新一代银行网点终端管控平台①

吴德柱, 孙晓春

(微软(中国)有限公司上海分公司, 上海 200030)

摘 要: 分析了采用 Windows 图形化终端后所存在的管理难度大、复杂度高、监控不到位等问题, 提出了针对银行业的网点终端管控安全框架, 强调从终端管理安全策略、标准入手, 结合终端管控平台系统的建设, 在流程规范的指导下完成相关的安全任务操作, 实现终端安全管理的集约化、标准化、自动化. 重点介绍了终端管控平台系统及其参考的建设方案. 实践证明, 新一代银行网点图形化终端管控平台可以对网点终端进行全方位的管理与监控, 有效地支撑了银行业务创新能力.

关键词: 银行网点; 终端管理; 终端管控安全框架; 终端标准化; 装机车间

Management and Controlling Platform for New-Generation Graphical Terminals of Bank Counter

WU De-Zhu, SUN Xiao-Chun

(Microsoft (China) Company Shanghai Branch, Shanghai 20030, China)

Abstract: This article highlights the issues of management of graphical terminals, such as high complexity of management, lack of monitoring. A security framework of terminal management and controlling is provided with the focus on the building of management and controlling platform to solve the issues. The importance of secutiry strategies, procedures and standards is emphasized in the framework. Practice has proved that the management and controlling platform can help IT manage and control the terminals in all its aspects, effectively supporting bank business innovation.

Key words: bank counter; terminal management; security framework of terminal management and controlling; standardization of terminal; setup workshop of terminal

1 银行网点终端管控平台背景

为了提高自身的竞争力, 国内银行正在积极探寻转型, 进行业务创新. 但在国内, 很多银行终端还是采用基于字符界面的 Unix 终端, 在以客户为中心、支持业务创新方面还存在很多不足的地方, 包括柜员体验较差、无法全方位展现客户信息等问题.

为适应新业务的需求, 国内的银行开始改造营业网点, 开辟新的低柜服务区, 引入图形化终端, 为客户提供贵宾理财、个人保险等服务, 并尝试在高柜上也引入图形化终端, 进行业务流程上的再造创新.

但是在柜面上大量应用图形化终端, 大大增加了银行 IT 系统的复杂性, 为银行带来了新的挑战[1-3]:

① 图形化终端固有特性: 图形化终端由于开放性、易用性容易被随意使用, 包括修改配置、使用 U 盘等, 从而导致各种安全事故的发生.

② 网点终端管理难度大: 很多银行在各个省市都设有网点. 地域分布广、数量众多, 网点环境又可能受外来因素影响, 将使得网点终端管理难度非常大.

③ 网点终端管理复杂度高: 银行业图形化终端需要经常进行软件发布、升级等管理工作. 而且, 一般银行在管理上采用了总行-分行-支行模式, 每个分支行都可能有自身的特色, 更加剧了管理的复杂度.

④ 网点柜员安全意识与技能不足: 柜员通常重视业务安全, 但可能忽略了终端安全, 终端相关安全技能也有所缺乏. 比如终端外围设备、端口被泄露等. 还可能会像家用终端一样随意安装游戏软件等.

⑤ 网点终端管理配套体系不足: 长期以来, 银行

① 收稿时间:2012-08-27;收到修改稿时间:2012-10-20

的终端安全管理体系是围绕字符终端来展开的, 通常是被动防预. 这使得在采用图形化终端之后, 存在安全死角, 往往是事件发生并引起不良后果后才进行处理; 对图形化终端设备运行缺乏有效的全过程、全生命周期的监控管理.

2 银行网点终端管控安全框架

为了解决上述问题, 经过深入分析, 结合银行的 IT 实际现状, 建议银行采用以终端管控平台为核心的终端管控安全框架来指导新一代网点图形化终端安全管理体系的建设. 终端管控安全框架如图 1 所示.

