

数字图书馆计算机网络安全防护技术

龚晓林

摘要: 随着时代发展,信息技术手段越发先进,对很多行业产生深远影响,融入生产生活方方面面。将计算机技术引入图书馆工作管理中可谓顺势而为,既能够提高图书馆书籍借阅与阅读的管理效率,又能够扩展图书馆业务范围边界。这就对图书馆工作人员提出更高要求,如何才能做好图书馆网络防护工作,避免出现安全隐患威胁图书馆数字信息安全,就成为图书馆工作人员的重中之重。本文旨在研究数字图书馆计算机网络安全防护技术,以期数字图书馆发展提供借鉴经验。

关键词: 数字图书馆; 计算机网络; 安全防护技术

Digital library computer network security protection technology

Xiao-lin gong

Abstract: With the development of The Times, information technology means more and more advanced, has a profound impact on many industries, into all aspects of production and life. Introducing computer technology into the management of library work can be said to follow the trend, not only can improve the management efficiency of library books borrowing and reading, but also can expand the boundary of the scope of library business. This puts forward higher requirements for the library staff. How to do a good job of library network protection and avoid the occurrence of security risks threatening the digital information security of the library has become the top priority of the library staff. The purpose of this paper is to study the computer network security technology of digital library, in order to provide reference experience for the development of digital library.

Key words: Digital library; Computer network; Safety protection technology

引言

计算机信息技术已经成为生产生活中不可或缺的一部分,以其非常庞大的信息资料库为人们带来极大便利,依托此种便利性,将计算机网络信息技术引入图书馆管理工作,打造数字图书馆也成为各高校当下管理图书馆的一种手段。将图书馆带入信息化管理体系中,可以极大降低图书馆管理成本,利用网络共享性打破时间和地点的桎梏,为学生学习生活提供支持。因此要注重数字图书馆网络安全防护工作,避免为不法分子带来可趁之机。

一、数字图书馆发展现状

数字图书馆是网络技术发展下的产物,具有体积小、储量大的特点,可以利用网络便利性更加快速实现信息交互,提高数字图书馆整体工作效率,在具体发展情况中有以下几点状况:第一,数字图书馆方便快捷。数字图书馆望文生义就是将数量庞大,资料繁杂的实体书籍资料进行信息化处理,最大限度提高图书馆工作效率。随着信息技术手段逐步完善,数字图书馆的便捷性也越发凸显,一方面,对于高校学者、教授来说,数字图书馆的出现使得其免于往返于图书馆和实验室,资料查询依靠网络就能实现,极大程度节省时间,提高工作效率,同时也能够利用数字图书馆检索特性将所研究课题的关联内容尽可能全面的查询。另一方面,数字图书馆没有实体书籍限制,同一种书籍可以进行多次借阅,加强了书籍自身共享属性,能更好满足借阅者需求,提高书籍使用效率,也正是基于此种便利性,数字图书馆越来越受到欢迎。第二,对数字图书馆研究越来越深入。数字图书馆作为互联网时代的产物,对各行各业都有着便利性和共享性,也使得数字图书馆受到各行业重视。随着5G时代到来,数字图书馆发展真正步入正轨,实现全面创新服务和全新发展机遇,以OPAC检索为基础开发出可视化参考咨询、移动学生社区等新型服务项目,让使用者更加方便。同时由于网络共享性和便利性,大部分数字图书馆经营重心已经从借阅为主的经营模式转变为以电子图书和专业数据为主的全文库服务,真正实现全文化数字服务。

二、数字图书馆计算机网络安全防护技术定义

数字图书馆计算机网络安全防护技术顾名思义就是利用一些安全防护措施和管理办法,避免图书馆内容信息化数据受到外部侵害和损毁,防止信息数据受到主观意识篡改。让信息数据能够在安全、平稳的环境下进行工作,为用户通过相应数据服务。在数字图书馆网络安全防护技术层面,主要有以下几点特点:第一,有较强保密性。保密性对于数据安全来说是重中之重,对于数字图书馆管理者而言,为用户数据保密处理是应有之义,防止数字图书馆访问地址和信息权限被窃取,是核心工作之一。能够保证所有非公开信息数据不会被他人非法获取,数字图书馆所发出的用户通知信息等也不会被随意拦截,保证图书馆管理工作能够顺利进行。第二,具有完整性。这种特点是数字图书馆保密性的延伸,在所有数字图书馆登录的个人账号与资料信息都能保持信息完整性,不会被未经授权的情况被外界不法分子获取,保证信息数据安全性与可靠性。第三,具有实用性。用户在利用数字图书馆进行信息交互时,信息数据必须通过数字图书馆主机才能进行数据外流,而主机除了管理员谁都无法拥有操作权限,这就保证主机独立性和完整性,不会被外界信息干扰,从根本上保证主机可操作性和实用性。全面避免木马病毒对数字图书馆主机的攻击,保障信息数据安全。

