满朗

23

李帅琪

网络

网络安全

网络的安全是指通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。网络安全的具体含义会随着“角度”的变化而变化。比如：从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护。而从企业的角度来说，最重要的就是内部信息上的安全加密以及保护。网络的安全是指通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。网络安全的具体含义会随着“角度”的变化而变化。比如：从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护。而从企业的角度来说，最重要的就是内部信息上的安全加密以及保护。

网络安全问题

计算机系统硬件和通讯设施极易遭受到自然环境的影响，如:各种自然灾害(如地震、泥石流、水灾、风暴、建筑物破坏等)对计算机网络构成威胁。还有一些偶发性因素，如电源故障、设备的机能失常、软件开发过程中留下的某些漏洞等，也对计算机网络构成严重威胁。此外管理不好、规章制度不健全、安全管理水平较低、操作失误、渎职行为等都会对网络安全造成威胁。

在网络的应用中，由于网络具有较为开放的特征，因此在网络中信息的传输和交换非常频繁，由此造成的信息安全也成为了网络安全面临的主要问题。在互联网中，用户之间由于现实的数据传输需求，需要保证自己的网络终端属于开放的状态，由此就给他人以植入木马程序等电脑病毒的机会。所以，网络使用中存在的不安全问题是网络安全问题的重要类别。

网络安全法

第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第四条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

如何预防

1、防火墙安装必要的防火墙，阻止各种扫描工具的试探和信息收集，甚至可以根据一些安全报告来阻止来自某些特定 IP 地址范围的机器连接，给服务器增加一个防护层，同时需要对防火墙内的网络环境进行调整，消除内部网络的安全隐患。

2、漏洞扫描使用商用或免费的漏洞扫描和风险评估工具定期对服务器进行扫描，来发现潜在的安全问题，并确保由于升级或修改配置等正常的维护工作不会带来安全问题。

3、安全配置

关闭不必要的服务，最好是只提供所需服务，安装操作系统的最新补丁，将服务升级到最新版本并安装所有补丁，对根据服务提供者的安全建议进行配置等，这些措施将极大提供服务器本身的安全