附件 2

工业领域数据安全风险排查和防范指导手册（2024 版）

目 录

1.数据安全防护能力薄弱引发的风险排查和防范

1.1 风险 1：数据库安全保障措施不健全引发数据泄露、非法访问风险

1.1.1 排查方式

（1）核查数据库是否根据数据级别和安全防护需要，配置相应的权限管理、访问控制、数据加密、数据脱敏等措施；是否建立数据库安全管理相关规范，明确数据库使用、运维等方面的安全管理要求。

（2）涉及重要数据和核心数据的，核查是否采用校验技术、密码技术等措施进行安全存储；核查数据库备份恢复措施落实情况、数据恢复测试记录等，是否实施数据容灾备份，并定期开展数据恢复测试。

（3）核查是否留存数据库操作日志记录，日志记录留存时限是否满足 6 个月，日志记录内容是否完整、准确，包括执行时间、授权情况、操作账号、处理对象、处理方式等；通过日志分析等手段核查是否存在数据短时高频访问、越权访问、异常复制或导出等情况。

1.1.2 防范措施

（1）建立数据库安全管理相关规范，明确数据库使用、运维等方面的安全管理要求。

（2）根据数据库安全防护需要，采取数据库用户鉴别和认证、访问控制、数据加密、数据脱敏等安全措施。存储

重要数据和核心数据的，还应当采用校验技术、密码技术等措施进行安全存储，并实施数据容灾备份和存储介质安全管理，定期开展数据恢复测试。

（3）明确数据库操作日志管理要求，确保日志记录留存完整准确，开展日志审计，及时发现处置违规使用、异常操作等安全风险。

1.2 风险 2：漏洞、“后门”引发数据泄露、篡改风险

1.2.1 排查方式

（1）根据工业和信息化领域数据安全风险信息报送与共享平台通报的，以及 CNNVD、CNVD、NVDB、CICSVD、CVE 等国内外漏洞库中公开的与数据安全风险强相关的硬编码、目录遍历、远程代码执行、未授权访问、弱口令等漏洞及后门程序信息，对照排查数据处理系统是否存在威胁数据安全的漏洞、“后门”，核查相关漏洞、“后门”是否可被攻击者利用并窃取数据、发起勒索攻击等风险。

（2）通过技术检测等手段排查数据处理系统是否存在漏洞、“后门”，核查相关漏洞、“后门”是否可被攻击者利用并窃取数据、发起勒索攻击等风险。

1.2.2 防范措施

（1）采取漏洞扫描、“后门”巡检等措施，定期对数据处理系统开展扫描检测，及时发现并修复漏洞和“后门”，在不影响生产经营正常运行的情况下，保证应修尽修。

（2）采取网络隔离、边界防护、入侵检测、身份认证、访问控制等措施，关闭不必要的端口或服务（如 3389、22 等远程访问服务端口，135、139、445 等局域网共享端口等），避免攻击者利用漏洞、“后门”窃取数据、发起勒索攻击等。

1.3 风险 3：数据勒索引发数据泄露、破坏等风险

1.3.1 排查方式

（1）排查是否存在利用木马、钓鱼链接等引发的勒索风险。攻击者通过挂马网站、电子邮件等渠道散播钓鱼链接，诱使企业人员下载木马程序并植入勒索软件。

排查方法：排查企业邮件是否存在含有勒索软件的钓鱼邮件等情况。利用木马检测等手段排查数据处理系统是否存在植入勒索软件的木马、钓鱼链接等情况。排查主机等是否安装木马病毒查杀软件并定期开展检测。

（2）排查是否存在利用失窃认证凭证引发的勒索风险。攻击者通常利用暴力破解、密码喷洒、代码共享平台检索等方式获取企业数据处理系统的远程登录用户名和密码，进而通过远程协议登录并植入勒索软件。

排查方法：排查数据处理系统是否存在弱口令等问题，是否定期开展弱口令自查、口令修改等工作。

（3）排查是否存在利用第三方软件引发的勒索风险。攻击者通过入侵第三方软件（包括但不限于 PLM、ERP、MES、SCM、SRM、CRM 等），在软件分发、升级、打补丁等过程中，对软件

进行劫持篡改后用以植入勒索软件。

排查方法：排查是否对第三方软件进行安全检测后再部署应用，是否在软件应用过程中定期开展勒索防范检测。

（4）排查是否存在利用移动存储介质引发的勒索风险。部分勒索软件可将自身复制隐藏至移动存储介质中，同时修改存储介质盘符、图标，创建与移动介质图标相同或相似的快捷方式，诱导用户点击运行后植入勒索软件。此外，攻击者也可利用工作便利主动发放特制的移动存储介质植入勒索软件。

