内网安全病毒防范

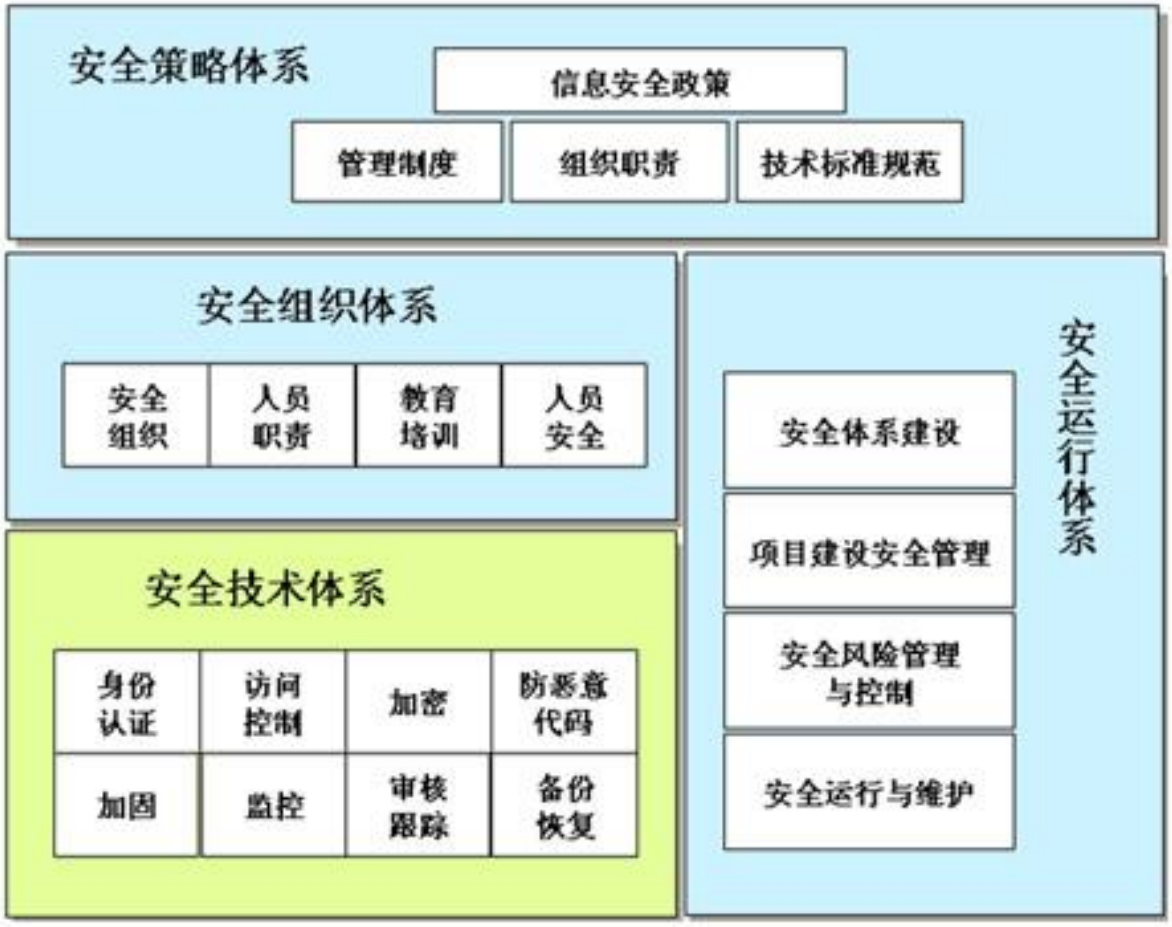
——瑞星信息安全沙龙

2011年09月23日

概述

- 与互联网实现完全的物理隔离
- 可能存在一定涉密性要求
- 主要面临内部威胁
- 强调监控审计

内网安全体系


安全策略体系
信息安全政策
管理制度
组织职责
技术标准规范
安全组织体系
安全组织
人员职责
教育培训
人员安全
安全技术体系
身份认证
访问控制
加密
防恶意代码
加固
监控
审核跟踪
备份恢复
安全运行体系
安全体系建设
项目建设安全管理
安全风险管理与控制
安全运行与维护

