企业计算机网络系统安全问题分析

滕启艳
国网山东省电力公司莒南县供电公司　山东　临沂　276600

摘　要：在当今的商业环境中，企业计算机网络系统不仅是企业运营的关键支撑，更是企业与外部世界沟通的桥梁。随着数字化转型的加速，许多企业的核心业务和重要数据都集中在这一系统中。这意味着一旦网络系统遭受攻击或出现故障，可能会对企业的日常运营、客户关系管理、供应链合作等造成巨大的影响。正因如此，确保企业计算机网络系统的安全变得至关重要。但与此同时，网络环境中的威胁和挑战也在不断演变，使得企业计算机网络系统的安全防护工作变得更加复杂和迫切

关键词：计算机网络系统；安全问题；应用措施

引言：随着网络技术的不断演进和黑客攻击手段的日益复杂，企业计算机网络系统面临着越来越多的安全威胁和挑战。这些威胁可能来自外部的恶意攻击、内部的误操作、软件漏洞或是物理环境的安全问题等。因此，本文对企业计算机网络系统的安全问题进行深入分析，并探讨相应的应对策略，对于保障企业的稳定发展和信息资产的安全具有至关重要的意义。

1 企业计算机网络系统安全的重要意义

在当今信息化时代，计算机网络系统已经成为企业运营不可或缺的组成部分。然而，随着网络技术的迅猛发展，网络安全问题也日益凸显。因此，企业计算机网络系统的安全对于企业的稳定发展和信息安全具有重要意义。首先，企业计算机网络系统安全保障了企业的正常运营。企业的日常运营涉及大量的数据传输、处理和存储。一旦计算机网络系统遭到攻击或出现故障，可能会导致数据泄露、系统瘫痪、业务中断等严重后果，给企业带来巨大的经济损失。因此，维护计算机网络系统的安全是确保企业正常运营的必要条件。其次，企业计算机网络系统安全有助于保护企业的核心竞争力[1]。许多企业的重要信息，如客户数据、产品研发资料、财务信息等，都存储在计算机网络系统中。一旦这些信息被非法获取或篡改，将对企业造成重大损失。因此，计算机网络系统的安全对于保护企业的核心竞争力至关重要。此外，企业计算机网络系统安全有利于提升企业的形象和信誉。企业的网络安全状况往往会被客户、合作伙伴等关注。一个遭受网络攻击或存在安全隐患的企业，很容易失去公众的信任，影响其品牌形象和市场地位。因此，维护计算机网络系统的安全对于提升企业的形象和信誉具有重要意义。

2 企业计算机网络系统安全存在的问题

2.1 内部人员使用不规范

内部人员使用不规范是导致IT系统出现问题的主要原因。在日常工作中，一些员工可能会采取一些不正确的操作习惯，这可能会导致计算机设备的安全风险和性能问题。首先，不等计算机完全关闭就关闭UPS电源是一个常见的问题。这种做法可能会导致计算机设备出现损坏或数据丢失的问题。因为计算机在运行过程中，硬盘还在高速旋转，如果突然断电，可能会导致硬盘损坏，数据丢失。其次，在多机上使用U盘、活动硬盘拷贝文件而不注意杀毒也是一个不可忽视的问题。由于U盘、活动硬盘等存储设备是病毒传播的主要途径之一，如果不进行安全检查或杀毒处理，就可能在拷贝文件的过程中将病毒引入计算机系统。这不仅可能导致系统运行缓慢或出现故障，还可能泄露公司机密或客户信息。此外，有些用户在计算机设备上随意安装软件也是一个常见的问题。

2.2 操作系统不能及时升级

操作系统作为计算机的核心软件，承担着管理计算机硬件和应用程序的重要职责，并为它们提供服务。然而，由于操作系统的复杂性，不可避免地存在一些缺陷和漏洞，这为黑客利用这些漏洞植入木马、病毒等恶意程序提供了机会，从而威胁到计算机的安全，可能导致机密信息的泄露或系统的损坏。对于企业而言，保护内网安全至关重要。但现实中，内网的操作系统经常无法及时升级，这为内网安全带来了潜在的风险。一方面，企业可能担心升级会影响现有系统的稳定性和兼容性，从而避免进行升级。另一方面，企业的内网规模可能较大，升级操作系统需要耗费大量时间和人力，因此无法及时完成。此外，一些企业可能对操作系统漏洞的认知不足，缺乏足够的重视，导致不能及时发现和修复漏洞。同时，一些企业的安全管理制度可能不完善，缺乏对操作系统升级的规范和监督，导致升级工作不能及时

