论网络金融会计信息系统安全体系的构建

□ 郑兴云

摘要:随着金融会计信息系统进入网络化时代,由于黑客病毒等因素造成各类电子信息文件篡改,严重地破坏银行会计信息系统,对金融会计信息造成安全隐患,因此构建金融会计信息系统安全体系就显得非常必要。本文从网络金融会计信息系统的含义出发,分析对网络条件下金融会计信息系统存在的主要安全隐患,提出如何建立全方位网络金融会计信息系统安全体系的框架。

关键词:会计信息系统;系统安全体系;金融会计

一、网络金融会计信息系统的含义

网络金融会计信息系统是指建立在网络环境基础上的会计信息系统网络环境,包括两部分:一是金融企业内部网络环境,即内网,通过组建金融企业内部网络结构实现内部各部门之间的信息交流和共享;二是国际网络环境,即通过互联网使金融企业同外部进行信息交流与共享,基于互联网的会计信息系统,也可以说是基于内联网的会计信息系统,即金融企业的内联网和互联网连接,为金融企业内各部门之间,金融企业与客户、税务、审计等部门之间建立开放、分布、实时的双向多媒体信息交流环境创造了条件,也使金融企业会计与业务一体化处理和实时监管成为现实,原来封闭的局域网会计信息系统被推上开放的互联网世界后,一方面给金融企业带来了前所未有的会计与业务一体化处理和实时监管的优越性,另一方面由于互联网系统的分布式、开放性等特点,其与原有集中封闭的会计信息系统比较,系统在安全上的问题也更加突出,互联网会计信息系统的风险性更大。

二、当前网络金融会计信息系统存在安全隐患

(一)金融会计信息安全组织管理体系不完善

目前,金融企业尚未建立起一套完整的计算机安全管理组织体系,金融会计信息系统的建设在安全设计方面缺乏总体考虑和统一规划部署,各系统根据自己的理解进行规划建设,技术要求不规范,技术标准各异,技术体制混乱。国家标准制定严重滞后,法律法规不能满足金融会计信息系统的安全需求,现行计算机安全法律法规不能为金融会计信息系统安全管理提供完整配套的法律依据,在一定程度上存在法律漏洞、死角和非一致性。

(二)网络金融会计信息数据不安全

网络金融会计数据是记录在各种单、证、账、表原始记录或初步加工后的会计资料,它反映企业的经营情况和经营成果,对外具有较高的保密性,连接互连网后,会计数据能迅速传播,其安全性降低,风险因素大大增加,网络金融会计的信息工作平台是互联网,在其运作过程中,正确性、有效性会受到技术障碍的限制和网络与应用软件接口的限制,如网络软件选配不合适,网络操作系统和应用软件没有及时升级,或安全配置参数不规则,网络线路故障导致工作站瘫痪、操作失误等,系统间数据的大量流动还可能使金融企业机密数据无形中向外开放,数据通过线路传输,某个环节出现微小的干扰或差错,都会导致严重的后果,互连网结构的会计信息系统,由于其分布式、开放性、远程实时处理的特点,系统的一致性、可控性降低,一旦出现故障,影响面更广,数据在国际线路上传输,数据的一致性保障更难,系统恢复处理的成本更高。

(三)网络金融信息泄露导致金融会计信息失真

在信息技术高速发展的今天,信息已经成为金融企业的一项重要资本,甚至决定了金融企业在激烈的市场竞争中的成败。而金融会计信息的真实、完整、准确是对金融会计信息处理的基本要求。由于金融会计信息是金融企业生产经营活动的综合、全面的反映。金融会计信息的质量不仅仅关系到金融会计信息系统,还影响到金融企业管理的其他系统,目前利用高技术手段窃取金融企业机密是当今计算机犯罪的主要目的之一,也是构成金融会计信息系统安全风险的重要形式。其主要原因:一是电信网络本身安全级别低,设备可控性差,且多采用开放式操作系统,很难抵御黑客攻击;二是由于电信网络不负责对金融企业应用系统提供安全访问控制,通信系统已成为信息安全的严重漏洞,但许多金融企业对此未加以足够重视而采取有效的防护措施。由于这些原因导致了金融会计信息系统的安全受到侵害,造成了信息的泄露,使金融会计信息失真。

