计算机网络安全策略浅议

汇报人：

2023-12-19

目录

01

引言

网络安全的重要性

01

信息保密性

保护个人、组织或国家的信息不被未经授权的访问、使用、泄露或破坏。

02

信息完整性

确保信息在传输或存储过程中不被篡改或损坏，保持信息的真实性和可信度。

03

可用性

确保授权用户需要时能够访问和使用信息，防止拒绝服务攻击等导致信息不可用的情况。

网络安全策略的目的和意义

规范网络行为

通过制定明确的网络安全策略，规范用户在网络中的行为，减少网络攻击和数据泄露的风险。

保障业务连续性

有效的网络安全策略能够确保业务的连续性和稳定性，避免因网络安全事件导致的业务中断或损失。

提高安全意识

网络安全策略的制定和实施有助于提高用户的安全意识，增强对网络安全的重视和认识。

应对法律和合规要求

遵循相关法律法规和行业标准，制定和实施网络安全策略是组织应尽的义务和责任。

02

计算机网络安全威胁分析

外部威胁

黑客攻击

黑客利用漏洞和弱点，通过恶意软件、病毒、木马等手段入侵计算机系统，窃取敏感信息或破坏数据。

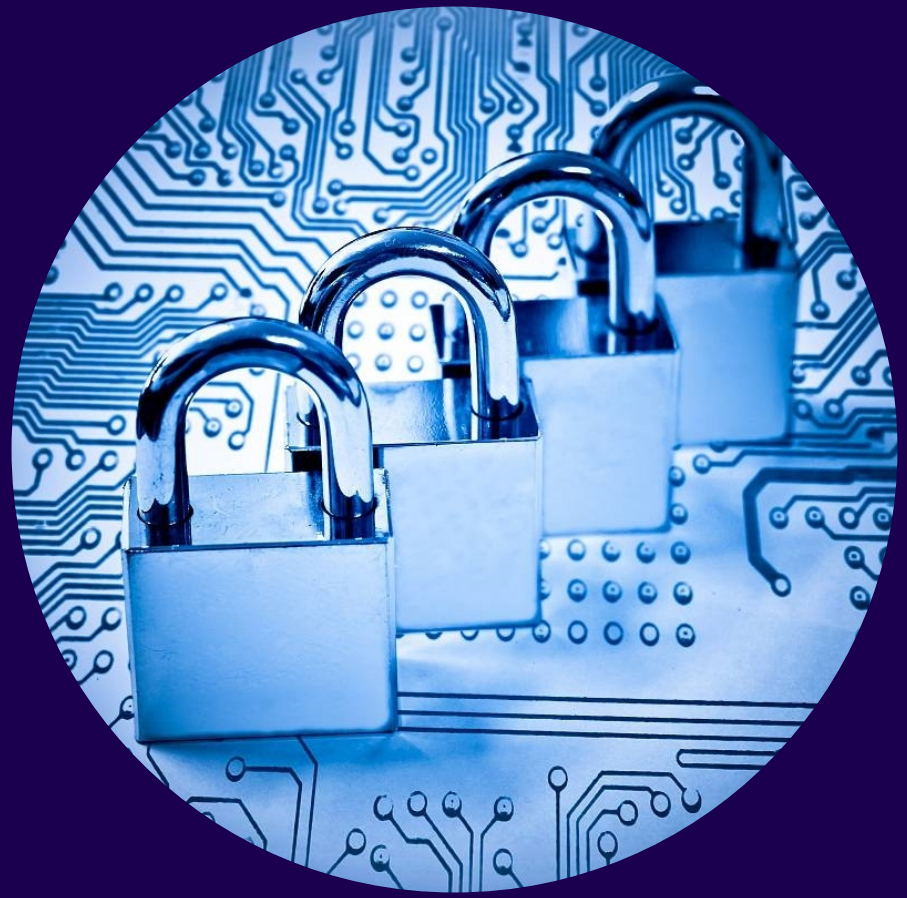
钓鱼攻击

通过伪造信任网站或电子邮件，诱骗用户输入用户名、密码等敏感信息，进而窃取个人信息。

分布式拒绝服务攻击

攻击者利用大量计算机发起攻击，使目标服务器过载，导致服务不可用。

内部威胁



