# “互联网+”网络信息安全现状与防护研究

彭 实
杭州安恒信息技术股份有限公司 浙江 杭州 310000

**摘 要：**随着网络的快速发展，拉近了人们彼此之间的距离，同时也为我们快速地获取信息提供了便利。目前，各行各业中均可以看到网络的身影，在网络技术的帮助下，生活变得更加方便、快捷。在这一情况下，“互联网+”网络信息安全等级也成为人们重点关注的内容。针对“互联网+”网络环境下，网络信息安全技术的发展问题，进行深入探析，并提出改进措施，以达到提升网络信息安全技术等级，促进网络信息安全技术可持续发展的目的。

**关键词：**“互联网+”；网络信息安全；现状与防护

## 引言

随着信息化的快速发展，“互联网+”为各个行业带来发展机遇的同时，也衍生出很多安全问题。因此，在“互联网+”快速发展的背景下，采取合适的网络信息安全防护手段是十分必要的。构建一套具有自身硬功能的网络安全防护体系，不仅能够保证企业自身的利益，同时也能够保护每一名员工的个人隐私和信息数据。

## 1 网络信息安全防护的必要性

伴随网络的逐渐普及，我们的生活变得越来越丰富，置身网络时代，我们随时随地都能获取海量数据信息。在互联网时代背景下，我们的生活发生了翻天覆地的改变，云计算、虚拟技术、大数据开始成为我们平时工作与生活中的常见词汇，这些技术为我们的工作和学习提供了很多方便。随着网络技术的快速发展，黑客活动日渐猖獗，由其带来的危害也越来越大。在这种情况下，信息数据、网络系统的整体运行都面临着严重威胁。虽然防火墙、通道控制以及代理服务器等安全技术的应用，从一定程度上提升了网络信息的安全性与稳定性。但是，随着黑客技术的快速发展，在互联网时代背景下，网络信息安全体系的构建也被处于一种危险的位置上。面对上述问题，有关人员应该以加强网络信息安全技术应用的前提下，探索更加实用的防护性举措，这同时也是提升网络信息系统应用的安全性、稳定性的重点所在。

## 2 网络信息安全现状

### 2.1 安全管理体系残缺

目前，我国很多企业在进行网络安全防护体系建设过程中，对于规章制度的完善以及人员的管理重视程度较低，且落实的情况相对较差。在所有的网络攻击中，社会工程学是一种针对性强而防护难度大的攻击类型。因为社会工程学攻击针对的不是网络，而是企业内部的员工和管理人员，常用的攻击方式包括窃听、废物搜寻、钓鱼邮件等。一旦企业缺乏严谨完善的安全管理体系，加之员工的网络安全意识薄弱，将会导致大量信息数据被窃密。

### 2.2 黑色产业链猖獗

黑色产业链是利用黑客技术和黑客工具，通过勒索或威胁的方式获取利益的一条非法途径。近年来，勒索病毒出现的频率越来越高，给广大企事业单位带来了极大损失。在遭受勒索病毒之后，用户方会表现出数据访问和数据受限的情况，只能通过勒索病毒提示的种类信息以及表现特征尝试破解，但破解几率较低。如果是定制化的新型勒索病毒，几乎无法破解，只能向勒索方支付比特币换取密码。黑色产业链的猖獗，给无数企业带来了阴影和损失，而吸引黑色产业链注意的根本原因完全在于两点：第一，企业的规模大，网络复杂且存在漏洞；第二，企业自身的网络全防护能力较低，管理体系不完善，很容易出现易于被利用的高危漏洞。由于黑色产业链大部分黑客都是利用大范围扫描的方式检索漏洞，那些利用难度低，同时危害性较高的漏洞就成为了最先被攻击的对象。

