第6章 Windows系统的安全机制

Windows NT安全系统概述

Windows NT安全架构

Windows NT安全架构是基于对象的访问控制模型，通过定义用户权限和角色来控制对系统资源的访问。

安全子系统组件

安全子系统组件包括安全账户管理器(SAM)、本地安全授权(LSA)、安全引用监视器等，它们共同工作以确保系统安全。

安全策略与管理

安全策略定义了系统安全规则，包括密码策略、账户锁定策略等，而管理则是通过组策略和安全模板来实现。

用户账户与权限管理

01

用户账户类型与创建

Windows NT支持不同类型的用户账户，包括本地用户和域用户，创建时需设定账户名、密码及权限级别。

02

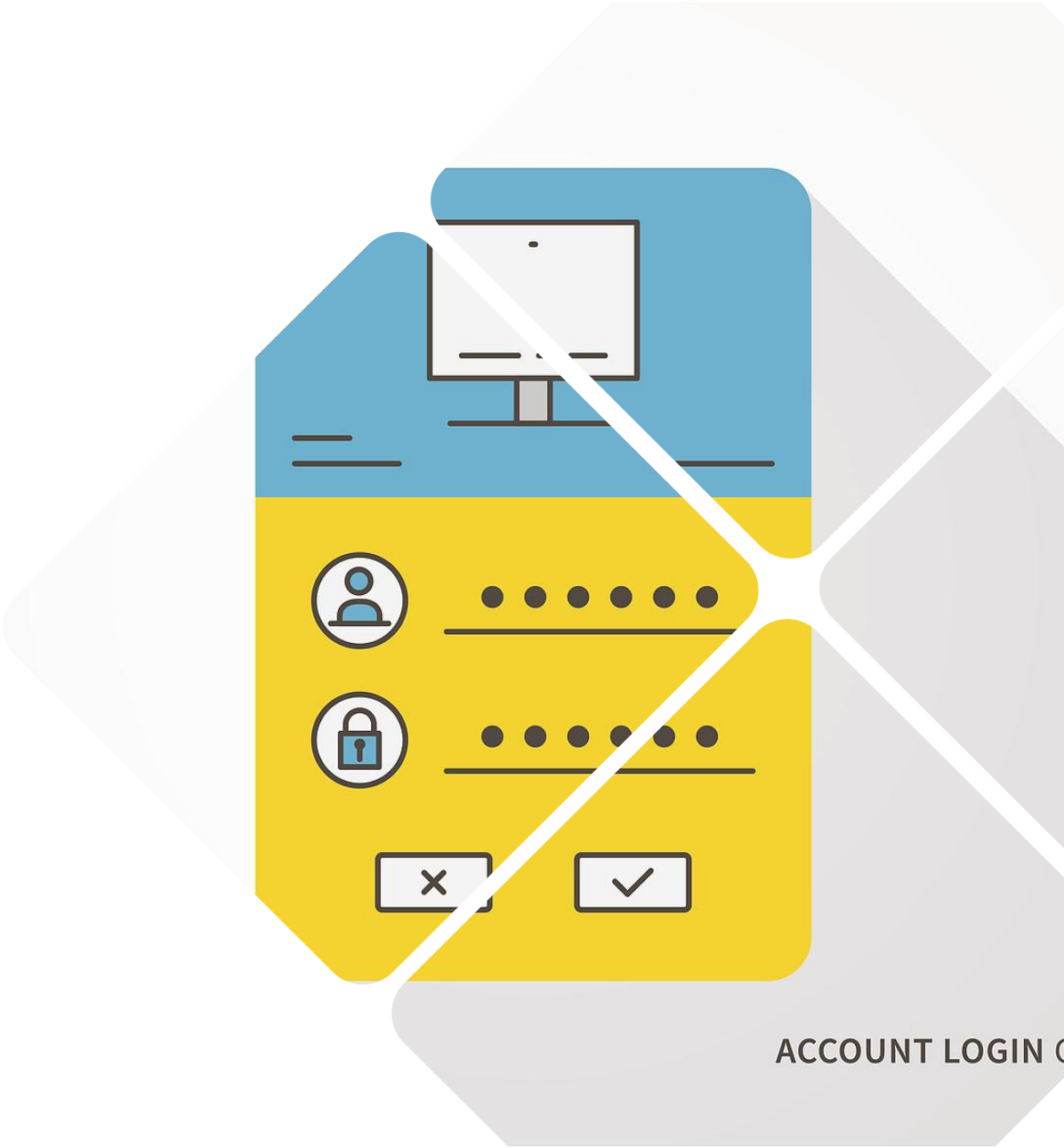
权限分配与控制

权限分配是通过设置文件、文件夹和注册表项的访问控制列表(ACL)来控制用户和组的访问权限。

03

组策略的应用

组策略允许管理员集中配置和管理用户和计算机的设置，通过编辑组策略对象(GPO)来应用安全设置。



审核策略与日志管理

01

审核策略的配置

配置审核策略可以追踪系统事件，如登录尝试、文件访问和系统错误，以帮助检测和分析潜在的安全威胁。

02

安全日志的分析

安全日志记录了审核策略捕获的事件，通过分析这些日志可以发现异常行为并采取相应的安全措施。

03

审计结果的处理

处理审计结果包括定期审查日志、识别和响应安全事件，以及根据审计结果调整安全策略和权限设置。

系统服务与进程安全

关键系统服务的管理

关键系统服务如DHCP、DNS和远程注册表服务需要严格管理，以防止未授权访问和配置错误。

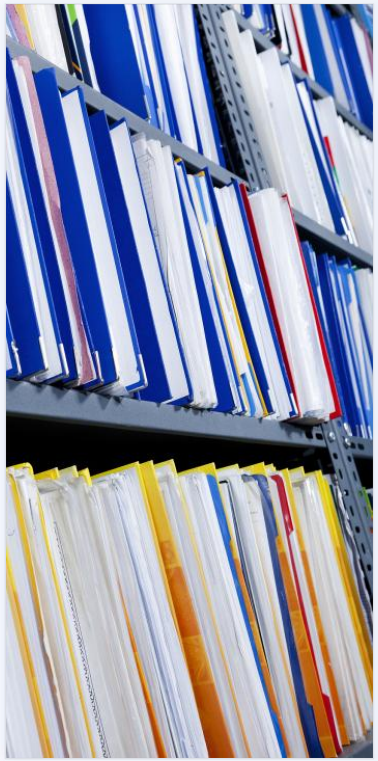
进程权限的控制

控制进程权限可以防止恶意软件和病毒利用高权限进程执行破坏性操作。

服务与进程的监控

监控服务和进程可以及时发现异常活动，包括服务的启动和停止、进程的创建和结束，以及它们的资源使用情况。

注册表与文件系统安全



注册表安全设置

