如何做好融媒体中心网络安全防护

董香云
梁山县融媒体中心，山东 济宁 272600

[摘要]由于互联网正在企业工作中扮演日益关键的角色，因此网络安全的重要性也越来越凸显。网络安全怎样进行维护、安全威胁怎样处理、人们在网络空间中应当怎样进行已就是新形势下存在的突出问题。本章重点总结当前互联网安全遇到的最新威胁，给出了相应措施与建议。
[关键词]安全；网络；病毒；威胁
DOI：10.33142/sca.v5i2.6172 中图分类号：TP393.08 文献标识码：A

How to Protect the Network Security of Financial Media Center

DONG Xiangyun
Liangshan County Financial Media Center, Ji'ning, Shandong, 272600, China

Abstract: As the Internet is playing an increasingly key role in the work of enterprises, the importance of network security is becoming more and more prominent. How to maintain network security, how to deal with security threats, and how people should do it in cyberspace have become prominent problems under the new situation. This chapter focuses on summarizing the latest threats to Internet security, and gives corresponding measures and suggestions.
Keywords: safety; network; virus threaten

引言

网络等新兴科技给传媒产业开启了一个智能化的大门，新旧传媒不断深入交流。网络等新兴科技对融传媒建设中来说是把双刃剑。在未来，融媒建设中的网络安全系统如果出现了问题，必定会给融媒业务造成毁灭性的冲击。所以，未来在融媒安全工程当中，应该从以下这样的一些方面入手。

1 网络信息安全面临的新威胁

1.1 中国网络空间的思想文化主权遭到了严重侵害

经过多次无辜栽赃、任意指控之后，美方针对中方的抹黑骤然提升。在二零一三年，美国政府的另一个主要网络安全企业曼迪昂特集团在一篇报道中声称，由于近年美国所发生的互联网"黑客攻击"多与中国军方相关，而西方各国新闻媒体迅速将这一事情扩大为全球舆情，中国国防部被迫出来辟谣。事实上，在对于我国实行互联网"黑客攻击"的时候，美国政府却在对我国实行着远超互联网限制的战略"黑客攻击"。由美方所制造的以苹果公司、微软、谷歌等为代表的高级信息技术产业，已经控制了整个全球经济食物链的最顶层，并且利用其高信息技术产业自身携带着破解对方军事防御系统的互联网核心技术。这种贼喊捉贼式的黑客指控，乃为掩饰其实质性的互联网策略安排，为肆意侵害中华民族思想文化主权营造舆情支持。

1.2 服务器成为重点攻击目标

数字化的网络时代，在线业务、网络设备以及数据传输的信息量都在急剧增加。在对客户端防护更加严格的基础上，服务器也被列为了重要进攻目标。在二零一三年初，中国国内外几个重大门户网站均爆出了被骇客拖库的消息，骇客在入侵了网络服务器、盗取用户数据库以后，又使用了其所掌握的巨量账号密码在网上银行等重要平台上试探盗号，也正是所谓的前拖库、后撞号，间接造成几个有名的支付平台和微博门户网站先后遭遇了大面积撞号威胁，大批客户的账号密码也瞬间被曝光了起来，此前仅在局部区域流传的巨量数据也一夜之间曝光在了公众眼中。

1.3 电脑病毒制造者们针对智能手机的进攻将会越来越严重

高性能智能手机市场份额的快速增长，以及智慧型手机的恶意软件种类逐渐呈现多样性，都导致了手机信息安全威胁的出现。而目前，使用塞班操作系统的手机市场正快速地被 Android 操作系统所替代，而国内的 Android 市场管理也比较松散。高性能智能手机在移动网络上的应用体验与 PC 又没有根本区别，因此基于 PC 网络的袭击者不断地向电脑平台迁移，由最开始的暗扣话费、购买服务、浪费流量，逐渐演变到盗取隐私信息和云端操控电脑。至二零一二年底，数以千万计的智能手机被曝植入了 CIQ 电脑间谍，一时引起了世界关注。

