计算机通信网络安全与防护策略的相关思考

韦焯思
广东培正学院　广东　广州　510830

摘　要：随着当前信息技术的快速发展，使得计算机通信网络被广泛使用。但是人们在享受计算机网络便捷性的同时，也让自身的关键信息暴露在不法人员的面前，并通过其使用来窃取内部重要内容，这对当前人员的财产与信息安全产生了威胁。为了改变这样的状况，须对当前的安全工作加大重视力度，并要强化在防护上的研究。正基于此，笔者根据自身的工作经验，立足于目前我国计算机通讯网络安全所遇到的具体安全隐患及特征，并给出了相应的防护对策，以期有效保障用户的网络安全。

关键词：计算机；通信网络；安全和防护；策略

1 计算机通信网络安全隐患的特征

第一，受网络攻击的概率进一步提高。网络信息传递的主要特点是信息传递的范围具有不确定性、信息传递的速率较高。然而在网络信息快速传递的同时，被攻击的现象也日益明显，甚至是网络信息传输攻击变成了常态化。第二，网络信息传输的攻击针对性越来越强基于大数据、区块链技术的不断发展，网络信息的传输更加精确，而部分网络不法分子利用大数据技术可以实现对特定网络信息传输的攻击，这样就增加了网络信息被破坏的危险程度。比如，对于使用网络比较规律的用户而言，其在网络中的留痕比较突出，所产生的信息泄露的可能性就比较大，这样就更容易受到特定的攻击[1]。第三，网络攻击的形式呈现多元化。随着网络技术的不断发展，针对计算机通信网络的攻击手段呈现多元化的趋势，例如，当前对于通信网络的攻击手段已经由过去单一的植入病毒扩大到通过骗过IT和通信行业最信赖的供应商进行攻击。

2 计算机通信网络安全存在的隐患

2.1 计算机操作系统的漏洞。网络攻击存在不确定性与隐蔽性，网络攻击发生初期不易被察觉，并且会以多种伪装逃避计算机安全系统的检查。当计算机系统自身存在漏洞的情况下，网络攻击会趁机对计算机系统展开肆意攻击，使计算机安全防护系统迅速陷入瘫痪状态。计算机系统漏洞通常是由于日常维护工作缺失造成的，计算机系统漏洞并不能在短时间内修复完成，在修复漏洞的过程中网络攻击就可以趁虚而入，因此计算机系统的漏洞也是引发计算机网络安全风险的常见原因[2]。

2.2 黑客攻击，窃取用户信息。黑客是一种专门运用计算机技术手段，非法入侵、攻击他人计算机系统的群体，黑客的目标是为了摧毁对方的计算机系统，或窃取对方计算机系统中存在的信息。黑客对计算机安全的干扰具有迅速、短暂、强大的特点。黑客本身是可以熟练运用计算机技术的人员，因此黑客技术也伴随着计算机网络技术的发展而不断提升，高级黑客甚至可以运用其他用户自身的习惯与特点达到攻击、入侵的效果，特别伴随信息时代的快速发展，黑客攻击、入侵手段日渐多元化，对计算机网络安全造成持续性威胁。

2.3 病毒侵害。网络病毒的侵害会对计算机网络中的相关程序、指令等造成影响，且病毒存在自我复制的功能，一旦侵入一台计算机，便会迅速传播并造成整个系统的瘫痪。从宏观角度来看，计算机网络病毒实际上是人为编写的一种针对性程序，且具有大范围传播的特点，在网络安全控制领域中属于一种“定时炸弹”，始终潜伏在网络中，对用户的日常工作和个人信息安全造成一定影响。除了病毒外，计算机网络系统还会受特洛伊木马程序和蠕虫的影响，虽然这两种并不属于计算机病毒，但同样具备传播范围广、速度快的特点。其中，蠕虫的存在形式以组合式为主，能够实现设备间的转换，且不需要特定的宿主即可实现传播。而特洛伊木马程序则会在技术人员编程过程中侵入，若用户此时启动计算机则会造成病毒入侵使得网络瘫痪。

2.4 用户使用计算机不规范。除了内部软件、硬件问题外，用户自身操作的不规范性也是导致计算机网络存在安全隐患的重要原因之一。造成该类型风险的原因在于用户安全意识淡薄，在操作过程中并未遵循相关规范，亦没有对应的安全措施。这一系列行为导致计算机网络运营存在潜在隐患，如尚未设置登录密码或密码过于简单，账号自动登录等设置，忽视计算机风险预警肆意下载软件，没有杀毒软件。这一系列行为均会导致计算机网络安全受到侵害[3]。

