

等级保护信息技术安全！一站式过等保

产品名称	等级保护信息技术安全！一站式过等保
公司名称	国源天顺安全服务有限公司
价格	.00/个
规格参数	机构:等级保护测评机构 服务:一站式等保服务 优点:拥有5年等级保护项目经验
公司地址	北京市东城区广渠家园25楼5层501（注册地址）
联系电话	15652968977

产品详情

1、影响系统正常运行的风险

在现场测评时,需要对设备和系统进行一定的验证测试工作,部分测试内容需要上机验证并查看一些信息,这就可能对系统运行造成一定的影响,甚至存在误操作的可能。

此外,使用测试工具进行漏洞扫描测试,性能测试及渗透测试等,可能会对网络和系统的负载造成一定的影响,渗透性攻击测试还可能影响到服务器和系统正常运行,如出现重启、服务中断、渗透过程中植入的代码未完全清理等现象。

2、敏感信息 泄露风险

测评人员有意或无意泄漏被测系统状态信息,如网络拓扑、IP地址、业务流程、业务数据,安全机制,安全隐患和有关文档信息等。

3、木马植入风险

测评人员在渗透测试完成后,有意或无意将渗透测试过程中用到的测试工具未清理或清理不彻底,或者测试电脑中带有木马程序,带来在被测评系统中植入木马的风险。

4、等级测评 风险规避

在等级测评过程中可以通过采取以下措施规避风险:

签署委托测评协议

在测评工作正式开始之前,测评方和被测评单位需要以委托协议的方式明确测评工作的目标、范围、人员组成、计划安排、执行步骤和要求以及双方的责任和义务等,使得测评双方对测评过程中的基本问题达成共识。

签署保密协议

测评相关方应签署合乎法律规范的保密协议,以约束测评相关方现在及将来的行为。保密协议规定了测评相关方保密方面的权利与义务。测评过程中获取的相关系统数据信息及测评工作的成果属被测评单位所有,测评方对其的引用与公开应得到相关单位的授权,否则相关单位将按照保密协议的要求追究测评单位的法律责任。

现场测评工作风险的规避

现场测评之前,测评机构应与相关单位签署现场测评授权书,要求相关方对系统及数据进行备份,并对可能出现的事件制定应急处理方案。

进行验证测试和工具测试时,避开业务高峰期,在系统资源处于空闲状态时进行,或配置与生产环境一致的模拟/仿真环境,在模拟/仿真环境下开展漏洞扫描等测试工作;上机验证测试由测评人员提出需要验证的内容,系统运营、使用单位的技术人员进行实际操作。整个现场测评过程要求系统运营、使用单位全程监督。

测评现场还原

测评工作完成后,测评人员应将测评过程中获取的所有特权交回,把测评过程中借阅的相关资料文档归还,并将测评环境恢复至测评前状态。