



终端安全管理(监控审计)方案

桌面终端计算机因其日益强大的运算和存储能力,已经发展成为组织单位内部重要的信息存储和处理工具,为了保护终端计算机上存储的这些重要数据,防止内部人员有意或无意的信息泄漏,必须采取技术手段加强对内部终端计算机的安全管理。

● 安全风险分析:

- 1) 终端计算机上的软件由用户自己维护,无法集中监控和管理终端计算机的软件安装,易被装入木马或黑客软件等恶意程序,造成计算机信息失泄密。同时也可能因为使用盗版软件而引起法律诉讼;
- 2) 内部计算机的使用缺乏统一的监控,无法对各种移动存储设备进行监控,也无法对计算机是否增加第二块网卡等硬件资产变更情况监控,由此可能造成计算机信息和网络信息失泄密;
- 3) 终端计算机的系统升级和补丁操作缺乏统一的管理,一旦出现需要升级的文件或补丁程序,需要终端计算机用户手动运行,容易造成管理上的漏洞,给内部计算机和网络安全造成隐患;
- 4) 终端计算机上带有各类设备端口,内部工作人员很容易通过计算机外设端口和打印机将内部敏感信息带走;
- 5) 对终端计算机的上网行为管理困难,也无法进行统计,内部工作人员访问不健康网站行为无法及时发现和阻断,容易引起刑事事件;同时内部工作人员也可能通过网络途径泄漏内部敏感信息;
- 6) 内部工作人员通过 Modem 拨号、ADSL 拨号和无线拨号等私自建立对外的网络连接,形成非法的网络出口,从而为外部黑客非法入侵提供途径,容易造成安全隐患;
- 7) 外部计算机通过非法接入方式接入内部网络,访问内部信息系统中的计算机和服务器资源,可能造成信息失泄密;
- 8) 内部移动存储介质的使用难以控制,容易成为内部网络病毒感染和传播的重要源头。同时,通过移动存储介质随意拷贝内部文件,也很容



易造成内部重要数据信息的失泄密。

- 9) 终端计算机缺乏强审计系统。没有审计系统,对终端计算机用户的违规行为和其他入侵行为缺乏监管手段,也无法进行责任认定。

● 解决方案:

中安源可信网络安全平台为终端计算机提供了全面的管理、监控和审计功能。

具体功能描述如下:

- 1) 系统实时远程监视和控制客户端计算机的状态,这些状态包括:安装的应用程序、服务、驱动及他们的运行状态;当前网络连接状态、打开的窗口、运行的进程、系统的用户和用户组、共享目录、当前的屏幕截图等信息,并可以实时远程控制;
- 2) 对终端计算机上的硬件设备、安装的软件、进程和服务等进行有效的集中管理,当硬件设备和软件信息等发生变更时,会及时通知报警,并留下记录,并可根据日志记录进一步生成审计报告;
- 3) 管理员可以对每台终端计算机进行设备使用授权,比如允许或者禁止 USB 存储设备的使用等;
- 4) 可以对内网中的终端计算机的应用程序进行控制。这些应用包括:进程、窗口和服务。管理员可以以黑名单或者白名单的方式授权,在“白名单”应用模式下,可以确保不在允许清单中的应用程序不能被允许运行。
- 5) 支持对多种网络协议的审计和控制,包括 POP3/SMTP 电子邮件、Web 邮件、网页访问和 FTP 协议,并可以记录全部访问记录和内容;
- 6) 系统支持操作系统和应用程序的自动和强制的升级,一旦出现需要升级的代码,可以通过本系统进行网络全网范围内的所有计算机的自动检查和升级。
- 7) 支持用户文件操作记录、打印行为记录、Web 附件上传记录等功能;
- 8) 支持远程桌面控制,可以远程对选定的计算机终端进行实时维护;
- 9) 提供 IP 绑定、非法拨号阻断和非法接入计算机阻断功能;

- 10) 支持移动存储介质的完善管理, 提供针对 U 盘等存储介质的注册、授权、注销全生命周期的管理;
- 11) 支持多级管理、负载均衡和双机热备等大规模部署能力;
- 12) 提供完整的可定制化的审计报表图文输出显示功能。

● 系统部署示意图:

