基于大数据背景下的计算机网络信息安全问题研究

吕 达
（中国石油化工股份有限公司石油物探技术研究院，江苏 南京 210000）

摘 要：针对大数据背景下的计算机网络信息安全问题，本次研究结合我国计算机网络信息技术的发展现状，首先对计算机网络信息安全的基本概念以及风险特点进行简单分析，在此基础上，对可能出现的信息安全问题进行全面总结，提出信息安全问题的解决对策，为推动我国计算机网络信息安全的进一步发展奠定基础。研究表明：尽管我国在计算机网络信息领域的发展速度相对较快，但是仍然面临众多的信息安全问题，这些问题的存在对于我国计算机网络的进一步发展十分不利，因此，工作人员需要从加强安全管理、引入网络防火墙、应用杀毒软件、加强入侵检测以及信息数据加密等角度出发，分别采取多项有效措施，全面提高计算机网络信息的安全性。

关键词：大数据；计算机网络；信息安全；问题研究；防范措施
【DOI】10.12231/j.issn.1000-8772.2021.06.142

1 前言

近些年来，我国在计算机网络方面的发展速度相对较快，我国已经逐渐成为计算机网络应用最广的国家。在计算机网络发展的过程中，如何保障信息安全属于一项重大研究内容，网络信息的安全与普通网络用户之间具有直接的联系，如果网络的信息安全性降低，将使得网络用户产生巨大的经济损失，这对于社会的稳定性会产生消极影响[1]。针对此问题，本次研究主要是对网络信息安全问题进行全面的总结，并针对信息安全问题提出针对性的解决措施，为推动我国网络信息安全的进一步发展奠定基础。

2 计算机网络信息安全概念及风险特点

2.1 信息安全概念

所谓的信息安全主要指的是对网络中的相关信息进行全面的保护，防止出现信息泄露以及信息破坏等多种类型的问题。目前，我国计算机网络中的数据资源相对较多，这些数据资源将会应用于数学、通讯技术等各个领域，在保障信息安全性的过程中，只有在经过相关用户的同意以后，数据资源才能得到有效的调用，在进行信息处理的过程中，还需要全面保障数据资源的准确性，一般情况下，在用户访问数据资源的过程中，首先需要向授权人发出申请，在授权人同意以后，用户才能得到数据资源。事实上，信息安全保护可以分为两个方面，首先，确保整个网络空间处于相对较为安全的状态，此时需要对网络硬件设施进行合理的维护及升级，保障整个网络处于正常的工作状态，该种类型保护措施主要是为了防止出现木马入侵自己硬件损坏等问题；其次，对网络中的信息可靠性进行保护，以此防止出现信息泄露以及网络危害等问题，这就要求工作人员全面提高传输内容以及传输渠道的安全性[2]。

2.2 安全风险特点

在大数据快速发展的背景下，我国在计算机网络信息安全方面的特点主要可以分为四个方面：(1)隐蔽性，网络空间相对较为庞大，虚拟空间的数量相对较多，网络中存在大量的虚拟人物，这些人员与其身份之间都具备隐蔽性的特征，在出现非法信息窃取行为的过程中，时间和空间都不会出现限制性，即违法人员可以在任何的时间以及任何的空间中使用相关技术进行信息窃取，同时，这种类型的违法行为难以留下有用的痕迹，这使得工作人员难以有效的察觉；(2)智能性，在应用网络信息安全问题的过程中，受到大数据技术快速发展的影响，其智能性也得到了较大的提升，出现智能性特点的另一个原因在于非法人员掌握了全面的网络知识，可以根据网络存在的漏洞问题，利用自身的知识以及技术，使用各种类型的工具对网络信息攻击，最终到达破坏网络以及窃取信息数据的目的，在这种背景下，防止出现网络信息安全问题的难度提升；(3)突发性，即工作人员难以对网络信息安全问题进行全面的预测，无法提前采取合理的措施保障信息安全，同时，对于计算机中的病毒而言，其主要具有潜伏性特征，随着病毒的不断改进，使用传统的杀毒技术也难以发现，如果无法对其采取合理的防范措施，在病毒问题爆发以后，必然将会使得整个网络出现崩溃问题；(4)严重性，随着我国大数据领域相关技术的快速发展，在出现网络信息安全问题以后，必然会出现更为严重的危害，由于网络中的数据量在不断的提升，在进行数据收集以及分析的过程中，对于工具的需求逐渐提升，在出现信息泄露问题以后，必然会引发严重的损失[3]。

