计算机网络安全防范的几种关键技术

赵成君

（四川水利职业技术学院　四川成都　611200）

摘要：伴随社会经济的快速发展，计算机的应用越来越普及，加上互联网渗透人们生活与工作的方方面面，信息化时代的到来为人们带来了极强的便利性。但我们在获得便利的同时，大量的危害也悄然来袭，计算机网络安全遭受了巨大的安全隐患，一旦遭受不法份子和病毒的恶意入侵，轻则无法正常工作，重则引发瘫痪，将对整个社会带来极大的亏损。所以，强化对计算机网络安全的了解和良好的防范，是有效发展网络化的必然。

关键词：计算机网络；安全防范；关键技术

计算机网络技术作为现代社会飞速发展的产物，全世界利用互联网搭建了计算机网络系统，为社会和经济的发展创造了高效的信息流通和数据共享平台，极大增强了社会信息的传递效率。但伴随着计算机网络技术的持续开发和使用，计算机网络安全隐患也不断增加，所谓计算机网络安全指的是硬件与软件信息资源在网络系统运营时并不能遭受突发、恶性的入侵和损害，从而造成信息泄露，并对计算机网络系统的安全、稳定、持续运作带来极大影响。怎样做好计算机网络安全防范措施任务是成为计算机网络技术安全发展的关键工作。

一、计算机网络中用户所面临的安全危害

（1）来自网络自身的安全危害。因当下互联网的状况是计算机网络用户数量过于庞大，用户使用计算机状况参差不齐，网络技术高速发展等，甚至互联网自身拥有许多漏洞或是 BUG，这类情形都极易造成网络安全上的缺陷。计算机网络的运行要有硬件设备的支撑，但就目前的硬件设施安全方面在整体网络搭建里属于弱项工程，很多网络设备的物理防御手段欠缺，极易遭受自然破坏以及认为损害等。计算机网络也是个系统，在这个系统里无法幸免的存有一定的安全隐患，网络的安全性和稳定性不能获得完全的保证，倘若网络用户并没有采用相关的安全手段实施自我防御的话，一经发生病毒或是入侵网络等问题，用户不但会遭受影响，还极有可能传播给其他用户。

（2）网络入侵对网络安全造成的影响。当网络系统或是用户端系统无法避免的存有一定的漏洞，倘若漏洞被一些不怀好意的人利用并入侵计算机网络系统时，将会致使网络信息的完备性遭到破坏，乃至一些机密文件的暴露。这类入侵形式关键分成两种：首先是恶意干扰入侵，黑客经过对网络传输里的数据进行干扰或是迫害以达到妨碍用户正常接收网络信息或是阻止网络系统正常运行的目的；其次是非授权性质访问，黑客经过恶意攻击窃取用户端的计算机信息或是服务器端系统权限等，以非正常手段截获用户信息数据的目的[1]。

二、影响计算机网络安全的因素

（1）浏览网站时的安全漏洞

伴随计算机技术的持续发展，网络技术日趋完善，计算机网络技术已进入了人们日常生产和生活之中，尽管计算机网络技术为我们带来了许多方便，但是也形成了不少的安全漏洞。近些年，私人数据的暴露问题愈发增多，人们浏览网站时常常会遇到不良插件，这就对广大网民带来很大的困扰。浏览网站的时候引发的安全问题是当下紧要的网络信息损害之一。浏览器 WEB 服务器的安全是致使网站浏览安全问题的首要技术漏洞，大部分网民都不清楚网站开发技术，技术信息不对称就会给民众造成不小的安全危害。

（2）计算机病毒

自打计算机技术诞生之时，计算机病毒就已经出现，并且伴随计算机网络安全技术的更新，计算机病毒机也随着更新迭代。事实上，计算机病毒就属于一类特殊的程序，它会迫害计算机里面的文件，并且能够在用户不知情的情形下盗取用户端的信息。所以，电脑病毒拥有传播性、危害性、隐匿性和批量复制等特征，近几年我国地区接连发生许多通过电脑病毒来获得自身非法目的的计算机网络安全漏洞事件。