制度建设和意识培养

- 制度的建设
  - 完善的机房管理制度；
  - 完善的网络使用制度；
  - 责任到人的设备管理制度；
  - 网络安全应急预案和定期网络评估制度；
- 人员安全意识的培养

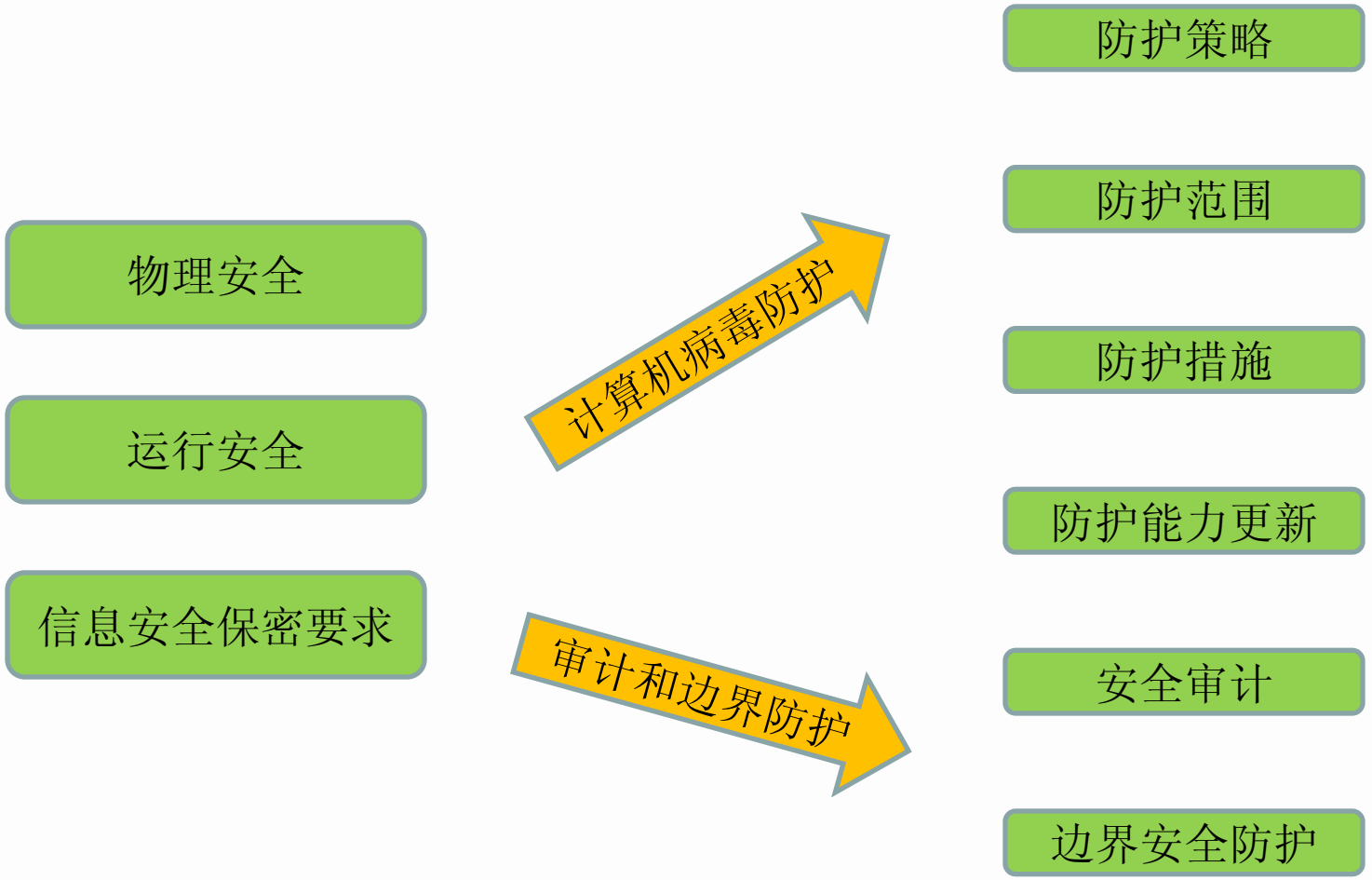
网络安全防护系统建设

- 合理的网络安全区域划分
- 网络安全防护系统建设
  - 使用防火墙来进行网络安全边界的防护
  - 入侵检测系统对网络内部的做到了实时的监控和预警
  - 合理利用安全审计系统
  - 利用网关防病毒系统将病毒拦截在网络外部
  - 非法外联系统做好实时预警和阻断
  - 身份验证
  - 综合网络安全管理平台

安全可控的网络

- 连入网络的节点的监控
- 非法对外访问的监控
- 网络数据和审计
- 实时病毒监控
- 全网的统一监控

涉密信息系统基本要求


物理安全
运行安全
信息安全保密要求
计算机病毒防护
审计和边界防护
防护策略
防护范围
防护措施