### 2.3 内部因素

影响网络安全的内部因素主要包括网络环境因素以及网络系统管理漏洞。首先，网络环境因素主要由于网络的开放性和共享性所决定，网络可跨越时间和空间进行用户之间数据的传输，网络的开放性对于数据信息安全保障提出了较高的要求。但目前来讲，现代信息安全管理技术更新速度较慢，很多网络黑客和不法分子常常利用未升级的网络所存在的漏洞进行信息数据的窃取，威胁个人信息安全和隐私安全，同时也会影响企业的正常运营。尤其一般的网络信息安全模式所采取的是互联网协议环境，其防御能力相对较弱，安全等级较低，无

法满足用户对于信息数据安全的实际需求。而计算机网络系统本身所存在的漏洞对于信息安全的影响最为明显，在面对外部网络入侵攻击时，需要利用网络信息相关技术予以维护升级，提升网络信息安全防护水平。

2.4 网络软件自身漏洞

随着用户需求的不断上升和互联网技术的迅速发展，越来越多的网络软件应运而生。然而，软件的质量并没有达到设定要求。软件设计人员在进行设计的过程中过于注重软件的运行能力而忽略了软件自身的安全性。软件自身漏洞与测试人员脱不了干系，每一款新软件的推出都需要经过测试人员的测试。测试工作是检验软件各方面性能的关卡，只有满足相关要求的软件才能成功投入运营。因此，因网络软件自身漏洞导致的安全问题也有一部分责任来自软件测试人员。

2.5 计算机病毒

它对网络信息安全有着较大的影响。通常是借助人为方式，对计算机系统程序进行设置，以此对系统中的数据造成破坏，进一步对计算机系统功能产生影响，实际上它是一种程序代码。该病毒主要包含两种类型，分别是良性与恶性，病毒本身是能够开展复制的，它的传染性非常强，并且还有较大的破坏性，隐蔽性还非常好，不易被发现。一般情况下，是利用计算机网络开展传播，对系统中的软硬件造成破坏，导致计算机无法有效应用，甚至会造成计算机网络瘫痪，导致计算机系统不能正常工作，对用户的网络系统产生损害，由此，想要确保计算机系统安全，应对该病毒加以重视，强化有关的安全防范工作。

2.6 信息安全监管不足

第一，网络安全信息管理者并未对上传至网络的相关信息开展全面审核，导致不良信息被上传至网络上，针对部分重要信息也未实施科学的安全设置，导致不法分子利用漏洞，对网络信息安全形成了较大的威胁。第二，网络监管平台缺乏监管力度，在这之中没有构建完善的监管体系，无法构建长效的监管机制，针对不良信息没有相应的监管及惩处，无法发挥震慑力。第三，网民监督意识比较薄弱，针对网络上存在的不法信息，没有相应的举报及监督意识。第四，没有构建健全的信息安全监督及法律法规。网络信息安全与社会发展存在密切的关系。从网络信息安全来看，立法机关还没有发布科学的法律来提高信息安全保护力度，这导致网络安全管理者及网络参与人员都不够重视。

## 3 “互联网 +”网络信息安全防护优化

3.1 做好网络漏洞的修复工作

进入互联网时代以后，网络信息安全防护成为一项重要工作。为了达到防护信息安全的目的，必须对网络系统存在的漏洞加以关注，及时采取措施修复。在修复网络系统漏洞时，可以采用修复软件完成这项工作，这需要相关人员及时了解、掌握修复网络系统漏洞的原理，明确相关知识内容，对网络漏洞的修复流程有一个清晰的了解，只有这样才能在应用修复软件与修复技术时，充分发挥出软件的修复优势，达到理想的修复效果。一般而言，修复软件应该保持一定的新颖性、创新性，换句话说，网络系统修复软件要做到与时俱进，要与当前网络的发展趋势相符。所以，必须对修复软件进行及时的更新。同时，要以计算机系统安全为基础，积极运用系统补丁技术，通过利用系统补丁可以很好地修复网络系统漏洞，在最大程度上确保网络信息安全。在最初使用计算机网络时，应该将具有修复功能的软件安装在计算机中，这样即可自动对网络系统漏洞进行修复。如果其中存在无法通过自动修复方式修复的漏洞，那么技术人员则必须承担起责任，及时落实好各项修复工作。

