论计算机信息管理技术在网络安全中的应用

张震

（苏州大学　215000）

摘要：网络在给人们日常生活带来诸多便利的同时也蕴藏着风险。电脑中的资料经常会因病毒入侵或黑客攻击而遭到损坏甚至丢失。所以提高网络安全性十分重要。本文阐述了信息管理技术在计算机的网络安全中的重要性，希望能够提高网络环境的安全性。

关键词：计算机；信息管理技术；网络安全；应用

引言：

计算机技术在最近几十年的时间里飞速发展，覆盖了衣食住行等多个领域，人们的日常生活已经离不开网络技术的使用。网络成为人们生活的必需品，那么相对应的，网络安全问题也得到了越来越多的关注。信息管理技术能够确保网络安全，提升网络运作速度。

1 网络安全的含义和现状

1.1 网络安全含义

在网络运行过程中，网络资料和数据不会被有意入侵或篡改，也不会因硬件出现问题而被破坏，网络能够稳定运行，这就是网络安全。也就是说，无论面临主观还是客观的原因，网络都不会因为任何意外的发生而中断运行。网络安全既包括其存储内容的安全，如资料、数据、信息等，也包括各种设施设备的安全。还可以从使用和运行角度，将其划分为静态和动态安全。静态网络安全，是指网络系统中存储信息在存储和管理时的安全。动态网络安全，是指网络信息在动态处理过程中的安全，即接收和发送的信息不会出现丢失或被损坏的情况。

1.2 网络安全现状

随着近些年我国在信息化建设上不断加大投资和发展力度，计算机网络已经覆盖了人们生产、生活的方方面面。网络给人们的生活带来了很多的便利，信息有了便利的获取途径和共享方式，超大的存储空间也使得越来越多的人将数据信息存储在网络中，这些数据信息涉及到个人隐私、研究成果、企业甚至是国家的机密等，如果无法保证网络安全，就会造成数据信息的损坏和泄露，给个人和社会造成恶劣影响和严重损失。因此，网络安全问题十分重要，为此采取了多种方式保证网络安全"。

2 计算机信息管理技术在网络安全中所存在的问题分析

2.1 监测技术落后

信息管理技术十分重要，能够保护大家的网络安全。一些常见的恶意入侵和有意无意的数据损坏，比如黑客攻击、钓鱼网站、电脑病毒、软硬件破坏等对计算机造成的损坏，计算机内部的数据信息会遭到丢失和破坏.对个人和社会的生产生活造成严重影响。

2.2 无法有效控制信息访问

使用互联网时，用户遇到的信息访问并不一定都是有用及安全的，例如某些病毒木马、弹窗连接等频繁出现，影响计算机的正常使用。这也反映出了信息管理技术的缺失。计算机管理技术应该能够在技术水平上对访问对象加以管控，减少恶意的入侵，做到有效的控制信息访问。同时还可以对境外的网站信息进行监察、防止色情暴力、违法犯罪等不良信息的出现。

2.3 缺乏有效的应变能力

互联网技术在近些年得到了飞速发展，与此同时，技术人员也要提升计算机维护的水平，加强网络安全的管理，提高应变能力，对一些常见问题要做出预案，对计算机安全要予以重视。黑客入侵、病毒侵入等已成为全世界都面临的网络安全问题，给无数企业甚至国家层面都造成了严重损失，我国必须要提高计算机信息管理技术，增强应变能力，维护网络信息的安全。

2.4 缺少加密技术手段

如今的网络环境已经十分复杂，利用好加密技术可以更好地保护个人信息及财产安全。所谓加密技术就是对源文件设置加密钥匙，从根本上杜绝黑客入侵。病毒侵入以及一些非法链接等。但随着网络技术的发展，恶意入侵的手段也在不断更新，相关技术人员也要在传统的加密技术上不断创新和改进，丰富加密技术的手段，这样才能有效阻止恶意入侵，保护数据信息，维护网络安全。

3 计算机信息管理技术在维护网络安全中的应用

3.1 构建防火墙系统。防火墙能够有效地保障网络信息的安全，其构成主要分为硬件和软件两个部分。利用防火墙系统对信息进行加密处理，然后建立通信监控系统，对网络的边界实行信息监控，将网络分成内外两个部分。外部网络用户在访问网络时，如果没有得到授权，那么将会受到防火墙拦截。除了个人外，还可以应用在公司管理上，将公司办公系统划分为独立空间，登记内部人员信息，防止外部信息的入侵，保障公司内部数据资料的安全。防火墙的应用对维护信息安全有十分广泛且重要的作用

