

# 大数据背景下计算机网络信息安全问题研究

童俊儒

(杭州电子科技大学 浙江 杭州 310000)

**[摘要]** 大数据体系的建设下, 计算机网络运行效率极大提升, 方便人们对信息的获取与辨识。基于此, 文章以大数据为切入点, 指出计算机网络信息安全存在的问题, 并对防护对策进行研究。

**[关键词]** 大数据 计算机网络信息安全问题

**【DOI】** 10.12252/j.issn.2096-6261.2021.03.105

## 引言

大数据时代的到来下, 提高计算机网络的运行质量, 通过对数据信息的高效处理, 满足企业及用户的个性化网络服务诉求, 进而提高整体数据处理质量, 推动数字化经济的发展。但是在计算机网络为各项处理事物带来便利的同时, 也存在严重的信息安全漏洞问题, 造成用户及企业内部信息的丢失, 影响社会稳定发展。本文则是针对计算机网络信息安全问题进行探讨, 仅供参考。

## 一、大数据概述

大数据技术在具体实践时, 其是通过作用于数据信息本体上实现处理、运算、传输等功能。对于计算机网络而言, 通过大数据可进一步拓宽信息传输路径, 保证在同一时间节点下对不同类型的数据进行处理, 强化数据信息传输效率。对于现阶段海量数据增长趋势而言, 可以真正契合到用户日常生活工作中, 满足人们对数据信息的获取及处理诉求, 为相关决策功能提供数据支撑。从长远发展角度而言, 大数据时代的到来下, 进一步加快数字化体系的完善进程, 令人们工作及生活方式形成质的突破, 同时也对社会经济稳定发展起到重要的促进效用。

## 二、大数据时代下计算机网络信息安全问题

大数据时代到来下, 令用户各项信息呈现出一定的透明性, 而此类机制作用于计算机网络系统时效性、共享性传输功能之上, 将令用户无隐私可言, 这就造成数据信息, 在传输过程中一旦价值类的信息被盗取时, 将令用户造成严重的经济损失。从现阶段计算机网络信息安全所产生的动因来讲, 大体可分为人员操作及计算机系统两方面, 第一, 在人员意识操作, 如果用户并不具备专业的计算机操作技能, 在获取某一类信息时, 通过不规范的操作行为, 将产生基于互联网开放式平台的数据泄漏现象, 从而为不法人员对计算机的侵入及信息到盗取提供路径, 在一定程度上, 影响着计算机网络的安全性。第二, 在计算机内部环境中, 主要由于计算机软件或者是病毒黑客等攻击行为所产生的信息丢失与被盗取的风险。例如黑客及病毒在侵入计算机系统时, 其所形成的定向化攻击特点、潜伏性特点、蔓延性特点等, 将对计算机软件系统造成不可修复的损坏, 且可通过依附于数据信息实现在计算机网络下的传输运行进而造成系统崩溃、文件丢失的现象。对于计算机软件来讲, 其在研发过程中需要留有可更新的插件及拓展接口, 这就意味着系统软件存在一定的漏洞问题, 为非法人员侵入软件提供可乘之机, 加大系统安全问题的产生概率。

## 三、大数据下计算机网络信息安全防护对策

### (一) 加强网络安全教育

近年来, 我国网民数量呈现出直线性上涨的趋势, 这就造成网民在上网过程中, 因为自身操作度不足而引发的数据安全风险。为此, 必须正视网络安全教育对于计算机用户所带来的约束与引导, 结合计算机网络运行环境与用户当前

的操作行为, 制定出可行性、科学性的安全教育方案, 利用互联网共享性、时效性的信息传输模式, 对人员进行全方位的教育普及, 以提高计算机用户的操作意识, 保证各类计算机操作行为是符合计算机网络安全运行的。除此之外, 可以搭载大型社交平台, 例如微信平台、微博平台等向人们传达网络安全知识, 令人们深刻认识到计算机网络安全操作时具备的重要价值, 在实际操作过程中降低自身隐秘信息的泄漏风险, 提高计算机网络运行能力。

### (二) 加大计算机网络信息安全管理力度

在法律制度的逐步完善下, 计算机网络中所产生的安全问题已经完全纳入法律体系内, 令计算机网络不再是以一个法外之地的形式呈现在大众视野中, 而是通过法律规范制度与计算机用户的日常操作行为相连接, 构筑出一个更为完整的计算机网络安全监测体系。但是, 此类管控工作的落实仅限于基础类技术方面, 对于专业型技术难以实现有效约束。为此, 必须进一步提高计算机网络信息管理力度, 按照部门所具备的职能属性深化实际管理效应, 保证每一项管理任务可以落实到职能人员身上, 进而从根本上提高网络安全监管质量, 为计算机用户构筑一个安全上网环境。

### (三) 防火墙技术的应用

防火墙是指在计算机系统内部及外部网络环境之间, 建设一个基于信息识别的防护体系, 即可有效甄别外界环境中信息是否存在病毒或者非法入侵行为。如果用户指令操作下的数据信息存在安全风险时, 防火墙技术将自动识别信息, 阻止此类信息进入到计算机系统中, 并跳出弹窗对计算机用户起到警示作用。为此, 必须进一步加大对防火墙技术的应用力度, 定期对防火墙系统进行更新处理, 有效对实时更新的病毒及黑客攻击行为进行数据更新, 对新型病毒及黑客攻击手段进行立体化防护, 提高计算机网络运行安全性。

## 结语

综上所述, 大数据支撑下的计算机网络体系在运行过程中, 将提高信息传输效率, 为用户及企业的规划发展提供数据支持。为此, 必须加大对计算机网络环境的检测力度, 结合管理机制、技术体系, 构筑全方位的管控策略, 提高计算机网络的安全性能。

## 参考文献

- [1] 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(04): 118-119.
- [2] 张映勇. 计算机网络信息安全管理系统面临的问题探讨[J]. 江苏通信, 2021, 37(02): 110-111.
- [3] 李小康. 大数据技术在计算机网络信息安全问题中的应用探析[J]. 无线互联科技, 2021, 18(07): 86-87.

## 作者简介:

童俊儒(1991.01), 男 汉族 浙江杭州人 学士, 从事信息安全、软件可靠性研究。