1.4 最危险的攻击来自企业内部

内部攻击可能是最具破坏性。由于特权用户能够访问

大量数据，但大部分公司都还不具有监视这些数据的力量和设施，且来自内部的威胁也往往是动态的，特征也在持续改变着。因此正如防范恶意软件那样，防御者们需要及时进行内部的控制措施。

2 融媒体中心网络安全防护对策与措施

2.1 高度重视发展和保护网络空间的思想文化主权

首先，中国从政治思想意识中要把信息安全问题提高到国家的战略高度。中国应该要像强调国土海域主权问题那样，高度重视中国互联网空间的政治思想文化权利。认真学习借鉴世界其他民族的成功经验做法，尽快建立中国互联网领域成体性的法规，以及对网络战的攻防策略。第二，大力发展中国信息产业，以尽快脱离对欧美的科技依赖性。现在，全球网络信息流量三分之二以上来源于美国，第二位的日本占百分之七，而我国信息输出流量却只有百分之零点零五。这一方面表明了美国的信息网络霸权何等强势，但同时也突出了我国在这一领域的优越性。因此中国应该尽快改革高低科技发展模式，及早地把资本、人才等转入新兴的战略支柱产业上来。其三，以爱国教育为旗帜，以民族危亡为警策，防范境外非政府机构的渗入，有效控制了外资进入中国国内政治资讯型网络，并从思想文化领域中夺取了网上舆情的主导权。

2.2 融媒体时代下网络安全体系构建的总体规划

2.2.1 网络区域的划分

在这个网络技术越来越发达的今天，一种高效、完善的安全系统将是融媒体技术发展的重要基础。首先，安全系统的核心组成部分是以防火墙。防火墙将整个的互联网区域分割为二个部分：内网和外网。它具备了很好的安全保障功能，在网中，系统能够针对不同的服务需求，从数据库中快速找到相匹配的信息内容，以便更有效地为用户，企业提供高质量的信息服务。另外网也是和应用密切相关的一个平台。根据工作的流程，包括了三部分：连接应用与网络的连接区域、信息安全共享平台、安全信息区域。在不同地域的分工，使得安全系统的建设工作更为完整。

2.2.2 网络安全设备的实现

首先，侵入防御体系的首要条件。针对一系列的安全问题，侵入防御体系必须能够正确、快速地作出反应，加以有效抵御。并能够准确检查出问题的所在区域，给整个网络防御体系划定了不同的等级范围。第二，防火墙体系。在整个互联网范围内，防火墙都是防御体系的核心。防火墙将整个互联网范围分割为内、外部二层范围。由于防火墙具备了非常好的安全防护功能，因此任何非法侵入都必须通过防火墙。所以，防火墙必须能够阻止网络上的一些非法侵入（病毒，非授权访问）或者渗入互联网内。第三，安全监测体系。面临海量的信息数量，以及错综复杂的互联网区域，为了达到互联网领域的安全化，必须具备敏锐的检测机制，针对网络上发生的威胁，迅速、精准地定位威胁根源。从源头解决。第四，网络管理组织的运转。庞大完善的网络安全体系离不开背后的管理人员的运转。根据网络安全中的各种问题，形成了处理各种问题的管理工作组。所有工作组各司其职而又彼此联系，共同为在网络安全下，融媒体的发展创造了一个高效的管理平台。

2.3 对融媒体建设下网络安全防护的未来期望

2.3.1 安全体系智能化

在构建国家安全系统同时，还要建立具备高度认知、学习、推理、预测和策略等能力的智能防范体系，在这种新一代人工智能科技越来越完善的大趋势下，人工智能技术也不失为一种很好的选项。首先，当人工智能技术在面临如此海量的消息时，机器的信息处理反应速度和准确率远大于一般人。然后，人工智能已经熟悉所有机械、装置的使用规则以及所有复杂的控制系统运行。可以解决某些维护技术人员无法解决的紧急事件。而且智能的大脑使他们具有超常的记忆力。

