务实的网络安全

安恒信息互联网事业部总经理　张开

关于这个胖子

- 工作经历：
- 2004年开始 瑞星 websense
- 启明星辰
- 病毒 木马 漏洞分析
- 电话： 13693375655
- QQ: 58115562

常见的一些问题

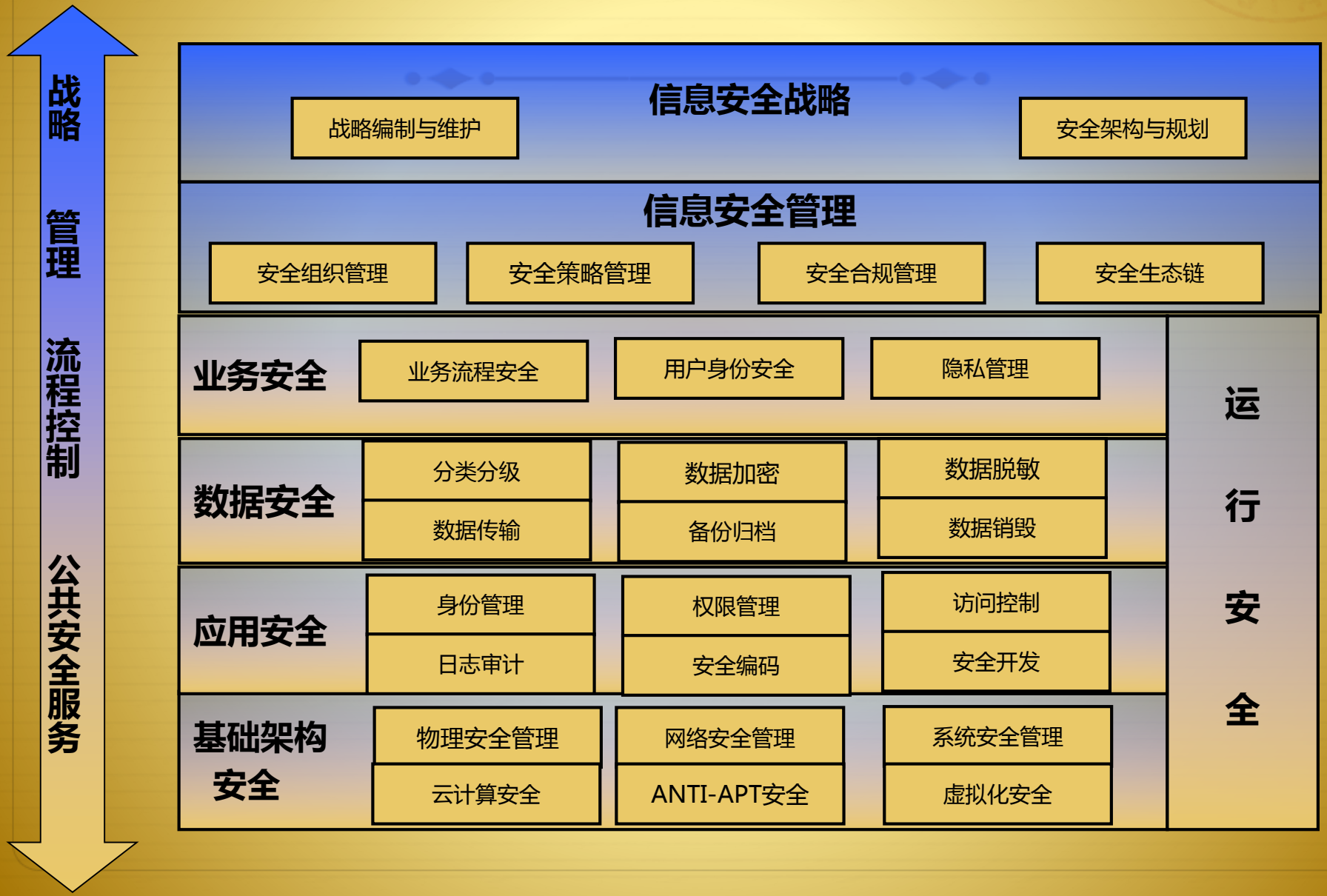
- 恶意黑客攻意行为导致用户信息泄漏
- 恶意冒充投资人进行恶意提现
- 大型Ddos攻击和CC攻击
- 来自黑客的恶意勒索

对手可能来哪世界的任何地方， 因为，P2P你们值得攻击

我们该怎么做

- 信息安全管控策略与商业目地的统一，并且成为公司战略
- 优先保护有价值的数据。
- 建立应急响应策略（因为不可能不出事）
- 寻找多个靠谱的安全合作商
- 向主动安全迈进

