

大数据时代计算机网络安全及防范措施

张明皓

中国五矿 北京 100010

摘要: 计算机网络安全和防范措施在大数据时代变得尤为重要。随着信息技术的快速发展,我们越来越多地依赖网络与他人进行沟通、交流和获取信息。然而,这也带来了一系列的网络安全威胁和漏洞,出现因黑客攻击、恶意软件等导致个人或组织的敏感信息泄露的问题。

关键词: 大数据时代; 计算机网络安全; 防范措施

引言

本文将探讨大数据时代的计算机网络安全挑战,并提供一些有效的防范措施。首先,我们将介绍常见的网络安全威胁和攻击方式,包括网络钓鱼、恶意软件、拒绝服务攻击等。然后,我们将详细讨论如何保护计算机网络免受这些威胁的影响,包括网络安全策略、访问控制、加密技术、身份验证等方面的应用。

1 网络安全威胁和攻击方式

1.1 网络钓鱼攻击

网络钓鱼攻击是一种常见的网络安全威胁,它通过伪造合法网站、电子邮件或消息来欺骗用户,以获取他们的敏感信息。攻击者通常冒充信任的实体,如银行、社交媒体平台或在线商店,诱使用户在不知情的情况下提交个人信息、账号密码、信用卡等机密数据。钓鱼攻击常见的类型包括:假冒网站:攻击者创建与合法网站相似的假网站,通过修改URL或使用类似的域名来迷惑用户。当用户在假网站上输入个人信息时,这些信息会被攻击者获取并进行恶意利用。钓鱼邮件:攻击者发送看似真实的电子邮件,声称来自可信赖的组织,如银行或购物网站。邮件通常包含引诱性的内容,例如要求用户点击链接验证账号信息或更新密码。然而,这些链接实际上指向钓鱼网站,目的是获取用户的敏感数据^[1]。社交工程:攻击者可能通过社交媒体平台或即时通讯应用程序与受害者建立联系,并试图获取其个人信息。他们可能冒充朋友、同事或亲戚,以获取信任并引诱受害者分享敏感信息。

1.2 恶意软件

恶意软件是一种在未经用户授权的情况下通过计算机网络传播并对系统造成损害的软件。下面将介绍一些常见的恶意软件类型、传播方式以及防范措施。病毒(Virus):病毒是一种能够自我复制并植入其他可执行文件中的恶意程序。它们可以通过感染文件、邮件附

件、共享文件等方式传播,并在被执行时对系统进行破坏或盗取信息。蠕虫(Worm):蠕虫是一种独立运行的恶意程序,通过利用系统漏洞自动复制和传播。它们可以通过网络互相传播,占用大量带宽和系统资源,甚至导致系统崩溃。间谍软件(Spyware):间谍软件在用户不知情的情况下追踪并收集用户的个人信息。这些软件通常通过广告、软件捆绑、恶意链接等方式传播,并窃取用户的敏感数据、浏览习惯和登录凭证。木马(Trojan):木马是一种伪装成合法软件的恶意程序,背后隐藏着恶意功能^[2]。当用户安装并运行木马时,攻击者可以远程控制被感染的系统,获取敏感信息或进行其他恶意活动。

1.3 拒绝服务攻击

拒绝服务攻击(Denial of Service, DoS)是一种攻击方式,攻击者通过发送大量请求或耗费目标系统的资源,使其超负荷运行,从而导致系统无法正常工作。这种攻击可能会造成严重的影响,包括服务不可用、数据丢失和业务中断。拒绝服务攻击的原理在于利用系统的弱点或限制,例如网络带宽、计算资源或应用程序设计上的漏洞。攻击者可以使用多种方法实施拒绝服务攻击,其中一些常见的类型包括:网络层攻击:攻击者以高速率向目标系统发送大量的网络流量,例如UDP flood攻击、ICMP flood攻击等,消耗目标系统的网络带宽和处理能力。操作系统层攻击:攻击者利用操作系统或网络协议的漏洞,通过发送特制的请求或恶意代码来耗尽系统资源,例如TCPSYN flood攻击、Ping of Death攻击等。应用层攻击:攻击者针对应用程序的漏洞或资源耗尽进行攻击,如HTTP请求攻击、Slowloris攻击等^[3]。

