信息化条件下的图书馆计算机网络安全研究

郝　欣
长春市图书馆　吉林长春　130021

摘　要：近年来，信息技术获得跨越式发展，信息化数据管理设备开始被应用于图书馆馆藏书籍管理活动中，取得了一定成果。为有序推进图书馆信息化管理制度的建设与发展，提升管控水平，消除潜在安全隐患，技术人员必须基于实际情况，选用架构完善、安全性较高的服务器与核心程序，解决网络安全问题，抵御来自不法分子的侵害，安装可持续运作的智能化防御系统，让接入在线计算机服务器的用户验证自身身份。部分图书馆开始建设支持云端分享书籍信息的数字化服务体系，顺应了电子化、无纸化发展趋势，引领了发展潮流，为提升安全性，控制数据传播范围，避免数据被他人私自截取、转发、编辑修改，必须建立能够抵御网络攻击的计算机安全管理系统，让在线服务器能够更好地服务于大众。本文明确指出了在信息化时代维护图书馆计算机网络安全的必要性，指出了现阶段具备一定威胁性的影响因素，总结了提升计算机网络安全水平的调控措施。

关键词：信息化时代；图书馆管理；计算机网络安全；安全隐患

Research on library computer network security under the condition of informatization

Hao Xin
Changchun Library, 130021, China

Abstract: in recent years, information technology has achieved great leap forward development, and information-based data management equipment has been applied to library collection management activities, and some achievements have been made. In order to orderly promote the construction and development of the library information management system, improve the management and control level, and eliminate potential security risks, technicians must, based on the actual situation, select servers and core programs with perfect structure and high security, solve network security problems, resist the infringement from criminals, install an intelligent defense system with sustainable operation, and allow users connected to online computer servers to verify their identity. Some libraries have begun to build digital service systems that support the sharing of book information in the cloud, which conforms to the development trend of electronization and paperless, and leads the development trend. In order to improve security, control the scope of data transmission, and avoid data being intercepted, forwarded, edited and modified by others, it is necessary to establish a computer security management system that can resist network attacks, so that online servers can better serve the public. This paper clearly points out the necessity of maintaining library computer network security in the information age, points out the threatening influencing factors at this stage, and summarizes the control measures to improve the level of computer network security.

Keywords: information age; Library management; Computer network security; hidden danger

步入新时代以来，服务于社会大众的图书馆数量逐步增加，规模有所扩大，在图书馆馆藏管理、数据传输等领域开始使用网络技术，信息化建设水平不断提升，信息化环境改变了图书馆的经营方式，资料分享渠道增加，部分内部重要信息容易因管理不善而泄露或丢失，影响图书馆整体社会形象，馆内服务系统容易因受到网络攻击、内部数据文件感染病毒而直接瘫痪。为保护读者信息，提升安全管理水平，应当放弃传统经营方式，搭建自动化数据转化器与多个安全认证节点，重新制定防火墙黑名单与信号认证标准，保证图书馆线上服务系

统能够稳定运作。

一、信息化时代维护图书馆计算机网络安全的必要性研究

互联网技术的快速发展改变了多个行业的生产经营方式，对我国图书馆管理活动产生了影响。信息时代计算机系统是不可或缺的办公工具，为更好地服务于群众，提升图书馆馆藏信息资料的传播效率，各部门开始汇聚资源建立在线图书借阅系统与数字化服务体系，间接扩大了读者群体规模，强化了图书馆对社会文化的影响力，通过使用高度发达的信息化技术传播信息，可向更多用户传输图书资源与重要出版业信息。在信息化条件下建立的图书馆管理模式具备便捷性、新颖性，可为读者提供高质量服务，然而存在较大安全漏洞，网络服务系统具备脆弱性，部分用于在线服务的主机和本地总服务器建立了连接，管理员账号密码设置方式不严谨，容易出现盗号、非法连接接入系统等问题，导致图书馆内部信息流失或服务器停止运作。为提升技术资源利用效率，改善现阶段图书馆经营状况，技术人员应当酌情处理计算机网络安全问题，采取有效措施，备份图书馆中的重要信息，如档案登记、图书版权记录、读者个人信息等资料，安装本地数据处理器与存储装置，重新制定防火墙安全防护策略，避免社会上非法分子登入系统并私自修改信息[1]。

二、影响图书馆计算机网络安全的环境因素分析

（一）计算机病毒感染系统或服务器

网络病毒具备传播速度快、难以完全根治、隐蔽性等特性，是一种人为制造并投放的特殊计算机程序，其运作方式、感染渠道在不同种类之间有着较大差异，可在短时间内进行自我复制并感染其他计算机，通过磁盘、本地服务器、信息传输信道等途径快速传播。安全管理人员可通过更新网络病毒黑名单、重新制定计算机安全策略的方式，强化网络安全管理力度，发现并杀灭寄存在系统文件或数据库中的病毒。由于多数网络病毒从传播到感染计算机、劫持账户所用的时间较短，因此安全、快速处理病毒的窗口期不长，容易因管理人员采取错误处理方法而影响计算机正常运作。现阶段多数图书馆不重视计算机安全管理工作，未能在病毒检测、查杀等领域投入大量资金与人力，导致可用技术资源不足，计算机内置服务系统更新频率较低，未能及时打上安全补丁。新出现的计算机病毒具备传播速度快、隐蔽性强等特性，可记录用户密码并搜集本地数据库中的资料，占用系统资源，使得图书馆服务器运行速度下降，网络处于瘫痪状态，大量重要安全数据被破坏[2]。

