WANGLUOANQUAN HE XINXIHUA

网络安全和信息化

Cybersecurity & Informatization

赛迪出版物
6
2022年

原《网络运维与管理》
《网管员世界》
邮发代号：2-99 零售价：30元（不含APP25元）

主管单位：中华人民共和国工业和信息化部

2022安全样板工程

——云原生安全、数据安全、零信任篇

ISSN 2096-2215

2022年6月刊

目次

本刊已被中国知网收录
网址：www.cnki.net

视点
Viewpoint

发现
Discovery

聚焦
Focus

数智时代，网络安全正在向体系化、常态化、实战化方向迈进。《网络安全和信息化》杂志推出“2022安全样板工程”系列专题，本期聚焦云原生安全、数据安全、零信任三大领域，通过样板案例展示，向广大企业用户推介网络安全建设思路和经验，更好地护航数字经济发展。

特别企划
Special Project

由于IC卡存在严重的安全缺陷，我国交通、安防等行业已经普遍采用非接触CPU卡取而代之。本文通过对非接触CPU卡几种典型的攻击方法进行分析，解释了安全漏洞产生的原因，并给出相应的缓解对策。

主管单位
中华人民共和国工业和信息化部
主办单位
中国电子信息产业发展研究院
赛迪工业和信息化研究院(集团)有限公司
出版：北京赛迪出版传媒有限公司
社长兼总编辑：宋波
总编助理：郭涛
编辑部：季莹 章继刚 赵志远
编辑部E-mail:
netadmin@365master.com
编辑部电话：010-88559469/9450
IT运维网：http://www.365master.com
编辑：章继刚
网站运营电话：010-88558043
市场部：崔朝伟 郭娟妮 赵锦
市场部电话：010-88558559
美编：刘骏楠
发行部：郭娟妮
发行部E-mail:
guojuanni@ccidmedia.com
发行部电话：010-88558703
编辑：《网络安全和信息化》编辑部
地址：北京市海淀区紫竹院路
66号赛迪大厦18层
邮政编码：100048
传真：010-88558030
邮发代号：2-99
国际标准连续出版物号
ISSN 2096-2215
国内统一连续出版物号
CN 10-1416/TN
广告发布登记通知书编号
京海工商广登字20170178号
承印：廊坊市鸿煊印刷有限公司
每月5日出版发行
零售价：30元（不含APP25元）

文章通过研究分析国内外政务数据风险现状，结合政务数据的特征，设计政务数据安全风险评估模型，并给出风险评估模型中各要素的计算方法，提出政务数据安全风险的定量分析方法。

面向政务数据的安全风险评估方法研究

■ 中国软件评测中心 李安伦 刘龙庚 马士民

政务数据是政府部门满足经济社会治理需求，履行职能过程中产生或使用的重要资源，蕴藏着难以估量的经济发展、社会运行以及国家战略价值。数据要素的高效配置，是推动数字经济发展的关键一环，随着大数据应用的日益广泛，政务数据开放已成为政府机构合作的重要内容，政务数据资源共享和开放可以极大地促进大数据产业发展。

由于政务数据的敏感性，如果政务数据被恶意分析利用，可能威胁到国家安全，如黑客对政府网站的攻击、金融数据被不法分子窃取以及个人敏感信息大规模泄露等。另一方面，近年来各行业数据泄露事件频发，给企业带来了巨大的经济损失，严重影响了公众的正常生活，同时将数据安全推向了“重灾区”，数据安全问题已成为社会、企业和用户最为关注的热点。数据安全是数据应用的基础，政府开放数据的安全更是直接影响国家安全和社会稳定。

国内外研究现状

政务数据作为政府部门组织和执行各项事务或者活动中产生的数据，包含了广泛的数据内容，小到公民的个人信息，大到国家的重大决策和机密数据。因此，政务数据的安全至关重要。进入 21 世纪，“互联网 + 政务服务”等理念得到广泛推广，云计算、大数据等技术迅速发展并得到广泛应用。然而，大数据等技术在为政府部门提供科学决策、为民众提供便利的同时，也成为攻击者获取政务数据中敏感信息的便捷工具，使得政务数据面临更大、更难以预料的安全风险。

政务数据的安全风险分析评估对于有效地防范政务数据中存在的安全问题是必不可少的。自 1985 年美国国防部颁布可信计算机系统评估准则，国外关于信息系统的安全风险评估的研究已经有 30 余年。包括美国、加拿大和法国等在内的许多发达国家都在安全风险评估方面相继颁布了相应的标准，包括信息技术安全评估准则、可信计算机产品评价准则。我国关于安全风险评估的研究起步较晚，但是近十年来，随着我国信息技术的快速发展，一系列标准，如《信息安全技术 信息安全风险评估规范》《信息安全技术 信息安全风险评估实施指南》等也相继颁布。除了遵循已有的标准规范之外，采用合适的评估方法对于政务数据的安全风险分析也是非常重要的。