内部人员泄密

员工无意或故意泄露敏感信息，如企业机密、客户资料等。

误操作

员工在操作过程中误删除、修改数据或配置不当，导致安全问题。

恶意软件感染

内部网络中存在恶意软件，如病毒、蠕虫等，导致数据泄露或系统崩溃。

威胁发展趋势

01

高级持续性威胁

攻击者针对特定目标发起长期、复杂的网络攻击，窃取敏感信息或破坏数据。

02

物联网安全

随着物联网技术的发展，设备之间的互联互通带来了新的安全挑战。

03

人工智能与网络安全

人工智能技术在网络安全领域的应用逐渐增多，如自动化漏洞扫描、威胁情报分析等。

03

计算机网络安全策略制定

访问控制策略

01

身份认证

通过用户名、密码、指纹等方式对用户进行身份认证，确保只有授权用户才能访问特定资源。

02

访问权限

根据用户角色和职责，分配不同的访问权限，确保用户只能访问其所需的数据和功能。

03

访问控制列表

通过设置访问控制列表，对用户访问进行细粒度控制，防止未经授权的访问。

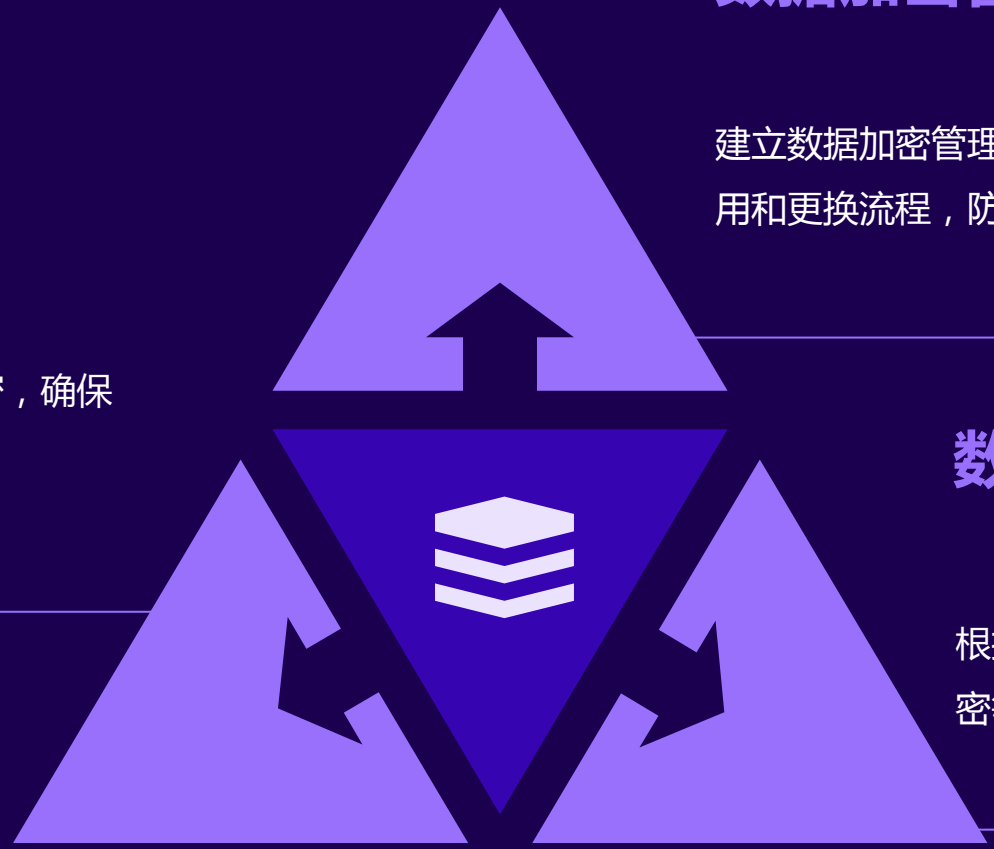
数据加密策略

数据加密管理

建立数据加密管理制度，明确加密密钥的管理、使用和更换流程，防止密钥泄露。

数据加密算法

采用高强度加密算法对数据进行加密，确保数据在传输和存储过程中的安全性。



数据加密等级

根据数据的重要性和敏感性，确定不同的加密等级，对重要数据进行更高级别的加密。