Education and Learning, 教育与学习(3)2021, 6
ISSN:2705-0408(P); 2705-0416(0)

试谈大数据时代的计算机网络安全及防范措施

宋　刚
（重庆艺术工程职业学院　重庆　400000）

【摘　要】网络技术和网络设备已经成为人们学习生活中不可或缺的部分，而网络的开放性使其可能存在诸多的网络安全问题。网络完全问题不仅会引起人们的隐私信息泄漏，人们日常的网络活动都可能成为黑客侵犯人们隐私信息的温床。此外，网络自身的特点也容易受到病毒、恶意软件、黑客等的攻击和侵害，这也使得互联网存在诸多安全隐患，尤其是近年来不断发展的网络安全事故，使得政府部门和互联网企业愈发重视网络安全问题。以此为背景，本文重点阐述大数据背景下计算网络安全技术以及网络安全防范措施。

【关键词】大数据时代；计算机网络安全；防范措施
DOI：10.18686/jyyxx.v3i6.47797

网络使得人们的生活变得非常便捷，但是网络技术的应用是一把双刃剑，其也有不好的一方面，尤其是日益严重的网络安全问题，现在已经成为当前迫切需要解决的问题。作为对网络新生技术接受能力较高的学生们，网络安全的建立和普及，也有效的促进了校园管理和教学工作的顺利开展，但是当前网络也面临着越来越严重的网络安全问题，使得网络的相关数据时常被严重的损害。对此，要充分利用和发挥网络安全技术，从而有效的保证企业网络的安全平稳运行。本文对网络安全技术进行了讨论和研究，并提出了相应的有效策略，以期能够帮助网络的安全平稳运行。

1　网络安全发展状况

网络技术已经渗透到人们的日常生活中，使得人人都或多或少地参与到网络活动当中，人们利用网络可以学习、工作、娱乐以及购物等，可见，计算机网络已经犹如空气一样在人们生活中不可或缺。此外，随着国家倡导的“互联网+”经济的发展以及人工智能时代的到来，网络技术已经成为不可替代的部分。

人们对网络的依赖和网络的使用也会造成另一方面的问题，网络数据泄露、网络诈骗、网络木马病毒以及网络篡改等问题时有发生，这对人们的生活和生产活动造成了严重的影响，国家对此极为重视，一方面从技术上来进行扶持网络安全技术的研发，另一方面从法律法规上来保障网络安全的发展，网络安全技术的快速发展为我国计算机网络的快速发展起到了保驾护航的重要作用。

2　计算机网络安全问题及原因

2.1　网络安全问题

计算机网络能够极大的促进社会各领域的发展和进步，网络安全问题也与日俱增，越来越严重地影响到社会各领域的发展，也严重地影响到人们的日常生活，如数据窃取、黑客行为等，也阻碍了社会和经济的发展。当前计算机网络安全问题可以归纳为以下几类情况：第一，网络非法入侵，其指的是利用计算机技巧来非法访问网站的行为，网络入侵能够对网络数据进行非法改写，取得非法权限，更为严重的将会导致计算机系统被破坏，从而使得计算机系统不能正常的运行；第二，后门和木马程序，后门和木马是网络黑客惯用的手段，通过为硬件设备留有的后门来进行硬件的入侵，通过木马来远程控制用户的计算机。第三，计算机病毒，其指的是在计算机正常程序中加入特定的能够自我复制的程序代码，使得用户的计算机软件系统容易被攻击，造成网络系统的崩溃；除此之外，网络安全问题还包括垃圾邮件、对加密算法的攻击、数据窃取、数据窃听等网络安全问题。

2.2　网络安全问题的原因

网络安全问题的发生并非偶然，第一，设计思想导致网络缺陷，由于计算机网络起初来源于军事系统，开发之初只注重系统的稳定性和可用性，但是计算机网络安全性却没有得到应有的重视，这就导致在计算机设计之初其安全设计欠缺，使得计算机网络容易被监听、欺骗、篡改等网络攻击问题来随意攻击；第二，硬件问题，计算机硬件是否安全可靠，硬件参数等都直接关系着网络安全问题的出现，此外，软件设计缺陷，软件漏洞也能够引起网络安全问题；第三，病毒和木马程序，使得其引起的网络安全问题也较为突出；第四，缺少网络维护，计算机网络需要不断的去更新软硬件补丁，需要不断的去日常维护、数据备份等工作，才能做好网络的维护，才能有效的避免网络安全问题。

3　大数据时代计算机网络安全防范措施

3.1　防火墙技术

防火墙分为硬件防火墙（Firewall）和软件防火墙（WAF），硬件防火墙使借助硬件设备隔离内网和外网，硬件设备中配置一定的防御策略，用以阻隔外网中不安全的访问或非法攻击，进而达到保护内网的作用，硬件防火墙允许合法信息访问内部网络，阻止非法信息访问内部网络；软件防火墙则主要以绿盟科技、长亭科技等互联网企业研发的 WAF 为代表，软件防火墙主要通过添加各类防御规则保护软件安全，如通过 or、and、select 等规则与非法注入特征匹配，一旦匹配到非法特征值，则判断该访问为非法访问或 Seq 注入等。

防火墙有诸多功能，首先，其均可以有效的保护企业内网的网络安全，将非法访问和恶意攻击屏蔽在内网以外，从而有效的避免内网被非法入侵，此外，防护墙会将拒绝入侵的报文以日志的形式展示给防护墙管理元员，使

