大数据时代的计算机网络安全及防范措施思考

田永民
湖南大众传媒职业技术学院　湖南长沙　410100

[摘　要] 近年来，计算机信息技术在不断地发展，正日益改变社会的生产生活方式，人类也由此逐渐迈入了大数据时代。在信息高速发达的环境下，大数据被广泛运用于社会生产生活的方方面面，一方面给人们生活生产带来巨大的便利，也给企业、社会带来巨大的经济效益和财富积累；但在另一方面，信息的高速膨胀，个人信息严重泄露，促使网络安全岌岌可危，不少不法分子通过网络利用信息非法传播来谋取私利，构成大量的网络犯罪行为，对人们的安全造成巨大威胁。因此，加强网络安全防护，维护信息安全是重中之重。笔者就大数据时代下的计算机网络安全问题作出浅显分析，并提出防范措施。

[关键词] 大数据时代；计算机网络安全；防范措施

引言

大数据时代的发展是以信息技术的进步为前提的，信息技术的不断发展促使人们的生产生活方式发生巨大的转变，给人们的生活提供了巨大的便利；同时也使得大数据得以充分发挥其作用，被广泛运用在社会的各个领域，特别是企业在生产经营中依据大数据分析、挖掘潜在客户，获得收益。大数据作为一项重要的数据资产，为社会政治、经济与文化生活的发展提供了关键性的助力，给计算机网络的高效运行提供数据支持。但在计算机网络高速发展的时代，这些也将会带来一系列的安全隐患，威胁网络安全。因此，在大数据时代的前提下，应当高度重视计算机网络的环境维护，着力完善计算机网络信息安全管理系统，促进信息时代的高效、安全发展。

1 大数据的定义

大数据从表层含义来看就是巨大的数据流，并且其内容呈现出多元化的数据集合，多指计算机网络中的海量数据。计算机通过云计算对数据进行处理分析。整合的大数据综合了各种数据来源，具有一定的综合性和多样性，借用此特征的计算机网络会更加高效便捷处理问题。大数据存在的海量的数据规模、快速的数据流转和多样的数据类型以及价值密度低的重要特点都促使其被运用在各类信息行业中，改变了人们传统的思维方式和处理手段。随着时代的发展，大数据作为一项重要资源也被提升到国家战略化发展的层面。

2 大数据时代的特点

2.1 海量的数据资源

大数据最基础的数据特点就是它一项具有多元化的数据资产，其内容丰富多样，蕴含生活的方方面面。它通过互联网传播，经过云计算整合形成，数据存储单位也随之发生改变，如从最开始的 MB、GB 至 TB、PB、EP 都在昭示数据信息呈现出爆炸式增长。其数据存储类型也多种多样，如图片、文字、音频、视频等。在计算机网络时代，人们的生产生活已然离不开网络世界，这也为大数据的更新和发展提供信息来源，同时，在更新和发展的大数据中，各行各业也挖掘出所需要的信息资源，通过数据的整合再利用，促进其自身发展。

2.2 大数据的广泛运用

在大数据时代，计算机网络技术高速发展，促使社会信息资源逐渐公开化，实现共享，打破了时间、空间上的局限性。大数据通过网络、服务端等方式传播，最终被运用在各个领域。人们在做重大决策的时候，往往会以数据为依托，分析其潜在发展可能性。特别是在新兴行业的发展，如电子商务、共享经济等，多借用大数据技术，分析各项指标，科学研究，提高生产、运营效率。如淘宝运营商多运用后台数据分析，发觉店铺浏览量和潜在客户、作出相应的战略调整，以此提高店铺的曝光度，吸引顾客，从而获得收益。可见大数据对生产生活的广泛影响。

2.3 大数据时代的网络安全

大数据时代给社会带来巨大的经济效益和社会红利，也促使大数据技术的高速发展。但与此同时，大数据的来源复杂多样，传统的计算机网络安全维护已经跟不上信息膨胀的速度，无法快速高效辨别信息的真伪安全，导致网络安全存在巨大的隐患。且信息膨胀带来信息维护成本增加，技术要求高，加大了维护难度。本身计算机网络系统存在一定的技术漏洞，经常会出现黑客入侵、系统瘫痪、病毒席卷的情况。因此，大数据时代的网络安全存在一定风险。

