图书馆网络安全探析

文/李东林

近年来，网络的快速发展和广泛应用，使图书馆的管理水平迈上了新台阶。但是网络安全问题也愈发突出和尖锐，成为关系到现阶段图书馆的各项业务工作能否正常开展的重要问题及核心因素。如何保障图书馆网络安全运行日益成为倍受同仁们关注的一个重点问题。本文结合工作实践，就此问题展开探析。

1、网络安全的概念及图书馆网络的特点

1.1网络安全的概念

网络安全是一个系统概念，指网络系统的各个组成部分不受偶然的或恶意的原因而遭到破坏、篡改和泄露，网络系统可以正常可靠运行、网络服务持续不断，这包括了实体安全、软件安全、信息安全和运行安全等几方面。

1.2图书馆网络的特点

图书馆作为知识信息存储的场所，其网络具有信息资源的密集性、多样性、开放性、共享性等优势，它主要具有以下三个特点：

1.2.1数据容量大　图书馆网络数据容量大，一般都是由十几万、几十万、上百万种各种知识载体的文献信息的组合。其数据是图书馆整个系统的生命，一旦数据破坏或损失将难以恢复。因此，保护好馆藏各种电子数据资源和信息资源至关重要。

1.2.2访问频率高　图书馆网络提供丰富的电子资源，为学校的教学、科研、管理和对外交流发挥着重要作用，所有电子资源的访问率都是相当高的。因此，只有保证网络畅通与安全运行才能使图书馆各项业务工作的正常开展。

1.2.3网络安全意识淡薄　“重应用，轻安全”的现象普遍存在，一些图书馆甚至连专职网络管理员都没有，更谈不上配备网络安全管理员，而对网络安全防护的资金投入几乎为零，网络安全管理仍未能引起足够重视。

2网络安全问题的成因

图书馆网络安全主要包括馆藏数据安全、文献管理集成系统运行安全和运行环境的安全。网络安全问题自计算机网络开始出现在图书馆的那天起就已经存在，随着人们对网络的依赖越来越大，网络安全诸多问题日益明显，主要是由下列问题所引起。

2.1硬件方面

硬件主要包括两个方面：一是设备各部件配置是否合理，质量是否有保证；二是元器件是否有不兼容、接触不良、磨损、老化等现象。设备各部件配置不合理、不优化、不兼容、质量上存在安全隐患，损坏、老化、不能正常工作的元器件和设备应及时维修或更换，否则都可能因此而使系统出现故障，甚至使整个网络处于瘫痪症状。

2.2软件方面

图书馆许多软件都是从软件公司购买的，很多都留有后门，这些“后门”都是软件公司的设计编程人员为了自便而设置的，一般不为外人所知，一旦“后门”被洞开，所造成的后果将不堪设想。另外，网络软件不可能是百分之百的无缺陷和无漏洞的。目前国内图书馆计算机软件系统的开发者，对系统的安全性认识不够，软件设计中心防止误操作，防止非法侵入的措施不足，缺乏完善的安全保护功能。

2.3人员方面

网络系统对于大多数图书馆来说，普遍存在一个从认识、学习到掌握、熟练的过程，在此期间，各种人为的操作失误都会出现，涉及系统组成的各个部分，如系统规划、软硬件选购、技术水平、规章制度、人员管制等，这都将形成许多危害系统安全的薄弱环节。此外，用户的成分复杂，也潜藏着许多不安全因素。最不确定指是的是它发生的时间具有随机性、破坏程度无法预料。人为因素大致分为两类：

2.3.1无意行为。主要有四点：其一，专业人员缺乏。图书馆普遍缺乏专业的或经过系统培训的网络管理员和网络安全员，现有人员专业水平较低，不能及时发现已经存在的和随时可能出现的安全问题。其二，专业安全意识不强。大部分网络管理员都使用静态口令来保护系统，一旦口令遗失就意味着安全系统的全面崩溃。其三，缺乏严格的管理制度。没有制定或严格执行网络安全管理制度，容易留下管理漏洞而造成一些不必要的损失。其四，领导对网络安全重视不够，有些领导在认识上存在误区，忽视了安全保障投资。

