电子信息工程与网络安全浅析

裴建新[1] 柳盈辰[2] 张丹丹[1]
1. 中国建筑第八工程局有限公司华北分公司 天津 300450
2. 中国电子工程设计院股份有限公司 北京 100080

摘 要：本文深入探讨了电子信息工程与网络安全的紧密关系。分析了网络安全威胁对电子信息工程的多方面影响，包括数据泄露、系统瘫痪和知识产权侵犯等。阐述了网络安全保障电子信息工程正常运行的关键机制，如加密认证、访问控制等。详细介绍了网络安全防护的多种策略，涵盖访问控制、加密技术、防火墙与入侵检测系统、安全审计与监测以及员工培训与安全意识教育。

关键词：电子信息工程；网络安全；防护策略；技术手段

引言：随着电子信息工程在各个领域的广泛应用，其对社会发展的推动作用日益显著。然而，网络安全问题成为了制约电子信息工程发展的关键因素。网络攻击、恶意软件、数据泄露和系统漏洞等威胁不断涌现，给电子信息工程带来严重挑战。因此，研究电子信息工程中的网络安全具有重要的现实意义。本文将深入剖析网络安全在电子信息工程中的重要性、面临的威胁及有效的防护策略。

1 网络安全在电子信息工程中的重要性

1.1 网络安全威胁对电子信息工程的影响

网络安全威胁对电子信息工程产生了多方面的严重影响。（1）数据泄露是其中极为严峻的问题。在电子信息工程中，大量敏感信息如个人身份信息、金融交易数据、商业机密等被数字化存储和传输。一旦网络安全防线被突破，这些数据就可能落入不法分子手中。这不仅会给个人带来隐私泄露、财产损失的风险，对于企业而言，可能导致核心竞争力的丧失、客户信任的崩塌，甚至面临法律诉讼和巨额罚款。（2）系统瘫痪是网络安全威胁带来的又一灾难性后果。恶意的网络攻击，如DDoS攻击，能够使电子信息系统的服务器承受巨大压力，导致服务中断。这对于依赖在线服务的企业，如电商平台、在线教育机构等，意味着业务的停滞和巨大的经济损失。同时，对于关键基础设施如电力、交通等领域的电子信息系统，系统瘫痪可能会影响到社会的正常运转，造成广泛的混乱和不便。（3）知识产权侵犯在电子信息工程中也屡见不鲜。创新成果如软件代码、专利技术等在网络环境中容易被窃取和非法复制。这严重打击了企业和个人的创新积极性，阻碍了行业的技术进步。

1.2 网络安全保障电子信息工程正常运行的机制

为了保障电子信息工程的正常运行，一系列的网络安全机制至关重要。（1）数据加密与认证是保护数据机密性和完整性的关键手段。通过对数据进行加密处理，即使数据在传输或存储过程中被截获，攻击者也难以解读其内容。认证机制则确保了数据的来源可信，防止了伪造和篡改。（2）访问控制与权限管理能够有效地限制用户对系统资源的访问。根据用户的身份和职责，为其分配适当的权限，避免了未经授权的访问和操作，降低了内部人员误操作或恶意行为的风险。（3）安全审计与监测则如同电子信息系统的“监视器”。它能够实时记录系统中的活动，并对异常行为进行监测和报警[1]。通过对审计日志的分析，可以及时发现潜在的安全威胁，追溯安全事件的源头，为后续的处理和防范提供依据。

2 电子信息工程中的网络安全威胁

2.1 网络攻击

网络攻击是电子信息工程面临的主要威胁之一，其形式多样，破坏性极大。（1）DDoS攻击（分布式拒绝服务攻击）是一种常见且极具破坏力的攻击方式。攻击者通过控制大量的傀儡机，同时向目标服务器发送海量的请求，使服务器的资源被迅速耗尽，从而无法处理正常用户的请求，导致服务瘫痪。这种攻击不仅会影响企业的正常运营，如在线购物网站无法交易、金融机构无法提供服务等，还可能对社会公共服务造成严重影响，如政府部门的在线服务中断。（2）SQL注入攻击则利用了网站在数据交互处理上的漏洞。通过精心构造恶意的SQL语句，攻击者能够绕过网站的正常验证机制，直接对数据库进行操作。这可能导致数据库中的数据被窃取、篡改甚至删除。对于依赖数据库存储重要信息的电子信息系统，如企业的客户数据库、医疗系统的患者信息库等，SQL注入攻击的后果不堪设想。（3）网络钓鱼是一种针对用户个人的欺诈手段。攻击者通过伪造看似合法