防护能力更新
安全审计
边界安全防护

计算机病毒防护

- 制定文档化的防病毒策略；
- 防护范围包括：工作站、服务器和移动计算机；
- 能够防止病毒通过网络、电子邮件、移动存储介质等途径进行传播；
- 加强存储设备的接入管理；
- 软件的安装需先经过检查处理；
- 应及时更新计算机病毒库；
- 不得通过互联网进行在线升级；

审计

- 审计记录存储的时间
- 审计终端防病毒软件的卸载
- 防止审计记录被人为删除

边界安全防护

- 防火墙
- 入侵防范
- 防病毒网关
- 信息过滤
- 边界完整性检查

内网管理面临的问题

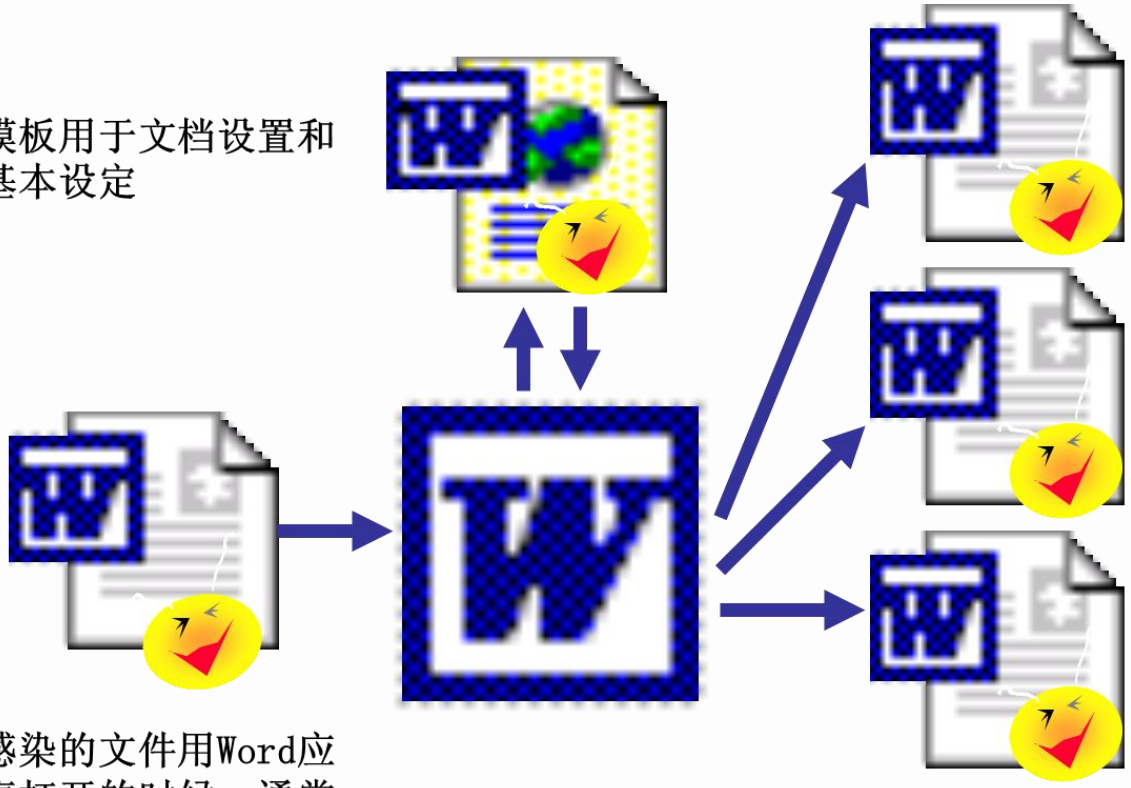
- 如何及时发现系统漏洞并自动分发补丁；
- 如何防范移动电脑和存储设备随意接入内网；
- 如何防范内网设备非法外联；
- 如何在全网制订统一的安全策略；
- 如何点对点控制异常客户端的运行；
- 如何防范内部涉密重要信息的泄露；
- 如何快速有效的定位网络中病毒并处理；

