网络安全

Network security

国内外网络安全现状与存在的问题

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。

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、分布式拒绝服务攻击

表现形式：网站受到来自多个站点的同时攻击，使网站服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，导致网络或系统不胜负荷以至于瘫痪而停止提供正常的网络服务。

后果：网站无法提供正常服务，通过网站接受订单服务被中止，同样造成营业中断的后果。

计算机网络法律法规

第一条 为了保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行，制定本条例。

第二条 本条例所称的计算机信息系统，是指由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

第三条 计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。

第四条 计算机信息系统的安全保护工作，重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全。

第五条 中华人民共和国境内的计算机信息系统的安全保护，适用本条例。

第六条 公安部主管全国计算机信息系统安全保护工作。国家安全部、国家保密局和国务院其他有关部门，在国务院规定的职责范围内做好计算机信息系统安全保护的有关工作。

第七条 任何组织或者个人，不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机信息系统的安全。

如何预防网络诈骗

1.避免网络诈骗我们首先在进行网络浏览的时候要在自己的电脑上安装杀毒软件，杀毒软件也要保持更新的习惯，因为很多网络诈骗是通过杀毒软件的漏洞...

2.避免网络诈骗，我们不要点击陌生人发过来的网络链接以及二维码相关内容，很多是用来钓鱼的，目的是让你点击后，然后盗取你的相关密码，最常见的...

3.避免网络诈骗我们要做的就是自己的微信头像以及自己朋友圈的照片不要对陌生人可见，诈骗犯会通过你发的日常生活照片来判断你的生活近况甚至你的...

4.避免网络诈骗我们在登陆相关银行以及各大网站的时候一定要选择官网登陆，不可以选用其他莫名的链接，很多诈骗者用相似的链接来让上网者点入来盗取...

5.避免网络诈骗我们也不要轻信任何网络上的中奖信息，除非是官网发布的，我们也一定要打官方的客服进行核实，天下没有掉馅饼的好事，请不要轻易上当...