2 保护计算机网络的防范措施

2.1 针对网络钓鱼攻击的应对措施

收到可疑邮件时,不要轻易相信邮件中的信息。首先核实发件人的身份,通过其他渠道进行确认。可以查

看邮件头部信息,验证发件人的电子邮件地址是否与正常的发件人相匹配。避免随意点击邮件或网页中的链接,尤其是来自未知来源或可疑的链接。使用鼠标悬停在链接上,查看链接的URL是否与预期目标相匹配。如果链接看起来可疑,就不要点击。另外,可以手动输入网站的URL来访问,而不是通过邮件或其他不明来源的链接访问。培养员工对网络钓鱼攻击的认识,并提供相应的培训。教育员工如何识别可疑邮件、链接和附件,以及如何正确处理它们。提醒员工注意社交工程攻击,并教授他们如何验证身份和确认信息的真实性^[4]。定期组织网络安全意识培训,帮助员工了解最新的网络钓鱼攻击技巧和防范措施。部署反钓鱼工具可以帮助阻止大部分网络钓鱼攻击。这些工具可以检测和屏蔽恶意链接、欺诈网站和伪造的电子邮件。选择合适的反钓鱼软件或服务,并确保其及时更新和升级,以保持对新威胁的有效防护。提醒用户保持警惕,不要随意泄露个人和机密信息。教育用户如何判断一个网站的可信度,避免向可疑网站提供个人信息。此外,及时向用户提供网络钓鱼攻击的最新实例和警告,让他们了解并采取相应的预防措施。通过核实发件人身份、谨慎点击链接、加强员工培训和意识、使用反钓鱼工具、强化密码策略以及加强安全意识,可以有效地减少网络钓鱼攻击对计算机网络的威胁。

2.2 针对恶意软件攻击的应对措施

保持计算机设备上安装有效的防病毒软件,并及时更新病毒定义文件以确保检测最新的威胁。防病毒软件可以扫描、检测和清除计算机中的恶意软件,提供实时保护和防御措施。限制访问未经验证或不受信任的网站,以减少感染恶意软件的风险。非正规网站可能包含恶意软件的下载链接、欺诈性内容或其他潜在的网络威胁。用户应始终谨慎选择访问的网站,并避免点击可疑的链接。只从可靠的来源下载和安装软件,在安装前仔细审查软件的来源和信誉。源自不明或不可信的来源的软件可能会携带恶意代码或广告软件,导致系统被感染或遭受其他安全问题。下载和安装软件时,应使用官方网站或受信任的应用商店,同时注意软件的评价和用户反馈。保持操作系统、应用程序和防病毒软件等的最新版本^[5]。厂商通常会发布补丁和更新来修复已知漏洞和安全隐患,以提高安全性。教育用户有关网络安全的基本知识和最佳实践,提高他们对潜在威胁的认识。这包括警惕钓鱼邮件、社交工程、恶意广告和其他常见的网络欺诈手段。通过开展安全培训和定期更新员工的网络安全意识,可以减少恶意软件攻击的成功率。在遭受恶意软件感染或勒索软件攻击时,可通过恢复备份数据来

避免损失。备份数据应存储在离线设备上,并保持安全性。除了安装防病毒软件之外,还可以启用实时保护功能。实时保护会监视计算机上的活动,并检测和阻止恶意软件的执行。这提供了即时的保护,减少了被感染的风险。不仅要定期更新操作系统和防病毒软件,还应保持应用程序的最新版本。恶意软件常常利用过时和未修补的应用程序漏洞进行攻击。通过及时应用程序更新,可以修复已知漏洞,增加系统的安全性。为了防止恶意软件通过自动运行感染计算机,建议禁用自动运行功能。这样,当插入可移动介质或下载文件时,系统不会自动运行其中的程序,从而减少恶意软件传播的风险。为每个用户设置独立的账户,并使用最低权限原则^[1]。这可以限制恶意软件对系统的访问和影响范围。管理员账户应仅在必要时才使用,以减少系统被攻击的潜在风险。配置系统监控和事件日志记录,以便及时检测和回溯潜在的安全问题。通过分析日志信息,可以追踪恶意软件的来源和行为,并采取相应的反应措施。通过综合运用上述措施,可以提高计算机网络的安全性,减少恶意软件攻击的风险。安全是一个持续的过程,需要不断更新和加强措施来适应不断变化的威胁环境。

