清朗网络空间

什么是网络安全

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。

知法守法

网络不是法外之地，对于散布网络谣言，让他人“社会性死亡”的人来说，是要承担法律责任的。今年 1 月 1 日起施行的《中华人民共和国民法典》明确规定，任何组织或者个人不得以侮辱、诽谤等方式侵害他人的名誉权。任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息。网络用户、网络服务提供者利用网络侵害他人民事权益的，应当承担侵权责任。这些都是制止网络谣言的法律支撑。

此外，根据我国《治安管理处罚法》的规定，公然侮辱他人或者捏造事实诽谤他人的，偷窥、偷拍、窃听、散布他人隐私的，处五日以下拘留或者五百元以下罚款；情节较重的，处五日以上十日以下拘留，可以并处五百元以下罚款。如果造成严重后果还有可能构成犯罪。根据《刑法》规定，以暴力或者其他方法公然侮辱他人或者捏造事实诽谤他人，情节严重的，处三年以下有期徒刑、拘役、管制或者剥夺政治权利。

如何预防网络安全隐患

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

4、优化代码

优化网站代码，避免 sql 注入等攻击手段。检查网站漏洞，查找代码中可能出现的危险，经常对代码进行测试维护。

5、入侵检测系统

利用入侵检测系统的实时监控能力，发现正在进行的攻击行为及攻击前的试探行为，记录黑客的来源及攻击步骤和方法。

这些安全措施都将极大提供服务器的安全，减少被攻击的可能性。

网络安全真实案例

国外

2012 年 02 月 04 日，黑客集团 Anonymous 公布了一份来自 1 月 17 日美国 FBI 和英国伦敦警察厅的工作通话录音，时长 17 分钟，主要内容是双方讨论如何寻找证据和逮捕 Anonymous, LulzSec, Antisec, CSL Security 等黑帽子黑客的方式，而其中涉及未成年黑客得敏感内容被遮盖。

目前 FBI 已经确认了该通话录音得真实性，安全研究人员已经开始着手解决电话会议系统得漏洞问题。

国内

2011 年 12 月 29 日下午消息，继 CSDN、天涯社区用户数据泄露后，互联网行业一片人心惶惶，而在用户数据最为重要的电商领域，也不断传出存在漏洞、用户泄露的消息，漏洞报告平台乌云昨日发布漏洞报告称，支付宝用户大量泄露，被用于网络营销，泄露总量达 1500 万～2500 万之多，泄露时间不明，里面只有支付用户的账号，没有密码。目前已经被卷入的企业有京东(微博)商城、支付宝(微博)和当当(微博)网，其中京东及　支付宝否认信息泄露，而当当则表示已经向当地公安报案。