3.2 提升技术人员的安全意识。随着互联网技术的发展和在个人社会生产生活上的广泛应用，互联网环境日益复杂，威胁网络安全的因素也逐渐增多，信息被泄露和破坏几率也在提高。因此，技术人员必须要增强安全意识，充分认识到保障网络安全的重要性。如果在思想层面放松警惕，那在实际过程中的管理和维护必然会松懈，难以主动提高信息管理技术水平，有效保障网络安全。相关部门应该定期对技术人员加以培训，从思想上增强网络安全意识，从技术上培养信息管理水平，有效提升技术人员的思想认知和工作能力，维护网络安全，实现网络技术持续高效发展[1]。

3.3 加大风险监测的管理力度。信息管理技术能有效保障网络安全，但突发风险会阻碍计算机的正常管理，对网络安全造成严重损害，因此，要对可能存在的风险进行日常监管，明确风险原因，制定防范计划，对可能出现的风险进行严格监控。另外还可以联络相关部门，共同组建风险预警信息平台，对可能性较高的网络安全风险进行监测预警，共同进行风险管理[2]。

3.4 对网络密码和数据进行加密处理。密码被盗和数据丢失是日常生活中十分常见的网络安全问题，对个人和社会都造成严重损失。相关部门应该对密码和数据进行加密处理。现阶段我国采用加密手段相对落后，无法满足目前高速发展的网络安全要求，必须要对加密技术进行研发和创新，调整改进加密算法，降低数据被盗的风险。技术人员应该学习最新的密码学理论知识，创新和改进当前我国的加密技术，为国民创造安全放心的网络环境，从根本上降低个人信息泄露、数据流失等事情发生的概率。

3.5 对操作系统进行安全防护。除了网络安全之外，还应该注重计算机操作系统的安全性，只有保证操作系统安全，计算机才能维持正常的运行状态。然而在实际使用过程中，操作系统很容易出现故障，计算机无法正常运行，带来一系列安全问题。保证操作系统安全是计算机正常运行和维护网络安全的基础条件。因此定期对操作系统进行检测和维护十分重要，技术人员对操作系统进行检查，如补丁升级、查杀病毒、漏洞修复等，保证计算机操作系统的安全，从根本上避免恶意入侵的发生，维护网络安全。

4 提高计算机信息管理技术在网络安全中应用的有效措施

4.1 加强网络安全风险控制意识

信息管理技术对网络安全有非常重要的作用，但想要发挥出它

（下转第 223 页）

针对这种情况就需要及时地进行修复。要是遭受破坏的数据，数值处于阈值内，可以借助于变慢来将原始数据进行恢复；这一过程中，要是验证已经通过了，用户就可以实现到云端上进行处理，尤其是计算机运行时，这时是非常容易导致计算机数据受到损失，而编码就可以对这种情况进行恢复。在这样一个过程中，就可以借助于可取回性证明算法，保证用户能够验证运算数据库系统，将符合完整、安全性的标准进行明确，分析出其中存在的失误之处，这样更有利于进行管理。

（二）MC-R 端

为了能够保证在云端上更加安全的存储数据，一般就会使用 MC-R 端，借助于多元化的方式来保证对数据的管理，让数据更加的安全。云计算技术中对 MC-R 端进行应用中，首先，对用户 MC 进行加密处理，将云计算技术采用合适的方式应用于网络安全存储系统中，对网络系统中是否存在着隐患展开分析，对具体的问题展开探究，并做到严格管理。在应对黑客过程中，就需要做到合理的预防，预防借助于程序、客户端中存在的漏洞会进入到数据中心中，避免数据遭受到泄露的情况。其次，在数据库、云端角度上，就需要加强管理工作的开展，以更好的创建数据隐私、伪装管理模块，以建立出完善的数据管理模块，真正发挥出以上模块中的作用。经过相互之间的协调性发展，真正意义上实现了安全存储管理。最后，实际工作开展过程中，也是需要应用 RSA，全面分析出大数据中具有的消耗，以这种方式来建立起加密和解密模块，并保证其是完善的，并实现严格的管理、协调。此外，对用户实际情况也需要做到引导，建立起 RSA 密钥以后，数据信息可以实现自动的出巡到其中，MC 加密算法下，保证数据实现了有效的加密处理，在将其传到云端以后，实现了数据的安全性，并真正实现安全管理，让整个系统都更加的安全。

四、提高计算机安全存储的策略

（一）优化云计算信息库防火墙设备

计算机安全存储过程中，通过运用云计算技术，保证了数据的安全性，预防出现丢失、泄露的情况，为了能够保证数据存储过程中的安全性，可以优化云计算信息库防火墙设备。防火墙在计算机系统中可以保证数据的安全性，也能抵挡病毒、攻击，这对于提高计算机防御功能具有非常重要的作用。因此，将云计算技术应用于计算机安全存储过程中，需要安装高性能的防火墙。如，对于防火墙设备应用虚拟化保护措施过程中，需要将保护性的措施作用于计算机终端，这样在保证计算实现独立运行的同时，还能实现实时监控计算机信息数据，让多台计算机都能够实现同时进行安全管理，经过互相监督，最终实现了信息数据的有效存储，所以，提高云计算技术在计算机安全存储中效果是可行的[5]。

