|  |  |  |  |
| --- | --- | --- | --- |
| 信息系统基本情况 | | | |
| 系统名称 | XXX系统 | 安全保护等级 | 三级(S3A3G3) |

说明：

下表中“2012年等保测评安全问题”中列出的是2012年3月参照国家等级保护标准《GB/T22239-2008信息系统安全等级保护基本要求》进行测评时发现的安全问题。由于2012年5月底国家广电总局科技司颁布了广电行业信息安全等级保护行业标准——《GD/J 038—2011广播电视相关信息系统安全安全等级保护基本要求》。该标准中对国家标准中不适用于广电行业的要求进行了修改。因此，本次安全规划将主要参考广电行业标准（即《GD/J 038—2011广播电视相关信息系统安全安全等级保护基本要求》）

下文中的“是否根据广电等保要求调整”即是参照《GD/J 038—2011广播电视相关信息系统安全安全等级保护基本要求》（以下简称“广电等保要求”）进行对比后判断的是否需要对原有“2012年等保测评安全问题”进行调整。如为“保留”即表示广电等保要求参照国家等保要求，仍然需要进行整改。

下文中的“是否建议立即开展整改”即是按照目前调研所了解的情况给出的建议，“”表示可以根据目前的资源立即进行整改；“”表示目前由于资源不足，整改时间，但是要纳入下一年的整改计划中。

**请各位系统管理员在“系统管理员反馈”中填写关于是否同意参照整改建议立即开展整改，如有疑问请与网管科朱霖或咨询服务商天讯瑞达程晓峰13580461060或李雄武15018770557联系。**

| **序号** | **问题类别** | **2012年等保测评安全问题** | **是否根据广电等保要求调整** | **整改建议** | **是否建议立即开展整改** | **系统管理员反馈** | **处理意见** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 物理安全 | 机房未划分区域，并在区域与区域之间设置物理隔离装置。 | 根据广电等保要求10.2物理访问控制，不需要对机房划分区域进行管理 |  |  |  |  |
|  | 部分通信线缆铺设在桥架上裸露在外。 | 保留 | 建议对裸露在外的通信线缆加装导线槽 |  |  |  |
|  | 无专门存放介质的介质库或档案室。 | 根据广电等保要求10.2物理访问控制，不需专门存放介质的介质库 |  |  |  |  |
|  | 机房无光、电防盗报警系统。 | 保留 | 建议在12楼新机房加装机房防盗报警系统，具备在非授权进入时通过红外线等措施进行报警 |  |  |  |
|  | 机房未设置监控报警系统。 | 保留 | 建议在机房设置安防监控报警系统 |  |  |  |
|  | 机房温度和湿度跨度太大，机房各部分的温度和湿度不均衡。 | 保留 | 机房的温湿度、防尘、防静电、电磁防护、接地、布线等按照GB 59174-2008  的有关规定执行  温度：23+1  湿度： 40%-55% |  |  |  |
|  | 机房的关键设备无电磁防护措施。 | 保留 | 建议对机房所有服务器及网络设备统一接地，防止外界电磁干扰和设备寄生耦合干扰 |  |  |  |
|  | 网络安全 | 网络中未启用动态路由协议认证。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.1基础网络安全，无该项要求 |  |  |  |  |
|  | 网络中未配置针对重要主机的QOS。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.1基础网络安全，无该项要求 |  |  |  |  |
|  | 网络中未部署相关非法内联措施。 | 该要求为等保3级的要求，等保2级中没有该项要求  等保2级的要求是：应能够对内部网络用户私自联到外部网络的行为进行检查。 | 建议在办公终端采用IP-MAC地址绑定，增加统一终端管理软件，防止用户私自增加网卡，并且要指定相应管理措施（禁止私自架设无线路由、使用3G网卡等） |  |  |  |
|  | 网络中未部署相关非法外联措施。 | 该要求为等保3级的要求，等保2级中没有该项要求  等保2级的要求是：应能够对内部网络用户私自联到外部网络的行为进行检查。 | 建议在办公终端采用IP-MAC地址绑定，增加统一终端管理软件，防止用户私自增加网卡，并且要指定相应管理措施（禁止私自架设无线路由、使用3G网卡等） |  |  |  |
|  | 网络中未配置独立的防毒墙设备和IDS设备。 | 该要求为等保3级的要求，等保2级中没有该项要求  等保2级的要求是：应在与外部网络连接的网络边界处进行恶意代码检测和清除，并维护恶意代码库的升级和检测系统的更新 | 建议在重要的系统网络边界出增加IDS入侵检测设备和增加入侵防御设备（防火墙），并且要开启所有防护功能 |  |  |  |
|  | 网络中未配置最大流量数和网络连接数限制。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.1基础网络安全，无该项要求 |  |  |  |  |
