大数据时代计算机网络信息安全防护策略探讨

陈少英*
海南省三亚技师学院 海南 三亚 572000

摘 要：随着大数据时代的到来，计算机网络俨然成为推动社会发展的内驱载体，但同时也暴露出一定的网络信息安全问题，对计算机用户带来一定的损害。因此需针对大数据时代背景下，应对计算机网络信息安全现状加以了解，并认知到可影响计算机网络信息安全的因素，同时对计算机网络信息安全防范策略展开探讨。

关键词：大数据时代；计算机；信息安全；防护策略
DOI：https://doi.org/10.37155/2717-5170-0306-4

1 大数据时代计算机网络信息安全防护的意义

所谓大数据时代，实际上就是数据爆炸式增长的时代。大数据本身就是指的内容庞大的信息数据体系，单从其字面意义来看，大数据的最为突出的一个特点便是“量大”，人们在使用互联网的过程中会产生大量的数据，这些数据本身就具备一定的使用价值，如果能将这些数据充分的利用起来，便可以从这些数据中分析出可用的信息。当然，大数据本身并非单纯的指客观存在的巨量数据，而是一系列与数据收集、数据处理、数据分析、数据运算相关的技术集。在这样的条件下，资源获取的途径与模式都发生了变化，为了满足学习工作的需求，就必须要做好信息的传递与分享，同时做好信息安全管理。

人们在使用互联网的过程中会产生大量的可供分析的数据，对这些数据加以分析会了解一个人的爱好、行为习惯，甚至是一个人的个人隐私和饮食习惯等，广告商十分精准的个性化广告推送正是基于大数据计算的原理。许多重要信息都可能会被盗用，随后对用户的信息安全构成损害。在一个网络环境当中，安全技术、管理制度以及保障体系等都是安全性的主要影响因素，通过安全信息管理，可以避免被不法分子攻击。

随着大数据时代的不断发展，现阶段计算机网络的多元化特征逐渐被激发，用户也开始尝试多渠道进行的分享与收集，这进一步增加了计算机网络信息安全的工作难度，需要更关注一些客观存在的风险与问题。如果在大数据时代不做好计算机网络信息安全防范工作，一个人将会完全的暴露在虚拟的网络中，这也是为什么在大数据时代人们的信息安全会面临更大的挑战。

2 大数据时代下计算机网络信息安全的影响因素

2.1 网络黑客刻意入侵

随着计算机网络技术的发展，网络黑客出现了，其对于网络系统开展信息攻击行为，对计算机网络信息安全造成极大的威胁，其伤害程度与病毒可以相提并论。网络黑客主要通过其自身具有的高端技术方法和手段对计算机网络系统中的服务器、主机等展开信息盗窃、信息拦截、信息破译等行为，进而从中获取对其有利的网络信息资源，并将所获取的相关信息数据资源进行买卖。这对于计算机网络信息资源[1]。

2.2 开放的网络环境

互联网最大的特点是其开放性和虚拟性，由于在网络中的行为没有实名制，使得任何一个人都可以在网络中尽情的发言和获取信息，但是很多人的安全意识薄弱，对在网络中保护个人信息安全的重要认识不到位，导致网络隐患的产生。同时，在网络开放使用的时候，互联网背景下的TCP/IP协议无法体现自身的安全性，导致网络基建的安全性缺乏，从而使得安全防护问题难以得到有效的解决。除此之外，开放的网络环境也让网络犯罪更难被监管，针对国内网民的境外组织网络犯罪几乎无法做到彻底禁止，由于这些不法分子都置身于国外，国内网络安全部门对其身份和犯罪手法的追查异常困难，这也是导致网络诈骗和个人信息泄露的重要原因[2]。

*通讯作者：陈少英，1985年8月，汉，女，海南，海南省三亚技师学院，教师，中级讲师，本科，研究方向：计算机网络。

2.3 非法用户的网络授权与访问

计算机网络系统的资源访问与使用，往往要经过网络防火墙、TCP/IP通信协议等的筛选，以及获得系统管理员的授权，才能进入某一网站或网页端口，完成自身需要的网络数据资源的访问、浏览与下载。但某些黑客针对网络系统存在的代码、程序漏洞为不法分子的入侵提供机会。黑客会通过程序调试与重写的方式，侵入到计算机信息系统内部，进行重要文档、网站或网页等的访问、篡改与资源下载。而非法授权或访问的行为，对计算机门户网站、重要数据资源、功能服务等，造成严重的攻击与破坏，使得现有的后台信息、代码执行出现严重的安全威胁。

