大数据背景下计算机网络安全与防护研究

王 云

四川职业技术学院 四川遂宁

【摘要】计算机网络与民众生活、社会生产关系密切，是推动社会建设发展的重要力量。计算机和互联网快速发展，打破了空间与时间的界限，使人们可以通过网络平台快速的获取信息，进行无障碍的交流。计算机网络虽然能为大众带来便利，也存在一定隐患，可能出现信息泄露的问题，不利于工作个人隐私的保护。本文立足大数据背景，对计算机网络的使用情况进行分析，梳理计算机网络安全问题并寻找引发问题的原因，给出计算机网络安全防范的可行手段，希望可以为我国计算机网络安全等级提升有所贡献。

【关键词】大数据；计算机；网络安全；安全监管

【收稿日期】2023 年 1 月 26 日 【出刊日期】2023 年 3 月 21 日 【DOI】10.12208/j.aics.20230016

Esearch on computer network security and protection under the background of big data

Yun Wang

Sichuan Vocational and Technical College, Suining, Sichuan

【**Abstract**】Computer network is closely related to people's life and social production, and is an important force to promote social construction and development. Although the computer network can bring convenience to the public, there are certain hidden dangers, information leakage may occur, is not conducive to the protection of personal privacy. This article, based on the big data background, analyzes the use of computer network, combs through computer network security problems and looks for the causes of problems, presents feasible methods of computer network security prevention, hoping to contribute to our country's computer network security level enhancement.

【**Keywords**】Big data; Computer; Network security; Safety supervision

在计算机网络的使用中，大数据技术发挥不小的作用，可以实现信息的大量传输、存储、分析，但也增加计算机网络结构的复杂性，可能在计算机网络运行时出现不少安全问题。容易出现网络诈骗、用户信息被盗的情况，导致用户在计算机网络使用中出现较大的不安感，担心数据被盗。做好计算机网络安全的维护，需要分析大数据背景下计算机网络的环境，针对常见的网络安全问题，寻找该情况出现的原因，立足实际给出可靠的防护方法，从而在公众使用计算机网络时，成功规避信息被盗取的安全问题。

1 大数据背景下计算机网络环境分析

在大数据背景下，计算机网络得到进一步发展，支持用户进行海量信息的传输、存储，还能通过技术手段快速分析数据，从数据中找到有价值的内容。在技术支撑下计算机网络的整体水平得到提升，数据处理能力出现飞跃，主要体现在海量信息处理质量与工作效率。在互联网网民增多的过程中，计算机网络每时每刻均会出现不少数据，在数据运行时对计算机网络安全管理施加一定压力，增加数据出现隐患的概率，也为安全管控提出不小的挑战。在计算机网络使用中，考虑到大数据带来的变化，使网络环境变得异常复杂，信息真实性在辨别方面难度变大。计算机用户行为操作不当或黑客入侵，均可能导致计算机内部数据泄露，损害到用户的权益[1]。

2 大数据背景下计算机网络常见的安全问题

2.1 黑客入侵

计算机网络作为用户传输信息的载体，在网络平台有不少信息资料，信息资源是企业经济收益与发展的基础，所以部分不法之徒会采用技术手段，攻击计算机网络，试图盗取其中的信息资源牟利。计算机网

络安全问题中，黑客入侵占比较大，其中可以细分为黑客被动入侵与主动入侵。黑客被动侵入是指黑客入侵用户计算机网络，破解用户数据信息并进行数据截取，在用户不知情情况下完成系统入侵操作。用户在计算机使用中并没有察觉到异常，此时用户可以正常操作计算机。黑客入侵用户计算机网络可以使用技术手段，对安全防火墙进行设置（图 1 为防火墙示意图），在不触动网页防篡改预警机制的条件下，完成入侵动作。黑客主动入侵针对性、目的性较强，黑客根据自己的目标使用技术手段攻击用户计算机，用户在计算机网络使用中，可以察觉到黑客攻击行为并会被黑客以一定的方式盗取或篡改计算机内的数据，还可能因黑客攻击行为导致计算机瘫痪。

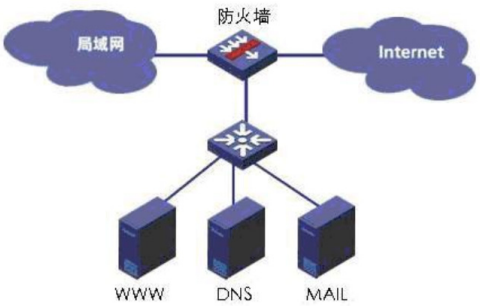

图 1 防火墙示意图

2.2 木马病毒

计算机网络使用中，木马病毒属于常见的安全问题。木马入侵计算机一般存在潜伏期，潜伏期中用户使用计算机并不会受到影响，同时很难察觉到病毒入侵计算机网络。在一段时间后，木马病毒启动对计算机系统造成破坏，用户不能正常操作，会出现信息被盗的问题。在计算机网络发展中出现很多木马病毒，一部分木马病毒对计算机系统的攻击性较强，引发的后果也极为严重，在计算机网络发展期间，木马病毒更新速度较快，大部分病毒查杀软件对新出现的木马防御能力较弱，无法发现木马病毒或发现木马病毒却不能进行有效的防御，导致木马病毒在计算机网络中大肆传播，出现大规模用户信息被盗的情况。我国病毒查杀软件的更新速度与木马病毒的发展速度不同步，病毒查杀软件滞后性明显，对于新出现的病毒处理能力较弱[2]。