内网安全面临的病毒

- 宏病毒：通过office文档传播
- 脚本病毒：CAD病毒、VBS病毒
- U盘病毒：利用自动播放特性进行传播
- 蠕虫病毒：通过网络进行传播

宏病毒

通用模板用于文档设置和宏的基本设定

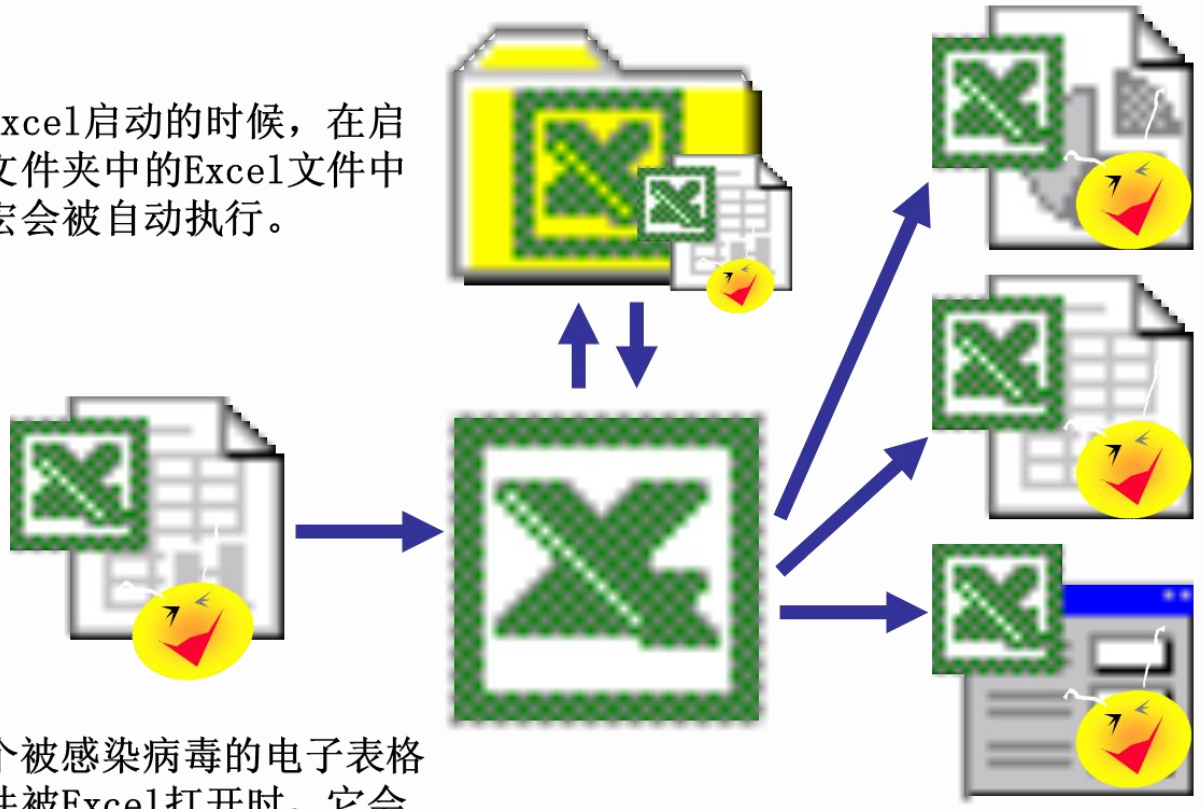


当被感染的文件用Word应用程序打开的时候，通常其中包含的宏代码就会复制到通用模板中去

当病毒长驻在通用模板中时，它会自动生成一些额外的拷贝到别的被Word打开的文档中去

宏病毒

当Excel启动的时候，在启动文件夹中的Excel文件中的宏会被自动执行。



一个被感染病毒的电子表格文件被Excel打开时，它会自动在启动文件夹中添加一份自身的副本。

当启动文件夹中有宏病毒时，它会在所有用Excel打开的电子表格中添夹自身的副本。

宏病毒防范

- 进行完整的全盘杀毒
- 文件监控中勾选未知宏和包含宏的文件

脚本病毒

- CAD脚本病毒：生成多个acad.lsp文件；
- VBS脚本病毒：通过共享、网页、聊天工具传播；

脚本病毒防范

- 进行完整的全盘杀毒
- 文件监控中勾选未知脚本和包含脚本的文件

U盘病毒

下面的防范方法是否起到作用？

- 组策略——关闭自动播放
- 创建免疫文件夹Autorun.inf
- 软件限制策略：?:\autorun.* “不允许的”

U盘病毒

- svchost.exe读取autorun.inf
- explorer.exe读取autorun.inf
- explorer.exe将autorun.inf里的相关内容写入注册表中MountPoints2这个键值

MountPoints2具体位置：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

该注册表主键下，记录并管理了系统对所有“盘符”的双击操作和右键菜单内容

U盘病毒

[autorun]

OPEN=EXPLORER.EXE

shell\open=打开(&O)

shell\open\Command=EXPLORER.EXE

shell\open\Default=1

shell\explore=资源管理器(&X)

