大数据时代计算机网络安全防范策略

刘新汉

（贵州财经大学， 贵州贵阳 550025）

摘要：在大数据时代的背景下，计算机网络已经面临了前所未有的安全威胁，本文针对这一问题进行了分析，并针对性地给出了相应的网络安全防范策略，希望能提供一些进行计算机网络安全风险化解的建议，促进大数据时代计算机网络的健康可持续发展。

关键词：大数据时代；计算机网络；网络安全

1、前言

科学发展的过程中，计算机网络现在已经越来越完善。但是在大数据时代中，计算机网络信息安全依然是人们难以解决的一个重点问题。这样的背景下，大数据虽然为人们的生活和生产提供了较大的帮助，但是与此同时也带来了较高的安全风险问题。

2、计算机网络安全

2.1 有关概述

大数据是分析和处理大型复杂数据的技术，大数据具有数据量大、多样性强、数据处理速度快、数据值密度低等功能。计算机网络安全的关键是计算机网络的信息安全。顾名思义，它是指计算机网络环境中用户网络信息的安全性。主要的使用方法和手段是相关的安全技术。目的是为了避免网络用户泄露信息以及网络用户和其他黑客的恶意攻击。为了保证计算机网络的安全，必须建立专门的计算机网络信息保护系统。先进的技术是建立这样一个体系的先决条件。最终目标是有效保障网络环境的纯净与和谐，保障计算机网络用户各方面的信息安全。大数据主要指海量数据。数据中有很多有用的信息。大型数据处理和应用严重依赖于云计算，云计算是计算机网络的核心，改变了人们获取资源的方式。在全面分析信息内容的安全性时，要保护数据信息的安全，防止数据泄露和破坏，并设置有权限的特定用户，防止非法用户非法操作信息、任意修改数据和窃取信息，对合法用户的安全构成威胁。信息数据销毁时，要及时维护数据安全，制止非法操作。在分析数据分布和管理安全性的基础上，防止病毒入侵和网络攻击。维护网络安全系统，确保数据传输的安全。在管理和分析数据的安全性时，需要全面分析软件的可操作性，实时监控计算机网络的安全性，并针对威胁网络安全的因素采取相应的对策，才能达到保护数据的目的。

2.2 网络安全现状

在大数据时代，计算机网络安全保护不仅包括计算机网络硬件的维护，还包括计算机网络数据安全的日常维护和管理，以及计算机网络通信和管理安全的综合分析。在大数据时代，更有必要采取严格的措施防止网络安全遭到破坏。逻辑安全涉及数据完整性、机密性和可用性，防止非法用户破坏和篡改数据。日益增长的存储容量导致了当今大规模的数据安全问题。在大数据时代，最重要的问题不仅是数据的数量，而且是数据的多样性和数据的集成、交换和分析，以及数据的安全。

3、大数据时代的信息安全问题

3.1 环境因素

客观地说，计算机外部的硬件问题构成了计算机网络潜在的信息安全风险。为了保证计算机网络外部设备的安全运行，必须创造一个舒适的外部环境，避免在高温高湿的环境中使用计算机网络外部硬件和设备。此外，雷电、洪水、火灾、地震等自然灾害造成的破坏，将直接导致计算机网络数据信息存在丢失隐患，如用户信息数据的丢失。目前，世界范围内自然灾害造成的计算机网络信息安全风险是难以完全避免的。

3.2 系统软件漏洞

计算机网络信息安全的诱因是系统软件本身的脆弱性。系统软件是计算机本身的软件。如果系统软件本身存在漏洞，将存在巨大的安全风险。例如，别有用心的人发现并利用系统软件存在的漏洞进行攻击，将直接导致计算机网络信息的泄露或遭到破坏。目前，在开发计算机系统软件的过程中，为了避免上述情况的发生，系统软件本身通常是经过加密和授权的。这是一种预防性战略，但不是绝对的安全战略。它起作用的前提是，系统不存在漏洞，或漏洞被及时修补，从而避免系统不会受到别有用心的人的恶意攻击。如果系统软件被成功攻破，损失将不可估量。

3.3 人为因素

一些犯罪分子利用高科技手段窃取网民信息，可能给受害者造成严重的财产损失。随着计算机网络系统在我国的普及，越来越多的人可以接入计算机网络。其中一些人的计算机基础知识水平较低，对计算机系统的运行情况知之甚少。因此，在使用电脑的过程中人们经常会做的偶然安装计算机病毒和恶意软件，浏览非法网站等问题都会很容易导致窃取个人信息的情况发生，简单的网络支付密码也会很容易导致财产损失，各种安全风险都与计算机网络用户个人的具体行为有着直接的联系，这些都属于是人为因素形成的计算机网络信息安全风险，可能导致不必要的损失。