注册表是Windows系统的核心数据库，通过限制对特定注册表项的访问，可以增强系统的安全性。

文件系统权限配置

文件系统权限配置确保只有授权用户和程序能够访问或修改文件和文件夹，从而保护数据不被未授权访问。

数据保护策略

数据保护策略包括使用加密技术、定期备份和灾难恢复计划，以确保数据在面临威胁时的安全性和完整性。

网络安全与防火墙配置

网络安全策略的制定

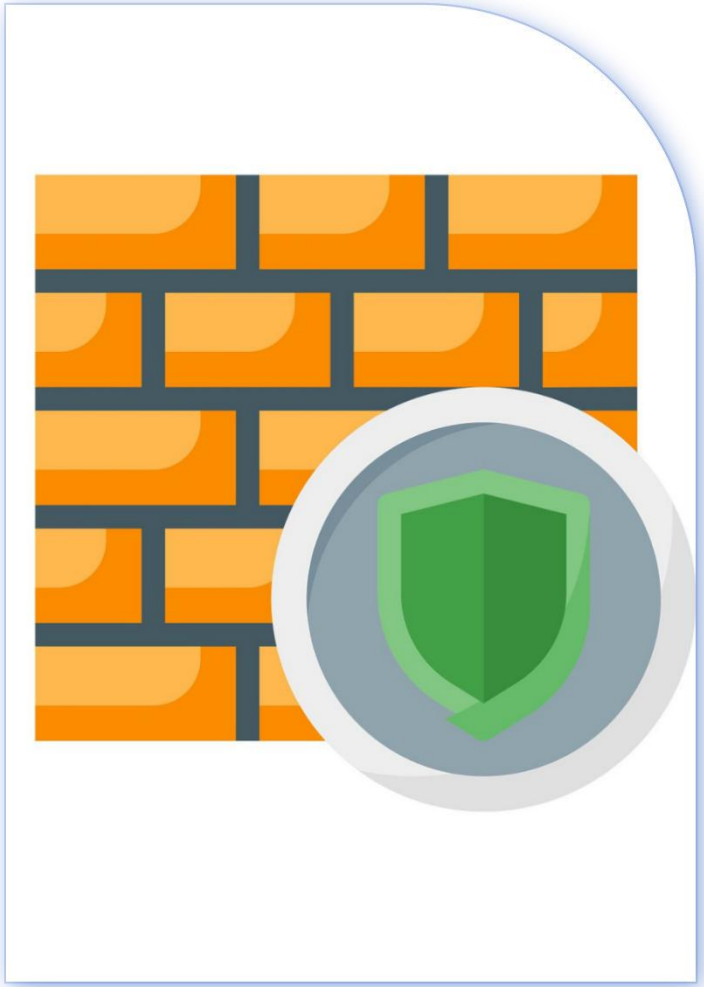
网络安全策略包括定义哪些网络流量是允许的，哪些是被阻止的，以及如何处理入侵尝试。

防火墙规则的设置

防火墙规则的设置涉及配置入站和出站规则，以过滤网络流量并防止未授权访问。

入侵检测与防御

入侵检测系统(IDS)和入侵防御系统(IPS)能够识别和响应潜在的网络攻击，保护网络不受威胁。



加密技术与数据保护

加密文件系统(EFS)

EFS允许用户对文件和文件夹进行加密，确保数据即使在物理存储介质被盗或丢失的情况下也能保持安全。

BitLocker驱动器加密

BitLocker提供全盘加密，保护整个驱动器的数据，包括操作系统和启动数据，防止未经授权的访问。

数据备份与恢复策略

定期备份数据和制定有效的恢复策略是防止数据丢失的关键，确保在系统故障或安全事件后能够迅速恢复。

远程访问与VPN安全

01

远程访问策略

远程访问策略控制谁可以连接到网络，以及他们可以如何连接，包括通过VPN或远程桌面连接。

02

虚拟私人网络(VPN)配置

VPN配置涉及设置加密通道和身份验证机制，以确保远程用户与企业网络之间的通信安全。

03

远程桌面与远程协助安全

远程桌面和远程协助功能需要适当配置和管理，以防止未授权访问和数据泄露。

安全更新与补丁管理

01

自动更新的配置

自动更新配置确保系统及时接收到最新的安全补丁和更新，以防范已知漏洞。

02

补丁部署的最佳实践

补丁部署的最佳实践包括测试补丁、计划部署时间以及回滚机制，以减少对业务连续性的影响。

03

应对零日攻击的策略

零日攻击指的是利用尚未公开的漏洞进行攻击，应对策略包括及时应用安全补丁、使用入侵检测系统和加强监控。