**{{projectName}}数据安全检查报告**

|  |  |  |  |
| --- | --- | --- | --- |
| **版本编号** | {{version}} | **密级** | {{classification}} |
| **制作人** | {{producer}} | **日期** | {{generatedTime}} |

|  |  |  |  |
| --- | --- | --- | --- |
| **版本变更记录** | | | |
| **时间{{tab}}** | **版本** | **说明** | **修改人** |
| [historyTime] | [historyVersion] | [historyExplain] | [historyAuthor] |

**{{logo}}**

**{{generatedTime}}**

|  |
| --- |
| 目录 |
| [一. 数据安全检查介绍 1](#_Toc36126144)  [1.1 数据安全检查的概念 1](#_Toc36126145)  [1.2 数据安全检查的必要性 1](#_Toc36126146)  [1.3 数据安全检查客户收益 1](#_Toc36126147)  [1.4 数据安全检查的依据 2](#_Toc36126148)  [1.5 数据安全检查的原则 3](#_Toc36126149)  [1.6 数据安全检查的范围 4](#_Toc36126150)  [1.7 数据安全检查的流程 4](#_Toc36126151)  [1.8 数据安全检查风险控制 5](#_Toc36126152)  [二. 数据安全检查工具介绍 7](#_Toc36126153)  [2.1 漏扫工具简介 7](#_Toc36126154)  [2.2 漏扫工具截图 7](#_Toc36126155)  [三. 测试目标说明 8](#_Toc36126156)  [3.1 测试对象 8](#_Toc36126157)  [3.2 时间 11](#_Toc36126158)  [3.3 参与测试人员 11](#_Toc36126159)  [3.4 测试环境 11](#_Toc36126160)  [四. 扫描过程 12](#_Toc36126161)  [4.1 隐患介绍 12](#_Toc36126162)  [4.2 数据安全检查结果简介 12](#_Toc36126163)  [4.3 隐患分析 13](#_Toc36126164)  [4.3.1 高风险项 13](#_Toc36126165)  [4.3.2 中风险项 27](#_Toc36126166)  [4.3.3 低风险项 34](#_Toc36126167)  [五. 总结 40](#_Toc36126168)  [5.1 风险项统计 40](#_Toc36126169)  [5.2 风险扇形图 42](#_Toc36126170)  [六. 测试结论 43](#_Toc36126171)  [七. 感谢 44](#_Toc36126172) | |

1. 数据安全检查介绍
   1. 数据安全的概念

数据安全是保护数字信息资产免遭未经授权的访问、披露、修改或盗窃的做法。这种做法保护数据免受意外或故意威胁，并在组织的整个生命周期中保持其机密性、完整性和可用性。。

* 1. 数据安全检查的必要性

数据安全检查工作往往作为数据安全风险评估的一个重要环节，为风险评估提供重要的原始参考数据。

面向重要基础设施、系统，以检查评估为基础，全面深入排查隐患，以查促建、以查促管、以查促改、以查促防，进一步增强网络数据安全意识，m明确数据安全责任，强化安全措施，提升数据安全防护水平，筑牢网络安全屏障。

* 1. 数据安全检查客户收益

对于客户而言，数据安全检查可以带来以下收益：

* 明确安全隐患点

数据安全检查是一个对网络系统中未知隐患全面排查的过程，让我们清楚的了解隐患的大致范围，以及网络系统的脆弱级别，以此明确整体系统中的安全隐患点。

* 提高安全意识

如上所述，任何的隐患在检查服务中都可能造成“千里之堤溃于蚁穴”的效果，因此检查服务可有效督促管理人员杜绝任何一处小的缺陷，从而降低整体风险。

* 提高安全技能

在测试人员与用户的交互过程中，可提升用户的技能。另外，通过专业的检查报告，也能为用户提供当前流行安全问题的参考。

* 1. 数据安全检查的依据

{{测试单位}}数据安全检查服务将参考下列国内、国际与数据安全检查有关的标准结合{{测试单位}}在数据安全检查方面的规范和经验进行工作。

* 国内可参考的标准、指南或规范
* ISO/IEC 27001:2005信息技术-安全技术-信息系统规范与使用指南
* ISO/IEC 13335-1: 2004 信息技术-安全技术-信息技术安全管理指南
* ……
* 国际可参考的标准、指南或规范
* 信息系统审计标准（ISACA）G3 利用计算机辅助审计技术
* 信息系统审计标准（ISACA）G7 应有的职业谨慎
  1. 数据安全检查的原则