图 1 终端管控安全框架

2.1 网点终端安全策略

独立于具体实施的、概念上的终端信息安全策略, 用来指导银行网点终端安全管理的目标和方向. 建议的网点终端安全策略如下:

① 建立安全的终端运行环境, 不受内外部攻击, 支持业务的持续创新

② 保护终端的重要资产安全, 不被泄露或损害, 增强银行的市场竞争力

③ 增强监控与审计, 与现有安全体系整合, 形成银行完整的安全体系

2.2 网点终端安全标准

定义确保终端安全策略有效执行的技术标准等具体信息. 除了国际标准、国家标准外(如《信息系统安全等级保护技术要求》), 还确立以下标准用于指导终端安全体系的建设:

① 终端硬件配置标准化, 所有的终端硬件采购在总行集中指定的范围内进行选择, 降低采购和维护成本, 提升安全管理能力

② 终端软件配置标准化, 所有安装的终端软件和应用在总行集中制定的基线中, 降低管理维护工作量, 减少安全问题的发生

2.3 安全环境

指现有银行安全运行环境以及为了终端安全而建立或采购的新安全产品或系统. 网点终端是银行 IT 运行体系的不可分割的一部分, 必须利用现有安全环境, 包括: 网络安全体系(比如办公网络与业务网络分离), 防火墙, 防病毒体系, IT 服务支持体系, 知识库等.

2.4 安全任务

人员在图形化终端执行的任务或动作的定义. 通过对不同任务的定义, 实现基于策略的管理, 包括但不限于:

① 开机、登录、注销、关机

② 拷贝、删除、移动文档

③ 接入外设、开启 U 盘/光盘

④ 网络访问.

2.5 安全流程

为确保安全策略的执行而设定的执行过程. 通过建立规范的管理制度和流程, 提高终端管理的规范性. 网点终端必须要考虑以下流程的安全可控:

① 终端采购/领用/替换/报废流程

② 终端安装流程

③ 终端接入控制流程

④ 补丁管理流程

⑤ 软件分发流程

⑥ 病毒库更新流程

⑦ 终端安全应急处理流程

2.6 人员

人员是终端管控安全框架中非常重要一环, 包括 IT 人员和终端用户的意识、技能以及权限. 终端管控安全框架必须强化终端安全培训, 提高相关人员对安全管理重要性的认识并促使其积极参与, 建立“谁主管谁负责、谁运行谁负责、谁使用谁负责”的绩效考核体制.

2.7 终端管控平台

终端管控平台是整个终端管控安全框架的核心, 通过将策略、标准、流程等固化在终端管控平台系统中, 驱动人员与任务, 实现集中管理, 统一监控, 管理流程自动化. 终端管控平台系统至少必须包括的功能如下:

① 软硬件标准化信息管理

登记终端软硬件信息, 并根据标准化要求设定基线, 定期统计、汇总终端的使用情况, 及时发现非法软

硬件的安装和使用, 以便及时采取措施.

② 自动化装机管理

根据终端软硬件标准化, 统一制作操作系统及应用装机镜像, 进行操作系统的自动化安装, 无需人工的干预. 同时, 提供个性化安装配置.

③ 终端准入控制管理

终端准入控制从网络访问开始, 通过主动发现终端, 并实时监控其安全运行情况, 对不符合接入策略的终端自动隔离并进行修复, 解决安全接入和认证问题. 通常需要网络设备配合.

④ 终端安全策略管理

通过集中化的管理, 对不同类型的客户端制定不同的管理和安全策略. 包括准入策略、桌面安全策略、外设使用策略、文件访问策略等等.

⑤ 软件分发管理

应用系统客户端的安装和更新, 均可采用集中管理、集中分发的方式实现, 保证银行内部各种软件的版本统一, 提高工作效率; 保证各种新业务系统、应用系统的推广工作.

⑥ 系统补丁管理

制定系统补丁管理流程, 实现补丁的定期自动更新、手工强制更新. 系统补丁需要经过测试验证.

⑦ 终端日常监控与审计

能够监控当前终端的网络状况、运行情况、病毒信息、安全事件日志等, 在发生安全问题时自动报警. 同时, 对终端进行日常审计, 检验相关安全策略执行效果, 确保终端使用合规性.

