银行计算机网络信息系统安全管理研究

路晨曦[1]　于　昊[2]

（1. 沈阳航空航天大学，辽宁 沈阳 110000;
2. 辽宁省农村商业银行，辽宁 沈阳 110000）

摘　要　为了做好银行计算机网络信息系统安全管理工作，本文论述了系统安全管理现状，随后指出安全管理的主要缺陷，最后提出相关策略。银行必须对银行计算机网络信息系统进行安全管理，避免系统内信息受损或外泄是该项工作的最终目的，但要做到这一点就必须不断完善安全管理体系，因此有必要展开相关研究，重点分析当下安全管理问题，再用策略进行强化，这样才能让安全管理与时俱进，始终保持良好安全水平。文中策略可以弥补银行计算机网络信息系统安全管理的缺陷，提高系统安全水平，能有效防护安全攻击，最大限度避免系统信息受损或外泄。

关键词　银行　计算机网络信息系统　信息安全管理

中图分类号：F83；TN915.08　　**文献标识码**：A　　**文章编号**：1007-0745（2021）04-0043-02

银行的主营业务决定了其在工作中会产生许多关键信息，类如用户身份、住址、银行卡密码等，还包括银行本身的一些关键信息，这些信息不仅具有隐私性，还具备一定的危险性，如果这些信息受损会导致银行工作受阻，容易造成业务纠纷，如果外泄则可能带来巨大的经济损失，受害方往往是用户。

1 银行计算机网络信息系统安全管理现状

1.1 权限限制

银行内的相关信息普遍被保存在计算机网络信息系统的数据库中，要获取所需信息就必须进入数据库，这样就形成了初步的安全防护，但数据库本身没有防护能力，因此为了避免非法人员进入数据库窃取、篡改信息，在安全管理方面现代多数银行都采取权限限制功能，该功能的安全管理原理为：任何人要进入数据库都必须先进行登录，登录时的账号与操作人员的身份相互绑定，随后系统管理员针对不同账号进行权限分配，使得拥有不同账号的操作人员只能查看权限范围内的信息，诸如财务人员通过账号登录数据库，在权限限制下该人员就只能查看财务相关信息，而用户身份信息等则无法查阅。从这里可以看出，权限限制功能具有安全管理作用，身份未得到认证的人无法进入数据库，未得权限许可的人无法获取权限外信息，因此起到了安全防护作[1]。

1.2 用户识别功能

在人脸识别、电子签证等先进信息识别技术的作用下，现代银行针对计算机网络信息系统均配置了用户识别功能，该功能是预先记录每一个用户的关键信息，类如用户脸部图像信息，随后借助大数据系统进行储存，同步通过智能系统获取图像信息特征，这样要进入系统获取个人信息，诸如个人账户余额等，就必须通过“刷脸”等手段获得认证，随即才能进入个人页面查阅信息。从这里可以看出，用户识别功能的主要作用是识别用户身份，基本原理与上述的“权限限制”功能类似，因此也具备良好的安全防护作用，是一项出色的安全管理功能。

1.3 防火墙应用

防火墙是传统的安全管理技术，经过多年发展已经广泛普及，且安全性能更加优异，因此许多银行都选择了防火墙技术。在银行计算机网络信息系统中，现代防火墙技术的应用方式有两个特点：第一，防火墙布局普遍采用纵横形式，这样能够形成多重防护，安全性有大幅提升；第二，防火墙主要应用于网络通信链路方面，内附安全系数计算逻辑，能根据用户 IP 地址、计算机电子标识等计算本次访问的安全系数，得出系数等级，等级一般可分为优秀、良好、一般、差，其中优秀与良好会直接通过，一般和差则会向管理员发送警告信息，由管理员作出决策。

1.4 病毒查杀软件应用

病毒查杀软件是专门针对病毒攻击的一种程序，其核心为病毒库，即病毒库本质是数据库，记录了大量病毒的程序代码以及攻击特征，这样通过筛查机制即可知道计算内部是否存在病毒，当发现病毒或发现疑似病毒的文件时，软件会直接删除病毒，或者通知操作人员，由人工定夺，但在人工作出决策之前，病毒会被保存在“黑名单”中，不会对计算机造成影响，实现杀除病毒。

2 银行计算机网络信息系统安全管理缺陷

2.1 系统复杂，边界模糊

首先，现代银行计算机信息系统中有多个子系统，还并存着各种网络系统、各种型号的硬件设备等，因此系统的复杂性较高。在高复杂性下，安全管理工作难度上涨，有可能无法做到全面防护，同时复杂的系统会不断生成漏洞，导致安全管理系统与人员应接不暇，因此面对复杂系统，银行安全管理工作存在缺陷。其次，复杂的系统还造成了边界模糊的问题，即复杂系统中的部分子系统与网络环境连接紧密，而网络本身具有开放性与可拓展性，这两个特

性使得网络边界模糊，因此部分子系统也会受到间接影响，出现边界模糊现象，诸如信息系统中的某个业务系统需要对外进行信息传输，而传输后信息就进入到了边界模糊的网络中，这时非法人员就可能通过特定手段获取信息。

