计算机网络信息安全在大数据下的防护措施探究

唐　超
广州科技职业技术大学 广东 广州　510800

【摘　要】计算机技术的出现改变了人们生活习惯和方式，人们足不出户便可知晓天下事，在提升工作效率、信息传播、娱乐生活等方面发挥着积极作用。但计算机技术是把双刃剑，在促进社会进步的同时带来了网络信息安全隐患，网络上的用户个人信息存在被非法利用的情况，人们的隐私权受到了极大威胁。尤其是在大数据不断发展背景下，用户任何网络足迹都能成为不法分子获取利益的来源。为了促进计算机技术的稳定、长久发展，相关部门有必要对网络信息安全做好充足防护,保护网民合法权益。因此,本文在阐述影响计算机网络信息安全因素基础上,从多方角度提出做好网络信息防护的措施,希望其能维护良好网络环境。

【关键词】网络信息安全；大数据；防护措施

随着我国科学技术的不断蓬勃发展，计算机技术得到了显著提高,我国网民的数量也逐年呈上升趋势。可见，计算机技术已经逐渐渗透至人们的日常生活，不断改变着人们的生活和娱乐方式，为人们生活和工作提供了诸多便利。人们在享受计算机技术带来的便利同时，个人隐私信息也面临着被非法泄漏、被利用的威胁。计算机网络中的诸多不安全因素值得我们进行深入研究，并制定行之有效的网络信息安全措施给予解决，最大程度降低计算机网络信息安全事件的发生。

一、影响计算机网络信息安全的因素

1. 计算机硬件客观因素

计算机上的信息是依靠硬盘进行存储的，信息的安全程度由硬盘信息保护程度决定[1]。从目前的计算机硬件研究进程来看，硬盘普遍不具备自我保护能力，一旦受到停电、自然灾害、外界损坏等情况，计算机中的网络信息和数据就会丢失。计算机硬件因素是影响计算机网络信息安全的非主观因素，需要在硬盘存储技术进步的基础上才能解决。比如，当网民在互联网登陆个人相关的账号、密码信息时，如若出现停电、意外事故等情况，网络上的信息便不会得到保存，甚至在上述突发情况下网民信息会出现被不法分子盗取的情况。因此，计算机硬件因素带来的信息安全风险仍然值得重视，对计算机硬件信息保护技术的研发是必要的。

2. 黑客技术威胁

互联网最大的特点就是开放性和包容性，这正是因为其开放和包容给予了黑客盗取信息的机会。在我国，绝大部分系统网络采用 IP 协议，此种协议的安全性是较低的、黑客进入互联网途径是容易的。一些数据服务器较为集中且包含大量信息数据，这类服务器更容易被黑客攻击，重要信息容易出现被盗取、被篡改的情况。黑客对数据服务器的入侵主要受到利益趋势，很多黑客为了个人利益自主或者受他人委托对一些服务器进行攻击，从而盗取行业内、企业内重要数据信息，损害了整个互联网环境的健康、和谐，损害了相关主体的合法权益。可见，黑客技术是影响计算机网络信息安全的又一重要因素。为了防止黑客技术的入侵，国家监管部门应加强对黑客行为的立法和打击，借助法律手段强制打击黑客行为。

3. 计算机病毒

如今是大数据时代，互联网上的网页信息、链接信息呈爆炸式增长，如何在海量信息中发现并处理计算机病毒是较为困难的事情[2]。计算机病毒往往借助链接、软件等载体入侵计算机，并以极为隐蔽的身份藏匿于计算机系统中，当计算机使用者处理重要信息时记录这些重要信息，待时机成熟窃取这些信息让计算机使用者毫无防备。同时，计算机病毒还极具破坏性，借助程序可以实现病毒的海量复制和传播从而攻击计算机原有的软件和数据信息，甚至会造成信息永久丢失的后果。可见，计算机病毒也是威胁网络信息安全的重要因素。计算机病毒的防治需要监管部门加强对信息发布的监管，更需要网民自身的信息保护意识，做到不轻易点击不明链接、不轻易下载盗版软件。

二、做好计算机网络信息安全的防护措施

1. 加强计算机硬件设施建设，保证存储信息安全

为了降低计算机硬件问题对信息安全的影响，在对计算机硬盘进行设计时应开发硬盘的自动存储功能，使计算机在遇到不可抗因素时也能帮助使用者保存信息[3]。为了实现这一目标，可以应用硬盘数据管理系统，对硬盘存储的信息进行分布式管理，对相关重要信息可以进行多层保护和监测，提高关键信息的安全性。分布式数据管理系统的应用既能够解决非主观因素造成的信息泄漏问题，还能够在一定程度上防止黑客入侵，提高信息存储的安全性。计算机硬件设施建设需要国家科技部门进行支持和研发，提升计算机硬件对信息的存储和安全保护功能，降低非主观因素对网民信息的威胁和影响。

