

计算机网络安全技术的影响因素与防范措施

凌晨 唐清荣

四川吉利学院

摘要：计算机网络安全技术是保护计算机系统免受潜在威胁的关键。本文讨论了影响网络安全技术的各种因素，包括网络攻击、自然灾害、技术故障等，并提出了相应的防范措施，如建立备份系统、实施访问控制、使用加密技术等。

关键词：计算机网络安全；防范措施；网络攻击；技术故障；备份系统；访问控制；加密技术

【DOI】10.12252/j.issn.2096-6288.2023.10.079

一、引言

随着计算机技术的飞速发展，计算机系统已经成为企业和个人不可或缺的工具。然而，与此同时，计算机网络安全问题也变得越来越突出。计算机网络安全技术是保护计算机系统免受潜在威胁的关键。本文将深入探讨影响网络安全技术的各种因素，包括网络攻击、自然灾害、技术故障等，并针对这些威胁提出相应的防范措施，如建立备份系统、实施访问控制、使用加密技术等。

二、计算机网络安全技术的影响因素

计算机网络技术的飞速发展给人们的生活带来了便利，但同时也带来了安全问题。网络安全技术是保护计算机系统免受潜在威胁的关键。本文将详细探讨计算机网络安全技术的影响因素，包括网络攻击、自然灾害和技术故障等，并针对这些威胁提出实用的防范措施。

（一）网络攻击

1. 恶意软件攻击

恶意软件攻击是一种危害性极大的网络攻击，它利用各种恶意软件，如病毒、蠕虫、特洛伊木马等，来攻击计算机系统。这些恶意软件可以通过各种渠道进入系统，例如通过电子邮件、网络下载、移动设备等。一旦进入系统，恶意软件就可以窃取敏感信息、破坏数据、删除文件、远程控制等，给用户带来严重的损失。为了防范恶意软件攻击，我们可以采取一系列安全措施。首先，建议使用杀毒软件，这些软件可以检测和清除恶意软件，保护系统免受攻击。其次，定期更新操作系统和应用程序的安全补丁，这些补丁可以修复系统漏洞，防止恶意软件利用漏洞进行攻击。此外，不打开未知来源的附件或下载未知来源的文件也可以有效防止恶意软件的入侵。除了以上措施，还需要提高用户的安全意识。用户应该注意保护个人隐私信息，不轻易下载未知来源的文件或打开未知来源的邮件和链接，避免点击不明链接或下载恶意软件。同时，定期备份重要数据也可以减少因恶意软件攻击而带来的损失。

总之，防范恶意软件攻击需要采取综合措施，包括使用杀毒软件、定期更新系统、提高用户安全意识等。只有这样，才能有效保护计算机系统免受恶意软件的攻

击。

2. 社交工程攻击

社交工程攻击是一种非常危险的攻击方式，它利用人类心理和社会行为中的弱点，通过欺骗、诱导、威胁等手段获取目标对象的个人信息或权限。攻击者通常会冒充可信的人或机构，如银行、政府机构等，通过虚假的电子邮件、网站、电话等手段诱导目标对象泄露个人信息或下载恶意软件。

社交工程攻击往往比其他类型的攻击更加难以防范，因为它利用了人类本身的思维和行为习惯。例如，攻击者可能会利用人们的信任心理，通过虚假的电子邮件或网站诱导目标对象输入个人信息或下载恶意软件。这些恶意软件可以窃取用户的个人信息、破坏数据、删除文件、远程控制等，给用户带来严重的损失。

为了防范社交工程攻击，我们需要提高人们对可信度和风险的认识，同时加强对个人信息和权限的保护。首先，用户应该保持警惕，不轻易相信来自未知来源的邮件、电话、网站等信息。其次，用户应该加强对个人信息和权限的保护，例如设置复杂的密码、定期更换密码、不轻易泄露个人信息等。此外，用户还可以使用一些安全工具，如杀毒软件、防火墙等来加强计算机系统的安全性。

除了以上措施，还需要提高整个社会的安全意识。政府、企业、社会组织等应该加强安全宣传和教育，提高公众对安全问题的认识和意识。同时，政府还应该加强对网络安全的监管和管理，打击网络犯罪行为，维护网络空间的安全和稳定。

总之，防范社交工程攻击需要全社会的共同努力。我们需要提高用户的安全意识、加强个人信息和权限的保护、加强网络安全管理等方面的工作。只有这样，才能有效保护个人和社会的安全和稳定。

3. 零日漏洞利用攻击

零日漏洞利用攻击是指利用未公开的漏洞进行攻击的行为。这些漏洞通常是在软件发布后发现的，而且往往没有及时得到修复。攻击者可以利用这些漏洞获取系统权限或执行恶意代码，造成数据泄露、系统崩溃等危害。防范零日漏洞利用攻击需要加强软件安全性的测试

和审核，及时修复漏洞并更新软件版本。

（二）自然灾害

1. 地震

地震是一种自然灾害，它可能导致计算机系统受到损坏甚至失效。地震波及范围内的计算机设备可能会受到震动和冲击，从而导致硬件故障、数据丢失等问题。为了防范地震对计算机系统的影响，建议将计算机设备放置在稳定的平台上或安装防震支架，同时定期备份重要数据并确保备份数据的存储设备也处于稳定的平台上。

