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

一，严格监管新媒体网站。网站是文化传播的客观平台，也是人们直接接触文化内容的平台。网络建设中存在大量的非法网站和钓鱼网站等，严格监管力度打压不法网站，打压的方法包括罚款、强制关闭网站、通告批评、追究相关负责人的刑事责任等。第二，丰富举报途径。监督不仅包括政府监督、国家监督、企业监督，还包括人民群众监督。人民群众对网站建设的监督工作需要丰富监督途径和举报途径，包括电话举报、邮件监督、上门监督及其他发方式等。人民群众对于文化传播力的相关建议和意见有利于文化发展，有利于政府工作的进行，政府及其相关单位应该要积极鼓励，发布政策支持。脱离群众的方法最不可取，人民群众才是政府工作的受益者。

（二）提高新媒体工作人员的职业核心素养

新媒体的发展依赖于信息技术改革和设备更新换代，对于新媒体工作人员的自身要求随之增加，新媒体工作人员必须要掌握新媒体技术的应用方法，不断培养自身的职业核心素养。在文化传播领域，我们需要防范不良文化的形成和传播，抵制非法文化。为了实现文化传播朝着正向发展，对新媒体工作人员评价制度需要不断加强，只有新媒体工作人员的职业核心素养提高了，才能为媒体传播工作打好基础。严格新媒体工作人员的筛选制度，在聘请人才的环节需要对人才进行全方位审核，提高学历要求，提高人才核心素养要求。对于现有新媒体工作人员来说，企业应该要定期对她们进行专业技能培训，培训不局限于职业技能，还可以是经验培训和道德文化素养培训等[4]。建立新媒体工作人员正确的核心价值观和精湛的专业技能，有助于文化传播和发展，有助于新媒体的应用。为了提高新媒体工作人员的工作积极性，对新媒体工作人员进行培训的同时需要加入考核制度和奖惩制度，考核新媒体工作人员的现有知识掌握程度和应用程度，对于考核优秀者予以精神奖励和物质奖励，对于考核不合格者予以精神批评和物质惩罚。提高新媒体工作人员的职业核心素养，有利于提升新媒体在文化传播力方面的影响。

（三）利用新媒体提高文化传播覆盖率

当下的新媒体表现形式有视频、图像、声音等，借助新媒体平台例如抖音短视频、微博等实现多种文化高效融合和表达。人们对于一些高深文化的理解力不够，此时，如果采取新媒体的方法，可以化复杂文化为通俗易懂的文化，提高文化的覆盖率和传播范围。利用新媒体提高文化传播覆盖率是新媒体应用的常见方法，它使文化变得更有人情味，让人们更容易接受文化，感悟文化的魅力与感染力，提高文化传播效率，促进文明社会的发展。

三、结束语

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，是创新文化的传播和发展的途径。新媒体有助于构建资源共享、多样化、实时互动的文化传播模型，我们需要利用新媒体提高文化传播覆盖率，提高新媒体工作人员的职业核心素养，建设网络宣传制度，严格监管新媒体网站，充分发挥新媒体在文化传播力方面的影响力和作用力。

参考文献

[1]陆晓燕.新媒体时代城市文化传播力的现状及提升路径——以武汉为例谈“5W”的传播模式[J].北方传媒研究，2019.

[2]黄碧玉.新媒体平台对文化传播力的负面影响及价值塑造——抖音APP的“罪与罚”探析[J].黑河学院学报，2019（5）.

[3]秦慧媛.论互联网背景下新媒体对文化传播力的嬗变与发展[J].北京印刷学院学报，2019（11）：15-18.

[4]孟颖，高军.新媒体环境下微博在文化传播中的作用[J].科技创新与生产力，2018，000（002）：P.11-13.

攻击图应用下的网络安全风险评估技术探讨

张振庄

（河北千诚电子科技有限公司 河北 石家庄 050011）

[摘 要] 网络安全风险评估技术是解决网络安全问题的一种有效技术。可以通过网络安全模型构建、攻击图构建、网络安全风险评估框架、系统验证等方法来避免网络攻击，从而营造绿色网络环境。

[关键词] 网络安全；风险评估；脆弱性；攻击图

引言

最新的《中国互联网络发展状况统计报告》指出，我国的互联网普及率超过了60%，乡村教育、在线政务、网络消费等都有了显著的进步和发展。本文首先介绍了网络安全风险评估的定义，几大国际性评估标准的发展，将网络安全风险评估的相关方法分为四类，分别是：基于漏洞扫描和入侵检测的评估方法，基于知识推理的评估方法，基于资产价值的评估方法和基于模型的评估方法。随后详细介绍了基于模型的评估方法，定性评估选取了攻击链模型、攻击表面模型、自动机模型3种模型，定量评估以常见的攻击树模型、攻击图模型、网络传染病模型为例，给出了模型的定义、发展和研究状况以及不同学者对模型的修改，对比了不同模型的适用范围和优劣势，方便根据实际需要选择合适的评估方法。而后补充介绍了几种交叉学科的评估方法，如模糊理论和神经网络，这些方法目前的研究还较少，不够成熟，但是对网络安全风险评估的发展起了一定的推动作用。