排查方法：核查是否明确移动存储介质安全管理相关要求。排查主机、服务器等系统设备中是否存在移动存储介质非授权插拔现象，以及与移动存储介质图标相同或相似的快捷方式等情况，是否定期查杀移动存储介质。

1.3.2 防范措施

（1）加强数据勒索防范教育培训，提升相关人员的数据勒索风险防范意识和能力，切实做到不点击来源不明的链接、图标及附件内容，不轻易打开可执行程序，不从不明网站下载安装软件，不插拔来历不明的存储介质等。

（2）建立针对勒索软件的木马检测、病毒查杀等技术能力，并对重要数据和核心数据处理系统、主机设备、第三方软件等定期开展勒索软件检测。

（3）定期排查数据处理系统存在的弱口令，并定期更换系统口令，避免攻击者利用弱口令植入勒索软件。

（4）结合实际建立数据安全风险监测手段，强化数据勒索攻击监测分析和风险防范。

（5）针对数据勒索攻击风险场景，建立应急响应机制，明确应急人员、职责、流程和措施等。根据应对勒索攻击的需要，加强重要数据和核心数据备份，在数据遭勒索攻击时能够及时切换利用备份数据保障系统设备稳定运行。

1.4 风险 4：数据暴露面引发数据泄露、非法访问风险

1.4.1 排查方式

（1）排查企业是否履行重要数据和核心数据公开环节的登记、审批程序，是否对数据公开采取了必要的安全防护措施。

（2）采用 wireshark、tcpdump 等工具对联网数据处理系统进行抓包分析，排查是否存在重要数据和核心数据明文传输、直接暴露于公网等问题。

（3）在 Github、CSDN 等代码平台以及云盘、网盘等进行关键词检索，排查是否存在重要系统源代码、研发设计文件等数据被公开披露等情况。

（4）排查 SCADA/MES 等系统，PLC/RTU/远程 IO 模块等工业控制设备，工业数据采集/工业数据转换/串口服务器等工业通信设备，工业云、工业互联网平台、工业大数据平台等平台是否与公网直接相连，是否存在因弱口令、默认口令、默认配置等导致数据可从公网直接访问、获取等风险。

1.4.2 防范措施

（1）加强对数据处理系统联网情况的梳理和安全管理，建立联网数据处理系统台账和资产清单。

（2）根据数据公开环节安全防护的需要，采用数据脱敏、数据标注、数据水印等安全措施。

（3）加强联网数据处理系统数据接口的安全管控，采用访问控制、接口鉴权等手段，保障数据公开涉及的接口调用安全。

（4）定期对联网数据处理系统开展远程检测，根据检测结果对系统的数据安全薄弱项进行整改加固。

（5）定期对重要系统源代码等进行扫描跟踪，避免源代码泄露。

（6）分类施策开展数据暴露风险防范，如针对数据处理系统弱口令、默认口令、空口令等产生的风险，要提高口令强度并定期更换，必要时可采用多因子认证等方式；针对数据处理系统直接暴露于公共互联网的风险，要加强边界防护和访问控制，必要时可采用 VPN 传输数据、设置 IP 白名单等措施，或者视情断开相关系统与公共互联网的直接相连；针对因接口安全防护不足导致的数据资产暴露风险，采用接口鉴权、访问控制等方式加强接口安全管理。

（7）结合实际建立数据暴露风险监测预警等技术能力，强化对联网数据处理系统的数据安全风险监测分析和防范。

1.5 风险 5: 数据上云上平台安全措施不足引发数据泄露风险

1.5.1 排查方式

（1）查验是否建立企业自建云平台、使用的第三方云平台清单以及上云上平台的数据清单。针对企业自建的云平台，核查云平台在上线运行前是否具备数据收集、存储、传输、使用等环节的安全保护能力；针对使用的第三方云平台，核查企业与云服务商签订的相关合同协议，是否明确云服务模式（如服务器托管服务、存储服务、计算服务），是否针对具体服务模式清晰界定数据上云上平台全流程数据安全保护相关责任义务。

（2）核查重要数据和核心数据上云上平台过程中，是否采取校验技术、密码技术、安全传输通道或安全传输协议等措施，确保数据传输安全；在上云上平台后，是否采取校验技术、密码技术、备份恢复、访问控制等措施，确保数据存储和使用安全。

（3）核查云平台相关服务支撑组件（包含但不限于 Zookeeper、Yarn、Kafka、Hive、Elasticsearch、Logstash、Kibana 等）口令、权限、接口配置等安全策略，是否存在威胁数据安全的策略配置不当等问题。

1.5.2 防范措施

（1）建立企业自建云平台、使用的第三方云平台清单以及

上云上平台的数据清单。针对自建云平台，同步建立适配的数据安全防护能力，并在上线前进行测试验证，确保云平台数据收集、存储、传输、使用等全生命周期安全；针对使用的第三方云平台，在与云服务商签订的相关合同协议中，明确云服务模式，加强数据安全保护责任界定，细化数据上云上平台全流程数据安全保护责任义务。

