探究电子计算机的信息数据安全

赵 刚
兴安盟大数据中心 内蒙古 乌兰浩特 137400

摘 要：电子计算机信息数据安全是当代信息社会面临的重要课题。本文深入探讨了电子计算机信息数据安全的关键问题，包括木马病毒攻击、网络黑客攻击、计算机系统漏洞等方面，分析了现有安全措施的不足，并提出了加强信息数据管理的策略，旨在提高电子计算机信息数据的安全性和可靠性。通过综合研究与实践，为信息数据安全领域的发展提供了有益的参考和启示。

关键词：电子计算机；信息数据；安全

引言：信息技术的迅猛发展，为各行各业带来了无限机遇。然而，电子计算机的广泛应用也带来了信息数据安全问题，对行业发展产生着深远影响。在新时代背景下，我们必须采取合理、科学的方法，强化信息数据管理，确保数据的安全性。这不仅是保障各行业稳定发展的基石，更是推动社会进步的重要保障，加强电子计算机信息数据安全管理，对于促进各行业健康、可持续发展具有重要意义。

1 信息数据安全概述

在信息化、数字化的时代大潮中，电子计算机的信息数据安全已经变得尤为重要。它不仅关乎个人隐私保护，更影响到企业竞争力和国家安全稳定，因此必须高度重视并加强防范。信息数据安全，是指保护信息免受未经授权的访问、使用、泄露、破坏、修改或销毁的一系列措施和方法。这些信息可能包括个人身份信息、财务数据、商业机密等，其安全性和完整性对于个人、组织乃至国家都具有举足轻重的意义。信息数据安全的重要性在于其直接关系到个人权益、企业利益和国家安全。一旦信息数据泄露或被篡改，可能导致个人隐私被侵犯、企业竞争优势丧失、甚至国家安全受到威胁。因此，加强信息数据安全防护，防止数据被非法获取或滥用，已经成为当今社会亟待解决的问题。电子计算机作为信息存储、处理和传输的主要工具，其信息安全问题尤为突出[1]。计算机系统的漏洞、网络攻击、恶意软件、内部人员泄密等因素都可能对信息安全构成威胁，信息数据安全的防护与应对措施包括但不限于：加强物理安全防护，如机房安全、设备安全等；提升网络安全防护能力，如防火墙、入侵检测系统等；采用数据加密技术，保护数据的机密性和完整性；建立完善的安全管理制度，明确安全责任和义务；加强人员安全意识和技能培训，提高整体防范水平。电子计算机的信息数据安全是一个复杂而重要的问题，需要我们从技术、管理、人员等多个方面进行综合考虑和应对。

2 现存的信息数据安全主要问题

2.1 网络黑客攻击造成的信息数据安全隐患

在电子计算机信息数据安全领域，网络黑客攻击无疑是一个不容忽视的威胁。黑客，作为网络安全的反面角色，利用各种技术手段，对计算机系统、网络设施及信息数据进行非法访问、窃取、篡改或破坏，从而给个人、组织乃至国家带来巨大损失。网络黑客攻击的手段多种多样，包括但不限于：利用系统漏洞进行渗透攻击，通过钓鱼网站、恶意软件等方式窃取用户敏感信息，实施DDoS攻击导致网络服务瘫痪，以及通过社交工程手段诱骗用户泄露关键信息等。这些攻击手段不仅技术性强，而且隐蔽性高，往往让受害者防不胜防。网络黑客攻击对信息数据安全造成的隐患主要表现在以下几个方面：第一，黑客攻击可能导致敏感信息的泄露。这些信息一旦被泄露，就可能被用于非法活动，如身份盗窃、金融诈骗等，给受害者带来严重的经济损失和信用危机。第二，黑客攻击可能破坏数据的完整性和可用性。黑客可能通过篡改数据、删除文件或制造网络故障等手段，破坏数据的完整性和可用性，导致企业业务中断、服务瘫痪等严重后果。第三，黑客攻击还可能对受害者的声誉造成负面影响。一旦企业或个人遭受黑客攻击，其信息安全能力将受到质疑，可能导致客户流失、合作伙伴信任度下降等连锁反应。

2.2 计算机系统漏洞造成的信息数据安全隐患

在信息化社会中，计算机系统是信息数据存储、处理和传输的核心。然而，计算机系统本身并非完美无缺，其存在的漏洞往往成为黑客和恶意攻击者利用的目标，进而引发严重的信息数据安全隐患。计算机系统漏洞是指系统中存在的安全缺陷或弱点，这些漏洞可能源

