检查	对整个网络系统开展专项检查。
6	安全应急保障	建立健全的通信保障和通信恢复应急工作机制，提高对突发事件的组织协调能力和应急处置能力，最大程度降低重大灾害、事件、故障等对通信业务的损害。
7	网络安全培训	根据需求定制培训计划，从技术和管理两个维度进行网络与信息安全的培训。
8	安全预警	定期搜集最新的安全预警信息、及时了解业界动态、最新漏洞、最新风险、协同预警等信息。
9	信息安全管理体系建设	设计信息安全制度体系，包括信息安全策略、信息安全规范、信息安全操作流程和细则。开展重要、紧急的安全体系文件落地执行。

OWASP
Open Web Application Security Project

安全建设方法

1	通过各种纵深防御体系，安全产品、威胁情报、态势感知等手段尽可能的将威胁阻挡在外。
2	假设攻击者渗透了部分内网服务器，但经过一定的混淆和蜜罐误导，让攻击者不知道敏感数据在哪，也分不清资产分布。
3	倘若遇到更坏的情况，攻击者找到了部分重要资产信息，但当他想回传这些信息时，这时候会采取一些措施让攻击者尽可能拿不走。
4	万一攻击者成功获取到了数据，但是数据加密强度足够，攻击者依然无法解密出明文。

OWASP
Open Web Application Security Project

反入侵方法

纵深防御	多维防御，也许单一的安全机制防御不了那些技术过硬的黑客，那就增加其他更多的安全防御体系。这样一来即便黑客再厉害，能同时破数道防御关口的难度已经明显增加。
降维	在攻击者不可控、不可感知的更深层次上做防御。例如入侵者在进入一个内网之后进行了一系列的信息搜集操作。但是入侵者可能不知道实际上自己进入的是蜜罐系统。蜜罐系统所做到的判定、感知对于入侵者来说是完全不可控的。
入侵容忍	当今的安全体系都不可能保证百分百安全。因此在进行整个安全体系设计的时候，要考虑的是假设在一定程度入侵的情况下，如何能够保证数据的完整性，而不是一味地追求零入侵，零入侵其实是不现实的。

OWASP
Open Web Application Security Project

企业安全**长期建设**

工程技术能力	安全做得好不好，很大程度上依赖于它的整体工程技术能力。因为对于企业而言，要使安全产品和安全技术最终转化为实现阶段，就必须要在IDC上全部落地，这个落地的能力依靠的就是企业整体的工程技术能力。
架构统一	一套成熟的安全体系架构可以让一个公司的安全建设更为高效。
深入研发	深入源头，把安全设计的理念融入产品，最终才能达到安全建设的效果。

OWASP

Open Web Application Security Project

谢谢