

基于网络信息安全技术管理的计算机应用

崔景

襄阳汽车职业技术学院 湖北 襄阳 441000

摘要: 基于网络信息安全技术管理的计算机应用,指的是借助网络安全技术,对计算机应用进行监管、管理和保护。主要涉及入侵检测、防火墙、数据加密、虚拟专网等技术,可以预测和防范各种攻击和安全威胁,保障计算机应用的安全和稳定。该应用在互联网时代显得尤为重要,是保护信息安全和推进社会数字化转型的关键之一。

关键词: 网络信息安全; 技术管理; 计算机应用

引言:随着计算机技术的飞速发展,人们越来越依赖计算机以及与之相关的网络技术,在各个领域中应用也愈发广泛。然而,这也带来了一系列的网络安全问题,如黑客攻击、病毒侵袭、数据泄露等等,这些安全问题不仅损害了个人和机构的利益,更可能对整个社会带来严重的影响。因此,基于网络信息安全技术管理的计算机应用尤为重要。

1 计算机应用的概念

计算机应用是指利用计算机及其相关技术,对人类生活和各个领域的工作进行科学化、智能化、信息化处理,提高生产效率或解决人们日常生活中的各类问题的一种技术手段。计算机应用包括各种领域,如教育、医疗、金融等等。计算机应用以其高速度、高效率的特点,带来了极大的方便和便捷^[1]。例如,在医疗领域中,计算机应用可以帮助医生更精准地判断病情、更加详细地记录病人信息、更加方便的查阅病例等等。在金融领域中,计算机应用可以帮助银行实现网络支付、移动支付等等便捷的服务。

2 网络信息安全技术管理的概念

网络信息安全技术管理是指企业或组织对其网络设备、网络安全技术、网络设备申请、外部网络通讯安全、网络维护与监控等方面进行规范化、专业化、高效化管理的过程。它是通过专业的技术手段、标准的管理规范以及完备的安全策略来保障网络信息安全的一种综合性的管理方式。在网络时代,网络信息的安全性问题日益凸显。为保障网络信息的安全性,在组织的网络信息安全管理中,网络信息安全技术管理体系以其高效性、实用性、适应性等优势特点成为网络安全防范系统中的重要组成部分^[2]。

3 网络信息安全技术管理的应用方式

3.1 建立完备的网络安全技术管理体系

现代化的经济活动越来越向网络化、智能化、信息

化方向发展,企业和组织对于网络安全技术管理的需求也越来越迫切。建立完备的网络安全技术管理体系是保障网络信息安全的重要手段。网络安全技术管理体系是指企业或组织对网络安全技术、网络设备申请、外部网络通讯安全、网络维护与监控等方面进行规范化、专业化、高效化管理的过程。一个完备的网络安全技术管理体系应包括以下几个方面:首先,企业和组织应建立健全的安全管理制度和流程,如安全策略、安全标准、安全程序、安全手册等。这些制度和流程可以让企业和组织全面了解网络安全的重要性和技术要求,同时也可以规范员工的行为,减少不必要的风险。其次,企业和组织应加强对网络设备、网络通讯和数据传输等方面的管理。通过规范网络设备的安装、调试、维护和更新等各个环节来有效保证网络安全^[3]。企业和组织应使用高质量的网络设备,及时升级和修补安全漏洞,进行备份和维护,保证网络安全设备的正常和高效运行。另外,企业和组织需要加强对员工的安全意识教育。员工是企业 and 组织信息安全的重要保障和最后防线,扮演着至关重要的角色。加强对员工的安全知识普及和培训,提高员工的防范意识和防御能力,就能够在关键时刻做出正确处理,有效抵御安全威胁。最后,企业和组织应建立完善的安全响应机制,在遇到网络安全事件时,组织专业的安全人员和部门进行急救措施,快速排查和解决网络安全问题,以减少安全事故的影响和损失。同时,可以进行安全事件的分析、总结和修正,不断提高防范和应对能力。建立完备的网络安全技术管理体系对于来源于各个领域的企业和组织都至关重要。通过建立规范化、专业化、高效化的网络安全技术管理体系,可以提高网络信息的安全性和稳定性,保护企业和组织的信息系统,促进企业和组织的持续稳定发展。

