[趋势科技成功案例]

趋势科技 TDA 为中国农业银行风险管理“出谋划策”

数十万终端不留“威胁死角”

IT 技术日新月异的发展为中国农业银行（以下简称：农行）的业务创新与管理创新带来了革命性的变化。然而，在病毒攻击多元化、Web 恶意代码爆发增长的今天，如何实时监控到数十万台网络终端，全面保护办公与业务服务器；如何防止网络罪犯攻击到相对薄弱的基层网点，这些都成为农行 IT 风险管理所需要面对的突出问题。

为此，农行携手全球服务器安全、虚拟化及云计算安全领导厂商——趋势科技，通过趋势科技威胁发现设备（TDA）在试点应用中取得了最佳的实践经验，进而进行了全行推广，并利用威胁管理服务平台（TMSP）实现了 IT 风险管理的全网覆盖。

“200 多万”条病毒攻击日志数量　TDA 试点效果显著

网络技术为商业银行的经营管理、产品创新和风险控制提供了新的思路、方法和工具，也成为银行在激烈的市场竞争中抢占制高点的关键要素。但是，网络的开放性也为黑客敞开了大门，网络罪犯希望攻击尽可能多的银行，以获取最大利益。其次，互联网生态环境的逐步恶化，使得病毒及其变种在黑色产业链中的滋生速度更加迅猛，而银行用户在不断变化的威胁面前已变得势单力薄。

从农行信息化建设的整体情况来看，领导层的 IT 风险管理意识都非常强，核心业务系统和数据中心建设不断完善，应急体系的建设也取得了较大的进步，提升了网络风险的管控能力。但是，IT 风险具有隐蔽性，在日常管理难以发觉。目前，农行主要业务流程均已实现信息化，业务的开展主要依托信息平台，以及每个终端的安全高效运行。但是，终端操作系统和应用层面本身的脆弱性给风险管理留下了缺陷，风险只有通过“上报”方式才能逐渐被发觉。尤其是在基层银行，由于受到先天资源不足、技术人员匮乏等因素的影响，IT 风险管理优势正在被逐层削弱。

为此，从 2007 年开始，农行就与趋势科技联手展开了病毒防护体系的建立工作，至 2012 年，防毒软件已经覆盖了所有终端和 PC 服务器。为了更好地评估全行范围内病毒流量分布情况，对于病毒攻击能够及时准确预警，避免病毒在全行蔓延，2010 年下半年，总行启动了生产网病毒流量监测系统项目，并在部分一级分行单位试点部署趋势科技威胁发现设备 TDA，截止到 2012 年 5 月，TDA 记录的病毒攻击日志数量达到 200 多万条，涉及的病毒攻击源数量达到千余个，并且各单位管理员对所发现的病毒攻击源可以及时处理，消除了病毒传播的安全隐患。

农行 TDA 项目负责人冯涛表示：TDA 主动发现病毒威胁源头和恶意攻击流量的效果十分明显，因此，在 2012 年初，总行防病毒项目组对 TDA 监控方案进行了优化调整，监控区域从生产网络扩展到部分办公网络区域。同时，为了全面掌握全行范围内病毒流量扩散情况，农行决定在全行推广趋势科技的 TDA 产品。

TMSP 形成全网威胁监控平台 风险管理报表“每日必达”

据了解，由于集成了趋势科技云安全中的“多协议关联分析技术”，TDA 可全面支持检测 2-7 层的恶意威胁。TDA 可通过“数据包”和“会话”视图对这些主机通讯的数据进行自动关联分析，即从云端数据库进行比较，自动将占用网络带宽的应用和造成网络通讯拥塞故障的信息建立威胁关联。

在农行第一阶段的试点部署中，TDA 起到了“主动”发现的效果，尤其是在木马检测、僵尸程序检测、、蠕虫病毒扩散等非法流量检测方面，TDA 能够快速定位 “威胁”来源， 基本上做到“秒”级的预警功能。但以上这些特点，都只能说明技术上的突破，而对于更注重全局效应，风险管理报表呈交时间尽可能短的银行风险管理要求，TDA 又是如何帮助农行实现所有支行、所有网点、所有终端统一管理的呢？

据冯涛介绍：为了实现威胁事件的统一管理，在第二阶段，农行将趋势科技提供的 TDA 威胁事件分析展示系统采用了“总分”两级的部署方式。通过在总行端部署总控 TMSP，收集各单位集成在 TDA 设备里的分控 TMSP 相关数据，自动在每天生成综合报表，为全面评估全行病毒流量分布情况提供必要的依据。另外，高风险事件也实时上报到总控 TMSP 端，让总行人员可以立即掌握全网恶性事件。同时，农行将 TDA 注册至 TMCM（趋势科技防毒墙控管中心）上，进行了产品特征码的自动更新， 保障了全局安全策略的一致性。并且，从分行 TMCM 上，也可以单点登录 TDA 进行远程统一管理。

“TDA+TMSP”等于“技术+管理”

从我国银行业的风险管理体系结构来看，风险管理已经渗透到银行业务的每一个环节，包括了识别、计量、监测、报告和缓释等不同类型的业务活动。由于风险管理的有效性取决于数据分析和决策支持，这就需要按照各种风险管理模型和报表规则，进行风险状况的识别、计量和监测，并实时报送给各层级风险管理人员。

而趋势科技所提供的 TDA+TMSP 威胁解决方案，从技术和管理两个角度，都为中国农业银行提供了更加全面的风险评估手段。针对网络威胁，这种组合模式可以更直观、多样、实时、统一的提供可见性和深入分析，以便安全专业人员可专注于实际风险、进行深入的取证分析并快速实施抑制和补救措施。

###

关于趋势科技（Trend Micro）

趋势科技是全球虚拟化及云计算安全的领导厂商，致力于保障企业及消费者交换数字信息环境的安全。趋势科技始终秉持技术革新的理念，基于业内领先的云计算安全技术(Smart Protection Network)核心技术架构，为全世界各地用户提供领先的整合式信息安全威胁管理技术能防御恶意软件、垃圾邮件、数据外泄以及最新的 Web 信息安全，保障信息与财产的安全。同时，遍布全球各地的 1,500 余名趋势科技安全专家可为各国家和地区的企业级个人用户提供 7×24 的全天候响应及技术支持服务。更多关于趋势科技公司及最新产品信息，请访问：www.trendmicro.com.cn。请访问 Trend Watch：www.trendmicro.com/go/trendwatch 查询最新的信息安全威胁的详细资讯。