2.3 计算机系统漏洞

计算机网络在运行时被黑客盗取信息，有一部分因素是系统存在漏洞，所以防护能力较弱。用户在计算机使用中，系统网络需要定期更新，修补系统存在的漏洞，保证计算机在使用时不会被他人攻破，盗取其中信息。然而，很多用户缺乏专业知识且不具备计算机网络安全意识，在日常操作计算机时，不注意安全防护，即便出现安全漏洞也没有及时进行修复。系统存在漏洞，计算机在运行时存在较大的安全隐患，难以保证数据在计算机运行中不会出现被盗或被篡改的情况。

3 计算机网络安全问题出现的原因

3.1 安全防范技术运用不足

计算机网络的用户群庞大，必须在网络运转中做好安全防护工作。在计算机网络发展中出现不少安全防范技术，杀毒软件防火墙是大众耳熟能详的安全防范技术，在计算机网络使用中进行安全防范工作，可能遇到杀毒软件与防火墙无法兼容的情况。部分主体根据自身使用需要放弃防火墙，将杀毒软件作为安全防护的主要手段，但因杀毒软件自身对木马病毒筛查的局限性，无法做好病毒的鉴别与防护，可能为黑客入侵用户计算机网络提供可乘之机[3]。

3.2 安全监管不到位

计算机网络安全管理涉及的环节多、范围广，在安全管理时操作难度较大，可能因安全监管不足，出现数据被盗的问题。很多人在计算机网络安全监管时，因安全意识不足，对网络安全监管认识不到位，使计算机用户很难参与到网络安全监管中。在计算机网络安全监管时，大数据技术拥有较好的作用，但因相关主体专业技术不足，无法根据网络安全防护需求，合理使用大数据技术，在安全监管方面处于弱势。在计算机网络安全监管阶段，法律法规和监管制度并不完善，无法基于实际情况做好安全监督管控工作，容易在计算机网络运行时出现安全问题。

3.3 用户操作不规范

在计算机网络运行中，如果用户操作不规范可能引出安全问题。用户使用计算机因对专业知识掌握不足，可能做出降低计算机安全防护能力的行为，比如部分主体为增加计算机存储空间卸载杀毒软件，或者在杀毒软件安装时仅考虑软件占用的大小，没有基于安全防护需求进行合理选择。还有部分用户在安装杀毒软件时，不理会杀毒软件给出的风险提示信息，由此埋下安全隐患[4]。

4 大数据背景下计算机网络安全防范的实施策略

4.1 宣传计算机网络安全知识

在大数据背景下，计算机网络使用人群变多，计算机网络安全工作应该得到全体用户的支持，并参与到计算机网络安全防护的活动中，提高计算机网络运行的稳定性与安全性。网络安全部门需要积极推进网络环境净化工作，在计算机网络安全管控中，以网络安全宣传作为主要手段，相关部门应该发挥自身具备的优势，在社会面宣传计算机网络安全内容，向公众说明计算机网络在使用中出现的黑客入侵、木马病毒传播、计算机网络系统漏洞等安全类问题，使用简洁易懂的方式对安全问题进行阐述，说明引发安全问题的原因，还会告知计算机用户做好安全防范工作。比如，在日常使用计算机网络时，选择数据加密方式或设置用户密码（图 2 数据加密示意图），使用相对复杂的密码，增加黑客在密码破译时的难度。计算机用户需要拥有较强的安全防护意识，不要随意接入网络，由此提高个人信息防护的安全等级，不会轻易出现信息泄露的情况[5]。

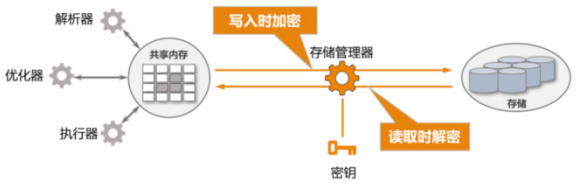

图 2 数据加密示意图

4.2 推广先进的计算机网络安全防范技术

在计算机网络安全防护中，有必要开展安全防护工作，使用先进的技术手段，提高计算机网络运行时的安全等级。在计算机网络安全防护领域出现不少技术，比如身份识别技术、安全漏洞扫描技术、防火墙等，需要在安全防护方面基于数据使用安全需求，定期对安全防护技术进行升级，还可以选择组合方式，将安全防护技术按照防护能力进行合理编排，从而通过多种安全防护技术的组合使用，提高计算机在黑客防御病毒查杀中的能力，防止信息外漏。在计算机网络安全防范中，防火墙是基础且重要的措施，可以将控制器、交换器与互联网隔绝开来，在计算机网络使用中过滤互联网信息，避免计算机终端用户在网络使用期间出现数据被盗的情况。