2.3.2有意行为。主要是由职业道德不好的工作人员，道德水平低下的用户、网络黑客的恶意攻击等造成的网络系统故障。

2.4网络方面

传统的数据网络主要通过电缆和光缆来传送信息，存在诸如电磁泄露、信号泄露、监听/干扰、假冒通信和信息假冒等问题。现在图书馆开始布置的无线局域网更容易造成信息向非授权外部访问的泄漏，或成为攻击其它网络的跳板。数据的共享和传输增强了系统的脆弱性和受攻击的可能性。网络的核心设备服务器，网络的各种外围设备，如交换器、集线器、网络联线以及软件系统与布线结构都能引起不安全的原因。

2.5数据库方面

图书馆的数据库中存放着很多至关重要的各种数据信息，这些数据或信息是图书馆赖以生存的物质基础。因此，如果因为网络的安全问题而导致数据丢失或者信息被盗，必将对图书馆造成重大的损失；而且，针对数据库系统安全漏洞的攻击，还可能会殃及公共网络，那样就会造成难以预料的严重后果。

3影响网络安全的主要隐患

造成图书馆网络系统不安全的因素很多，常见的隐患主要表现在如下方面。

3.1黑客问题

黑客是指利用不正当的手段窃取计算机网络系统的口令和密码，从而进入计算机网络的人。黑客攻击早在主机/终端时代就已出现，主要手段有：窃取口令、强力闯入、窃取额外特权、植入“特洛伊木马”、植入非法命令过程或程序“蠕虫”、清理磁盘等。现代黑客从以系统攻击为主转为网络攻击为主。通过网络监听获取网上用户帐号和密码进行攻击；利用文件传递协议采用匿名用户访问进行攻击，突破防火墙等等。到目前为止，已知黑客的攻击手段多达500多种，突破口主要是利用休息日，选择薄弱环节进行攻击，给用户及社会造成重大的损失。

3.2病毒问题

图书馆网已普遍接入到互联网，为病毒的侵入开了方便之门。一旦服务器和工作站被病毒感染，就会迅速扩散至整个图书馆网络。可能造成系统损坏、数据丢失。应用程序无法使用，甚至导致网络瘫痪，造或无法估量的损失。随着因特网迅猛的发展，计算机病毒的种类急剧增加，扩散速度大大加快、而且破坏性也加大，受感染的范围也越来越广，如1998年发展的CIH病毒，能直接攻击和破坏计算机硬件系统，造成主板损坏，系统瘫痪。计算机网络病毒传播的方式有4种：从电子邮件附带的文件；从因特网、BS下载的文件；浏览Java和ActiveX网页时感染病毒；“黑客”恶意侵入计算机系统，传播病毒等。电脑系统一旦被病毒侵入，其效率会急骤下降，系统资源会遭到破坏，系统甚至很短时间内就陷入瘫痪。而病毒的清除是件很困难的工作。

3.3软、硬问题

软件一般由许多人合作以软件工程的方式编制，它包含有千百万条程序指令、变量、常量等，尽管在正式使用前往往经过一定的测试和试用，但其“缺陷”不可能完全被发现。软件设计方面的“缺陷”与错误往往会造成系统在一定条件下响应时间延长，程序非正常运行等问题。质量再好的硬件设备，难免有时也会出现故障。有些是小故障，有些是大故障，所造成的损失很难挽救。

3.4环境问题

不可预料的自然灾害：火灾、地震、水灾、尘灾、风灾、雷电等。电气故障：电源质量差、停电、静电影响、磁场影响、电压的波动幅度、机房布局不当、机房辅助设备故障等。这都是危害网络系统安全的隐患。

4网络安全的防范措施

我们应在计算机硬件、软件及运行环境等网络的各个环节上，针对图书馆网络系统内部和外部两方面的因素，从人员、技术及环境上着手，实行较为完善的、有层次的网络系统安全管理的举措。

4.1人员管理方面的安全措施

4.1.1建立完善的岗位责任制。明确各个岗位的职责、任务到人，责任到人。制定设置密码的原则，尽可能使用本馆信箱，设置登录权限，成立网络安全管理委员会等。制定各个岗位人员的行为规范的操作规范，如硬件管理人员强调设备的配套、兼容和日常维护，软件管理人员强调数据流动中的控制管理，特别是交送数据、设置参数及发放权限，备份数据等等，工作站操作人员以及用户，应根据本部门的安全规章制度，合理操作，以最少的投入达到最佳安全状态。同时，还应定期检查安全规章制度的执行情况，及时发现薄弱环节并提出改进措施。只有将安全目标层层分解到相应的岗位上，量化为具体的岗位责任，安全管理才能落到实处。