面向政务数据的安全风险分析

随着物联网、大数据、云计算和人工智能等技术的飞速发展与推广应用，政务信息化不断推进，当前

的政务数据正面临如下的安全风险。

1. 政务数据集中管理风险

当下政务云已成为个地方数字政府建设的关键基础设施，集中化的政务云平台和大规模数据的管控、调度模式面临着许多新的安全挑战和风险，存在“一点突破，全线泄漏的数据安全风险”。

2. 政务数据共享和分发安全

政务数据开放、共享涉及监管机构、其他政务部门和第三方，数据共享的频度非常高，数据利用、共享场景非常复杂，也导致数据安全手段落实难度大。

3. 政务系统、数据开发利用存在供应链安全隐患

随着开源工具在政务领域的广泛使用，政务系统平台开发和运维，政务数据挖掘利用的外包形态、人员和技术组件等存在很高的安全隐患。

4. 政务数据敏感度非常高，易被攻击

政务数据大多和国计民生、国家经济发展等紧密关联，数据量巨大、附加价值非常高，在经济和政治双重因素叠加的情况下，政务数据面临的安全威胁剧增。

5. 政务数据的跨境风险

政务数据公开过度、政务数据对外合作审查不严，极易导致政务数据的泄露，从而被境外组织甚至有政府背景的间谍机构获取，从而危害国家安全。

6. 政务数据协同安全风险

随着基于政务数据开发的办公和业务应用App，安装运行在智能移动设备上，面临着敏感信息泄露、应用仿冒、用户身份冒用、个人隐私侵犯、移动终端丢失或被盗等主要安全风险。PC 端、移动端的办公和业务信息泄露，是行业机构普遍关注的重要风险移动端敏感信息泄露。

由于政务数据涉及数据广泛，价值巨大，往往其数据敏感级别比个人消费应用数据敏感级别更高，是国外情报机关、黑产链等关注的重点，政务数据通信过程中，会面临通信窃听导致敏感信息泄露的风险和非法篡改通信内容危害通信完整性的风险，一旦发生信息窃取或篡改，往往造成更加严重的不良影响。政务应用数据资产会面临与传统互联网应用相似的数据安全风险，包括越权、数据丢失和操作抵赖等，从而导致政务数据泄露。

政务数据安全风险评估方法设计

数据安全风险评估模型如图所示，风险识别过程中得到的基本要素及其属性作为输入，通过风险计算过程得到风险值，同时描述如何评价风险计算结果，在完成了数据资产识别、数据应用场景识别、数据威胁识别、脆弱性识别，以及对已有安全措施确认后，将采用适当的方法与工具确定数据威胁利用脆弱性导致安全事件发生的可能性，以及安全事件发生对组织的影响，获知安全风险。

1. 资产识别

为了对政务数据资产的价值进行准确的评估，本文以政务数据的重要程度属性为根据，并从政务数据的作用范围和敏感程度两个维度计算数据资产的重要程度。政务数据的作用范围表示使用数据产生的利益辐射范围。根据数据的作用范围，将政务数据分为 3 个类别。

（1）较小：数据的作用在业务发展战略中的定位相对较低，作用范围只覆盖到业务、组织内部或数据资产本身，对组织和社会的经济和声誉等影响较小。

（2）一般：数据的作用在业务发展战略中的定位中等，作用范围能够覆盖业务、组织或企业等较大范围，对组织或企业的经济及信誉影响较大。

（3）很大：在业务发展战略中的定位非常高，数据作用范围上升到社会层面，直接影响到国家的政

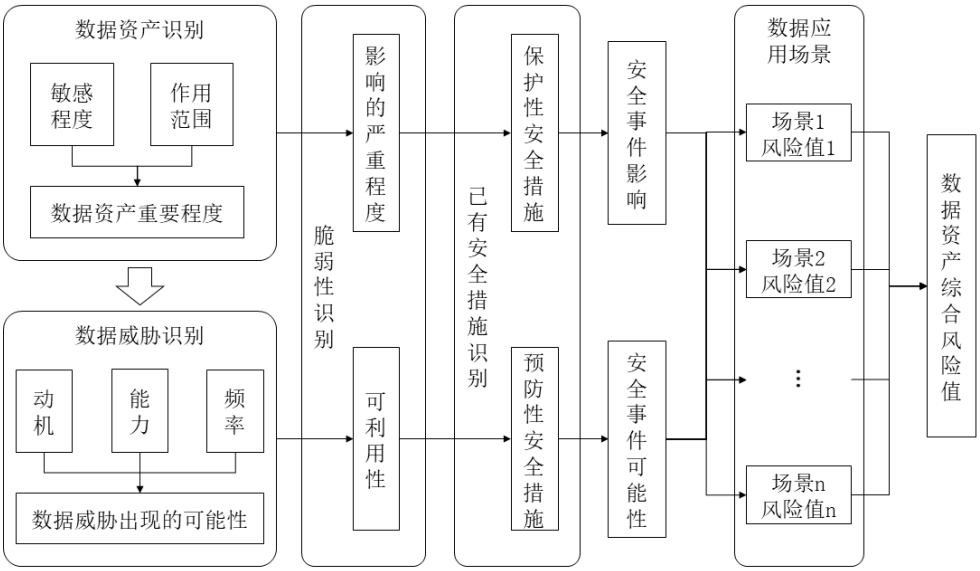

图 数据安全风险评估模型

治、经济和文化等方面。

政务数据的敏感程度表示数据泄露后造成的危害程度，根据数据的敏感程度将数据分为 3 个类别，分别为敏感数据（Sensitive Data）、内部数据（Internal Data）和公开数据（Public Data），如表 1 所示。

