浅谈数字图书馆的网络信息安全

胡　龙

（黑龙江省望奎县图书馆　黑龙江　望奎　152100）

［摘　要］ 信息与数字图书馆如同书籍文献与传统图书馆，是其核心与灵魂，没有了信息，数字图书馆便成为一个空壳，再无任何用处。因此，数字图书馆的信息安全问题，随着数字图书馆的诞生而诞生，随其发展而更加严峻。

［关键词］ 数字图书馆；网络信息安全；预防机制

1 目前阶段数字图书馆所面临的信息安全威胁

1.1 计算机恶意、病毒攻击

当前计算机有一个很大的威胁，那就是计算机病毒这种病毒有传染性，如果一台电脑感染了病毒，那么，和他们连接的这些计算机都会遭到病毒的感染，整体的速度非常快，甚至会导致网络崩溃。计算机的病毒就是计算机程序，这种程序具有很强的破坏性，当前网络发展迅速。这个过程中计算机病毒也成为人们需要防范的重点。

1.2 计算机系统本身存在的漏洞和计算机软件本身存在的问题而导致的攻击

如果有一个软件出现了漏洞缺陷，那么攻击者就有了攻击的机会，而且软件更新的速度很快，如果不及时的更新这些软件也会出现更多的漏洞。当前，很多用户缺乏安全意识，这也提高了网络攻击的成功率。

1.3 数字图书馆硬件设备与软件的维护与安全保障

设备老化，设备在长时间使用的过程中也会出现较多的问题。这些硬件如果出现问题，计算机系统以及相应的应用软件也会出现问题。很多备份的数据可能会受到损坏。

2 数字图书馆的数据安全以及安全预防机制

2.1 建立有效的维护策略和统一的管理机制

采取有效的维护措施，可以主动地进行防御，这样攻击来临之际，就能够提前做好准备。除此之外，也要建立安全管理制度，针对当前的管理制度进行完善。负责人要有两个同时进行，这样能够互相监督。防止内部人员因为一些错误或者是失误，导致计算机的操作系统受到影响。

2.2 建立专业的的技术人才和组织机构

计算机设备的种类是非常多的，涉及的范围也比较广，对于技术以及专业性的要求比较强，我们必须要组织专业的人员接受培训，对他们进行技能管理。这也是为了更好的保护计算机的安全性。

2.3 制定好各个环节的管理章程和内控制度

在管理工作顺利进行的过程中，我们需要规章制度的支持，这样每个人才能够根据这些规章制度的内容来执行每个环节的任务。无论是技术人员还是非内部的计算机人员，都要根据工作制度完成自己的工作，每个人的职责都十分的分明，这样能够减少违反安全行为的发生。

2.4 岗位职责分明

不同的岗位都要组织专业的人员进行管理，坚持职责分明，一些比较核心的技术要寻找责任心比较强，比较专业的技术人员进行管理。不同的账号，不同的口令要保密管理。不要出现多人管理的情况，这样数据的安全性也会受到威胁。

2.5 数据使用登记工作，坚持记录制度

记录是非常有必要的，能够给安全做出一定的补充，在记录更新数据的过程中，我们就能够通过这些记录的内容，查找想要的东西。尤其是机房必须要做好日志的更新，每个工作人员都要认真地进行工作日志的填写，进行交接的过程中需要双方共同填写，这样能够减少一些安全隐患。

2.6 数字图书馆部门之间的协调

数字图书馆的安全性会影响到整体的图书馆。图书馆作为一个比较庞大的群体，这个过程中不仅需要技术部门的支持，还需要不同部门相互协调。很多图书馆的内部工作人员缺乏专业的计算机知识，不了解什么是计算机安全。在使用的过程中，可能会随意的安装一些软件，这就可能会出现一些病毒，使得计算机受到攻击。各部门之间也应该互相监督，互相管理，在没有允许的情况下不能够擅自的安装软件。也要让他们认识到计算机安全对于图书馆的重要性。

3 安全技术预防机制在数字图书馆中的应用

3.1 磁盘阵列

磁盘阵列，就是把容量比较小，无法满足客户需要的很多个硬盘整合在一起，借助专业的设备组成一个容量比较大，稳定性比较高的组合，这样能够提高使用的速度，确保使用的安全性。把这些数据分割成不同的小块放置在不同的硬盘，这样能够快速的进行数据的读取。

3.2 数据备份

为了防止数据受到破坏，我们要采取防备措施。如果数据丢失或者是因为自然灾害，或者是人为的原因导致数据受到了破坏，我们就能够在较短的时间内恢复这些数据。我们可以采取异机或者是异地备份等多种方法。异地备份能够避免同一个地方同时发生了灾害导致数据受到了破坏，而造成数据无法恢复。当前，我们还会选择磁带机备份，这种方式能够储存较多的数据，而且十分的方便快捷。

3.3 双机容错

双机容错，是为了避免单独服务器工作的过程中出现服务终止的情况。这种方式是两台服务器共同运行，如果一台服务器出现了问题，无法工作，另一台就立刻会开始工作，弥补这些问题。一台服务机永远在工作，另一台服务机随时待命，这样就能够出现永不停机的情况了。

3.4 数据迁移

数据迁移，我们可以理解为访问比较多的数据，可以把它们单独放置在性能比较好的储备设备之中，如果一些数据访问率比较低，那么我们可以稍稍放置在储备性能比较差的设备中。

3.5 异地容灾

很多企业的数据在不断的增加，人们也认识到了数据的重要性。一旦出现了自然灾害，或者是因为人为的原因破坏了这些数据，导致数据丢失，那么一个企业的发展就会受到沉重的打击。所以，数据备份是非常重要的，我们可以利用这些备份的数据，快速的恢复丢失的数据。

3.6SAN

SAN 做为千兆速率的网络，能够进行共享和网络的交换，能够提高储备设备以及服务器的速率，在远距离的范围之内，可靠性也更强。

3.7 检测技术

为了抵御外来的入侵，我们可以采取一种比较主动的防御措施，那就是入侵检测。这种技术能够在网络以及系统中进行数据的采集，之后进行规则匹配数据的分析查询是否出现了恶意数据。如果出现了这些，就要立刻进行阻断。这些恶意数据的来源，会形成备份生成日志。

3.8 身份认证

身份认证是为了更方便确认操作人员的身份，实际上就是用户和系统之间设立的防线。当前，这种确认技术十分的常见，就像是一个住宅区的大门，只有拥有这把钥匙的人才能够打开这个门。有了身份权限，才能够进行访问，才能够获取其中的数据。当前比较安全，可行使用较多的认证系统就是和密码相关的措施，这样能够阻挡一些非法用户的进入。

4 总结

影响数字图书馆网络信息安全的因素很多，硬件和软件方面都有影响，工作人员的素质和专业技能也是很重要的影响因素，因此需要从硬件、软件以及工作人员三个方面共同努力，才能够最大限度确保数字图书馆网络信息安全，促进数字图书馆安全稳定运行。

参考文献

[1] 陈迁．网络安全防范体系及设计原理分析 [J]．信息安全与技术，2016（13）．

[2] 廖辉．网络终端安全状况评估指标体系的研究 [J]．计算机工程与设计．2014（05）．

万方数据