3 大数据时代下的计算机网络安全风险分析

3.1 计算机系统本身存在的漏洞

计算机网络在开发中必然会存在一定的漏洞。技术人员在开发系统时不可能完全预知系统的运行和发展走向，并推测出存在的诸多问题，因此，当系统投入市场运行后，漏洞出现，技术人员可对漏洞进行修复，完成软件的更新；同时，系统在下载安装的过程中也会夹带某些漏洞，甚至浏览网页、下载资源时也会出现同样的问题，不少不法分子借系统漏洞，窃取用户隐私，对信息安全造成严重威胁。另一方面，软件的个性化升级也会扩大漏洞存在的可能性，个性化的服务满足各类网络用户的需求，同时也会增加技术的难度，这要求技术人员对不同客户群体作出不同的导向，加重了软件开发和维护的难度，使得黑客得此趁机入侵。除此之外计算机硬件、软件遭到破坏，信息也会流失，个人信息完全易受到威胁。

3.2 网络用户隐私防范意识较差

在计算机网络使用中，网络用户的隐私常常存在被盗取的现象，一方面是由于用户自身隐私防范意识较差，不能很好的做到自我防护。例如在网站上登录个人信息时，使用简单容易猜出的密码，如个人生日或简单的数字等等，或是多个账号同一个密码的情况，都会容易被网络上不法分子窃取资料信息，造成隐私泄露的问题。同时，由于大数据技术的高速发展，人们在网络上浏览的路径都会得以保存，如登录地显示、浏览器记录、定位系统以及个人账号管理等，使得个人隐私难以被控制，造成安全隐患。日常的生活信息被网络化，形成数据资源造成泄漏，对个人隐私、社会安全都造成严重的威胁。

3.3 网络用户操作不当

计算机网络发展迅速，如今人们的生活已经逐渐离不开网络，但是由于网络用户的素质差异较大，对于计算机网络运用的水平也大有不同。许多人在使用计算机时，个人判断力不足，往往因操作不当造成信息泄露，例如点开匿名连接、随意下载不明软件等或是陷入网络不法分子的圈套受其指引上当受骗，这些不经意的行为都会造成安全隐患，为非法侵入埋下伏笔。

3.4 网络管理制度不健全

在计算机网络时代，人们通常会在网络上留下踪迹，例如在某些网站绑定银行卡，登录微信账号，手机号，登录个人资料等等，都会存入大数据中。但由于网络管理制度不健全，管理制度不规范，许多后台工作者利用搜集到的后台数据，进行二次非法销售，造成个人信息泄露，甚至存在银行卡盗刷等现象，对个人隐私和财产安全造成重大威胁。

3.5 计算机病毒入侵危害

在下载和使用计算机软件的过程中，都或多或少会有病毒入侵。随着计算机技术的发展，对于程序员的技术水平要求也越来越高，但与此同时，黑客的技术水平也随之提高，反侦查能力与日俱增，导致许多病毒在入侵软件时并未被及时的发现，最终造成系统崩溃，数据泄露，信息流失。

3.6 大量钓鱼网站的存在

在计算机网络的发展中，最为常见的变化就是人们越来越依赖网络购物，各种网购软件的兴起。人们登录时留下的信息如手机号码、身份证信息、银行卡账户等等都存储于大数据中，但由于网络管制不严，存在漏洞，不法分子利用购物连接导致银行卡误刷，财产流失；还有不法分子盗用账号，利用网络用户的名义进行诈骗。这些网站的存在，导致不少网络用户在记录自身账号信息时得不到安全保障，从而造成一定的财产损失。

3.7 信息传播层面存在的安全隐患

在网络信息传播的过程中也存在较大的安全隐患，计算机网络信息传播的方式主要借助有线、无线等客户端及各类的通信协议进行的，在传播过程中，容易因各个通信商存在认知偏差或不协调的问题，造成安全漏洞，从而导致病毒攻击，在信息传播的过程中也携带病毒，造成及计算机网络安全损害。由于计算机网络的快速发展，信息具有较大的自由传播度，这会加深安全隐患，构成网络安全威胁。

4 大数据时代下计算机网络安全防御措施

4.1 提高网络技术人员的技术水平

在软件开发和运行中常存在漏洞的现象，使得黑客顺利入侵，造成网络安全损伤。因此，应当加强网络技术人员的技术水平，培养网络尖端人才，在开发软件时做好软件的试运营工作，能够对软件的发展有一定的可预测性，构建防黑客入侵的反攻系统保护软件安全，同时出现问题时能够第一时间修复漏洞，完善系统安全的紧密度，避免系统因自身不完善而导致用户隐私安全泄露等问题的出现。优秀的网络技术人员能够为网络安全提供一定的技术支持以及安全保障，对黑客入侵有强有力的防范作用。