的网站，如银行网站、电商平台等，或者发送看似来自正规机构的欺诈性邮件，诱导用户输入个人敏感信息，如账号密码、信用卡信息等。一旦用户上当受骗，攻击者就能获取这些信息并用于非法目的，给用户带来直接的经济损失和隐私泄露风险。

2.2 恶意软件

恶意软件也是网络安全的一大“毒瘤”。（1）病毒具有自我复制和传播的特性。它们能够迅速在计算机系统中扩散，破坏文件、篡改系统设置，甚至导致整个系统崩溃。一些病毒还会隐藏在可执行文件或文档中，当用户不经意间打开时就会被感染，进而传播到其他相连的设备。（2）木马程序则以其隐蔽性著称。它们常常伪装成正常的软件或程序，在用户不知情的情况下被安装到计算机中[2]。一旦植入，木马就会在后台悄悄运行，窃取用户的个人信息、账号密码等重要数据，或者为攻击者打开远程控制的“后门”，使攻击者能够随意操纵用户的计算机。（3）蠕虫与病毒类似，但它的主要特点是能够自我传播。蠕虫会利用网络中的漏洞和弱点，迅速扩散到其他计算机和网络设备上。在传播过程中，它会大量占用网络资源，导致网络带宽被耗尽，网络拥堵，严重影响正常的网络通信和服务。

2.3 数据泄露

数据泄露是电子信息工程中极为严重的安全问题，其来源主要包括内部人员泄露和外部攻击泄露。（1）内部人员泄露往往是由于员工的疏忽大意或故意为之。例如，员工可能在未加密的移动存储设备上存储敏感数据，然后不慎丢失；或者由于对企业不满，故意将内部数据出售给竞争对手或第三方。这种泄露不仅会损害企业的商业利益，还可能导致法律纠纷和声誉受损。（2）外部攻击泄露则主要由黑客组织或不法分子通过各种技术手段突破企业的网络防线来实现。他们利用系统漏洞、网络监听、社会工程学等方法获取企业的敏感数据，如客户名单、财务报表、研发成果等。这些数据一旦落入不法分子手中，可能被用于欺诈、勒索、竞争分析等非法活动，给企业带来巨大的经济损失和竞争压力。

2.4 系统漏洞

系统漏洞是网络安全的潜在隐患，无论是操作系统还是应用软件，都难以完全避免。操作系统漏洞，如Windows、Linux等广泛使用的操作系统中存在的安全漏洞，为攻击者提供了可乘之机。这些漏洞可能存在于系统的内核、服务组件、驱动程序等部分。攻击者一旦发现并利用这些漏洞，就能够获取系统的最高权限，从而完全控制整个系统，安装恶意软件、窃取数据或者破坏系统。应用软件漏洞同样不容忽视。浏览器、办公软件等常用的应用程序由于其复杂性和广泛的用户基础，成为了攻击者的重点目标。这些漏洞可能存在于软件的功能模块、插件接口、更新机制等方面。一旦被利用，攻击者可以通过诱导用户访问恶意网页、打开恶意文档等方式实施攻击，从而在用户的计算机上执行恶意代码，达到窃取信息或控制计算机的目的。

3 电子信息工程中的网络安全防护策略

3.1 访问控制

访问控制是网络安全防护的重要手段之一，旨在确保只有合法授权的用户能够访问特定的资源和信息。（1）用户身份认证是访问控制的基础。采用多种认证方式可以极大地提高认证的准确性和安全性。除了传统的密码认证，生物识别技术如指纹、面部识别等正逐渐得到广泛应用。指纹识别基于每个人独特的指纹特征，具有高度的准确性和难以伪造性。面部识别则通过分析面部的几何形状和特征来验证用户身份，使用方便且不易遗忘。此外，还可以采用智能卡、短信验证码等多因素认证方式，进一步增强身份认证的可靠性[3]。例如，在金融领域的电子信息系统中，用户登录可能需要同时输入密码和通过手机接收的短信验证码，以确保是本人操作。（2）权限管理是访问控制的核心环节。根据用户在组织中的角色和职责，为其分配相应的权限。对于敏感信息和关键操作，如财务数据的修改、重要系统配置的更改等，应限制只有特定的高级管理人员或授权人员能够进行操作。同时，权限应根据用户的岗位变动和业务需求及时进行调整和更新。比如，当员工离职时，应立即撤销其所有权限，避免潜在的安全风险。