|  | 未对网络设备日志记录数据进行分析，并生成审计报表。 | 保留  根据广电等保要求6.1基础网络安全，对应要求为：应对关键网络设备的运行状况、用户行为等重要事件进行日志记录 | 建议增加日志服务器，对关键网络设备的日志经行收集，然后统一对日志文件进行分析。 |  |  |  |
|  | 未对审计记录进行单独保护。 | 保留  根据广电等保要求6.1基础网络安全，对应要求为：应保护审计记录，避免受到未预期的删除、修改或覆盖等，审计记录至少保存90天 | 建议增加审计的设备能对审计记录的保存时间要大于90天  存储在本地要保证保存时间要大于90天 |  |  |  |
|  | 存在多人共用管理账户的现象。 | 保留 | 建议对网络设备设置多个账号，口令应有复杂度要求并定期更换，用户名和口令禁止相同 |  |  |  |
|  | 未配置网络设备的双因子认证机制。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.1基础网络安全，无该项要求 |  |  |  |  |
|  | 未采用安全的ssh对网络互联设备进行远程管理。 | 保留 | 建议当对网络设备进行远程管理时，应采用HTTPS、SSH等安全的远程管理手段，不要采用telnet和http，防止用户身份鉴别信息在网络传输过程中被窃听 |  |  |  |
|  | 未针对不同特权管理人员配置不同权限账户。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.1基础网络安全，无该项要求 |  |  |  |  |
|  | 未在服务器接入交换机上配置防地址欺骗技术。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.1基础网络安全，无该项要求 |  |  |  |  |
|  | 主机安全 | 操作系统及数据库系统“密码策略”未对密码长度、复杂度、更换周期进行设置。 | 保留 | 建议对登录网络设备的用户进行身份鉴别，身份鉴别信息应具有不易被冒用的特点，不要使用弱口令和容易猜测的账号，口令应有复杂度要求并定期更换，用户名和口令禁止相同（服务器对应的策略要开启） |  |  |  |
|  | 操作系统及数据库系统未开启登录失败处理功能。 | 保留 | 建议操作系统开启登录失败阀值，如：登录5次失败后锁定10分钟。 |  |  |  |
|  | 操作系统及数据库系统未采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.4服务端系统安全，无该项要求 |  |  |  |  |
|  | 操作系统管理员和数据库系统管理员为同一人。 | 保留 | 建议操作系统的账号和数据库的账号不一样，账号的管理人员也要不一样。 |  |  |  |
|  | 未在操作系统层面上实现对重要信息资源设置敏感标记。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.4服务端系统安全，无该项要求 |  |  |  |  |
|  | 服务器操作系统及数据库未开启安全审计服务。 | 保留 | 建议开启服务器操作系统及数据库未开启安全审计服务或者增加审计设备对系统中的接口服务器、Web服务器、应用服务器、数据库服务器等重要服务器的操作系统和数据库进行审计（审计粒度为用户级） |  |  |  |
|  | 无第三方工具对服务器操作系统及数据库系统审计记录数据进行分析，并生成审计报表。 | 保留 | 建议增第三方加审计设备后，定期对审计记录进行分析，并导出报表，以便及时发现异常行为 |  |  |  |
|  | 未采取措施保护审计进程，避免受到未预期的中断。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.4服务端系统安全，无该项要求 |  |  |  |  |
|  | 未定期备份审计记录或采取其他措施保护审计记录，避免受到未预期的删除、修改或覆盖等。 | 保留 | 建议增加审计的设备能对审计记录的保存时间要大于90天  存储在本地要保证保存时间要大于90天 |  |  |  |
|  | 在系统资源被释放或再分配给其他用户前未采取措施清除系统剩余信息。 | 根据广电等保要求6.4服务端系统安全，无这一点要求 |  |  |  |  |
|  | 服务器未配置主机入侵防御措施。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.4服务端系统安全，无该项要求 |  |  |  |  |
|  | 无对重要程序完整性检测措施及恢复措施。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.4服务端系统安全，无该项要求 |  |  |  |  |
|  | 操作系统及数据库补丁不是最新。 | 保留  根据广电等保要求6.4服务端系统安全，对应要求为：定期更新操作系统补丁，新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心服务器可根据需要进行更新 |  |  |  |  |
