基于大数据的计算机网络安全防范对策

朱颖芳
中国电信股份有限公司宁波镇海区分公司　浙江　宁波　315200

摘　要：伴随大数据技术的不断应用推广，进而对网络安全分析提出新的解决策略，主要利用大数据技术加强计算机网络安全智能化，以及对网络安全及时预测干预，从而减少网络安全问题引发的信息数据丢失等问题。本文主要探究大数据技术背景下信息技术在网络安全中如何规避风险并提高工作效率，供相关读者参考。

关键词：信息技术；大数据技术；网络安全

引言

如今我国计算机技术得到了大幅度提升，越来越多的企业逐渐开始利用大数据技术进行日常管理，但是由于计算机网络特殊性，相关工作人员在进行数据传输管理过程中很容易遭受网络安全威胁，导致数据出现漏丢情况，对于企业运行产生严重的影响，因此相关工作人员必须以大数据时代为背景，针对其特性提高计算机网络整体的安全性、可靠性，做好数据处理工作，从而保障企业正常、可持续发展。

1 大数据技术的应用价值

随着科技的不断发展，原本的纸质数据已被取代，更多的是电子数据应用在人们的生产生活中。电子数据的储存大多记录在计算机中，借助于网络信息技术进行传播。因此，在使用电子信息时，一定要注意网络环境的安全。电子数据方便了数据的储存和传递，数据本身也呈现多样化发展，对于存储要求有一定程度的提高，且数据信息也在不断扩充。为保证网络数据库平台的稳定运行，一定要对计算机网络信息安全的防护措施进行研究。最早的数据应用只是将大量的数据通过整合分类，分别编入不同的数据库，然后再对数据进行精化处理，保存最核心的数据。在竞争市场上，单位拥有的核心数据也体现了单位的竞争能力和实力强弱，是单位的一个发展基础。所以为保证企业内部的运营安全，必须要加强网络信息技术防护，保证数据安全。云技术发展所带来的是信息数据存取传输便利优势，在错综复杂的网络空间中能够储存大量的数据。而这些数据，其不仅仅代表着本身的数字意义，还蕴含着各个企业生存发展空间和未来的成长价值。数据爆炸的时代，能够及时接收到更多信息，更加方便日常的生活和工作需求。但同时，信息的大量传播也会导致用户私密信息恶意泄露，使用户自身的信息处于不安全的状态。所以，计算机网络也是一把双刃剑，无论如何都要加强对网络信息安全的重视[1]。

2 计算机网络信息安全的影响因素

2.1 计算机病毒的攻击

针对计算机网络来讲，具有非常强的开放性特点，不会受到地域、空间以及时间的限制，这对于计算机病毒的侵入能够提供有利条件。病毒不仅仅能够将自身有效的隐藏在计算机软件、存储器等多个空间和媒介中，并且也能够为后期对计算机的侵害带来很大的便利。除此之外，计算机病毒也就具有较强的传染性以及迫害性，不仅仅能够对计算机后期的运行，同时对计算机当中存储的数据，也能够带来较大的危害，其主要的传播途径还能够分为硬盘、光盘以及软件。

2.2 网络黑客恶意攻击

计算机网络面临另一安全隐患问题就是网络黑客的攻击，尤其是近年来随着经济的快速发展，市场竞争环境的日益激烈，部分网络黑客为了获取更多利益，采取盗取企业商业信息，窃取相关信息转卖他人从中赚取利益。黑客之所以能够恶意攻击计算机网络，一大部分原因与网络安全系统保护力度不强有很大关系。部分企业不重视网络安全信息保护，简易的安全系统给不法分子可乘之机，严重扰乱企业网络正常运行，危害企业正常工作秩序，给企业各个人带来严重损失，所以加强计算机网络安全系统尤为重要。

2.3 系统漏洞

操作系统或应用系统中存在的缺陷被称为系统漏洞。当系统漏洞被黑客利用时，数据和信息就会泄露和丢失，给数据的合法用户带来无法弥补的损失。大数据存储了大量数据，通常需要以分布式方式存储，这使得数据保护相对简单，黑客利用的难度也较小。如今，人们通常使用补丁修复来修复系统漏洞，而在修复操作完成之前，计算机面临着更为严重的信息安全威胁。

2.4 网络安全意识不足

就目前情况分析来看，计算机技术在大数据背景下的应用对人们的生活工作形成极大的便利。但在使用过程中仍然存在较多网络安全问题，这主要体现在部分用户使用计算机的习惯和意识，部分用户在使用计算机的过程中，对网络安全意识薄弱，因此对计算机和移动终端的安全配置没有进一步完善，从而导致网络安全问题极易发生。此外，用户的甄别能力也较差，对于不正规网页会因为好奇心理随意打开，对于钓鱼网站也没有较高的防备心理，将使用弱口令、信息系统资产信息随意存放且不加密保护，这些使用习惯都会对网络安全产生较大威胁[2]。