2.5 网络新问题。在移动互联技术快速发展的大背景下，计算机信息技术正在持续不断地发展与进步，计算机网络成为连接世界每个角落的纽带，对于推进人类社会信息化发展具有根本性作用。信息时代下，人们对计算机网络的利用率高达100%，计算机网络与电力一样成为社会必不可少的组成部分，也因如此计算机网络技术飞速发展、不断革新。

3 计算机通信网络安全防护策略分析

3.1 强化网络用户安全意识

计算机网络安全涉及的层面较多，包含网络技术、网络管理等。对此有关部门就需重视对计算机网络安全管理机制的完善，建立相应的法律法规，动态监督计算机网络安全问题，以促进计算机网络安全管理水平及效果的提高。网络用户是计算机技术的使用者，该群体的安全意识与计算机技术的可持续发展有着紧密的联系。数字化背景下，随着计算机技术的进一步发展，强化网络用户的安全意识也极为关键。个人或企业均需加大对网络安全意识的培养，掌握相关计算机技术，提高安全意识。另外，考虑到计算机工作具有一定的难度，内容及形式较为复杂，故需要充分发挥计算机网络优势，合理地应用网络知识，落实计算机相关宣教工作，不断促进用户网络安全意识的增强，促使其在实际应用中能够严格遵守相关要求，合理地运用计算机解决问题。例如，可通过举例防范措施的方式，为用户普及计算机网络安全问题，增强用户的网络安全意识，正确引导其操作计算机，尽可能地规避误操作等因素引发的安全隐患问题。

3.2 构建规范化、立体化的管理体系

一方面，需在基于工作任务的前提下，完成工作岗位的制定，并对岗位职责予以明确，促使人员能够了解、掌握工作任务。另一方面，还需结合工作内容，对各流程节点的工作任务、岗位人员等进行明确，避免流程混乱等情况的发生，实现各工作的流程记入平台。同时，要进一步规范化计算机网络安全管理工作，结合新型技术设施库的体系架构，构建健全的管理平台，促使管理体系越来越规范，为计算机网络安全管理工作的高效展开提供保障。另外，在开展计算机网络安全管理时，需充分考虑工作项及技能项，从而制定出全息数据库管理体系，实现工作库和技能库的立体融合，以充分发挥管理效果。在实际的管理中，应在基于管理流程定义的前提下将事件、问题、配置等管理内容进行明确，以达到合理约束管理行为的目的，这有利于促进网络安全管理效率的提高。此外，还需将业务作为核心内容，落实全流程监控，以更好地开展日常网络安全管理，并重视对各安全隐患事件的跟踪处理及评分，将各类设备的使用情况等进行统一，并确保其统计的灵活性。

3.3 数据加密技术

数据加密的方法。第一，对称式加密。采用对称式加密方法时，需使用相应的算法和公式，确保明文转换更加顺利，使数据得到全面的加密处理。由于加密和解密的公式算法一致，因此，该方法还存在一定的安全隐患。一旦公式算法遭到泄露，就意味着这一加密技术失效。在具体操作时，通常会根据原文的内容和相应的算法，将其转换成毫无规律的64位数据组。正式设置密钥之前，需对这些数据进行分组，将数据组和密钥进行有效结合，就可确保原文得到顺利加密。第二，非对称式加密。对数据进行传递时，为了确保加密后的数据得到有效破解，通常要经历两个过程，一是公钥解密，二是私钥解密。实施双重加密方式，可以进一步降低数据面临泄露的可能性，而且该加密方法中的加密和解密算法公式并不一致，这样就会进一步提高数据的安全性和可靠性。非对称式加密的弊端在于操作速度比较慢，工作效率比较低。

数据加密技术。第一，链路加密技术。在某链路上传递信息和数据时，信息与数据形式主要以报文为主，当信息和数据通过某一节点时，需利用这一节点的密码装置对数据进行解密。在正式开启报文传递模式之前，会对报文进行再度加密。当报文经过下一个节点时，该节点的密码装置同样会以上述的方式进行破解。以此循环，尽管报文形式会陆续经过相应的加密和解密处理，但由于在整个过程中的数据信息处于加密状态，加之加密过程比较复杂，因此，采用这种方式之后，往往并不容易被破 解。使用链路加密技术时，要确保所有节点加密顺利，一旦某一环节出现差错，就会失去加密效果。第二，节点加密技术。采用节点加密技术时，要考虑到对各项节点的管理。在进行信息传递时，当信息正式传递到节点之前，主要是以明文为主，一旦信息正式到达节点，明文就会转化为加密形式。因此，为了发挥出节点加密的效果，首先要在这一节点处对报文数据进行解密处理，然后再将其设置在比较安全的模块之中，完成加密工作。对所有的节点处进行加密时，均要延续上述操作方式，工作人员要采用不同的秘钥，保证解密和加密工作安全开展。在设置接收报文数据的设备时，需保证各个节点的设备相符。第三，端到端加密技术。采用端到端加密技术时，要考虑到是否为明文加密。在操作时，首先要了解到信息接收的地址，然后明确传递途

