Educational and teaching research, 教育教学研究 (10)2022,4
ISSN:2705-1277(Online); 2737-4130(Print)

互联网环境下图书馆计算机网络安全防范方法

龚晓林

贵州医科大学　贵州　贵阳　550025

摘　要：规避图书馆计算机网络系统运行各类风险与安全隐患，是防范方法再设计的主要目标。管理者需在互联网环境下重新确认图书馆计算机网络安全的主要性能，明确目标实现所必须使用的核心技术，继而设计多元方法全面防范安全风险，一做到网络安全防范核心技术的动态升级与高效使用，二构建安全策略实施的长效保障机制，三建设操作性灵活的计算机网络安全预防机制。

关键词：互联网；图书馆；计算机网络；安全防范；方法

引言：

网络技术和互联网技术的高质量发展，加快整个社会的数字化和信息化速度。在高新技术获得普遍和广泛使用的新时代下，图书馆管理从传统实体场所转移到虚拟网络空间，强化信息数据管理能力、增强数据流动性的同时，衍生出诸多确定与不确定风险因素。互联网环境下，图书馆基于计算机网络系统智慧作业的过程中，需加强系统软件、应用软件、数据信息的安全管理与防范，在应对各类安全隐患和系统漏洞等方面提出新的方法。

一、互联网环境下图书馆计算机网络安全的主要特性

（一）保密性

图书馆计算机网络安全防范的意义和目的，在于保障应用系统运行的畅通性与稳定性，充分满足用户的个性化需求，如安全和高速的获取目标信息源。系统中存储的各类信息数据，需获得长久与安全的存储，禁止任何非授权者下载与使用。图书馆信息管理系统中的数据，仅是部分公开，用以满足用户获取信息资源的需求，机密文件必须通过授权才能获得，由此可见，图书馆计算机网络安全有着突出的保密性。因此，在系统运行与使用的过程中，必须对图书馆计算机网络安全防范，以网络安全核心技术为支撑，保障各类信息数据的安全存储，不能被病毒或黑客等侵袭造成数据丢失与损毁的严重后果。

（二）完整性

计算机网络安全防范方法，实际上是保障信息数据完整性的有利工具，必须要根据整个网络环境特点及系统运行安全性能及时升级，确保且在防用户篡改和盗用文件等方面发挥显著作用。信息数据的存储与共享，应依托健康和安全的网络空间，尤其在输入输出的过程中必须防控违规修改，更不能破坏信息数据的完整性与安全性。互联网环境下，图书馆管理和服务方式发生改变，可在虚拟网络平台即时传输与共享文献资料，但需利用科学和有效的安全防范方法保持计算机网络系统完整状态。从这个层面来看，互联网环境下管理图书馆，需着重信息数据的安全管理，持续和一贯的展现其完整特性。

（三）可用性

互联网环境下的图书馆管理逐渐向数字化方向发展，利用技术手段增强总系统和子系统的可用性，这也是图书馆计算机网络安全的主要特性之一。图书馆计算机网络系统在使用的整个过程中，需科学的设置使用权限，确保重要文献资料为授权用户所用，并全面和有效控制风险因素和安全隐患。而在互联网环境下推进图书馆计算机网络安全防护工作，必须注重增强系统的可用性，无论是自然因素还是人为因素，都不能常态的干扰正常使用。图书馆计算机网络系统运行的过程中，不可避免或受到病毒攻击，但绝对不能拒绝服务，更不能被非法用户远程控制与实用，必须利用有效和可操作性强的防范方法保证整个网络的可用性。

二、互联网环境下图书馆计算机网络安全防范的核心技术

（一）防火墙技术

防火墙技术在图书馆计算机网络安全防护中的应用，本质是以技术为支撑获取多元防范方法，即“防火墙”既是方法，又是互联网时代蓬勃发展催生的“新技术”，可有效的隔离网络，主要包括局域网和外网。防火强技术在使用的过程中，所表现出的功能主要体现在以下两个层面，一隔离超出既定技术规则的信息；二允许满足流通条件的信息进入信息管理系统，且允许用户间自由和安全交换与共享。目前，防火墙技术已然成为图书馆计算机网络安全防护的重要方法，更是不可或缺的核心与关键技术，在使用时需科学设计与动态优化技术规则，明确何种信息数据被隔离与放行。在对图书馆计算机网络系统进行安全管理的过程中，需用好防火墙技术，即将含有安全隐患的数据隔离墙外，保障整个系统安全与顺畅运行，并为授权用户提高优质的信息服务。防火墙技术有着突出的保护与病毒防护作用，可有效保护内部网络，为用户提供良好的使用体验。网络安全管理与维护人员，需始终在 TCP/IP 协议层展现防火墙技术的功能与作用，即在应用层上高效与安全的运行，并将其作为拦截信息的重要工具，利用这种技术和方法隔离外网有害数据流，确保图书馆计算机网络的安全性和可用性。