2.5 人为操作问题

导致数据错误计算机网络信息的录入需要人工操作完成。计算机网络本身就是一个比较复杂的环境，信息技术门槛还是比较高的，对于普通的群众来说无法深接触。但其在信息传输的过程中，很有可能会受到人为操作因素的干扰，因为整个过程是按照指令进行，一旦某一环节出错将会使数据泄露，同时，整个传输系统还会受到损害。系统的损害是一个不可逆的环节，对计算机的防护功能产生影响，导致数据丢失或者泄露。人为操作失误可能是数据录入错误，对于这样的问题，要想实现有效预防可从录入系统着手进行处理，系统假设数据性质和划分数据范围，从而可极大程度降低录入错误率。信息传递错误，需要从发出站点与接收站点进行管理，站点设置特定的传输路径对于异常数据进行拦截返回。人为失误将会导致信息存储位置发生改变，致使系统无法对数据进行有效识别，管理防护系统不能正常发挥作用。

3 大数据时代背景下网络安全存在问题的原因

3.1 计算机信息管理技术不高，影响社会网络运行

近年来随着经济的快速发展，市场竞争环境的日益激烈，部分网络黑客为了获取更多利益，采取盗取企业商业信息，窃取相关信息转卖他人从中赚取利益。黑客之所以能够恶意攻击计算机信息网络，一大部分原因与网络安全系统保护力度不强有很大关系。部分企业不重视网络安全信息保护，简易的安全系统给不法分子可乘之机，严重扰乱企业网络正常运行，危害企业正常工作秩序，给企业各个人带来严重损失，所以加强计算机信息网络安全系统尤为重要[3]。

3.2 计算机网络维护管理体系缺乏规范性，不利于网络维护工作开展

受到计算机网络环境及行业影响，加之计算机网络维护成本相对较高，所以导致计算机网络维护管理体系缺乏规范性，不利于计算机网络维护工作的开展。忽视基层计算机网络维护工作人员，在部分企业单位，由于人事管理部门缺乏对计算机网络维护的认识，所以在人员调配上将一些专业化计算机人员全部调往技术研发部门，而将一些非专业计算机人员配置到计算机网络维护工作中。严重影响计算机网络维护工作质量，无法确保计算机网络安全工作的顺利实施。尤其是非专业计算机网络维护人员缺乏对计算机网络维护的相关知识与技能，缺乏对计算机网络维护工作设备原理的掌握。所以即使一些威胁计算机网络安全的简单问题都不能够在短时间进行解决，很可能致使问题的扩大化，给后续计算机网络维护工作带来困难。不利于计算机网络安全维护工作的顺利实施。

4 保障大数据时代计算机网络信息安全的有效措施

4.1 加强安全系统建设，弥补漏洞

为保证计算机使用的安全，应提前建立合理的安全防范措施，优化计算机网络运行环境，弥补可能存在的漏洞。通常软件系统不可能尽善尽美，所以用户应根据自己的具体需求，在多留意软件的官网的更新补丁、软件版本的同时，对软件和补丁的更新规则进行仔细阅读和了解，然后根据自身的实际需要更新下载补丁和系统软件。漏洞扫描软件的使用可以帮助用户定期修补系统漏洞，使软件系统进行自我防御，防止病毒因为系统漏洞侵入计算机。

4.2 加强杀毒软件的杀毒能力

大数据时代下，随着用户数量的增加，计算机网络病毒的种类和数量也日益增多，加大了网络安全的防控难度。因此，在加强计算机的防火墙设置的前提下，还应注重网络安全性的提高。在不影响数据的正常传输的前提下对网络上的数据进行过滤，能够有效地阻断恶意病毒和垃圾邮件，防止病毒对计算机的入侵是计算机防火墙的重要作用。公司和个人用户的信息可以分为内部管理和外部管理两部分。一般情况向外部管理的安全性远不如内部管理。因此，计算机防火墙除了定期检查内部和外部系统，还应对计算机系统外部环境的安全进行检查，抵御病毒和垃圾邮件对计算机的入侵[4]。

4.3 安装杀毒软件以及防火墙技术

一般情况下计算机用户在使用前都会安装主机防火墙技术和杀毒软件。杀毒软件能够有效将病毒从数据中识别，也能够及时发现是否有病毒是否入侵电脑。比如现在大多数用户使用的杀毒软件是360杀毒或者鲁大师软件等，这些都是能够很好保护计算机网络安全的杀毒软件，可以有效避免计算机网络受到恶意攻击，同时杀毒

