运维安全管理

**运维安全的四个层次**

## **网络安全**

### **网络设备的安全**

* 思科、华为等网络设备定期升级，修复bug和曝出的漏洞
* 公网防火墙，核心交换机等核心网络设备的管理

### **外网安全策略**

* IDC，防火墙策略，严把上行端口开放
* 公网上下行流量监控
* 对DDos攻击提高警惕，提前准备应急预案
  + 临时提高流量，硬抗
  + 启动流量清洗，将攻击流量引入黑洞，有可能误杀正常用户

### **专线安全策略**

* 对涉及金融、支付等项目设立专线

### **VPN安全策略**

* IPsec VPN：site to site
* OpenVPN： peer to site
* 摒弃PPTP等不含加密算法的vpn服务
* 端口全禁止，需要通信的申请审批后，再由管理员开放

## **数据安全**

### **数据库用户权限**

* 管理员权限限定，不允许远程root
* 定期更换管理员密码
* 应用权限最小化，专人管理
* 手动查询权限可审计

### **数据库审计设备**

* 数据库主库不能开一般查询日志（为了性能）
* 交换机上镜像流量，接入审计设备，实现实时审计
* 不要设计串行在系统里，形成单点和瓶颈

### **数据库脱敏**

* 姓名、身份证、手机号、银行卡号等敏感信息应脱敏处理
* 对程序脱敏协同系统架构部共同出规范
* 对手动查询权限脱敏，按列授权，录屏

### **备份策略**

* 每周全备，每天增备
* 备份文件要每天利用内网流量低谷时间，推送到远程主机，有条件的应跨机房备份
* 一定要规划定期恢复测试，保证备份的可用性

## **应用安全**

### **操作系统安全**

* 系统基础优化（内核优化，优化工具）
* 日期，时区同步
* root密码复杂度足够高，需要在操作系统里做定时过期策略
* 每三个月使用脚本更新服务器的root密码和iDrac密码，并将更换后的密码加密打包发送给指定管理员邮箱，同时提交gitlab
* 对系统关键文件进行md5监控，例如/etc/passwd，~/.ssh/authorized\_keys文件等，如有变更，触发报警
* 定期查毒，漏扫，定期安排更新操作系统
* /etc/ssh/sshd\_config里配置：
  + PasswordAuthentication no
  + PermitRootLogin without-password
* 使用saltstack等批量管理软件进行特权命令执行和备份脚本执行（避开ssh协议）

### **应用系统安全**

#### **WEB应用防火墙（WAF）**

* 防SQL注入
* 防CC攻击
* 防XSS跨站脚本

#### **应用系统漏洞**

* 关注0day漏洞新闻
* 及时整改并上线投产
* 组织技术力量测试，复现

#### **日志收集和分析**

* 完善日志收集方案，集中转储
* 通过应用系统日志分析，进行安全预警

#### **DNS劫持**

* 全站https，购买泛域名证书
* 有条件的可以自己维护公网DNS，上dnssec数字签名
* 采购基调、听云等第三方拨测服务，分布式监控网站质量
* 向ISP投诉，工信部举报

#### **Basic Auth**

* 在nginx上做，非常简单
* 对防脚本攻击有奇效

### **企业邮箱服务器安全**

#### **推荐使用微软的Exchange**

功能强大，维护相对简单

#### **投产反垃圾邮件网关**

投产梭子鱼反垃圾邮件网关，防伪造发信人

#### **群发审核管控**

#### **用好邮件组**

#### **接入AD域控**

### **域名安全管理**

#### **做好ICP备案**

* 域名证书
* 域名实名认证（公司模板）
* 接入商处蓝色幕布拍照
* 法人身份证、管理员身份证
* 网站真实性核验单

#### **公网解析**

* 专人管理，邮件申请，审批
* 将业务解析至不同公网IP出口，双活机房
* 智能解析，解析至不同线路
* 如有条件，可购买公网解析套餐服务，安全服务等

## **内网安全**

80%以上的企业IT安全问题出自内网安全

### **堡垒机**

* 一定要强制使用堡垒机登录服务器
* ssh私钥通行短语机制，避免密钥失窃
* 定期审计堡垒机操作日志
* 如果有必要，可以上2FA（双因子验证）

### **AD域控**

有条件一定要接入windows域控，要求密码复杂度和定期过期

* 邮箱
* wifi
* vpn账号密码
* 内网系统账号
* 业务系统账号
* 网络设备等

### **办公网安全**

* 专业的HelpDesk团队
* 企业级杀毒软件
* 办公电脑接入域控
* 上网行为管理
* 流量监控，mac地址绑定
* 有条件的可以在办公环境上一个小型的业务机房
* wifi管控，单做guest接入点，不能访问业务核心网络

坚持原创技术分享，您的支持将鼓励我继续创作！

打赏

[基于ITIL的IT运维管理](https://blog.stanley.wang/2019/02/13/%E5%9F%BA%E4%BA%8EITIL%E7%9A%84IT%E8%BF%90%E7%BB%B4%E7%AE%A1%E7%90%86/" \o "基于ITIL的IT运维管理)

[OSI网络参考模型](https://blog.stanley.wang/2019/02/14/OSI%E7%BD%91%E7%BB%9C%E5%8F%82%E8%80%83%E6%A8%A1%E5%9E%8B/" \o "OSI网络参考模型)

* 文章目录

* 站点概览

1. [1. 运维安全的四个层次](https://blog.stanley.wang/2019/02/13/%E8%BF%90%E7%BB%B4%E5%AE%89%E5%85%A8%E7%AE%A1%E7%90%86/" \l "%E8%BF%90%E7%BB%B4%E5%AE%89%E5%85%A8%E7%9A%84%E5%9B%9B%E4%B8%AA%E5%B1%82%E6%AC%A1)

© 2020  Stanley Wang | 278k | 4:13