(四)金融会计信息系统的存在安全威胁

目前金融企业计算机已广泛联网,这是金融企业扩大业务范围,实现信息共享的必然结果。由于网络分布广,不容易集中管理,许多系统又是在存在安全漏洞与威胁的环境下工作的,不法分子可以在网上任意地点攻击,使金融企业不知不觉中被偷盗资金或泄露机密。金融企业经营的资金,不法分子作案得逞就能弄到金钱,因此其已成为犯罪分子攻击的主要目标,且作案手段繁多,方法越来越高明。作案分子有以下三类:(1)内部人员作案。金融企业内部人员熟悉金融企业业务和金融企业会计软件的薄弱环节与漏洞,若禁不住金钱的诱惑,就会铤而走险,钻制度不严的空子,利用合法身份或明或暗或用高科技手段作案,侵吞国家资产或非法转移客户存款。(2)外部攻击。外部攻击具有作案地点广泛、案情复杂且作案手段日趋技术化、智能化等特点,给金融企业及客户造成巨大损失,跟踪与破案难度很大。(3)内外勾结作案。犯罪分子利用金融企业管理上的漏洞与松懈,内外勾结,冲破重重关卡联合作案。此类攻击后果尤为严重,风险最大。

三、构建网络金融会计信息系统安全体系思路与方法

采用现代信息系统实用安全概念、安全防护、安全检测、安全反应是构成计算机安全管理的核心环节,各个环节形成循环密切相关。构建网络金融会计信息系统安全体系关键在以下几个方面把握:

1、完善网络金融会计信息系统技术法规、标准和制度体系建设

加快标准规范和制度体系基础工作步伐,统筹规划、结合国家和行业监管部门,重点加强电子支付及信息产品与服务的测评、准入、认证等相关技术法规与标

准。密切结合金融企业信息化发展实际，借鉴国内外先进经验和做法，加紧建立和不断完善集中式数据中心运营规范和制度体系，加强网络金融会计信息安全的各项规章制度建设，逐步实现一个岗位一项制度，全面落实“让标准说话，按制度办事”的信息安全管理准则。

2、金融会计信息系统的物理安全的控制

建立金融会计信息物理安全控制，主要有三种关键技术:第一种是防火墙技术。防火墙是一组基于互联网和金融企业内联网之间的访问控制系统，它充当屏障作用，保护金融企业信息系统(内联网)免受来自互联网的攻击。防火墙由软件系统和硬件设备组合而成，它执行安全管理措施，记录所有可疑事件。防火墙产品主要包括过滤型和应用网关型两种类型。所有互联网与金融企业内联网之间的信息流都必须经过防火墙，通过条件审查确定哪些内容允许外部访问，哪些外部服务可由内部人员访问。因此，防火墙以限制金融会计信息的自由流动为代价来实现网络访问的安全性。第二种是反病毒技术。在金融会计信息系统的运行与维护过程中，应高度重视计算机病毒的防范及相应的技术手段与措施。如采用基于服务器的网络杀毒软件进行实时监控、追踪病毒等等。第三种是备份技术。备份是防止网络环境下金融会计信息系统意外事故最基本、最有效的手段，它包括硬件备份、系统备份、会计软件系统备份和数据备份四个层次。

3、构建金融会计信息保密的安全体系

(1)建立用户分类安全控制体系。在金融企业内部，不同的信息使用者，由于他们的身份不同，以及他们对获取的会计信息要求也不同，因而有必要对这些用户进行分类，以保证不同身份的用户获取与其身份及要求相符的会计信息。对用户分类是通过对用户授予不同的数据管理权限来实现的，一般将权限分为三类即数据库登录权限、资源管理权限和数据库管理员权限等。只有获得了数据库登录权限的用户才能进入数据库管理系统，才有可能进行数据的查询，以获取自己所需的金融会计数据或金融会计信息，但其不能对数据进行修改。而拥有数据管理权限的用户除了拥有上述数据访问权限之外，还可拥有数据库的创建、索引及职责范围内的修改权限等。至于拥有数据库管理员权限的用户他将有数据库管理的一切权限，包括访问其他用户的数据，授予或收回其他用户的各种权限，完成数据的备份、装入与重组以及进行系统的审计等工作。但这类用户一般仅限于极少数的用户，其工作带有全局性和谨慎性，对于金融会计信息系统而言，会计主管就可能是一个数据库管理员。