|  | 服务器操作系统未安装防恶意代码软件。 | 保留  根据广电等保要求6.4服务端系统安全，对应要求为：应部署具有统一管理功能的防恶意代码软件，并定期更新防恶意代码软件版本和恶意代码库；新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心服务器可根据需要进行部署  和更新 | 建议部署具有统一管理功能的防恶意代码软件，并定期更新防恶意代码软件版本和恶意代码库；新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心服务器可根据需要进行部署和更新，如：linux、aix、unix等操作建议采购专业软件 |  |  |  |
|  | 登录终端未设置超时锁定。 | 保留 | 建议操作系统开启登录失败阀值，如：登录5次失败后锁定10分钟。 |  |  |  |
|  | 应用安全 | 未采用两种或两种以上组合的鉴别技术实现用户身份鉴别。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.5应用安全，无该项要求 |  |  |  |  |
|  | 未提供身份唯一性检查功能。 | 保留 | 建议增加对用户身份标识进行检查，如：手机号码、身份证号码、生日等唯一性标识 |  |  |  |
|  | 未提供登录失败处理功能。 | 保留 | 建议操作系统开启登录失败阀值，如：登录5次失败后锁定10分钟。 |  |  |  |
|  | 由授权主体配置访问控制策略，未严格限制默认帐户的访问权限。 | 保留 | 建议删除临时帐户和测试帐户，重命名默认帐户，修改其默认口令，限制其访问权限，不允许匿名用户登录 |  |  |  |
|  | 未授予不同帐户为完成各自承担任务所需的最小权限，未形成相互制约的条件。 | 保留 | 建议每个账号都有各自不同的权限，如：系统管理员不建议拥有系统审计员权限、一般系统用户不建议拥有系统管理员权限等 |  |  |  |
|  | 未对重要信息资源设置敏感标记的功能。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.5应用安全，无该项要求 |  |  |  |  |
|  | 未依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.5应用安全，无该项要求 |  |  |  |  |
|  | 未对审计记录数据进行分析，并生成报表。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.5应用安全，无该项要求 |  |  |  |  |
|  | 未采用密码技术保证通信过程中数据的完整性。 | 保留 | 建议信息系统与外部网络进行通信时，利用校验码技术、特定的音视频文件格式、特定协议或等同强度的技术手段等进行传输，保证通信过程中的数据完整性 |  |  |  |
|  | 未采用加密技术保证通信过程的保密性。 | 保留 | 建议信息系统与外部网络进行通信时，在通信双方建立连接之前，应用系统应利用密码技术进行  会话初始化验证，并对通信过程中的用户身份鉴别信息等敏感信息字段进行加密 |  |  |  |
|  | 未采用CA技术保证系统抗抵赖性。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.5应用安全，无该项要求 |  |  |  |  |
|  | 应用系统不具备自我保护功能。 | 保留 | 建议增加备份系统或者冗余设备，当软件发生故障时，信息系统应能够继续提供部分功能，确保能够实施使系统恢复正常或保护数据安全的必要措施。 |  |  |  |
|  | 未限制系统的最大会话并发数。 | 保留 | 建议对应用系统的最大并发会话连接数进行限制，如：限制一个IP地址访问应用系统的会话数为200， 防止DDOS攻击 |  |  |  |
|  | 未限制单个账户的多重并发会话数。 | 保留 | 建议对应用系统的单个帐户的多重并发会话进行限制，如：只允许一个账号同时在同一个地方登录，如果要在其他地方登录要先退出现在的登录账号 |  |  |  |
|  | 未限制单个账户的进程占用资源率。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.5应用安全，无该项要求 |  |  |  |  |
|  | 系统未提供服务优先级功能。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.5应用安全，无该项要求 |  |  |  |  |
|  | 数据安全及备份恢复 | 无数据完整性检查与恢复措施。 | 保留 | 建议对重要业务信息进行备份，保证出现故障时可以马上恢复。 |  |  |  |
|  | 系统管理数据、鉴别信息和重要业务数据未实现传输保密性和存储保密性。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.6应用安全，无该项要求 |  |  |  |  |