进行。

2.3 软件存在安全漏洞不能得到及时修补

软件是计算机的重要组成部分，它负责执行各种任务和功能，为人们的工作和生活提供便利。然而，由于软件的复杂性和规模庞大，它也存在着一定的缺陷和漏洞。这些缺陷和漏洞可能被黑客利用，通过植入恶意代码等方式攻击计算机，窃取机密信息或者破坏系统。对于企业而言，应用软件的安全至关重要。但是，由于种种原因，一些软件的安全漏洞不能得到及时修补。一方面，一些编程人员对于软件安全性的重视程度不够，导致软件中存在缺陷和漏洞。另一方面，一些软件是第三方开发的，企业可能缺乏对软件的掌控力，无法及时发现和修复漏洞。此外，一些软件中可能存在“后门”，这是编程人员为了自便而设置的。这些“后门”可能被黑客利用，导致企业信息泄露或系统崩溃。同时，一些企业的安全管理制度可能不完善，缺乏对软件安全的规范和监督，导致安全漏洞不能及时修复。

2.4 网络结构漏洞引发攻击入侵

网络结构是整体设计构思的参考，用于开放系统互联通信系统。它是一个复杂的结构系统，通常企业的网络与外部网络相连接。建筑企业部门众多，网络覆盖面广，应用广泛，因此面临的风险和威胁也大。网络结构漏洞可能会引发攻击入侵。很多入侵者利用外部网络结构的缺陷侵入到企业内部网络结构中，进行不法活动。一旦外部网络结构受到攻击，与之连接的所有单位的网络都有被入侵的危险。许多企业的管理者缺乏防范意识，办公系统未安装安全防护软件，安全措施不到位。一些不法分子利用企业内部网络结构的漏洞进行入侵攻击，造成企业电脑无法正常工作。企业内部只要有一台电脑被入侵，其他电脑也会受到影响，企业的各种信息数据容易被盗取，不利于企业安全管理。

2.5 网络应用不当致使信息泄露

网络应用已经成为了现代企业不可或缺的一部分，为企业带来了巨大的便利和价值。然而，在进行网络应用时，如果不具备计算机应用基本知识和网络安全的相关知识，就可能会因为操作不当而引发各种风险，其中最常见的就是信息泄露[2]。对于建筑企业来说，工程资料、数据、客户信息等都是至关重要的商业机密，关系到企业的可持续发展。在网络应用过程中，如果员工没有掌握正确的操作方法，很容易因为误操作而导致数据泄露或被篡改。网络病毒也是一个巨大的威胁。它们传播速度极快，危害巨大，能够在短时间内感染大量的计算机。有些不法分子甚至在网络上投放病毒，导致电脑死机、文件丢失、信息泄露等严重后果。这些不当的网络应用都会给企业带来巨大的损失和不利影响。

3 企业计算机网络系统安全的重要措施

3.1 制定和执行网络安全策略

制定和执行网络安全策略是企业保护网络系统安全的重要措施。企业需要制定详细的网络安全策略，包括访问控制、数据加密、备份和恢复等措施，以确保网络系统的安全性和可靠性。首先，访问控制是网络安全策略的核心。企业应该对网络系统进行严格的访问控制，限制对敏感数据的访问权限。只有经过授权的人员才能访问相应的数据和资源，防止未经授权的人员获取敏感信息。其次，数据加密是保护数据安全的重要手段。通过数据加密，可以确保数据在传输和存储过程中的机密性和完整性。企业应该对敏感数据进行加密处理，以防止数据被窃取或篡改。此外，备份和恢复也是网络安全策略的重要组成部分。企业应该定期备份重要数据，并确保备份数据存储在安全可靠的地方。在发生安全事件或数据丢失时，可以快速恢复数据，降低损失。

3.2 安装和更新防病毒、防间谍软件

安装和更新防病毒、防间谍软件是保护企业网络系统免受恶意软件攻击的另一个重要措施。防病毒软件和防间谍软件可以检测、清除恶意软件，防止企业网络系统被攻击和感染。首先，企业应该选择可靠的防病毒和防间谍软件供应商，并安装适合企业网络系统的软件版本。在安装完成后，应该及时更新软件病毒库和定义规则，以确保软件能够抵御最新的病毒和间谍软件。其次，企业应该制定定期更新计划，及时更新防病毒和防间谍软件，以确保软件始终处于最新状态。在更新过程中，应该遵循供应商的指导说明进行操作，避免因为不当操作导致更新失败或安全风险[3]。此外，企业还应该定期进行全面扫描和实时监控，检测网络系统中的病毒和间谍软件。在发现可疑文件或行为时，应该及时进行清除和隔离，防止恶意软件的进一步传播和感染。

