附件 :

2016年度公安机关网络安全执法检查自查表

表五：网站安全情况自查表

|  |  |  |  |
| --- | --- | --- | --- |
| 一、网站的基本情况 | | | |
| 网站中文名 |  | IP地址 |  |
| 网址 |  | | |
| 网站责任单位 |  | 网站运行单位 |  |
| 网站责任单位负  人及职务 |  | 联系电话 |  |
| 网站运行安全责任人及职务 |  | 联系电话 |  |
| 网站责任单位所在地 |  | | |
| 工信部ICP备案号 |  | | |
| 国际联网备案号 |  | | |
| 隶属关系 | □中央 □省(自治区、直辖市) □地(区、市、州、盟)  □县（区、市、旗） □其他\_\_\_\_\_ | | |
| 单位类型 | □政府机关 □事业单位 □国企  □互联网 □其他\_\_\_\_\_ | | |
| 行业类别 | 如：财政（根据等级保护备案表行业分类划分） | | |
| 等级保护定级备案 | □二级 □三级 □四级 □未定级 | | |
| 等级测评 | □已开展 □未开展 | | |
| 网站安全责任书 | □已签订 □未签订 | | |
| 网站服务栏目 | □新闻发布 □政策宣传 □事项办理 □论 坛 □即时通信  □电子邮件 □留言版 □政务公开 □其他\_\_\_\_\_ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 二、网站安全保护情况 | | | |
| 1 | 网站安全责任部门和安全责任人落实情况 | 是否落实了单位网站安全责任部门？ | □是 □否 |
| 是否落实了单位网站安全责任人？ | □是 □否 |
| 2 | 主要领导对网站网络安全工作的重视情况 | 是否将网站安全工作的执行情况纳入到年度考核指标？ | □是 □否 |
| 开展网站安全工作的经费是否纳入年度预算？ | □是 □否 |
| 3 | 单位网站网络安全责任制落实情况 | 是否明确了网站建设单位、运维单位和内容更新单位等部门的责任？ | □是 □否 |
| 是否对发生的网站安全事件（事故）按照安全责任制进行追责？ | □是 □否 |
| 4 | 关键岗位人员配备情况 | 是否有明确的安全管理员，并签订保密协议？ | □是 □否 |
| 是否有内容管理员，并签订保密协议？ | □是 □否 |
| 5 | 网站定级备案执行情况 | 单位网站是否确定了安全保护等级？ | □是 □否 |
| 单位网站是否按要求到公安机关进行了备案？ | □是 □否 |
| 6 | 网站等级测评情况 | 是否从《全国信息安全等级保护测评机构推荐目录》中选择测评机构开展等级测评？ | □是 □否 |
| 是否对网站系统定期进行安全测评？ | □是 □否 |
| 是否对网站系统进行了外部渗透测试？ | □是 □否 |
| 是否根据测评和渗透测试结果对网站进行安全加固改造？ | □是 □否 |
| 7 | 安全事件报告处置 | 是否制定网站安全事件（事故）报告制度？ | □是 □否 |
| 发生网站安全事件（事故）是否向属地公安机关报告？ | □是 □否 |
| 是否有完整网站安全事件处置记录？ | □是 □否 |
| 是否按照要求保留网站完整日志？ | □是 □否 |
| 8 | 开展网站安全监测和预警情况 | 本单位是否开展日常网站安全监测？ | □是 □否 |
| 是否有网站安全监测记录？ | □是 □否 |
| 是否有网站安全预警和处理记录？ | □是 □否 |
| 9 | 网站内容管理 | 是否制定网站内容发布管理制度？ | □是 □否 |
| 是否制定网站内容发布流程？ | □是 □否 |
| 10 | 应急预案的制定、演练和完善情况 | 是否有应急预案，并有相应的预案文档？ | □是 □否 |
| 是否有应急保障队伍并有人员联系方式？ | □是 □否 |
| 是否定期应急演练并有应急演练的文档记录？ | □是 □否 |
| 是否根据演练结果对应急预案进行完善？ | □是 □否 |