4.2 加强网络用户安全意识

加强网络用户安全意识，避免由于自身轻视网络造成一定的隐私、财产安全损失。在登录系统账号密码时，尽量选取较为复杂的密码如数字和字母组合而成，且多账号多密码，不使用统一密码登录所有账户；在公共场所，尽量避免使用公共 WiFi，以防止个人信息泄露；在使用网站后，定期删除浏览记录和及时销毁不使用的账号，避免信息盗用。网络用户应提升好自身防范意识，加强个人网络安全能力，做好隐私维护。

4.3 提高网络用户的操作水平

对网络用户在计算机网络操作的时候，要及时提高自身的网络操作水平。学习网络基本操作，提升自己的技能，满足自身使用计算机网络的需求。如可以通过计算机网络学习课程进行培训学习，了解计算机知识，提高自己的操作能力；或通过亲朋好友的指导，掌握基本操作等等。通过学习能够及时对网络上的信息作出判断，不随意点开不明连接、下载不明软件，杜绝因自身操作不当导致失误，从而造成信息泄露。

4.4 完善网络安全管理制度

建立健全网络安全管理制度，对于恶意泄露他人信息，非法盗用、贩卖等网络诈骗行为进行严加管制，制定相应的法律制度、使用法律手段维护网络安全；同时也要提升网络安全管理工作人员的综合素质，重视网络安全，及时处理存在的安全隐患，不疏忽不懈怠自己的职责。

另外，应该做好网络安全道德宣传工作，鼓励人人做一个知法守法的网络用户。

4.5 加强安全防火墙技术，构建安全检测系统

重视对网络高端人才的培养，同时提升加强安全防火墙技术，必要时引进先进安全防御技术，从而提升我国计算机网络安全的防御能力。通过安全防火墙等技术和软件支持，构建一套有效的安全监测系统，对黑客入侵进行实时关注，对大数据进行一个有效的保护，促使计算机网络处于安全、高效、便捷的环境之中，防止外来病毒入侵。

网络用户应及时下载和使用最新的安全防火墙软件，定期对自身计算机进行清理和维护，从而对个人网络信息进行有效保护。

与此同时，针对大数据的存储应该构建一个安全且大容量的存储平台，使得海量数据能够被妥善安放，且备份用户信息，做好用户信息的安全维护。

4.6 严厉打击钓鱼网站，清除网络安全隐患

对于这类诈骗、信息盗用的钓鱼网站，个人用户一经发现就应当及时进行举报，不要因损失少量财产而认栽，要积极利用相关法律维护自身的利益；同时，相关的网络安全维护人员应当对网站进行定期的检测，一经发现，立刻封除。

4.7 处理好信息传播层面的问题

对于信息传播存在的问题，首先要做好各个通信商之间的协商与沟通，签订合理且明确的协议，为网络安全负担责任，同时通信商应该实时更新协议，跟上高速发展的数据时代，同时，通信商应对各类信息有一个较好的把控，防止各种垃圾信息的传播。

小结

在计算机网络高速发展的背景下，大数据也得以充分运用在社会生产生活的方方面面，特别是在金融、国防等领域，得到充分发挥。但是大数据在为社会带来便利的同时，也会带来巨大的安全隐患，给人们的生活造成损害。在面对当前计算机网络管理制度不健全、黑客入侵、技术人员水平层次不齐，网络用户操作不利等多种潜在安全隐患，应当做出及时的调整，利用法律手段保卫网络安全，提升技术人员的素质，建立有效的安全防御机制，提升网络用户个人素养等方式逐渐解决当前问题，保卫网络安全，促进大数据时代的高效、安全发展。

[参考文献]

[1] 张东光 . 分析大数据时代的计算机网络安全及防范对策 [J]. 时 代农机，2018,45(11):106.

[2] 周小健，鲁梁梁 . 大数据时代背景下计算机网络安全防范应用与运行 [J]. 网络安全技术与应用 ,2017(05):24.

[3] 曾生根 . 试谈大数据时代的计算机网络安全及防范措施 [J]. 中国 新通信，2017,19(22):66-67.

[4] 张勇 . 新时期下计算机网络信息安全问题及防范对策 [J]. 电子技术与软件工程 ,2017(19):213.

[5] 田言笑，施青松 . 试谈大数据时代的计算机网络安全及防范措施 [J]. 电脑编程技巧与维护 ,2016,12(10):90-92.