**一期密评（2020.05.11）**

信息系统密码应用安全性评估根据 **GM/T 0054-2018《信息系统密码应用基本要求》**的第三级标准作为测评指标。

**二、主要安全问题及改进建议**

1. **密码算法**

* **问题描述：**远程管理时，服务器操作系统、数据库和网络设备使用RSA软算法实现数据传输保护。使用的密码算法不符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。
* **改进建议：**部署通过国家密码管理部门核准的密码产品，使用商用密码算法保护数据的机密性和完整性。

1. **密码技术**

* **问题描述：**在远程管理时，服务器操作系统、数据库和网络设备使用RSA密码算法和SSL协议防止鉴别信息被窃听，未使用商用密码算法和技术。
* **改进建议：**使用支持双因素鉴别的堡垒机产品或者VPN产品，对服务器操作系统、数据库和网络设备进行远程管理。

1. **密码产品**

* **问题描述：**在远程管理时，服务器操作系统、数据库和网络设备使用RSA软算法实现数据传输保护，应用管理支撑系统、安全管控系统、集中管控系统、应用运行支撑系统的管理员口令使用SM4软算法进行存储保护，均未使用通过国家密码管理部门核准的密码产品。
* **改进建议：**使用通过国家密码管理部门核准的密码产品实现密码运算和密钥保护。

1. **物理和环境安全**

* **问题描述：**
  1. 未使用密码技术保护物理访问控制身份鉴别信息，保证重要区域进入人员身份的真实性；
  2. 未使用密码技术来保证电子门禁系统进出记录的完整性；
  3. 未使用密码技术来保证视频监控音像记录的完整性。
* **改进建议：**
  1. 使用遵循GM/T 0036《采用非接触卡的门禁系统密码应用技术指南》的门禁系统；
  2. 部署服务器密码机产品来保证电子门禁系统进出记录的完整性；
  3. 部署服务器密码机产品来保证视频监控记录的完整性。

1. **网络和通信安全**

* **问题描述：**未采用密码技术建立一条安全的信息传输通道，对网络中所有安全设备或安全组件进行集中管理。
* **改进建议：**部署堡垒机或VPN产品建立一条安全的信息传输通道，对网络中的所有安全设备或安全组件进行集中管理。

1. **设备和计算安全**

* **问题描述：**
  1. 未使用密码技术对登录用户进行身份鉴别；
  2. 在对服务器操作系统、数据库和网络设备进行远程管理时，均未使用商用密码算法和技术实现鉴别信息的防窃听；
  3. 未使用密码技术保证系统资源访问控制信息的完整性；
  4. 未采用可信计算技术建立从系统到应用的信任链；
  5. 未使用密码技术对设备日志记录进行完整性保护。
* **改进建议：**
  1. 在用户名/密码的基础上，增加使用基于密码技术的鉴别方式对管理用户进行身份验证，如数字证书Ukey、动态口令等，并配置口令复杂度策略和定期更换策略；
  2. 远程管理时，采用基于数字证书的方式进行身份鉴别，防止鉴别信息在传输过程中被窃听；
  3. 部署服务器密码机或密码卡产品来保证设备访问控制信息的完整性；
  4. 部署可信计算产品建立从系统到应用的信任链；
  5. 将设备日志记录转发到统一的日志服务器中，并部署服务器密码机产品对日志服务器上的日志记录进行完整性保护。

1. **应用和数据安全**

* **问题描述：**
  1. 应用管理支撑系统、安全管控系统、集中管控系统、应用运行支撑系统和PKI系统未采用密码技术保证业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记的完整性；
  2. 应用管理支撑系统、安全管控系统、集中管控系统、应用运行支撑系统未采用密码技术保证系统配置数据在存储过程中的机密性；
  3. 应用管理支撑系统、安全管控系统、集中管控系统、应用运行支撑系统、PKI系统未采用密码技术保证鉴别信息和系统配置数据在存储过程中的完整性；
  4. 未使用密码技术实现日志记录完整性的保护。
* **改进建议：**
  1. 使用密码机或密码卡保证业务应用系统访问控制策略和数据库表访问控制信息的完整性；
  2. 部署密码机或密码卡实现存储数据的机密性和完整性；
  3. 部署密码机产品实现日志记录的完整性。