表 1 政务数据敏感程度等级划分

	政务数据敏感程度		
	非敏感数据	涉及用户隐私数据	涉及国家秘密数据
等级划分	公开数据	内部数据	涉密数据

（1）公开数据。公开数据的使用对象为所有社会公众，可主动公开在面向社会公务服务的政务系统中，如公开的通知公告、已发布的标准规范等。

（2）内部数据。内部数据的使用对象为组织内的所有人员，仅可在组织内部被读取和使用，如职工电话表、内部通知公告等。

（3）敏感数据。敏感数据的使用对象为组织内的部分人员，仅可在内部可控范围被读取和使用，如一些未公开的研究数据等。

结合针对数据资产的作用范围和敏感程度，可以得到表 2 所示的政务数据重要程度矩阵，其中，政务数据的重要程度共分为 5 个等级。

表 2 政务数据重要程度矩阵

作用范围	敏感程度		
	公开数据	内部数据	敏感数据
较小	1	2	3
一般	2	3	4
很大	3	4	5

2. 数据应用场景识别

确定待评估的数据对象后，针对每一类待评估的数据对象，识别其涉及的各类应用场景。数据应用场景涉及业务流程或使用流程、相关数据活动以及流程各环节参与主体。在不同的数据应用场景中，

数据威胁、脆弱性以及已有的安全措施可能存在差异，因此需要分别结合数据风险值进行综合评价。

3. 威胁识别

威胁是一种对资产构成潜在破坏的可能性因素，是客观存在的。数据威胁要素属性包括数据威胁动机、能力及频率。分析出具体数据威胁后，需要进一步根据威胁可能的来源分析其攻击动机、攻击能力，并根据调查分析威胁产生的概率。数据威胁发生可能性的赋值由数据威胁动机赋值、能力赋值及频率赋值共同确定。

4. 脆弱性识别

脆弱性是数据应用场景自身存在的，如没有被数据威胁利用，脆弱性本身不对数据资产造成损害，如数据应用场景中涉及的信息系统、存储系统、业务系统足够健壮，数据威胁难以导致安全事件的发生。一般通过尽可能消减数据应用场景的脆弱性，来阻止或消减数据威胁造成的影响，所以脆弱性识别是数据安全风险分析中最重要的一个环节。

脆弱性要素属性包括脆弱性可利用性、脆弱性影响严重程度。通过分析数据应用场景中脆弱点可能被利用的访问路径、访问复杂性、鉴别次数判断脆弱性可利用性，应用场景中已部署了安全措施，可视情况调整可利用性等级。通过分析脆弱性对数据机密性、完整性、可用性和可控性影响，判断对数据影响的严重程度。

脆弱性可从技术和管理两个方面进行审视，技术脆弱性涉及 IT 环境的物理层、网络层、系统层和应用层各个层面的安全问题隐患。管理脆弱性又可分为技术管理脆弱和组织管理脆弱性两方面，前者与具体技术活动相关，后者与管理环境相关。

5. 已有安全措施识别

安全措施可以分为预防性安全措施和保护性安全措施两种。有效的安全措施与脆弱性识别存在一定的联系。一般安全措施的使用将减少系统技术或管理上的脆弱性，已有安全措施在脆弱性分析过程中，分别影响脆弱性可利用性与脆弱性影响严重程度的赋值。

6. 风险计算

数据安全风险分析的主要过程：

（1）根据数据威胁脆弱性利用关系，结合数据威胁的可能性、脆弱性和可利用性计算安全事件发生的可能。

（2）根据数据重要程度及脆弱性影响严重程度，计算安全事件一旦发生后对数据、业务及组织造的影响。

（3）部分安全事件的发生造成的损失不仅仅针对该数据资产本身，还可能影响业务连续性、组织声誉，造成经济损失等；不同安全事件的发生对业务与组织造成的影响也是不一样的。在计算某个安全事件的影响时，应将对组织的影响也考虑在内。计算出安全事件发生的可能性及安全事件的影响程度。

（4）综合数据资产在各应用场景中的风险，确定数据资产在不同应用场景下的风险值，最后根据不同场景对于风险的影响因子，综合计算数据资产风险，根据综合风险值计算结果，最终对政务数据的安全风险进行评估。

结语

本文提出了一种面向政务云的数据安全风险评估方法，首先对政务数据面临的安全风险进行详细的分析，提供了针对政务数据的资产识别、应用场景识别、威胁识别、脆弱性识别以及安全措施识别等要素信息的识别方法，并通过量化各要素信息，最终实现针对政务数据的安全风险评估。N