⑧ 客户端协助

为柜员提供一个日常协助、排错、诊断助手功能, 提高柜员的工作效率和对 IT 服务的满意程度.

⑨ 开发接口

一方面, 终端管控平台系统需要提供标准化的、开放的接口, 供第三方系统访问相关的数据; 另一方面, 还要有一个灵活的接口构架, 可以很方便地整合其他系统, 实现互联互动.

综上所述, 以终端管控平台为核心的终端管控安全框架, 结合银行现有 IT 安全平台, 从安全策略、标准入手, 在安全环境支撑下, 通过终端管控平台的建设, 实现终端安全管理的标准化、自动化, 只允许人员在流程规范的指导下完成相关的操作或任务, 从而形成一个集中统一的、全方位的、主动式的图形化终端管控体系, 可以有效地解决银行网点多、终端管理难度大、复杂度高、使用不规范等问题.

3 网点终端管控平台建设方案

终端管控安全框架的核心是终端管控平台, 因此重点介绍终端管控平台的建设方案. 目前, 与图形化终端管控相关的产品主要有微软公司的系统管理软件 (System Center Configuration Manager, SCCM)[4,5], 赛门铁克公司的 Altiris 管理软件以及蓝代斯克公司的 LANDesk 管理软件. 现有各个银行在网点部署的图形化终端绝大部分是基于 Windows 操作系统. 所以, 在建设网点终端管控平台系统时, 考虑到成熟性、集成性、兼容性和可实施性, 这里选择了微软公司系统管理软件 (SCCM) 与微软部署工具软件 (Microsoft Deployment Toolkit, MDT)[6], 并采用管理门户技术 (Portal)来构建集成式的网点终端管控平台系统. 一个参考架构如图 2 所示.

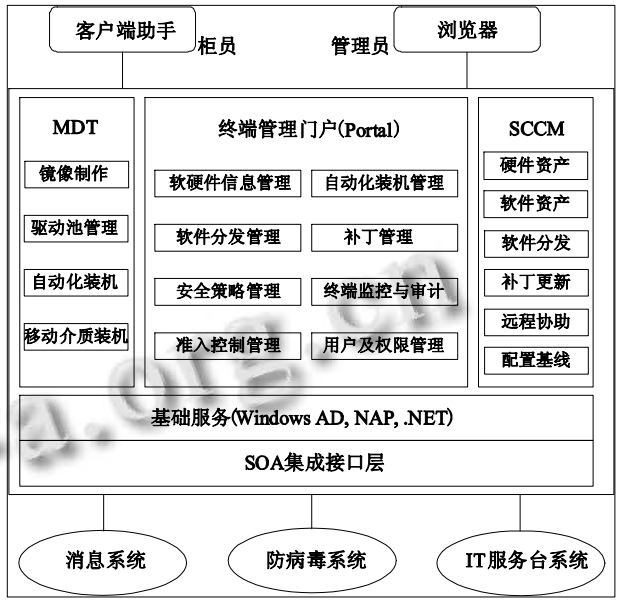

图 2 网点终端管控平台系统参考架构

网点终端管控平台系统参考架构主要由六个部分组成. 其中客户端助手部分部署在网点终端, 其余部分部署在总行数据中心:

① 客户端助手

客户端助手部署在网点终端, 主要包括有准入控制、日常监控、行为审计、远程协助、错误诊断等功能模块. 客户端助手通过 Web Service 方式与总行端系统交互.

② 微软部署工具软件(MDT)

微软部署工具软件 MDT 提供了自动化部署/装机功能，包括了镜像制作、自动化装机流程定制、驱动池管理、移动介质装机定制等功能，很好地实现了硬件与驱动程序的分离、解决远程网点安装带宽不足的问题. 同时，MDT 提供了丰富的接口，方便与其他系统模块的互连.

