网络安全等级保护2.0数据安全的探究

侯建龙

（河北千诚电子科技有限公司 河北 石家庄 050011）

[摘 要] 当前，构建网络安全等级保护体系，并确保网络安全标准具有一定的适用性和可操作性，能够有效的避免网络安全漏洞，提升国家信息安全保护质量。

[关键词] 网络安全；等级保护；个人信息保护

引言

数据安全是计算机以及网络等学科的重要研究领域之一，具有多层次、多环节、多场景的特点。首先，数据安全具备“三性”特点，机密性、完整性以及基础特性可用性；其次，数据安全涉及多类技术和管理领域，制度安全治标，技术安全治本，其他方面的安全也是必不可少的环节，都是数据安全的多维度组成部分；再次，数据安全涉及面广，不仅关系到个人隐私、企业商业隐私甚至会直接影响国家安全，需要审慎对待。

1 数据安全威胁

造成数据泄漏或篡改的原因主要包括外部攻击、内部威胁、系统故障三类。根据《2017年全球数据泄漏成本研究》报告，在数据泄漏事件中，47%的事件涉及恶意或犯罪行为；25%是由于员工或承包商疏忽；28%涉及系统故障，包括IT和业务流程故障。内部人员有意或无意的数据泄漏已经替代外部攻击，成了数据泄漏的主要原因，因此，要保障数据安全就必须内外兼修。

2 数据安全管理要点

首先是业务特性。各类数据在企业生产运行、经营管理、客户服务等领域发挥着重要的作用，同时，网站门户、在线业务应用和通信群组的内容安全已成为国家网络意识形态安全的重要组成部分。由于企业数据量大、分布面广、利用价值高、数据采集点多、发布渠道多样化等，各类数据泄漏的风险大幅提升，企业数据安全防护面临严峻挑战。其次是保障要求。充分认识新形势下数据安全的重要性，从责任、管理和技术上进一步夯实基础，强化全员数据安全与保密教育，将数据安全上升到企业安全乃至国家安全的高度，完善数据安全措施与手段，确保将企业各项数据保护要求落实到位。

3 网络安全等级保护2.0数据安全

3.1强化2.0安全体系标准建设

2.0安全体系标准不仅包含了云计算系统的安全拓展需要，而且在多个领域进行拓展，使得网络信息安全管理的内容更加全面。同时，2.0安全体系新标准对网络信息系统安全技术的应用进行内容归纳；现阶段，网络信息系统的安全技术被划分为四个层面，其分别为：物理与环境安全管理；网络与通信安全管理；设备与技术安全管理；应用与技术安全管理。此外，当前网络信息系统的安全评价指标也发生变化，实际评价中，安全制度与策略，管理结构与人员、设备与安全技术、应用和数据是2.0安全体系评价标准的重要内容，其实现了网络信息系统安全管理结构的清晰划分，有助于企业安全管理质量的进一步提升。

3.2加解密技术的应用

对称、非对称等加密技术在保护数据隐私安全方面确实有很好的性能，能够对数据安全提供有效的技术保障。对称加密：IDEA、AES以及DES加密算法里，加、解密密钥大多是一样的，原始的数据和密钥加密成密文后发送给接收者，接收者在获得密文后用同样的密钥和逆算法把密文解密成原始的明文。非对称加密：常用的非对称加密有RSA及DSA等算法，因加、解密密钥不同，所以无法相互推算得出，由加密密钥（公钥）加密后的数据只能通过解密密钥（私钥）来解密，即接收者可将明文发给发送者，发送者将初始数据加密后重新发给接收者，接收者利用保留的私钥将密文解密。属性粒度加密：当前电网的数据加密技术很有限，主要是元组粒度及属性粒度加密技术，前者在处理字符型数据及多表查询时会产生大量失效元组，后者可以在准确查询数据结果的同时极大地降低客户端资源消耗，使查询的透明性得以增强，减轻了大量数据堵塞客户端的问题。对称加密、非对称加密以及属性力度加密在运算效能、密钥管理、场景应用等方面各具优势，因此，在具体使用过程中需要进行比较细致的甄别分析，从而最大化发挥加密保护的效能。

3.3全寿命周期管理

首先是数据采集与传输环节。明确可采集数据的内容及重要程度，明确数据安全保护的对象，落实重要数据内容加密传输以及数据完整性、有效性检测措施，强化数据质量、数据分类和重要性定级机制。其次是数据存储环节。明确重要数据的安全存储与使用级别，对重要数据进行必要强度的加密存储，强化重要数据备份措施，禁止与互联网或其他公用网络相连的计算机、智能手机、平板电脑等终端设备存储、处理企业涉密数据。然后是数据使用环节。落实企业业务授权及账号权限管理要求，合理分配数据访问权限，强化数据访问控制；排查整改业务逻辑缺陷和漏洞，防止丢失泄密事件；加快数据脱敏等用户敏感数据的保护措施建设；健全数据安全日志审计、监测预警、态势感知机制。最后是数据销毁环节依据国家和国家电网公司电子数据恢复、擦除与销毁工作的相关要求开展数据恢复、擦除与销毁等工作。