2.3 针对拒绝服务攻击的应对措施

定期进行漏洞扫描和渗透测试可以及时发现并修复系统中的安全漏洞。漏洞扫描工具能够检测系统中存在的潜在漏洞,并生成报告供管理员分析。渗透测试则模拟真实攻击行为,评估系统的脆弱性,从而找到可能被利用的漏洞。保持操作系统、中间件、数据库和应用程序的最新版本,并及时安装官方发布的安全补丁。厂商会发布补丁来修复已知漏洞,因此定期更新系统可以有效地减少攻击者利用漏洞的机会。与网络服务提供商(ISP)合作,共同制定和实施防御策略以减轻拒绝服务攻击的影响。ISP可以通过配置网络设备来过滤恶意流量,协助在攻击发生时进行应急响应,并提供防御建议和解决方案。部署流量监控和入侵检测系统(IDS/IPS)有助于及早发现并阻止潜在的DoS攻击行为。IDS负责监测网络流量并识别异常行为,而IPS则能主动阻止恶意流量进入受攻击的网络。针对大规模的分布式拒绝服务(DDoS)攻击,使用专门的DDoS缓解服务可以帮助减轻攻击的影响。这些服务通常通过多个数据中心分散流量,过滤恶意请求,并确保合法用户能够正常访问目标系统^[2]。使用负载均衡器可以将流量平均分配到多个服务器上,从而降低单个服务器遭受DoS攻击的风险。通过实施有效的策略和访问控制措施,限制来自未经授权的流量和恶意请求,包括设置防火墙规则、使用反垃圾邮

件技术、强化身份认证等。提供网络安全教育和培训,使员工和用户能够了解DoS攻击的类型和应对方法。加强用户的安全意识和合规性,减少社会工程等攻击方式的成功率。因此,实施多层次、综合性的防御措施,结合定期风险评估和漏洞修复,可以大幅提高网络的安全性和稳定性。

2.4 网络安全策略

网络安全策略是组织为确保网络安全性而制定的一系列规则和流程。下面将介绍网络安全策略的重要性,并提供一些有效的实施方法。首先,网络安全策略可以帮助组织建立一个稳固的安全框架,为网络提供必要的保护措施。通过规范和约束网络访问、数据传输和信息存储等方面的行为,网络安全策略可以减少潜在的安全漏洞和风险。其次,网络安全策略有助于建立强大的密码策略。制定强密码策略是防止未经授权访问的关键步骤之一。组织可以要求员工使用强密码,并定期更改密码。强密码应包含字母、数字和特殊字符的组合,长度不少于8位。避免使用容易猜测的密码,如生日、姓名等。此外,重要系统应启用多因素身份验证,以提供额外的安全层次。第三,定期备份数据是网络安全策略中不可或缺的一部分。通过定期备份数据,组织可以在发生数据损坏、系统故障或恶意攻击时迅速恢复数据,最大程度地减少潜在损失。此外,网络安全策略还包括实施强大的防火墙和入侵检测系统^[4]。防火墙可以监控和管理网络流量,阻止未经授权的访问和恶意活动。入侵检测系统可以及时发现并响应潜在的网络攻击,帮助组织采取必要的措施进行反应和防御。同时定期进行安全审计和漏洞扫描,以检查系统和网络中存在的潜在弱点和漏洞。这可以帮助发现并修复安全问题,确保网络处于良好的安全状态。建立和实施应急响应计划,以迅速应

对安全事件和网络威胁。这包括制定恢复策略、明确责任分工和培训响应团队等^[4]。最后,教育和培训员工是网络安全策略不可或缺的一部分。提供网络安全意识培训可以帮助员工识别和避免潜在的网络威胁,同时加强对网络安全政策的理解和遵守。总之,通过建立稳固的安全框架、制定强密码策略、定期备份数据、使用防火墙和入侵检测系统、定期安全审计和漏洞扫描、建立和实施应急响应计划以及教育员工等措施,组织可以最大限度地减少网络威胁和风险,确保计算机网络的安全性。

结语

在大数据时代,计算机网络安全至关重要。面对日益复杂的网络威胁和攻击,我们必须采取有效的防范措施来保护我们的数据和系统。从管理和技术两方面来提高网络的安全性。同时,教育用户提高网络安全意识也是至关重要的。只有共同努力,才能确保我们在这个数字化时代中享受便利的同时,不受网络犯罪的侵害。

参考文献

- [1]张明华,张光辉,王云鹏.(2021).大数据时代计算机网络安全及防范措施研究.计算机工程与设计,42(2),548-553.
- [2]刘晓宇,陈琳,赵新宇.(2020).大数据时代计算机网络安全问题与应对策略.信息技术与标准化,21(4),63-68.
- [3]李伟,张建平.(2019).大数据时代计算机网络安全威胁与防范研究.网络与信息安全学报,5(2),25-30.
- [4]张鹏,陈敬波,王勇.(2020).基于大数据分析的计算机网络安全态势感知技术[J].计算机科学,47(7):1-6.
- [5]周小超,李明,殷涵晨.(2019).大数据时代计算机网络安全态势感知技术研究综述[J].光电技术应用,34(3):19-23.