大数据时代计算机网络信息安全及防护策略

林　颖

（福建商学院，福建 福州 350001）

摘　要　随着科学技术的不断创新与发展，计算机技术广泛应用于各个行业领域，为大众的生活、生产提供了便利条件。网络信息安全是计算机发展面临的主要问题之一，若存储、传输的个人隐私信息遭到泄露，将会对个人财产、人身安全造成极大的威胁。因此，本文认为应结合大数据时代背景，结合计算机网络信息存在的安全问题，制定切实可行的应对策略，即增强用户网络信息安全意识、提升网络软件安全性能、加强网络信息安全监管力度等，从而为维护网络环境安全打下坚实基础。

关键词　大数据；计算机网络；信息安全；防护策略

中图分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1007-0745(2023)09-0029-03

大数据时代，数字化技术为传统计算机网络的运营和发展提供了新的机遇，将大数据技术与人工智能、神经网络等技术相融合，可在一定程度上提高计算机网络的数据处理效率。虽然大数据技术为人们的生活、生产带来了更多的便利条件，但在数字化技术不断优化升级的进程中，计算机网络也存在一些漏洞，不法分子利用漏洞攻击人们的计算机系统，窃取人们的个人隐私数据及财产等，不仅给人们的财产带来威胁，甚至还会影响人们的人身安全。因此，针对计算机网络中存在的信息安全问题，要提前做好防范措施，制定切实可行的解决方案，为用户提供良好的网络运行环境。

1　大数据时代计算机网络信息安全概述及风险类型

1.1　大数据时代计算机网络信息安全概述

1.1.1　大数据理论概述

随着我国科学技术的不断创新与发展，社会融入更多大数据技术元素，使得人们的生活更加多样化。大数据时代，将先进的信息技术融入计算机网络发展进程中，形成一种新型的市场、经济、文化形态，使得计算机网络技术在满足人们基本需求的基础上发挥更多价值。大数据技术打破了不同行业间的壁垒，实现不同领域范畴的相互融合，让整个社会朝着多元化发展，大数据在时代发展进程中具有不可估量的价值。针对大数据而言，其主要特点有：

1. 数字类型多元化。计算机网络中充斥着各种各样的数据形态，数据资源之间的属性各不相同，使得数据类型呈现得更加多元化。

2. 数据规模庞大。一般情况下信息的综合容量均高于10TB。

3. 数据处理效率高。传统模式下的数据资源逐步被新资源取代，新型的数据在信息传输、处理、编辑等阶段均具有较高的效率，使得计算机网络系统的应用性能得到显著提升。

1.1.2　网络信息安全概述

网络信息安全，是指通过大数据技术保护计算机网络系统的数据信息、软硬件等的安全，使其不受病毒、黑客等恶意攻击，保障网络信息的安全平稳运行。对于网络信息安全而言，其具有的主要特征是：一是网络信息安全事件具有突发性；二是网络运行环境具有开发性、交互性，虽然为人们提供了网络数据共享的便捷，但也为病毒、黑客的入侵提供了机会。一旦计算机网络受到内外部攻击，系统内包含的数据资源将会面临丢失的风险，系统可能会全面瘫痪，从而造成不可估量的损失[1]。

1.2　网络信息安全风险类型

当计算机网络进行数据传输时，面临的主要信息安全风险可划分为4种基本类型：一是拦截，通过网络窃取他人的通信数据信息；二是中断，采用非法手段恶意中断他人之间的通信；三是篡改，将病毒植入他人计算机篡改系统内数据信息；四是伪造，在网络发布伪造的数据信息误导、迷惑、诱骗他人，从而造成严重后果。

传统模式下的网络信息安全防御机制，其中最为常见的就是通过公钥密码形式保护通信数据，即用户A通过公钥 PKB 对传输的明文数据X进行加密，当终端B成功接收加密的数据信息后，通过私钥 SKB 对其进行解密，就可获取传输的明文数据，公式为[2]：

$$DSKB(Y)=DSKB(EPKB(X))=X$$

其中加密的密钥*PKB*是开放型的，无法直接解密，即：

$DPKB(EPKB(X))\neq X$

转换后的解密算法：

$EPKB(DSKB(X))=DSKB(EPKB(X))=X$

对传输的数据信息进行加密操作，通过加密明文的形式传输数据，这样就将数据A伪装为密文B，从而保证通信数据的安全可靠性。对于现阶段的数据加密形式而言，数据包含的密钥位数越长，安全级别就越高，破译的难度就会显著提升，具体如表1所示[3]。

