数字化背景下计算机信息网络系统安全管理策略

黄玲琳，丁宇琼，姚质彬
华信咨询设计研究院有限公司，浙江 杭州 310000

摘　　要： 数字化时代背景下，信息技术的发展为互联网行业规模延伸提供了支撑，计算机信息网络系统的构建可为人们生产生活提供较大便捷，但其中仍旧存在较为明显的安全隐患问题，威胁网络用户信息及权益。现阶段，计算机信息网络系统应用已经成为人们生活中的重要内容，解决其所存在的安全隐患问题可为用户提供更优的网络体验。本文主要研究了数字化背景下计算机信息网络系统存在的安全问题及相关安全管理措施，以期为相关技术人员提供参考。

关 键 词： 计算机信息网络；安全问题；管理策略

Security Management Strategies for Computer Information Network Systems in the Context of Digitization

Huang Linglin, Ding Yuqiong, Yao Zhibin
Huaxin Consulting Co. Ltd, Hangzhou, Zhejiang 310000

Abstract: Under the background of the digital era, the development of information technology provides support for the extension of the scale of the Internet industry, and the construction of computer information network system can provide greater convenience for people's production and life, but there are still obvious security risks that threaten network users' information and rights. At this stage, the application of computer information network system has become an important part of people's lives, and solving the hidden security problems can provide users with a better network experience. This paper mainly studies the security problems of computer information network system and related security management measures in the context of digitalization, in order to provide reference for relevant technical personnel.

Keywords: computer information network; security problems; management strategy

引言：

在数字化时代发展与计算机信息技术不断创新的背景下，互联网使用范围更加广泛。互联网信息技术可为企业工作、各政府部门及组织机构处理事务提供支撑，因此，计算机信息网络系统与我们的生产生活存在密切联系，但是，该系统运行受到运行环境、网络病毒等因素的影响存在较多安全隐患问题。相关技术部门需深入探究数字化背景下计算机信息网络系统安全管理策略，以减少网络信息系统安全问题的出现。

一、数字化背景下计算机信息网络系统特点及安全管理原则

（一）数字化背景下计算机信息网络系统特点

（1）高效性与灵活性。数字化技术与计算机信息网络系统融合可快速、准确与自动处理业务，以提升各企业工作效果，且数字化背景下计算机信息网络系统运行可自动处理业务数据，优化业务流程，以减少人为因素对数据处理结果的影响，同时，数字化技术与计算机信息网络西融合可结合用户需求调整系统功能，以在最大程度上满足用户对计算机信息网络系统的要求。（2）可拓展性与数据化。数字化 IT 系统应用运用中系统模块与功能也会随之扩张，从而为用户提供多样化服务，同时，数字化 IT 系统运行可存储与分析业务数据，以为企业决策提供准确的数据参考。（3）安全性与共享性。数字化背景下计算机信息网络系统较为关注数据安全内容，可在加密数据、控制数据访问权限等基础上，保护企业业务数据安全性与完整性，同时，计算机信息网络系统可通过数字化技术与其他系统相连接，以构建不同系统之间数据共享模式，提升企业内各个部门联系。

（二）数字化背景下计算机信息网络系统安全管理原则

（1）保密性原则。保密性原则实施中计算机信息网络系统中数据信息需得到相应保护，以减少数据泄露等问题的出现，此过程中组织与企业需严格限制数据方位权限，在设置合理访问控制规则的基础上，加强网络安全防护，保障数据安全。（2）完整性原则。完整性要求确保计算机信息系统中的数据在传输和存储

过程中不受损坏或篡改，该原则落实中可应用加密技术、数据备份和恢复机制等，同时，企业与组织需建立严格的审计和监控机制，及时发现和防止数据的意外修改和破坏。（3）可用性原则。可用性原则要求计算机信息网络系统及时为用户提供服务，该原则落实中技术人员需维护数据完整性与机密性，且检查计算机信息网络系统运行状况，以及时发现与处理系统故障问题，保障系统运行稳定性，使其可在遭受攻击的状况下快速恢复正常。