于系统设计的不完善、编码错误、配置不当等多种原因。黑客和攻击者往往能够利用这些漏洞，绕过系统的安全防护机制，实现对系统的非法访问和操控。漏洞可能导致敏感信息的泄露，攻击者通过利用漏洞，可以获取系统中的敏感数据，如用户密码、财务数据、商业机密等。这些信息的泄露不仅会对个人和企业造成直接的经济损失，还可能引发更严重的社会后果。漏洞可能被用于实施恶意攻击，攻击者可以利用漏洞植入恶意代码，如病毒、木马等，对系统进行破坏或窃取数据。这些恶意攻击可能导致系统崩溃、数据丢失或业务中断，给企业和个人带来巨大损失[2]。计算机系统漏洞还可能成为拒绝服务攻击的源头，攻击者可以利用漏洞发起大量无用的请求，使系统资源耗尽，导致正常用户无法访问系统。

2.3 木马病毒攻击造成的信息数据安全隐患

在信息化社会中，木马病毒攻击是电子计算机信息数据安全面临的一大挑战。木马病毒是一种恶意软件，其名称源于“特洛伊木马”的典故，即表面看似无害，实则隐藏着破坏性的功能。木马病毒通过伪装成正常程序或文件，诱骗用户下载并执行，进而在受害者的计算机系统中潜伏并执行恶意操作，造成严重的信息数据安全隐患。木马病毒攻击对信息数据安全带来的隐患不容忽视。（1）木马病毒能够窃取用户的敏感信息。一旦木马病毒侵入系统，它会潜伏在后台，监视用户的键盘输入、网络活动等信息，并将这些敏感数据收集起来，发送给黑客或恶意攻击者。这些敏感数据包括个人身份信息、银行账号、密码等，一旦被窃取，将可能导致严重的财务损失和隐私泄露。（2）木马病毒能够破坏系统的正常运行。木马病毒在感染系统后，会占用系统资源，导致计算机运行缓慢、卡顿甚至崩溃，木马病毒还可能对系统文件进行篡改或删除，破坏系统的正常功能，使受害者无法正常使用计算机和其中的数据。（3）木马病毒还可能成为黑客远程控制受害者计算机的工具。黑客通过植入木马病毒，可以在受害者不知情的情况下，远程操控其计算机，执行各种恶意操作，如查看文件、下载数据、执行命令等。这种远程控制行为不仅侵犯了用户的隐私和权益，还可能被用于实施更复杂的网络攻击和犯罪行为。

3 保护计算机信息数据安全的防护与应对措施

3.1 防火墙技术的运用

在保护计算机信息数据安全的过程中，防火墙技术是一项至关重要的防护措施。防火墙如同计算机系统的“守门员”，它站在网络的前端，对进出的网络流量进行严格的审查和过滤，确保只有符合安全策略的数据包才能通过。防火墙技术的核心功能在于其包过滤机制，通过对数据包进行逐一检查，根据预设的规则集，判断数据包是否允许通过。这些规则集可以基于源地址、目标地址、端口号、协议类型等多种因素进行定义，从而实现对网络流量的精细化控制。除了基本的包过滤功能外，现代防火墙还具备了更为复杂和高级的安全特性。例如，状态检测防火墙能够跟踪网络连接的状态，并根据连接的状态动态调整安全策略，从而提高防护的精准性和灵活性。此外，防火墙还可以与入侵检测系统（IDS）和入侵防御系统（IPS）等安全设备联动，共同构建多层次的安全防护体系。在运用防火墙技术时，我们需要注意以下几点：第一，合理配置防火墙规则是关键。规则设置过于宽松可能导致安全隐患，而过于严格则可能影响正常业务的开展，我们需要根据实际应用场景和安全需求，仔细规划并测试防火墙规则，确保其既能有效阻止恶意流量，又不会对正常业务造成干扰。第二，定期更新和维护防火墙也是必不可少的。随着网络攻击手段的不断演变，防火墙需要及时更新其规则和特征库，以应对新的安全威胁，我们还需要定期对防火墙进行巡检和维护，确保其处于最佳工作状态。第三，防火墙技术虽然强大，但并非万能。它只能在一定程度上降低安全风险，而不能完全消除风险，在运用防火墙技术的同时，还需要结合其他安全措施，如数据加密、访问控制等，共同构建全面的信息数据安全防护体系。

