防病毒整体外包服务帮助提升光大银行整体安全水平

随着银行业务的迅速发展，银行业务的连续性对计算机网络的依赖程度越来越高，如何保证银行内部网络的稳定，避免病毒侵害内网核心网络对银行业务造成影响，成为银行业关注的焦点问题之一。中国光大银行采取了防病毒整体外包的方式，针对病毒问题构建起了一整套包含主动发现问题，及时处理问题，实时跟踪进度，总结经验教训的良性循环的病毒防范体系，以便适应现代银行业发展需要。

传统的病毒防护模式无法满足银行发展的需要

随着银行业务的不断发展，中国光大银行在全国各地建立起了越来越多的支行网点，随之而来的是支行网点的计算机维护给总行和分行的科技部人员带来巨大的工作量，分行的防病毒管理员就像消防救火员一样每日穿梭于各个支行网点，而最终结果却不尽人意。

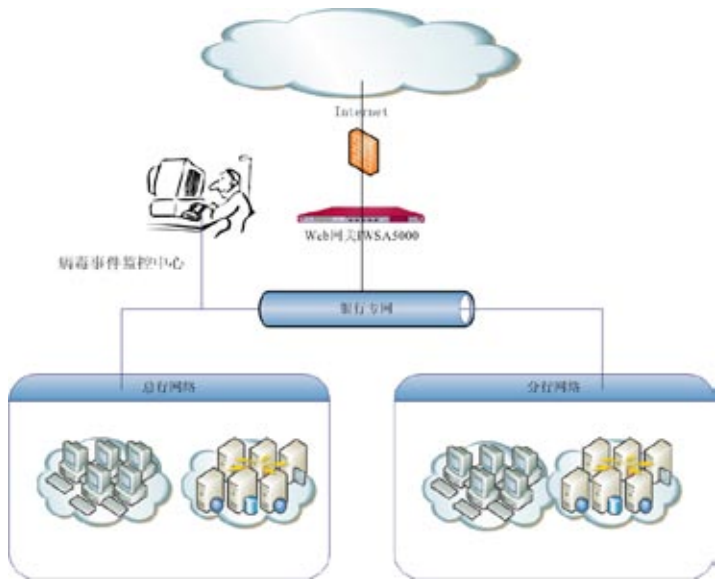
是防病毒产品的问题？中国光大银行安全处经过全面调查与分析找出了威胁银行办公网络的根源： 首先，传统的病毒防护模式面对病毒只能采取被动防御的策略，只有当局域网络受到严重攻击的情况下才会通知管理员，然而往往为时已晚；其次，作为一家网点遍布全国的金融服务机构，光大银行无法在每一个网点都配置专业的技术人员，分行的防病毒管理员大都没有经过专业的防病毒技能培训，有的分行甚至没有专职的防病毒管理员，这就让一些小的隐患无法解决，从而累积成大问题；第三，病毒技术随着网络的发展也是迅速发展，病毒种类也爆发式增长，单一的桌面端防毒已经很难有效制止病毒的感染。

在分析出上述原因之后，光大银行安全处认为要想改善防病毒状况，必须要建立一套能够主动监控的防病毒安全系统，它既能发现病毒的感染情况，在发现之后还能够及时处理，在处理过程中能够时时跟踪直到问题解决；同时为了提高分行人员的专业能力，还需要定期对分行安全人员进行技能培训，提高工作效率；最后为了阻断病毒的传播，需要在Internet出口处增加病毒防护设备，以减少桌面端的压力。

此外，银行网点数量多、覆盖地域广、安全技术人员紧张的特点，让光大银行无法完全依靠行内安全技术人员来建立新的防病毒体系，需要引入专业的防病毒厂商来协助搭建新的防病毒体系。

整体外包服务助光大银行建立新的防病毒体系

为了能够减缓安全技术人员短缺的压力，同时提高整体的防病毒水平，光大银行科技部采用防病毒整体外包的模式，引入了专业的防病毒服务厂商趋势科技，由原厂专家为光大银行提供专业的防病毒支持服务。为了提高光大银行整体的防病毒水平，趋势科技通过以下几种方式建立起了一套新的防病毒系统，如下图所示：