网络管理人员及时知晓非法入侵；其次，防火墙有助于强化网络安全策略，防火墙并非只是简单的防御设备，管理人员会在防火墙上配置多种安全防御策略，换言之，其是对网络安全的集中管理，相比于以往分散的管理策略，防火墙使管理策略更加科学化、更具集中性，无疑也更为经济；最后，对高级的黑客而言，即使是很小的细节也可能成为引起网络安全的导火索。

3.2 入侵检测系统（IDS）

入侵检测系统是指通过对网络环境的实时监控监测其中是否有非法的入侵或访问，并借助收集到的信息判断用户的网络行为中是否有违反安全策略或遭受网络攻击的行为。相比于防火墙技术，入侵检测系统更为高深，首先是事件产生器，当然这也是核心部分，其实时地对系统进行监控，并在整体的系统中获取事件，将其提供给系统的其他事件；进而是事件分析部分，事件分析器是对事件产生器中产生的事件进行合理的分析，并过滤出其中可能涉及的非法入侵数据；再次是响应单元，即对事件分析器的结果进行相应的处理，如监控到有非法数据则对其进行预警或拒绝等处理；最后是事件数据库，事件数据库是入侵检测系统独有的部分，其中保存了事件数据以及处理结果等。

入侵检测系统中的事件产生器可以及时的获取各类互联网事件，入侵检测系统中事件获取器并非只获取非法访问，同样的，事件分析器也会对网络异常通信进行识别和处理。

3.3 防病毒技术

网络病毒不仅传播性强且对系统伤害性也极强，可能导致系统崩盘或重要数据被损坏的危险，由代理对计算机系统进行实时监控，监控之前系统中会预先保存好病毒特征数据，进而将监控的网络行为和数据与预存的病毒特征匹配，若监控中发现网络数据或文件与病毒特征相似则经管理员确认后将其删除，从而保护电脑主机不受病毒的侵害。网关防病毒措施主要是在网关位置安装相关的杀毒软件，杀毒软件会在病毒进入时对其进行截留查杀，这也是保护计算机系统的有效措施。

针对计算机病毒的防治，我国相关部门也制定了相对科学合理的病毒防治体系，各大型互联网企业也针对此建立了病毒防范体系，均能够在短时间内给出预警，并捕获病毒，从而保证计算机系统的正常运行。此外，相关科研人员也应及时并准确的掌握未来计算机病毒的发展趋势，从而不断研发出更为先进的病毒防范技术。

3.4 环境安全策略

政策制度分为政府部分管理制度、网络安全相关的法律制度以及国家相关的科研机构等。首先是政府部门的管理制度，网络安全的落实离不开政府部门的管控和协调，网络安全的发展也需要政府部门运用科学合理的管控手段从全局意识管理网络安全，从而使网络真正的造福于人类。当然，政府部门与科研部门相辅相成、相互合作，共同创造一个干净整洁的网络环境；其次是法律制度，近年来网络安全事故的频繁发生对人们的生活和经济造成了极大的损失，尤其是对大型企业造成的影响更是不可估量，因此网络安全问题已经成为国家安全问题。为了推动互联网和谐、稳健的发展，相关部门逐步出台了针对网络安全发展的相关法律性文件，借此规范网络安全和网络行为，真正实现网络为人们提供便利的目标；最后是研究机构方面，研究机构包括国家科研单位和大型互联网企业，其应借助经济实力和高端的技术不断地研发出更为高端的防御技术，并不断的更新和探究，使其能够防御不断更新的攻击技术，此外，也包括网络设备的制造商，其也应该加强技术探究力度，以保证硬件设备的可靠性。物理保护对应于体系层次模型的物理层，即各类网络硬件设备。硬件设备是网络安全的前提和基础。硬件设备的安全策略从规划和使用两方面入手，规划是指机房及设备、电缆等在存放和规划时应综合考虑，避免其受到物理危害，也应避免网络设备受潮、起火等现象，物理保护不当会造成不可估量的经济损失，因此应在规划初期就考虑到对设备的合理保护。

3.5 加密技术

网络加密技术是保证信息安全的有效途径，加密技术的核心是通过加密算法对原文进行一定的保护，对称密钥主要有 DES，不可逆加密技术并没有密钥，而是通过对加密后数据的对比判断其是否被篡改，这类加密算法目前已经甚少使用，尤其是国密算法出来以后，网络安全企业大多使用国密算法。以国密算法为例来说明加密技术，国密算法在加密技术中应用非常广泛，其主要广泛应用于商业密码中，用于不涉及国家秘密的企业公司内部信息、政府部门可公开的政务信息以及商业经济信息等加密。比如国密算法应用于门禁系统中，其是通过 SM1 国密算法来鉴别客户身份以及实现对通讯数据的加密，从而实现对门禁卡的加密设置和验证，最终实现对客户身份的有效识别和验证。

4 结语

网络攻击技术在不断的提高，网络安全防范任重而道远，有关部门要高度重视网络安全问题的影响，充分利用当下的新技术和新策略来预防和解决网络安全问题，使得网络健康、安全的发展。此外，各个互联网企业要针对不断出现的网络安全新问题进行及时的研究，积极开发新的网络安全技术和新策略来进行应对，进一步的保障网络安全的发展，进而有效的促进社会各领域的健康、快速的发展。

作者简介：宋刚（1979.5—），男，蒙古族，重庆人，讲师，研究方向：信息技术。

【参考文献】

[1] 张敏.试谈大数据时代的计算机网络安全及防范措施[J].中国多媒体与网络教学学报(中旬刊)，2021（2）：206-208.

[2] 何峥.试谈大数据时代计算机网络安全及防范措施[J].中国新通信，2021，23（3）：119-120.