新形势下计算机通信网络安全防护策略

江志晃
广东培正学院　广东　广州　510830

摘　要：随着电脑网络安全科技的提高与发达，国内计算机用户数量日益增多，这不但为人民提供了便利，也暴露出不少网络安全问题。所以，人们必须建立一种完善的网络安全防护措施，已保证认识日常生活中的信息安全。鉴于此，本文对新形势下的计算机通信网络安全隐患以及防护措施进行了进一步的阐述。

关键词：新形势；计算机；通信网络；安全防护；策略

1 计算机网络威胁的特征

第一，隐蔽性。隐蔽性是计算机网络威胁的最大特点，网络攻击凭借这种隐蔽性攻破计算机网络主动防护，并且计算机网络安全防护人员面对隐蔽性极强的网络攻击经常防不胜防，直至计算机网络安全已经受到严重侵害时，安全防护人员才能察觉到问题的严重性；第二，破坏性。计算机网络攻击通常具有强大的破坏性，严重时甚至会对计算机网络系统造成严重损坏，引发信息安全事件，更会造成不可估量的经济损失；第三，突发性。目前计算机网络技术还有许多不足之处，存在着不少漏洞，容易被攻击。有不少病毒有着活跃以及无法预测的特点，且有着极强的攻击能力，它们对计算机的影响是十分严重的，如果不能第一时间进行阻止以及修护的话，将会有网络瘫痪的可能，用户信息将会被泄露以及篡改[1]。

2 计算机通信网络存在的安全隐患

2.1 自身系统存在问题

计算机网络运行中经常会因为外界环境或人为因素而造成网络不稳定情况，埋下安全隐患。随着计算机网络的逐渐普及，安全风险因素会随着使用者数量的增加而成比例增长。从计算机角度来看，现阶段大部分系统都支持数据共享模式，交流途径扩大，加大信息泄露风险，甚至会被黑客所利用，比较常见风险如下所列。第一，TCP/IP存在脆弱性。这一问题具体可以归纳为协议中的缺陷，针对计算机网络安全的关注度较低，在TCP/IP协议中归于强调网络的开放性，这一特点会被黑客利用，并寻找运行漏洞，造成安全隐患。第二，网络结构问题，运行过程中不稳定。由于网络的形成主要依靠局域网，一旦发生通信行为，攻击者只需一台主机便可实现信息窃取。除此之外，系统更新阶段也是风险发生率较高的时期。第三，信息被窃取风险。造成这一问题的主要原因在于保密程序设置不当。第四，工作人员安全意识薄弱。用户在进行操作时由于意识的缺乏造成严重隐患问题，例如认为防火墙影响电脑流畅性便卸载或关闭，并在未获得代理认证时连接网络，防火墙形同虚设[2]。

2.2 网络黑客入侵

黑客在计算机网络应用初期便始终存在于计算机网络系统中，并对信息安全带来严重危害，一旦遭受侵入便会造成大范围服务器瘫痪，不能正常供用户使用，就会影响生产生活。此外，黑客还会利用服务器进行网络控制，寻找通信协议中关于网络开放性、网络稳定性以及用户所缺乏的防护意识实施攻击行为。尤其针对安全防护弱的系统，主要分为两种情况。一是被动攻击模式。主要由黑客监视用户行为，从而获取一些隐秘数据信息，用户难以很快地察觉到自己处于被监视状态，攻击行为十分隐秘。二是主动攻击。与被动攻击的最大区别在于黑客实施攻击行为时会有详细的措施，能够篡改数据信息或拒绝相关服务，主动攻击无法采取预防措施，且攻击行为很容易会被用户发现，针对主动攻击则需要设置入侵检测系统或防火墙，从防护角度提升网络安全。

2.3 欺骗技术入侵

通过对路由条目、DNS中的解析地址以及IP地址的欺骗，将会造成服务器无法对这些请求做出准确响应，或是无法对这些请求做出准确判断，进而导致缓冲区发生严重阻塞甚至死机的情况。如果通过将局域网中的某台计算机设置成主要的网关IP地址，也可以使互联网上的数据包产生转发不良的情况，导致某一个用户无法访问。

2.4 管理缺陷问题

倘若管理人员的规范性不足，安全意识较为孱弱，都会对安全产生一定的危险。就例如系统关于账号或口令的设定并不合理，并且没有对重要的机密数据信息进行保密，并不能在第一时间内对数据信息进行备份，以及关于用户等级权限的界定也缺乏明确性等等，都会使