表1 不同密钥的基本破译时长

密钥长度（位）	密钥组合数量	破译密钥时长
16	2^{16}=65536	0.06h
32	2^{32}=68719476736	4h
56	2^{56}=72057594037927936	20h
64	2^{64}=18446744073708551616	200d
128	2^{128}=3.402823669209*10^{3}	1.07*10^{19}y

通过表1可知，当密钥长度超过32位时，数据的破译难度将大幅度增加，安全密钥的应用在一定程度上降低数据信息被恶意攻击的风险。随着我国网络技术的不断创新与发展，安全密钥的弊端也逐渐显现，其属于单传输路径的加密技术，难以达到计算机网络海量数据信息交互所期望的安全防御效果，且恶意攻击程序已能够破译部分密钥，无法保证通信数据的安全性。大数据技术具有的高效数据处理能力和智能化的逻辑学习能力，恰好能够在一定程度上弥补传统计算机网络信息安全防御机制的短板，保证网络的安全性，为用户提供更加可靠的网络应用环境。

2 大数据时代计算机网络存在的主要信息安全问题

2.1 数据安全管理规范性薄弱

计算机网络信息安全工作的实际推进，与数据安全管理工作的落实密切相关，基于现阶段计算机网络信息安全工作的管理现状，由于对计算机网络信息安全的技能培训、级别认证等工作的重视程度不足，使得部分专业技术人员在技术规范方面有所欠缺，网络信息安全防御工作落实不到位，未能实现“对症下药”。

在大数据时代背景下，智能化信息技术手段在不断优化升级，已被应用到越来越多的领域范畴内，数据信息安全管理工作与大数据技术的应用推广程度“渐行渐远”，无法跟上技术的推广速度，在计算机网络遇到数据信息漏洞时，也不能在第一时间给予针对性的解决方案，从而造成无法挽回的后果。

2.2 病毒查杀软件升级不及时

在计算机网络信息安全防御过程中，由于部分用户不能及时地更新升级计算机网络，使得不法分子有机可乘，通过病毒植入、黑客攻击等手段攻击用户计算机系统，从而对整体网络的安全运行造成严重影响。有时用户在未采取任何安全防御措施时，就直接将计算机与外部设备相连接，致使外部带有病毒的程序进入计算机系统内，窃取系统内的敏感数据，甚至危及用户人身安全。

还有一些用户在网页下载应用软件时，会遭遇捆绑软件的恶意侵扰，若执意下载该软件就必须同时加载恶意软件，但往往这些带有捆绑性质的软件含恶意程序；当用户随机浏览计算机网络的网站时，可能在无意间点击到带有病毒的页面，这样的话就会在不知情的情况下，将木马、蠕虫等病毒间接加载到计算机网络内，严重威胁计算机网络的安全性。

2.3 用户缺乏网络信息安全意识

随着网络的不断发展，海量的数据信息充斥在网络中，由于部分用户网络信息安全认知不强，上网时不注意保护个人隐私数据信息，给不法分子可趁之机，使得个人隐私数据受到威胁，甚至对人身安全造成伤害。

该情况发生的根本原因主要在于，当用下载网络软件、浏览网页时，无法精准地区分哪些软件、网页存在安全风险，非法网站诱使用户在其首页填报个人相关数据，其中包括姓名、身份证号、银行卡号等，这样不法分子不费“吹灰之力”就轻易获取用户个人相关数据，从而盗取资金或网络诈骗等。与此同时，部分用户缺乏识别网络诈骗的能力，现在越来越多的网络诈骗都是通过微信、电话形式与用户建立联系，然后精心地给用户布置“陷阱”，一步一步地骗取用户资金[4]。

2.4 网络信息安全监管力度不足

大数据发展背景下，计算机网络具有虚拟性、隐蔽性等特征，一些从事网络业务的公司，其将公司的办公场所安置在特别隐蔽的地方，未办理任何正规营业手续就开始运营，开发一些带有病毒的软件、网页等，从而规避监管机构的管控，非法运营。

由于我国对软件的管理制度不够严格，审核门槛较低，使得这些非法运营公司加工制造的软件未经审查就非法流入市场，从而给计算机软件市场和用户带来不良影响。因此，计算机网络信息安全监管力度不足，缺乏完善的安全管理机制和惩处制度，其将严重影响计算机软件市场的管理。

3 大数据时代提升计算机网络信息安全的防护措施

3.1 规范数据安全管理制度

大数据时代，在计算机网络信息安全管理工作的实施过程中，需科学合理地运用各方资源条件，强化计算机网络信息安全技能的专业审核力度，并特设专业的安全技术培训机构，制定具体可行的考核措施，规范安全管理制度体系。