（3）防火墙安全配置缺乏引发安全漏洞

在相当一长的时间内，防火墙技术是计算机网络安全技术的主要标志，防火墙软件安全性是抵抗外界危害的第一道良好的屏障，较大程度上保护了计算机网络的安全应用。但是目前的防火墙技术安全性时常遭到攻击，倘若不法攻击者采取了不良方式入侵了防火墙，就能够轻易闯入私人电脑中删掉、损害或是读取内部资料与文档，在这种状况下，计算机网络的安全性就无从谈起。所以，要想提升计算机网络安全技术能力，必须做好防火墙配置的安全。

（4）木马入侵

木马是一种特别的后门程序，计算机使用人在毫不知情的情形下，黑客会通过各类先进的非法路径连入用户的电脑或是登录用户的网络服务器，潜伏在电脑内部，在没有获取正是授权的情形下随便处置计算机里面的数据。由此可见，木马作为一个非法潜入的程序，是计算机网络安全技术的主要危害之一[2]。

三、几种关键计算机网络安全防范技术分析

从近些年的计算机网络安全问题来看，计算机网络安全隐患愈发严峻，计算机网络入侵方式持续升级，入侵手段越来越复杂，计算机网络安全防范工作一定是当前急需处理的关键问题。下列针对计算机网络安全问题提出一系列关键防范技术：

（1）改进防火墙技术

在计算机网络安全防范技术里，防火墙技术属于一项关键的安全防范技术，也是每一台计算机网络安全措施的重要基础，能够利用防火墙强制性的管控外部网络和内部网络。防火墙技术关键包含了网关技术、状况检测和过滤等技术措施，其中过滤技术关键是指经过网络层过滤、筛选信息包，依照之前预定的过滤罗辑检验各个经过数据的起源地址、适用端口和目标地址是否通过，要是状况检

测技术的链接发生错误的状况下，会让整体运作停止。当前，防火墙技术在企业局域网和网络交接带得以普遍使用，这不但能够更好的清理计算机网络病毒，并且还能够更好的维护用户信息。我们需要在不断实践的时候，持续总结，让防火墙技术具备针对性和实用性。

（2）访问控制技术和身份认证技术

访问控制技术和身份认证技术是计算机网络安全技术的重要构成要素，运用这两项技术能够识别并确定使用人的身份信息。当前，在计算机使用时经常会运用到这两项技术，使用权限设置不一样的话，登录口令也将会不一样，进一步说就是每一类使用权限设置应当对照相应登录口令，这就能够更好避免不法人员利用关键的权限实施不良的网络入侵。正常情况下，登录口令关键是由数字和字母构成，用户最好定期对口令进行更改，并且应当对口令实施保密，这样就能够正确保护计算机用户的个人隐私。在传输信息和收发邮件的时候，用户有必要多留意不要暴露个人信息，要是黑客获取到用户的关键信息，很容易发生相关的网络安全问题。

（3）计算机病毒防范技术

在当今互联网繁荣的时代，单单采用唯一的预防技术来应对瞬息万变的计算机病毒已经意义不大了，要想保障计算机安全，做到有备无患，就应当选用和计算机网络相匹配的全面预防病毒的软件。要是保护对象为网络上的安全，那么抛开有关预防病毒的软件以外，还应当时常将计算机网络安全进行全方位的检查和增强。但是紧靠一个预防内部互联网病毒的应用平台是根本不足的。关于防范各类桌面应用的病毒，电子邮箱和附件内的隐藏病毒等，应当根据不同的情况来选用不同位置，不同保障的侧重点，不同基础的杀毒软件。因此可以看到，倘若要想彻底的明白计算机网络里感染的病毒，紧靠人为操作是远远做不到的，要采用先进的全面的杀毒软件的配合。

此外，在生活和工作里要增强防范意识，做到未雨绸缪。在应用互联网的过程中，要加强访问可信任的网站，在下载文件资料或是邮箱附件时，应预先扫描病毒再进行下载，对于计算机里的关键文件要即时进行备份，来减小被病毒入侵后造成的损害。