4、强化网络安全的措施

4.1 加强权限管理

计算机网络信息安全系统从系统层面上保证计算机网络信息的安全，也是从信息源上采取的基本措施，同时从制度层面上也要加强保护，对访问权限进行严格限制。第一步是限制对计算机用户信息的访问，建立基本的访问认证流程：密码、指纹、短消息认证、计算机用户认证和系统登录认证。限制访问违反规则的计算机用户。严格对相关网站用户行为和访问权限的管理，对网站的访问实行完全封闭的管理。没有访问权限的计算机用户将被阻止进行后续操作，防止非法访问计算机网络信息数据。同时，未经授权的计算机用户将被关闭对该网站的访问。

4.2 提高意识

一些高科技罪犯可以利用计算机网络获得不公平的回报。

（下转第 246 页）

（上接第 232 页）

大数据时代的背景为这些人提供了强大的技术支持和便利。普通计算机网络用户必须防范此类高科技犯罪，才能保护自己的财产和人身安全。对于每一个企业来说，都需要掌握常见的网络攻击技术，提高防范计算机网络黑客窃取信息的预警速度。从内部计算机系统本身入手，不断更新自己的系统，减少系统软件本身的漏洞。其次，采用防火墙、杀毒软件等技术，防止各类病毒的入侵。企业还应对数据保密，严格控制计算机网络信息的外部实时认证，维护计算机网络信息安全。

4.3 完善计算机网络安全管理制度

完善计算机网络安全管理制度是管理层面的宏观调控。这是打击网络犯罪的前提，可以有效地提高计算机网络的安全管理效果。网络信息安全与人们的隐私和财产息息相关。在大数据时代，这些信息尤为重要。一旦犯罪分子利用技术从计算机用户那里窃取个人信息，他们可以在极短的时间内利用这些信息窃取受害者的金钱或其他财产。企业需要开发相关的计算机网络安全管理系统，并在系统中实现网络安全管理的相关内容，如定期培训、提高计算机用户的安全意识和风险意识等。通过建立奖惩机制，鼓励员工从企业系统内部信息资源的角度自觉实施信息安全管理。

4.4 改进身份认证技术

网络身份认证技术的改进主要是为解决计算机网络信息安全中的密码窃取、身份假冒等问题，有利于计算机网络信息安全的管理。目前，计算机网络主要使用口令来认证身份和管理信息。传统上，这种方法比较落后，主要是因为它的安全性较低。近些年来出现了多种具有更高安全性的技术，其中一项已经得到广泛使用的就是生物特征识别技术，这项技术具有相对较强的安全功能，因为这一技术可以针对性的利用人体大量难以复制的生物特征进行身份标识，可以有效避免被假冒，从而进一步避免信息泄露。网络身份认证技术向生物识别技术的发展，对有效保护人们的网络信息和人身、财产安全具有重要作用。

网络安全系统软件可以有效地防止大多数恶意攻击。在大数据时代，人们的生活和工作往往离不开计算机网络，这有利于网络安全系统软件的推广。防火墙和杀毒软件是网络安全系统软件推广的两个主要内容。外来非法用户想要进入计算机或者影响计算机的运行，首先要面临的就是杀毒软件和防火墙，杀毒软件是一种既能保证网络安全又能抵抗传统病毒攻击的安全软件。网络安全系统软件开发部门应采用大数据技术对病毒库进行更新，以适应不断更新的各种网络病毒，在提高自身技术水平的基础上促进网络信息技术安全的稳定发展。

5、结束语

在大数据的时代背景下，计算机网络信息安全一直是广大网络用户普遍关心的重点问题所在，大数据给人们的生产生活带来了便利的同时也带来了一些安全问题，结合大数据技术自身的特点可以对这些安全问题进行针对性的解决，首先要了解其中存在的安全风险，然后加强安全管理意识，随后可以针对性的应用一些技术手段来进行安全风险的化解。

参考文献：

[1]董德尊. 大数据时代的计算机网络安全及防范措施[J]. 网络安全技术与应用, 2019(6):49-50.

[2]李存璐. 大数据时代计算机网络安全防范应用与运行[J]. 电大理工, 2019, 278(1):16-18.

[3]顾文斌. 浅析大数据时代下的计算机网络安全防范[J]. 科学与信息化, 2019(13):42-42.

[4]王振雄. 大数据时代的计算机网络安全及防范措施[J]. 数字通信世界, 2019(4):264-264.

[5]刘建清. 大数据时代的计算机网络安全及防范策略的分析[J]. 信息与电脑(理论版), 2019, 425(7):195-196.

[6]赵明藻. 大数据时代的计算机网络安全及防范策略的相关研究[J]. 科技风, 2019(9):72-72.