（二）黑客网络攻击

社会上个别不法分子为谋求经济利益，使用技术工具侵入图书馆或其他公共服务设施的服务器，盗取大量数据与内部资料。此类不法活动严重影响了图书馆的正常运作，损害了图书馆社会形象，黑客网络攻击的防御难度较高，必须消耗大量社会资源与技术资源。黑客攻击主要来源于能力较强、水平较高的计算机专家与相关行业从业者，可在短时间内发现图书馆服务系统中的漏洞并破解管理员账号，获取系统最高管理权限并找到重要资料，将加密数据进行解密处理，导致图书馆内部机密信息被窃取并流入社会，系统安全漏洞较多，无法及时修复，容易被黑客发现并加以利用。为建立成熟的计算机网络安全管理系统，防范黑客攻击，必须加密数据库资源，重构网络服务系统，设置好各版块、各层面的安全防护协议，提升信息数据安全性，填补潜在安全漏洞[3]。

（三）服务系统管理不善，可用资源不足

在技术层面，图书馆内置网络服务系统未能及时更新，潜在安全漏洞未能及时发现，计算机服务系统的更新速度较快，正版系统采购价格较高，图书馆可用资金不足，新系统无法被一线工作人员合理利用，其运作效率较低。图书馆现有软件系统具备落后性、不完整性，信息处理效率不高，缺乏专业性安全防护功能，无法自动识别未能验证的远程调试信号与用户命令，安全性不高。部分工作人员错误地在计算机中设置了虚拟账户，允许远程控制，系统管理策略缺乏合理性，容易出现安全隐患。参与图书馆管理工作的职工可能做出错误行为，访问钓鱼网站，点击未经安全验证的错误超链接，使得不法分子有机会入侵图书馆内部服务系统。新时代图书馆逐步走向信息化、数字化发展道路，技术水平逐步提升，管理人员开始引入先进计算机设备，建立本地数据库与服务系统，然而整体上用于计算机系统更新与设备采购的资金较少，一线工作人员物质待遇不高，未能制定配套激励措施，职工管理效能较低，缺乏熟悉国内网络环境、掌握高层次网络安全技术的综合性人才。

三、提升计算机网络安全管理水平、利用信息化资源的措施

（一）建立完善安全管理体系

为提升计算机网络安全性，抵御来自不法分子的网络攻击，图书馆管理人员必须集中可用技术资源搭建多层次安全防护体系，明确管理主题与核心控制目标，在

技术层面更新计算机系统内在防御机制，使之具备自动查杀病毒、进行不间断实时监控、智能加密重要信息与数据的能力。首先，技术人员必须强化信号接入控制力度，建立在线服务系统访问审批机制，服务系统必须允许网络用户以个人账户身份登入网站并获取信息，共享网络资源，然而由远程交换系统发送的访问信号可能是由虚拟主机伪装传送的，具备难以控制的潜在安全风险，因此必须建立强制性的审批机制，让用户自行提交验证口令，输入多道验证码，使之接受默认的账户资质核查，一旦用户提交的认证信息与本地服务器中数据不符，则可拒绝此类用户登入网站访问资源。通过建立这一防护机制，可提升图书馆在线服务系统的安全性，使之获得稳定运行[4]。其次，技术人员还可控制访问账户的个人权限，赋予不同类型用户账户一定权限，如编辑数据、修改或复制资料等，部分内部文件可进行加密处理，拒绝权限不足、级别较低的用户访问并编辑，合理分配在线网络资源。通过资格认证的用户可访问指定目录的文件与数字化资料，不可编辑、修改馆藏数字化文献或档案，仅有管理员才能修改文件，通过将享有不同权限的多个账户混合使用，可提升管理水平，有效完成数据处理、馆藏资源借阅等工作，提升对服务器与在线网站的控制力。

防火墙是图书馆计算机网络安全系统的重要组成部分，可发挥隔离非法信号、控制用户活动的特殊作用，去除容易影响系统安全性与稳定性的未知信息，对输入、输出的信息进行审核，一旦发现黑名单中的账户或特殊类型文件，则可进行隔离处理或完全删除，安全性较低、未经认证的文件难以通过防火墙进行传输。技术人员可选择在路由器或本地数据存储设备中安全防火墙，检测访问服务系统的用户所做出的各种活动，精确判定隐蔽地址与用户IP，搜集相关数据，可对整个图书馆本地服务系统施加全面保护。管理者还可在计算机系统中安装代理服务器，严格控制不法访问，定期验证用户的安全证书。

