学校网络安全年度工作总结报告

汇报人：XXX

2024-01-01

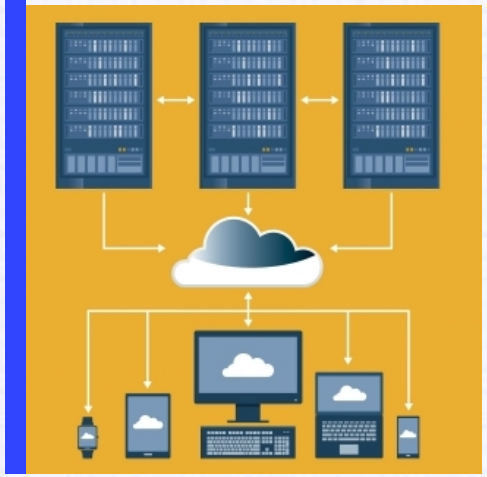
目录

CONTENTS

01 工作概况

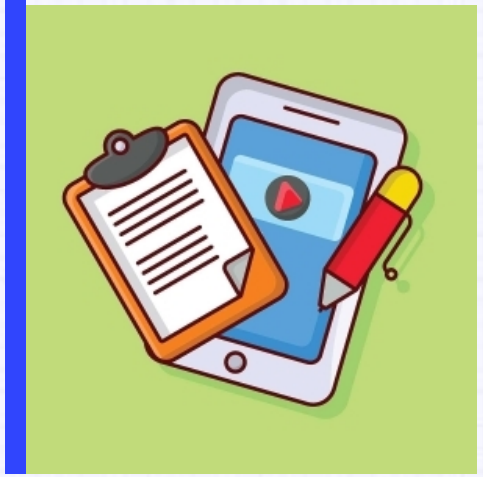
工作目标

确保学校网络系统的安全稳定运行。



提高师生网络安全意识，预防网络攻击和数据泄露。

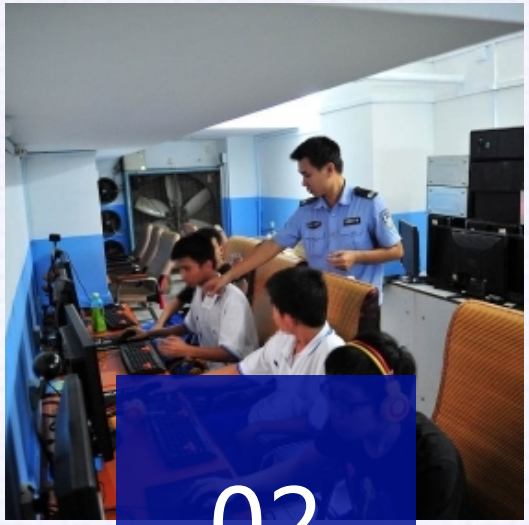
建立完善的网络安全管理体系，提升学校网络安全防护能力。



工作内容

01

制定网络安全管理制度和应急预案。



02

定期进行网络安全漏洞扫描和风险评估。

03

组织师生参加网络安全培训和演练。

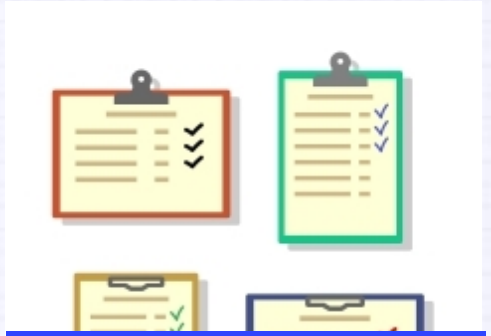
04

加强校园网出口管理和网络监控。

工作成果

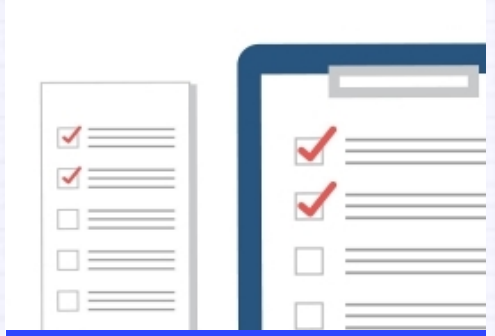
01

成功防御多次网络攻击和数据泄露事件。



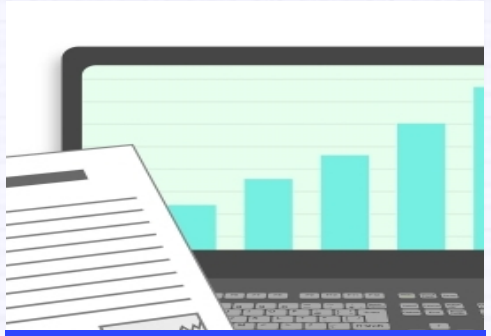
02

提高师生网络安全意识和操作技能。



03

完善了网络安全管理体系和应急响应机制。



04

