计算机系统安全与计算机网络安全浅析

蔡堂华
广西壮族自治区教育技术和信息化中心　广西南宁　530000

摘　要：在信息化时代下对计算机技术的应用正在逐渐加深，所以新时期需要做好计算机的网络安全管理工作，尤其是当前的企业与个人在使用计算机过程中遇到的网络安全问题类型愈加复杂，需要对相关的计算机安全技术加以合理应用，进而保障个人的隐私与企业信誉。本文从维护计算机系统和网络安全的必要性入手，讨论计算机系统中存在的安全问题，最后提出维护计算机系统和网络安全的措施，希望通过多项举措打造更加健康的网络环境。
关键词：计算机；系统安全；网络安全

Analysis of computer system security and computer network security

Tanghua Cai
Education Technology and Information Center of Guangxi Zhuang Autonomous Region，Nanning, Guangxi，530000

Abstract: Under the information era the application of computer technology is gradually deepened, so need to do a good job of computer network security management in the new period, especially in the current enterprises and individuals in the use of computer network security problems in the process of type more and more complex, need to be reasonable application of relevant computer security technology, to safeguard the privacy of personal and corporate reputation. This paper starts with the necessity of maintaining computer system and network security, discusses the security problems existing in computer system, and finally puts forward the measures to maintain computer system and network security, hoping to create a more healthy network environment through a number of measures.
Keywords: Computer; System security; Network security

在科学技术不断发展的背景下，计算机开始在诸多领域中得到应用，让社会发展面貌焕然一新。人们在日常的生活与工作中也频繁的应用计算机，为人们带来便利的同时也存在诸多的网络安全隐患，比如个人信息泄漏与企业网络瘫痪等，问题的背后在于人们缺乏网络安全提意识，没有采取有效的安全管理措施，需要采取有效的应对策略，以下进行相关分析。

一、维护计算机系统和网络安全的必要性

对于计算机的安全管理来说就是采取相关措施对内部的信息与硬件进行安全保护，比如避免出现信息非法访问、信息窃取等。在硬件安全管理过程中主要是配套设置物理安全措施，为系统的正常运行带来帮助，而功能安全性体现在对系统正常运行的控制，还包括故障出现后的恢复能力。网络安全体现在内容安全和传输安全，其中信息内容安全体现在信息的真实性和保密性，而传输安全及时计算机在网络中传输信息的技术，如今做好计算机的安全管理工作受到人们高度关注，其中网络病毒与黑客持续威胁计算机安全，只有合理采用计算机网络安全管理措施才能营造良好的网络环境，促进社会健康发展。

二、计算机系统中存在的安全问题

1. 网络安全管理问题

对于计算机的管理来说，当前我国不断完善相关制度，尤其是企业单位针对计算机操作制定了相关的规定，不过现阶段的监管制度还不完善，难以保障用户的安全，比如部分分子利用法律漏洞从事违法犯罪。此外，目前的网络监管技术也不够先进，使得部分企业的信息被盗用，甚至导致企业发展危机。

2. 网络安全技术问题

一种是计算机病毒。在计算机功能不断完善的今天，网络病毒也更加多样化、破坏性也在提升，部分病毒复制计算机代码之后开始主动对硬件和软件系统发起攻击，比如“熊猫烧香”导致程序图标无法使用，再如“鬼影病毒”重装系统依旧存在与电脑。

3. 硬件和软件问题

在计算机系统中如果运行大量的问题硬件，会对系统的运行造成不利影响，在系统的运行过程中也会受到质量较差元器件的影响，出现相关故障。从软件的角度讲，程序运行错误就会影响人们正常使用计算机，尤其是当前的计算机精密化程度不断提升，系统的运行中出现编程问题会引发很大影响。使用需要在编程结束之后加以调试。

三、维护计算机系统和网络安全的措施

1. 提高安全防护意识

在计算机的使用中需要对外部安全威胁与内部的网络安全隐患重视起来，使用不管是个人用户还是企业用户都需掌握一定的计算机操作技术与安全管理方法，企业更加需要打造一支专业化的管理队伍。网络病毒与黑客攻击是由计算机系统运行漏洞导致的，因此需要对计算机系统进行长期的监控，对计算机的硬件和软件进行定期检查、维护与升级，在网络监控模式下可以及时处理不良信息，避免计算机网络被入侵，对系统的安全构成威胁。在实际工作中主要是对数据与系统的安全进行监控，排查安全隐患，企业还需要对现有的网络安全管理机制改革，进而为网络资源整合与方案调控带来帮助，数量安全管理意识是减少网络安全问题的根本工作，有利于企业减少购买安全管理产品的费用。