4.1.2建立技术资料与技术档案管理制度。对网络系统的硬件、软件、通信线路的说明书、技术手册、网络系统服务器、工作站的硬件、软件配置号数，系统的各种代码以及系统硬件、支持软件、应用软件的更新、升级与维护的记录应分类建档，并建立妥善的保管制度。

4.1.3加强网络安全知识的学习。加强各类专业人员对网络安全知识的学习，是保障各项安全

措施得以落实的根本保证。首先要加强对系统管理人员进行职业道德教育，不断提高他们的事业心和责任感，使他们以高度负责的精神和一流的工作，尽可能的减少或者避免安全隐患对网络运行造成的威胁。其次要利用互联网、报刊和各种学习的机会，做好图书馆网络安全和信息安全知识的宣传。领导要首先认识到，在网络环境下，图书馆网络的安全运行对整个图书馆工作的重要性，创造各种学习、培训的机会，不断提高全体图书馆工作人员的综合素质。

4.1.4建立培训制度。为了确保网络系统的安全运行，各类操作人员上岗前，应进行计算机知识及操作技能的培训，考核合格后方能上岗，并应有计划、有步骤地定期或不定期对网络各类人员进行业务知识的培训，以提高网络各类人员网络系统安全运行知识及安全操作能力。

4.1.5加强用户网络安全教育。图书馆的用户主要是学生，图书馆网络受攻击也主要来自于学生，因此，加强对学生的网络安全教育，增强学生的网络道德意识、法律意识及责任感也是解决图书馆网络安全问题最简单有效的途径。一些图书馆每到新学年，都要组织新生进行入馆教育，其中包括对图书馆每个服务窗口的使用，然而对学生的网络安全教育地几乎为零。如果能在入馆教育中加入对图书馆网络安全使用的教育，或专门组织学生进行教育，就会对图书馆网络安全管理起到很大帮助。

4.1.6制定网络系统的应急预案。为了将由意外事故引起的网络系统损害降低到最小程度，图书馆应制订应急预案，以防意外事故使网络系统遭受灾难性破坏，该应急预案应包括紧急行动方案及软、硬件系统恢复方案等。

4.2技术防范措施

4.2.1构筑多层防护体系。第一层防护——防火墙。这是当前网络信息安全防范措施最重要的手段。 随着新的网络安全问题的发生，出现了许多具有不同功能的防火墙，如病毒防火墙、电子邮件防火墙、ETP防火墙、Telet防火墙等。通常把各种防火墙置于一起使用来弥补各自的缺陷，增加网络系统安全性能。防火墙对于来自网络内部的攻击显得无能为力。据统计，60%的网络信息安全问题来自于网络内部，单靠防火墙是不行的，而需要配合其它安全措施来协同防范。第二层防护——路由交换机。购买路由交换机来做主交换同机是大中型图书馆的必然选择。充分利用三层交换机的路由功能。科学地划分VLAN。并合理地设置访问控制策略，能有效地防止内部黑客的攻击，抑制“广播风暴”的发生，形成图书馆网络安全的第二层防护。第三层防护——本机安全设置。对于本机的安全设置，需从操作系统的安全管理和安装反病毒产品两方面来考虑。重视本机安全设置，构筑起图书馆网络安全的第三层防护。第三层防线的实施能保证图书馆局域网内的每台计算机都有自己的防疫功能，减少因操作系统上的漏洞造成的网络攻击，进一步保障图书馆文献信息服务的正常运转。

4.2.2加密。加密技术是网络信息安全的主动的、开放型防范手段，按传输方式分为网络加密和存储信息加密两种。通过对网络传输的信息进行加密，使信息传输在全封闭状态下运行，传输的信息不会被第三者识别、修改、盗取和伪造，从而可保证信息的完整性和统一性，给不同等能的用户或系统操作管理人员授予大小不等的权限，还要对各个子系统的细小功能也能进行权限限制，这对系统的安全是十分必要的。