二、数字化背景下计算机信息网络系统存在的安全问题

（1）环境危害。自然环境与社会环境均属于运行计算机信息网络系统运行的重要因素，且会破坏计算机网络体系结构。从自然环境的角度来看，旱涝、火灾、地震等问题的出现直接影响计算机信息网络系统运行安全性，且会造成其他网络安全问题的存在；从社会环境的角度来看，用户安全防范意识缺失、安全防范能力不足等因素的存在会威胁自身信息的安全性与完整性。除此之外，部分社会不法分子为谋求经济利益攻击计算机信息网络系统的行为，也会破坏计算机网络稳定运行。（2）黑客、病毒。数字化时代背景下，越来越多计算机技术人才涌现出来，但受到意识的影响，部分计算机技术人员会出现攻击计算机信息网络系统的行为，各区域计算机信息网络系统在运行中均可能会受到黑客攻击，出现安全问题，黑客攻击行为还设计木马病毒植入等操作，严重威胁企业及各单位组织数据信息的安全性。（3）信息共享危害。数字化技术与信息化技术的发展促使人们在日常生活中应用计算机设备进行交流的次数更加频繁，此过程中，信息共享模式随之构建。大部分计算机终端与服务器均具有信息共享功能可为用户获取网络信息提供便捷，但是，共享信息构成中可能会出现黑客攻击网络信息安全的行为，从而岛主数据丢失、泄露问题出现，损害用户权益。（4）网络软件自身漏洞。在用户需求与数字化技术不断发展的背景下，网络软件类型更加方法，但是，网络软件应用难以满足计算机信息网络安全运行的需求，此类问题出现的根本原因在于，软件设计人员在工作中较为关注软件性能，而缺少对软件应用安全性的重视，且软件测试人员在工作中未能全面检查软件各方面性能，导致不符合网络安全要求的软件得到应用，从而威胁计算机信息网络稳定运行[1]。（5）网络信息管理力度不足。网络信息安全需要以互联网技术及健全信息管理制度为支撑，但是受到管理制度缺少等因素的影响，计算机信息网络系统运行可能会出现用户信息泄露等问题。

三、数字化背景下计算机信息网络系统安全管理策略

（一）计算机网络信息系统安全技术应用

（1）防火墙技术应用。防火墙技术应用具有识别安全隐患问题的功能。在计算机网络信息系统安全管理工作中可应用防火墙技术，以优化信息安全建设效果，使计算机网络系统可自动限制身份识别失败的用户访问权限，以保护用户信息安全，且基于防火墙技术功能多样化的特点，网络安全管理人员可借助防火墙技术检测存在安全隐患问题的数据信息，以隔离有害数据与计算机信息网络系统内部相接触，从而保护用户信息安全性。同时，防火墙技术应用可有效抵御外界攻击，控制不良数据信息对整体计算机信息网络系统的影响，且该技术还具有自动识别功能，可破解带有伪装的攻击行为，以保护系统安全[2]。（2）反病毒技术应用。计算机病毒是影响计算机信息网络系统安全的重要因素。反病毒技术应用可实时检测计算机系统中是否存在网络病毒，以及时发现与控制病毒入侵行为，从实际应用来看，反病毒技术在计算机信息网络系统安全管理中的应用可特点在静态层面与动态层面两方面，静态层面中反病毒技术应用不能实现全程跟踪病毒轨迹的目标，难以及时发现与处理计算机信息网络系统运行存在的病毒。而动态层面反病毒技术应用可全面实时跟踪病毒轨迹，在检测到病毒后自动开启保护功能，以减少计算机信息网络系统运行安全问题的出现[3]。（3）数据加密技术应用。数据加密技术应用可以数据加密、密钥、身份验证等方式，提升数据信息安全性，此类技术常见应用形式为网站登录密码设置，而计算机信息网络系统安全管理中常见数据加密技术为非对称性数据加密技术，其可在设置独立加密密钥与解密密钥的基础上，避免用户通过算法违法获取计算机网络信息数据。

（二）网络秩序构建及重要信息备份

（1）构建规范网络秩序可约束用户在使用计算机过程中的行为，且可在保障用户自身信息安全性的基础上，优化用户体验感。用户是计算机网络信息系统组成的重要部分，因此，良好网络秩序构建也需要用户的积极参与。用户在日常操作计算机设备中需强化自身信息安全保护意识，自觉约束操作行为，以营造健康的网络环境，减少计算机信息网络系统出现安全问题的概率。相关部门也需积极参与网络秩序构建环节，以出台法律法规等方式，约束各类人员在信息网络系统中的操作行为，并以网络信息系统建设要求为依据落实安全执法活动，严格处罚威胁信息网络系统安全的人员与行为[4]。（2）重要信息备份。用户在登录计算机信息网络系统中需树立信息安全保护意识，主动备份重要信息，以减少信息泄露、数据丢失等问题对自身工作与生活的影响，且在虚拟技术不断发展的过程中，用户可通过虚拟空间对数据信息进行备份处理，例如，在云空间或网盘中备份数据，以提升计算机信息网络系统操作安全性。

（三）网络入侵检测系统设置

计算机信息网络系统安全管理是企业及各部门组织关注的重点问题，设置网络入侵检测系统可减少此类问题出现。（1）在设置网络入侵检测系统之前，相关技术人员需明确内部计算机信息网络系统安全管理对网络入侵检测系统的需求，且详细划分入侵系统中网络拓扑结构、网络流量类型、系统敏感性等要素的设计方案，以规范网络入侵检测系统布局，同时，综合考虑企业网络环境选择基于网络的入侵检测系统（NIDS）以实时检测企业内部计算机信息网络系统流量及潜在风险，且选择网络入侵检测系统解决方案中综合考虑网络系统性能、稳定性及可拓展性[5]。（2）优先在网络入口与敏感系统设置网络入侵检测系统，使其快速分