三、数字图书馆计算机网络安全防护存面临的问题

(一) 病毒威胁

病毒作为直接威胁计算机网络安全罪魁祸首,能够直接对计算机网络系统进行攻击,将网络数据大肆破坏,造成损失。在数字图书馆被病毒入侵后,不法分子会通过病毒大肆攻击数字图书馆内部信息数据,将用户信息进行复制后销毁,对数字图书馆产生严重威胁。网络病毒一般潜伏于硬盘文件中,会对计算机磁盘内容进行恶意篡改和随意破坏,导致计算机文件磁盘产生改变,造成私密信息泄露,最严重时会导致磁盘格式化,将其中内容全部删除,如果没有备份文件,数据信息将会永久丢失。同时病毒还会对系统运行产生影响,轻者系统运行过程中产生卡顿和跳帧,严重者直接攻击

网络连接方法,致使网络运行停止,造成损失。随着信息技术不断发展,网络病毒也在不断进化,无论是潜伏性还是破坏性都不是传统网络病毒所能比拟的。

(二) 黑客威胁

网络黑客是基于网络技术发展所诞生的群体,其具备高超的网络技术和程序能力,黑客原本只是对网络技术高超人员的统称,但随着信息技术发展,黑客群体不断扩大,其中鱼龙混杂、良莠不齐,现在已经成为利用非法手段随意入侵他人计算机的贬义词。对于黑客来说,入侵计算机的最终目的是获取精密信息数据或对计算机系统破坏。在一般情况下,黑客进行网络攻击时都会寻找计算机系统漏洞,以此来实现入侵目的,比如:拒绝客服攻击形态,此种攻击方法主要依托信息数据下载,能以最快速度将用户计算机系统造成瘫痪,无法正常运行;无法访问形态,是黑客利用系统漏洞完成入侵后,对系统文件进行破坏导致用户无法正常使用计算机。这也是数字图书馆可能受到的网络攻击方法,由于数字图书馆具有数据量大、机密信息多等特点,因此要格外注重网络安全防护,避免黑客攻击造成损失。

(三) 信息泄露

信息泄露是数字图书馆所面临的网络安全问题之一,在进行数字图书馆构建时,网路系统出现漏洞就会导致信息泄露,为用户带来不必要损失。在信息技术飞速发展的当下,数据共享已经成为网络数据交互主要方式,在进行数据共享过程中,如果无法做到全面防护就会产生信息泄露情况,从而降低数字图书馆整体信任度。同时人为因素也是导致信息泄露的主要原因之一,有些操作人员没有足够安全防护意识,在操作过程中对自身信息私密性不够重视,同时很多数字图书馆管理员网络安全意识不足,没有相关职业技能,对网络安全防护了解不深,无法有效进行信息保护与防范,使得数字图书馆信息安全受到威胁,数字图书馆正常运行也会受到阻碍。从硬件层面来看,数字图书馆网络安全与计算机设备关联性较高,如果网络交换机出现问题也会导致信息泄露情况发生,影响计算机网络安全防护措施发挥应有作用,削弱数字图书馆网络安全体系。

四、数字图书馆计算机网络安全防护方法

(一) 加强反病毒技术

病毒作为数字图书馆网络安全的头号大敌,对数字图书馆有着巨大的破坏能力和不可预测性,在遭受病毒攻击前,数字图书馆无法预测病毒种类和攻击形式,因此只能加强病毒防御,提高反病毒技术。防御病毒攻击作为数字图书馆网络安全防护体系中重要一环,应该从基础工作做起,在进行反病毒工作时,技术人员应该将市面上所存在病毒种类和攻击方法进行汇总和梳理,建立病毒数据库,以此为根基进行反病毒技术开发和安全产品研究,在网络安全防护软件选择上要注重正规性,避免使用盗版软件,以免留下漏洞为网络病毒提供可乘之机。无论购买何种防护软件,都必须对运行模式和底层逻辑进行解析,将软件运行情况与相应病毒库进行一一对照,从根本上防止网络病毒入侵。要对安全技术手段进行定期转换,从系统底层逻辑入手进行完善,保证安全技术产品防护措施到位,将病毒阻挡在系统之外。同时对数字图书馆重要资料和信息数据设定访问权限,只有利用特定账号与方法才能完成信息访问和调用,对相关高机密文件内容进行复制备份,避免出现资料丢失情况。在数字图书馆运行系统中安装病毒查杀程序,管理人员应每天对数字图书馆内部进行整体病毒查杀,将威胁消灭于无形。还应重视数字图书馆相关工作软件选取,尽量选择能够对外来入侵数据产生反应的工作软件,这样才能第一时间发展状况,将损失降至最低。

