如何打造“ 数字黄河 ”安全管理网络（二） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/353/2021_2022__E5_A6_82_E4_BD_95_E6_89_93_E9_c101_353488.htm 五、建立网络病毒防护系统 一套好的网络版的防毒产品是搞好病毒防护的基础平台，没有好的防毒软件，作好病毒防护是一句空话，但有了防毒软件就万事无忧，也不现实。我们的经验是，好的技术是支撑，运作和管理是关键，两者配合，才能做好工作。我院的病毒防护系统是以趋势科技网络防毒墙officescan、防毒墙服务器版protect server以及防毒墙控管中心为技术支撑，按照实时监控，主动遏制，快速响应，跟踪结果的病毒防护理念，制定病毒防护安全预警管理机制，具体的运作方式如下：（一） 预防为主，全面布防，杜绝网络漏洞 在采用域管理模式基础上，防毒软件的客户端使用“ 登录脚本安装 ”，当计算机登录到域服务器时，自动在该计算机上安装客户机软件，病毒特征文也的自动分发和升级。同时，定期扫描未装杀毒软件计算机（运行tmsv.exe），定期对域用户进行系统安全评估，查找网络存在的系统漏洞，人工及时进行处理。保障网络中没有病毒防护盲点。保证客户端的杀毒软件始终是最新的。这些工作都在后台进行，在提高网络安全性的同时，没有增加用户负担。（二） 严密监控，主动处理。 采用自动监控和人工监控相结合的方式，一方面，利用趋势科技防毒墙控制中心自动进行病毒爆发监控，实施病毒爆发阻止。另一方面，指定专人，随机查看网络所有计算机病毒防护情况，发现有网络病毒，通知用户，立即排查，及时处理。（三） 采用多种技术手段清除病毒防毒软件发现的病毒，并

不都能自动清除。所以对病毒的处理，我们采用三级处理方式：实时监控发现病毒未能清除的，从控制台启动手动扫描，若不能清除，通知用户，到安全模式下，利用趋势科技提供的在DOS和安全模式下运行的杀毒软件syslean.exe进行扫描；若还不能清除，网管人员从趋势科技病毒百科站点，下载解决方案，到现场给于解决。每周网管人员到趋势科技站点，下载最新Sysclean.exe 程序和最新的病毒库。放在ftp服务器上，供用户使用。（四） 制定合理防护策略病毒防护程序是占用一定的计算机资源，安全和资源占用一个矛盾，在制定病毒防护策略时，采用了高配置高防护，地配置低防护的策略。对CPU是P41G以上使用win2000/winxp 的计算机，安全配置都比较严，而对P3 以下使用win98的计算机，实时监控和防火墙配置相对较低，重在手工扫描。在保障系统的安全下，尽量不影响计算机的正常应用。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com