网络电子安全

网络安全的概念

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。

狭义解释

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。

广义解释

网络传输的安全与传输的信息内容有密切的关系。信息内容的安全即信息安全，包括信息的保密性、真实性和完整性。

广义的网络安全是指网络系统的硬件、软件及其系统中的信息受到保护。它包括系统连续、可靠、正常地运行，网络服务不中断，系统中的信息不因偶然的或恶意的行为而遭到破坏、更改或泄露。其中的信息安全需求，是指通信网络给人们提供信息查询、网络服务时，保证服务对象的信息不受监听、窃取和篡改等威胁，以满足人们最基本的安全需要（如隐秘性、可用性等）的特性。网络安全侧重于网络传输的安全，信息安全侧重于信息自身的安全，可见，这与其所保护的对象有关。

网络安全问题

1.网络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。

2.几乎有计算机的地方，就有出现计算机病毒的可能性。计算机病毒通常隐藏在文件或程序代码内，伺机进行自我复制，并能够通过网络、磁盘、光盘等诸多手段进行传播。正因为计算机病毒传播速度相当快、影响面大，所以它的危害最能引起人们的关注。

3.病毒的"毒性"不同，轻者只会玩笑性地在受害机器上显示几个警告信息，重则有可能破坏或危及个人计算机乃至整个企业网络的安全。

4.有些黑客会有意释放病毒来破坏数据，而大部分病毒是在不经意之间被扩散出去的。人们在不知情的情况下打开了已感染病毒的电子邮件附件或下载了带有病毒的文件，这导致了病毒的传播。这些病毒会从一台个人计算机传播到另一台，因而很难从某一中心点对其进行检测。

5.任何类型的网络免受病毒攻击最保险和最有效的方法是对网络中的每一台计算机安装防病毒软件，并定期对软件中的病毒定义进行更新。值得用户信赖的防病毒软件包括 Symantec、Norton 和 McAfee 等。然而，如果没有"忧患意识"，很容易陷入"盲从杀毒软件"的误区。

6.随着越来越多黑客案件的报道，企业不得不意识到黑客的存在。黑客的非法闯入是指黑客利用企业网络的安全漏洞，不经允许非法访问企业内部网络或数据资源，从事删除、复制甚至毁坏数据的活动。一般来说，黑客常用的入侵动机和形式可以分为两种。

7.黑客通过寻找未设防的路径进入网络或个人计算机，一旦进入，他们便能够窃取数据、毁坏文件和应用、阻碍合法用户使用网络，所有这些都会对企业造成危害。黑客非法闯入将具备企业杀手的潜力，企业不得不加以谨慎预防。

8.防火墙是防御黑客攻击的最好手段。位于企业内部网与外部之间的防火墙产品能够对所有企图进入内部网络的流量进行监控。不论是基于硬件还是软件的防火墙都能识别、记录并阻塞任何有非法入侵企图的可疑的网络活动。

对于网络安全我们能做什么

一、免费且不设密的 WIFI 谨慎连接

二、不要使用破解或共享密码的手机 APP

三、在网络中使用弱口令（弱口令是指将密码设的过于简单）

四、下载软件最好在官网下载

五、各种包含个人信息的物件不要在网上公布

六、在选择查杀病毒的软件时最好选择火绒，愿意花钱的选择金山毒霸（不要用 360 和 2345 此类流氓软件）

网络的安全防护其实只要我们在日常生活中适当的注意就能在很大程度上避免个人的隐私泄露。