

基于网络安全视角的医院信息管理计算机数据库技术应用分析

辛灵

(内蒙古呼伦贝尔市人民医院 021008)

【摘要】 本文从计算机数据库技术的特征出发,详细论述了在医院信息管理中运用计算机数据库技术的重要性及功能,并从网络安全的角度,详细地分析了在医院信息管理中运用计算机数据库技术的具体策略。希望通过本文的研究,能够为提高医院的安全水平,增强医院计算机数据库的安全防护能力,起到一定的借鉴作用。

【关键词】 网络安全; 医院; 信息管理; 计算机数据库

Application analysis of computer database technology for hospital information management based on the perspective of network security

Xin Ling

(Inner Mongolia Hulunbuir People's Hospital 021008)

[Abstract] Based on the characteristics of computer database technology, this paper discusses the importance and function of using computer database technology in hospital information management, and analyzes the specific strategies of using computer database technology in hospital information management from the perspective of network security. It is hoped that through the research of this paper, it can improve the safety level of the hospital, enhance the safety protection ability of the hospital computer database, and play a certain reference role.

[Key words] network security; hospital; information management; computer database

一、关于网络安全信息管理的几个问题

1.1 网络信息安全管理的基本概念

网络安全信息管理是一种旨在保障计算机网络及信息系统安全的技术、管理和组织工作的相关行为,包括安全的规划、实施、运行和监测等。在安全管理方面,主要包括:安全,风险,控制,架构等。

在安全管理方面,安全性是指信息系统或网络在保持其完整性、机密性、可用性和可控性的前提下,抵御来自内部或外部的威胁与攻击。其中,完整性是指资料及资料不受破坏或破坏。机密性是指非授权人员无法阅读的信息或资料。可用性是指能够及时地存取和利用这些信息,并且能够对其进行适当的加工和传递。可控性是指能够有效地控制、管理网络及系统。要保证信息安全,就必须提高安全意识、开展系统的安全性评价、对存在的安全问题进行及时的发现、分析、改进、完善。风险就是计算机应用系统及网络中所蕴含的潜在危险,并有可能引发信息安全事件。风险分析主要是对风险等级、影响范围和防范措施进行评价,并给出相应的对策建议。监控是对信息系统进行管理、监视、保护和检查的一种行为。通过对失效、威胁等行为的预防和检测,可以有效地保障网络及系统的安全。架构就是网络及其内部的功能和组织结构,是根据网络的特征和应用需要而进行的,能够从加强对网络的管理,对各种安全策略进行规划和实施,

从而提升网络和系统的安全性。

1.2 网络安全信息管理的意义

网络安全信息管理主要是指为了保证重要的网络和系统的完整性、保密性、可用性和可控性,对计算机网络和信息系统进行一系列的技术、管理和组织工作的相关行为。其目的在于规划、实施、运行和监督信息系统的安全,从而保证信息资源在网络中的安全与稳定。需要从安全规划、安全设计和运行维护三个方面对网络安全进行研究。通过对网络中的网络安全隐患进行分析,可以对网络中潜在的网络攻击行为进行预测,并据此制定相应的预防与应对措施。

二、计算机数据库技术特征

计算机数据库的建立,主要是针对使用者的需求,以及搜集的资料加以整理、整理与储存。数据库构建完成之后,所采用的计算机数据库技术主要有两个部分:数据的存储和使用。具体而言,数据的存储可分为存储之前的数据分类、存储过程中的去冗余以及存储后的安全防护。数据的使用方法主要有:建立多个数据库表的视图,对不同级别的用户进行权限划分,对同一级别的不同用户进行数据共享。

在医院的信息化中,最重要的是计算机数据库的功能,包括门诊单、病历单、化验单、收费单、设备清单等资料要进行合理的管理,同时因为医院患者、医生、病情等信息要

保密,所以医院的计算机数据库也要保证对储存在数据库中的数据信息进行安全保管。上述所有的功能都离不开数据库技术,而这些技术在数据管理中扮演着非常重要的角色,下面将对计算机数据库技术的应用特征进行具体的分析。

2.1 整理数据

在医院资料储存之前,计算机数据库必须预先产生一个或多个空白数据库表格,表格内仅有各个表格的表格,如此才能确保将混乱的资料储存到数据库中,可以在一个稳定的结构中寻找其相应的存放地点,这样就可以形成一个有序的系统,便于数据库及工作人员进行数据的管理。例如,当医院保存病人的病历资料时,可以在数据库表格中设定身份、性别、疾病等,处方、发病时间、是否收费等头条资料,都要仰赖库表中所提供的关键字,关键字可以是身份识别码或病人识别码,在其它部门要检索某个数据的时候,只要填写主索引信息,就可以实现信息的检索。

2.2 保证数据的独立性

为了确保存入库中的数据既有物理上的独立,又有逻辑上的独立,首先要通过物理方法来调整数据的存储位置,确保同一个人的相同的数据可以存放在不同的数据库中,从而达到两种不同的数据存储架构。其次,通过修改数据的属性与类型,使同一人的不同属性的数据能够共存于同一数据库中,从而实现逻辑上的独立。例如,在医院给病人用药时,医师在利用这些资料时,主要是要让病人更加科学用药,而这些数据,则是用来收费的,一个数据可以存放在不同的数据库中。

2.3 消除数据冗余

通常情况下,数据库都会定期剔除冗余或无用的数据,以节约内存,提高检索效率,特别是随着用户数据系统的日益复杂和庞大,必然会出现数据的复制,对其进行及时的清理有助于提升数据库的数据质量。如果一家医院在不同的时间段接受了相同的病人,那么他们的个人信息就会被重新录入,而通过数据库的方法,可以将多个病人的身份信息删除,保留一份以备不时之需。

2.4 实现数据的共享

数据库技术的最大特征在于允许多个用户单元来浏览所存储的数据,形成一种服务器终端对多个客户端的方式,这种共享方式既能保证各个行业之间的信息互联,又能保证各部门之间的信息共享,而且不同的使用者也可以对相同的数据进行增删、修改、查,从而丰富了数据库的数据内容。要知道,可以浏览资料的使用者是要满足某些条件的,有些使用者可能只有浏览的权利,而有些使用者则有修改的权利,简单来说,就是可以跨越时空,提高工作效率。

2.5 保证数据安全性

数据安全保护是每个数据库在设计时都要考虑的一个重要问题。一是数据盗窃,黑客可以通过数据库的漏洞进行网络攻击,而医院里的罪犯也可以通过自己的身份潜入到数据库中,对数据库进行拷贝或者删除,这对数据的隐私造成了很大的威胁。二是数据损毁,当数据库接入到信息管理平台之后,因为操作人员的工作环境不一样,或者没有足够的安全意识,就有可能让网络病毒通过网络平台侵入到数据库,损坏了里面的资料,造成了不可挽回的伤害。三是数据损失,当数据库处于离线状态并进行备份时,因自然灾害等原因,数据库会受到物理上的损坏,造成数据的局部或完全的损失。数据库网络保护技术可使数据库具有一定的防御能力,数据库的权限设计可防止被内部人员盗用,数据库的异地备份可使医院免受人为或人为因素的侵害。可以改善资料信息的安全性。

三、计算机数据库技术应用于医院信息管理的意义

计算机数据库作为医院信息化建设的基础,对实现医院信息化建设具有重要的作用。第一,有了数据库,可以改善资料输入的精确度,避免因医师手写或字迹不清而引起的资料差错。第二,数据库为医师提供了一个模板,使医师、护士能够按照预先设定好的模板进行录入,减轻了医务人员的工作负担。第三,数据库能向收费科提供各种药品、化验等项目的明细帐资料,确保收费公开透明。第四,数据库能为病人节省就诊时间,病人首次将个人资料录入数据库后,即便是到其他科室就诊,每个部门的工作人员,都可以直接从电脑上调出自己的记录。第五,数据库能使医院各个部门之间的数据信息进行共享,使各个部门之间能够真正地连接在一起,从而把医院运作、医疗工作、病人就医等各个环节的信息联系在一起。第六,数据库技术可以保证医生和病人的个人隐私不容易被人盗取。

四、基于网络安全视角的医院信息管理计算机数据库技术具体应用

4.1 加强制度的作用

由于操作数据库和信息管理系统的工作人员不够专业,或者对自己的安全意识不强,因此,在日常工作中,这些工作人员经常要面对大量的数据,很容易由于对系统功能的每一个步骤不熟悉而陷入慌乱。最后,将某些重要的系统功能暴露于互联网,让黑客可以很容易地盗取他们所需要的信息,从而导致信息和数据的泄漏。所以,在信息管理中运用数据库技术,首先要加强系统的功能,特别是各个功能的连

接与跳跃,保证一些与数据相关的重要功能不会被轻易地暴露在网络环境中。

就像是病人的病历资料查询,信息管理系统不能把这个功能直接暴露在网页首页或者第二个页面上。首先要将自己的账户登录到系统的首页,在自己的功能页面上点击相关的病人基本资料,再一次跳到病人基本信息页,才能决定要不要查看病人的病历资料。其目标是依赖于系统设置的网络保护功能来阻挡网络黑客的侵入,并在几次跳跃之间通过某种信息干扰等方式加大了黑客的侵入难度。此外,通过这种方式,还可以防止由于对系统不熟悉而造成的错误操作。