shell\explore\Command=EXPLORER.EXE

把notepad.exe复制到U盘重命名为EXPLORER.EXE

U盘病毒

- 组策略——关闭自动播放　失败
- 原因：没有阻止Autorun.inf运行

- 创建免疫文件夹Autorun.inf　失败
- 原因：很轻易被删除

- 软件限制策略：?:\autorun.*　“不允许的”　失败
- 原因：没有阻止explorer.exe读取Autorun.inf

U盘病毒防范

- 开启瑞星U盘拦截功能
- 开启瑞星系统加固功能
- 禁用停止Shell Hardware Detection服务
- 修改注册表MountPoints2 键值权限
- 安装KB967715补丁，并通过组策略禁用自动播放
- 注意：安装更新 967715 时，系统仅在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\ 注册表中创建 HonorAutorunSetting 注册表项。注册表项的默认值为 0x1。安装最新更新之前，系统中不存在此注册表项。
- 安装KB971029补丁

蠕虫病毒

- 独立程序，不需要宿主文件
- 寄存在内存中，并不感染引导区和文件
- 通过网络、移动介质传播

MS08-067病毒症状

- 进程中多个rundll32.exe进程，导致计算机运行速度减慢；
- 创建大量计划任务文件：AT*.job
- 不断的向外发送垃圾数据包，使用netstat命令可以看到多个通过139、445端口建立的连接；
- 内部网页打开速度减慢；
- 不能访问安全网站和微软网站，停止dns client服务后，可以正常访问；
- 开机时报svchost.exe进程错误

MS08-067病毒处理方法

- 全网安装KB958644补丁
- 设置强密码
- 坚持全网全盘杀毒
- 关闭读写共享
- 可关闭139、445端口

MS08-067病毒源确认方法

- 通过抓包工具进行抓包分析
- 通过netstat命令查看
- 通过NT日志查看
- 通过染毒文件路径判断

指： C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5下index.dat文件内容

谢谢大家