该系统主要通过以下几个部分组成：

一、 全天候的病毒事件监控中心（MOC）：通过在总行搭建病毒事件监控中心，监控中心由趋势原厂专家进行监控，收集分行的病毒日志，并对各分行定义合适的各种病毒相关事件KPI，实现24小时监控，一旦发现问题，系统自动通知分行进行处理，原厂专家会在问题处理过程中对分行提供远程支持，同时系统还会对事件进行自动跟踪，在直到事件处理完毕才会停止报警。该系统实现了病毒问题的主动监控，及时处理以及自动跟踪。

二、 Web网关处病毒过滤：通过在总行和分行的Internet出口处部署趋势的Web防病毒网关IWSA5000，对internet访问进行过滤，避免计算机由于访问恶意网站而感染病毒。

三、 组织全行的防病毒培训：为了提高分行防病毒管理员的专业技能水平，科技部每年组织全行的防病毒管理员集中进行培训，由趋势科技专业讲师为学员提供专业的防病毒技能培训；同时趋势科技每月为光大银行定制针对普通员工的安全小贴士，通过诙谐幽默的方式将一些防毒小技巧和注意事项告知给普通员工，提高员工的安全意识。

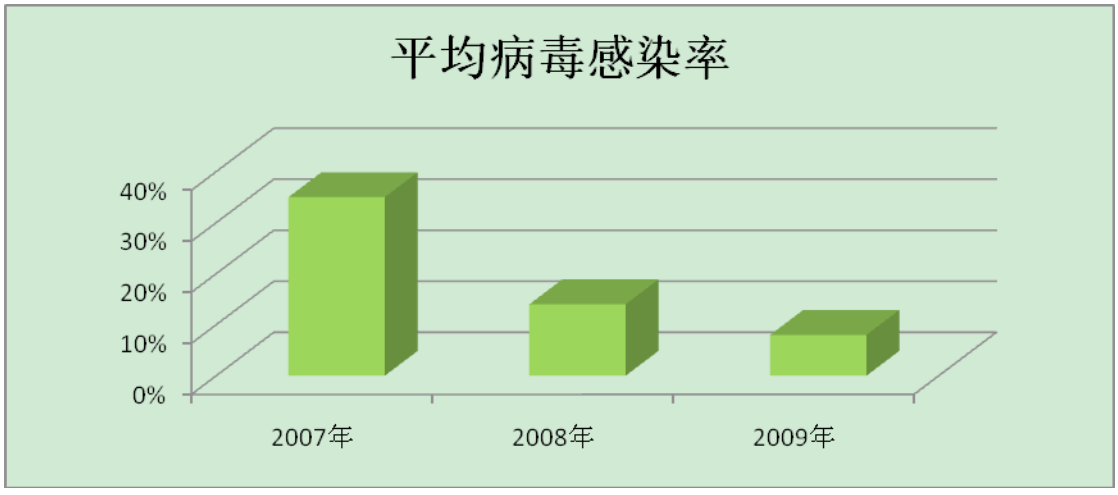
四、 组织全行的防病毒巡检：为了了解分行的具体情况和困难，光大银行总行与趋势科技每年组织对分行的巡检，通过现场调研的方式，了解分行的具体困难，同时对能够解决的问题提供现场解决方案，对于需要后续跟进的则制定详细的计划方案，并指定相关人员进行跟踪，直到问题解决。

新的防病毒体系提升光大银行整体防病毒水平

“病毒问题是个筐，什么问题都能往里装”，这是在部署新的防毒体系之前，光大银行病毒问题负责部门对防病毒工作的难点的经典描述。

通过实施防病毒外包服务，经过两年多的共同努力与完善，目前光大银行已经建立起了一套完善且行之有效的防病毒体系。且通过两年多的外包服务，光大银行的整体防病毒水平有较大的提高，其全行办公网月均病毒感染率由2007年的35%左右下降至2008年的14%左右，至2009年更是下降至10%以下；生产网未出现一起病毒事件。防病毒外包服务有效的保证光大银行业务的连续性，提升了整体的防病毒水平。

现在防病毒项目负责人表示“自实施防病毒外包以来，普通用户的报警少多了，开会的时候也不再有人说病毒问题了，感觉轻松了好多。”



光大银行近3年病毒感染率情况