（4）入侵检测技术

针对计算机网络遭受入侵攻击，积极实施检测并保护计算机的技术就属于入侵检测技术。入侵检测不但会将来源于内部或是外部的入侵实施拦截保护，还能够将用户失误的操作给予实时保护。正常状况下，采取更多的是异常检测技术和失误检测技术。通常所说的异常检测技术，指的是解析并构造出用户的生活活动模式，倘若已经发生和模式不相称的活动规律，就能够迅速准确的发现入侵攻击行动。而失误检测技术指的是和异常检测技术正好形成互补，它先将已保存到数据库的攻击行为做出建模解析，做出一连串攻击行为特征模式的匹配搜索。一经发生入侵行动，就会检测其是否和特征模式相符合，要是不相符，就不是，要是相符合，便是。但无论是失误检测技术或是异常检测技术，自身都有着很大的缺陷。准确程度高，但对于新式的入侵或是变化的已知入侵检测保护范围比较脆弱；而异常检测技术就弥补了失误检测技术的缺陷，它将未知的攻击检测特别敏锐，然而，很多状况下用户的行为方式特点较为含糊，对其实施建模比较有难度，而现如今的黑客攻击手段更加愈发强大，相当多的攻击行为都没有在统计规律上有异常表示。所以，要想保证攻击检测技术持续有效的作用，就应当强化升级失误检测技术里模型库的模型和异常检测技术里的异常检测给予提升革新并改善。

计算机网络安全包含被动预防措施，被动预防措施里包含了 IP 地址的隐藏，变更管理员账号，关闭端口...第一，针对隐藏 IP 地址，网络里的 IP 地址意义很大，因此存在较高的被窃取的危险，因而只要应用代理服务器，代理服务器的作用就是隐藏好用户自身的 IP 地址，黑客攻击也仅能检验到代理服务器，进而有效的保护了用户的网络安全。第二，将不需要的端口都关闭掉，防止黑客经过某类端口监测并扫描用户的计算机，第三，将权限最高的管理员账号实施重新设置，防止被黑客攻击。

（5）漏洞扫描技术

这类计算机网络安全预防技术是一种计算机系统自我筛查技术，它包含了 PING 扫描、OS 探查和端口扫描技术等，但这类扫描技术的关键作用和任务目标并没有多大的差别，决定这类扫描技术的工作原理也没有很大差别。工作目标的差别关键是为了保证可以在各个角度以及全方位检查总体计算机网络的安全，将威胁系统安全的技术实施动态指导。

四、网络安全技术发展趋势

（1）IDS 入侵检测技术。为填补网络防火墙技术的缺陷，在当下的网络安全技术里引进了 IDS 入侵检测技术。此项技术将部分关键节点信息给予收集和解析来认定其操作是否归为非法操作，或是否有违背安全策略。这个技术相比于其他技术来说更加积极，所以也可称作主动防御技术。就是把网络设施发生问题后在给予处理的工作形式转换成在网络设施遭到入侵或是损害之前就将危险设施阻拦的工作模式。此技术具备特别强的发展空间[3]。

（2）云安全技术。伴随云计算技术作为当今计算机互联网使用的重要趋势，基于云的网络安全技术也获得了普遍注重。云安全技术就是通过网络里的计算机集群的超级计算与解析能力将用户的网络安全实施保护和管理，把网络安全经用户端转移到云端，保证终端和传递过程的数据安全。

结束语：

互联网为我们的工作和生活带来便利和快捷的同时也面临着很多的安全问题，自从计算机出现以来其两面性就一直存在着，但归根结底是利大还是弊大，各执己见，要想安全的应用计算机并施展其最大的效用，就有必要做出一定的策略来进行防范，通常不同的安全隐患要实施不同的应对手段，说是防范，但不要无目的的运用各类预防措施，可先从民众的素养培育着手，加强计算机安全防护措施等，乱用安全防范措施只能让网络安全添堵，进而造成网络安全问题实现不了想要的处理成效。

参考文献：

[1]文晓浩.关于计算机网络安全防范的几种关键技术探究[J].2022,(01):19-22.

[2]王华.关于计算机网络安全防范技术的研究和应用[J].信息记录材料, 2021,(01):2-4.

[3]乔娟.计算机网络安全防御系统的实现及关键技术研究[J].通信电源技术, 2021, (04):3-5.