{{测试单位}}在提供数据安全检查服务中，将遵循下列原则。

* 保密性原则

保密性原则是数据安全检查服务中最重要的原则，它是鼓励客户实施数据安全检查服务的心理基础，同时也是对客户隐私权的最大尊重。数据安全检查的保密范围，包括实施过程的保密性和输出成果的保密性。对服务过程中获知的任何客户系统信息均属秘密信息，不得泄露给第三方单位或个人，不得利用这些信息进行任何侵害客户的行为；对服务的报告提交不得扩散给未经授权的第三方单位或个人。

* 标准性原则

{{测试单位}}数据安全检查服务将在国家法律、法规允许的范围内进行，特别是遵照并履行《中华人民共和国人民警察法》第六条第十二款、《全国人大常委会关于维护互联网安全的决定》、《刑法》第二百八十五条、第二百八十六条等相关规定等。

遵守国内、国际与数据安全检查有关的标准进行工作。同时在道德方面，也会严格遵守业界普遍认同的《计算机道德10个戒律》、《信息安全职业道德规范》、以及《网络道德的基本原则》。

* 规范性原则

{{测试单位}}数据安全检查服务将按照{{测试单位}}安全服务工作规范、{{测试单位}}数据安全检查实施规范进行严格落实。实施必须由专业的安全服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，提供完整的服务报告。

* 可控性原则

可控性原则就是数据安全检查服务中对被测试系统造成的可能的各种影响要能够控制得住，既要全面测试，又不能影响生产，服务的工具、方法和过程要在双方认可的范围之内，服务的过程中，避免出现被测试系统运行不稳定，影响生产运行的情况。

* 整体性原则

整体性原则是系统思维方法的一条基本原则。整体原则认为，世界上任何一个有机整体系统，不但内部各组成要素之间是相互联系的，而且系统与外部环境之间也是有机联系的。我们在处理与解决问题时，应当从整体出发，从分析整体内部各组成部分的关系以及整体与外部环境之间的关系入手，去揭示与掌握其整体性质。在原则指导下的数据安全检查服务，强调以综合为基础，在综合的控制与指导下，分析发现的安全问题，对分析结果进行恰当的综合。

* 最小影响原则

数据安全检查服务工作应尽可能小的影响被测试系统和网络的正常运行，不能对现有系统、网络的运行和业务的正常运行产生显著影响。

* 1. 数据安全检查的范围

从整体看，数据安全检查包括：数据安全管理是否到位、数据安全防护措施是否有效、数据处理活动是否合规、个人信息保护要求是否落实、网络数据安全台账是否建立、网络数据安全风险隐患是否排查。

* 1. 数据安全检查的流程

{{测试单位}}数据安全检查服务主要分为四个阶段，包括测试前期准备阶段、测试阶段实施、复测阶段实施以及成果汇报阶段。

1. **前期准备阶段**

在实施数据安全检查工作前，技术人员会和客户对数据安全检查服务相关的技术细节进行详细沟通。由此确认数据安全检查的方案，方案内容主要包括确认的数据安全检查范围、最终对象、测试方式、测试要求的时间等内容。同时，客户签署数据安全检查授权书。

1. **测试阶段实施**

在测试实施过程中，{{测试单位}}测试人员在晚上或者非业务繁忙截断，使用自动化的数据安全检查工具，完成资产识别和数据安全检查等工作。然后由人工的方式对安全扫描的结果进行人工的确认和分析。结合自动化测试和人工测试两方的结果，测试人员需整理数据安全检查服务的输出结果并编制数据安全检查报告，最终提交客户和对报告内容进行沟通。

1. **成果汇报阶段**

根据一次自动化的数据安全检查测试和人工确认分析，在于客户进一步沟通完成之后，整理数据安全检查服务输出成果，最后汇报项目领导。

* 1. 数据安全检查风险控制

为保障客户系统在数据安全检查过程中稳定、安全的运转，我们将提供以下多种方式来进行风险规避。

* 时间控制

从时间安排上，测试人员将将尽量避免在数据高峰时进行测试，以此来减小测试工作对被测试系统带来的压力。另外，测试人员在每次测试前也将通过电话、邮件等方式告知相关人员，以防止测试过程中出现意外情况。

* 工具使用

在使用工具测试的过程中，测试人员会通过设置线程、插件数量等参数来减少其对系统的压力，同时还会去除任何可能对目标系统带来危害的插件，如：远程溢出攻击类插件、拒绝服务攻击类插件等等。

* 技术手段

{{测试单位}}的数据安全检查人员都具有丰富的经验和技能，在每一步测试前都会预估可能带来的后果，对于可能产生影响的测试（如：溢出攻击）将被记录并跳过，并在随后与客户协商决定是否进行测试及测试方法。

