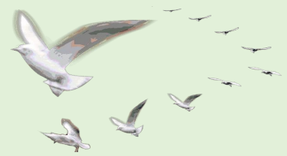
--

网络安全问题



网络安全是什么

网络安全，通常指计算机网络的安全，实际上也可以指计算机通信网络的安全。计算机通信网络是将若干台具有独立功能的计算机通过通信设备及传输媒体互连起来，在通信软件的支持下，实现计算机间的信息传输与交换的系统。而计算机网络是指以共享资源为目的，利用通信手段把地域上相对分散的若干独立的计算机系统、终端设备和数据设备连接起来，并在协议的控制下进行数据交换的系统。计算机网络的根本目的在于资源共享，通信网络是实现网络资源共享的途径，因此，计算机网络是安全的，相应的计算机通信网络也必须是安全的，应该能为网络用户实现信息交换与资源共享。下文中，网络安全既指计算机网络安全，又指计算机通信网络安全。

安全的基本含义：客观上不存在威胁，主观上不存在恐惧。即客体不担心其正常状态受到影响。可以把网络安全定义为：一个网络系统不受任何威胁与侵害，能正常地实现资源共享功能。要使网络能正常地实现资源共享功能，首先要保证网络的硬件、软件能正常运行，然后要保证数据信息交换的安全。从前面两节可以看到，由于资源共享的滥用，导致了网络的安全问题。因此网络安全的技术途径就是要实行有限制的共享。

从网络运行和管理者的角度来讲，其希望本地信息网正常运行，正常提供服务，不受网外攻击，未出现计算机病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁。从安全保密部门的角度来讲，其希望对非法的、有害的、涉及国家安全或商业机密的信息进行过滤和防堵，避免通过网络泄露关于国家安全或商业机密的信息，避免对社会造成危害，对企业造成经济损失。从社会教育和意识形态的角度来讲，应避免不健康内容的传播，正确引导积极向上的网络文化。

网络安全在不同的应用环境下有不同的解释。针对网络中的一个运行系统而言，网络安全就是指信息处理和传输的安全。它包括硬件系统的安全、可靠运行，操作系统和应用软件的安全，数据库系统的安全，电磁信息泄露的防护等。狭义的网络安全，侧重于网络传输的安全。

国内外有什么网络安全问题

国家互联网应急中心发布的《2019 年上半年我国互联网网络安全态势》显示，2019 年上半年，我国互联网网络安全状况具有四大特点：个人信息和重要数据泄露风险严峻；多个高危漏洞曝出给我国网络安全造成严重安全隐患；针对我国重要网站的 DDoS 攻击事件高发；利用钓鱼邮件发起有针对性的攻击频发。

国家互联网应急中心从恶意程序、漏洞隐患、移动互联网安全、网站安全以及云平台安全、工业系统安全、互联网金融安全等方面，企业面临的网络风险或者网络威胁主要有以下几种形式：

1、网站入侵、网页内容篡改

表现形式：黑客利用网站漏洞侵入网站，篡改网页内容，甚至贴上反动标语。

后果：造成严重的政治影响，对企业公关形象产生负面影响，被监管部门处罚，影响正常业务开展。

2、数据泄露

表现形式：生产运营中积累大量客户数据的企业遭受黑客攻击，数据被窃取并用于非法用途，如 2018 年华住酒店的客户数据泄露事件、2017 年美国 Equifax 数据泄露事件等。

后果：面临监管处罚，美国 Equifax 为 1.5 亿用户数据泄露支付了至少 5.75 亿美元的罚款。此外，还可能面临第三方的索赔。

3、网络勒索

表现形式：遭受网络勒索软件攻击，需向对方支付勒索金后方可解锁相关软件或数据。2017 年 6 月马士基总部 IT 系统遭到勒索软件攻击，集团全球系统瘫痪，码头停止作业，最长的一周后才恢复运营。

后果：支付勒索款项造成经济损失；或者生产经营中断造成营业中断损失，营业中断损失是目前大家公认的网络安全风险中最大的风险。马士基网络瘫痪事件导致的直接损失超过了 3 亿美金，营业中断的损失金额未见公开披露。

我们应该如何预防

1、全面规划网络平台的安全策略。

2、制定网络安全的管理措施。

3、使用防火墙。

4、尽可能记录网络上的一切活动。

5、注意对网络设备的物理保护。

6、检验网络平台系统的脆弱性。

7、建立可靠的识别和鉴别机制。

网络安全（Network Security）包含网络设备安全、网络信息安全、网络软件安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。具有保密性、完整性、可用性、可控性、可审查性的特性。

面对这些风险，普通网民如何防范？任彦表示，普通网民应增强网络安全保护意识，不随意透露、填写个人信息，特别是个人敏感信息，不要访问不正规的、高风险的网站，不点击来历不明的邮件和链接。应从正规渠道下载安装 App，避免下载到仿冒 App。

做好密码管理，如不使用简单密码、定期更换密码等，不同平台网站最好使用不同的账户密码，避免出现一个平台的数据泄露导致所有平台的账号密码泄露风险。

安装终端病毒查杀工具，定期升级，安装软件时特别注意是否有较为隐蔽的捆绑安装等情况。

安全是发展的前提，发展是安全的保障。共建网络安全人人有责，要时刻感知网络安全态势，做好网络风险防范，增强网络安全防御能力，我们就能让人民群众在信息化发展中有更多获得感、幸福感、安全感，推动网络安全和信息化工作再上新台阶。

25 戚宇涵