在满足目前信息安全管理规章制度的同时，不断创新信息安全管理形式，提高计算机网络信息安全管理工作的主动性，及时发现计算机系统内存在的安全隐患，并给予针对性的解决方案。此外，在大数据背景下，还需充分结合网络的安全运行情况，构建多元化、多模式的网络信息安全管理方式，并根据实际情况制定更为详细的安全应急解决方案，在一定程度上提高计算机网络信息的安全性能，保证其安全稳定地运行。

3.2 及时升级病毒查杀软件

大数据时代，计算机网络信息安全技术在不断地更新迭代，但相应的木马、蠕虫病毒等也在不断升级。一旦木马、蠕虫等恶意病毒侵入计算机系统内部，不仅会使整个系统处于瘫痪状态，而且还会破坏或窃取用户的机密数据，在对用户个人造成经济损失的同时，还将会对人身安全造成威胁。

用户在平时使用计算机网络时，务必安装正版的病毒查杀软件，并定时升级更新杀毒软件，不给木马等恶意病毒留任何可趁之机。对于企业而言，可根据自身的系统的安全需求，设置不同的安全等级，并部署专门的企业版病毒查杀软件，安排专人定时对整个内部网络系统进行病毒查杀，不给病毒留任何“死角”，保证整个计算机网络的安全性。

3.3 增强用户网络信息安全意识

随着科学技术的不断创新与发展，网络已走进千家万户，用户是网络发展的核心要素。对于社会大众而言，在应用网络过程中必须提高网络信息安全防范意识。首先，需要了解、学习网络信息安全相关知识，增强自身防范意识，在网站下载应用软件时，务必提前用系统杀毒软件对其安全性进行检测，最好在正规网站下载软件[5]。其次，在浏览网页时，禁止浏览色情、赌博等相关网站，强化对个人隐私数据的保护。如设置计算机开机密钥、网银支付密码等，最好设置较高等级的密钥，增加密码的安全性，保护个人财产安全。最后，定期用杀毒软件对计算机进行病毒查杀，保证计算机使用安全性，在正规网站下载防火墙等杀毒软件，及时更新升级，设置一定的计算机检查周期，在规定时间及时对计算机内部进行全部检测，杜绝一切危险源，避免计算机网络信息安全事件发生。

3.4 加强网络信息安全监管力度

在大数据发展背景下，计算机网络信息安全不仅需要增强用户网络信息安全意识和提升网络软件安全性能，而且还需要加强政府部门对网络信息安全的监管力度。首先，需要完善计算机网络信息安全的相关法律条例，无法精准打击计算机网络犯罪的核心要素就是缺乏完善的法律法规管理制度，因此，需要完善相关法律制度，通过法律条例规范计算机网络犯罪的具体内容及相应的处罚制度，增强网络信息安全犯罪的成本，威慑不法分子的野心。其次，加强网络警察的监管作用，可以增加网络警察的数量，定期开展专项的打击网络犯罪的相关培训，提升网络警察自身综合素质，当发生举报网络犯罪行为时，能够在第一时间出警进行相应的调查，获取证据，抓捕罪犯。最后，完善计算机网络信息安全监督管理规章制度，强化对网络公司资质审查力度，加强对其研发软件的安全检测，对研发病毒软件、窃取个人隐私数据、盗取资产等违法行为的网络公司，必须严惩不贷，一追到底。

4 结语

在大数据时代背景下，人们与网络之间的关系变得越来越密切，但计算机在实际应用过程中会受到网络信息安全问题的影响。虽然市场充斥着多种多样的网络信息安全技术与防范产品，但依然存在病毒、黑客入侵计算机的情况。基于此，相关企业需根据计算机网络的实际现状，开发更为先进的计算机网络信息安全防护产品，提升网络防护策略，强化日常防护手段，保障计算机网络的数据信息安全，为用户提供良好的网络环境。

参考文献：

[1] 蔡广松 . 大数据时代计算机网络信息安全及防护策略研究 [J]. 计算机应用文摘 ,2023,39(01):96-98.
[2] 于晶晶 , 宋庆龙 , 李文博 . 大数据时代计算机网络信息安全防护 [J]. 电子元器件与信息技术 ,2023,07(02):4-6.
[3] 张定祥 . 大数据背景下的农村计算机网络信息技术的发展研究 [J]. 中国稻米 ,2021,27(06):1-3.
[4] 李根 . 计算机网络信息安全在大数据下的防护措施探究 [J]. 福建茶叶 ,2020,42(02):147-149.
[5] 郭秀峰 . 大数据时代下计算机网络信息安全及防护策略研究 [J]. 计算机应用文摘 ,2022,38(23):77-79.