（二）虚拟专用网技术（VPN）

虚拟专用网技术（VPN）在图书馆计算机网络安全防范中运用的过程中，主要是依托安全的公用网络，对图书馆管理系统科学拓展，搭建可信和稳定的内网连接，用以为用户提供优质的信息服务，或是利用内部网实现远程办公及跨时空交换信息数据。对图书馆计算机网络进行安全管理的过程中，引进虚拟专用网技术（VPN）主要是为了更好的防范非授权用户入侵，可有效的控制成本是其突出的优势，相对于租电话拨号，使用 VPN 更节省费用，便于图书馆控制经营与管理成本，并为用户提供个性化和多样化的图书情报服务。同时，利用虚拟专用网技术（VPN）防范风险的过程中，展现出突出的可拓展性，如新增用户时快速更新网络配置即可，或指导对象安装专门软件，而后就可进入网络系统中读取和下载授权的信息数据。虚拟专用网技术（VPN）可实现高级加密，亦或通过验证协议控制非法访问，由此增强整个图书馆计算机网络的安全性。

（三）入侵检测技术

图书馆计算机网络系统运行，需以多种技术为支撑，以保证各个子系统协同工作，为授权用户提供想要的的信息源，但传输重

要数据时会出现非授权访问现象，即对虚拟空间存储的重要文件和数据恶意使用或损坏。为此，必须利用入侵检测技术（IDS），对恶意行为精准识别，起到防范数据盗用与丢失的作用。而无论针对内部网络用户，还是网络系统外的非法使用行为，入侵检测技术都可发挥一定的防护和防范作用，如网络系统运行的过程中出现非授权操作，IDS 就会精准与快速识别恶意使用行为，针对异常现象生成相应的报告。入侵检测技术实际上是作为安全技术进行使用，主要是依托入侵检测软件，通过与硬件科学组合构成安全性能更好的监测系统。功能和作用发挥的表现是，全程监督网络系统运行状态，并对恶意使用行为动态识别与分析，明确整个系统当下动作特点或安全隐患后，可立即报告异常行为，以此保证图书馆计算机网络系统的安全性及数据完整性。

（四）安全扫描技术

图书馆计算机网络系统有着明显的虚拟性与开放性，展现出较高的信息存储和共享能力的基础上，也会因系统漏洞不可避免的存在安全隐患。若想对图书馆计算机网络有效安全防范，就必须在系统运行全程动态监测和优化漏洞，即通过使用安全扫描技术，实现实时和精准识别安全隐患。安全扫描技术在图书馆计算机网络中的植入，有助于快速发现系统漏洞，继而提醒管理员有效防范和问题应对。否则，会受到恶意行为和网络病毒攻击，导致网络系统瘫痪，难以为用户创建可信、高效、安全的信息交换空间。而这种技术的应用，主要是利用扫描的方式检测风险因素，并快速识别与处理安全隐患，实现对图书馆管理系统的主动保护，无论是端口扫描，还是操作系统探测，亦或漏洞扫描与主机探测等方式，都可即时识别安全风险，并对系统漏洞进行及时的完善与优化。

三、互联网环境下图书馆计算机网络安全防范的多元方法

（一）网络安全防范核心技术的动态升级与高效使用

上述内容中所提及的防火墙技术、虚拟专用网技术、入侵检测技术、安全扫描技术，都是图书馆计算机网络安全防范的核心技术，更可将其作为操作性灵活的防范方法。在使用这些技术时，管理员必须具备良好的“防范于未然”意识，提前敏锐感知网络系统安全隐患，根据实际情况发挥多种核心技术的协同效应。在对图书馆计算机网络安全防范的整个过程中，必须对核心技术动态升级，保证持续具备风险识别与处理的功能与作用，继而对网络系统主动保护。当网络系统中同时出现恶意使用行为和系统漏洞问题时，就必须协同使用入侵检测技术和安全扫描技术，精准发现与快速处理系统系统漏洞，并有效打击非法入侵行为。互联网环境下，图书馆管理人员必须形成良好的互联网思维，明确虚拟和开放网络空间中运行信息管理系统的各类风险，有意识的对网络安全防范核心技术动态升个级与高效使用，无论是入侵检测技术和安全扫描技术，还是虚拟专用网技术或防火墙技术，都应根据网络安全问题协同且高效作业，从而建立稳定和安全的安全屏障，阻隔破坏系统安全状态的所用因素。