3 大数据时代计算机网络信息安全防护策略探析

3.1 利用数据加密技术

数据传输的一种常见技术类型即为数据加密技术，以不对称密钥及对称密钥作为主要技术功能，以此在网络信道中实现数据信息接收及发出的加密、解密对数据传输双方网络信息安全加以保障。利用Noekeon算法展开对称密钥加密技术传输时，密钥函数Round-ct，多以16进制轮常数为主，如6C、3D、5A、64等，而加密明文数据时，此组轮常数则按照由右至左依次选择，解密明文数据时，此组轮常数，按照由左至右依次选择，在此过程中，应注意的是，此技术的优势为应用便利且加密、解密简单，因此也是此技术类型的缺陷之处，若入侵者可对此函数规律加以掌握，则加密防护无效。而以非对称密钥加密技术为基础的数据加密时，数据包收发两端的密钥内容存在一定差异。在此过程中，数据传输双方无需交换密钥，而需多次处理链路节点解密此种方式虽可推动数据加密强度的大幅度提升，然而此过程较为复杂，所耗费时间较长，因此，相关人员需以自身安全等级需求为依据，合理选择两种加密技术类型[3]。

3.2 杀毒软件方面的防护策略

计算机软件在设计时，需要留有一定的操作权限，实 现对软件的更新处理，但其将造成软件安全漏洞问题。对此，必须正确利用杀毒软件，及时修复各类程序运行过程 中所存在的安全隐患，进一步提高计算机内部的杀毒等级，对大数据环境下产生的各类数据进行病毒识别，同时也可 针对计算机内部的隐藏风险进行逐一查证。此外，在实际应用过程中应针对杀毒软件进行定期更新，因为系统本身 所具备的属性是针对于当前病毒库而实现逐一查杀的，一旦出现新型病毒的话，极有可能造成因为杀毒软件更新力 度不足引发的病毒查杀缺位现象，特别是在大数据运行体系下，多节点的数据爆发将产生更为严重的数据交错问题。为此，通过对杀毒软件定期更新，则可进一步提高数据查杀的安全性，保障计算机网络的安全运行[4]。

3.3 利用防火墙技术

防火墙以字面含义分析即指对计算机网络系统外部环境风险因素加以阻隔的网络屏障。此项技术主要即指预防未授权外部用户的入侵。大数据时代背景下，计算机操作过程中，用户实施网络行为时，多会借助网络信道的应用在外部公共网络、内部局域网间搭建数据连接，此为木马及病毒等危害程序的入侵提供机会，因此可借助防火墙技术的应用在内部网络空间、外部网络空间之间构建网关结构。分析检测当前外部网络的TCP分组、UDP报文及IP地址等，借此还可有效过滤冗余信息，提高外部数据包传输安全。除此之外，防火墙技术具备日志记录功能，所以相关人员完成防火墙的部署后，可通过防火墙访问日志的定期查看，对拦截频繁的危害因素加以分析，以此为依据，展开载体软件卸载及漏洞修补等方式，清除安全隐患，对计算机的稳定运行加以保障。除此之外，还可通过杀毒软件的安装，如360杀毒卫士、卡巴斯基及金山毒霸等杀毒软件的安装，提高网络信息安全防护效果，借此除可将杀毒软件所具备的自动防护及实时更新特点加以应用外，还可结合近期所新出现的病毒因素升级自身杀毒技术，对网络信息安全防护所存在的滞后性问题加以消除。而另一方面，伴随杀毒软件发展，病毒专杀及文件恢复等个性化功能推出，可将文件损坏及数据篡改等不良风险降至较低。

3.4 网络监测方面的防护策略

入侵检测技术是针对目前大数据网络中所传输的信息进行分析，利用统计学原理、大数据深度挖掘技术等，分析出信息在传输过程中存在的一系列隐患问题，进而规避数据信息被篡改或盗用的风险。常用的入侵检测技术可以分为统计法与签名法两种，统计法是针对计算机网络的信息传输模式进行预期化分析，检测出当前数据传输行为对于固有的计算机程序可能造成的影响，进而罗列出相对应的解决方案，规避数据安全风险问题。签名法则是针对计算机网络运行中的系统漏洞及弱点问题进行分析，通过全方位的监测与监控，对用户操作行为进行对接式的检测，且只有计算

机拥有者或者是相关权限人员才可正确操控内部数据的运作，以此来提高计算机运行的安全性。

4 结束语

在大数据时代，用户在互联网中留下的信息数据更多，个人信息安全和计算机网络信息安全防护更加重要，想要做好防护工作，应在提升个人信息安全防范意识的基础上，通过一系列有效的技术手段来实现。因此，计算机网络应用过程中，需重视良好计算机网络环境的构建。在此过程中将信息自动化、智能化等诸多优势加以充分发挥，借此还可推动大数据时代的良好发展。

参考文献：

[1]冯庆亮.大数据时代计算机网络信息安全与防护策略研究[J].企业科技与发展,2020,(01):94-95,98.

[2]赵培琨.大数据时代计算机网络信息安全及防护策略[J].计算机产品与流通,2020(05):38+54.

[3]张玉英.关于计算机网络信息安全中数据加密技术的运用分析[J].电子世界,2021(8):15-16.

[4]王晓生.基于大数据的计算机网络信息安全防护措施[J].中小企业管理与科技(中旬刊),2021(4):118-119.