3.2 加强人员培训

网络信息安全技术管理的应用方式主要包括管理机

制和技术手段两方面^[1]。其中管理机制主要着眼于规范人员行为,提高安全意识,制定规章制度等方面;技术手段则包括对网络设备、信息传输和数据存储等方面的技术方案的加强和优化。而在网络信息安全技术管理的过程中,加强人员的培训和教育也是至关重要的。因为在安全保障的整个过程中,保护人员的主观能动性和创造力是一个重要的方面。在员工安全培训计划中,必须保证培训的内容详实清晰,包括网络基础知识、安全意识、网络攻击和防御方法等。这些培训内容既可以教授基本的安全技术知识,提出安全风险的预防和应对方法,同时也可以增强员工的安全意识,使员工从内心深处认识到网络安全的重要性。加强人员的培训还包括提高技术水平和专业素养。网络安全领域更新换代的速度很快,承载网络安全的技术和服务演化也十分迅猛。因此,持续不断的培训和学习无疑是必不可少的。加强人员的培训还包括与员工个人实际相结合,从实践中发现问题,着手解决问题。在实际的安全事件中,通过总结教训,分析原因并且提出应对策略,让员工切实理解到安全事件的实际影响和威胁,提高员工主动学习和创新的能力。加强人员培训在网络信息安全技术管理中非常关键,能够避免单纯的靠技术手段而忽视员工作用的情况出现。因此推广安全文化、加强培训中与员工个人实际相结合以及建立技术和经验分享平台,都是有效提高网络信息安全管理的企业和组织的安全性和稳定性的关键^[2]。

3.3 加强入侵检测与防范

网络信息安全技术管理的应用方式中,加强入侵检测和防范是非常重要的部分。随着互联网技术和应用的不断普及,网络攻击和安全威胁也愈加猖獗和复杂,严重威胁着企业和组织的安全和业务连续性。因此,加强入侵检测和防范已经成为了网络信息安全技术管理中需要高度重视的问题。加强入侵检测和防范需要遵循四个基本的原则,即全面、深入、准确和及时性。全面意味着需要对不同网络层面进行检测和防范,从网络设备到操作系统以及应用服务,进行全方位的覆盖照顾。深入意味着需要深入到代码层面、用户行为逻辑,对可疑行为进行详尽的分析和鉴定。准确度则包括通过安全基线配置、历史数据分析等方式提高检测精度。及时性则强调通过实时监测和预警的方式,避免一旦发现漏洞,及时进行修复和响应。在具体操作上,加强入侵检测和防范可以采用多种技术手段。其中比较常见的方式包括使用安全设备,如防火墙、入侵检测系统等设备,提高网络流量的可视化,早期发现各种网络漏洞和攻击行为。此外,还可以使用安全监测软件,如网络扫描和利

用工具、日志跟踪和异常监测系统等。这些工具可以帮助管理员轻松地发现线上网络漏洞和问题,及时解决和修复。在防范网络安全事故的过程中,最重要的是加强对人员和员工的教育和培训。员工不良行为或不慎的失误,往往是内部网络安全漏洞的主要来源。因此,通过丰富的安全培训和教育计划,提高员工对于网络安全的认识,让员工真正成为安全防范的最后一道防线,对于提升网络安全保障水平,具有积极的意义和作用^[3]。加强入侵检测和防范是网络信息安全技术管理中需要充分重视的问题。只有采取一系列科学和有效的措施,对可预见的风险展开全面的分析、及时准确地发现并解决,才能有效地保护网络安全、确保企业和组织信息技术的快速、可靠、可持续的发展。

3.4 强化网络设备安全管理

网络设备是连接公网和内网的桥梁,能够在多个系统间传输数据和信息,因此保护网络设备的安全,对于整个网络的安全保障具有重要的作用。针对日益复杂的网络威胁和攻击,网络信息安全技术管理需要强化网络设备的安全管理,以提高网络安全防范能力和保障网络的稳定性。网络设备需要进行安全全面的安全保护,包括对网络设备进行加固,配置更安全的管理密码和用户权限;为网络设备安装安全软件,包括入侵检测系统等;加强对网络设备的管理和监控,提高发现漏洞和安全隐患的效率;以及定期对网络设备进行安全检查和应急演练,以增强网络设备安全的可靠性^[1]。网络设备的安全管理需要采取多层次的保护措施。在管理过程中,应该采取分层管理、权限控制等有效方法,确保网络设备的安全性。在设备硬件上,可以通过外链加密设备、防火墙等手段对网络设备进行安全加固。同时,在网络拓扑结构上,也可以采用隔离技术来防止入侵和恶意攻击造成的连锁反应和扩散。加强对网络设备的安全管理,也需要充分考虑到人员因素。网络设备管理人员是关键的角色,他们需要高度认识和理解网络安全保障的重要性。在网络设备管理人员的招聘和培训过程中,需要制定相应的管理规章制度、技术标准,加强对设备管理人员的培训和实践,从而提高管理人员的安全意识和应急处置能力。网络设备安全管理还需要定期进行漏洞扫描和弱点补丁修复,以增强网络设备的安全稳定性。此外,也需要加强对网络设备安全漏洞的跟踪和研究,避免新漏洞或新威胁的发生,从而提高网络信息安全技术管理的保障水平。加强网络设备的安全管理,可以有效降低网络安全风险,提高网络安全防范能力,保证用户的信息安全,对于企业和组织的可持续发展和运营安全

