计算机网络安全现状及网络安全技术措施

吴秀娟 荣 曦

济南市气象局 山东 济南 250000

摘要: 在数字化时代, 计算机网络已深度融入社会生活的各个层面, 从日常办公、线上交易到关键基础设施的运行, 都离不开网络的支撑。本文聚焦计算机网络安全领域, 阐述其现状及技术措施。当前, 计算机网络安全面临严峻挑战, 网络攻击手段愈发多样, 数据泄露频繁, 恶意软件、网络钓鱼攻击肆虐, 物联网安全问题也日益凸显。为应对这些问题, 需采取一系列有效技术措施, 如防火墙技术、入侵检测与防御系统、加密技术、身份认证技术、安全漏洞管理及网络安全审计等。这些措施的合理运用, 对提升计算机网络安全水平、保障网络环境稳定具有重要意义。

关键词: 计算机网络; 安全现状; 网络安全; 技术措施

引言: 随着信息技术的迅猛发展, 计算机网络已深度融入社会生活的方方面面。无论是个人的日常网络活动, 还是企业的业务运营、政府的公共服务, 都高度依赖计算机网络。然而, 网络安全威胁也随之不断增加, 给个人隐私、企业数据安全和国家安全带来了严重挑战。了解计算机网络安全现状, 掌握有效的网络安全技术措施, 对于维护网络空间的安全与稳定至关重要。本文将对计算机网络安全现状进行分析, 并探讨相应的技术措施。

1 计算机网络安全概述

计算机网络安全是指通过采取各种技术和管理措施, 确保网络系统的硬件、软件及其系统中的数据受到保护, 不因偶然的或者恶意的原因而遭到破坏、更改、泄露, 系统连续可靠正常地运行, 网络服务不中断。从本质上来说, 计算机网络安全包括网络设备安全、网络信息安全、网络软件安全。网络设备安全是基础, 保障网络中各类硬件设备的正常运行, 避免因物理损坏、电磁干扰等导致网络故障。网络信息安全则重点关注数据的保密性、完整性和可用性, 防止数据被窃取、篡改或丢失。网络软件安全旨在确保网络操作系统、应用软件等没有安全漏洞, 不会被恶意利用。在当今数字化时代, 计算机网络安全的重要性不言而喻。个人层面, 它关乎个人隐私和财产安全, 比如个人网上银行信息、社交账号等若遭泄露, 可能导致经济损失和个人生活被干扰。企业层面, 企业的商业机密、客户数据等是核心资产, 一旦出现安全问题, 会严重损害企业声誉, 带来巨大经济损失。国家层面, 关键基础设施的网络安全直接关系到国家主权、经济安全和社会稳定。因此, 持续加强计算机网络安全防护, 是保障各方利益和社会稳定发展的必要举措^[1]。

2 计算机网络安全现状

2.1 网络攻击手段日益多样化

过去, 网络攻击手段相对单一, 大多集中在简单的端口扫描、密码破解等方式。但如今, 黑客的攻击手段层出不穷。比如分布式拒绝服务攻击(DDoS), 通过控制大量的僵尸网络, 向目标服务器发送海量请求, 使其资源耗尽而无法提供服务。以某知名游戏公司为例, 在热门游戏上线时, 就曾遭受大规模DDoS攻击, 导致服务器瘫痪数小时, 大量玩家无法登录, 公司不仅经济损失惨重, 还严重影响了用户体验和品牌形象。还有利用系统漏洞进行的攻击, 黑客一旦发现未修复的系统漏洞, 就会迅速编写针对性的攻击代码, 入侵系统获取权限, 窃取重要数据。

2.2 数据泄露事件频发

在大数据时代, 数据成为了重要的资产。然而, 数据泄露事件却屡见不鲜。许多企业由于安全防护措施不到位, 用户数据被黑客轻易获取。像某知名社交平台, 曾因数据库安全漏洞, 导致数亿用户的个人信息, 包括姓名、邮箱、联系方式等被泄露。这些泄露的数据被非法买卖, 用户可能会收到大量的垃圾邮件、诈骗电话, 严重干扰了用户的正常生活。而且, 数据泄露对企业自身也造成了巨大的负面影响, 不仅面临用户的信任危机, 还可能面临法律诉讼和巨额赔偿。

2.3 恶意软件肆虐

恶意软件的种类和数量不断增加, 给网络安全带来了极大的威胁。常见的有病毒、木马、勒索软件等。病毒会自我复制并感染其他文件, 破坏系统的正常运行。木马则隐藏在正常程序中, 偷偷窃取用户的敏感信息, 如账号密码等。勒索软件更是猖獗, 它会加密用户的文件, 然后索要赎金才提供解密密钥。例如, 一些医疗机

