

主机监控审计

产品名称	主机监控审计
公司名称	张家口中科网安科技有限公司
价格	.00/个
规格参数	
公司地址	河北省张家口市桥西区赐儿山街19号
联系电话	0313-5928238 13520132483

产品详情

虽然大多数企事业单位已经采取了防火墙、入侵检测、漏洞扫描等网络安全手段和管理措施，但是对越权访问、违规操作、内部泄密等安全事件仍无法及时告警响应、准确定位事件源头。如何有效监控业务系统访问行为和敏感信息传播，准确掌握网络系统的安全状态，及时发现违反安全策略的事件并实时告警、记录，同时进行安全事件定位分析，事后追查取证，是企事业单位迫切需要解决的问题。

定义：

安全审计，是指由专业审计人员根据有关法律法规、财产所有者的委托和管理当局的授权，对计算机网络环境下的有关活动和行为进行系统的、独立的检查验证，并作出相应评价。安全审计通过测试系统对标准的符合程度来评估其安全性。

实施：

通常，安全审计会转化为一组对系统的具体问题。例如：

- 1、密码破解有多困难？
- 2、网络资源是否有访问控制列表管理？
- 3、是否有访问日志，记录“谁访问了哪些数据”？
- 4、个人电脑是否定期扫描恶意软件和广告软件？
- 5、组织中，谁有访问备份库的权利？

四要素：

控制目标：指企业根据具体的计算机应用，结合单位实际，制定出的安全控制要求。

安全漏洞：指系统的安全薄弱环节，容易被干扰或破坏的地方。

控制措施：指企业为实现其安全控制目标所制定的安全控制技术、配置方法及各种规范制度。

控制测试：将企业各种安全控制措施与预定安全标准进行一致性比较，确定各项控制措施是否存在、是否得到执行、对漏洞的防范是否有效，评价企业安全措施的可依赖程度。

网络安全审计：

网络安全审计，是指针对互联网行为提供有效的行为审计、内容审计、行为告警、行为控制及相关审计功能，满足用户对互联网行为审计备案及安全保护措施的要求，提供完整的上网记录，便于信息追踪、系统安全管理和风险防范。从管理层面提供互联网的有效监督，预防、制止数据泄密。

数据库安全审计：

数据库安全审计，主要用于监视并记录对数据库服务器的各类操作行为，通过对网络数据的分析，实时、智能地解析对数据库服务器的各种操作，及时地发现网络上针对数据库的违规操作行为并进行记录、报警和实时阻断。记入审计数据库中以便日后进行查询、分析、过滤，实现对目标数据库系统用户操作的监控和审计，为数据库系统的安全运行提供有力保障。

—— E N D ——

文字来源：《漫画信息安全保密》