北大校园网安全服务与ARP病毒防治

钱杰

北京大学计算中心

介绍提纲

- 安全现状及防范措施
- 桌面病毒防范
- 防病毒软件选型
- 北大ARP欺骗防治

校园网安全现状

- 蠕虫病毒
- ARP病毒
- 木马程序
- 盗版软件的大量使用
- 操作系统漏洞
- 防病毒手段单一
- 用户安全知识匮乏、水平参差不齐

主要安全防范措施

- Fortinet-5000千兆防火墙、Cisco 6509千兆防火墙模块
  - 基础IP攻击防护；保护关键服务器
- Cisco SCE
  - 主干流控、P2P限流
- 网络管理系统
  - 用户定位：用户帐号->IP->MAC->交换机端口
- 微软关键补丁分发系统WSUS
- 邮件、桌面防病毒系统：Symantec
- IDS部署于总出入口处，监控异常事件

桌面病毒防范

- 现状:
  - Symantec企业版10.1
  - 实际使用用户数：15,000多
- 系统构成：
  - 集中管理服务器：
    - 用户策略管理
    - 病毒定义码分发
    - 收集客户端安全状况
  - 用户桌面病毒库更新方式
    - 推模式：集中管理服务器向用户桌面推送病毒库更新
    - 拉模式：用户开机到集中管理服务器检查病毒库是否有更新，并以此实施更新

桌面病毒防范

- 客户端病毒库更新策略：
  - 推模式+拉模式
  - 病毒码更新后，系统自动推送
  - 用户每天定时到系统拉
  - 更新及时

桌面病毒防范

- 办公区使用情况
  - 正版系统, 有微软补丁的支持
  - 以工作为主、简单上网功能，安装来路不明软件少
  - 使用情况良好

桌面病毒防范

- 学生和教工家属区使用情况
  - 以学习、生活、娱乐为主
  - 盗版系统占主流，系统漏洞多，下载安装软件多
  - 效果不佳

桌面病毒防范

- Symantec优点:
  - 企业版：
  - 资源占用不大、安静
  - 稳定：体现隔离机制，在没有正确处理方式前提下不会删除
  - 简单：适合初级用户
  - 误判率低: 与病毒更新频率有关系
  - 非常适合企业办公用
- 存在问题:
  - 表现在木马防御能力弱
    - 脱壳差（靠传统静态特征扫描码）
    - 以防为主、无主动防御

防病毒软件选型：测试情况

- Kaspersky:
  - 脱壳能力强
    - 国内现状,木马多, 多次加壳, 特征码技术
  - 具有主动防御功能
    - 监控系统进程行为和注册表的修改
  - 更新频率高，每天多次，误判率高
  - 内存、CPU资源消耗大
  - 适合个人用户(尤其学生)
  - 稳定性差
  - Licence控制严格

防病毒软件选型：测试情况

- McAfee
  - 按访问扫描/实时监控
  - 缓冲区溢出保护的功能，通过截取一些API函数方式，对缓冲区代码进行判断，检查返回的父函数是否在堆栈内。若在就结束当前有问题的进程。
  - 定制访问保护规则, 功能强, 配置灵活
  - 指定端口、文件、文件夹和共享资源的访问来主动防止入侵
  - 适合有一定计算机安全知识的用户使用

防病毒软件选型：测试情况

- NOD32
  - 软件体积小, 消耗系统资源少、速度快
  - 简单、易用性好, 无任何配置
  - 稳定、安静
  - 虚拟机强, 预测未知病毒能力强
  - 病毒库小(基因码)
  - 以防为主, 无主动防御功能
  - 适合初级用户/爱好者

防病毒软件选型

- 校园网服务要用企业版
  - 优点：
    - 实现集中管理、统计报表、License管理、病毒库统一校内更新。
    - 经济：购置成本低、运行成本低
    - 更新及时
    - 节约出口带宽
  - 缺点：
    - 策略集中,灵活性差
    - 校园外更新困难
    - 流动用户多，授权用户数控制管理困难
  - 对校园网松散管理模式, 套装产品:
  - 防火墙，IPS功能策略无法统一定制

防病毒软件选型

- 用户的多样性对于防病毒软件的多样性需求
  - 完全不了解计算机的教工和部分学生：
    - Symantec/NOD32 以防护为主的防病毒软件
    - 中病毒后建议:重做系统
  - 对具有一定动手能力和计算机安全知识的用户（大部分学生）
    - 具有主动防御的防病毒软件
    - Kaspersky、McAfee（访问保护策略的定制）
  - 办公区部分
    - 考虑到易用性、稳定性
    - Symantec/NOD32

防病毒软件选型

- Symantec：　0.5万用户
- NOD32：　0.5万用户
- Kaspersky：　1万用户
- McAfee：　0.5万用户
- 使用期：　3年

辅助安全工具

- 不能过分寄希望于防病毒软件
- 采用主动防御措施
  - 奇虎360
  - 需要具备一定计算机安全知识
- 系统还原、虚拟机、影子系统

北大ARP欺骗防治

- 理想方式
  - 全自动方式
  - 程序自动分析、自动辨别、自动封禁
  - 存在问题
    - 准确性
    - 共享HUB
    - 单MAC→多口

北大ARP欺骗防治

- 方式一：系统辅助、人工确认
  - 疑似主机获得
    - 网管系统定期搜索疑似ARP病毒感染主机
    - 用户主动报告：电话、BBS、ITS
  - 人工核实确认，封禁交换机端口
  - 在线公布校园网中被封禁的MAC地址清单

北大ARP欺骗防治

- 方式二： 静态绑定、减少扩散
  - 在路由器:
    - 静态MAC绑定, 即把DHCP中已分配IP池进行MAC静态绑定
    - 由程序每隔5分钟进行一次操作
    - 封禁特定病毒网段
  - 实施范围
    - ARP病毒高发的学生宿舍区、图书馆
  - 效果：提高较大

北大ARP欺骗防治

- 桌面系统的防护思考
  - 安装常用ARP防火墙
    - AntiARP
    - 金山ARP防火墙
    - 360安全卫士
  - 开发ARP防护客户端
    - 以上网认证客户端为载体
    - 增加ARP防火墙功能

北大ARP欺骗防治

中了ARP病毒后的处理

中了ARP病毒，各种防病毒软件或专杀工具很难完全清除，只有重装系统，并施加相关防护措施，才可以得到比较彻底的恢复，具体步骤如下：

- 格式化系统盘，重新安装操作系统
- 安装完操作系统后，不要打开除操作系统盘之外的任何操作盘符（因为其它盘里有自动执行的病毒存在）。
- 连接网络，下载Windows补丁，安装防病毒软件
- 启动防病毒软件，查杀系统所有的硬盘
- 今后注意不要轻易运行来历不明的软件。

谢　谢！