病毒与黑客等进入到系统中，使得重要数据信息发生了泄漏、删除等问题，甚至还会导致系统的崩溃。

3 新形势下计算机通信网络安全防范策略

3.1 提升用户防范意识

根据计算机通信网络安全风险内容来看，造成风险问题频发的主要原因之一在于用户使用过程中的安全意识不足，导致信息泄露风险扩大，针对这一问题，还需从用户意识的角度出发，加强网络安全知识宣传，拒绝访问非法网站或下载未经过扫描的软件[3]。重点关注一些浏览网页中的信息安全判断窗口，了解其运行可行性后再继续浏览。针对一些风险网页需要立即关闭，并向系统举报。相关单位应当建立计算机网络安全的宣传通知，使用户了解风险因素对财产及个人信息安全所带来的危害，引导用户规范自身操作行为。例如在使用计算机时第一步需要设置重复性的密码登录，切忌与个人身份证件或号码等一致。除了基础密码外还需设置访问密码和访问权限，利用IP、口令等形式降低恶意入侵率。

3.2 部署数据加密

网络自身的开放性对于信息安全防护工作来说属于劣势条件，针对这一情况，首先需要以用户安全意识为切入点，从根源处提升网络风险防控等级。在实际操作中，可以从源头处和传播处两个层面进行加密处理，传输者想要保证信息传输的安全性，则需要应用加密函数和密钥转换信息，将其变为无意义密文。接收方在收到数据后还原密文，可以保证数据传输过程中不会被不法分子查看和复制。数据加密的方式主要包括异或和加密机，详细的加密方式和主要内容可以划分为以下几种：第一，专用密钥。是最简单的计算机网络安全防护方式，主要针对本地文件的保护，在没有密钥的情况下无法读取和更改信息，例如Bitlocker技术；第二，对称密钥。对称密钥的应用主要将数据分为64位数据块，在转换后形成分散组，再均分两段应用密函加密，这种方式相对古老，其优势在于运算量小、转换速度快，安全性相对较高，目前在计算机网络数据加密领域应用十分广泛；第三，非对称密钥。与专用密钥相反，所应用的加密方式和解密方式由完全相反的运算方式进行加密，非原理在于进行明文转换，最终获得一个值，作为核实签名，接收数据方会根据标准化的解密运算，对传输数据进行解密。

3.3 科学设置防火墙

随着科学技术的发展，网络技术发展也更加迅速，但是不论发展多快，网络技术自身都存在着一定的安全隐患，是需要一些手段来进行防御的。防火墙技术的出现就是人们对网络安全的一个重要防御手段。防火墙与网络技术有着相互促进的关系，信息技术的成熟，人们可以发明出安全性能更高的防火墙技术，而防火墙的运用可以确保技术的安全，是网络技术能够正常运行的保护措施，是一道结实的屏障，防火墙技术能够帮用户筛选过滤存在着网络信息安全的邮件或者网站链接。不过并不是有了防火墙，网络信息安全就完全没问题，目前市面上大部分用户使用的都是普通的防火墙，用户除了在使用计算机时打开防火墙，还需要使用安全杀毒软件。随着网络技术发展，几年来智能防火墙应运而生，虽然应用不是很广，但是作用不是普通防火墙所能比的，它能够直接阻止高端病毒对计算机的侵入，大大提高计算机信息安全。

3.4 推动入侵检测技术的应用

所谓的入侵侦测技术是指为了侦测网络资源和非法利用计算机的活动，同时开展有关的技术处理工作，重点包括内部人员对网站个人信息进行不法利用和外部侵犯的情况。通过使用侵入测试技术，可以最大限度提高计算机系统在操作过程中的稳定性，并能够对系统问题和异象进行有效拦截，为计算机系统的正常使用提供完善的安全防护环境。在具体使用环境中可利用下列三点进行入侵的监控：①严密监视与系统相关的运行行为和操作系统，并对用户实际的使用情况进行监控分析；②密切观察会对网络安全运行造成危害的情况，并第一时间向相关技术人员做出报告使他们做出相应补救；③统计计算机网络应用的异常情况，并对应用中出现的安全行为做出详细分析[4]。

3.5 关闭服务端口

一些针对性的计算机网络所应用的服务器需要在所规定的协议端口上开放，不要随意在其他端口开放，以免给黑客更多入侵机会，例如文件、设备、邮件等系统。可以关闭FTP和HTTP，保证内部计算机网络安全运行。

