基于 P2DR 模型的高校财务安全策略应用研究

贺文杰,阳宗妤
(湖南科技大学 财务处,湖南 湘潭 411201)

摘　要:信息化时代,采用现代计算机网络技术是财务管理和会计核算发展的必然趋势,但其势必面临黑客攻击、病毒感染等诸多风险,财务网络安全问题研究因而受到重视。在高校财务网络环境的现状及其存在的安全问题基础之上,提出了使用硬件防火墙、加装服务器版防病毒软件、配置目录权限管理、将应用程序池独立、加强 SQL 注入式攻击防范以及强化数据库链接账号和计算机用户账号管理等网络安全管理新策略。

关键词:财务安全;网络安全;策略;实时查询;高等院校
中图分类号:G647　　**文献标志码:**A　　**文章编号:**1674-5884(2014)03-0156-03

在信息化时代,由于对财务会计信息及时、高效、共享的需求等原因,广泛采用现代计算机网络技术必将成为财务管理和会计核算发展的必然趋势[1]。但在网络环境下的财务管理和会计核算处于一种开放平台上,势必面临黑客攻击、病毒感染等诸多风险。解决财务网络的安全问题、维护数据安全是实现网络化财务管理和会计核算的前提。本文以某高校为例,首先介绍其财务网络环境现状,然后分析其财务网络可能存在的安全问题,最后提出在保证内部核算和财务管理安全,用户对财务会计信息实时查询需求的前提下,强化财务网络安全管理,创新财务网络安全策略的解决方案。

1　高校财务网络环境现状

某高校在财务网络环境及其财务网络安全管理等方面具有代表性。本文以此为典型案例开展深入研究。

该校于1990年就实现了会计账务核算、资金管理的网络化,并在2003年搭建财务网,实现了财务会计核算信息的网络实时发布,师生员工能通过网络实时了解教学、科研、管理等项目的收入/归还、支出(经费报销)/借款、结余以及学杂费缴纳/欠费等情况,并对其进行核对和监督,有效解决了财务会计信息实时查询和财务会计错弊等问题,其典型网络拓扑结构如下图1。

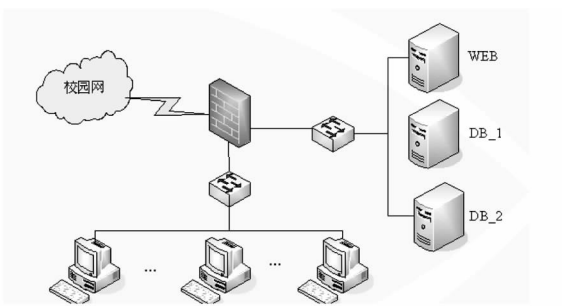

图1　高校财务网络典型拓扑结构

2　高校财务网络可能存在的安全问题

目前财务网络服务器在安全性上可能存在以下几个问题:(1)网络后门未及时堵漏,给黑客攻击以可乘之机(见图2、图3),危害极大。(2)服务器 Administrator 账号的密码为空或者太短太简单。(3)数据库链接采用 SA 最高权限账号。(4)提供 WEB 服务的账号没有独立。(5)存在一些不应该在服务器上直接使用的应用程序,如 QQ。(6)Web 目录的权限没有细分。(7)关机或者重新启动的时候要输入时间跟踪原因(造成发生中断时,一些后台服务不能自动启动)。(8)未能有效配置防火墙方案。

图2　黑客攻击后建立的账号

收稿日期:2013-12-18
作者简介:贺文杰(1974-),男,湖南宁乡人,会计师,高级网络师,主要从事经济管理与财务会计研究。

名称	原位置	删除日期	大小	类型
cvcadmin	C:\Documents and Settings	2011-2-28 21:09	3,692 KB	文件夹
RavBin	C:\	2011-2-28 21:06	4 KB	文件夹
Rising	C:\Program Files	2011-2-28 21:06	164 KB	文件夹
webadmin	C:\Documents and Settings	2011-2-28 21:08	3,808 KB	文件夹
webadmin$	C:\Documents and Settings	2011-2-28 21:08	27,884 KB	文件夹
webadmin$.HP-42970DCCCEDO	C:\Documents and Settings	2011-2-28 21:08	33,144 KB	文件夹
webadmin$.HP-42970DCCCE...	C:\Documents and Settings	2011-2-28 21:08	2,504 KB	文件夹