3.4应用和数据安全

信息系统身份鉴别，可以采用用户账户和密码的方式，密码要设置复杂度要求，也可以采用用户账户与USB-KEY进行绑定的双因子方式进行认证，为安全事件的跟踪审计提供有效依据。应配置对登录的用户账号和权限访问控制的功能，并及时删除或停用应用系统中多余的、过期的账号；删除或修改系统默认账户及登录口令，设置不同的管理员权限，操作系统和数据库管理员分权管理，安排不同人员担任并分配不同的账号。开启应用系统及其使用的中间件的自带审计功能，并把相应的日志发送到日志审计系统，统一进行审计分析。同时部署数据库审计系统，对管理员操作数据库的相关记录进行安全审计，防止非法操作及更改相关数据信息。应用系统在资源控制方面，应设置一个客户端只允许一个用户同时登录，并且一个用户只允许同时在一个客户端上登录，从而保障信息资源的安全。在数据完整性和保密性方面，通过部署加密机实现网络传输层数据的完整性和保密性防护。对信息及业务数据加密传输和存储，确保传输的数据是加密后传输和存储。在数据备份和恢复方面，重要数据实现本地备份和恢复并且异地能够实时备份实现数据的备份和恢复。

结束语

总之，随着网络安全形势的日益严峻，国家有关部门先后出台了一系列文件，明确了等级保护的重要性。为了履行国家《网络安全法》法律义务，落实网络安全保护责任，企业需开展网络安全等级保护建设工作，按照技术与管理的需求进行建设实施，并加强日常运维与监管。

参考文献

[1]马力，祝国邦，陆磊.《网络安全等级保护基本要求》（GB/T22239-2019）标准解读[J].信息网络安全，2019，19（2）：77-84.

论新媒体对文化传播力的影响与提升

王一恒

（东北大学国防教育学院 辽宁 沈阳 110000）

[摘 要] 随着媒体信息技术的发展，人们越来越重视新媒体传播的重要性。新媒体可以为文化传播提供新途径，创新文化传播方法，推动我国文化产业的发展。本文通过分析新媒体对文化传播力的影响，详细阐述了新媒体在提升文化传播力方面采取的措施，希望能给相关人士提供借鉴。

[关键词] 新媒体；文化传播力；提升策略；影响力

引言

我国的先进文化正处于改革的关键时期，文化的传播和发展的方法需要得到创新。新媒体是媒体行业的新形势，在文化传播方面发挥重要作用。随着传播文化的环境的变化，文化的传播限制越来越宽松，管理文化传播内容越来越困难。

一、新媒体对文化传播力的影响

（一）新媒体有助于构建多样化的文化传播模型

新媒体技术的优点在于信息多样化、技术功能丰富、使用途径广和传播成本低等，新媒体可以构建多样化的文化传播模型，让多种文化拥有发展的潜能。在新媒体技术下，人们乐于表达自己，表达的基础是不违反相关的法律法规，表达的自由度很高，不受社会经济、文化、地域环境等限制。例如人们可以在不同平台上表达自己，根据平台的不同定位，表达自己的感悟与价值观，这些平台包括微博、微信等新媒体社交平台[1]。

（二）新媒体有助于构建实时互动的文化传播模型

新媒体的显著特点在于媒体信息实时性高和互动性强，使得信息传播具有共享性和发展性。对于传统的文化传播方式来说，传播的途径较为固定和缺少多样化，一般借助传统媒介例如报纸、广播、可视化电视等，传播的信息不能和信息获取者间产生良性互动，且信息时延性很高，不利于构建实时互动的文化传播模型。新媒体在传统的文化传播模型上进行改进，强调了信息传播的实时互动特性，让信息的接受者不再是被动接受，可以主动交流，文化传播的效率得到快速提高。新媒体有助于构建实时互动的文化传播模型，帮助丰富文化传播内容与途径[2]。

（三）新媒体有助于构建资源共享的文化传播模型

资源共享对于文化传播来说具有重要意义，文化不是一个人的文化，是多种集体间产生的多种文化的融合。现有的资源需要重组再利用，在资源的传播方面需要做到共享化和便利化。新媒体有助于构建资源共享的文化传播模型，利用媒体信息技术实现高效应用集成电路完成文化传播的目的，在卫星等通讯方式成熟发展下，实现文化传播方法的改革。加强文化传播力不仅是要发展文化传播途径，更需要实现文化传播的时效性。文化传播的目的在于实现不同文化间的沟通交流和融合利用，新媒体技术可以提高文化传播的效率，实现文化资源共享。

二、新媒体在提升文化传播力方面采取的措施

（一）建设网络宣传制度，严格监管新媒体网站

新媒体在传播文化的过程中需要有规范的网络宣传制度约束，发挥新媒体自身优势和文化影响力。新媒体有利于先进文化的传播，但是同时也存在着传播的弊端，网络宣传制度的建设正是为了解决这些问题，提升网络参与人员的素质以及文化传播的全面性和及时性[3]。对于新媒体网络建设，我们需要做到以下几点：第