构遭受勒索软件攻击后,患者的病历等重要数据被加密,导致医疗工作无法正常开展,严重威胁到患者的生命健康。而且,恶意软件的传播途径广泛,可通过网络下载、电子邮件附件、移动存储设备等多种方式传播。

2.4 网络钓鱼攻击猖獗

网络钓鱼攻击利用人们的心理弱点,通过伪装成合法机构发送欺诈性邮件或消息,诱使用户提供敏感信息。比如伪装成银行发送邮件,要求用户点击链接更新账户信息,一旦用户点击并输入账号密码等信息,就会被黑客获取。还有通过社交媒体进行网络钓鱼,骗子冒充熟人发送虚假的求助信息,骗取用户的钱财。由于网络钓鱼攻击手段不断翻新,且具有很强的欺骗性,很多用户难以辨别真伪,导致大量用户上当受骗,造成经济损失。

2.5 物联网安全问题凸显

随着物联网技术的广泛应用,越来越多的设备接入网络,如智能家居设备、智能穿戴设备、工业物联网设备等。然而,这些设备的安全防护水平参差不齐。许多物联网设备存在默认密码未修改、安全漏洞未修复等问题,容易被黑客攻击。一旦黑客控制了物联网设备,不仅可以获取设备收集的用户数据,还可能利用这些设备发起进一步的攻击,如组成僵尸网络发动DDoS攻击。比如,一些智能家居摄像头被黑客入侵后,用户的隐私生活被曝光,给用户带来了极大的困扰^[2]。

3 计算机网络安全技术措施

3.1 防火墙技术

防火墙技术历经多年发展,已成为网络安全防护体系的关键组成部分。早期防火墙主要以简单的包过滤功能为主,随着网络威胁的日益复杂,其功能不断迭代升级。防火墙能够依据预设规则,对网络流量进行细致管控。它可以基于源IP地址、目的IP地址、端口号等关键信息,对进出网络的数据包进行筛选。比如,企业可设置规则,仅允许特定IP地址段的外部用户访问企业官网,阻止其他未经授权的访问,从而有效降低外部恶意攻击的风险。同时,防火墙还能对内部网络的访问行为进行约束,防止内部人员因误操作或恶意行为导致的数据泄露。防火墙具备强大的入侵防范能力。它能够实时监测网络流量,一旦发现异常流量,如大量的端口扫描行为,立即进行阻断,有效抵御常见的DDoS攻击、端口扫描攻击等。然而,防火墙技术并非完美无缺。它难以应对来自内部网络的恶意攻击,对于利用合法端口进行的恶意数据传输,防火墙也可能无法及时识别和拦截。并且,随着网络应用的多样化,新型的网络威胁不断涌

现,防火墙需要持续更新规则和升级技术,才能更好地适应复杂多变的网络安全环境。

3.2 入侵检测系统(IDS)和入侵防御系统(IPS)

入侵检测系统(IDS)与入侵防御系统(IPS)在维护计算机网络安全中发挥着关键作用。IDS的核心功能是对网络流量进行实时监测,运用模式匹配、异常检测等技术,对网络数据包进行深度分析。一旦发现符合入侵特征或异常行为的数据,便迅速发出警报,告知管理员及时介入处理,就像网络中的“监察员”,时刻警惕潜在威胁。IPS则在检测基础上强化了主动防御能力。它不仅能精准识别人侵行为,还能在攻击发生瞬间采取措施,如阻断连接、过滤恶意流量等,直接阻止攻击的进一步扩散,充当网络“保镖”的角色。在实际应用场景中,金融机构部署IDS和IPS,实时监测网络交易,防范黑客窃取客户资金和信息;大型企业利用它们保护内部数据和业务系统,防止商业机密泄露。随着网络技术的不断发展,网络攻击手段日益复杂,IDS和IPS也在持续进化,未来将更注重智能化、自动化,提升对新型复杂攻击的检测与防御能力,为网络安全提供更有力的保障。

3.3 加密技术

加密技术是保障计算机网络安全的核心技术之一,它的基本原理是将原始数据(明文)通过特定的算法和密钥转化为密文,只有拥有正确密钥的接收方才能将密文还原为明文,从而确保数据在传输和存储过程中的保密性、完整性和不可否认性。常见的加密技术主要分为对称加密和非对称加密。对称加密使用同一密钥进行加密和解密,这种方式加密和解密速度快,适合大量数据的加密,但密钥管理存在一定风险,一旦密钥泄露,数据安全就无法保障。非对称加密则采用一对密钥,即公钥和私钥,公钥可以公开,用于加密数据,私钥由用户自己保存,用于解密。这种方式解决了密钥分发的难题,安全性更高,常用于身份认证、数字签名等场景。在实际应用中,加密技术广泛用于网络通信、电子商务等领域。例如在网上银行交易中,用户的账号、密码以及交易信息等都通过加密技术进行加密传输,防止被黑客窃取和篡改。在云存储中,用户的数据也会被加密存储,确保数据在云端的安全性。