（2）针对重要数据和核心数据向云平台传输环节，采取校验技术、密码技术、安全传输通道或安全传输协议等措施，确保数据传输安全；在云平台存储、使用环节，采取校验技术、密码技术、备份恢复、访问控制等措施，确保数据存储和使用安全。

（3）定期巡检云平台相关服务支撑组件的口令、权限、接口配置等安全策略设置情况，避免云平台因配置不当威胁数据安全。

2.数据处理人员违规操作引发的风险排查和防范

2.1 风险 6：内部员工不当操作引发数据泄露、非法访问等风险

2.1.1 排查方式

（1）对数据处理活动涉及的操作人员及其操作权限进行梳理，形成数据操作人员权限记录表，包括姓名、部门、岗位职责、涉及数据处理活动、系统平台账号、操作权限等。同时，对重要数据和核心数据处理活动涉及的操作人员进行梳理，形成重要数据和核心数据操作人员清单。

（2）依据数据操作人员权限记录表，排查相关人员平台系统账号分配、开通、使用、变更、注销等的审批记录，研判权限审批环节是否存在安全风险。

（3）依据数据操作人员权限记录表，排查权限设置是否遵循安全策略和最小授权原则，是否对数据处理、数据安全管理、安全审计等岗位角色进行分离设置，研判是否存在权限设置不合理等安全风险。

（4）排查是否定期对数据处理权限记录表进行更新，重点关注离职人员、操作权限发生变化等情况，研判是否存在权限记录表更新不及时、不准确等风险。

（5）依据重要数据和核心数据操作人员清单，排查相关人员是否签署数据安全责任书或保密协议，包括岗位职责、相关义务、处罚措施、注意事项等，研判是否存在人员管理缺失等风险。对重要数据处理活动是否开展重要数据处理活动风险评估。

2.1.2 防范措施

（1）明确数据操作人员权限管理要求，以及相关平台系统账号分配、开通、使用、变更、注销等的审批流程和操作要求，重点关注沉默账号、离职人员账号回收等情况。遵循安全策略和最小授权原则，结合业务需求界定数据处理权限，形成并定期更新数据处理权限记录表。利用技术手段执行权限配置要求、记录账号权限变更操作，避免非授权账号

访问处理数据。

（2）明确重要数据和核心数据处理岗位管理要求，细化岗位职责，人员情况登记入册，相关岗位人员签署数据安全责任书或保密协议，包括岗位职责、相关义务、处罚措施、注意事项等。

2.2 风险7：技术服务外包引发数据泄露、非法访问等风险

2.2.1 排查方式

（1）梳理涉及技术服务外包的业务、系统，包括但不限于数据汇聚（含个人信息）业务/系统、数据共享业务/系统、跨境业务/系统等；对涉及技术服务外包业务、系统收集和产生的数据进行识别梳理，形成涉及技术服务外包数据分类分级清单。

（2）核查技术服务外包方（以下简称合作方）数据安全保护措施落实情况，包括是否明确合作方数据处理安全责任、是否有效约束合作方数据处理范围、是否对合作方数据处理情况进行监督管理、是否落实数据安全保护要求等。

（3）结合合作方的数据安全措施落实情况，分析数据在收集、存储、传输、使用加工、提供、公开等环节存在的数据泄露、篡改、非法访问、滥用等风险。

（4）排查底层软件供应链风险，包括因供应商未落实数据安全保护要求等带来的数据泄露、非法访问等风险。

（5）排查人员管理风险，包括未配备人员权限管理、

操作审批、访问控制、安全审计等措施引发数据非法访问、滥用等风险。

（6）排查技术外包涉及的重要数据和核心数据处理介质使用情况，核查是否存在非授权介质使用等情况。

2.2.2 防范措施

（1）建立完善技术服务外包管理制度，合理确定技术服务外包的范围，明确规定技术服务外包的方式、条件、程序和实施等相关内容，强化技术服务外包审批管理。

（2）加强技术服务外包合作方考察，充分调查合作方的合法性，以及承担相关业务的资质、技术实力、安全能力、业界影响力及从业人员背景等情况。

（3）严格审核签订合作方合同，充分考虑技术服务外包可能带来的风险因素，并通过合同条款予以有效规避或降低风险。

（4）加强技术外包涉及的重要数据和核心数据处理介质使用管控，避免出现非授权介质使用情况，以及病毒、木马通过U盘传播等安全风险。

（5）加强重要数据和核心数据处理系统集成、外包运维等安全管控，及时取消测试账号，规范管理系统管理员等高权限账户，建立并完善覆盖重要操作的日志记录。

（6）加强对企业供应链的安全管理，防范企业重要数据和核心数据通过外包途径泄露。