大数据背景下计算机网络安全及防范措施研究

赵中枢

（广东科技学院计算机学院，广东 东莞 523083）

摘 要 在当今社会之中，信息技术非常发达，在大数据科技发展的背景下网络安全越来越重要。有时候一些网络的黑客会窃取人们的重要数据，使得网络变得不安全，而相关的技术人员则需要做到维护网络安全，多寻找合适的维护网络安全的方案，使得计算机中的数据可以安全地留存下来，而不会有未知的隐患存在。本文主要探讨大数据背景下计算机网络安全及防范措施，旨在为相关人员提供参考。

关键词 大数据背景 计算机网络安全 网络黑客 木马病毒 防火墙

中图分类号：TP393.08 **文献标识码**：A **文章编号**：1007-0745(2022)11-0019-03

在大数据时代的社会背景下，IT 信息技术创新发展的同时渗透到社会的生产和生活的方方面面，能为人们提供优质、方便的服务，但这也在一定程度上为计算机网络安全埋下了新的隐患，一个小小的疏忽就可能导致巨大的损失。计算机网络存在着潜在的安全隐患，可能被不法分子所利用，从而窃取关键资料，危害社会的稳定发展。因此，在这样的情况下，网络安全就显得至关重要，只有网络安全了，人们的这些基本的日常活动的安全和人身安全才可以得到保障。以现有的网络环境为基础，利用大数据进行有效识别、发现和防范安全问题，保障数据安全可靠传输，既能满足人们的生产和生活需求，又能促进计算机网络的高质量发展。

1 影响网络安全的因素

1.1 计算机系统自身存在的安全漏洞

部分计算机的系统自身就存在着一些隐患，比如其中会有安全的漏洞。即使是一些比较完美的软件系统，也会存在着不安全的问题隐患，这些漏洞会给不法分子机会，让他们趁机入侵系统之中，窃取一些重要的文件或者是个人的信息，将这些信息拿去做违法的事情，从而造成网络的不安全。计算机是所有人在日常生活中都会使用到的，在计算机之中，软件系统是必不可少的，在长时间的使用之后，一些系统会有老化的现象，或者是系统没有及时地更新，这些都会导致网络不安全，使得重要的信息发生泄漏，让一部分人有比较大的损失产生。这些安全漏洞在平时没有信息被盗取时，可能不是那么引人注目，绝大部分的人都会忽略掉它，但是不可否认，这样的隐患漏洞是极其不安全的。

1.2 用户安全意识较差以及一些不安全的操作

部分用户的安全意识比较差，他们在使用计算机时，经常会有一些不规范的操作。比如他们会去点击一些陌生的链接，进入不安全的网站，或者是去扫描一些未知的二维码，这些情况在年老的或者是年幼的用户中发生的概率尤为大，这些用户的安全意识还不够强，相关的部门需要做好合理的宣传工作，让他们的安全意识提高，不要让不法分子有机可乘，让人们保护好自己的个人信息以及钱财，尽量避免不必要的损失。个别用户在不经意之间就进入了一些钓鱼网站或者是一些诈骗的群聊之中，从而被诈骗分子逮到机会，造成个人的损失，这些都是造成网络不安全的因素。

比如在商场之中会有一些不安全的二维码张贴，在这些二维码下面往往会有一些比较有诱惑性质的介绍，吸引没有防备的人上钩，然后这个二维码之中包含着的病毒或者是一些相关的不法网站就会乘机侵入扫描者的计算机系统之中，窃取相关的随意放置的资料，或者是重要的密码，这些都会威胁到人们的资金安全，乃至是人们的生命安全，从而影响到社会的稳定。因此相关的部门一定要加强宣传，提高人们的防范意识。一些网站是不良的网站，会有一些人有比较强的好奇心点进网站之中，从而使得自己的计算机系统瘫痪，信息外泄，资金大量损失。[1-3]

1.3 网络黑客的入侵

在网络上总是会有一些恶意满满的网络黑客在搞

破坏，他们随意地入侵个人的计算机，盗取别人重要的资料去获得自身的利益。有这些黑客的存在，即使网络系统比较完善，在网络上依旧是存在着比较大的安全隐患，而且这些隐患几乎是一直存在的，很难进行消除。这时候就需要人们的安全意识足够强大，尽量不要将一些重要的资料在网络上随意放置，在社交软件上也要减少对于自己相关信息的暴露，防止黑客对其进行不合法的利用。黑客为了达到自己的目的，会经常性地恶意入侵人们的计算机，对其中的软件进行攻击，从而使得计算机发生大面积的瘫痪，进而窃取大量相关用户的信息。