| 11 | 机房安全管理制度执行情况 | 本单位机房进出人员管理是否按照制度执行，并有详细记录？ | □是 □否 |
| 本单位机房日常监控是否制度执行并有监控记录？ | □是 □否 |
| 12 | 网络安全检查情况 | 是否有网站安全自查工作总结报告？ | □是 □否 |
| 13 | 网站交互式栏目信息巡查情况 | 单位网站是否有交互式栏目？ | □是 □否 |
| 是否有专人负责网站交互式栏目信息巡查？ | □是 □否 |
| 14 | 网络边界安全防护设备情况 | 是否部署防火墙？ | □是 □否 |
| 是否对外屏蔽了不必要的服务/端口？ | □是 □否 |
| 是否部署入侵检测（防护）设备？ | □是 □否 |
| 是否部署防病毒网关？ | □是 □否 |
| 是否部署抗拒绝服务攻击设备？ | □是 □否 |
| 是否部署Web应用防火墙？ | □是 □否 |
| 是否部署设备？ | □是 □否 |
| 15 | 网页防篡改措施 | 是否定期对网站文件进行检测？ | □是 □否 |
| 是否采取网页防篡改措施？ | □是 □否 |
| 16 | 漏洞扫描措施及修复升级情况 | 是否进行过系统层漏洞扫描，并有详细记录？ | □是 □否 |
| 是否进行过应用层漏洞扫描，并有详细记录？ | □是 □否 |
| 发现的漏洞是否及时修复？ | □是 □否 |
| 17 | 网站恶意代码防护 | 是否有网页挂马检测系统？ | □是 □否 |
| 18 | 网站内容安全防护措施 | 内容编辑、审核及发布权限是否分离？ | □是 □否 |
| 关键信息发布是否多级审核？ | □是 □否 |
| 网站发布内容是否过滤？ | □是 □否 |
| 19 | 管理终端安全防护措施 | 是否有控制措施（如地址绑定，网络接入控制等）？ | □是 □否 |
| 20 | 网站后台管理系统防护措施 | 是否对网站后台管理系统的接口进行隐藏？ | □是 □否 |
| 网站后台管理系统登录是否采取验证机制？ | □是 □否 |
| 是否对网站后台管理系统的登录失败尝试次数进行限制？ | □是 □否 |
| 是否对网站后台管理系统的用户口令复杂度进行强度限制？ | □是 □否 |
| 21 | 主要设备可用性 | 网站服务器和数据库服务器是否双机热备？ | □是 □否 |
| 网站服务器和数据库服务器是否采用冷备方式？ | □是 □否 |
| 22 | 网站前、后台系统隔离情况 | 是否采用逻辑隔离？ | □是 □否 |
| 23 | 网站应用远程管理情况 | 是否不允许远程管理网站的应用？ | □是 □否 |
| 应用远程管理时是否采用加密通道？ | □是 □否 |
| 24 | 网站内容远程维护情况 | 是否不允许远程维护网站内容？ | □是 □否 |
| 网站内容远程维护时是否采用加密通道？ | □是 □否 |
| 25 | 网站服务器操作系统安全措施 | 网站服务器操作系统安全补丁是否及时更新？ | □是 □否 |
| 网站服务器操作系统是否存在弱口令？ | □是 □否 |
| 26 | 网站服务器数据库安全措施 | 网站服务器数据库是否存在弱口令？ | □是 □否 |
| 网站服务器数据库是否共用同一管理口令？ | □是 □否 |
| 27 | 网站服务器中间件安全措施 | 网站服务器中间件管理界面是否允许外部访问？ | □是 □否 |
| 网站服务器中间件是否存在弱口令？ | □是 □否 |
| 28 | 网站安全整治专项工作情况 | 是否完成网站通信管理部门备案？ | □是 □否 |
| 是否完成网站等级保护备案？ | □是 □否 |
| 是否完成网站统一标识？ | □是 □否 |
| 三、互联网大型综合网站数据安全保护情况 | | | |
| 29、互联网大型综合网站数据资源采集、存储、传输、应用和安全保护情况 | | | |
|  | | | |
| 30、利用互联网大型综合网站数据资源从事大数据分析挖掘、增值服务情况 | | | |
|  | | | |
| 31、互联网大型综合网站数据资源的转租情况及实际应用企业情况 | | | |
|  | | | |