

Sophos 咨询服务

在网络威胁持续演变的时代，主动降低风险，提升业务韧性

定制化，专家主导的安全评估

在数字化转型不断深入、AI 技术快速发展、网络威胁日益复杂的当下，前瞻性的企业深知，网络安全不仅是技术问题，更是企业战略中的一项重点。面对高级攻击者、监管机构的严格要求以及利益相关方的关注，企业需要以主动且全面的方式保护自身数字资产。Sophos 咨询服务提供独立的专业视角、丰富的实践经验和针对性的安全策略，帮助企业识别系统性风险、增强防御能力、提升整体韧性。

我们的资深安全专家采用真实威胁行为者常用的战术、技术和流程 (TTPs)，对企业的网络、系统和人员进行全面测试，助力企业实现以下目标：

- 在漏洞被攻击者利用之前主动发现并修复。
- 提升抵御复杂威胁的防御能力。
- 满足监管合规要求。
- 评估事件响应能力。
- 增强客户、合作伙伴及利益相关方的信任。

主动强化防御能力，优化安全态势

渗透测试

渗透测试通过模拟真实网络攻击，帮助企业识别系统、网络和应用中的安全漏洞。经验丰富的测试人员（道德黑客）会尝试利用这些漏洞，模拟攻击者可能造成的影响。

渗透测试主要分为两类：外部渗透测试：针对可通过互联网访问的系统（如网站、VPN、公网服务）进行测试，模拟攻击者从外部突破企业防线的情景。内部渗透测试：模拟内部威胁或攻击者已突破外围防线后，针对内部网络中的系统、应用和数据进行测试。

价值体现：

- 发现常规扫描难以侦测的隐藏风险。
- 提供可操作的改进建议，助力企业强化防御。
- 满足行业合规要求（如 PCI DSS、HIPAA、GDPR、NIS、ISO 27001、SOC 2）。
- 展现企业主动管理安全风险的承诺。
- 全面覆盖外围与内部潜在风险。

帮助解答的关键问题：

- › 我们基础设施中存在哪些关键漏洞？
- › 攻击者能否轻易突破我们的外部防线？
- › 若攻击者已进入内部网络，可能面临哪些风险？
- › 成功攻击可能造成哪些影响？
- › 针对发现的漏洞，企业应采取哪些补救措施？

无线网络安全测试

无线网络安全测试评估企业 Wi-Fi 网络及其基础架构的安全性，并检查是否符合相关合规要求。测试人员将尝试利用加密、身份验证和访问控制中的弱点发起攻击。

无线安全测试一般包括两个范围：被动评估：通过监听无线流量，识别未经授权的设备、恶意接入点以及配置错误，不主动连接或干预网络。主动评估：模拟攻击者破解加密、绕过身份验证、获取未经授权的访问权限，主动测试无线网络中的漏洞。

价值体现：

- › 保护通过无线网络传输的敏感数据。
- › 发现恶意接入点及配置问题。
- › 确保无线安全策略符合最佳实践。
- › 降低因 Wi-Fi 漏洞导致的数据泄露风险。
- › 同时评估被动暴露风险和主动利用风险。

帮助解答的关键问题：

- › 是否有未授权用户可访问我们的无线网络？
- › 我们是否采用了强加密和安全的身份验证机制？
- › 是否存在恶意设备接入我们的网络？
- › 攻击者能否绕过我们的无线安全防护？
- › 我们可以采取哪些措施提升无线网络安全性？

Web 应用安全评估

Web 应用通常处理企业核心业务数据和客户数据，因此也是攻击者的重点目标之一。Web 应用安全评估通过针对常见漏洞（如 SQL 注入、跨站脚本攻击 XSS、身份验证缺陷）进行测试，保障 Web 应用的安全性。

这些评估可以采用黑盒测试，即测试人员在对应用程序内部机制一无所知的情况下，模拟外部攻击者进行攻击；也可以采用白盒测试，测试人员拥有完整的源代码和架构信息，能够对潜在漏洞进行更深入的分析。

价值体现：

- › 保护通过 Web 应用处理的客户和企业数据。
- › 识别增加风险的代码缺陷和配置错误。
- › 支持满足 OWASP Top 10、PCI DSS 等安全标准。
- › 降低网站被篡改、数据泄露及声誉损失的风险。
- › 提供外部攻击视角和深入的应用安全分析。

帮助解答的关键问题：

- › 我们的 Web 应用是否存在常见攻击漏洞？
- › 是否由于代码缺陷或配置问题导致敏感数据暴露？
- › 外部攻击者是否能利用漏洞，或者代码中是否存在更深层次的问题？
- › 我们如何提升用户身份验证和会话管理的安全性？
- › 应采取哪些补救措施修复 Web 应用中的漏洞？

安全评估服务概览

评估类型	重点领域	关键问题	示例场景
渗透测试	基础设施、系统和网络	系统存在哪些漏洞？攻击者如何突破防御？	外部：测试对公网开放的网站和服务；内部：测试内部访问控制和权限提升
无线网络安全测试	Wi-Fi 安全、加密、访问控制	我们的 Wi-Fi 是否安全？是否存在未授权或恶意设备？	测试办公 Wi-Fi 安全性，识别恶意接入点，尝试进行未授权连接
Web 应用安全评估	Web 应用、代码缺陷、身份验证	应用是否安全？是否存在敏感数据暴露？如何修复漏洞？	测试客户门户、电商网站、内部 Web 应用，识别 SQL 注入、XSS 或身份验证缺陷

其他安全测试服务

没有单一的测试方法或单项评估可以全面反映企业的整体安全状况。每项攻击模拟测试都有其特定目标和可接受的风险范围。Sophos 可协助您设计和组合适合自身环境的评估方法和技术手段，帮助全面评估企业的安全状况与防护措施，识别潜在漏洞。

了解更多：
sophos.com/advisory-services

中国 (大陆地区) 销售咨询
电子邮件: salescn@sophos.com