（二）构建安全策略实施的长效保障机制

互联网环境下，图书馆管理系统作业过程中有着突出的敏感性，既要设计高效可行的安全策略，还要构建策略实施的长效保障机制。即用好网络安全防范核心技术的同时，需组建专门的安全管理机构，秉承垂直管理原则部署图书馆计算机网络安全防范工作。无论是安全策略，还是支撑策略高效实施的保障机制，都应成为识别、发现、处理安全隐患的辅助工具。例如，安全管理机构，需对网络系统运行全过程进行安全保卫，并安排专人负责。同时，需设置系统稽核岗位，根据图书馆规模和安全防范工作量确岗位人员数量。此外，管理层需科学设定机构和岗位职能，将责任落实到个人，所有人员都能高效和有序的落实本职工作，自觉配合其他岗位突发事件处理。图书馆管理人员需科学设计安全管理制度、技术安全管理规范、人员安全管理制度，在制度要素和技术要素的协同作用下，创建安全、顺畅、可信、稳定、安全的网络环境，确保授权用户不受时空限制的获取目标信息源。

（三）建设操作性灵活的计算机网络安全预防机制

图书馆计算机网络安全的有效防护，必须以完善规章制度和预防机制为支撑，生成可行的安全管理制度外，需建设操作性灵活的预防机制。管理者应构建科学的硬件管理预防机制，根据图书馆计算机网络系统预期所要达到的性能，购买品质好、适配度高、可拓展性强的品牌机，为软件系统高效与安全运行提供良好的物质载体。特别是在选配服务配时，必须要根据图书馆计算机网络系统的网络配置和性能要求等，购买高于系统要求的硬件设备，且充分考虑的日后的系统升级。同时，管理人员应在防火、防水、防震、防盗等方面，均生成相应的预防机制，由此创建安全和健康的物质空间，为图书馆计算机网络系统的安全运行和风险防范提供优质的环境支持与条件支持。对应硬件安全管理预防机制，构建科学和完善的软件管理预防机制，用以支撑系统软件和应用软件安全和顺畅运行。例如，可设计智慧的图书馆计算机网络安全系统，包含网络服务系统、办公自动化系统、数字图书和文献资料管理系统、一卡通系统、网络安全管理系统等，并通过设计对应的安全管理制度和规定，确保各个子系统协同作业。利用智慧系统实现智慧化管理，在系统工作的整个过程，都能有效控制用户登录与信息获取，充分保证整个系统运行的安全性。

结语：

计算机网络安全防范方法的升级，是创建健康和可信系统运行空间的必然选择，管理者必须根据网络系统运行状态，以及用户个性化需求，对传统的工作方法进行全面创新，要利用多种手段应对诸多安全隐患。既要发挥防火墙技术和入侵检测技术等核心技术的作用，还要协同制度手段优化工作环境与系统运行空间，确保数字图书和重要文献等信息资源在虚拟网络获得安全和高效的流通，为授权用户提供个性化和差异化的信息服务与图书服务。

参考文献：

[1] 陆晟 . 互联网环境下图书馆计算机网络安全的防范与对策 [J]. 信息记录材料 ,2021,22(10):78-79.

[2] 赵建霞 . 图书馆计算机网络安全的防范对策探讨 [J]. 数字通信世界 ,2021(08):149-150.

[3] 沈铭珠 . 图书馆计算机网络安全的防范与对策 [J]. 传媒论坛 ,2020,3(02):125+127.

[4] 陶艳 . 图书馆计算机网络安全的防范对策 [J]. 电子技术与软件工程 ,2019(21):187-188.

[5] 谢辉 . 图书馆计算机网络安全的防范对策分析 [J]. 管理观察 ,2019(10):100-101.

[6] 张渊 . 图书馆计算机网络安全的防范对策 [J]. 山东工业技术 ,2018(16):226.

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。