1.4 木马病毒的入侵

在计算机之中可能会有一些木马病毒的入侵，但是在这些病毒不发出攻击的时候，绝大部分的人是无法发现这些病毒的，这些木马病毒有比较高的隐藏性，需要专业的人员去发现。而这些病毒一旦发出攻击，那么计算机系统会在比较短的时间之内就发生瘫痪，其中的大量信息也会被运输到木马病毒所想要传输的地方去，而且木马病毒比较难清理，即使是比较专业的人员，他们在比较短的时间中也无法完全将一些未知的木马病毒清理掉，因此部分信息就被运输出去了，造成了计算机网络的不安全，但是绝大部分的人又只能依靠计算机中的杀毒软件去消除这些病毒，除此之外就别无他法了，因此木马病毒是非常可怕的一种病毒，会使得人们造成比较大的损失。

2 大数据背景下网络安全的防护措施

2.1 加强计算机网络安全立法工作

国家以及政府方面需要完善相关的计算机网络安全的法律法规，不能让不法分子逍遥法外，在遇到一些比较棘手的网络法律相关的问题时，政府法律人员需要做好协商，保证每一个不安全的网络问题中都有对应的法律措施去约束。对于部分网络不安全的事件，一些法律还是可以起到规范以及约束的作用的，有了这些法律，不安全的事件就会减少许多。除了立法之外，相关的工作人员还需要加强相关的网络安全宣传，增强人们的网络安全意识，减少被盗取个人信息的概率，尤其是面对一些经验不丰富的年轻孩子而言，相关人员需要在社会之中普及相关的教育，并且成立相关的法律。

2.2 做好网络个人账号和企业账号安全保护

针对个人而言，网络账号的安全防护需要做好，相关密码系统的人员需要提高密码的相关设定要求，这样人们在设置密码时等级就会有所提高，非法人员或者是木马病毒在获取个人的账号的可能性上就会小很多。企业的密码设置也非常重要，在企业中，一般都会有比较机密的文件，或者是数额比较大的金钱放置在企业的系统之中，因此企业最好是特别设置密码的相关安全软件，或者是申请安全防护中心的保护，这样可以在最大限度上保护企业的安全，而且企业密码的复杂程度应该比个人的等级要更加高一些，这样才可以做到比较安全的密码系统防范。当然相关的技术人员也需要定期去检查相关的系统，保证其中的密码安全，以及防止系统的老化，这些都是比较重要的事情。[4-5]

比如人们在设置完自己的密码之后，最好不要将自己的密码存放在手机或者是电脑之中，如果存放了，那么一旦遇到黑客入侵，或者是相关的病毒出现，那么这些密码就会暴露无遗，从而对人们造成比较大的安全隐患。当人们在遇到陌生的链接时，如果有输入密码等要求，那么人们需要及时地停止他们的行为，打电话给相关的人员确认之后再进行下一步的操作。相关的企业需要做好自己企业的内网安全，这样才可以在最大限度上避免自己企业的机密被泄露出去。而且企业的密码一定要尽可能地复杂，多加几位数字以及相关的符合，用这样的方式去保证自己企业的密码安全。

2.3 进一步强化防火墙以及病毒的防护工作

相关的技术组人员需要加强防火墙的相关设定，不定期去清除重要的病毒，或者是对相关的软件进行检查，对其中的病毒进行查杀。防火墙在设置完成之后，相关的人员一定需要对其进行反复的验证和确认，保证防火墙的绝对安全性，当遇到有一些危险的选项时，相关的技术人员需要及时地制止，并且将防火墙上面的漏洞补齐，这样可以在最大程度上防止一些恶意的破坏。防火墙的更新速度必须要足够快，这样才可以跟上木马病毒以及黑客的技术进步的速度。相关的人员每天都需要值班，如果遇到紧急的情况，需要有备选的方案可以解决突发情况，在最大限度上保证网络的安全。

比如在大型的企业之中，需要多邀请一些靠谱的技术人员对自己的系统进行定期的检查，企业的防火墙需要每天都定时检查，如果有漏洞就需要及时地整改，在最大限度上保证自己防火墙的绝对安全。病毒的查杀是必不可少的，企业的设备需要购买一些安全等级比较高的设备，这些设施的相关性能需要足够强

大，尤其是在防病毒这一块内容上，相关企业一定要邀请计算机企业的技术人员进行定期的维护和更新。在资金安全方面是非常重要的，一旦有病毒入侵，就会给企业造成难以估量的损失，因此计算机安全非常重要，防火墙的检查必不可少。