|  | 备份数据未场外存放。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.6应用安全，无该项要求 |  |  |  |  |
|  | 主要网络设备无硬件冗余。 | 该要求为等保3级的要求，等保2级中没有该项要求  根据广电等保要求6.6应用安全，无该项要求 |  |  |  |  |
|  | 安全管理机构 | 未以文件方式明确安全主管、安全审计员岗位及职责。 | 保留 | 目前南京有线已经发布《苏网宁发〔2012〕128号》明确安全管理各个岗位及职责，基本满足要求。但是各个安全岗位的安全工作内容需要常态化、周期性执行。 | 已满足 |  |  |
|  | 未配备安全审计员。 | 根据广电等保要求：具有第三级及以上信息系统的单位应设立系统管理员、网络管理员、安全管理员等岗位，并明确各个工作岗位的职责、分工和技能要求；该系统属于第二级。 |  |  |  |  |
|  | 安全管理员非专职人员。 | 保留 | 部分部门科室（网管科）内部已经设定专职安全管理员，建议播出科也要设定专职安全管理员，负责信息安全各项工作的组织和落实。 |  |  |  |
|  | 未与兄弟单位、电信公司、公安机关建立合作机制。 | 保留 | 与兄弟单位建立合作机制，学习兄弟单位的先进安全管理技术。  与电信公司建立合作机制，解决信息系统网络出口等问题。  与公安机关建立合作机制，确保发生安全事件后的解决方案，例如备案等 | （由公司信息安全工作小组负责） |  |  |
|  | 未聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划。 | 根据广电等保要求：具有三级及以上信息系统的单位应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。该系统属于第二级。 | 南京有线已经聘请信息安全专家（天讯瑞达）作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。 | 已满足 |  |  |
|  | 人员安全管理 | 未与人员签署保密协议。 | 保留 | 应签署保密协议，明确保密协议的内容界定、保密期限、追责条款。 |  | 公司人事部门签署劳务合同时可以考虑 |  |
|  | 未与关键岗位人员签署岗位安全协议。 | 保留 | 应签署岗位安全协议，明确签订协议的关键岗位（例如管理岗，业务岗、系统运维岗等），职责（角色）、任务工作、处罚条款。 |  | 公司人事部门签署劳务合同时可以考虑 |  |
|  | 现场未发现人员离岗时的保密承诺文档。 | 保留 | 应办理严格的调离手续，关键岗位人员离岗须签订禁业协议，承诺调离后的保密义务后方可离开。内容包括：根据所属岗位涉及企业机密重要程度，保密期限、追责条款。 |  | 公司人事部门签署劳务合同时可以考虑 |  |
|  | 对人员信息安全方面的培训较少。 | 保留 | 应定期对各类人员进行安全意识教育、岗位技能培训和相关安全政策、技术培训； 培训时需要区别对待，并对信息安全培训和考核情况进行记录并保存。 |  | 公司人员部门统一安排 |  |
|  | 系统建设管理 | 系统定级备案材料尚未完成。 | 保留 | 目前南京有线已经对11个系统（该系统已经定级）进行系统定级备案，建议其余等系统也应该尽快定级。 | （由公司信息安全工作小组统筹） |  |  |
|  | 未根据系统的等级划分情况统一考虑安全保障体系，进行相关的安全措施调整。 | 保留 | 正在进行中，建议对已经定级的系统统一考虑信息安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划、远期和近期建设计划等，采用相关的安全措施进行保护。  对未定级备案的系统进行定级。 | （由公司信息安全工作小组统筹） |  |  |
|  | 软件安装之前未检测软件包中可能存在的恶意代码。 | 保留 | 应在软件安装之前使用公司统一的、具有权威性的防病毒软件检测软件包中可能存在的恶意代码； |  |  |  |
|  | 未审查软件中可能存在的后门。 | 保留 | 应制定代码编写安全规范，要求开发人员参照规范编写代码  在合同中承诺提供的软件不存在后门  验收时，测试、审查软件中可能存在的后门漏洞等  必要时要求软件提供商将软件送检 |  |  |  |
|  | 未委托第三方进行安全性测试。 | 保留 | 已经委托具有资质的第三方（金盾公司）对系统进行安全性测试，并出具安全性测试报告；  建议年度邀请有资质的第三方机构进行此项安全性测试 | 已满足 |  |  |
|  | 系统运维管理 | 未对工作人员离开座位应确保终端计算机退出登录状态做说明。 | 根据广电等保要求：11.5.1 环境管理未对该项进行要求 |  |  |  |  |
|  | 现场未发现介质安全管理制度。 | 保留 | 制定《介质安全管理制度》，对介质的存放环境、使用、维护和销毁等方面作出规定； |  | 公司相关部门统一规划 |  |
|  | 未对备份数据实行异地存储。 | 保留 | 根据数据备份的需要对某些介质实行异地存储（距离5至10公里），存储地的环境要求和管理方法应与本地相同。 |  | 公司相关部门统一规划部署 |  |
