计算机网络安全管理与有效运行探究

陈国栋
广东科贸职业学院　广东　广州　510430

摘　要：随着计算机网络的普及和信息化时代的到来，网络安全问题逐渐凸显。计算机网络安全管理不仅是技术问题，更是涉及组织运营、风险管理等多个层面的综合问题。本文对计算机网络安全管理进行了深入探究，旨在为确保网络安全的有效运行提供指导。

关键词：网络安全；管理；有效运行

1 计算机网络安全概述

随着信息技术的迅猛发展，计算机网络安全已成为当今社会的核心议题。简单地说，计算机网络安全涉及的是保护计算机网络系统中的硬件、软件及其数据，使其免受各种威胁，保持其正常运行和机密性的过程。在计算机网络安全的领域中，威胁主要来自各个方面，包括但不限于：黑客攻击、病毒和蠕虫的传播、拒绝服务攻击、恶意软件的威胁、物理设备损坏、以及人为错误等。这些威胁可能导致数据泄露、系统崩溃、服务中断，甚至对整个社会造成严重的影响。为了应对这些威胁，计算机网络安全的防护体系应运而生[1]。这个体系通常包括防火墙、入侵检测系统（IDS/IPS）、安全事件管理（SIEM）、加密技术、身份认证等众多组件。这些组件协同工作，旨在预防、检测、响应和恢复各种网络安全事件。尽管有这些防护措施，网络安全问题依然层出不穷。这主要是因为网络攻击者的手段不断更新，新的威胁不断涌现。我们必须保持警惕，持续关注和学习新的安全知识和技术，以确保我们的计算机网络始终安全有效。

2 计算机网络安全威胁类型

计算机网络安全威胁类型繁多，以下是一些主要的类型：（1）恶意软件（Malware）：包括病毒、蠕虫、特洛伊木马等，这些软件旨在破坏、干扰或恶意利用计算机系统。（2）拒绝服务（DoS）攻击和分布式拒绝服务（DDoS）攻击：通过大量请求拥塞目标系统，使其无法正常处理合法用户请求。（3）网络钓鱼（Phishing）：通过伪装成合法来源，诱骗用户提供敏感信息，如账号、密码等。（4）跨站脚本攻击（XSS）：攻击者在网页中注入恶意脚本，当用户访问该网页时，脚本会在用户浏览器上执行，窃取用户信息。（5）SQL注入攻击：攻击者通过输入恶意的SQL代码，获取、修改或删除数据库中的数据。（6）中间人攻击（Man-in-the-Middle，MITM）：攻击者截获并篡改两个通信实体之间的信息。（7）网络侦查（Eavesdropping）：攻击者通过监听网络流量，获取敏感信息。（8）系统漏洞利用：利用操作系统或应用程序的漏洞，进行非法访问或破坏。（9）身份盗用和假冒：使用他人的身份信息进行非法活动。（10）网络钓鱼（Spear Phishing）：针对特定组织的成员进行网络钓鱼，窃取敏感信息。

3 计算机网络安全管理策略

3.1 安全管理组织与人员培训

为了确保计算机网络的安全，需要制定一套全面的安全管理策略。制定并发布安全政策，明确员工在网络安全方面的责任和义务。确保所有员工都了解并遵守这些规定，确保只有授权人员能够访问关键设备和区域，例如服务器机房、数据中心等。实施严格的访问控制策略，包括用户身份验证、权限管理和审计跟踪，定期备份重要数据，并制定应急恢复计划，以应对数据丢失或系统故障。使用入侵检测系统（IDS）和防火墙等工具，实时监控网络流量和潜在威胁。及时更新操作系统、应用程序和数据库，以确保安全漏洞得到修补，定期开展网络安全培训，提高员工对网络安全的认识和防范意识。制定针对不同安全事件的应急响应计划，包括安全事件报告、调查和恢复流程，定期进行合规性检查，确保公司政策和国家法律法规得到遵守，与合作伙伴和供应商建立安全协议，确保供应链的安全[2]。

安全管理组织与人员培训为了实施上述安全管理策略，需要建立一个安全管理组织，并定期进行人员培训。以下是一些关键的步骤：成立一个由IT专家、安全专业人员和业务领导组成的安全管理团队。该团队负责制定、实施和维护安全策略，为团队成员分配明确的职责，确保每个人都清楚自己的任务和责任，根据组织的需要和员工的技能水平，制定个性化的培训计划。培训内容应涵盖网络安全基础、安全工具和技术、应急响应

