计算机信息系统管理技术在网络安全中的应用

王　峥
滨州市投资促进中心　山东滨州　256600

摘　要：在我国现代信息化技术水平不断提高的过程中，网络安全逐渐受到了较大的重视，旨在营造安全的网络环境，减少信息化技术应用期间产生的数据信息泄露问题。目前，各个领域在建设发展中都开始利用计算机信息系统管理技术提高工作质量和效率，解决传统工作形式下的弊端，但是还是面临显著的网络安全问题，难以全面保证计算机信息系统运行的安全性及稳定性。文章简要概述计算机信息系统管理技术特征，对其在网络安全中的应用进行分析，探讨提高网络安全成效的措施，为降低计算机信息系统运行风险奠定良好的基础。

关键词：计算机；信息系统；管理技术；网络安全

数字化发展使得各类高效率技术形式在各个行业中得到了广泛应用，计算机信息系统管理技术作为新时期建设发展中的一项主要网络技术形式，可以在很程度上提高各类工作的效率，充分体现新时期科学技术的优势。但是在应用相关技术的过程中，还是会受到较多因素的影响导致网络安全性不高，计算机系统还会受到频繁的网络攻击，这就需要加强对计算机信息系统管理技术的安全控制，解决潜在的威胁，提高技术应用过程中的安全性。

一、计算机信息系统管理技术特征

第一，综合性。计算机信息系统管理技术的应用需要以多个方面的技术和知识作为基础，技术人员在实践操作当中不仅要掌握专业的计算机网络、信息安全等理论知识内容，还应在技术操作中融合数据库管理知识实现科学的网络操作。落实这项技术操作时，会涉及到多个环节的工作，技术人员需要从硬件设备到软件系统采取多样化的技术手段和方法，还要整合多样化的信息资源，结合专业的管理手段达到技术应用目标。

第二，安全性。利用计算机信息系统管理技术的过程中需要非常注重系统安全性保障，虽然会受到各方面因素的影响导致系统安全性受损，但是还是需要采取身份认证、加密传输、访问控制等方式保护系统和数据，防止其受到恶意攻击，才能够满足技术应用的基本要求。

第三，灵活性。与传统的技术形式相比，计算机信息系统管理技术可以根据不同系统的需求自主调整安全策略和访问控制规则，如果系统在运行期间检测到安全隐患和风险，就可以根据系统运行需求灵活变换运行形式，形成更加符合系统运行需求的安全环境，减少技术操作中产生的安全问题。

二、计算机信息系统管理技术在网络安全中的应用

（一）防火墙技术

防火墙技术在目前的网络安全中得到了广泛的应用，技术人员可以利用其监管数据的访问权限，还能够开展数据交互筛选工作，将其应用到网络安全保护各个方面，为计算机信息管理工作的开展打下良好的基础。在网络安全中利用防火墙技术时需要以软件系统和硬件系统的应用作为要点，形成内部与外部网络环境之间的保护屏障，构建能够保护用户信息的系统化内网和外网，一旦出现恶意攻击就可以避免用户信息泄露。就目前的计算机信息系统管理技术防火墙技术应用情况来看，可以将其氛围标准模式和双网关模式这两种，其中，标准模式需要以Unix工作站作为核心，利用两侧端口实现彼此之间的交互与联通，实现系统与内网之间的有效连接。如果在特殊软件中应用防火墙技术就可以在激活程序时主动调高管理级别，提高标准模式防火墙的网络安全保护成效，但是在传输数据的过程中无法保证及时性，所以需要综合这种模式的优缺点分析防火墙技术的必要性及可行性。技术人员还可以在网络安全中应用防火墙双网关模式，其可以在单独利用系统的情况下实现多样化功能，为网络用户提供多项服务，面对复杂程度时也可以体现较高的效率水平。总的来说，在网络安全中以防火墙技术作为计算机信息系统管理的主要技术形式时，可以有效保障数据传输的安全性，规避非授权用户的访问，

