**中国医学科学院肿瘤医院**

**安全运维项目需求**

**信息中心/计算机室**

**2020-8**

目录

[一、 项目概述 2](#_Toc48813867)

[二、 服务需求 2](#_Toc48813868)

[2.1 安全运维服务 2](#_Toc48813869)

[2.1.1 渗透测试 2](#_Toc48813870)

[2.1.2 漏洞扫描 3](#_Toc48813871)

[2.1.3 应急响应 4](#_Toc48813872)

[2.1.4 安全预警 4](#_Toc48813873)

[2.1.5 安全培训 4](#_Toc48813874)

[2.2 安全咨询与安全检测服务 5](#_Toc48813875)

[2.3 备案服务 5](#_Toc48813876)

[三、 其它要求 5](#_Toc48813877)

[四、 资质要求 6](#_Toc48813878)

# 项目概述

随着信息技术在医院业务与管理上的深入应用，医院信息系统和网络的安全与否直接关系到医院的正常工作。按照《网络安全等级保护基本要求》、公安执法检查要求，医院除了需要开展网络安全等级保护相关工作，还需要聘请网络安全专家顾问。目前医院缺少网络安全工作人员，需要引入专业的信息安全服务团队，根据医疗行业、国家以及国外的先进的信息安全标准，建立一套安全运维与应急体系，为我院提供全面、合规、先进的信息安全服务，保障我院业务系统及互联网服务系统安全平稳运行。同时支持新建系统安全体系的建立与测评，逐步实现动态、完整、高效的信息安全体系。

# 服务需求

##  安全运维服务

### 2.1.1 渗透测试

要求次数：一年一次

服务对象：互联网系统、内网业务系统（HIS、集成平台）

对用户选定的渗透对象，按照国际通用的PETS渗透测试标准，进行深入的模拟黑客攻击的渗透测试。测试中为保证整个渗透测试过程都在可以控制和调整的范围之内，以人工渗透为主，并辅助用户认可的渗透测试工具，发现业务和应用系统中的安全隐患，要求测试者有较强的专业技能，可以准确发现逻辑性更强、更深层次的弱点。

通过渗透测试发现业务系统存在的可能被利用的安全隐患，提出解决方案，协助用户进行全面的安全加固。

具体的渗透测试手段包括但不限于：

1）已知漏洞攻击

通过被披露的操作系统及应用软件（或模块）的安全漏洞，利用这些漏洞及相关工具对网站及其应用进行测试。

2）口令猜解

对于采用口令进行用户认证的应用，将使用工具进行口令猜测以获取用户帐号/密码，口令猜测使用字典攻击和蛮力攻击。

3）注入攻击

对网站应用程序的输入数据进行合法性检查，对客户端参数中包含的某些特殊内容进行不适当的处理，进行预判。具体方法主要为SQL语句注入、隐蔽命令执行、遍历目录/文件

4）异常处理

当应用程序中的方法调用出现故障时，应用程序进行哪些操作？显示了多少？是否返回友好的错误信息给最终用户？是否把有价值的异常信息传递回调用者？应用程序的故障是否适当。

5）后门

利用工具对信息系统进行彻底扫描，对异常进程、网络异常连接、异常流量、启动项等进行深入分析，查找系统是否存在后门。

6）溢出攻击

通过前期资料收集掌握的系统运行的各种应用程序进行分析、总结，利用工具与工程经验结合的方式对各种应用程序进行缓冲区溢出攻击测试，发现存在溢出的程序，充分信息系统安全运行。