2.4 确保计算机网络安全硬件和软件更加可靠

在计算机网络安全上，相关的硬件以及软件的安全是需要保证的，相关部门在售卖相关的软件和硬件之前，需要检查上面是否存在某些病毒，如果存在，那么相关的软件以及硬件就是不合格的产品，这些都是需要相关的技术人员进行检测的，以及市场的负责人在售出之前及时地进行问题产品的解决。同时人们在选择相关的产品的时候，一定要到正规的地方购买，当遇到问题产品时，需要及时地停止使用，并且维护自己的网络相关的权益。人们在安装软件之前，一定要通过正规的安卓市场去安装，在其他渠道上安装的软件需要经过计算机自带系统的检查，如果发现问题，那么人们应该立即停止安装，这样可以在最大限度上减少问题发生的可能性，减少人们的资金损失。

2.5 充分发挥大数据云计算技术的优势

在维护网络安全时，相关的技术人员可以充分发挥大数据云计算技术的相关优势，比如计算出来病毒入侵所需要的时间，这样相关的技术人员就可以做到心中有数，或者是预判相关木马病毒的类型是什么，这样判断完成之后，相关的人员就可以进行计算机安全维护工作了。运用大数据的技术可以去跟踪黑客的相关的运行轨迹，预判出来将会造成的危害，以及危害的大小，这样可以保证计算机的安全稳定，当有问题发生时相关的技术人员也可以在最短的时间内就知晓，然后集体策划出合理的解决方案，解决计算机安全的危机。云计算技术的优势比较多，需要相关的人员积极去探究，将云计算技术的作用发挥到极致。

2.6 制定合理的信息传输技术规范和建立安全管理体系

在大数据背景下，计算机网络的安全管理必须从计算机网络结构特性的角度来考虑，它是一种综合性的运行系统，它可以通过多路径进行安全保护，如访问安全防护和提供安全保障等。在大数据的信息环境下，根据不同的信息源，有针对性地采取相应的技术防护措施，完善各个环节的安全防范措施，以保证数据的传输和存储路径。根据实际情况，建立基于大数据的信息传输技术规范，并结合相关的信息产品，建立多种大数据安全保障体系，使计算机网络的安全得到最大的保护。利用安全保护机制对海量数据的信息进行分析，将其录入安全信息模型中，对各个节点的数据进行有机的集成和存储，利用大数据挖掘技术的优点，对数据进行自动的评价和检测。这样既能确保各个节点的信息进行加密处理，又能识别出相应的数据信息，并能确定相应的信息安全级别，并能在以后的信息存储过程中实现自动分类，将数据信息的风险从萌芽状态消除。

要转变安全管理观念，构建适合我国国情的计算机网络安全管理系统，明确责任主体，围绕用户的使用和需要制订一套完整的安全管理制度。信息存储系统、用户身份认证系统等，加强用户信息资料的安全管理，增强用户的安全意识，为建立健全的网络安全管理系统提供支撑。与此同时，推进标准化的安全管理，设立专门的评估机构和培训机构，根据实际情况组织有关人员进行技术培训，提高其专业技术水平；采取积极的管理方式，对潜在的安全隐患进行深入的探索和分析，以便采取有效的预防和控制措施。根据目前的计算机网络安全状况，制定出多种管理方案，以适应各种情况，有效地提高了计算机网络的安全管理水平。

3 结语

综上所述，在大数据时代，要实现计算机网络安全的最大控制，必须大力推进相关技术的创新与优化，建立健全的安全管理体系，并通过相应的防火墙技术、数据加密技术和反病毒技术的创新优化，优化计算机网络结构，建立安全可靠的网络环境，将这些未知的或者是已知的隐患解决掉，保证整个网络体系始终处于一个比较安全的环境。

参考文献：

[1] 陈哲 . 计算机网络安全中的防火墙技术应用研究 [J]. 信息与电脑 (理论版),2019,31(24):181-182.
[2] 王玲玲 , 张倩 . 计算机网络安全中防火墙技术的应用探索 [J]. 现代信息科技 2019,03(23):154-155.
[3] 倪春 , 肖承望 , 黎惟梁 . 防火墙技术在计算机网络安全中的应用研究 [J]. 现代信息科技 ,2019,03(23):161-162.
[4] 石书红 . 大数据背景下计算机网络信息安全管理及防范措施 [J]. 普洱学院学报 ,2020,36(06):15-17.
[5] 吴佳豪 , 张娴静 . 大数据时代下计算机网络技术中人工智能分析 [J]. 九江学院学报 (自然科学版),2020,35(03):77-80.