3 大数据背景下的计算机网络信息安全问题分析

3.1 黑客攻击

黑客攻击属于一种最为常见的安全风险问题，这属于一种人为的恶意攻击行为，其攻击主要可以分为两个方面，首先，可以发动主动的恶意攻击，不法人员在对攻击目标进行选择以后，将会以固定破坏的方式发出猛烈的攻击，还将会对网络中的漏洞进行充分的利用，对整个网络中的信息进行窃取或者修改，最终可能会出现信息缺失问题；其次，可以对相关信息进行破解，这属于一种非常隐蔽的攻击方式，并不会对网络系统产生严重的破坏，但是必然会出现信息泄露。事实上，无论不法人员采取何种类型的攻击方式，都会对网络的完整性产生影响，对信息安全性产生破坏，如果不法人员的攻击行为十分恶意，则会对整个系统的使用产生影响，甚至会出现系统瘫痪问题[4]。

3.2 网络开放性

对于整个网络系统而言，开放性属于其非常重要的特征，这也是网络系统可以得到快速发展的重要原因，由于开放性特征的存在，使得网络系统受到攻击破坏的概率提升，如果网络系统的安全性相对较低或者存在较大的漏洞问题，必然会出现信息泄露问题，开放性特征的存在使得网络系统的脆弱性提高。在目前计算机网络相对较为开放的前提下，传统的网络协议已经无法满足信息安全的基本需求，这使得整个系统的安全性严重降低，在安全协议运行的前提下，网络服务将无法满足用户的基本需求。

3.3 人为操作失误

尽管我国在计算机网络领域的发展速度相对较快，但是网络的安全性与用户的操作以及知识储备之间具有直接性的联系，在进行网络操作的过程中，出现人为操作失误的可能性相对较大，这使得网络信息面临众多的风险问题。随着大数据时代的来临，在各行各业使用网络系统的过程中，都会使用信息系统对所需要的数据资料以及信息进行收集及整理，由于部分工作人员的安全意识相对较差，缺乏系统的操作培训，操作过程中的用户口令与正确口令之间存在一定的偏差，最终会出现信息泄露或者丢失等问题，事实上，这也是网络系统时刻面临安全风险问题的重要原因。

3.4 垃圾信息

尽管网络中的信息数据量在逐渐的提升，但是垃圾信息的数量也在不断的增加，一般情况下，大量的垃圾信息主要是通过邮件的形式进行传播，该种类型的传播机制具有很强的强制性，通过使用邮件方式，可以对商业等各个方面的信息进行全面的传播。在另一方面，在进行垃圾信息传播的过程中，还会存在大量的病毒，在用户对信息进行点击以后，病毒会进入到网络系统之中，对网络中的信息进行窃取，同时，还会对网络系统进行全面的破坏，这会对系统的安全运行产生严重的威胁。

4 大数据背景下的计算机网络信息安全防范措施

4.1 加强安全管理

为了全面提高网络系统的安全性，首先需要采取合理的安全管理措施，通过对网络系统安全风险问题进行调研后发现，大量的安全问题都是由于平台账号存在漏洞所引起，因此，工作人员首先需要从平台账号的管理入手，通过加强内部管理以及提高安全防护两个角度入手，把账号的安全管理工作纳入到信息安全管理工作之中，账号的管理包括系统账号管理、邮箱账号管理等多个方面，全面提高账号的安全等级，这是防止出现安全风险问题以及提高网络系统管理水平的重要措施。同时，在进行账号管理的过程中，还需要树立正确的账号安全意识，提高账号密码的复杂性，如果账号密码相对较为简单，对于不法分子而言，其破坏的难度相对较低，通过提高其复杂性，不法人员难以对其进行破解，出现信息泄露问题的概率必然会大幅降低，用户还可以通过定期对密码进行更换的方式，防止出现密码泄露问题，账号的安全等级将会得到全面提升。综上所述，为了提高网络信息的安全性，用户首先需要对账号密码进行合理的管理及设置。

4.2 引入网络防火墙

通过引入网络防火墙的方式，可以从内部出发，对网络系统的访问进行全面的控制，防止外部的用户进入到网络系统之中，这是防止出现非法入侵问题的重要措施，通过引入防火墙的方式，还可以对内部的网络环境进行全面的优化，系统使用的稳定性也将会得到提升，由此可见，防火墙对于网络系统的使用十分重要。在应用该种技术的过程中，防火墙会定期对网络系统进行检查，可以及时发现系统中存在的病毒，通过进行全面的网络交互，对病毒进行清理，在进行数据传输的过程中，还可以采取阻止不法交互的措施，最终达到安全保护的目的。目前的防火墙技术相对较多，例如地址转换型防火墙、代理型防火墙以及检测型防火墙等，不同类型的防火墙技术应用原理存在一定的区别，但是都可以形成具有特色的控制特性，对外部的侵入行为进行控制，对目前网络中存在的威胁进行清理，最终保障网络系统的安全性。在防火墙引入以后，工作人员还需要根据防火墙的特点，对其进行合理的配置，使其可以发挥有效的作用，工作人员还需要定期对防火墙进行升级及更新，使其有效性得到提升。