来说,具有重要的战略意义。

4 常见的网络安全技术管理措施

4.1 网络加密技术

网络加密技术是一种常见的网络安全技术管理措施,它通过加密算法对网络数据进行加密,保证数据在传输过程中不被窃取、篡改或者破坏^[2]。网络加密技术主要包括对称加密和非对称加密两种方式。对称加密是一种加密方式,使用单一的密钥同时进行加密和解密,加密速度较快,适用于大规模数据的加密和传输。而非对称加密则需要一对密钥,即公钥和私钥,公钥用于加密,私钥用于解密,其安全性更高,适用于数据安全性要求较高的场合。此外,网络加密技术还包括数字签名技术,用于验证数据的完整性和真实性。网络加密技术在网络通信和数据存储中得到广泛应用,能够有效保护数据隐私,防止黑客攻击和泄漏,最大化保障信息的安全性。随着网络攻击和黑客入侵技术的不断升级,网络加密技术也将会不断发展和完善,进一步提高网络安全水平,并成为保障数据安全的重要手段之一。

4.2 防火墙技术

网络安全技术管理措施包括完善的网络安全策略、加密技术、入侵检测、安全防御和安全培训等。其中,防火墙技术是最基本,也是最重要的一种网络安全技术管理措施之一。防火墙技术通过将网络分割成不同的区域,设置不同层次的安全策略,将网络连接和通信对不需要访问网络的用户进行阻拦和限制,从而达到保护网络安全的目的^[3]。防火墙技术基于网络层、传输层和应用层等多个层次的安全控制,通过各种安全策略和规则进行过滤和限制,防止未经授权的用户和敌对的恶意攻击者进入网络。常见的防火墙技术包括有包过滤、状态检测、代理服务 and 网络地址转换等。防火墙技术可以提高网络安全性,有效预防网络攻击行为,同时也能够监控和记录网络行为,发现并及时处置安全漏洞和攻击行为。

4.3 入侵检测技术

入侵检测技术是一种常见的网络安全技术管理措施,其通过实时监视网络活动,检测异常行为来及时预警并防御各种威胁和攻击。它可以基于签名、行为或异

常等方式进行检测,在网络和主机上实现全面和可靠的监控,可以非常有效地帮助企业 and 组织保护其信息系统和数据安全。随着网络安全威胁不断增加,入侵检测技术也不断发展和完善,未来将会更加智能化和自适应,可以有效解决各种网络攻击,从而使网络安全得到更加充分和全面的保障,也为企业和组织提供了更加强大的安全支撑^[1]。

4.4 安全审计技术

安全审计技术是一种常见的网络安全技术管理措施,它通过收集、分析和监视网络安全活动,包括用户访问、系统配置和网络传输等行为,来检测安全漏洞、异常活动并提高系统安全性。其中,安全审计技术主要包括主机审计和网络审计两种方式,主要从日志和事件数据中提取有用的信息,了解系统进程,检测安全事件,通过分析,找出潜在的安全问题。安全审计技术在企业和政府等组织中得到广泛应用,能够有效帮助管理员发现并处理不当使用、未经授权访问、数据泄露等违规行为,及时禁用账号并进行数据备份,从而保障网络数据的基本安全。随着网络安全威胁的不断升级和变异,安全审计技术对于提高网络安全和保护关键信息仍然具有重要的作用,并将会随着技术的发展而进一步完善和提高效能^[2]。

结语

随着计算机应用的广泛普及,企业和组织应该加强对网络安全技术管理的重视,并采取各种措施提高信息系统的安全性。本文着重讲述了网络信息安全技术管理在计算机应用中的重要性,并探讨了计算机应用中网络信息安全技术管理的应用方式。

参考文献

- [1]刘铭.网络信息安全技术管理视角下的计算机应用[J].网络安全技术与应用,2022,(03):175-176.
- [2]吴海威.基于网络信息安全技术管理的计算机应用分析[J].无线互联科技,2021,18(07):31-32.
- [3]迟江波.基于网络信息处理及安全的计算机应用[J].数字通信世界,2020(6):2.