Qunar安全：从0到1

去哪儿网安全组

郭添森 2015/07

去哪儿? Qunar.Com 聪明你的旅行

关于我

- 2001.05 – 2011.05 艺龙网,OPS
- 2011.05 – 至今 去哪儿网,安全组
- 联系方式
  - 微信：eyasguo

目录

- ESG信息安全成熟度模型
- 第一阶段
- 第二阶段
- 第三阶段
- 如何建立安全团队威信
- 业务和安全如何平衡
- 未来

Enterprise Strategy Group
信息安全成熟度模型

Category	Basic Organizations	Progressing Organizations	Advanced Organizations
Philosophy	Cybersecurity is a "necessary evil."	Cybersecurity must be more integrated into the business	Cybersecurity is part of the culture.
People	CISO reports to IT. Small security team with minimal skills. High burnout rate and turnover.	CISO reports to COO or other non-IT manager. Larger security team with some autonomy from IT. Remain overworked, understaffed, and under-skilled.	CISO reports to CEO and is active with the board. CISO considered a business executive. Large, well-organized staff with good work environment. Skills and staff problems persist due to the global cybersecurity skills shortage.
Process	Informal and ad-hoc. Subservient to IT.	Better coordination with IT but processes remain informal, manual, and dependent upon individual contributors.	Documented and formal with an eye toward more scale and automation.
Technology	Elementary security technologies with simple configurations. De-centralized security organization with limited coordination across functions. Focus on prevention and regulatory compliance.	More advanced use of security technologies and adoption of new tools for incident detection and security analytics.	Building an enterprise security technology architecture. Focus on incident prevention, detection, and response. Adding elements of identity management and data security to deal with cloud and mobile computing security.

Source: Enterprise Strategy Group, 2014.

如何建立安全威信

- 领导力来源：专业技能、人格魅力、职权
- 专业技能
  - 专业、靠谱的安全解决方案
- 人格魅力
  - 服务部门，替对方考虑，权衡ROI等
- 职权
  - 组织架构
  - 插入关键流程
  - 奖惩

第一阶段

- 时间范围
  - 第1年
- 环境
  - 人员、设备、业务等
- 主要方向
  - 组建团队
  - 熟悉环境
  - 灭火
  - 设立基础的制度流程、技术标准
  - 解决网络层面的问题

网络

- 问题
  - 办公网：未隔离
  - 生产网：无ACL
  - VPN：用户名/密码认证
- 方案
  - 办公网
    - 做VLAN隔离：只出不进
  - 生产网
    - 设置ACL：只开http/https端口
    - Web服务统一由nginx做反向代理
    - Nginx配置走变更流程
  - VPN
    - 双因素认证

第二阶段

- 时间范围
  - 第2～3年
- 环境
  - 人员、设备、业务等
- 主要方向
  - 完善制度流程、技术标准
  - 合规：SOX404、PCI DSS
  - 建立自动化系统、确保安全规划能落地执行
  - 主要解决操作系统、数据库、系统应用、WEB应用层面的问题

操作系统

- 问题
  - 用户名/密码认证
  - 弱口令
  - 离职人员帐号
  - 通用用户名/密码
- 方案
  - 双因素认证
  - tcp wrapper
  - 公钥/私钥认证
  - 定期清理

数据库

- 问题
  - 空口令/弱口令: mysql, pg,mongod
  - Trust: pg
- 方案
  - 检测配置文件
  - Hash碰撞

系统应用

- 问题
  - 有哪些软件？版本？配置？漏洞?
- 方案
  - 收集软件版本、配置等信息
  - 漏洞检测，告警邮件

常见系统漏洞

- Web server
  - 默认管理后台:tomcat, jboss等
  - 启动帐号:nobody
  - 目录权限:root,755
  - 解析漏洞:nginx fastcgi, apache httpd等
  - Auto index
  - 压缩文件
- Spring/struts
- Jenkins/es等命令执行
- rsyncd
- Redis
- ……

WEB应用

- 问题
  - 鉴权：密码？复杂度？定期更改？离职员工？
  - OWASP TOP 10
- 方案
  - QSSO：集中管理，双因素认证
  - QWAF：静态、动态
  - 制定《安全标准》
  - 内部测试、众测

第三阶段

- 时间范围
  - 第4年+
- 环境
  - 人员、设备、业务等
- 主要方向
  - 数据安全
  - 业务安全

数据安全

- 问题
  - 用户隐私、交易详情、产品技术文档、源码等数据如何有效保护
- 方案
  - 制定标准
  - PCI DSS(支付卡行业数据安全标准)认证
  - 数据加密、清洗、打码
  - 自动抽样
  - 授权
  - 人工巡查github等渠道，处罚?
    - 处罚方式：通报批评？罚金？降级？开除？
    - 处罚对象：当事人？直接上级？

业务安全

- 问题
  - 帐号安全：垃圾注册？撞库?
  - 反欺诈：用户/商户作弊
- 方案
  - 帐号安全
    - 统一入口，收缩防线
    - 动静结合，多层防御
  - 反欺诈
    - 异常行为分析

业务和安全如何平衡

- 安全的使命
  - 消除风险？控制风险？
- 基础架构：OPS
  - OPS核心职责：安全稳定高效
  - 合作共赢
- 业务部门：开发/QA/产品
  - 产品流程：需求-开发-测试-上线-运营
  - 插入时机和方式
    - 过早优化？过度优化？
  - 冲突解决办法：妥协？升级？

未来

- 挑战?
- 机遇?

Q&A

- 谢谢