3.2 加密技术

加密技术是保护数据机密性和完整性的关键策略。（1）数据加密通过对数据进行编码和转换，使其在未经授权的情况下难以理解和读取。常见的加密算法包括对称加密算法（如AES）和非对称加密算法（如RSA）。对称加密算法速度快，适用于大量数据的加密，但需要安全地共享密钥。非对称加密算法则解决了密钥分发的难题，但加密和解密速度较慢。在实际应用中，常常结合使用两种算法，例如使用非对称加密算法来交换对称加密算法的密钥，然后使用对称加密算法对实际数据进行加密。对于重要的商业机密、个人隐私数据等，加密技术能够有效防止数据泄露和篡改。（2）传输加密则侧重于保障数据在网络传输过程中的安全。SSL/TLS协议是目前广泛应用的传输加密协议，为网页浏览、电子邮件传输等提供了加密通道。当用户在浏览器中访问使用

HTTPS协议的网站时，浏览器与服务器之间的通信就会通过SSL/TLS协议进行加密，防止通信内容被窃听和篡改。此外，虚拟专用网络（VPN）技术也常用于建立安全的远程访问通道，使得员工在公共网络中能够安全地访问企业内部网络资源。

3.3 防火墙与入侵检测系统

防火墙是网络边界的第一道防线，能够有效阻止未经授权的网络访问和恶意攻击。（1）防火墙可以根据预设的规则对网络流量进行过滤和控制。例如，可以禁止外部网络对内部特定端口的访问，或者只允许来自特定IP地址的流量进入。状态检测防火墙还能够跟踪连接的状态，判断数据包是否属于合法的连接，从而提高了防护的准确性。在企业网络中，通常会部署硬件防火墙来保护整个网络的安全，同时在个人计算机上也可以安装软件防火墙来增强本地防护。（2）入侵检测系统则是对防火墙的有效补充，能够实时监测网络活动，发现潜在的入侵行为。入侵检测系统通过分析网络数据包、系统日志等信息，识别异常的活动模式和攻击特征。一旦检测到可疑的活动，如异常的端口扫描、大量的错误登录尝试等，就会发出警报并采取相应的措施。入侵预防系统（IPS）则更进一步，不仅能够检测入侵行为，还能够主动阻止攻击流量。

3.4 安全审计与监测

安全审计与监测是发现和预防网络安全事件的重要手段。（1）日志审计通过收集和分析系统、应用程序和网络设备产生的日志信息，提供对过去活动的追溯和审查。这些日志包括用户登录日志、系统操作日志、网络访问日志等。通过对日志的定期分析，可以发现异常的活动，如异常的登录时间、频繁的访问敏感数据等，从而及时采取措施。同时，日志审计也有助于满足合规性要求，为企业的安全管理提供证据支持。（2）实时监测则能够及时发现当前正在发生的安全事件。通过使用网络流量监测工具、系统性能监测工具等，可以实时了解网络和系统的状态。例如，通过监测网络流量的异常变化，可以发现可能的DDoS攻击；通过监测系统性能指标的突然下降，可以发现潜在的恶意软件感染。实时监测还可以结合威胁情报，及时了解最新的攻击手法和威胁信息，提高对新型威胁的防范能力。

3.5 员工培训与安全意识教育

员工是网络安全防线中的重要环节，然而往往也是最容易被忽视的薄弱点。（1）定期的安全培训可以让员工了解最新的网络威胁和防范方法。培训内容可以包括网络安全基础知识、常见的网络攻击手段（如钓鱼邮件、社交工程攻击等）、安全的计算机使用习惯等。通过实际案例分析和模拟演练，让员工亲身体验网络攻击的危害和应对方法，提高他们的应急处理能力。（2）安全意识教育则着重培养员工的安全意识和责任感。让员工明白保护企业信息资产的重要性，以及自身在网络安全中的角色和责任[4]。鼓励员工主动遵守安全规定，如不随意共享账号密码、不使用未经授权的移动存储设备等。同时，建立奖励机制，对发现和报告安全隐患的员工给予表彰和奖励，营造良好的安全文化氛围。

结语：综上所述，电子信息工程中的网络安全至关重要。我们清晰认识到网络安全威胁带来的严重影响，也明确了保障其正常运行的机制和有效的防护策略。但网络安全是一个不断发展的领域，新的威胁和挑战层出不穷。未来，我们需要持续关注技术发展，不断完善防护策略，加强合作与交流，提高员工的安全意识和技能。只有这样，才能为电子信息工程的发展营造一个安全可靠的网络环境，充分发挥其在推动社会进步和经济发展中的重要作用。

参考文献

[1]王宇.电子信息工程中网络安全技术的应用[J].信息与电脑(理论版),2020(21):198-200.

[2]张晨.电子信息工程中的网络安全问题及防护策略[J].网络安全技术与应用,2021(09):12-14.

[3]李阳.浅析网络安全技术在电子信息工程中的应用[J].数字通信世界,2022(02):167-169.

[4]刘辉.电子信息工程中的网络安全防护研究[J].中国新通信,2023(06):87-89.