(2) 建立金融会计数据分类安全体系。虽然对用户进行了分类，但并不等于一定能保证用户都根据自己的职责范围访问相关金融会计数据，这是因为同一权限内的用户对数据的管理和使用的范围是不同的，如金融会计工作中的凭证录入员与凭证的审核人员，他们的职责范围就明显地限定了其对数据的使用权限。因此，数据库管理员就必须根据数据库管理系统所提供的数据分类功能，将各个作为可查询的金融会计数据逻辑归并起来，建立一个或多个视图，并赋予相应的名称，并把该视图的查询权限授予相应的用户，从而保证各个用户所访问的是自己职责范围内的会计数据。

(3)建立会计数据加密安全体系。普通的保密技术能够满足一般系统的应用要求，只是通过密码技术对信息加密，是安全的手段。信息加密的核心是密钥，密钥是用来对数据进行编码和解码的一种算法。根据密钥的不同，可将加密技术分为对称加密体制、非对称加密体制和不可逆加密体制三种。对一般数据库来说是较为有效的，但是对金融会计信息系统来说，仅靠普通的保密技术是难以确保金融会计数据安全的。为了防止其他用户对会计数据的非法窃取或篡改，为防止非法用户窃取机密信息和非授权用户越权操作数据，在系统的客户端和服务器之间传输的所有数据都进行双层加密。即第一层加密采用标准 SSL 协议，该协议能够有效地防破译、防篡改，是一种安全可靠的加密协议；第二层加密采用私有的加密协议，该协议不公开、不采用公算法并且有非常高的加密强度。两层加密确保了会计信息的传输安全，从而保证金融会计信息的安全性。

4、建立网络金融会计信息系统应急预案

制订应急预案的目的是为了确保金融企业正常的金融服务和金融秩序，提高金融企业应对突发事件的能力，在网络金融会计信息系统故障时，将系统中断时间、故障损失和社会影响降到最低，应急预案的核心是建立应急模式下的业务处理流程，详细阐述应急模式的操作步骤，建立相应的事后数据补录和稽核制度，网络金融会计信息系统安全应急预案规定:系统应用部门发现信息系统故障，应及时通知部门负责人；部门负责人应立即通知计算机中心；计算机中心应立即着手查明故障原因，预计系统修复时间，并通知相应部门负责人；若暂时不能修复(超过 15 分钟)，应向安全领导小组报告，由金融企业领导确定是否启动紧急预案；紧急预案启动后，计算机中心应通知各相关部门，启动紧急预案中相关的应急措施；在故障消除后，计算机中心应立即通知各应用部门，并报告安全领导小组，请求结束应急预案的实施；事后计算机中心应将详细的故障原因和处理结果报有关领导。

建立健全网络金融会计信息安全检查机制，加大监督检查工作力度。依据业已确立的技术法规、标准与制度，定期开展信息安全检查工作，确保信息安全保障工作落到实处。建立责任通报制度，对检查中发现的违规行为，按规定处罚相关责任人，对检查中发现的安全问题和隐患，明确责任部门和责任人，限期整改。在开展合规性检查的同时，应综合运用检测工具，明确安全控制目标，加强深度的专项安全检查工作，保证检查工作的针对性、深入性和时效性。

总之，网络金融会计信息系统所面临的外部和内部侵害，使得我们必须采取切实可行的安全对策，以确保系统具有信息保密性、身份的确定性、不可否认性、不可篡改性、可验证性和可控制性。

参考文献：

[1] 周慧.《商业银行电子化的风险控制》.《金融与保险》,2003 第 9 期

[2]乔立新、袁爱玲、冯英俊.《建立网络银行操作风险内部控制系统的策略》.《商业研究》,2003 年第 8 期

[3] 刘昊.《论我国网络银行的风险及其控制》.《新金融》,2003 年第 1 期

[4]杨周南.《论会计管理信息化的 ISCA 模型》.《会计研究》,2003 年第 10 期

[5]刘贵栓.《金融企业会计信息失真探析》,《经济师》,2003 年第 1 期

[6] 张金城.《计算机会计信息失真风险防范》,浙江人民出版社,2003 年 1 月第 1 版

[7] 谢赞恩.《中国金融信息化二十年》,《互联网周刊》, 2004 年第 3 期

[8]顾浩.《中国金融企业信息化任重道远》.《上海金融高等专科学校学报》,2003 年第 4 期

[9]曾永光，周利枚、徐运保.《城市商业银行信息化新思路》,《湖南工程学院学报》, 2005 年第 12 期

(作者单位:福建省海洋技术学校)