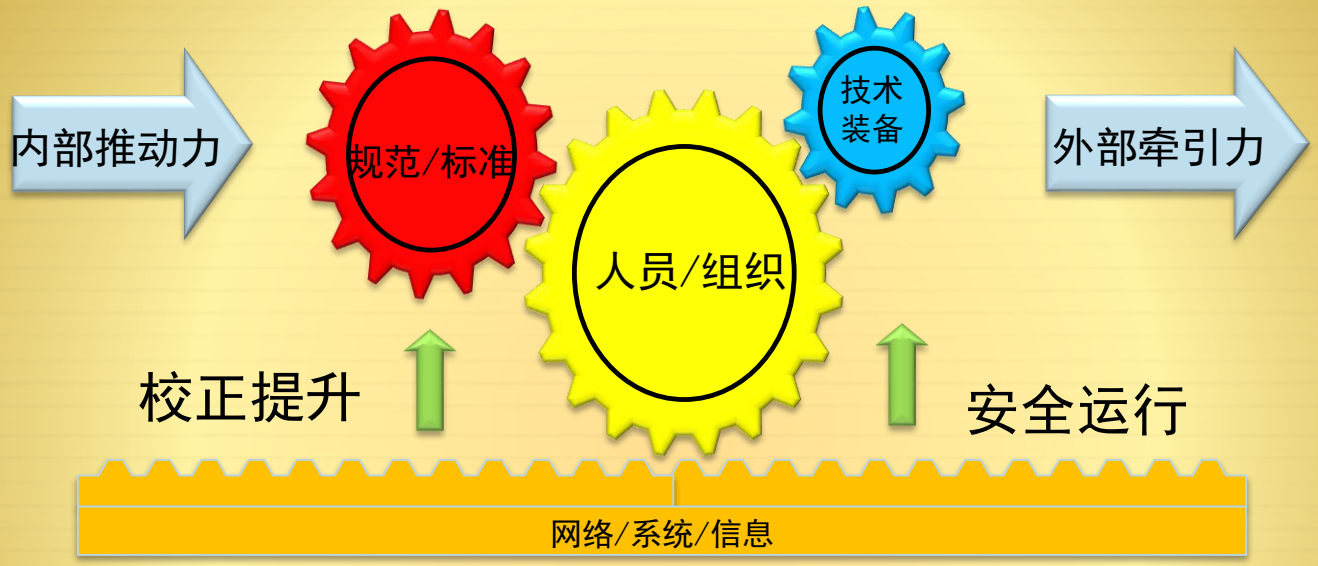
全面安全管理：IT安全管理框架




运营商安全增值
流量清洗与牵引
负载均衡
协议安全
CDN 内容发布
流量清洗与牵引
Web安全
联网环境
抗 Ddos设备
日志与监控
Email安全
防火墙
域名服务安全
虚拟化
网络边界
防病毒
云计算安全
入侵检测设备
终端权限控制
VPN设备
软件定义网络
用户端
堡垒机
安全域划分
操作系统安全
身份认证
路由器ACL
安全站点认证
存储与数据库安全
网络架构安全
补丁管理
核心设备
多链路与路由
行为审计
日志与监控
多层交换控制
主机级安全
加密与备份
通信加密
核心资产
安全域
日志与监控

具体的方法

信息安全整体工作思路



1、高层领导重视，中层策略清晰，基层执行得力；

2、宏观方向明确，中观概念清晰，微观标准统一；

3、操作有规矩，防范有措施，回查有依据；

4、横向联动、相互支援、知识共享。

离安全还有多远

挑战很多很多……

1、网络流量我们都知道有哪些吗？发生攻击或者入侵后我们可以发现吗，可以溯源吗？

2、业务处理发生拥塞，响应时间变长，我们是不是还在忙于定位问题，不停地找不同部门的不同负责人逐一定位和梳理？

3、我们现在基础架构、网络、系统、应用和数据到底安全吗？到底有多少漏洞，应该如何补长短板？

4、平台现在安全防护能力如何，安全措施是否到位，我们到底有哪些重要资产，会遇到哪些安全威胁，会遭遇哪些安全风险？

5、我们有信息安全团队和组织吗？我们有信息安全管理体系吗？我们的管理措施，流程控制和日常考核到位了吗？

6、我们的系统出了故障或者事故，应该怎么处理呢？我们有自己的应急预案吗？有知识库吗？进行过演练吗？是否可以真正管用？

7、我们的网络、系统、应用和数据库等配置合理吗？我们知道有多少帐户、进程和应用是该启动的吗？哪些配置应该是规范起来的呢？现有的虚拟化系统安全吗？

8、我们知道网站已经被挂马了吗？我们对于平台的现状是否清晰了解？

9、数码仓库的数据准确吗？是否被嗅探或者篡改了呢？交易数据是否安全，我们的交易平台会出新浪那样的问题吗？

……

关于未来

主要是给你们平事的。

关于这个胖子

- 工作经历：
- 2004年开始 瑞星 websense
- 启明星辰
- 病毒 木马 漏洞分析
- 电话： 13693375655
- QQ: 58115562