攻防场景下的安全解决之道

2019年11月12日　杭州

内容简介

- 从网络攻防的实际场景出发，着眼攻防时空，探索主动防御的解决方案。

目录

一、 网络安全的本质

- 网络安全的本质是攻防
- 网络攻防发生在
  - 数据传输的地方
  - 数据处理的地方
  - 数据存储的地方
- 网络防御面临的难题
  - 系统本身的缺陷和漏洞不可避免
  - 超常的重保措施难以持续

二、网络安全防御体系

- 结构-多层次覆盖
  - 控制平面
  - 管理平面
  - 数据平面
- 过程-多维度渗透
  - 配置管理
  - 故障管理
  - 性能管理
  - 计费管理
  - 安全管理

三、网络安全防御策略

- 最大化防御空间
  - 防控措施全面覆盖，使局部的安全漏洞和安全威胁被压缩在有限的空间内
- 最小化响应时间
  - 取决于威胁感知能力及其联动控制的自动化程度，把安全漏洞和安全威胁压缩在有限的时间内

四、解决方案

- 安全管理平面——信息安全通报平台
  - 网内资产台帐发现与管理
  - 威胁情报共享
  - 一体化管理网内风险、清单，安全评估、安全预案
  - 与上级部门通报平台联动，实现自主信息上传与接收

四、解决方案

网络系统-基于流量感知

- 威胁感知来源：多种流量监测工具
  - 防御系统支持的流量监测设备清单
- 阻断控制措施：网络访问控制、主机访问控制
  - 防御系统给支持的网络防火墙和主机安全控制系统
- 防御系统
  - 接收监测工具的源数据
  - 分类处理威胁数据源
  - 数据源分析
  - **决策阻断行为**
  - 自动化防问控制阻断，或结合人工干预

四、解决方案

网络系统-网络控制平面

- 威胁感知来源：路由器、防火墙、交换机等网络设备
  - 防御系统支持的网络设备清单
- 阻断控制措施：路由器、防火墙等网络设备访问控制
  - 防御系统支持的网络设备清单
- 防御系统
  - 自动化采集路由器、防火墙交换机等网络设备信息：路由表、ARP表、网关地址、访问控制策略、CPU利用率、接口流量等信息
  - 通过数据源分析识别威胁源
  - 决策阻断和控制行为
  - 自动化网络访问控制阻断、设备配置，结合人工干预

四、解决方案

主机系统

主机安全控制系统

- 操作系统加固
- 用户登录控制
- 文件系统保护
- 网络访问控制
- Web应用防护

防御系统

- 从Agent获取日志、告警、配置信息等数据源
- 通过数据源分析识别安全威胁
- 自动化主机控制和网络层访问控制联动

四、解决方案

数据库系统-生产环境

- 威胁感知来源：数据库审计工具
- 阻断控制措施：数据库防火墙
- 防御系统
  - 接收监测工具的源数据
  - 分类处理威胁数据源
  - 数据源分析
  - 决策基于SQL的阻断行为
  - 自动化访问控制阻断，或结合人工干预

四、解决方案

数据库系统-数据加密与脱敏

- 数据加密
  - 数据备份等脱离生产环境的数据只能回到生产环境才能解密
  - 非授权途径获取的数据无法解密
- 数据脱敏
  - 系统测试、分析研究等目的从生产环境到处数据做脱敏处理

谢谢观看！