等方面的知识。定期开展培训课程和研讨会，鼓励员工参加外部培训和认证。对员工的培训成果进行考核，以确保培训的有效性，鼓励员工不断学习新的安全技术和最佳实践，跟踪网络安全领域的最新动态。通过参加行业会议、研究文献和参与安全社区活动，提高团队的整体水平。建立有效的沟通机制，确保团队成员之间的信息共享和协作。定期召开安全会议，讨论安全事件、风险评估和改进措施，设立奖励机制，表彰在网络安全方面做出突出贡献的员工。这可以提高员工的工作积极性和归属感。定期审查现有的安全管理策略和流程，根据组织的业务发展和安全威胁的变化进行调整和优化。通过收集员工的反馈和建议，不断完善安全管理组织的工作。

3.2 安全策略制定与实施

安全策略的制定是确保组织信息安全的关键步骤，其实施则需谨慎且全面。首先，对组织的信息系统进行深入了解，识别关键资产、业务需求和潜在的安全风险。这一步骤有助于明确安全策略的目标和优先级，基于需求分析的结果，制定详细的安全政策和标准。这些政策应覆盖身份验证、访问控制、数据保护和事件响应等领域。对组织当前的安全状况进行评估，识别潜在的安全威胁和漏洞。利用风险评估工具和技术，对威胁进行定性和定量分析，确保安全策略符合国家和行业的法律法规要求。这有助于避免潜在的法律风险。在策略初步制定后，进行内部审查和外部咨询，收集各方意见，对策略进行必要的调整。

安全策略的实施：第一，资源分配：确保有足够的资源（人力、财力、技术）来支持安全策略的实施，根据策略的需求，合理分配资源。第二，培训与意识：为员工提供安全培训，提高他们对安全策略的认识和理解。通过宣传活动增强员工的安全意识，第三，工具与技术实施：根据安全策略的要求，部署合适的安全工具和技术，如防火墙、入侵检测系统、加密技术等，第四，监控与审计：建立监控和审计机制，实时监测信息系统的安全状况，定期进行内部审计，确保安全策略的有效执行。第五，事件响应与处置：制定详细的事件响应计划，培训专业的安全团队，以便在发生安全事件时迅速响应，减轻潜在的损失，第六，持续改进：定期审查安全策略的实施效果，收集反馈，持续优化和改进安全策略，以应对不断变化的安全威胁。第七，记录与报告：对安全策略的实施过程进行详细记录，定期生成安全报告，向上级管理层汇报安全状况，第八，合作伙伴与供应链管理：与合作伙伴和供应商建立紧密的安全合作关系，确保整个供应链的安全，第九，应急响应计划：制定针对不同安全事件的应急响应计划，明确各部门的职责和操作流程。第十，外部合作与情报共享：与外部机构和组织建立合作关系，共享安全情报，共同应对复杂的网络安全挑战。

3.3 安全审计与监控

安全审计是对组织的信息系统进行全面审查和评估的过程。它通过对系统的安全性、合规性和可靠性等方面进行检查，识别潜在的安全隐患和漏洞。审计的内容可以包括系统的硬件和软件配置、数据安全、用户权限等方面，通过审查相关的日志文件、配置文件和网络流量等数据，评估系统的安全性能和风险水平。

过部署监控工具和技术，可以实时收集和分析系统的网络流量、日志信息、异常行为等数据，及时发现异常情况和潜在的攻击行为[3]。监控的范围可以包括网络监控、系统监控、数据库监控等方面，以便全面了解系统的安全状况和风险趋势。安全审计与监控的目的是为了及时发现和处理安全问题，防止潜在的攻击和数据泄露事件发生。通过定期进行安全审计和实时监控，组织可以及时发现和处理安全问题，采取相应的措施进行防范和应对。

3.4 应急响应与恢复

应急响应与恢复是组织应对突发事件和安全事件的关键环节。在发生安全事件时，及时、准确地响应和恢复系统是至关重要的，以减少潜在的损失和影响，应急响应是指在安全事件发生后，迅速采取措施进行处置和应对的过程。这包括对事件的初步分析和评估、采取适当的缓解措施、启动应急计划等。应急响应团队应由具备专业知识和经验的人员组成，以便快速响应和处置安全事件。在应急响应过程中，应保持冷静和客观，对事件进行全面分析，了解事件的性质、影响范围和严重程度。应采取适当的措施来缓解事件的影响，防止事态扩大。如果事件可能涉及法律责任或合规性问题，应及时通知相关法律和监管机构。一旦事件得到初步控制，应立即启动应急计划，协调各方资源，进行系统恢复和重建工作。这包括数据备份和恢复、系统重构和漏洞修补等。在恢复过程中，应确保数据的一致性和完整性，并尽快将系统恢复到正常状态。

