

计算机网络数据库的安全管理技术分析

郭 鹏 廖盛滋

江西应用技术职业学院, 中国·江西 赣州 341000

【摘 要】尽管网络技术正随着经济的发展而备受人们所关注,与此同时,由这一技术所带来的安全问题更需要人们予以高度重视。网络数据库信息随时会更新,这些信息与用户的隐私安全密切相关,一旦信息被泄露,会给用户造成很大的损失。因此,需采取有效的安全管理措施,将数据库风险降到最低。

【关键词】计算机;网络;数据库;安全管理

引言

由于人们对计算机网络的依赖程度越来越高,需严格保证用户的信息安全,为用户带来更加完善的使用体验。为了进一步完善数据库的功能,保证数据和信息安全,需采取完善的安全管理技术,促进系统正常运行,避免黑客和病毒入侵数据库。

1 计算机网络数据库安全管理特点

1.1 安全性

为了避免数据库面临较大的安全风险,需采取有效的安全管理技术,对其风险进行合理控制,保护用户隐私。制定明确的风险防范措施,采取合理的数据加密技术,结合数据管理和数据保密的要求,优化系统的性能,为用户带来更加完善的体验^[1]。

1.2 完整性

由于网络数据规模庞大,类型众多,人们对数据库的功能提出更加严格的要求。进行数据传输时,需为人们提供所需信息,保证数据的完整性和准确性。需进一步优化存储功能,拓展存储空间,保证数据的传输更加稳定迅速,方便人们随时进行沟通和交流,实现资源共享。

1.3 故障性

为了满足人们多元化需求,各大生产商研制并开发出多种类型的电子设备。为了进一步发挥出设备的功能,要优化计算机网络体系。由于网络数据日益普及,一旦网络出现故障,不仅影响用户的正常体验,还可能会导致设备出现故障。如何解决故障,则成为广大技术人员需认真思考的问题。

2 计算机网络数据库安全管理存在的不足

2.1 安全管理不到位

若安全管理不到位,或由于人为操作出现失误,会导致数据库出现安全问题,影响数据库正常运行。比如,由于用户的计算机知识不足,操作有误,或者缺乏安全意识,会导致木马和病毒趁虚而入,影响系统的安全,导致系统出现瘫痪,甚至会窃取数据库中的信息,使得用户的利益受到损害^[2]。

2.2 网络存在安全隐患

可将计算机数据库视作各类数据的“阵地”,一旦其面临威胁,会导致库内的所有数据面临极大的风险。需确保网络安全,否则就会影响数据的安全性和可靠性。由于计算机网络管理包含的内容较多,一旦某一环节遭到病毒或黑客影响,可能会产生牵一发而动全身的后果。

2.3 硬件安全缺乏保障

为了进一步满足用户需求,需将网络数据库与先进的硬件设备相结合。如果设备出现安全问题,会对数据库的运行产生不

可避免的影响,比如,数据丢失,系统崩溃等。现阶段,计算机系统中存在许多漏洞。需及时对漏洞进行修复,否则,这些漏洞将会成为黑客等不法分子入侵系统的主要渠道,对用户的指令进行更改,或者窃取用户的文件和信息,使用户的利益面临严重损害。在各类计算机软件中也会存在漏洞,需避免漏洞长期得不到修复,才能进一步提高数据的安全性和可靠性。目前,黑客入侵电脑的方式多种多样,比如,黑客会利用常用的网络工具,对用户的系统进行入侵,一旦用户疏于防范,会给黑客留下可乘之机。许多软件的程序存在的漏洞较大,一旦用户将这些程序安装在计算机系统之中,会面临极大的风险^[3]。

3 计算机网络数据库安全管理的优化对策

3.1 充分发挥出安全管理模式的作用

为了保证计算机系统正常运行,优化数据库的功能,需采用完善的安全管理模式,确保各项信息数据得到分类存储与管理。安全管理模式还可根据不同等级特征的数据,设置相应的密码,打造差异化管理体系,保障用户数据的安全。工作人员要结合数据库的需求和用户需求,选择合理的管理模式,避免用户的信息频繁被泄露,使各类数据获得有效的识别与验证。要进一步优化数据库的结构,及时对系统中的漏洞进行修复,使数据得到正常的存储与传输。

3.2 采用完善的数据加密技术

数据加密技术不仅可以保护数据的安全,避免数据遭到窃取,还可对各类病毒进行有效的预防。利用专门的语言程序对数据库或数据进行加密处理,可避免用户的信息被泄露,维护用户的合法权益。加密技术具有良好的安全性和隐蔽性。常用的加密技术包括计算机密钥、防复制技术和保密通信技术等。可根据实际情况选择相应的技术,并将其作用于数据的传递过程,可达到事半功倍的加密效果。由于病毒或木马程序会不断更新,技术人员需及时更新加密技术,才能达到更加完善的保密效果。由于系统中的数据类型多样,数量庞大,可采用分层次划分法,对重要的数据进行加密处理,可进一步减少损失。

3.3 采用存储控制管理技术

为了保证数据得到有效的存储,满足用户的多元化需求,需为用户提供相应的权限,使其能够随时对数据库进行访问或查询所需信息。在设置权限时,要考虑到用户在登录过程中很容易受到外部因素的干扰,比如,病毒可能会在这一阶段趁虚而入,对系统进行攻击。因此,要采用存储控制管理技术,严格保障数据库的安全。在采用这一技术时,需保证用户对数据库的访问和

(下转 243 页)

因此,教育者在户外游戏空间规划时,需要从幼儿视角出发,了解幼儿的兴趣和需要,从而为幼儿提供他们真正需要的安全的游戏空间和丰富的游戏材料。让幼儿在成人所提供的有目的、有计划的环境中自由的游戏。

4.3 游戏时间表现出了教育者的高度控制

游戏时间是保证幼儿充分享受游戏的基本前提,在匆匆忙忙的的时间内,幼儿不能充分享受游戏过程。研究发现,幼儿想要拥有充足的自由游戏时间,在游戏的过程中不被成人打扰和干预。

所以,在幼儿进行游戏时,幼儿园要尽可能为幼儿提供充足的游戏时间,且在幼儿游戏的过程中减少不必要的关注,让幼儿充分享受户外游戏。针对幼儿意犹未尽或疲惫劳累的情况时,教育者可以灵活安排游戏时间,适当延长或缩短游戏时间,并可以在游戏结束前进行必要的提示,让幼儿有结束游戏活动的心理准备,感受到自己对游戏掌控权。

(上接240页)

存储权限得到有效控制,对其每一个操作环节进行实时监督,避免出现异常情况,严格保障数据和信息的安全,降低操作风险。在设定权限时,要有明确的界限,不同用户权限予以合理分配。一旦用户发出请求和指令,需对其进行全面的检查,在充分满足用户请求的基础之上,保证操作过程的安全,使其顺利获得相应的操作权利。需对认证用户的资格进行严格认证,并对其权限进行合理控制。如果其他用户并没有权限,需对其操作行为予以禁止。

4 其他安全技术分析

4.1 病毒查杀

病毒查杀技术主要是针对黑客的攻击、对病毒木马的入侵予以预防和清除的专业技术。由于网络数据库包含的数据数量庞大,一旦有不法分子对数据库进行攻击,极有可能会造成珍贵的数据遭到泄露。许多数据涉及企业的商业机密,各大企业积极采用多种安全技术,并将病毒查杀技术作为重要的内容。一旦某一计算机“中招”,其他计算机系统也将在较短的时间内感染病毒。由于病毒的隐蔽性极强,还可在较短的时间内形成大规模复制现象,因此,若采用传统的病毒查杀技术则很难根除病毒,甚至会威胁数据的安全。需安装专业的杀毒软件,保证病毒得到及时的排查与处理。合理利用杀毒软件,对系统进行检测,使病毒得到根除。即使病毒隐藏在较深的位置,也可在第一时间使其原形毕露。由于木马病毒的形式多种多样,需采用专业的查杀技术,对木马病毒进行检测与根除。要构建健全的木马分析系统,根据用户提交的文件,对木马病毒进行查询,一旦确认其存在于系统之中,就需在第一时间予以处理。

4.2 身份认证

身份认证技术可对用户的访问行为予以有效规范,在明确用户权限的基础之上,保护用户的隐私和信息安全。用户在登录某一系统时,除了要设置用户名之外,还要输入密码。随着访问控制模式的不断升级,用户可根据自身实际情况,确定是否要对其他人的访问权限予以设置。在强制访问控制模式下,用

参考文献:

- [1] 但菲,刘凌,赵琳. 幼儿秩序认知发展的特点及其重要价值[J]. 学前教育研究, 2013(07): 15-19.
- [2] 岳训涛. 儿童社会规则认知特点与游戏规则意识的培养[J]. 基础教育研究, 2012, 25(11): 58-59.
- [3] 张莹,华爱华. 游戏时长对幼儿积木游戏行为与作品的影响[J]. 学前教育研究, 2009(02): 36-43.

作者简介:

孙白茹(1997—),女,汉族,山西长治人,硕士,西北师范大学教育学院学前教育学专业,研究方向: 幼儿心理发展与教育。

吴小英(1997—),女,汉族,重庆云阳人,硕士,西北师范大学教育学院学前教育学专业,研究方向: 学前教育基本理论与实践。

户的访问权限比较小,系统会对用户的访问行为进行严格的控制,若其他用户并未获取访问权限,就无法登陆平台。由此可见,强制访问控制技术可进一步保障系统与数据库的安全。

4.3 常规备份与异地备份

由于数据库的功能并非万无一失,一旦受到外界因素的干扰或突发事件的影响,极有可能会造成数据库中的数据丢失。人们积极应用数据备份和恢复技术不断减少损失,并对人为因素进行有效控制,可提高数据库的安全性。该项技术不仅可以对数据进行备份,还能保证数据得到尽快恢复。即使系统依然面临被攻击,也能有效保证数据的安全性和可靠性。此外,该项技术还可进一步修复漏洞,使信息得到尽快恢复。为了确保数据库的备份工作合理开展,可发挥出常规备份技术的作用。为保证数据随时得到备份,还可利用异地备份技术,当数据得到更新时,可在第一时间将新数据予以备份,既能保证数据的安全,又能对副本进行合理的控制。即使数据并未及时得到恢复,只需运行副本也能满足用户的需求,维持数据库的正常功能,提高其安全性和可靠性。

5 结束语

综上所述,数据库安全管理是一项重要而复杂的工作,技术人员要保证与之相关的技术与与时俱进,才能使数据的安全更有保障。要提高用户的安全防范意识,规范用户的操作行为,使其了解安全管理技术的重要性,以及数据丢失所带来的一系列损失。由于数据库面临的安全威胁类型多种多样,需采用多种安全技术,打造完善的安全管理体系,融入防患于未然的思想,才能有效保障数据库更加安全、可靠。

参考文献:

- [1] 范文峰,王龙飞. 计算机网络数据库的安全管理工作研究[J]. 信息与电脑(理论版), 2021, 33(09): 200-202.
- [2] 李俊. 试析计算机网络数据库的安全管理技术[J]. 数字通信世界, 2021(02): 112-113.
- [3] 宋龙虎. 计算机网络数据库的安全管理技术研究[J]. 数码世界, 2020(12): 225-226.