* 监控措施

针对每一系统进行测试前，测试人员都会告知被测试系统管理员，并且在测试过程中会随时关注目标系统的负荷等信息，一旦出现任何异常，将会停止测试。

* 对象选择

为更大程度的避免风险的产生，数据安全检查还经常选择对备份系统进行测试。因为备份系统与在线系统所安装的应用和承载的数据差异较小，而其稳定性要求又比在线系统低，因此，选择对备份系统进行测试也是规避风险的一种常见方式。

* 操作记录

测试人员会在测试过程中形成操作记录文档，以便出现意外后进行追溯。

* 沟通配合

测试过程中，确定测试人员和客户方配合人员的联系方式，便于及时沟通并解决工程中的难点。

1. 数据安全检查工具介绍
   1. 检查工具简介

DX数据安全检查系统严格按照计算机信息系统安全的国家标准、相关行业标准设计、编写、制造。

* 1. 检查工具截图

DX数据安全检查系统可以对单个目标或者多个目标同时进行扫描，同时可以选择web扫描或者是主机扫描，支持自动生成报告和报告的导出。如图2.2.1：

图2.2.1

1. 测试目标说明
   1. 测试对象

|  |  |  |  |
| --- | --- | --- | --- |
| 单位名称 | 涉及系统 | 系统IP | 资产数目 |
|  | {%tr for 目标 in 目标详情%} | | |
| {%vm%}{{项目名称}} | {{目标.目标地址}} | {{目标.目标主机}} | 1 |
|  | {%tr endfor%} | | |
| 统计 | | |  |

* 1. 时间

|  |  |  |  |
| --- | --- | --- | --- |
| **测试工作的时间段** | | | |
| **起始时间** | {{开始时间}} | **结束时间** | {{结束时间}} |

本份测试报告分析的各种安全风险，仅限定于在上述时间段内测试反馈信息的整理，不包括非上述时间段内的因系统调整、维护更新后出现的其他变化情况。

* 1. 参与测试人员

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **参测人员名单** | | | | | |
| **姓名** |  | **所属部门** | {{测试单位}}检查小组 | **联系方式** |  |
| **姓名** |  | **所属部门** | {{测试单位}}检查小组 | **联系方式** |  |

测试人员名单

* 1. 测试环境

本次数据安全检查过程中，{{测试单位}}测试小组使用以下IP地址开展的分析工作，在此通知{{项目名称}}相关人员在对受测试的目标站点服务器、相应的网络入侵检测系统进行安全监控和日志分析时，排除以下IP地址产生的任何违规信息，以保证分析结果的准确有效。

|  |  |  |  |
| --- | --- | --- | --- |
| **IP地址** | **IP地址** | **IP地址** | **IP地址** |
| —— | —— | —— | —— |

1. 扫描过程
   1. 检查项介绍

所谓检查项就是指程序设计方面在安全性上存在缺失，留下了隐患，而网络黑客可以从这些隐患对远程计算机进行攻击，窃取数据，破坏远程用户电脑等等，危害很大。尤其是机密被窃，损失不可估计，就是个人用户也非常危险，个人账号密码被入侵后可能会被窃取。

* 1. 数据安全检查结果简介

数据安全检查项是在数据具体实现和具体使用中产生的错误，但并不是数据中存在的错误都是安全隐患。只有能威胁到数据安全的错误才是隐患。

**通过数据安全检查得出的隐患如下**：

**红色上箭头**代表高级风险安全隐患

**橙色横线**代表中级风险安全隐患

**蓝色下箭头**代表低级风险安全隐患

|  |  |  |
| --- | --- | --- |
| 风险名称 | 风险标签 | 风险数量 |
| {%tr for 隐患 in 高危统计 %} | | |
| {{隐患.风险名称}} | {{隐患.风险标签}} | {{隐患.风险数量}} |
| {%tr endfor %} | | |
| {%tr for 隐患 in 中危统计 %} | | |
| {{隐患.风险名称}} | {{隐患.风险标签}} | {{隐患.风险数量}} |
| {%tr endfor %} | | |
| {%tr for 隐患 in 低危统计 %} | | |
| {{隐患.风险名称}} | {{隐患.风险标签}} | {{隐患.风险数量}} |
| {%tr endfor %} | | |

* 1. 隐患分析

在本章节，对于数据处理活动将进行主要分析，一一列出检查项的隐患详情以及修复方案，和相关隐患所涉及的系统。

经过统计后风险项主要分布如下。

* + 1. 数据采集项

{{?var1}}

* + - 1. {{title1}}

|  |  |
| --- | --- |
| 风险ID | {{riskId1}} |
| 风险标题 | **{{title1}}** |
| 风险描述 | {{desc1}} |
| 风险选项 | {{option1}} |
| 风险分值 | {{score1}} |
| 修复建议 | {{adv1}} |
| 复测结果 |  |