2.2 硬件可靠性不足

任何计算机网络信息系统都需要大量硬件作为支撑，这一点对于银行系统而言也不例外，而现代网络攻击手段可以从硬件着手进行攻击，说明硬件是攻击要点之一，若银行网络信息系统的硬件的可靠性不足，就很容易被攻破，进一步引起网络安全事故。但现实情况中，很多银行的系统硬件都存在可靠性不足的问题，其中最具代表性的就是交换机，即交换机负责网络信号传输，有特定的 IP 地址，在可靠性不足的情况下，交换机的 IP 地址容易泄露，攻击者可能对这个 IP 地址进行监听，从中获取传输中的信息，实现信息窃取的目的 [2]。

2.3 资源共享漏洞

为了更好的整合相关资源，现代银行普遍都达成了合作协议，在协议基础上共建了资源共享平台，该平台确实实现了整合资源的目的，但同时也带来了安全漏洞的隐患，即资源共享平台独立于各个银行系统以外，地位相当于中转站，因此银行建立的安全管理系统并不能对该平台进行管理，这时只要银行使用该平台，就可能导致平台内的关键信息泄露，或受到其他攻击，诸如某些资源共享平台本身并不会对用户进行认证，导致一些未授权操作人员会进入平台 [3]。

2.4 协议漏洞

银行计算机网络信息系统需要与外界通信，通信所依靠的通信协议普遍为 TCP/IP，但其是一种以网络地址为基础的协议，因此在使用中攻击者可以从地址中获取口令，同时该协议还会执行一些无关程序，而这些程序也可能是泄密漏洞。针对 TCP/IP 协议的种种漏洞，现代银行普遍还没有进行针对性的管理，因此导致系统安全性不足，例如某银行在系统通信中就遇到了地址诈骗攻击，原因是攻击者通过 TCP/IP 的无关程序窃取了通信地址与口令，使得攻击者可以“假扮”通信方来骗取信息，造成信息泄密。

3 银行计算机网络信息系统安全管理策略

3.1 整合系统，建立封闭环境

计算机网络信息系统太过复杂是造成一系列安全漏洞的根源因素，因此要提高安全性，做好安全管理工作，建议银行着手整合系统，让系统的复杂性降低，自然可消除相关安全漏洞。系统整合的具体方法为模块设计法，即当前复杂的系统中，子系统之间是存在衔接关系的，因此银行可以根据业务项目建立业务模块，再将相关子系统纳入模块中即可实现系统整合，整合后的系统具有了模块化特征，每个模块相当于一个封闭的环境，内部每个子系统的运作都与外界隔绝，若要对外通信，这可以通过专门的通信渠道来实现，加之权限限制功能，可以同步保障系统安全性与通信能力 [4]。同时，在封闭环境建立后，每个模块之间有清晰的边界，且整个系统与网络之间的边界也更加清晰，因此边界模糊问题也迎刃而解。

3.2 数据加密

在条件允许的情况下，银行可以选择可靠性良好的硬件设备来支撑系统通信，除此之外还要重视数据加密的作用，建议银行采用数据加密手段来有效解决硬件可靠性不足的问题。数据加密的主要功能是对通信过程中的信息数据进行加密处理，要获取其中信息数据，就必须输入正确的密钥，而密钥是随即生成的，只有通信双方知道，因此即使攻击者对硬件进行了监听，也无法获得数据加密，使得监听攻击变得无意义，因此可有效地保障数据信息的安全。

3.3 做好资源共享安全管理

资源共享是一大优势，银行不可放弃，但针对资源共享平台带来的安全漏洞，银行必须予以重视，有必要对资源共享平台展开安全管理工作。资源共享平台安全管理工作的具体方法与银行本身的安全管理方法相同，因此不多加赘述，但为了全面落实该项工作，建议合作协议内的每个银行功共同组建安全管理小组，专门负责平台安全管理工作，最大限度地消除安全管理盲区。

3.4 更换通信协议

银行之所以选择 TCP/IP 协议，是因为该协议的通信性能良好，但该协议的安全性存在着一定的不足，因此建议银行更换通信协议，可选择 SSL 协议。SSL 协议是一种加密协议，能保护系统服务器和 Web 浏览器之间的通信，而且可支撑面向会话，安全加密功能为非对称密钥，秘钥的存在可提高机密性与完整性，让通信安全性更高。要更换该协议，银行只需要建立 Web 通信链路即可。

4 结语

综上所述，银行计算机网络信息系统安全管理现状表现良好，但也存在一些缺陷，故银行要针对缺陷强化安全管理工作，通过各种手段提高安全性。安全性的提升有利于银行网上业务开展，也避免银行本身的关键信息泄露，因此银行必须对安全管理工作予以重视，认真分析实际漏洞，秉持对症下药原则进行优化。

参考文献：

[1] 王作鹏 . 研究银行计算机网络信息系统安全管理要点 [J]. 电子世界 ,2016(18):152.
[2] 郭亮 . 银行计算机网络信息系统安全管理分析 [J]. 网络安全技术与应用 ,2018(09):111-112.
[3] 刘泳锐 . 新兴技术发展背景下互联网金融网络安全状况分析与研究 [J]. 网络安全技术与应用 ,2020(06):137-139.
[4] 安丙春 , 张健 , 陶蓉 . 基于大数据的互联网金融安全建设思路 [J]. 信息技术与网络安全 ,2018(08):7-10.