如何打造“ 数字黄河 ”安全管理网络（一） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/461/2021_2022__E5_A6_82_E4_BD_95_E6_89_93_E9_c101_461753.htm 引言 黄河水利科学研究院计算机网络系统作为“ 数字黄河 ”基础设施建设的组成部分。2000年开始运行，几年来网络规模和应用都有了长足发展。信息化建设以不可抗拒的力量，影响和改变着我们科研工作模式，管理工作模式，让我们充分享用到网络带来的方便、高效和利益。但开放互连的网络，也存在着自然和人为等诸多因素引发的脆弱性和潜在威胁，也要应对网络安全的新挑战和新危险。近年来，为落实黄总办提出的“ 实施精细管理，打造精品网络，为维持黄河健康生命而努力奋斗 ”的工作目标，在网络安全管理方面，从技术层面和管理层面作了一些工作，总结归纳如下，与大家切磋共勉。 一、 网络系统分析 （一）网络安全的问题分析 网络安全包括六个基本要素：机密性、完整性、可用性、可控性、可审查性与有效性。 机密性：确保网络上的信息不暴露给未授权的实体或进程。当信息可被创建信息人、收受人之外的第三者，以恶意或非恶意的方式得知时，就丧失了机密性。 完整性：只有得到允许的人才能修改网络信息，并且系统能够判别出信息是否已被篡改。 可用性：系统必须能够判定用户是否具备足够的权限进行特定的活动，如打开文件、执行程序等。即攻击者不能占用计算机和网络资源而阻碍授权者的工作。 可控性：可以控制授权范围内的信息流向及行为方式。 可审查性：对出现的网络安全问题提供调查的依据和手段。某用户对系统进行某项运作后，若系统事后能提出证明，而用户无法

加以否认，便具备可审查性。 有效性：某些网络服务因服务性质的因素，必须公开提供给非特定人使用（如公共网页、邮件服务等），但各项服务因为设计或硬件能力上的限制，势必都存在服务能力的上限，当该项服务被攻击，而使得经过身份鉴别及授权的正常用户无法取得服务时，便丧失了有效性。（二） 网络所面临的问题 计算机网络所面临的威胁大体可分为两种：一是对网络中信息的威胁；二是对网络中设备的威胁。影响计算机网络安全的因素很多，有些因素可能是有意的，也可能是无意的；可能是人为的，也可能是非人为的，归结起来，针对网络安全的威胁主要有以下几点： 人为的无意失误：由系统操作员安全配置不当造成的安全漏洞。用户安全意识不强，用户口令选择不慎，用户将自己的帐号随意转借他人或与别人共享等都会对网络安全带来威胁。 人为的恶意攻击：一种是主动攻击，有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息；另一类是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄漏。 网络软件的漏洞和“ 后门：网络软件不可能是百分之百的无缺陷和无漏洞的，然而，这些漏洞和缺陷恰恰是黑客进行攻击的首选目标。 信息泄漏或丢失：敏感数据在有意或无意中被泄漏出去或丢失。通常包括：信息在传输中丢失或泄漏，信息在存储介质中丢失或泄漏，通过建立隐蔽隧道等窃取敏感信息等。 拒绝服务攻击：拒绝服务攻击行为不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响用户正常的

使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。 利用网络传播病毒：计算机病毒是一种能自身繁殖和自动隐藏、自动传输的计算机程序，具有传染性、潜伏性、隐蔽性和破坏性四大特点，可以通过磁盘、网络、电子邮件等进行传播，其对计算机上的信息资源、系统运行环境、网络运行环境有极大的破坏作用。 网络安全工作的重点不是故障发生后，被动的处理，而应通过积极主动有效的管理，杜绝漏洞，防止故障的滋生。所以网络安全管理不单是个技术问题，而是一个系统管理的问题。不仅要注重建设前的规划、设备选型，还要注重网络二、三层的优化配置，软件应用层的安全认证体系，网络防病毒处理、建立安全预警体系，更主要的是制定和实施完善的安全管理规章制度，才能营造一个既方便、快捷、高效又安全可靠的网络环境。 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