（二）采取有效病毒查杀策略，做好数据保护

大多数网络病毒通过物理层面的介质或网络数据流传播，为及时杀灭系统中的病毒，必须采取有效防护措施，在计算机系统中安装国产杀毒软件，接入支持在线文件检测与数据审核的病毒查杀服务器，消除服务器文件中沾染的病毒。技术人员还可在使用未经安全验证的网络文件时，将其放入带有隔离作用的沙箱中，借助计算机操作系统内置安全防护功能，对病毒进行清理，每隔三到五天，使用电脑管家、智能安全助手等软件，扫描本地服务器中存储的各类文件，找出未能在文件目录中登记、未能携带安全证书的特殊文件并加以甄别，有效抵御网络病毒。通过在系统不同层级的接口处建立防毒墙与硬件隔离层，从而将图书馆内部与外部之间的信息通道进行隔离。数字信息在传输到局域网内部前，先在隔离层中进行解包，验证其中数据是否符合安全证书上的内容，并将其打散并重新组合，形成内容一致的完整信息，并对其进行扫毒，在清除完毕后再发送至系统的核心层。此类层级化病毒防御体系可最大限度提升网络安全性，避免一次性处理过多数据影响系统发挥正常服务功能，缩短带病毒文件的检索审核时间。管理人员必须强化数据保护力度，定期备份重要数据与安全信息，建立并及时更新白名单与系统防护黑名单，建立数据容量较大的本地信息存储器，重新编订数字化文件目录，基于日常生成数据量的多少调整本地存储器中的信息容量，将容易丢失的数字化文献信息存储在软盘或移动硬盘中，将体积较大、完整性较高的大文件存储到云端服务器中，以此提升数据存储安全性，让图书馆中的数字化资源得到合理运用[5]。

（三）做好人员培育工作，建立全新管理机制

为避免因员工错误行为导致潜在风险转变为安全漏洞，管理人员应当主动建立标准化纪律管控体系，定期组织开展人员职业素养培训活动，主动面向社会各界引进素质较高、能力较强的优秀技术人才，保证一线职工熟悉信息时代网络科技设备操作方式，使之掌握基础性安全防护技能。图书馆职工必须牢记个人账户密码，定期更换远程登入方式，修改组策略与防火墙黑名单，搜集可用的安全防护知识，限制一般职工账户基本权限，尽可能保护数据安全。职工必须树立安全防护意识，明确个人岗位基本职责，定期按照安全防护要求，更新计算机操作系统，为系统打上重要的安全防护补丁，抵御黑客攻击。管理人员必须优化系统配置，采用各不相同的技术参数，制定细化配置方案，提升重要主机服务器的安全管理级别，设置长度超过十二位的账户密码，建立配套账户认证机制。在有重大的系统更改时，应该操控内置防护系统的备用机，进行文件内容测试与安全检验，评估系统能否正常运作，在检测完成后再对主控制机进行操作；另外还应该备份系统，这样一旦发生错误还可以进行挽救，控制安全问题带来的负面影响。技术人员还可在图书馆多个计算机操作系统中安装系统还原软件，在基本参数与数据处理标准配置完毕后，自动开

启系统文件备份功能，用户在修改计算机系统的数据后，可根据自身要求进行恢复，这一软件可强化计算机系统抵御网络攻击的能力。

四、结术语

随着现代科技的发展，各地区图书馆开始建立在线自助服务系统，允许读者在线借阅电子书或预定其他服务，为弥补潜在安全漏洞，降低网络攻击成功率，必须把握影响计算机网络安全的主要因素，做好设备维护记录与信息整理等各项基本工作，提升管理人员对计算机网络安全的认知水平，消除导致安全事故发生的管理因素。管理人员必须主动建立多元化协管制度，规范在线图书馆管理流程，针对违规行为进行处罚，合理利用技术资源，将服务系统核心层与指令层隔离开来，让系统管理员做出标准化操作，完善配套安全管理制度，在用于传输数据的远程交换机与服务主机中安装加密系统，引入先进加密算法，提升网络系统中数据的破解难度，避免传输信息被截获并破解。

参考文献：

[1]魏政花.浅析大数据时代的计算机网络安全及防范措施[J].网络安全技术与应用，2022（06）：158-160.

[2]李洪亮.基于大数据的计算机网络安全防范对策[J].网络安全技术与应用，2022（06）：161-163.

[3]李璐，刘小宇.计算机网络安全管理技术在医院中的应用[J].科技与创新，2022（11）：168-170+177.

[4]陈登，张建敏.虚拟专用网络技术在计算机网络安全中的运用[J].信息系统工程，2022（05）：48-51.

[5]马艳平.计算机网络安全风险与控制措施应用[J].数字技术与应用，2022，40（04）：226-228.