4.3 应用杀毒软件

针对网络系统中的病毒入侵问题，使用高性能的杀毒软件十分重要，通过配置合理的杀毒软件，其会与防火墙之间相互搭配，定期对系统中的病毒进行全面的检测，事实上，用户只需要进行简单的点击操作，就可以使用杀毒软件完成环境检测以及漏洞修补等多种类型的功能，系统的安全性必然会得到大幅的提升，通过对系统中的病毒进行查杀，还可以有效保障数据资料的完整性。目前市场上的杀毒软件类型相对较多，对于不同类型的杀毒软件而言，其工作机制以及可以发挥的效果存在一定的差异性，因此，用户需要对杀毒软件进行合理的优选，随着大数据时代的到来，病毒会进行不断的变异，其攻击性会不断的提升，隐蔽性不断的增强，针对该种类型的问题，在配置杀毒软件以后，用户需要对其进行定期的更新以及升级，使得杀毒软件可以对最新的病毒进行识别，软件使用的效果得到提升。

4.4 加强入侵检测

入侵检测属于网络监控的一种技术，通过进行实时的入侵检测，可以对非法入侵行为进行不断的监测。事实上，网络系统中的入侵行为具有突发性的特点，非法入侵行为将不会受到时间以及空间的限制，用户难以觉察入侵行为，在这种背景下，进行网络实时监测十分重要。从监测的需求出发，常见的监测技术可以分为多种类型，例如统计分析方法类型以及签名分析方法类型等。所谓的统计分析方法主要是基于数学领域中的统计学理论，对系统操作行为进行全面的踪迹分析，以此对入侵行为进行识别，在发现入侵行为以后，可以及时发出报警，以便用户对其进行合理的处理；所谓的签名分析技术主要是对系统中的薄弱领域进行全面的监测，以此防止出现入侵行为。在另一方面，在使用入侵检测技术的过程中，还可以对系统中的病毒进行全面的检测，在发现病毒以后，可以使用杀毒软件对病毒进行处理。

4.5 信息数据加密

在使用网络系统的过程中，信息数据主要具有两种类型的状态，分别是保存以及传输，对于上述提出的众多措施而言，其主要是对保存中的数据资料进行保护，以此防止出现信息泄露问题，事实上，在对信息数据进行传输的过程中，出现泄漏问题的概率也相对较大。在大数据发展的背景下，对于保存中的数据资料而言，工作人员主要可以采取多种类型的加密技术，对信息数据文件以及文件夹进行加密，加密后的数据安全性必然会得到大幅提升，对于传输的数据而言，用户可以使用多种类型的数据签名技术，对传输的渠道进行全面的加密处理，防止在进行数据传输的过程中出现丢失问题，这是提高传输数据安全性的重要措施。

5 结束语

在大数据时代逐渐来临的前提下，网络信息的安全性成为了一项重要内容，网络信息的安全风险问题主要具有隐蔽性、智能性、突发性以及严重性等四种类型的特点，黑客攻击、网络开放性、人为操作失误以及垃圾信息等因素都会对网络信息的安全性产生严重的威胁，在出现信息安全问题以后，将会对社会发展的稳定性产生消极的影响，因此，用户主要可以采取加强安全管理、引入网络防火墙、应用杀毒软件、加强入侵检测以及信息数据加密等措施，全面提高信息安全性。

参考文献

[1]刘梦飞.大数据背景下计算机网络信息安全风险及防护措施[J].现代工业经济和信息化,2017,07(21):59-61.

[2]王永庆,张利民.对大数据背景下的计算机网络信息安全及防护的研究[J].科技资讯,2018,16(028):16+20.

[3] 闵晓玲. 大数据背景下计算机网络信息安全探究 [J]. 信息与电脑,2019,31(24):213-214.

[4]周亿城,陈靖,唐满华,等.大数据背景下计算机网络信息安全风险和解决对策研究[J].科技创新与应用,2020,27(35):89-90.

作者简介：吕达(1980-),男,工程师,从事软件研发及信息化管理工作。