1 网络安全风险评估方法

目前国内外现有的网络安全风险评估方法有很多，有基于漏洞扫描和入侵检测的评估方法，基于知识推理的评估方法，基于资产价值的评估方法等，在理论研究领域应用最广的是基于模型的评估方法。基于漏洞扫描和入侵检测的评估方法，利用专业扫描工具或者入侵检测系统，匹配已有知识库，自动检测规则，得出安全风险报告。此类方法不需要人为过多干预，选定扫描对象即可，评估结果集合各专业工具的优势，但评估过于依赖工具以及相关知识库的完善，构建的知识库只考虑了已知的威胁信息，不能匹配未知风险，评估只是针对系统局部，忽略了整体性。基于知识推理的评估方法引入了专家经验，将所要评估的目标以既定形式描述，如问卷，按照专家建立的规则库、风险库进行评估，产生评估报告，指出系统的风险指数。基于资产价值的评估方法是对风险行为造成的资产损失进行评估的过程，包括资产的固有价值、替换所需的代价、时间成本等，不考虑系统中的其他情况，以资产损失反映网络安全风险状况，该方法常用于企业内部的自我评估。基于模型的风险评估能够考虑网络的综合情况，科学的对系统状态和行为进行抽象和建模，为网络安全风险评估提供可靠依据，其中结构化和可重用的模型方便不同研究人员的改进，因此在理论研究领域最为常见。

2 入侵检测系统

入侵检测系统守护着网络的安全，每天都产生大量的日志.在网络安全领域中，这些日志信息能够有效的识别网络的安全状态，可以在不损害主机和网络安全的情况下检测网络用户的恶意，因此它们是接下来进行评估的主要依据.IDS的本质是一个分类器，用于标记用户的正常和异常行为，因此也存在着误报率和漏报率.由于IDS生成的告警日志关注的不仅是行为是否异常，更是具体到详细的攻击类别，若不解决漏报率、误报率较高的问题，就会影响告警日志的准确性，从而影响安全评估的结果.研究表明，改进特征选择方法或分类算法都能有效的降低IDS的误报率和漏报率.为防止较高的漏报率和误报率带来的评估准确性问题，提出了一种结合最大相关最小冗余方法（mRMR）和信息增益的特征选择方法来提高其检测率.

3 攻击图生成主要有两个要点：

a）构建合适的网络拓扑模型，指网络节点可达性信息，节点配置以及脆弱性信息；b）结合漏洞库生成脆弱性转移关系，网络攻击发生的原因是节点存在漏洞，因此漏洞利用的条件以及造成的后果便是攻击模板。网络度量相关信息的收集必不可少，网络攻防是在信息及能力不对称条件下，攻防双方的非合作博弈。网络系统安全量化分析分为三个阶段，数据融合、数据理解和安全度量。参考层次分析法，采取从上至下，先局部后整体的方法，将实际网络系统按规模和层次关系，分为系统，主机，服务三层。因此网络拓扑图的构建，应该先收集主机的配置与服务作为节点信息，并收集主机间的连接关系，构建整个系统的图模型。通过网络拓扑图模型构建攻击图，需要定义合适的变量。早期的模型有些引入过多的变量，导致模型过于复杂；而有些模型的参数过于简单，又不能表现一些复杂的网络攻击行为。建模的过程，是对目标网络和攻击者的抽象描述。在网络数据的采集方面，目前已经有了较为完善的方法和成熟的工具，在已知的漏洞方面，网络管理员需要比攻击者更了解网络系统脆弱性。

4 攻击模板

防信息不对称，网络防御方能得到网络系统的信息，预测攻击可能的发生点，对于攻击者的能力无从得知。攻击者能通过扫描，监听收集等方式获得目标网络的信息，对于网络内部情况很难获取，大部分只能是逐步的渗透测试，不断发现网络结构。其中前提集（Procondition）是一个状态，表示攻击发生必要的系统环境，如果结果为真，则表示当前安全态势下，攻击可以发生，反之则不能发生。后果集（Postcondition）为一组状态改变的集合，表示该类攻击发生后，状态可能发生的改变。例如，主机存在文件上传漏洞，并且攻击者可以远程连接到主机，则主机可能遭到攻击者上传木马，节点状态改变。

5 系统验证

现阶段我国所采用的网络系统主要有Linux、Windows、Unix等国产的一些麒麟系统。不同的网络系统有着不同的特点，因此在对这些网络系统的安全风险进行评估时，也要采用不同功能的网络评估技术。网络评估技术的功能是可支持在不同网络平台中进行风险评估，防止因平台不同而导致的网络故障。不过，由于网络风险评估技术存在一定的技术风险，这些技术风险无法被有效排除，因此通过攻击图来对网络系统的安全风险进行评估，能够大大提高网络系统安全风险的评估性能，实现对网络安全风险的跨平台评估，进而从根本上提高网络系统的安全性能，保障网络信息的安全。

结束语

总之，通过对网络系统进行安全风险评估，可有效实时地应对网络系统在应用过程中出现的各种网络安全问题，从而有效避免攻击者利用网络系统漏洞来实施网络攻击，大大提高网络系统的安全性，从而为我国绿色网络安全环境的营造做出重要贡献。

参考文献

[1]李涛，张驰.基于信息安全等保标准的网络安全风险模型研究[J].信息网络安全，2016，（9）：177-183.

[2]胡瑞敏，吕海涛，陈军.基于风险熵和Neyman-Pearson准则的安防网络风险评估研究[J].自动化学报，2014，（12）：2737-2746.