2. 建立健全相应的管理制度

在应用计算机的过程中不仅需要做好规范操作，还需要建立和完善管理制度，主要措施如下：其一，科学制定上岗制度。在企业应用计算机开展业务的过程中需要对操作人员进行系统的培训，尤其是信息、金融、财务等岗位人员需要严格遵守上岗制度，掌握计算机的操作规范；其二，完善培训制度。通过有效的培训措施提升技术人员的专业能力，掌握网络安全动态，可以处理企业常见的网络运行故障；其四，落实人员管理制度，企业需要将人员的责任明确，做到各司其职，避免员工出现推卸责任和态度不端正的问题，之后结合奖惩机制对计算机维护人员进行管理。

四、科学运用安全防护与管理措施

1. 加强防火墙技术

在计算机系统中防火墙是在不同网络中建立的安全网关，主要有硬件和软件组成，防火墙可以隔离本地网络、外界网络和公共网络，营造安全的网络环境。此外，防火墙可以控制网络数据的连接，达到数据的安全传输要求。防火墙简单实用，并且无需对本地网络改动，常用的防火墙包括应用级防火墙、网络级防火墙、规则检查防火墙、电路级防火墙，其中网络防火墙较为简单可以避免外部网络对本地网络非法入侵，还可以对地网络的不安全流量加以控制。网络防火墙主要是对比数据包源地址与防火墙安全规则，只能让达到规则的数据进入。电路级防火墙较特殊，连接内部和外部的网络并且访问系统。应用级防火墙可以对外部数据包进入程序起到拦截效果，之后将数据包隔离在被保护的系统外部。而规则检查防火墙具有以上三种防火墙的功能。具体应用如下：

（1）保护特殊网点访问安全

在应用防火墙的过程中凭借隔离作用对特殊的网络加以控制，其中网络防火墙可以允许或者禁止访问网络，进而起到避免木马或者网络攻击的效果，保护主机。

（2）提升防火墙技术利用的灵活性

在建立网络安全机制的过程中需要结合防火墙的技术要求，之后提升网段防护水平，也让防火墙的利用灵活性大大提升，比如在静态模式下和动态模式下自由切换，及时追踪攻击 IP 的情况，让网络安全管理更有保障。

（3）优化网络安全配置

防火墙是计算机网络技术的重要组成与模块，可以在计算机网络运行的过程中根据等级分成保护措施，使得不同等级的数据也被保护。进行安全配置期间防火墙可以对计算机的网络安全区域信息加以划分，对数据加以控制，避免计算机被入侵。

（4）监测网络日志

为了记录系统的运行问题需要建立网络日志，规范网络的运行状态，还可以建立临时数据库，通过防火墙的监控提取数据包密钥。安全管理防护需要审核日志，并且在检测中通过数据分析了解用户计算机使用特征，让局域网和 Internet 隔离，达到提升网络安全的作用。

2. 信息加密技术

这种技术是利用密钥控制用户访问网络数据，在网络用户访问到数据后没有密钥依然不能看到数据内容。数据加密技术灵活性好、安全性强，尤其是近年来的双加密技术得到了更加广泛的利用。在实际应用中通过操作人员置换数据位置与密钥控制，其包括了公开密钥和私用密钥，而混合加密的方法进一步提升了数据安全性，比如 DES 加密之后通过 RAS 非对称加密方法把数据传输到另一侧，之后需要对称加密数据才能解密。

（1）密钥分配管理

为了实现计算机的网络安全与通信安全，就要借助加密技术具有的挖完整性、保密性和确定性特点，关键在于分析安全性问题，数据加密技术中的密钥分配管理是重点，对称密钥加密的过程中不得公开密钥，加密期间通过原始数据提供给加密接收方，接收文件之后需要让前后密钥相同。

（2）链路加密要点

该技术的作用在于计算机网络通信链路中加密基础性信息，进而让网络信息安全的传输，需要在操作之前进行加密处理，解密之后再加密，由此让数据信息具有安全性。链路加密过程中出现了数据的多次加密，而递进式连续密钥消息加密模式更提供了安全保障。