{{/var1}}

* + 1. 数据传输项

{{?var2}}

* + - 1. {{title2}}

|  |  |
| --- | --- |
| 风险ID | {{riskId2}} |
| 风险标题 | **{{title2}}** |
| 风险描述 | {{desc2}} |
| 风险选项 | {{option2}} |
| 风险分值 | {{score2}} |
| 修复建议 | {{adv2}} |
| 复测结果 |  |

{{/var2}}

* + 1. 数据存储项

{{?var3}}

* + - 1. {{title3}}

|  |  |
| --- | --- |
| 风险ID | {{riskId3}} |
| 风险标题 | **{{title3}}** |
| 风险描述 | {{desc3}} |
| 风险选项 | {{option3}} |
| 风险分值 | {{score3}} |
| 修复建议 | {{adv3}} |
| 复测结果 |  |

{{/var3}}

* + 1. 数据处理项

{{?var4}}

* + - 1. {{title4}}

|  |  |
| --- | --- |
| 风险ID | {{riskId4}} |
| 风险标题 | **{{title4}}** |
| 风险描述 | {{desc4}} |
| 风险选项 | {{option4}} |
| 风险分值 | {{score4}} |
| 修复建议 | {{adv4}} |
| 复测结果 |  |

{{/var4}}

* + 1. 数据交换项

{{?var5}}

* + - 1. {{title5}}

|  |  |
| --- | --- |
| 风险ID | {{riskId5}} |
| 风险标题 | **{{title5}}** |
| 风险描述 | {{desc5}} |
| 风险选项 | {{option5}} |
| 风险分值 | {{score5}} |
| 修复建议 | {{adv5}} |
| 复测结果 |  |

{{/var5}}

* + 1. 数据销毁项

{{?var6}}

* + - 1. {{title6}}

|  |  |
| --- | --- |
| 风险ID | {{riskId6}} |
| 风险标题 | **{{title6}}** |
| 风险描述 | {{desc6}} |
| 风险选项 | {{option6}} |
| 风险分值 | {{score6}} |
| 修复建议 | {{adv6}} |
| 复测结果 |  |

{{/var6}}

1. 总结
   1. 风险项统计

通过对{{目标总数}}个目标进行数据安全检查，共发现所有级别风险{{风险总数}}个，其中高风险项{{高危总数}}个，中风险项{{中危总数}}个，低风险项{{低危总数}}个，

|  |  |  |  |
| --- | --- | --- | --- |
| 单位名称 | 系统名称 | 风险级别 | 隐患个数 |
|  | {%tr for 目标 in 目标详情%} | | |
| {%vm%}{{项目名称}} | {{目标.目标地址}} | 高 | {{目标. 风险数量.high}} |
| 中 | {{目标.风险数量.medium}} |
| 低 | {{目标. 风险数量.low}} |
|  | {%tr endfor%} | | |

* 1. 风险扇形图

{{级别饼图}}

{{全量饼图}}

1. 测试结论

经过本次对目标的漏扫测试，我们对此次漏扫目标的整体安全评价是 合格**。**

|  |  |
| --- | --- |
| **安全等级** | **资源内容描述** |
| 优秀  **（**符合任何一个条件**）** | 1、存在一个或一个以上严重的安全问题，可直接导致系统受到破坏；  2、与其他非安全系统连接，同时存在相互信任关系（或账号互通）的主机；   1. 发现已经被人入侵且留下远程后门的主机； 2. 存在3个以上中等安全问题的主机；   5、与其他非安全系统在一个共享网络中，同时远程维护明文传输口令；  6、完全不能抵抗小规模的拒绝服务攻击 |
| 合格  **（**符合任何一个条件**）** | 1. 存在一个或一个以上中等安全问题的主机； 2. 开放过多服务，同时可能被利用来进行拒绝服务的主机；   3、与其他非安全系统直接连接，但暂时不存在直接信任(或账号互通)关系；  4、远程维护通过明文的方式传递信息；  5、存在三个以上轻度安全问题的主机；  6、只能抵御最低级的拒绝服务攻击； |
| 不合格  **（**符合全部条件**）** | 1. 最多存在1-2个轻度安全问题； 2. 远程维护方式安全； 3. 与不安全或一般安全系统相对独立；   4、能抵挡一定规模的拒绝服务攻击。 |

安全等级评定

1. 感谢

在本次远程数据安全检查过程中，{{测试单位}}感谢相关人员和在数据安全检查过程中进行沟通、协调的相关部门和人员的大力配合，以使得我们的工作能够顺利完成。对于您的大力支持我们深表感谢。