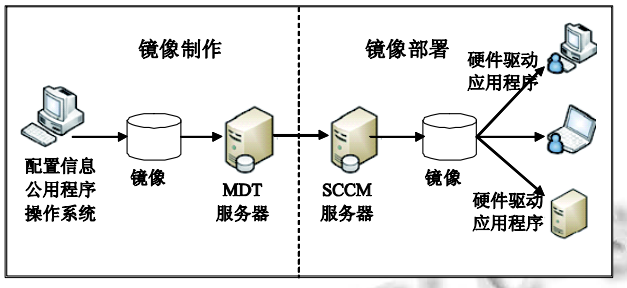

图 3 MDT 装机部署

基于 MDT，银行可以根据需要，在总行、分行建立装机车间. 装机车间是批量部署终端操作系统的场所. 装机车间使用已有的镜像，对新的终端或已有的终端进行客户端系统的自动化安装. 通过装机车间“生产”的终端，都是标准化终端，从而大大提升了终端安全性，提高了工作效率.

③ 微软系统管理软件(SCCM)

SCCM 通过流水线式的自动化管理方法对 PC 终端进行全生命周期的管理：从操作系统的安装到应用程序的安装/更新、补丁的更新(包括防病毒更新协同)以及软硬件信息监控与收集、基线定义与分析、远程故障协助等，为 PC 终端管理提供了一个全方位的管理视图. SCCM 还提供了开发接口和自定义配置，方便与其他系统模块的互连.

④ 终端管理门户(Portal)

终端管理门户为总行、分行管理人员提供了一个统一的入口与完整的管理视图. 通过统一的标准方式，终端管理门户使得桌面管理必需的信息可以从不同的存在地点、以不同的表现形式、在权限控制下方便地提供给总行、分行管理人员，成为快速方便获取管理信息、进行管理操作的大门. 终端管理门户表现在用户面前的，就是一个简单的、个性化的、集成的和统一的界面和环境.

⑤ 基础服务层

基础服务是网点终端管控平台系统的运行支撑，包括 Windows 活动目录(Active Directory, AD)[7,8]，网络访问保护(Network Access Protection, NAP)[9]，.NET 运行平台等.

Windows 活动目录 AD 保存着终端用户信息和终端资源，是实现终端安全管理和基于策略管理的基础，有利于终端管理标准化的实施，简化终端用户管理，加强终端安全性.

Windows 网络访问保护(NAP)通过终端健康状态检查、判断终端是否合规、从而决定是否允许终端访问网络来实现终端准入控制.

⑥ 集成接口层

基于 SOA 的集成接口层为终端管控平台系统提供了一个基于面向服务构架(Service-Oriented Architecture, SOA)的应用集成接口服务，从而使得终端管控平台系统可以灵活地与现有银行安全服务体系集成，成为银行安全服务体系中不可分割的一部分. 比如可以在预警时通过邮件系统发送消息，在需要支持时与 IT 服务台系统关联等.

4 实施效果

在终端管控安全框架的指导下，采用第 3 节所述的建设方案，国内一商业银行在 6 个月内建设了新一代网点终端管控平台系统. 在此平台上，通过整合防病毒系统、IT 服务台系统、消息系统等，制定终端标准化与管理流程，建立制度规范，银行 IT 管理部门实现了全方位、自动化、标准化的终端管理体系，达到了“可管理，可控制，透明化”.

① 建立了终端管理门户，全面集中管理，提升安全管理水平，提高工作效率

终端管理门户展现了全行终端统一管理视图，使得总分行管理人员可以有效地、全面地、准确地掌握每台终端的软硬件信息、安全配置情况以及使用状况，大大提高了工作效率，解决了网点终端多、管理难度大、复杂度高等问题. 比如：分行管理人员通过浏览器就清楚地知道网点终端是什么时候开关机的，哪个柜员登录过，安装了哪些硬件及外设、什么型号，安装了哪些软件、什么版本等，而以前需要人工电话询问或者每隔一段时间到现场去一台台登记；装机车间使得终端部署标准化、流程化、自动化、并行进行，从原先要花费几天甚至几周的分行终端上线安装工作缩减为几十分钟.