还可以自主过滤不良信息，实现对内外网络的有效访问与控制。

（二）访问控制技术

人们在使用计算机网络的过程中经常会出现未经允许可以直接访问某个系统的情况，虽然可以提高计算机操作的便捷性，但是很容易侵害别人的隐私。与此同时，个人的隐私信息也很看会在这种形式下被别人所侵害，引发不必要的网络争端。以维护网络安全作为主要目的时，技术人员可以利用访问控制技术体现充足的安全性，其可以对用户及系统进行科学管控，提高系统与资源交互的规范性与科学性，在经过允许之后才可以开展访问操作，有利于保护用户隐私。实际上，访问控制技术与防火墙技术存在一定的相似性，利用访问控制技术时可以通过对网络传输信息的筛选和监测对系统及资源进行保护，防止其在未授权的情况下被访问，还可以阻断与隔离危险信息，避免网络系统遭受不良侵害。在访问控制技术支持下，计算机网络系统需要经过严格的访问控制才能够展现相关的数据信息，还可以将其与综合应用身份认证技术相互结合加强网络连接控制的规范性，从根本上提高网络安全管控效果。

（三）信息加密技术

信息加密技术顾名思义是对计算机信息系统中的数据信息进行加密处理，减少信息泄露、恶意篡改、恶意破坏等问题，通过信息多重保护的方式规避网络安全风险，满足人们的网络系统运行需求。虽然计算机网络的发展使得人们在沟通交流的过程中更加便利，但是还是会受到网络环境的影响产生较多安全风险。为了加强网络信息安全性，就需要对内部信息进行加密处理，提高解密机篡改难度，还能够在较大程度上限制不良行为，进而达到提高网络安全的目标。利用信息加密技术开展网络安全管理工作时，应该做好电脑硬件设备加密处理工作，设置相应的密码与账户安全策略，以科学的技术手段降低电脑被暴力破解的可能性。如果计算机长期处于不工作的状态，系统就会自动解锁，这时就需要设定启屏幕密码还要增加安全认证，通过双重加密的方式提高网络安全性。此外，还应在传送资料的过程中利用信息加密技术，以节点密码技术做好资料传送处理工作，再采取链接加密这种二次加密的方式形成更加安全的网络环境。与此同时，还应采取端到端的加密技术形式提高解密难度，防止数据在传递过程中遭受入侵，避免其被篡改或者破坏，加强网络系统安全性。

三、优化计算机信息系统管理技术应用效果的措施

（一）完善安全检测管理制度

以维护网络安全作为主要目标开展计算机信息系统管理工作时，需要完善安全检测管理制度，从源头上加强网络安全性，减少网络系统在运行期间产生的问题。基于此，有关单位应该建立规范化网络安全检测管理流程及标准，根据新时期网络运行安全性要求形成更加完善的安全检测管理机制，保证各项检测工作能够有条不紊落实到位。由于计算机信息系统在日常运行当中经常会受到网络威胁，所以，安全检测管理制度中应该提出定期收集、整理与分析网络威胁情报的要求，技术人员与检测人员应按照相关管理制度做好威胁情报深入分析工作，为提高网络安全性提供可靠的参考依据。针对计算机系统在运行期间产生的安全问题，需要建立安全事件报告与记录机制，做好针对各类安全事件的记录跟踪工作，明确产生安全问题的主要原因，采取可行性措施提高安全检测管理成效。除此之外，还应加强网络安全管理部门与其他部门之间的紧密合作，构建符合网络安全要求的合作机制，部门工作人员要结合日常工作经验及自身的专业能力提出应对网络安全威胁的措施，加强资源信息共享，共同协作将安全检测管理制度落实到位，为提高计算机信息系统管理技术水平打下良好的基础。

（二）建立信息安全管理平台

信息安全管理平台的构建可以实现对系统和网络等多个层面的安全管理，直接在管理平台上监控计算机信息系统在运行期间出现的漏洞、安全事件等，提高网路安全管理实时性，减少系统在运行期间产生的安全问题。部分企业在生产经营期间存在破坏计算机信息系统的情况，针对这类现象就可以建立信息安全管理平台，在产生安全问题时及时发出预警，还可以构建科学的响应机制做好网络活动监控工作，规避黑客攻击、恶意代码等安全风险，使得预警信息更加准确。根据群众举报线索，2023年4月27日，南宁市生态环境局执法人员对广西某机动车检测服务有限公司开展现场检查，发现该公司机动车环保检测线电脑操作系统内，有某外挂软件运行记录。执法人员依法对该公司环保检测线操作间内的一个U盘及一台工位机主机实施了扣押，并委托广西某司法鉴定所进行司法鉴定。结果表明：上述U盘及主机自2022年1月3日起曾运行某外挂软件247次，运行后可实现对检测程序内存数据的修改。经进一步调查，为提高车辆检测的通过率，吸引更多的车辆到该公司检测，