又例如,当病人来看病的时候,医院的数据库会自动处理病人,让病人自己填写基本资料,并将其存储在数据库中,一旦病人被医师诊断并做出入院的决定,系统就会自动生成一份医疗记录表格供医师完成。为确保病人基本信息的安全,病历中的病人基本信息不需要再次填写,全部由数据库技术在后台进行自动处理,从而最大程度地避免了数据信息的泄露,同时也方便保存。

4.2 设定访问权限

为确保医院的信息不外泄,通常应该按照医院对不同身份级别的使用者资料设定不同的存取权限,让使用者按照自己的权限进行存取,采取适当的行动,并限制了超过许可范围的功能。权限的不同,代表着使用者可以看到的资料也是不一样的,就拿医生和护士来说,他们只能看到和自己有关的病人资料或者医疗器械的资料。科主任可以查询自己科室的医生、病人、仪器等信息。院长可以查询到最多的资料,也是最完整的,也是最容易管理的。另外,权限的设定也是为了明确职责,如果有一家医院发生了信息泄漏,而警方或者系统工作人员认为是内部泄密,那么就可以通过泄漏的数据信息级别,追踪到相应的用户。在第一时间内,可以将调查的范围缩小,从而可以迅速地解决泄密的问题,将造成的损失降到最低。

4.3 编制数据流图表

许多情况下,有些基本的信息资料可以由多个部门进行处理,单凭权限控制难以迅速地找到操作人员,从信息管理的费用来看,利用电脑资料处理技术,建立一个合理的资料流动图表,并在数据库中标示信息资料。在数据流通的过程

中,系统会按照标识产生一张数据流图表,在图表中记录数据所经历的每一个步骤,包括传输、存储、停留的位置,这使得数据的来源去向、输入输出、调取加工等操作过程都有了更清楚的了解。流量图能够让监控者对数据的变动进行判定,如果发现有什么不正常的地方,就说明系统的数据库受到了外来的攻击,监控者可以在最短的时间内发出警告。

4.4 数据加密

前三个方面的问题,包括数据访问的难度、数据的访问权限、数据的流动等,即使医院做到了,也不可能实现100%的数据安全,因为一旦数据被窃取,就没有任何的保护措施了。原始资料公开的状况,为犯罪分子提供了任意操纵利润的机会。为防止这样的情况发生,在医院中可以采用数据加密技术,这也是对数据进行保密保护的最后一道防线。通过一定的运算逻辑,将储存在数据库中的数据转化为另外一种形式,即便是黑客能够突破重重防御,进入到数据库中,也不可能对其进行任何处理。这年头,想要破解数据加密是一件很困难的事情,特别是公钥加密算法,它的保密性足以抵御一切密码攻击,但是这种算法会造成数据传输的缓慢,对于一般的资料,可以采用比较简单的加密方式,在确保正常资料传送的同时,也可以确保重要资料的安全性。

五、结语

在医院信息化建设中,计算机数据库技术的运用,对网络安全信息的管理起着至关重要的作用。网络安全信息管理就是要以一种综合性的技术、管理和组织方式,来保证一个完整的、完全的、保密的、可用的、可控的系统。以计算机数据库技术为中心的医院信息化系统,不但能有效地提高数据的处理效率与精度,而且能最大限度地实现数据的检索、共享和存储,从而实现各个科室之间的信息交流。同时,通过设置访问权限,跟踪数据流向,并对数据进行加密,实现对医院数据的全面保护。从而降低信息泄漏的风险,保证医院运行的安全性与稳定性。以计算机数据库技术为基础,以实现医院信息化的现代化、标准化、安全性的目标,从而为医院的信息化建设提供强有力的技术支撑与管理支撑。

参考文献:

- [1]吴海威.基于网络信息安全技术管理的计算机应用分析[J]. 无线互联科技.2021, 18(7): 31-32.
- [2]倪勇.基于网络信息安全技术管理的计算机应用分析[J]. 科学与信息化.2019, (35): 153, 159.
- [3]罗帅.基于网络信息安全技术管理的计算机应用分析[J]. 现代工业经济和信息化.2019, 9(8): 71-72.
- [4]熊劲磊.基于网络信息安全技术管理的计算机应用分析[J]. 数码设计(上).2022, (1): 33-36.