（3）节点加密要点

在利用节点解密技术的过程中需要应用节点机设备，之后连接密码装置，解密之后重新加密，让网络传输的安全性大大提升，并且这种操作方法与链路加密接近，需要说明的是，这种技术与链路加密模式差异较大，主要是解密技术不允许信息以文字的形式出现，并且对接收的额消息深度解密。

（4）端到端的数据加密

该技术是数据传统期间不对任何节点进行解密，因此对加密技术的要求不高，比如 E2EE 就是常见的端到端数据加密技术。在报文独立加密的过程中，主要优势在于应用效果好与维护便捷，并且避免了加密系统自身同步。此外，在报文独立加密之后即使出现错误也不会对后续的报文产生影响。

3. 加强计算机网络访问限制

在企业的计算机应用过程中，可能由于网络攻击出现密码篡改情况，而出现计算机安全问题的原因在于密码单一、密码未能定期修改。比如当前的网站与提供服务之前需要实名注册，如果被病毒攻击就户导致信息处于不安全的环境下，需要对计算机网络权限进行限制，主要操作步骤如下：首先 TCP_wrap-persr 软件对 IP 加以控制，其次用户使用和更改超级口令。此外，应用防火墙数据包的代理和过滤功能。在信息技术不断见进步的背景下，人脸识别技术、数据加密技术进一步提升了安全等级，让人们的信息安全更具有保障。

4. 及时维护操作系统

其一，维护计算机网络硬件对于计算机维修人员来说，在故障的处理中先是进行硬件的分析，比如是否是硬件故障导致并造成网络连接受到影响。在检查内部的设备过程中需要对周边的线路连接情况进行分析，比如下时期出现问题需要对显示管、元件分析，借助计算机诊断程序可以提升故障处理效益。其二，对于计算机的软件维护来说主要是在处理的过程中分析网络协议、系统问题网络参数，在处理操作系统的过程中需要先进行检修，然后对其优化升级，达到提升系统运行效率的目标，在参数的设定过程中也需要专业人员处理。

5. 利用遗传算法加强网络安全

在复杂的网络环境下，可以通过遗传算法的特征组合处理信号，遗传算法在网络安全系统应用过程中如果网络提取的入侵特征数据流是父代染色体，可以通过遗传算法交叉操作得到新的子代，之后将一代交叉定义为 1，以下类推，父代和子代染色体配对特征库配得到特征变化值，最小值就为特征库中寻找的最近染色体，之后将其代入函数当中计算 f 值，并且父代与子代组成的种群和适应性最强的半体交叉，多次处理后适应度超过阈值说明局部优化，再分析特征值的变异得到最适合目标值。

6. 计算机安全标记编码

为了进一步提升计算机网络系统的安全性，对标记编码关注十分必要，编码可将其理解为针对不同模块设定额 ID，之后根据实际情况安全标记 IPSO 携带的数据信息。从计算机的系统内数据来说，通过分布式存储、异地备份、数据找回可以避免其它人员获得数据，即便获取依旧不能解读，达到保证系统稳定和安全运行目标。此外，安全标记编码需要对安全等级字段长度检查，比如客体安全标记设定为 2 字节那么主体部分可设定成 10 字节，由于不同的字节存在安全等级的差异，所以需要结合机密程度加以划分，进行全部区域的标记，在每一次记录信息之后可让计算机安全运行。

五、结束语

综上所述，在网络技术飞速发展的今天，网络安全问题影受到人们的高度关注，为了让人们的财产安全与隐患得到保护，需要国家继续加强法律规范的建设，并且在应用计算机的过程中需要结合实际需要选择安全技术。从企事业单位的角度讲也需要加强人员的培训，对防火墙技术、加密技术有效利用，最终通过多种途径提升网络使用安全性。

参考文献：

[1] 夏文英 . 探究计算机网络安全技术在网络安全维护中的应用 [J]. 数字技术与应用 ,2021,39(7):175-177.

[2] 王伟 . 计算机网络安全技术在网络安全维护中的应用研究 [J]. 网络安全技术与应用 ,2021,23(1):155-157.

[3] 段秀红 . 浅谈计算机系统安全与计算机网络安全浅析 [J]. 消费电子 ,2013(18):110-110.

[4] 康铁峰 . 浅谈计算机系统安全与计算机网络安全浅析 [J]. 计算机光盘软件与应用 ,2013,(4):94-95.

[5] 田小虎，卢益强 . 计算机系统安全与计算机网络安全浅析 [J]. 黑龙江科技信息 ,2013(12):159.