2. 洪水

洪水是指大量的水淹没低洼地区而形成的自然灾害。洪水可能导致计算机设备被淹没或损坏，同时也会造成电力和通信网络的中断。这使得计算机系统可能会失效或数据丢失。为了防范洪水对计算机系统的影响，建议将计算机设备放置在较高的位置或安装防水设施，同时确保备用电源和通信设备也受到保护。

3. 雷击

雷击是一种常见的自然灾害，它可能导致计算机系统受到损坏甚至失效。雷击产生的高压电场和电流可能会破坏计算机设备的电子元件和电路板，从而导致硬件故障、数据丢失等问题。为了防范雷击对计算机系统的影响，建议安装防雷设施（如避雷针、接地线等），同时将计算机设备放置在较低的楼层或室内并确保其电子元件和电路板也受到保护。

（三）技术故障

1. 软件故障

软件故障是指计算机软件出现问题而导致系统无法正常运行的情况。这可能是由于软件本身存在缺陷、病毒攻击、非法操作等原因导致的。软件故障可能会导致数据丢失、系统崩溃等问题。为了防范软件故障的影响，建议定期更新软件版本、备份重要数据、安装杀毒软件等措施来保护系统的安全性。

2. 硬件故障

硬件故障是指计算机硬件出现问题而导致系统无法正常运行的情况。这可能是由于硬件设备本身存在缺陷、使用不当、自然灾害等原因导致的。硬件故障可能会导致数据丢失、系统崩溃等问题。为了防范硬件故障的影响，建议定期检查硬件设备的运行状态、备份重要数据、使用备用设备等措施来保护系统的可靠性。

3. 网络故障

网络故障是指计算机网络出现问题而导致系统无法正常运行的情况。这可能是由于网络连接中断、网络设备故障等原因导致的。网络故障可能会导致数据传输中断、远程访问失效等问题。为了防范网络故障的影响，建议定期检查网络设备的运行状态、备份重要数据、使用备用网络线路等措施来保护系统的可用性。

三、计算机网络安全技术的防范措施

计算机网络安全技术的防范措施是确保系统稳定、数据安全的关键。本章将详细介绍几种实用的防范措施，包括建立备份系统、实施访问控制、使用加密技术以及其他防范措施。通过对这些措施的深入探讨，我们将更好地理解如何在实际应用中保护计算机网络安全。

（一）建立备份系统

1. 本地备份

本地备份是一种常见的备份方式，它是指将数据备份到本地计算机或网络存储设备中。通过本地备份，即使发生灾难性事件，也可以快速恢复数据。为了确保备份数据的完整性和可靠性，建议定期进行备份，并测试备份数据的可恢复性。

2. 远程备份

远程备份是指将数据备份到远程服务器或云存储设备中。这种备份方式可以减少本地数据丢失的风险，并提供更可靠的备份存储。远程备份可以通过加密技术保护数据的机密性和完整性，并确保备份数据在受到攻击或自然灾害时仍可访问。

（二）实施访问控制

1. 基于角色的访问控制（RBAC）

基于角色的访问控制是一种广泛应用于信息安全管理访问控制方法。它通过将用户映射到不同的角色或权限组，从而控制用户对特定资源的访问权限。这种访问控制方法在很大程度上简化了权限管理，减少了由于人为错误导致的不必要的授权风险，同时提高了整个系统的安全性。它能够实现职责分离，即不同角色的人员所能访问的资源及所执行的操作是不同的，这大大增加了系统的安全性。

2. 基于属性的访问控制（ABAC）

基于属性的访问控制是一种非常灵活且有效的资源访问控制方法。它通过定义并评估对象的属性，如用户、资源、环境等，来决定是否允许特定用户对特定资源进行特定操作。这种访问控制方法能够根据用户的属性，如他们的角色、部门、地域等，资源的属性，如资源的类型、所有者、使用频率等，以及环境的属性，如时间、位置等，来进行授权。这种方法提供了更精细的访问控制策略，可以更好地满足不同的业务需求。

（三）使用加密技术

1. 数据加密标准（DES）

数据加密标准（DES）是一种相对较早的对称加密算法，它将明文分成64位的数据块，并使用56位的密钥进行加密。虽然它提供了一定程度的数据保护，但由于密钥长度相对较短，使得其安全性受到一定限制。如今，DES已经被更强大、更安全的加密算法——高级加密标准（AES）所取代。AES具有更长的密钥长度和更复杂的加密过程，能够提供更高的数据安全保护。

2. 高级加密标准（AES）

高级加密标准，或称AES，是一种广泛使用的对称

加密算法。它将明文分成128位、192位或256位的数据块，并使用与之匹配的128位、192位或256位的密钥进行加密。这种加密方法非常安全，因为它采用了复杂的数学运算和替换、置换等操作，使得解密过程非常困难。AES被广泛应用于各种领域，如数据存储、网络通信和电子商务等，为保障信息安全发挥了重要作用。