3.3 定期进行安全审计和监控

定期进行安全审计和监控是预防和应对网络攻击的重要手段。通过定期检查和评估企业的网络系统，可以及时发现潜在的安全风险和漏洞，采取相应的措施进行修复，降低网络系统被攻击的风险。首先，企业应该制定安全审计和监控计划，明确审计的范围、频率和具体操作方法。这个计划应该根据企业的实际情况和安全需求进行制定，确保能够全面覆盖企业的网络系统。其次，企业应该选择合适的安全审计工具和技术，例如漏洞扫描器、入侵检测系统等。这些工具和技术可以帮助

企业发现网络系统中的安全漏洞和异常行为，提供详细的审计日志和报告。在安全审计和监控过程中，企业应该重点关注关键信息资产的保护，例如服务器、数据库、网络设备等。这些资产是企业网络系统的核心，一旦被攻击或损坏，会对企业的正常运营造成严重影响。一旦发现安全漏洞或异常行为，企业应该及时采取措施进行修复和应对。这包括更新软件、修复漏洞、隔离受感染的设备、调整安全策略等。

3.4 严格管理对系统的物理接入

严格管理对系统的物理接入是保障企业网络安全的重要环节。物理接入的安全性直接影响到网络系统的整体安全，因此企业需要制定并执行严格的物理接入管理规定。首先，如果企业需要使用外部设备，应该经过严格的审批和授权程序。只有经过授权的员工才能使用特定的外部设备接入企业网络，并且在使用过程中需要进行严密监控和审计。其次，企业应该对所有接入企业网络的设备进行安全检查。这包括检查设备是否安装了防病毒软件、是否进行了最新的安全更新等。对于不符合安全要求的设备，企业应该拒绝其接入网络。此外，企业还应该建立完善的物理访问控制机制。只有经过身份验证和授权的员工才能访问企业的网络设备和数据中心。企业应该使用多因素身份验证方法，以提高身份验证的安全性。

3.5 提高员工网络安全意识

提高员工网络安全意识是预防网络攻击的比较重要的环节。员工是企业网络系统的最终用户，他们的行为和意识直接影响到网络的安全性。因此，企业应该采取措施，加强员工的网络安全培训和教育，提高他们的网络安全意识和技能水平。首先，企业应该制定网络安全培训计划，定期开展网络安全培训课程。培训内容应该包括基本的网络安全知识、常见的网络攻击手段和防护措施、以及员工在使用企业网络时应遵循的规定和操作方法。通过培训，使员工了解网络安全的威胁和风险，掌握基本的防护技能，增强安全意识。其次，企业可以通过多种形式开展网络安全宣传和教育活动[4]。例如，制作网络安全宣传资料、开展网络安全知识竞赛、定期发布网络安全提醒等。这些活动可以帮助员工更好地了解网络安全的重要性，提高安全防范意识。

3.6 建立应急响应机制

建立应急响应机制是应对网络安全事件的重要措施。通过制定详细的应急响应计划，企业可以在遭受攻击或出现安全事件时快速、准确地应对和处理，降低损失和影响。首先，企业应该明确应急响应流程和责任分工。在应急响应计划中，应该详细列出每一步的流程和操作步骤，包括事件报告、初步评估、响应措施、恢复计划等。同时，应该明确各个部门和人员的责任分工，确保在事件发生时能够迅速协调和配合。其次，企业应该建立安全事件监测和告警系统。通过实时监测网络流量和行为，及时发现异常和潜在的安全威胁，触发告警并通知相关人员进行处理。这样可以及时发现并应对安全事件，减少损失。此外，企业还应该定期进行应急响应演练。通过模拟常见的网络攻击场景，测试应急响应计划的可行性和有效性。通过演练，可以发现计划中存在的问题和不足，并及时进行更新和完善。

结语：综上所述，面对多种多样的安全威胁，企业需要构建一个综合的网络安全防护体系。这包括提高员工的安全意识、采用先进的安全技术、制定严格的安全政策和流程等。此外，持续的网络监控和应急响应也是必不可少的。只有全面、细致地做好安全防护工作，企业才能确保计算机网络系统的安全稳定运行，从而为企业的长远发展保驾护航。

参考文献

[1]黄永强.企业计算机信息网络系统的安全风险与控制[J].商场现代化,2018,(06):60-61.

[2]卢思彤.企业计算机信息系统的安全防御体系探讨[J].信息技术与信息化,2018,(11):134-136.

[3]崔彦亮.企业计算机网络系统安全分析[J].企业导报,2017,(04):142+144.

[4]孙黎,宋梓铭,孙雨.浅析计算机网络安全的主要隐患及管理措施[J].中国管理信息化,2019,22(16):173-174.