交付物《渗透测试报告》

### 2.1.2 漏洞扫描

要求次数：一年四次

服务对象：主机、应用、网络设备

对医院网络环境、服务器、操作系统、安全设备、应用系统等一系列对象进行漏洞扫描：

1. 使用多种技术手段，对网络设备、服务器、操作系统、安全设备、应用系统进行周期性的安全扫描；

交付物《漏洞扫描报告》。

### 2.1.3 应急响应

协助医院制订各系统应急预案，提供信息安全应急响应服务，当系统遭受网络攻击、系统攻击等相关安全事件时，及时提供解决方案，协助用户解决。当入侵或者破坏发生时，处理方法主要原则是首先恢复计算机、网络服务的正常工作，事后对入侵者进行追查，协助用户分析事件的起因，漏洞及后门检查，同时为用户提供事件的解决方案，尽快恢复服务，修补漏洞。

服务方式可以是远程支持或现场支持，当远程支持无法解决问题时，将派遣专业的紧急响应服务人员在2小时内到达客户所在地提供现场服务。

### 2.1.4 安全预警

1. 对医院外网重要系统，如门户网站、科研系统、教育系统等进行实时监测，对于黑客的攻击行为及WEBSHELL实时预警，并有专家团队进行分析，以短信或邮件等方式告知用户，如发现网站无法访问、网页被篡改等严重事件时，需立即电话通知用户，必要时到场提供安全服务。
2. 以邮件、电话等方式，将业界动态、国家安全政策及法律法规、漏洞信息、安全产品评测信息、病毒信息等及时传递给用户，对于严重漏洞或重大安全事件，需立即电话通知用户，提供相应的解决方案，必要时到场提供安全服务。
3. 对于操作系统、应用软件的安全漏洞、补丁和安全建议等相关信息12小时内即时口头通知，24小时内邮件正式通知；对于与医院IT资产无关的安全漏洞或者威胁时，每周发布通用安全通告。

### 2.1.5 安全培训

安全培训包括完成基于等保2.0的相关知识培训，包含等级保护备案流程，等级保护技术标准，网络安全政策法规，以及其他与等保相关的内容。培训完成后，将具体的培训情况进行记录与统计，并进行相应的归档，以便后期提供更全面、周到的服务。

## 2.2 安全咨询与安全检测服务

 在医院进行重要系统建设过程中，投标人负责设计各新建系统的安全建设方案，为医院提供安全相关咨询服务，协助医院进行安全产品的选型与测试，同时在新建系统开发完成及重大更新时进行全面安全检测，使用静态扫描、动态分析、数据流追踪等方式查看是否存在后门、漏洞及其他安全威胁，并提出详细的整改建议与方案，直到满足安全建设方案与相关技术要求，完成系统验收。

系统服务对象包括但不限于：医院APP系统、医院信息平台系统。

 安全建设方案应遵从以下标准：GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求、GB/T 25070-2019信息安全技术 网络安全等级保护安全设计技术要求。

## 2.3 备案服务

 投标人负责院方新增二级、三级信息系统的备案工作。工作内容包括帮助院方准备备案材料、帮助院方完成备案流程工作。

 遵从《GB/T 22240-2020 信息系统安全等级保护定级指南》，根据院方情况对系统进行定级备案工作。

# 其它要求

1. 项目组负责人与技术人员具有三甲医院安全运维项目实施经验，具备安全方案设计能力及实施能力，熟悉各类网络产品、操作系统、数据库、安全产品的功能及配置，从物理安全、网络安全、主机安全、应用安全、数据安全、管理安全等多方面配合医院完成安全体系的建立与运维；
2. 安排1名技术专家，作为本单位的安全顾问，随时沟通咨询，解决信息安全或等级保护相关问题；
3. 协助医院进行公安年度自查工作以及各种监管机关的安全检查；
4. 在国家重要活动、重大会议前，对医院门户网站及其他主要设施进行安全巡查，活动期间进行安全保障；
5. 提供电话支持、现场支持，提供24小时电话支持服务，若电话无法解决的问题，4小时内到场支持。

# 资质要求

1. 具有国家信息安全等级保护工作协调小组办公室颁发的信息安全等级保护测评机构推荐证书。
2. 项目经理应具备信息安全等级保护中级及以上测评师资质证书，项目组其他成员应具备信息安全等级保护初级及以上测评师资质。