阿里云 云栖社区

云栖社区 开发者的云中江湖

IT大咖说 知识分享平台

云平台安全 天公

企业上云安全加固最佳实践

个人介绍

相关经历：

- 聚石塔电商云安全
- 集团应用上云安全
- 云平台安全

问题是什么？

- 黑客入侵
  - 应用漏洞
  - 系统被黑
  - 数据泄露
  - DDOS攻击，网站不可用

- 该怎么办
  - 需要一支专业的安全团队？

云计算能帮我们什么？

- VPC
- 云waf
- DDOS防御
- 入侵检测

打一套组合拳

- 利用好云计算的安全能力 == 一支专业的安全团队
  - 网络架构安全：VPC VS Classic
  - 基础设施安全：ECS、RDS、OSS。。。
  - 账号安全：保管好钥匙
  - 应用安全：保护好我们的应用

网络架构安全

- VPC VS Classic
  - VPC：专有网络 （推荐）
    - 与企业私网打通的能力，构建混合云
    - 默认对公网网络隔离
    - 自定义网段、安全组隔离策略
  - Classic：经典网络
    - 每个ecs 一个公网ip+一个私网ip
    - 默认与其他租户处于同一网络平面
    - 安全组：访问控制能力

基础设施安全

- ECS安全（计算）
  - 远程登录：
    - ssh key验证（推荐）
    - 密码登陆：使用强密码，12位以上，同时包含数字、大小写字母、特殊符号
  - 端口开放限制：
    - 只开放必要的服务：公网开放80、443等，内网访问全部拒绝
    - 高危端口只允许本机访问：mysql、redis、memcache等
    - 部分服务设定ip白名单：ssh、rdp，安全组
  - DDOS防御：
    - 云盾5G免费清洗，商业用户云盾高防

基础设施安全

- RDS安全（DB）
  - 密码安全：
    - 使用强密码，12位以上，同时包含数字、大小写字母、特殊符号
    - 应用中密码：接入kms加密，防止应用漏洞导致密码泄露
  - 账号权限控制：
    - 根据不同角色，不同应用，使用不同账号，设置不同权限
  - 网络访问控制：
    - Classic：ip白名单设置
    - VPC：vpc内可访问，可通过ip白名单进一步控制
  - 日志审计：
    - sql执行日志审计查询
    - 云盾waf防SQL注入
  - 数据备份恢复

基础设施安全

- OSS安全（存储）
  - 按安全等级区分bucket，设置不同安全级别
    - 公共读：js、css、jpg等静态资源
    - 私有：敏感文件，云上云下系统数据中转
    - 公共读写：不建议使用
  - 防盗链功能
  - 日志审计

账号安全

- 云账号安全（云计算平台的钥匙）
  - 风险：弱密码、撞库、爆破
  - 策略：
    - 密码安全：
      - 强密码：12位以上，同时包含数字、大小写字母、特殊符号
      - 定期更换密码，与其他网站使用不同密码
      - 保密邮箱、保密问题
    - 二次认证：
      - MFA：绑定手机设备，随机动态口令，登陆验证
      - 控制台高危操作短信验证
    - 操作审计：
      - ActionTrail

账号安全

- AK安全（云产品API的钥匙）
  - 风险：AK泄露(github上传等场景)，导致数据泄露
  - 策略：
    - 禁用主账号AK
    - 权限分离：
      - RAM访问控制：不同角色，不同子账号，不同权限（支持阿里云绝大多数产品）
      - 减少泄露某个AK对全局带来的影响
    - 子账号AK白名单：
      - 可设置调用访问来源ip、VPC id
      - 即使AK泄露，也有额外多一层的保护

应用安全

- DDOS防御：SLB+云盾高防
- web攻击防御：WAF云防护，防御SQL注入、XSS、代码执行
- 应用安全漏洞扫描：态势感知扫描（主机基线漏洞扫描、web漏洞扫描）
- 云盾入侵检测和防御：
  - 防止远程爆破
  - 及时发现webshell和肉鸡行为
- 自主日志分析：
  - web访问日志+ODPS离线分析能力
- 威胁情报：
  - 加入先知，拥有自己的SRC
  - 先知众测，发现入侵隐患

安全不止这些

- 更个性化的安全需求
  - 堡垒机
  - VPN
  - 业务风控
  - 内容安全
  - 安全托管

总结

- 上云安全责任：企业与云平台共同承担
- 云平台：
  - 提供基础安全功能
  - 给企业赋能安全能力
- 企业：
  - 做好安全管理，打好平台安全能力组合拳
  - 以最小化成本，来最大化提升安全水位

THANKS