|  | 未对重要介质中的数据和软件采取加密存储。 | 保留 | 确保介质存放在安全的环境中，并根据所承载数据和软件的重要程度对介质进行分类和标识管理，进行相应的控制和保护；  采用加密措施时根据级别选择合适的密钥长度 |  |  |  |
|  | 暂未建立安全管理中心对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。 | 根据广电等保要求：并未对“建立安全管理中心”进行要求 | 针对设备状态、恶意代码、补丁升级、安全审计等安全相关事项，制定《安全事件报告和处置管理制度》，明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责； |  |  |  |
|  | 《XXX平台安全管理》未对审计日志保存时间、升级与补丁更新作出规定。 | 保留 | 应建立《网络安全管理制度》，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定；应建立《系统安全管理制度》，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定； |  |  |  |
|  | 未对系统进行漏洞扫描。 | 保留 | 网管科已对该系统进行漏洞扫描。  应该定期对网络、系统进行漏洞扫描；  并采用的多种不同类型的漏洞扫描工具综合扫描；  对发现的网络系统安全漏洞进行及时的修补；  对播出系统直接相关的信息网络根据需要选择合适时机进行； |  |  |  |
|  | 未对允许或者拒绝便携式和移动式设备的网络接入进行明确规定。 | 保留 | 对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理；其中包括：1. 可以访问哪一类设备;需要什么版本的操作系统。2. 你的用户群需要什么级别的访问权限。3. 用户需要安装什么应用。4. 最重要的一点，需要使用公共wifi网络的个人用户要安装VPN。5.要让用户知道设置密码的重要性。 |  |  |  |
|  | 未定期检查违反规定拨号上网或其他违反网络安全策略的行为。 | 保留 | 周期性对终端计算机进行检查，对于发现私自安装3G网卡的终端进行通报批评和限制 |  |  |  |
|  | 现场未发现系统安全管理制度，对系统安全策略、安全配置、日志管理作出规定。 | 保留 | 编制《XXX系统安全管理制度》，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定； |  |  |  |
|  | 未定期对运行日志和审计数据定期进行分析。 | 保留 | 应定期对运行日志和审计数据进行分析，以便及时发现异常行为。 |  |  |  |
|  | 未指定专人对网络和主机恶意代码进行检测。 | 根据广电等保要求：11.5.7 恶意代码防范管理未对该项进行要求 | 在业务系统管理员岗位职责中增加该项工作职责 |  |  |  |
|  | 未对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。 | 保留 | 在《XXX系统安全管理制度》中对该系统设备的防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定；建议代码库升级频率不低于一周。每月提交一份报告。 |  |  |  |
|  | 未定期检查恶意代码库的升级情况，并对发现的恶意代码情况进行分析并形成书面报告总结汇报。 | 保留 | 应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对防恶意代码产品上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。 |  |  |  |
|  | 现场未发现数据备份恢复安全管理制度对数据的备份方式、频度、存储介质和保存期进行规定。 | 保留 | 应建立《备份与恢复安全管理制度》，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范； |  |  |  |
|  | 现场未发现备份恢复策略，对备份数据的文件命名规则、介质替换频率和离站运输进行说明。 | 保留 | 应根据数据的重要性和数据对系统运行的影响，在《备份与恢复安全管理制度》中指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法； |  |  |  |
|  | 无要求机构人员发现安全漏洞及时汇报、不私自验证漏洞方面的管理规定。 | 根据广电等保要求：11.5.6 系统安全管理未对该项进行要求 |  |  |  |  |
|  | 未对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。 | 保留 | 应制定《安全事件报告和响应处理程序》，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等； |  |  |  |