径，采用明文形式，确保信息能够及时获得转换。将其转换成相应的加密报文包之后，就可以保证在各个节点和链路进行传递时始终不会泄密。设置在节点或链路的密码装置无法对报文包进行解密。根据相应的指示，以加密形式出现的报文最终可以达到指定地点。在进行加密处理时，信息具有高度的安全性，即使节点被损坏，或者报文包出现遗失，也不会影响数据和信息的安全性。第四，密钥加密技术。采用密钥加密技术时，要遵循以下操作流程。对经过加密的信息进行相应的认证；在传递信息时，要保证信息获得到专业的系统监督与控制，避免其受到病毒的攻击。要发挥出密钥管理系统的防护功能，明确信息访问的权限。当接收者需要接收信息时，需提前输入密码。第五，数字签名认证加密技术。采用数字签名认证加密技术时，接收者要根据相应的算法，对原信息进行信息摘要提取，保证摘要信息与信息发送者的签名摘要信息内容保持一致。在这一过程中，接收者要使用发送者所提供的公钥，确保信息得到全面的比对[4]。

3.4 建立可靠的安全防线

第一，入侵检测技术。对计算机网络的入侵检测系统进行设备配置，一方面，能够实现其他用户的非法入侵信息的防范和监控，并且记录入侵用户的信息及行为；另一方面，还可以快速地对网络系统的入侵及攻击信息进行整合分析，同时及时传递到计算机网络中。第二，防火墙技术。防火墙技术主要发挥着互联网隔离的作用，并且对于外界网络对各单位网络的入侵和访问，可以及时的发现和检测数据传输过程中的问题，完成对计算机网络运行状态的检测及管理，有利于网络安全体系的构建。另外，防火墙技术不仅能够避免内部信息的泄漏，对数据进行分类和隔离，还能够实现数据信息的过滤，进一步提高网络技术的安全性。第三，访问权限设置。设置访问权限是保障计算机网络安全的重要途径，通过把非法访问隔离在网络的外面，防止网络受到非法侵害。在这一过程中，计算机系统可以按照具体情况设置权限条件，并且给予计算机用户一定的访问权限和限制，确保用户能够在权限范围内进行资源的访问和查找，提高权限的管理[5]。第四，病毒查杀技术。计算机病毒的破坏性较大，因此必须加强病毒防杀技术的研究，提高计算机网络安全性能。病毒查杀技术主要以预防为主，查杀为辅，能够显著的减少网络病毒对计算机系统的不利影响。此外，计算机用户要及时安装病毒查杀软件，完成对杀毒软件的全面监控，及时的更新杀毒软件，以便快速发现网络病毒，实现对计算机病毒的快速、高效处理，维护网络系统的安全性。

3.5 强化信息化人才队伍建设

计算机技术的发展离不开人才的培养，尤其是信息化人才。因此，需加大人才队伍建设，相关部门要给予足够的支持，严格按照计算机技术的应用要求，不断强化技术人员的综合水平，促使其能够熟练、正确地应用计算机技术，提高计算机网络安全水平。同时，还需积极应用现代化管理模式，提高网络安全管理效率。

结束语

当前已步入数字经济大环境，加强计算机通信网络安全既是维护国家安全的重要内容，又是推动我国信息产业发展的必然举措，同时也是维护用户基本权益的关键举措。然而随着信息化建设步伐的加快，计算机通信网络安全问题日益突出。通过对网络运行状态、Web应用、主机、弱密码、中间件等网络安全脆弱点持续监测，以及网络安全风险事件的采集，可为实现数据驱动的网络安全风险事件预测提供相应的数据基础，从而为保证计算机通信网络安全工作的顺利开展保驾护航。

参考文献

[1]郭军虎，刘彦飞. 试论计算机通信网络的安全问题与应对策略[J]. 中国新通信，2019,21(22):33.

[2]张远.信息时代计算机通信技术的应用及安全防护策略[J].信息记录材料，2019,20(8):221-222.

[3]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.

[4]吴昊.浅析计算机通信中的网络安全[J].企业科 技与发展,2019(06).

[5]姚玉开,赵杰,陈洋.浅析计算机网络安全技术的影响因素与防范措施[J].中国设备工程,2022(1):235-236.