4.2.3硬件、软件的选购。要选择好计算机及其外围设备，在硬件配置中要注意高起点。主机的性能对整个系统的优劣影响很大，所以应选择产品质量好、性能稳定、可靠性高、售后服务好的品牌产品，以确保开发出的系统能正常运行。针对计算机等设备更新换代快的特点，对硬件的选择要具有一定的超前意识。系统软件是计算机网络的灵魂，直接关系互组网方式的选择及硬件设备的配置等一系列问题，系统软件包括操作系统和应用管理系统，因此考虑组网方式时还要考虑选用什么网络操作系统。软件配置尽量借鉴已有的研究成果，选择比较先进和成熟的软件产品，可以从系统功能、系统安全可靠性、先进性、网络性、软件质量、标准化程度等方面进行综合稳固衡量，选择成熟定型，系统管理严谨的自动化软件。

4.2.4备份。坚持不懈的备份，是保护系统与数据安全的基本要求。如软盘备份、磁带备份或硬盘备份，有条件的馆可采用双机热备或数据的定时备份。数据备份要有严格的规章制度，如每天进行归档备份，每周进行一次脱机备份，至少应保存两个以上最近数据库的完整备份并分存两处，以便 出现主机故障或运行中的故障后采取必要、及时的补救手段。数据的备份必须常抓不懈，以确保系统安全运行。

4.2.5检测与维护。在网络的规划阶段，应充分考虑网络设备的安全问题。根据网络拓朴结构和各个馆网络的应用功能来配备合适的服务器，选择好所需服务器的档次和图书馆网络的操作系统。同时，为了确保各个图书馆网络的安全运行，必须采用服务系统容错机制。例如：服务器双工，服务器集群、磁盘双工、磁盘镜像、RAID磁盘阵列等。此外，还要定期对图书馆网络系统运行的安全状况进行全面检查，及时进行预防性维护，及时更换性能不稳定或者超过寿命的部件和设备。

4.3环境安全防范措施

4.3.1在主机房的布线上。系统发生的故障中有50%至70%是与电缆有关的故障。将电缆的故障

定位是非常困难和耗时的，所以造成的损失也是较大的。因此，可靠的布线是系统安全的重要保证。

4.3.2创造良好的运行条件。在机房中要装自动火灾报警消防系统、干粉灭火器、不间断电源、空调等设备。将机器工作温度控制在14度到24度之间，以避免对设备的损耗；要有抽湿和加湿装置，使环境保持在一个合适的温度范围内；要有防尘和除尘措施；确保设备良好接地，防止静电对计算机的危害；在机房附近避免能产生强磁场的高压电源线通过，一个较好的环境中保证系统安全运行的因素之一。

4.3.3必要的安全措施。中心机房及各工作站点，都应建立健全电源保护、防尘、防尘、防火、防水、防漏电、防盗窃的设施和措施，并形成制度。另外，存储备份数据的磁带或磁盘等介质应放在金属柜内，以免被磁化，最好能和机房分开。

总之，图书馆网络安全是一个技术含量高复杂的系统工作，涉及到方方面面的问题。需要全面、协调地应用多种防范技术。加强制度建设和人员管理，才能达到有效保护的目的，同时，网络安全防范又是一种持续不断的工作。网络管理是需要学习最新的网络安全技术，在原有安全系统的基础上调整安全策略，添加相应的网络安全产品，给网络安全提供强有力的保障。安全工作任重道远，需要常抓不懈。没有安全，一切工作和努力都会付之东流。只要网络安全威胁存在，网络安全研究工作一刻也不能停止（作者单位：商丘师范学院图书馆）

相关链接

基于Internet的房地产网络广告研究
网络财务安全控制分析
电子商务网站盈利分析
图书馆网络安全探析
怎样建立营销性企业网站
对电算化系统管理的内部控制
网络安全的入侵检测系统及发展研究
构建图书馆电子阅览室与社会网吧的和谐发展
谈电子商务对我国国际贸易的影响与策略选择

地址：北京市朝阳区关东店甲1号106室 邮编：100020 电话/传真：（010）65015547/ 65015546

制作单位：集团经济研究网络中心