大数据时代计算机网络信息安全问题研究

亓 兵
(山东道普测评技术有限公司,山东 济南 250000)

摘 要:大数据时代下,计算机网络信息技术不断优化,在我国各行各业中得到了广泛应用,为促进行业转型、产业升级做出了重要的贡献。但是,由于受到各种因素的影响,目前计算机网络信息安全问题的存在影响着计算机网络信息技术的应用效果。文章主要对大数据时代下计算机网络信息安全问题的影响因素进行了分析,探讨了确保计算机网络信息安全的重要性及其有效措施。

关键词:大数据时代;计算机;网络;信息;安全问题
中图分类号:TP391.7 文献标志码:A 文章编号:2095-2945(2019)14-0052-02

Abstract: In the era of big data, the computer network information technology has been continuously optimized and widely used in various industries in our country, which has made important contributions to promoting the transformation and upgrading of the industry. However, due to the influence of various factors, the existence of computer network information security problems is affecting the application effect of computer network information technology. This paper mainly analyzes the influencing factors of computer network information security in the era of big data, and probes into the importance of ensuring computer network information security and its effective measures.

Keywords: big data era; computer; network; information; security problems

互联网技术飞速发展的同时,也带来了海量数据,使得现代社会进入大数据时代。大数据时代的到来,改变了人们的工作、交流方式,为思想观念的创新提供了有力的支持。但是,大数据时代同时也带来了计算机网络信息安全问题,信息数据失真现象的出现,影响着信息使用的实效性。基于这样的原因,必须加强对计算机网络信息安全防护技术的重视,明确影响信息安全的主要因素,采取有效的措施、技术确保信息安全。

1 计算机网络信息安全的主要影响因素

1.1 自然灾害

计算机网络的设备很难全面抵御外界因素的伤害,例如,在遇到雷击等自然灾害或者是污染的时候,无法进行自我保护,给信息安全造成了一定的威胁。

1.2 病毒侵袭

网络的开放性,给病毒侵袭提供了极大的便利。病毒的本质是恶意程序代码,具有保存性、隐藏性、潜伏性的特征,计算机网络一旦遭受病毒入侵,便可以迅速复制,破坏数据及计算机功能。以往的计算机网络以局域网的形式连接,未连接外界网络,因此能够安全、稳定运行,外界病毒难以入侵。目前,广域网的应用,虽然提高了信息资源的共享、利用效率,但也为外界病毒的侵袭提供了更多的途径。同时,病毒能够以硬盘、软盘为媒介传播,如 CIH 病毒、熊猫烧香病毒等,给计算机网路信息安全带来了严重的威胁。

1.3 网络的开放性

众所周知,计算机网络具有开放性特征,从另一角度来看,计算机网络有着脆弱性、不稳定性的缺点。网络协议是计算机网络中进行文件传递、信息传输的指令与标准,若是网络协议存在技术上的问题,则会带来巨大的安全隐患,一些不法分子可能会利用网络协议漏洞来拦截信息,进而使信息遭受破坏、损失或者是恶意篡改。目前,TCP/IP 协议是最为常用的一种网络协议,其主要面向资源共享,因此普遍存在异常、安全漏洞。同时,网络系统自身缺失信息处理功能,故容易产生计算机网络信息安全问题。

1.4 黑客攻击

计算机网络应用中,黑客攻击是影响信息安全的主要因素。黑客攻击指的是人类恶意破坏网络信息的一种行为,包括被动攻击、主动攻击两种类型。被动攻击指的破解、截获网络信息,不会影响网络的正常使用;主动攻击指的是针对攻击目标,破坏信息的完整性,会影响网络的正常使用。IP 欺骗、口令攻击、数据劫持与网络窃听是黑客攻击的常用手段。黑客攻击计算机的时候,主要是利用网络探测技术获取目标 IP 地址,实施 IP 欺骗,在协议传送报文的时候出现 IP 地址受到攻击的问题,黑客会提供一个虚假认证,将自身伪装网络主机,进而将 TCP/IP 地址复制下来,骗取返回的报文,导致信息泄露。口令攻击是指黑客通过入侵数据恶意攻击计算机网络系统,破坏相关数据,一些黑客为了盗取数据,确定目标后,便会应用抓包技术截取信息,在破解系统口令屏障的时候,主要采取“字典”穷举方法,得到正确口令。数据传输时最常会出现网络窃听与数据劫持,即在终端输送信息的过程中,受到黑客的网络窃听与数据劫持,导致信息数据被他人获取。

2 确保计算机网络信息安全的重要性

大数据指的是庞大的数据体系。大数据技术本质上指的是在大量数据信息中迅速、简捷地提出重要信息的一种

作者简介:亓兵(1986,09-),男,本科,学士,研究方向:信息安全。

技术，其特点包括：第一，信息数量多。随着科学技术的迅速发展，当今社会对数据信息的需求量、使用要求不断提高，为确保数据的准确度，必须不断提高对数据信息的筛选、加工、处理水平；第二，数据信息内容多样化。包括图片、文字、视频等，与以往单一的数据结果有着明显的不同，由于数据信息类型的多样化，使得信息筛选更加复杂、难度更大。