4 网络安全技术防范措施

4.1 防火墙技术

防火墙技术是一种用于隔离内部网络和外部网络的系统，可以阻止未经授权的访问和数据传输。通过防火墙的部署，可以有效地控制网络流量，过滤掉恶意请求和数据包，保护内部网络免受攻击和入侵。防火墙技术

的工作原理是基于访问控制列表（ACL）或安全策略，对进出网络的数据包进行筛选和过滤。根据预设的安全规则，防火墙可以拒绝或允许特定的网络流量通过，从而实现对网络访问的控制和管理。常见的防火墙技术包括包过滤防火墙和应用代理防火墙。包过滤防火墙通过检查数据包的源地址、目的地址、端口号等关键信息来确定是否允许该数据包通过。而应用代理防火墙则是在应用层上实现代理服务，对应用层的数据进行过滤和控制。部署防火墙时，需要根据组织的网络安全需求和实际情况选择合适的防火墙设备和配置。防火墙技术是网络安全技术防范措施的重要组成部分。

4.2 入侵检测与防御技术

入侵检测技术通过实时监控网络流量和系统状态，发现异常行为或潜在的攻击行为，及时发出警报并采取相应的措施进行防御。它能够检测出各种类型的攻击，如拒绝服务攻击、恶意代码注入、端口扫描等，同时还能识别出恶意流量的来源和传播途径。入侵防御技术则是在入侵检测的基础上，采取主动防御的策略，对恶意流量进行过滤和屏蔽，防止攻击的进一步扩散和危害。它通过在关键节点上部署入侵防御系统，能够有效地防御各种网络攻击和病毒传播[4]。

入侵检测与防御技术的主要作用有以下几个方面：（1）实时监控和检测：对网络流量和系统状态进行实时监控，及时发现异常行为和潜在的攻击行为。（2）警报和响应：在发现攻击时，及时发出警报并采取相应的措施进行防御，如隔离被攻击的主机、切断恶意流量等。（3）威胁情报：通过对攻击者的行为进行分析和挖掘，获取威胁情报，为后续的防御和反击提供支持。（4）防御和反击：采取主动防御的策略，对恶意流量进行过滤和屏蔽，同时能够追踪攻击者的来源和意图，进行反击。

4.3 数据加密技术

数据加密的基本原理是将明文数据转换为密文数据，使得未经授权的人员无法获取原始数据内容。这个过程通常涉及到一个加密算法和一个密钥，其中加密算法用于将明文转换为密文，而密钥则控制着加密和解密的过程。根据加密密钥的类型，数据加密技术可以分为对称加密和非对称加密两种。对称加密采用相同的密钥进行加密和解密操作，常见的对称加密算法有AES、DES等。非对称加密则使用两个密钥：公钥和私钥。公钥用于加密数据，私钥用于解密数据，常见的非对称加密算法有RSA、ECC等。在实际应用中，数据加密技术广泛应用于各类场景，如电子商务、电子银行、远程登录等。通过数据加密，可以确保数据的机密性，防止未经授权的访问和窃取。数据加密还可以提供数据的完整性保护，防止数据被篡改或损坏。

结束语

我们强调计算机网络安全不仅是技术问题，更是组织层面的综合管理问题。只有从组织层面进行全面的管理和协调，才能确保网络安全的有效运行。我们希望本文的研究能为相关组织提供有益的参考和启示，共同推动计算机网络安全的发展与进步。

参考文献

[1]孙海龙.计算机网络安全管理与有效运行探究[J].电子元器件与信息技术,2023,7(2):202-205. DOI:10.19772/j.cnki.2096-4455.2023.2.049.

[2]王萍,王玉静.计算机网络安全管理与有效运行探究[J].电脑采购,2023(1):23-25.

[3]李修滨.计算机网络安全管理与有效运行探究[J].数字化用户,2023(52):51-52.

[4]吴东亮.计算机网络安全管理与有效运行探究[J].电脑爱好者（校园版）,2022(20):13-15. DOI:10.12277/j.issn.1674-702X.2022.20.005.