3.6 及时更新杀毒软件，加强防黑客技术应用

随着科技的进步和计算机网络相关人才的涌现，现阶段杀毒软件领域的创新与优化也获得了显著成就，其功能更加齐全。相关杀毒软件不仅具备对病毒的拦截功能，还能实现对病毒的追踪与查杀，有效提升计算机网络安全维护等级。当前各类计算机系统中所应用的杀毒软件已经基本实现检测网络系统、全面扫描计算机、隔离与查杀病毒的功能。此外，还有一些软件能够起到预防效果，针对黑客的攻击进行自动抵御，同时进行数据拦截和恢复，避免造成重大损失。为保证计算机网络安全，用户需要定期进行系统扫描，找出隐藏在文件、邮

件等内容中的风险因子，并根据软件的升级情况及时更新，采用最新病毒数据库，全面抵御病毒入侵，从而及时解决潜在风险问题，谨防运行过程中感染病毒。

在计算机应用过程中还需加强防黑客技术，主要的风险来源在于黑客入侵或黑客设计的特定程序造成系统破坏情况，不仅影响一些重要文件的传输，还会窃取一些资金信息，如银行账号、密码等，并利用专业技术篡改用户个人注册信息为己所用。为有效规避这一问题，需要加强安全防护力度，例如建立外部网与局域网之间的防火墙，实现对用户IP地址的维护，避免黑客入侵[5]。在防黑客技术应用上需要明确故障情况，如电脑频繁无故宕机、更新系统后死机频率提升、忽然无法运行并自动重启、网络不佳经常掉线、程序加载时间延长、磁盘莫名出现坏块、数据丢失内存空间变小、文件扩展名日期及属性被更改等。以上行为均属于病毒感染后的常见情况，需要用户及时扫描计算机和网络安全情况，明确中毒文件，删除不认识的启动项目。

3.7 提供专业化管理服务，形成主动化管理机制

通常，在探索计算机网络安全管理的过程中，可基于专业版块、人员业务经验不同等，构建一支专业的管理团队，从而确保为用户提供更加专业的计算机网络服务。在此过程中，需实施负责制，管理团队要仔细地梳理网络安全管理特点，进一步对业务详情、关键用户等进行了解，并列成清单，从而为管理工作的高质量开展提供指导，对计算机网络服务质量的持续改善起着积极的促进作用。同时，还需严格遵守功能模块负责制原则，指派专门的人员负责相应功能模块，当数据、功能等发生问题时，需有相应的运维人员去处理，并予以跟踪。还可应用双向网格优化的方式，弥补传统管理模式的不足，通过对内部管理责任的细化及实施，提高计算机网络服务的专业化，最大化满足用户需求，改善用户的应用体验。

一般而言，计算机网络应用效果直接受数据的影响。为确保网络运行的安全性，就需重视系统功能的增加，包括数据逻辑校验等，推动主动化管理机制的构建。人员需定期主动对系统数据质量进行检查，基于系统数据，合理地对反馈系统应用状况予以判断，做好问题或缺陷排查工作，从而有针对性地提供主动化服务，并结合该机制，进一步对计算机网络安全隐患问题进行明确，完善和提升系统功能，避免计算机网络安全管理缺乏专业化等现象的发生。

3.8 促进技术水平的提高

计算机通信网络安全主要包含隐性资产、个人隐私等方面的安全，在社会发展或个人生活中有着重要的意义。因此，在应用计算机系统时，要重视技术水平的提高，为网络安全提供保障。在日常生产生活中，计算机网络遭到黑客攻击的可能性较高，会导致数据丢失，抑或是泄露等风险发生。同时，病毒植入也是造成数据丢失的常见原因。故为规避黑客攻击带来的损失，需落实对计算机相关数据的备份，对于重要文件的传输，可采取数据加密手段，防止信息丢失。另外，还需重视对计算机的保护，定期开展杀毒检查工作，不断强化技术手段，尽可能地规避信息泄露等安全风险的发生。

结束语

综上所述，在新形势下，计算机通信网络运行的过程当中存在各种各样的问题，而各类安全隐患则是当前必须要重视的问题，要求相关工作人员必须针对常见安全隐患，采取有效的解决策略，从而提高计算机通信网络运行的稳定性与安全性。

参考文献

[1]付强. 新形势下计算机网 络的运行及维护策略探究[J]. 通讯世界，2018（11）：36-37.

[2]李勇.浅析计算机网络安全与防范[J].蚌埠党校学报,2019,43（3）:109-114.

[3]杨佳兰.浅析计算机网络信息通信安全防范措施[J].南方农机，2021，52(7)：177-178.

[4]王懿嘉.新形势下计算机通信网络安全隐患及其对策探讨[J].科技创新导报，2020，17（17）：132-133.

[5]尹茜茜.新形势下计算机通信网络安全隐患及其对策探讨[J].信息通信，2019（11）：178-179.