图 3　黑客攻击账号遗留下的文件

3　P2DR 动态网络安全体系模型简介

P2DR 模型(见图 4)是美国 ISS 公司首先提出的,其核心包括四个主要部分:Policy(安全策略)、Protection(防护)、Detection(检测)和 Response(响应)[2]。(1)策略:是模型的核心,所有的防护、检测和响应都是依据安全策略实施的。网络安全策略一般包括总体安全策略和具体安全策略两个部分。(2)防护:根据系统可能出现的安全问题而采取的预防措施,这些措施通过传统的静态安全技术实现。采用的防护技术通常包括数据加密、身份认证、访问控制、授权和虚拟专用网(VPN)技术、防火墙、安全扫描和数据备份等。(3)检测:当攻击者穿透防护系统时,检测功能就发挥作用,与防护系统形成互补。检测是动态响应的依据。(4)响应:系统一旦检测到入侵,响应系统就开始工作,进行事件处理。响应包括紧急响应和恢复处理,恢复处理又包括系统恢复和信息恢复。

根据 P2DR 模型的 2 个数学公式(Pt > Dt + Rt ;Et = Dt + Rt),如果 Pt = 0,我们针对安全问题可以得出两个明确的方向:即如何提高系统的防护时间,如何降低检测安全问题的耗费时间及响应对策的实施时间。

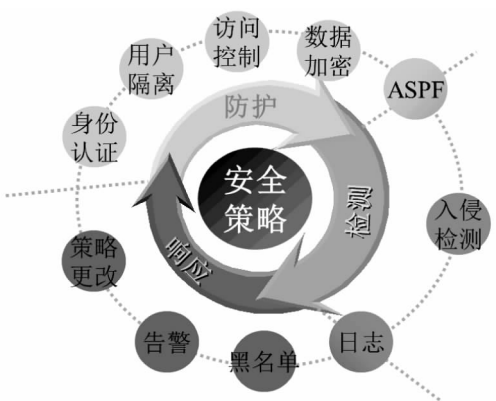

图 4　P2DR 动态网络安全体系模型

4　高校财务网络安全新策略

根据 P2DR 模型针对安全问题的解决方向,主要采取以下几个措施来进一步加强其安全性。

4.1　使用硬件防火墙

使用硬件防火墙通过安全规则(见图 5)的定义,开放尽量少的端口及协议,可以有效提高系统的防护时间;防火墙日志系统的分析,降低了检测安全问题的耗费时间;图形化简洁的界面可以有效地降低响应对策的实施时间。由此可知,拥有可便捷管理系统的硬件防火墙系统是高校财务网络的基础设置,必不可少。

4.2　加装服务器版防病毒软件

加装服务器版防病毒软件是保护网络安全的另一个提高系统防护时间的有效办法,对病毒的快速处理进一步提高了响应的速度和能力。以某高校为例,原先服务器安装的防病毒软件为瑞星杀毒软件,现安装了服务器版防病毒软件 McAfee 的 VirusScan8.5 版(见图 6),针对性更强,并进行了有针对性的配置,可设定其每日对服务器进行全盘扫描,及时发现部分隐患,并及时处理。

图 5　方正防火墙安全规则示例

图 6　网络防毒方案

4.3　配置目录权限管理

详细的配置目录权限是对访问控制的实施,用户的隔离能够加强系统的防护能力。根据一个网站一个独立目录的原则,分配独立的属于 GUESTS 组账号,不要随便使用系统默认账号,对 web 目录,如果只运行 asp,则只要求 administrators 组赋全部权限;IIS_wpg 赋读取、运行权限;匿名访问账号赋读取运行权限;对要求上传的目录或文件型数据库添加写入等独立权限,但要在 IIS 中选择相应文件夹,右键修改为目录—》执行权限—》无(见图 7、图 8)。