3.4 身份认证技术

身份认证技术是计算机网络安全的关键防线,用于确认访问者的真实身份,以此判断其是否具备访问特定资源的权限。在网络环境中,只有通过准确的身份认证,才能确保合法用户正常访问,同时阻止非法用户入侵。常见的身份认证类型丰富多样。基于密码的认证最

为普遍,用户输入预先设定的密码进行身份验证,但密码存在易被遗忘、被盗取的风险。基于令牌的认证则借助物理设备,如动态口令牌,生成一次性密码,大大提升了安全性。生物识别技术近年来发展迅速,包括指纹识别、面部识别、虹膜识别等,利用人体独特的生物特征进行身份确认,具有极高的准确性和唯一性,难以被伪造。身份认证技术在网络安全中起着举足轻重的作用。在金融领域,网上银行、移动支付等业务通过严格的身份认证,保障用户资金安全,防止账户被盗刷。企业内部网络通过身份认证,限制员工对敏感信息的访问,保护企业核心数据。

3.5 安全漏洞管理

安全漏洞管理是计算机网络安全防护体系中的关键环节,旨在对系统、软件及网络设备中存在的安全漏洞进行全生命周期管理,以降低因漏洞引发的安全风险。安全漏洞管理流程主要包括漏洞发现、评估、修复与验证。漏洞发现依靠多种技术手段,如定期的漏洞扫描工具,对网络系统进行全面检查,还可通过人工代码审查、安全测试等方式主动查找隐藏的安全隐患。评估环节则是判断漏洞的严重程度,综合考虑漏洞可能导致的影响范围、数据泄露风险以及被利用的难易程度等因素。修复阶段,根据评估结果制定相应的修复方案,若是软件漏洞,及时更新补丁;对于网络配置问题,重新优化配置。修复完成后,还要进行验证,确保漏洞已被成功修复,系统恢复到安全状态。安全漏洞管理至关重要。如果忽视安全漏洞,一旦被黑客利用,企业可能遭受数据泄露、系统瘫痪等严重后果。例如,某知名软件公司曾因未及时修复一个高危漏洞,导致大量用户数据被窃取,不仅引发用户信任危机,还面临巨额赔偿。因此,有效的安全漏洞管理能够提前预防安全事件,保障网络系统的稳定运行和数据安全。

3.6 网络安全审计

网络安全审计是对网络活动进行全面、系统记录、

分析和审查的过程,是保障计算机网络安全的重要技术措施之一。通过网络安全审计,能够实时监控网络中的各种行为,包括用户登录、数据传输、系统操作等。在工作方式上,网络安全审计系统借助专门的软件工具,对网络设备、操作系统、应用程序等产生的日志信息进行收集与整合。这些日志详细记录了网络活动的关键信息,如时间、用户、操作内容等。审计系统会依据预设的规则,对这些日志数据进行深度分析,一旦发现异常行为,如频繁的登录失败尝试、大量的数据异常传输等,就会及时发出警报。网络安全审计在网络安全防护体系中发挥着多方面的重要作用。从合规角度,它能帮助企业满足相关法律法规和行业标准的要求,如数据保护法规、行业监管规定等。在安全监测方面,有助于及时发现潜在的安全威胁,为及时采取应对措施提供依据,防范网络攻击的发生。在事故调查时,审计记录可作为追溯和分析的关键线索,查明事件发生的原因、经过和影响范围,帮助企业总结经验教训,完善安全策略^[3]。

结束语

网络安全现状不容乐观,网络攻击手段层出不穷,数据泄露、恶意软件、网络钓鱼等威胁不断涌现,物联网安全也问题频出。面对复杂严峻的态势,防火墙、加密技术、身份认证等安全措施成为关键防线。但网络威胁持续演变,我们必须保持警惕,持续优化技术措施,提升安全意识,加强网络安全监管与行业协作。只有这样,才能有效抵御各类威胁,维护网络空间的安全稳定,让网络技术更好地造福社会。

参考文献

- [1]范清永.试论当下计算机网络安全现状及对策[J].信息记录材料,2021(5):158-159.
- [2]刘超南.计算机网络安全现状及防御技术[J].通讯世界,2023(1):123-124.
- [3]陈瑞.计算机网络安全现状分析与防御技术探讨[J].科技资讯,2023(13):159-160.