**网络安全服务内容**

|  |  |
| --- | --- |
| 服务项 | 服务要求 |
| **1、网络安全规划与咨询服务** | 通过对徐州口腔医院安全情况调研、针对徐州口腔医院网络安全管理现状和技术防护现状，分析网络安全防护的问题和薄弱点，按照《网络安全法》、国家、部委、省级单位关于网络安全的最新要求，结合网络安全态势的变化趋势，配合本院完成年度网络安全管理制度、网络安全加固建设方案的编制和修订。 |
| 服务频次：周期性服务，每服务年度提供1次方案规划咨询服务、不限次数与网络安全年度规划相关的技术、管理、政策咨询以及修订服务；成果交付：《徐州口腔医院年度网络安全加固建设方案》;在我院指定时间内交付相关方案及服务报告。 |
| **2、漏洞扫描服务** | 漏洞扫描：利用专业漏洞扫描工具对服务范围内各种软硬件设备进行网络层、系统层、数据库、应用层的全面扫描与分析，对发现的操作系统漏洞、数据库漏洞、弱口令、信息泄露及配置不当等脆弱性问题进行人工验证，并提供修复建议。 |
| 漏洞检测报告应具有易懂的漏洞描述和详尽的安全修补方案建议，并提供相关的技术站点以供管理员参考，报告应可对安全的威胁程度分级，并能够形成风险趋势分析报表和主机间风险对比分析，对于重要漏洞，需提供详细的验证用例，且漏洞验证需要提供完整的http请求头，并要求提供详细的测试用例。 |
| ★服务单位自行提供漏洞扫描工具，所提供的漏扫工具应具备系统扫描、WEB扫描、数据库扫描、基线配置核查、弱口令扫描等功能；支持自适应网络扫描，根据网络状况自动控制发包速率，避免影响系统使用；支持漏洞库涵盖标准包含CVE、CVSS、CNVID、CNNVD、CNCVE、Bugtraq编号6种；支持SSH、SMB、TELNET、POP、POP3、IMAP、FTP、RSH、REXEC、WSUS协议的登陆扫描；支持三种漏洞验证方式如浏览器验证、注入验证、通用验证。漏扫服务过程中，需对对扫描结果进行验证，验证手段至少要采取工具与安服工程师人工组合的方式进行。 |
| 定期对徐州口腔医院网络系统中网络安全策略进行梳理、分析和调优，以提高网络安全防护基线。 |
| 服务频次：周期性服务，每服务年度内提供季度漏扫服务（每3个月实施一次）；成果交付：《网络安全漏洞检测报告》（季度、年度）、《漏洞验证与复测报告》（如有）；季度服务报告在服务完成后5日内交付、年度服务报告在服务年度完成后15日内交付。 |
| **3、应急响应服务** | 建立完善的技术支持平台和应急人员队伍，与徐州口腔医院院形成良好的协同工作机制，当系统一旦遭到攻击、入侵等网络安全威胁时，能提供快速的应急响应服务，在最短的时间内采用各种准确得当的技术手段进行安全防护，确保院网络信息系统的损失最小化。通过技术手段排查攻击、入侵的方法和途径，分析事件原因，及时修补漏洞，防止同样事件再次发生。 |
| ★服务周期内应急响应服务时间为 7×24小时，响应方式为工作时间内即时现场响应，节假日及非工作时间1小时内响应，事件初步处置不超过2个小时完成。 |
| 事件处置完毕后，形成处置报告，并协助我院完成上级单位网络安全信息通报要求中规定的重大事件处置表等材料的汇总上报。 |
| 应急响应为连续性服务，服务年度内不限时间、次数；成果交付：《网络安全时间应急处置报告》（如有）,服务报告须在事件完成处置后24小时内交付。 |