大数据时代下，做好计算机网络信息安全防护工作，是提高信息利用效率的前提与基础。大数据信息处理过程中，利用计算机网络，可以实现数据传递速度的提高，也有利于加强数据信息的处理效果。但计算机网络的实际应用过程中，存在着诸多安全隐患，信息安全问题频频出现，甚至导致企业机密信息、人们隐私信息泄露，带来巨大的经济损失。基于此，为确保个人、企业、国家信息安全，必须做好计算机网络信息安全防护工作。

3 确保计算机网络信息安全的有效措施

3.1 健全计算机网络信息安全防护机制

大数据技术近年来得到了十分广泛的应用，在人们生活、工作中占据的地位、发挥的作用越来越重要。科学技术迅速发展的当今，大数据与信息技术、计算机、网络技术的融合发展，促使人们在任何时间均能借助大数据、计算机、信息技术获取社会事件的相关信息，如了解电气设备发展现状、身体健康水平、物流产业的发展趋势等等，大数据时代下，计算机网络为人们提供了丰富的信息。因此，确保计算机网络信息安全，有着重要的意义。目前，必须针对大数据计算机网络信息安全，制定相关法律条款及安全防护机制，借助法律的权威性，确保信息安全。同时，国家还要制定网络信息安全保障法律法规，使人们能够借助法律武器保障个人信息安全、个人隐私不被泄露。

3.2 应用计算机网络信息安全防护技术

大数据时代下，为确保计算机网络信息安全，必须在遵循相关法律法规的基础上，加强对安全防护技术的应用，才能确保信息安全。

首先，加强对病毒检测技术的应用。做好对入侵病毒的检测，并加强安全防护，是确保信息安全的有效手段。病毒入侵检测系统可以监视黑客攻击行为的网络传输，有着规则更新迅速、识别率高、可靠性强等优势。同时，在进行事后分析时，还可以准确界定责任事件、责任人。同时，还可以联合网络控制技术、信息认证技术等，以有效控制、防范黑客入侵行为。

其次，加强对杀毒软件的应用。杀毒软件可以发现计算机网络中的病毒，并及时采取有效的措施予以处理。目前常用的杀毒软件有腾讯管家、360 安全卫士等，但是不同的杀毒软件存在干扰，应根据实际情况合理选择，并要及时更新，以提高计算机网络的安全等级。

再次，加强对防火墙技术的应用。防火墙是预防黑客入侵、病毒攻击的有效手段，有利于维护计算机网络的安全，也是目前计算机中广泛应用的安全防护屏障。防火墙主要借助网络通信监控系统构建而成，可对访问过程进行有效识别，对无授权网络的访问造成屏蔽，进而达到预防病毒入侵的效果。现阶段比较常用的防火墙主要有应用代理型防火墙、网络地址转换型防火墙、状态检测型防火墙以及包过滤型防火墙。其中，防火墙的最高层次便是应用代理型防火墙，其为一种特质代理程序，能够逐段传输信息，从而能够对网络进行全程监管，时效性、安全性较高，且可将入侵的病毒在第一时间内扫描出来。同时，还要对防火墙进行定期升级，做好信息备份工作，保障信息安全。

最后，应用对称加密、数字签名技术。对称加密技术，顾名思义，指的是对信息进行对称加密，这样的情况下，若是有人想要读取这些信息，需要在系统登录上提供解密密钥。对称加密技术具有算法效率高、可靠性好、破解难度大的优势，可有效保障信息安全。但是，其对密钥有着较强的依赖性，一旦密钥泄漏，那么任何人都能解锁、读取信息。基于此，在对称加密技术的实际使用过程中，应加强密钥保护。数字签名技术是在对称加密技术基础上研发的一种技术，具有独有密钥，密钥具有不可复制性、唯一性，B/S 模式认证后，无密钥授权的系统无法访问网络、调用信息，从而可以提高信息保护效果。

3.3 加强安全管理

近年来，科学技术迅速发展，计算机网络技术也在不断更新，各种数据信息的真实性逐渐加强，且具有多重价值。基于此，如今诸多企业均在致力于加大对计算机网络技术的开发与利用，以促进经济效益的最大化。但是，在这个过程中，计算机网络信息安全问题也是不容忽视的。针对这样的发展现状，国家及政府应高度重视，加强对相关企业的管理，成立专门的管理部门，安排相关人员定期核查网络运行代码，采取人为检查手段，保障计算机网络信息安全。

4 结束语

综上所述，自然灾害、病毒侵袭、网络的开放性以及黑客攻击是威胁计算机网络信息安全的主要因素。为确保计算机网络信息安全，应尽快健全计算机网络信息安全防护机制，对病毒检测、杀毒软件、防火墙、对称加密技术、数字签名技术等信息安全防护技术进行有效应用，并要加强安全管理，以促使计算机网络为人类提供更加安全的信息服务。

参考文献：

[1]赵海涛，赵毅.大数据时代计算机信息安全防范措施[J].电子技术与软件工程，2019(05)：200.

[2]龙振华.大数据时代计算机网络信息安全及防护策略[J].中国管理信息化，2019，22(06)：161-162.

[3]张黎明，刘燕.大数据时代计算机网络信息安全与防护措施[J].电子技术与软件工程，2019(04)：190.

[4]杨继武.简析大数据时代的计算机网络安全防范[J].科技传播，2019，11(04)：108-109.

[5]周宝富.大数据时代计算机信息处理技术分析[J].信息与电脑(理论版)，2019(04)：7-8.

[6]赵颖.大数据时代计算机网络信息安全及防护策略探析[J].中国新通信，2019，21(04)：63-64.