增加公司检测费的收入，该公司环保检测线技术员李某某在检测过程中擅自使用外挂软件对检测数据进行修改，为274辆车出具了虚假的尾气排放检验报告，违法所得共计1.6440万元。为了减少类似事件的发生，有关部门构建了区域信息安全管理平台，如果在区域内发现计算机信息系统异常运行就会及时组织专业人员予以处理，提高安全事件的相应和处置效率，以此加强网络安全运营成效。

（三）构建入侵防御体系

防火墙和入侵防御系统是网络安全防护的稳固防线，利用计算机信息系统管理技术维护网络安全的过程中，应该重视入侵防御体系的构建，在尚未产生安全问题时对其进行监测与控制，减少系统在运行期间产生的问题。所以，管理人员要将防火墙作为首要的安全屏障，启动计算机信息系统时设定严格的访问控制程序，对网络数据包进行过滤和检查，针对其中未经授权的访问及恶意流量进行阻拦，从根本上提高系统运行安全性。构建入侵防御体系时，应对网络流量中存在的异常行为和潜在威胁进行科学分析，尤其需要采取科学的检测与防御措施对其进行处理，使得数据信息在复杂的网络环境中可以得到安全保护。为了加强入侵防御体系建设成效，有关部门或者企业可以根据业务需求设置精细化的访问控制规则，只让符合规则的数据包进入内网，通过严格过滤对存在安全隐患的数据包进行阻拦。体现入侵防御体系的作用时，可以引进智能分析引擎，基于网络行为对其中存在的异常网络流量进行实时监测，一旦系统察觉潜在威胁就需要触发预警，自主对其进行阻断或者隔离处理，实现对不良网络行为的合理监测，从根本上防止恶意入侵行为。

（四）重视网络安全应急响应与处置

尽管技术人员和管理人员能够在计算机信息系统运行的过程中对尚未产生的安全问题进行预警和阻拦，但是还是难以完全规避网络安全问题，稍有不慎就会有漏网之鱼，给计算机信息系统造成较大的损害。所以，在维护网络安全的过程中需要做好网络安全应急响应与处置工作，明确安全事件报告与处置流程，将其作为构建应急响应体系的核心，针对已经产生的安全事件采取可行性措施予以处理。按照相应的流程处置安全事件时，需要做好针对网络威胁的敏感探测，还要迅速做出回应，在报告安全事件时应该对其进行专项检测与识别，一旦发现系统中的异常行为就要及时采取可行性措施予以处理。当检测人员意识到系统中的潜在威胁之后就需要立即转入报告环节，利用自动化报警系统及时传达相关信息，启动应急响应链，进入到具体的安全应急处置环节。对网络运行中的安全事件进行处置时，需要按照相应流程对其进行隔离与遏制、调查与分析、修复与恢复、监控与反馈、总结以改进等，严格按照流程将各个环节的工作落实到位，确保安全事件处置成效达到预期目标。做好这项处置工作之后，需要针对具体的事件进行调查分析，确定产生安全事件的主要原因及受害范围，再根据产生安全事件的原因修补系统漏洞、清除恶意代码，使得其中受到的影响得以恢复。

结语

综上所述，在网络安全中应用计算机信息系统管理技术能够以防火墙技术、访问控制技术、信息加密技术的应用为主，通过对多元技术的应用加强网络安全性。落实这些技术操作时，还应完善安全检测管理制度、建立信息安全管理平台、构建入侵防御体系、重视网络安全应急响应与处置，以提高系统运行安全性和稳定性作为主要目标，深化对计算机信息系统管理技术的理解与应用，减少系统运行中出现的安全问题，为加快我国数字时代信息安全发展提供保障。

参考文献

[1]塔丽，杨思齐.计算机信息管理技术在维护网络安全中的应用路径[J].信息与电脑（理论版），2024，36（16）：66-68.

[2]洪年芳.计算机信息管理技术在维护网络安全中的运用[J].软件，2024，45（06）：175-177.

[3]宋宪余.计算机信息系统管理技术在网络安全中的应用[J].中国高新科技，2024，（05）：50-52.

[4]杨星辰.网络安全中计算机信息管理技术的应用探究[J].信息记录材料，2024，25（02）：127-129.