2. 做好网络信息安全监管，借助法律法规实施

我国网络信息监管部门作为政府重要的职能部门，应重视对网络环境的治理和监管，对网络上的不法行为进行有预防的检测和治理，而不是当违法行为发生后进行管理和惩戒[4]。因此，网络信息监管部门应充分发挥自身职责，按照法律法规要求进行执法，对威胁网络信息安全的行为给予严厉打击，通过建设网络细腻安全监

管系统的方式完成对网络行为的监管，一旦出现黑客入侵、计算机病毒传播事件的发生应重拳出击、绝不手软。从现实情况来看，我国网络信息监管部门的人才构成不科学，缺乏专业性的高素质人才，一些原有的非专业人员对网络信息发展的敏感度和重视度不足，很难及时打击网络违法犯罪行为。为此，网络信息监管部门应加大对信息人才的引进力度，优化监管团队构成，实现监管能力提升。

3. 更新信息安全防护技术，保护个人信息安全

除了监管部门外，网络信息提供商也应具备信息安全意识[5]。网络信息提供商是信息流入广大互联网世界的关卡之一，如若其对网络信息的甄别和管理能力不足，便会加大网络信息安全事件的发生概率。因此，网络信息提供商应加大对信息安全防护技术的利用，有效保护网民个人隐私信息，防止其信息被泄漏、被攻击。以数据加密技术为例，网络信息提供商可以将包含海量用户的信息数据库进行加密处理，利用公匙加密路径保护用户整体信息、利用私匙加密路径保护用户个人信息，进一步保证信息的安全性。随着大数据技术的不断发展，依靠账号和密码进行登陆的方式安全性逐渐降低，为此网络信息提供商可以借助生物特征身份验证技术对用户登陆进行限制，加强用户个人登陆的安全性，降低信息被盗取事件的发生可能性。

4. 提高个人安全防护意识，做到日常防火和消杀

在大数据时代，人人都有麦克风，人人都是网络信息传播活动的主要参与主体[6]。为了有效杜绝网络信息安全事件的发生，个人应与网络信息监管部门、网络信息提供商等多方共同努力，在里外良好配合的情况保障网络信息的安全程度。为此，个人首先应提高自身安全防护意识，不主动点击不安全的网络链接、不主动下载不明来源的软件，不给黑客和病毒的入侵提供机会。其次，个人应为保护网络信息安全作出行动，提高防火墙应用意识，可以利用购买的方式加强计算机的防火等级，进一步打击黑客和病毒的入侵。同时，用户个人还应对计算机进行定期的软件杀毒工作，消除软件内隐匿的潜在病毒，既减轻了计算机负担又清除了危险因素。在个人、监管部门等多个主体努力下，网络信息安全能够得到有效保障，从而为网民营造和谐、健康的上网环境。

三、结束语

在大数据时代背景下，互联网成为人们与外界沟通、获得外界信息的重要渠道，互联网走进了越来越多民众的日常生活中。近几年，网络信息安全事件频发，不论是网络监管部门还是网民个人都应重视网络信息安全问题。为了维护健康、安全的网络信息生态环境，需要计算机开发商、监管部门和个人的共同努力。首先，应加强计算机硬件设备建设，实现存储信息的相对安全。其次，网络监管部门应做好信息监管工作，借助法律手段打击各种违法、犯罪行为。此外，技术部门应加强对网络信息安全保护技术的研发，实现个人隐私信息的保护。最后，网民个人应提高安全防护意识，定期对提高个人计算机防火等级、并进行病毒消杀。

参考文献：

[1] 赵振宇 . 大数据背景下的计算机网络信息安全及防护措施 [J]. 电子技术与软件工程 ,2021(11):249-250.

[2] 曹仰之 . 基于大数据的计算机网络信息安全防护措施研究 [J]. 电脑编程技巧与维护 ,2021(05):167-168.

[3] 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.

[4] 张晓伟 . 大数据背景下的计算机网络信息安全及防护措施 [J]. 数字技术与应用 ,2021,39(03):162-164.

[5] 李成 . 在大数据时代下计算机网络信息安全问题及其防护措施 [J]. 数码世界 ,2019(10):79-80.

[6] 刘锋 . 大数据时代计算机网络信息安全与防护措施 [J]. 山西青年 ,2019(14):189.

作者简介：姓名：唐超，出生：1974，性别：男，民族：汉族，籍贯：湖南衡阳，学历：硕士，职称：高级工程师，研究方向：大数据及信息安全