(二) 完善防火墙设计

有效利用防护墙能够实现数字图书馆网络安全防护,防护墙措施是计算机网络诞生以来就出现的防护措施,随着信息技术不断发展,防护墙技术也在不断更新换代,为网络安全防护贡献极大

量。防护墙作为保护网络安全的第一道防线,应确保防护墙运行良好,防护能力足够,首先,数字图书馆可以与网络科技公司进行合作,让其根据数字图书馆构建规律和发展计划开发特定防护墙程序,保证防护手段能够抵御病毒入侵,同时为内部网络预留访问权限接口,以此形成对外防御,对内查杀的全方位防护体系,最大限度消灭网络病毒。应完善防火墙设计,将防火墙功能进行拓展,让其结构属性囊括内部网络和外部网络,让内网和外网进行信息交互时必须通过防护墙认可才能给予访问权限,以此保证信息数据传递过程中的安全性和稳定性。在开启防火墙后,会产生一个联通内外的网关,能够将一切不安定因素都排除在外,还能随着对内部进行检验和查找。在受到外部攻击时,防火墙就会进行抵抗并发出警报,让管理台人员能够做出有效处理。但防火墙技术也不是万能技术,总会存在漏洞和反应不及时情况,这就需要管理人员定期对防护墙进行升级更新,保证防护墙技术时刻处于信息技术前沿,将先进防护理论融入防护墙技术开发中,保证防护墙能够最大限度应对各种问题,保护数字图书馆网络安全。还应与其他网络防护手段进行合作,结合相应网络防护技术才能保障防护墙发挥出最大效果,全面防护网络安全。

(三) 提高网络信息防护能力

在加强网络信息防护能力上,可以从硬件和软件两方面入手,第一,硬件方面,要注重计算机主机房物理环境防护,对场地需求、设备防护等方面要有充分考量,保证数字图书馆物理层面防护能力。在机房场地选择中要以安静为主,严格限制进入中心机房人员,禁止非相关工作人员进入中心机房。制定科学严谨的中心机房管理规定,保证中心机房安全性和稳定性。同时要注重中心机房内容温度与湿度,保证网络正常运行;加强基地电源与防火工作,在计算机房工作时,要选取不间断电源保护工具,防止电源中断或变压冲击等情况产生,同时在接地电源设计上应保证电源稳定性,为整体防护措施做出贡献,制定严格维护管理方法,对可能产生火灾地点进行详细检查,完善防火工具和防火措施,对管理人员进行相关培训。第二,软件方面,要对接硬件和软件应用,选择合适软件与硬件组成网络安全防护体系,在网站访问端口设定身份认证技术,通过授权和识别的方法加强数字图书馆前端网络安全防护,并将认知密钥进行定期更换,最大限度加大软件防护力度,同时可以对访问信息进行备份,发现问题时可以进行信息溯源追击,提高网络加密技术,避免数据传输过程中出现数据丢失情况,以此实现双重数据保护,保证数字图书馆网络数据安全。

结语

综上所述,数字图书馆以便捷性和共享性已经成为当下信息发展过程中的重要组成部分,为学术研究和数据交互提供有力支持。因此要注重数字图书馆网络安全状况,保证数字图书馆数据安全,避免遭受计算机系统攻击和网络病毒威胁,全面完善数字图书馆防护体系,加强从业人员网络安全防护意识,为数字图书馆整体发展提供推动力,保证数字图书馆良性发展。

参考文献:

- [1]陈章国.数字图书馆计算机网络安全防护技术[J].电子技术与软件工程,2020(22):241-242.
 - [2]宋亭.数字图书馆的计算机网络安全与防护[J].现代信息科技,2019,3(21):147-148.DOI:10.19850/j.cnki.2096-4706.2019.21.055.
 - [3]崔平丽.刍议数字图书馆计算机网络安全技术及其防护策略[J].企业导报,2016(12):152.DOI:10.19354/j.cnki.42-1616/f.2016.12.117.
 - [4]秦久英.数字图书馆计算机网络安全防护技术研究[J].考试周刊,2015(77):22.
- 作者简介:龚晓林,男,汉族,1975-12,贵州人,贵州医科大学,中级职称,本科学历,馆员,学士学位。