为提高对病毒或其他危险因素的监测能力，针对现有木马病毒类型，结合安全防护需要扩大扫描范围。在安全管控中，重新设定计算机网络安全漏洞的扫描标准，打造准确、高效的计算机网络安全漏洞扫描规则，可以快速发现漏洞并进行修复。在计算机网络运行中，进行全面监测，快速发现有问题的数据并进行拦截，剩余数据即便存在病毒，也可以通过服务器防御，最后经由网关将信息传递到内部网络。在网关、防御服务器多重阻隔下，及时发现病毒并进行处理，避免信息在传递时携带病毒。在数据安全监测与防御中，可以及时删除存在问题的内容，对监测数据进行合理控制，提高网络安全防护水平。

4.3 加大计算机网络安全监管力度

计算机网络运行时进行安全管控，根据安全防护需要建立监管制度，以规范的流程进行控制。对于企事业单位在网络安全管控中，需要选择科学的方法，加大计算机网络安全监管力度，可以及时锁定计算机网络存在的危险因素，以有效的方式进行处理，提高计算机网络在使用中的安全性。在计算机网络安全管控中，应该对各类企业的工作人员进行安全宣传教育，使用真实案例说明计算机网络常见的安全问题，根据案例出现的问题进行剖析。比如，向企事业单位的工作人员展现具体案例，使其认识到引发计算机网络问题的根源性原因，在日常使用网络时做好防护，避免出现系统被攻破的情况。在计算机网络使用中，分析计算机网络安全防御的能力，确定计算机网络安全特点，立足计算机网络安全防范技术发展情况，给出计算机网络安全监管制度的设定要求，完善制度内容。在安全制度运行中，做好计算机网络安全防范工作。在计算机网络安全监管时，需要明确计算机应用规范，全面升级计算机系统，定期修补系统漏洞，提高计算机运行时安全防护能力，防止出现信息丢失的情况。

4.4 规范用户操作行为

用户是否拥有充足的计算机操作知识，关系到计算机网络使用中的安全性，应该对计算机网络操作主体的行为进行规范。采取网络宣传、标语宣传等多样化的手段，让计算机网络操作知识可以在社会面广泛传播，提高用户对计算机网络使用的认知程度。用户学习网络安全知识，知晓计算机网络使用中应该进行的行为，对过往错误的操作方式进行纠正，可以在计算机使用中通过更加规范的方式，避免因人为因素引起系统故障。用户安全防护认知提升后，在日常操作中关注计算机网络安全防护，定期修补系统漏洞，挑选病毒查杀能力较强的杀毒软件，不会随意点开网页。在社会面发布计算机网络操作指南，根据计算机网络

安全防护需求，给出科学的设计方案，提高计算机网络操作指南内容的合理性、全面性与科学性。在内容设计时，需要获取计算机网络用户的操作习惯和使用需求，保证操作指南内容简洁易懂，可以被用户快速消化吸收，并能按照其中给出的安全防范内容进行操作。用户以规范的手段操作计算机，不会在计算机网络使用中出现系统被攻破、数据被窃取的情况。

5 结语

在大数据背景下，计算机网络的使用量进一步攀升。在用户使用计算机网络时，不仅需要看到计算机网络使用的条件，还需要针对计算机网络在信息安全方面的隐患，做好防护工作。对现阶段网络安全问题进行梳理，针对黑客入侵木马病毒、计算机系统漏洞等问题，查找计算机网络安全问题出现的原因，根据获得的信息进行计算机网络安全宣传，推广计算机网络安全防范技术，加大计算机网络安全监管力度，规范用户操作行为。在相关举措下，计算机网络安全等级得到提升，用户在计算机网络使用中，可以达到自己的操作目的，同时不会出现用户信息被盗或被篡改的情况。

参考文献

[1] 卞其翀.基于大数据背景的计算机网络信息安全与防护探讨[J].信息记录材料,2021,22(06):20-22.

[2] 丁萍,丁旭东.大数据背景下计算机网络安全与防护研究[J].网络安全技术与应用,2021(03):152-153.

[3] 马基英.大数据视角下计算机网络信息安全与防护策略研究[J].智慧中国,2020(10):85-86.

[4] 任鼎.浅析大数据背景下计算机网络信息安全与防护[J].数码世界,2020(08):257-258.

[5] 范玉霞.大数据环境下计算机网络安全与防护策略研究[J].信息记录材料,2020,21(07):223-224.