软件还能够有效防止病毒攻击网络所造成的数据流失，从而减免一些损失。但是使用用户要注意的现在杀毒软件种类繁多，尽量要选择适合自身系统的杀毒软件，并对杀毒软件及时进行更新。

4.4 加强防黑客技术

黑客的攻击性是有目共睹的，但是黑客攻击也提高人们对网络安全的重视，因此用户在使用计算机方面要定期更改账户密码，以及定期更换IP地址，并结合相关的权限管理，通过智能卡以及智能密码钥匙或者指纹密码等对自身的信息安全进行保护，这样才能够最大限度防止黑客的攻击。此外，通过安装一些杀毒软件也是预防黑客的方法，但是对于这些杀毒软件用户一定要定期更新，未能定期更新用户的杀毒软件会短暂性的无法识别非法访问，从而导致被黑客攻击。

4.5 关闭不使用端口

通过一台计算机是有多个端口存在的，而这些端口则是黑客进入计算机影响网络安全的途径之一。因此用户在使用计算机后要将个别不使用的端口及时关闭，从而减少黑客进入机会。一般计算机的端口主要是有TCPI35、139、1025等，这些则是用户经常使用的端口，同样也是黑客较为容易入侵的端口。因此用户在使用计算机后要将这些端口关闭，同时下载端口监视器，这样就可以避免当黑客入侵时候发现不及时而造成的损失[5]。

4.6 做好身份认证和加密工作

加密工作是提高数据安全性的重要措施之一，也是保障计算机网络安全工作得以顺利开展的基础，因此相关人员在应用计算机网络进行数据处理时要做好相应加密工作。如今我国计算机技术发展较为良好，加密技术要求也要逐渐提高，传统纯数字加密已经无法适应时代需求，相关工作人员可以利用数字与字母结合方式来进行加密，避免出现数据流失情况，同时在部分条件允许情况下，相关使用人员以及管理人员还可以利用身份认证方式来进行加密，如指纹识别、虹膜识别、人脸识别等，从而避免不法分子利用网络技术盗取重要信息，提高计算机网络整体的安全性。

4.7 提高使用者的信息安全意识

在现代社会，生活的地方已被网络缩短时间和空间上的距离。每个人都在网络的笼罩下，是网络的使用者也是受益者。但是信息安全教育却还没有得到很高的普及，导致民众在使用网络时没有较多的自我防护意识，使自己的隐私信息全部暴露于网络之中。为保证国家和个人的生命财产安全，国家应该加强计算机网络知识的普及宣传，对大龄网民和较小的儿童进行安全引导，规范使用行为，期间还要提升自我保护意识。可以帮他们免费安装一些杀毒软件，对电脑进行定期的健康体检。国家也要提升对网络的监管力度，对网络上的不法分子进行严查，彻查；对于一些不法消息或者谣言要及时地禁止，在网络信息平台上也要规范大家的语言，禁止传播不良消息，为广大使用者创建一个绿色使用环境[6]。

5 结束语

现代计算机网络普及程度不断加深，影响着人们的生活、学习与工作，给人们带来极大便利，对促进社会经济发展具有重大贡献。但是随着网络技术被委以重任，各种病毒、网络黑客为可盗取企业、个人机密、获取用户个人信息牟取暴利，加大计算机网络安全尤为重要。虽然各类计算机网络安全事件的爆发，人们已经开始加强对网络安全重视，但是随着计算机网络技术的不断发展，计算机网络将会面临新的安全问题。因而为了确保计算机网络安全，就需要不断创新更全面、更好的计算机网络安全与防护方式。本文基于此首先对计算机网络进行阐述，并阐述网络安全的重要意义。最后针对当前计算机网络中存在的问题进行分析，最后针对问题提出针对性策略，希望对提高用户计算机网络安全意识，加强网络安全维护技术，切实保证计算机网络安全有所借鉴。

参考文献

[1]张瑞显.大数据时代计算机网络信息安全及措施研究[J].轻工科技，2022（1）：72-74.

[2]王魏，赵奕芳.大数据时代计算机网络信息安全及防护策略[J].中阿科技论坛（中英文），2022（1）：72-75.

[3]李超.大数据时代计算机网络信息安全及防护策略研究[J].数字通信世界，2021（03）：138-139.

[4]刘浩.大数据时代计算机网络安全问题研究[J].数字技术与应用，2020，38（10）：180-182.

[5]田言笑,施青松.试谈大数据时代的计算机网络安全及防范措施[J].电脑编程技巧与维护,2019(10):90-92.

[6]曾生根.试谈大数据时代的计算机网络安全及防范措施[J].中国新通信,2019(22):91-92.