3.2 应对安全事件与威胁

在保护计算机信息数据安全的过程中，应对安全事件与威胁是一项至关重要的任务。随着信息技术的飞速发展，网络安全威胁也日趋复杂和多样化，因此，我们需要采取一系列有效的措施来应对这些安全事件与威胁。建立完善的安全事件应急响应机制是应对安全事件的基础，这一机制应包括明确的安全事件分类、等级划分、处置流程以及应急响应团队的组织架构和职责分工。当发生安全事件时，应急响应团队能够迅速启动预案，按照流程进行处置，及时控制事态发展，减轻损失。加强安全监控和日志分析是发现安全威胁的重要手段，通过部署网络监控设备、安全审计系统等工具，我们可以实时监控网络流量、系统日志等信息，及时发现异常行为和潜在威胁，对日志数据进行深度分析，可以挖掘出攻击者的行为模式、攻击路径等信息，为应对威胁提供有力支持。定期进行安全漏洞扫描和风险评估也是应对安全威胁的关键环节，通过扫描系统漏洞、弱口令等问题，我们可以及时发现并修复潜在的安全隐患，

提高系统的安全防护能力，对系统进行风险评估，可以了解系统的安全状况，为制定针对性的安全防护策略提供依据。在应对安全事件与威胁的过程中，加强人员安全意识教育和技能培训也至关重要。只有提高人员的安全意识，使他们了解并掌握基本的安全防护知识和技能，才能更好地防范和应对各种安全威胁。保持与相关安全组织和机构的沟通与合作也是应对安全事件与威胁的有效途径。

3.3 加强物理安全防护

在保护计算机信息数据安全的过程中，物理安全防护是不可或缺的一环。物理安全防护主要指的是对计算机硬件、存储设备以及整个数据中心进行的实体保护，以防范物理层面的安全威胁。要确保计算机硬件和存储设备的安全，这包括采取适当的防盗措施，如安装门禁系统、监控摄像头等，以防止未经授权的物理访问，对于重要的硬件设备，如服务器、路由器等，应进行定期巡检，确保其完好无损，防止被恶意破坏或篡改。数据中心的物理安全也至关重要，数据中心作为信息数据存储和处理的核心区域，其安全状况直接关系到整个信息系统的安全，必须采取严格的出入管理制度，限制人员进出，并对进出人员进行身份验证和记录。此外，数据中心还应具备防火、防水、防雷击等防护措施，以应对自然灾害等不可抗拒因素带来的安全风险。除了硬件和数据中心的安全防护外，加强物理环境的监控也是物理安全防护的重要方面。通过部署环境监控系统，可以实时监测数据中心的温度、湿度、烟雾等环境参数，及时发现异常情况并采取措施进行处理。这不仅可以保护硬件设备免受环境因素的影响，还能提高整个信息系统的稳定性和可靠性，定期进行物理安全检查和评估也是加强物理安全防护的重要手段。

3.4 提高计算机的信息数据管理水平

在信息化社会中，计算机信息数据的安全管理对于保障组织的正常运营、维护用户隐私以及防范潜在风险具有重要意义，提高计算机的信息数据管理水平成为一项紧迫而重要的任务。组织应制定一套科学、合理的数据管理制度，明确数据的收集、存储、处理、传输和销毁等各个环节的规范和标准，要确保制度得到有效执行，对违反规定的行为进行严肃处理，从而建立起严格的数据管理秩序。对于不同级别和敏感度的数据，应采取不同的保护措施。例如，对于机密数据，应使用加密技术进行存储和传输，同时限制访问权限，确保只有授权人员能够访问，还应定期对数据进行备份和恢复测试，以防止数据丢失或损坏[3]。除了采用防火墙、入侵检测等网络安全技术外，还应加强终端安全管理，如使用安全软件、定期更新操作系统和应用程序等，要对员工进行安全教育和培训，提高他们的安全意识和防范能力，从而构建起全方位、多层次的数据安全防护体系，建立数据审计与监控机制也是提高信息数据管理水平的有效手段。通过对数据的使用情况进行审计和监控，可以及时发现异常行为和潜在风险，并采取相应的措施进行处理。这有助于确保数据的合法、合规使用，防止数据泄露和滥用。

结语

总之，随着信息技术科技的发展，为各行各业带来了无限机遇，电子计算机的广泛应用也带来了信息数据安全问题，对行业发展产生着深远影响。在新时代背景下，我们必须采取合理、科学的方法，强化信息数据管理，确保数据的安全性。这不仅是保障各行业稳定发展的基石，更是推动社会进步的重要保障。因此，加强电子计算机信息数据安全管理，对于促进各行业健康、可持续发展具有重要意义。

参考文献

[1]叶华雄.大数据下计算机网络信息安全与防护分析[J].中国科技信息,2020(12):52-53.

[2]衡立业.数据加密和异常数据自毁技术在网络信息安全中的研究[J].网络安全技术与应用,2020(06):35-36.

[3]杨鑫源,毕文静,苏艺铄.大数据时代背景下财产隐私安全存在的问题及其对策分析[J].价值工程,2020,39(15):210-212.