析网络系统流程，并以系统规则为依据，判断潜在入侵行为，此过程中系统规则制定需参考病毒、黑客等各类攻击行为特点。同时，技术人员需设计网络入侵检测系统日志记录功能，以深入分析安全事件问题出现的根本原因。（3）定期更新与维护网络入侵检测系统。定期更新与维护网络入侵检测系统可灵活应对网络攻击行为的变化。系统安全管理人员需定期更新规则集与软件补丁，在修复网络系统漏洞与更新网络系统安全隐患问题检测规则的基础上处理系统故障问题，同时，技术人员需定期检查网络入侵检测系统硬件装置与软件性能。（4）监测与响应入侵事件。网络入侵检测系统设置具有主动响应入侵事件的功能，在获取网络入侵检测系统所发出的预警信息后，管理人员需及时以隔离系统、封锁入侵者等方式，高效处理入侵事件。

（四）身份认证与访问权限控制

身份认证与访问控制是保障计算机信息网络系统安全的重要措施。（1）构建身份认证机制及访问控制机制。企业或组织可以识别用户名及密码、指纹、身份令牌等方式验证用户在登录计算机信息网络系统中真实身份，以限制非法用户系统访问权限，且企业需规划网络系统访问控制措施，详细划分不同等级用户可访问的数据资源，明确指出各用户在访问计算机信息网络系统中的权限与职责[6]。（2）加密敏感数据。企业或组织可借助高效加密算法对敏感数据存储与传输环节进行加密处理，以避免数据丢失及数据泄露问题的出现，此过程中，企业需结合数据保密需求选择 AES、RSA 等加密算法的应用[7]。（3）建立审计与监控机制。企业和组织需对计算机信息网络系统中用户登录行为、访问行为等进行监督，将用户登录信息、注销信息、操作信息、数据访问信息等行为及时记录下来，从而在分析用户异常行为的基础上发现与处理系统潜在安全隐患。（4）加强用户培训。企业可定期组织用户参与培训活动，使其深入了解密码安全、计算机信息网络安全隐患等内容，且培训用户抵御网络攻击的能力，以保障计算机信息网络系统运行安全性[8]。

（五）加强物理安全防护

加强物理安全防护可有效减少自然环境及人为因素对计算机信息网络系统安全的影响。技术人员需定期检查计算机系统运行环境湿度状况与火灾隐患，且在计算机区域设置消防系统，以减少设备操作中安全问题的出现。同时，相关部门可在计算机设备运行区域安装自动报警装置，以便技术人员发现与处理系统运行环境中存在的安全隐患问题，并借助具有防火性能的材料在该区域设置相应防火隔离装置，以保护计算机网络信息系统完整性[9]。除此之外，技术人员还可以安装监控设备、湿度温度控制系统、防静电装置等方式，避免计算机信息网络系统受到运行环境影响出现安全事故问题[10]。

结语：

综上所述，数字化背景下计算机信息网络系统安全与人们生产生活联系更加密切，企业及各组织机构需深入探究数字化背景下计算机信息网络系统安全管理措施，从安全技术应用、网络秩序构建、重要信息备份、身份认证与访问权限控制、物理安全防护强化等多角度入手，减少计算机信息网络系统安全问题的出现，推动数字化技术与信息化技术的持续发展。

参考文献：

[1] 朱清臣. 计算机网络信息系统安全问题及相关建议［J］. 数字技术与应用，2023, 41 (05): 218-220. DOI
[2] 叶家骏. 计算机网络信息系统安全问题的分析与对策［J］. 网络安全技术与应用，2023, (02): 8-10.
[3] 陈柯. 医院计算机网络信息系统面临的安全问题及防范对策［J］. 信息记录材料，2021, 22 (07): 47-48. DOI
[4] 黄明毅. 数据时代医院计算机网络信息系统的安全分析［J］. 产业创新研究，2021, (12): 32-34.
[5] 李选超. 事业单位计算机网络信息系统存在安全问题及对策［J］. 电子技术与软件工程，2021, (08): 257-258.
[6] 孙苗. 计算机网络安全管理技术在医院中的应用［J］. 集成电路应用，2021, 38 (02): 120-121. DOI:
[7] 黄烁. 大数据时代医院计算机网络信息系统的安全分析［J］. 中国新通信，2020, 22 (19): 139-140.
[8] 王林. 大数据和智能控制技术在计算机网络信息安全系统中的应用［J］. 集成电路应用，2024, 41 (04): 292-293. DOI
[9] 王晴怡. 计算机网络中涉密信息系统安全控制研究［J］. 信息与电脑（理论版），2023, 35 (23): 193-195.
[10] 邹易奇. 涉密计算机信息系统网络安全监控技术的运用［J］. 科技与创新，2023, (19): 168-170. DOI