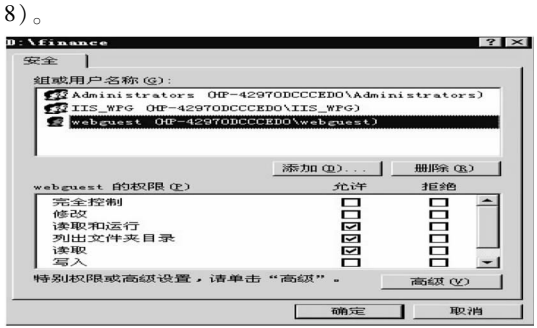

图 7　Web 目录用户权限

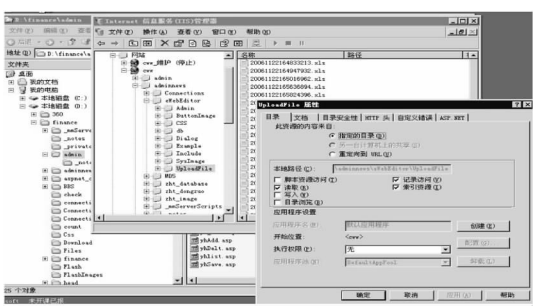

图 8　IIS 目录权限的修改

4.4 将应用程序池独立

应用程序池的独立不但能够提高防护时间,而且发生错误时,重启本应用程序池即可,无需重启 iis,这样也进一步加强了响应时间。具体可以对 IIS 中网站的应用程序池独立,深度隔离,相当于重启。另外不建议多线程,因为虽然能够增强效率,但是由于会话独立,会在程序中产生验证失败的结果。

4.5 加强 SQL 注入式攻击防范

针对目前网站最主流的攻击方式 SQL 注入式攻击,采取加强检测的措施,降低检测时间。因为 SQL 注入式攻击方式具有实现简单、效果明显的特点。它本质上是一种基于 SQL 语法组合的攻击,属于网络的应用层,因此 IP 层的防火墙对它无能为力。一般程序员在软件代码中对此类攻击进行防范。但是无法保证每个应用程序都经过严格的检查,因此可以从系统层考虑引入扫描系统,如微软的 URLSCAN3.1,对应用层字符串进出进行过滤。具体配置文件在 C:\WINDOWS\system32\inetsrv\urlscan\UrlScan.ini,被阻挡的 URL 请求记录在 C:\WINDOWS\system32\inetsrv\urlscan\log 目录下,可以根据自身情况酌情修改(见图 9)。

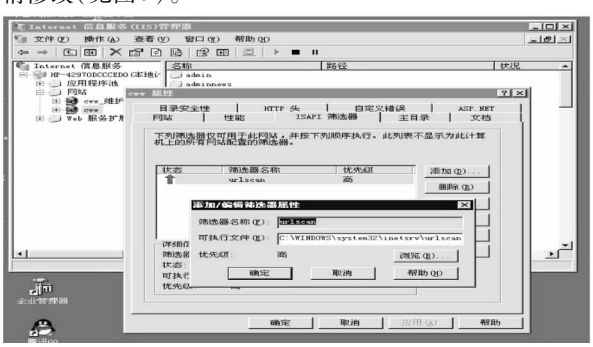

图 9 启用 UrlScan ISAPI 筛选器

4.6 强化数据库链接账号和计算机用户账号管理

为加强防护,提高访问控制力度,数据库链接账号不能够采用 SA,可以在数据库服务器中单独建立一个账号,遵从一个数据库限定一个账号的原则,这个账号一般只提供对这个库读写权限,甚至只是读取权限。这样,就算注入,也不能通过此账号建立系统账号,而 SA 特权账号则可以。对于其他有关账号的密码要符合复杂性要求,最好用字母、数字、符号的共有组合。

5 结 语

计算机网络的高速发展,对会计核算、会计信息的发布等管理领域的影响广泛而深远,财务信息化建设、财务网络管理模式等都将面临着新的机遇和挑战,高校广大财务工作人员要保持清醒的认识,既要充分利用网络环境,也要高度重视网络安全,积极探索安全高效的网络财务核算管理新途径,为高校财务事业的健康发展做出贡献[3]。

参考文献:

[1] 栗永锋. 基于校园网的高校财务信息公开化研究[J]. 财会通讯,2004(6):84-86.

[2] 冯 毅. 基于 P2DR 模型的网银安全体系方案设计[J]. 104-105.

[3] 刘俭辉. 网络环境下财务管理的安全性研究[J]. 审计理伦与实践,2003(1):54-55.

(责任校对 朱正余)