② 建立了集成 IT 运维支撑系统的统一终端监控平台，实施主动防范

建立了全行终端统一监控视图，并由专门的安全团队负责监控信息，包括终端接入情况、运行状态、病毒信息、安全日志、补丁情况、合规信息等，并与消息系统(邮件、短信)、IT 服务台系统相关联，及时响应，解决了网点柜员安全意识不够等问题，弥补了原来字符终端被动管理体系上的不足. 比如：总分行管理人员第一时间可以知道哪台终端中毒并进行隔离，强制进行补丁升级.

③ 形成了全行终端标准化体系，统一流程规范，节约成本，降低风险

建立了全行终端的标准化，制定了一系列的管理流程、制度与规范，实现了终端管理的标准化、自动化和系统化. 原先，终端都是由分支行根据自身的标准进行管理的，各式各样，即便是总行推行的一些制度、流程、规范等，也难于真正的贯彻实施. 现在，终端管控平台上固化的标准化要求，在降低采购成本的同时，减少了因为终端配置原因而导致的终端使用问题；而统一的终端管理流程与制度，规范了终端用户行为，降低了终端固有风险. 比如：柜员现在是无法随意乱装股票软件、乱插 U 盘等.

④ 形成了以柜员为中心的终端使用环境，强化安全意识，提高了 IT 服务满意度

建立了以柜员为中心的终端使用视图，围绕柜员行为、柜员技能、柜员安全事故等多方面进行审计、考核，促使柜员安全意识的提升；同时，为柜员提供更多的服务，包括知识库、远程支持与协助，及时解决在终端使用中出现的问题，提高了柜员满意度. 比如：柜员可以通过客户端直接与总分行的支持人员进行沟通，并在柜员授权许可的情况下，共享终端操作权限，快速解决问题，而原先可能需要隔天到现场去解决.

⑤ 管控平台推动了业务创新，增强了市场竞争力

终端管控平台系统的投入使用，在极大提升终端安全管理能力的同时，减轻了总分行管理人员的工作量，从而促进了银行向图形化终端迁移的进程，加快了业务的创新，为银行在市场竞争中取得了先机. 目前，客户银行已经在全行几十个分行分批向图形化终端迁移，实施以客户为中心的新一代网点平台系统.

5 结论

基于终端管控安全框架指导下的网点终端管控平台系统，充分考虑了国内银行业务创新需要及 IT 系统安全建设现状，在保护现有投资的情况下，通过管理集中化、终端标准化、流程自动化、策略强制化，构建了统一的终端安全管理体系，实现终端安全管理一体化，保证业务的稳定运行，促进业务的创新，提升市场竞争力.

实践证明，建立基于终端管控安全框架的网点终端管控平台系统是银行业务创新、提升竞争力的有力保证.

参考文献

1 刘威.网点终端安全治理的方法.中国金融电脑,2011,4:53–57.

2 王健肃.桌面终端安全管理的应用和探索.金融电子化,2009,6:77–78.

3 赖劲松.商业银行终端桌面安全解决方案的构建.中国金融电脑,2009,4:58–61.

4 毛振中,蒋国良.运用 SCCM2007 使 IT 资产管理更简单.电脑知识与技术,2010,6(33):92–92.

5 孔建蒙.系统管理员的好帮手 SCCM.中国传媒科技,2010,6:28–29.

6 Layfield R.使用 MDT2010 将 WindowsXP 迁移到 Windows7 迁移你的操作系统和应用程序.Windows IT Pro Magazine 国际中文版,2011,1:26–31.

7 许文明.浅谈 WindowsServer2008 活动目录的组策略部署.计算机光盘软件与应用,2011,22:113–114.

8 龚秀琴,张桂芬.Windows Server 2008 中 Active Directory 域的配置管理.数字技术与应用,2012,2:155–156.

9 梁林.Windows Server 2008 NAP 如何保护企业内部网络.Windows IT Pro Magazine 国际中文版,2008,3:26–29.