2.3.2 身份认证的专业化

由于媒体的传输工具多元化后，个人信息泄漏的危险性将相应提高。在网络安全建设中，人们在具备能够抵御互联网上非法入侵和消除互联网病毒能力以后，就要将注意力放到所欠缺的，身份验证专业化方面。在这种生物识别技术日益完善的新时代，身份验证技术已由传统的文字密码，逐步转化为：指纹鉴别、人脸鉴别、等全新的生物识别技术手段。这将大大提高身份验证的准确度。

2.3.3 云端防护

本地化的安全系统，虽然价格更加经济但稳定性并不好。在导入了云端防护系统之后，信息可以通过云端系统的大数据分析和人工智能计算，从而可以更好地预防网络攻击。云端防护系统能够非常方便地提高安全等级。并且当有需要时会启动服务，业务完成后马上暂停工作。云端防御在既快捷又节省了网络资源的同时，为使用者提供很大的方便。由于网络等新兴信息技术的日益发达以及越来越深入的使用，为融媒体的发展建设提供非常大方便，同时也在网络安全建设领域带来了更高的需求。

3 融媒体平台信息安全工程的重要内容

3.1 物理安全、网络安全

融媒体平台的物理环境安全性工程建设是信息安全系统构建的基本工作，其安防工程主要涉及许多方面，因此应该大力加强其环境安全设计和规范，以保证网络安全。工程主要侧重于机械式的选择、温湿度管理、准入、防水防火防震防盗防静电、视频监测等；而物理安全方面的工程则应该严格地按照国家法律及技术标准完成。环境安全主要包括的方面，包括接口安全、环境安全范围的规划、对网络资源的使用管理、网络系统路由体系的安全性、对远程连接的安全性、网络拓扑安全性、边界保护、对网络基础设施的防病毒、密码安全性攻击测试等。为了做好对这些风险的规避工作，可合理地对安全区域加以分类、加强身份验证，保护安全边界，设置防火墙、防病毒网关、安全审计信息系统、

攻击侦测管理、攻击防范系统、DDOS 攻击防范系统等。

3.2 数据安全、虚拟化安全

数据安全，即加强用户的账号管理、认证管理、权限管控和安全性审计。安全性侧重于对平台内的原始数据、系统配置信息、媒体内容和数据库文件等对这些数据信息加以防护，以防止其损毁、流失以及被盗用，具体可以使用数据加密技术、数据隔离技术等手段进行。由于云计算技术的基石是虚拟性技术，而由此产生的安全性问题也比较多，所以应该重视这方面的安全保护工作，并通过对虚拟机安全隔离、安全监控、安全防护和监测等技术增强其稳定性。

3.3 应用安全、系统安全

应用安全指基于应用的认证管理、应用账户管理、权限管控，以及安全性审计四大方面。系统安全研究主要侧重于服务器、客户端等方面的相应设备，以及操作系统、数据库等层面的安全保护[2]。

3.4 内容安全、通信安全

内容安全即防止违规信息内容的传输；数据通信安全性就是需要保证数据的安全性，具体实施上可采用特殊的音频文件格式、协议或校验码技术等以保证数据通信安全性。

4 融媒体平台信息安全建设的重点技术

4.1 访问控制

融媒体网络平台也为各级用户统一注册系统创造了机会，在这种统一注册形式下登录的系统将不需要对多个地址、登录名和密码等作出记录。云计算技术应用中联合验证技术的使用将可以极大保证信息访问的安全性，通过这种先进技术手段，当应用还在注册时，安全性凭证接着产生，使用者就可以完成对信息资料的取回工作。在具体使用时，也将结合应用中自主访问控制模块，与基于角色的访问控制模块共同管理，以尽可能的打造一种融媒体平台安全环境。