（二）完善云计算数据中心信息系统

计算机安全存储中应用云计算技术，虽然保证了信息的安全性，避免出现丢失的情况，但是其中却是存在着一定的安全隐患，所以此时就需要针对云计算中存在的不同之处，得到多领域的共同发展，不断完善云计算技术。如，建立有效的信息系统，这样就算是云计算出现了问题，也能将存在的问题快速备案，并将问题归入到信息系统中，在更新存储中遇到的问题后，也为云计算技术的应用奠定良好的基础。同时，借助于身份认证的方式，将云计算数据中信中的信息进行不断的完善，具体可以采用四种技术进行，如密钥、plk、kerberos、智能 IC 卡，通过这种方式保证每一条信息都能够验证身份，用户接收到服务器认证以后，才能登录到数据中心系统，采用确认身份的方式提供更好的防护，保证网络信息数据足够安全，这在一定程度上提高了云计算技术在计算机安全存储过程中的具体效果。

结束语

云计算属于一种新型的计算模型，能够将个人在计算中存储的数据转移到计算机集群上，实现了计算机较大的存储量。然而在计算数据库中不仅数量庞大，并且也是非常复杂的，这时安全存储功能就产生了威胁，非常容易受到病毒、攻击，最终让大量的数据丢失、篡改，为了保证数据中更安全，预防数据遭受到泄露，未来对于云计算中的存储还需要进行深入地探究。

参考文献：

[1]王利军.云计算技术在计算机安全存储中的应用研究[J].科技视界,2021(27):146-147.

[2]左毅,郭长金,游华.云计算技术在计算机网络安全存储中的应用[J].电子技术与软件工程,2021(18):246-247.

[3]孟大森.计算机网络安全存储中云计算技术的应用[J].电子技术与软件工程,2021(15):243-244.

[4]孙力.云计算技术在计算机网络安全存储中的应用分析[J].数字技术与应用,2021,39(07):184-186.

[5]陈德.云计算技术在计算机网络安全存储中的应用[J].江西电力职业技术学院学报,2021,34(06):20-21+25.

（上接第 219 页）

的价值，首先要提高技术人员的思想认知，加强风险管控意识。只有维护好网络安全，才能保护用户个人的数据信息，从而维护整个社会的和谐安定，因此，要从根源上铲除不良因素，维护网络安全。首先，用户自身要加强网络风险意识，注重个人隐私的保护，重要信息如身份证号码、手机号、银行卡账户及密码等信息绝不能轻易外泄；其次，技术人员要提高信息管理技术水平，对实际生活中可能会出现的风险因素进行分析和预防，制定相应的预防对策，对于出现的问题具备解决能力。

4.2 做好计算机信息管理技术的管理工作

目前. 计算机信息管理技术是维护网络安全的主要办法，因此，做好信息管理技术管理，加强其在实际生产生活中的应用十分重要。为此，要做到管理内涵和理论双管齐下，将其应用到网络安全的实际预防中。当前，计算机信息管理技术的应用越来越广泛，网络信息系统朝着现代化和科学化发展，信息管理技术也在不断地创新和完善，管理水平进一步提高。想要更好地实现信息管理技术在网络安全中的应用，必须要对网络安全防范机制有充分了解，做好信息管理工作[3]。

4.3 建立完善的计算机信息管理技术相关制度

除了加强安全意识和做好管理工作外，还应该建立健全信息管理的相关制度。相关部门可以建立科学合理的规章制度，筹备网络安全小组，负责日常的网络信息安全工作。同时，安全工作应该常态化，对于计算机的操作系统，应该做到定期的更新、杀毒、漏洞修复等，对于可能会遇到的风险问题，要做出预案并具备解决问题的能力。除了要防备黑客攻击或者病毒入侵外，计算机硬件系统的安全性也应该得到保障，应该及时更换功能和系统滞后的计算机，保障计算机的硬件功能能够胜任工作需要，以防硬件方面故障和问题影响信息安全。

5 结束语

信息时代的发展已经涵盖了人们生产生活的方方面面，在享受网络技术带给人们便捷生活的同时，也要意识到网络安全的重要性。只有增强计算机信息管理技术水平，才能够增强抵御网络安全风险的能力，保证数据信息不被泄露，维护好网络安全。

参考文献：

[1]李刚. 试论计算机信息管理技术在网络安全中的运用[J]. 无线互联科技, 2016, 78(2):123-124.

[2]胡恒金. 论计算机信息管理技术在网络安全技术中的应用[J]. 网络安全技术与应用, 2016(6):2.

[3]赵志鹏. 浅论计算机信息管理技术在网络安全中的应用[J]. 电子世界, 2016(7):82-83.