提升了学校网络安全防护能力和水平。

02 安全防护工作

防火墙配置

防火墙规则更新

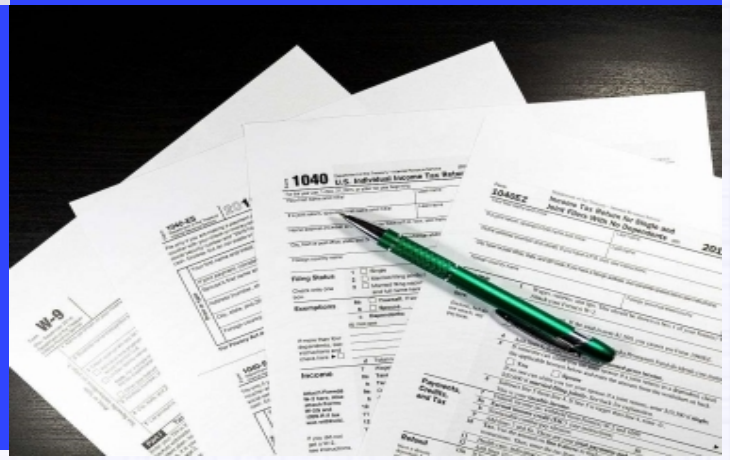
定期检查并更新防火墙规则，以应对新型网络威胁。

端口扫描与漏洞检测

定期进行端口扫描和漏洞检测，确保防火墙无漏洞。

访问控制策略

根据学校网络需求，制定合理的访问控制策略，限制不必要的网络访问。



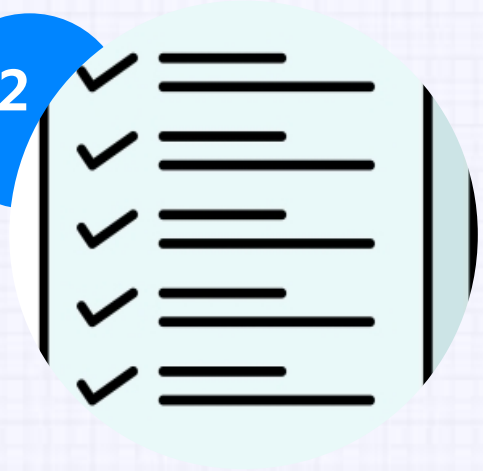
入侵检测与防御

01

入侵检测系统部署

配置入侵检测系统，实时监测网络流量，发现异常行为。

02



入侵防御系统升级

及时升级入侵防御系统，提高对新型攻击的防御能力。

03

安全日志分析

定期分析安全日志，发现潜在的安全隐患。

数据备份与恢复

数据备份策略制定

根据学校数据的重要性，制定合理的备份策略。

备份数据存储安全

确保备份数据存储在安全的环境中，防止数据泄露。

数据恢复演练

定期进行数据恢复演练，确保数据备份的有效性。

病毒防范与处理

防病毒软件部署

配置防病毒软件，实时监测和清除病毒。

病毒库更新

定期更新防病毒软件的病毒库，提高对新型病毒的防御能力。

病毒事件应急处理

建立应急处理机制，及时处理病毒事件，防止病毒扩散。

03 安全事件处置