3.2 建立良好的网络秩序

良好的网络秩序是各种互联网工作开展的基础，也是保障网络信息安全的重要法宝。安全的网络环境需要每一位用户的共同努力，因此建立良好的网络秩序首先应该呼吁人们养成“自律”意识，网络不是不法之地，在享受计算机信息技术带来的福利时应该遵守网络信息管理的“底线”。其次，良好的互联网秩序仅靠用户的自觉性是很难实现的，所以还需要相应的审查与处罚作为他律来确保互联网安全绿色的环境。对于窃取他人信息、蓄意破坏网络信息安保系统等影响计算机信息安全管理的行为应给予严厉的处罚。最后，引进高新计算机人才作为稳定网络秩序的技术保障。技术人员可以对计算机网络信息系统进行定期的维护，一旦发现安全隐患就会立刻采取有效措施进行补救。

3.3 查杀病毒

用户需提高对网络系统的安全保护意识，在使用过程中加强对携带病毒网站和软件的甄别能力，安装可自动更新病毒库和升级的杀毒软件，并定期对计算机系统进行查杀。对于不能自动清除的病毒，可设置紧急提醒，对病毒感染文件进行隔离，减少损失。

3.4 安全评估

可对接入互联网、物联网的终端设备采用统一的生产标准，并进行网络信息安全检测评估，防止生产的终端设备可能存在漏洞和后台程序，从而防范可能带来的

信息安全风险。

3.5 加强网络信息安全管理人才的培养

网络信息安全管理离不开高质量技术人才。高等教育是一个培养人才的重要方式，但是目前的高等教育存在一定的滞后性。学生所接触到的知识不足以解决当前计算机信息管理面临的问题，所以人才培养的效率并不高。及时更新高等教育的内容使其与人才市场的需求相接轨是培养高质量人才的关键。另外，高等教育培养出的人才严重缺乏实战能力。学校大多数是进行理论知识的教育，忽略了实践能力的培养。因此，高等教育培养出的人才不能直接满足市场人才需求。这就需要高校进行教育改革，不仅要严抓学生理论知识的学习，同时还要加强实践能力的培养。“校企联合”可以为学生创造更多实战的机会，加快计算机信息安全管理人才的培养效率。

## 4 网络信息安全的特征

4.1 规模安全

在大数据时代，为高效处理海量数据、实现数据资源集成应用和分摊成本，陆续建立若干数据中心与云端平台，大量用户将信息上传至平台执行存储、预处理、分类整理等操作，在用户支付少量费用前提下，即可享受高质量的网络信息服务。然而，在这类数据中心、云端平台遭受恶意攻击时，容易造成重大损失，造成后果包括大量用户隐私信息失窃、企业机构机密文件失窃、身份盗用、引发社会舆论探讨。

4.2 隐性安全

在移动信息技术加持下，信息传递过程有着独体型与个性化特征，具备点对点和点对圈的传播条件。相比于传统点对面的传播方式，网络信息传播具有较强的隐蔽性，很难在信息流通期间发现全部的信息安全隐患。

4.3 泛在安全

大数据技术的问世，极大地推动了物联网发展进程，构建起万物互联的网络体系。从不法分子角度来看，可以使用任何智能终端设备来侵入网络系统，无声无息地向各处渗透，对网络系统各处节点存储信息、软件程序与接入硬件设备的安全造成严重威胁。

## 结束语

在互联网时代背景下，国家的发展、社会的进步和个人的发展都需要网络安全技术保障信息的安全储存和传输。因此，网络信息安全的重要性已提升到一个全新高度。信息安全技术应建立在防御系统强硬，网络安全保护体系完善的基础上，提高安全防护技术手段，防止不良因素入侵网络。

## 参考文献

[1]刘文君.云计算环境下网络信息安全技术发展研究[J].中国新通信，2020，22（17）：33-36.

[2]李昂.云计算环境下网络信息安全技术发展探究[J].网络安全技术与应用，2022（7）：61-63.

[3]刘洪亮.云计算中网络信息安全技术的应用研究[J].科技资讯，2021，19（20）：10-12.