（四）其他防范措施

1. 安装杀毒软件

安装杀毒软件不仅可以有效防范恶意软件的入侵和传播，还可以提高计算机系统的安全性和稳定性。杀毒软件可以检测和清除计算机系统中的病毒、木马、蠕虫等恶意程序，保护您的数据和隐私。为了确保杀毒软件能够发挥最大作用，建议选择可靠的品牌，并定期更新病毒库和恶意软件库。此外，结合其他安全措施，如密码管理、电子邮件过滤等，可以进一步提高计算机系统的安全性。

2. 定期更新操作系统和应用程序的安全补丁

操作系统和应用程序的安全补丁对于保护系统免受恶意攻击和数据泄漏至关重要。通过定期检查并安装最新的安全补丁，您可以修复已知的安全漏洞和缺陷，提高系统的安全性。同时，及时更新常用软件和工具可以防范潜在的安全风险，确保您的计算机环境始终处于最新、最安全的状态。为了更好地保护您的系统和数据，建议将安全补丁和软件更新作为一项日常任务来执行。

3. 使用防火墙来限制网络流量和阻止潜在的攻击行为

防火墙是一种有效的安全工具，可以实时监控网络流量，并阻止未经授权的网络连接和攻击行为。通过配置防火墙规则，您可以限制对外开放的端口和服务，从而减少潜在的攻击面。此外，防火墙还可以设置只允许特定的网络流量通过，进一步提高系统的安全性。为了确保系统的安全，建议使用可靠的防火墙产品，并根据实际需求配置合理的防火墙规则。

四、案例分析

（一）遭受网络攻击导致数据泄漏的案例介绍和分析

在2014年，索尼影视娱乐公司遭受了一次严重的网络攻击，导致大量敏感数据泄漏。这次事件表明，即使是大型企业也面临着网络攻击的风险。网络攻击者不断演变出新的攻击手段，因此企业需要时刻保持警惕，及时修复系统漏洞，并提高网络安全防护能力。此外，制定完善的应急响应计划也至关重要，以便在遭受攻击时能够及时采取措施，尽可能减少损失。这一事件提醒我们，网络安全和数据保护对于企业和个人来说都是至关重要的，需要引起足够的重视。

（二）自然灾害导致网络中断的案例介绍和分析

2012年，泰国遭受的严重洪水灾害导致多个地区的互联网连接中断，基础设施损坏，对多个电信运营商的

网络服务造成影响。这场灾难使得企业和个人无法正常访问互联网，对生产和生活造成了严重影响。这个案例警示我们，自然灾害会对网络基础设施造成严重破坏，导致网络中断。因此，我们需要认识到自然灾害对网络的影响，并提前采取应对措施，例如在灾害多发区备份网络线路、备用电站等，以确保网络服务的稳定性和可靠性。

（三）技术故障导致数据丢失的案例介绍和分析

2016年，亚马逊公司的一个数据中心发生技术故障，导致大量用户数据丢失，给用户带来严重损失。这个案例表明，技术故障可能导致数据丢失，因此企业需要建立完善的数据备份和恢复机制，以确保数据的安全性和可靠性。此外，定期备份和存档数据也是必要的措施，以便在发生技术故障时能够及时恢复数据，减少损失。亚马逊公司的这个事件提醒我们，对于企业和组织来说，保护数据安全是一项至关重要的任务，必须高度重视并采取切实有效的措施。

（四）案例比较和总结

以上三个案例分别是遭受网络攻击导致数据泄漏、自然灾害导致网络中断和技术故障导致数据丢失的情况。这些案例都具有不同的特点和影响，但都说明了网络安全和数据保护的重要性。无论是遭受网络攻击还是发生自然灾害或技术故障，企业和个人都需要认识到风险的存在并采取相应的防范措施。同时，政府和社会各界也需要加强合作，共同应对网络安全和数据保护的挑战。

五、结语

综上所述，计算机网络安全技术是保护计算机系统免受潜在威胁的关键。本文深入探讨了影响网络安全技术的各种因素，包括网络攻击、自然灾害、技术故障等，并针对这些威胁提出了一系列实用的防范措施。通过建立备份系统、实施访问控制、使用加密技术等措施，我们可以有效增强计算机系统的安全性和稳定性，确保企业和个人的数据安全和隐私保护。在当今数字化时代，计算机网络安全技术的重要性不言而喻，我们每个人都应该加强对计算机网络安全认识和防范意识，共同维护一个安全、可靠的网络环境。

参考文献

- [1] 王世伟. 计算机网络安全技术的影响因素与防范措施[J]. 电子技术与软件工程, 2016(8): 230-230.
- [2] 韩建民. 计算机网络安全技术的影响因素与防范措施[J]. 科技资讯, 2017, 15(14): 30-31.
- [3] 王晓蕾. 计算机网络安全技术的影响因素与防范措施[J]. 信息系统工程, 2018(7): 70-70.

第一作者：凌晨（1991年1月），男，四川成都，硕士，讲师，主要从事计算机网络安全研究。

第二作者：唐清荣，1986年1月，女，四川成都，副研究员，主要从事算法分析。