4.2 安全风险评估

安全风险评价也是融媒体平台上安全防护系统的主要部分，通过这一防范举措的开展，可以科学分析各类安全威胁、安全防范举措中的薄弱环节等，从而可达到对各种安全问题的早期发现，从而适时采取相应的防范举措加以整治。具体来说，就可以通过对各类入侵监测软件如入侵型防范体系、网络和主机型监测体系等开展科学评价；使用专业的杀毒软件，实现木马预防；使用基于云计算的杀毒软件，实现对病毒的高效防护；利用漏洞的扫描技术，对出现的漏洞加以识别，并利用补丁管理软件对漏洞加以修补。

4.3 安全审计与监控

安全审核和实时监测是融媒体网络平台安全保护的重点环节，其中审计将重点根据重要应用的情况、信息系统指令的正常使用、整个控制系统的非正常运行、相应设备的变化情况等方面进行研究，对网络平台遭遇到的风险情况作出预警，并制定有针对性的保护举措进行阻断措施。要注重建立良好的审核记录，并长期进行保护。另外还要形成全面的综合日志审核体系，把全部审计信息汇总到综合日志审核中。对上报的业务接口信息应当统一，以保证系统管理人员实时动态掌握业务的工作状况，并完成对系统隐患的有效排除与处理。

4.4 安全灾备、加密技术及高可用性技术

为了防止和降低自然灾害所带来的安全风险，政府应当利用安全灾备技术实现重要的数据处理系统、信息服务体系、技术网络系统等灾后设备可以重新修复。利用加密技术可实现对各种密钥的有效防护，并能对关键的数据信息、媒体信息内容等加以保存，以防止其遭到非法修改和损坏。此外，为保证金融媒体平台业务的持续性发展，可借助高可用性技术，这个技术可以利用在多个主机上工作的冗余节点以及服务质量实现相互追溯，当其间一个核心部分发生问题后，其余核心部分就能接收其业务内容，并且对其还能够提供负载平衡咨询服务。

5 融媒体平台在各个业务阶段的安全保护重点

IaaS 层，应该侧重于对物理数据安全、网络安全、内存安全性、虚拟化安全性和应用接口安全性的保护，对公共设施应该形成全面的防护系统，对业务提供商也应进行基本安全保护。在 PaaS 层，应利用安全审计技术、访问管理等信息技术保证安全；提高软硬件系统的工作稳定性；对应用程序接口应该统一，涉及到一些关键的操作时应该进行验证和审核等工作，以最大限度地确保编程接口安全性；在线软件服务层面上，各业务系统应对自身应用安全管理，并通过可用性技术、灾难修复机制等手段保证业务的连续性；利用安全审计信息技术，提高对内部安全事件的管理能力；利用访客管理信息技术，实现身份验证；采用加密技术和加密管理系统以确保数据安全，并采用安全性审核、访问控制等技术手段保障信息安全。

6 总结

融媒平台安全建设制度的健全与完善是一个系统工程，须通过不断加强研究与实施，以推动人员安全管理体系和系统运维管理机制的形成，通过科学分析当前面临的主要风险原因，制定有针对性的防御对策，并形成完整的安全管理体系与组织机构，制定具体的安全策略与管控举措，强化人员安全管理制度、系统运维管理制度，以适应融媒平台的安全工作需要。

[参考文献]

[1]孙源.融媒体建设环境下的信息安全如何保障[J].西部广播电视,2018(23):39.

[2]田春.全媒体融合平台安全体系建设[J].中国新通信,2018,20(8):150.

[3]郭伟.打造媒体融合背景下的电视台生产系统安全防护体系[J].广播电视信息,2017(4):41.

作者简介：董香云（1977.12-）女，青岛科技大学本科，计算机科学与技术，技术员现在是助级想评中级工程师专业是计算机科学与技术工作 25 年，就职于梁山县融媒体中心。