证券交易背后的“安全故事”

——趋势科技 TDA 全面纳入 IT 运维流程　中原证券实现网络安全无忧管理

中原证券股份有限公司（以下简称中原证券）成立十年来，坚持规范发展、稳健经营的指导思想，融合了国内一流券商先进的管理经验，全面搭建起了综合券商的管理框架和网络平台，各项业务都呈现出良好的发展势头。中原证券作为国内非常有竞争力的证券企业，信息化建设长期以来持续发展，支撑着整个企业的所有业务运营，但随之而来的网络安全压力也越来越大。

全力避免威胁事件发生 杜绝资料外泄

中原证券 IT 技术部总经理韩先生认为：“对于越来越狡猾的网络袭击，证券网络系统上流动的巨大财富无疑会吸引无数‘冒险家’铤而走险。我们警惕网络中的每一个威胁事件，因为这些风险都可能造成客户资料丢失，企业的机密资料因网络漏洞而招致外泄损失。所以网络安全问题也就成了证券行业的关键性问题，保护网络安全，就是保证财产和用户安全，保护公司的生存。”

韩总的担心是非常正常的，根据趋势科技的最新统计结果显示，如今每 1.5 秒的就涌现一个新的网络威胁，仅趋势科技的云安全中心，一天就内就能拦截上亿个带有危险的档案。因此，某一个终端一旦因为漏洞被入侵，内部网络中的所有客户端都可能因为“共享机制”的存在，在几秒钟内被病毒内嵌的扫描功能侦测到，进而改写重要的系统文件，甚至成为新的攻击源。证券公司需要在第一时间发现威胁、准确定位、及时处理，避免恶意程序相互感染，以及进入到核心数据区。

第一时间定位威胁 有效避免 APT 攻击

中原证券 IT 技术部针对上述需求，对网络安全产品市场和最新的技术动向都进行了深入的调研。在针对 IDS、IPS 和网关型防毒产品进行比对之后，技术部发现趋势科技企业威胁管理解决方案中的威胁发现设备（Threat Discovery Appliance,简称 TDA）与这些产品有着本质上的区别。TDA 实现了传统安全设备无法实现的多重协议侦测、直接预警分析、零日攻击、未知病毒检测、专门针对内部网络功能设计，以及最重要的根源分

析功能等。由于中原证券的网络分为了互联网、办公网和交易网 3 大网段，因此将 3 台 TDA 6000 分别被放在这三个网络的核心交换的位置，并通过端口镜像的功能实现了透明接入。

中原证券专门负责安全管理的王先生表示：“之前，我们使用趋势科技的 OfficeScan 部署在每个终端设备上，已经少有病毒事件发生。现在部署在交易网和互联网访问网段的两台 TDA 都起到了 7×24 小时监控作用，使得这两个网络的安全防御等级得到了进一步提升。而在相对薄弱的办公网段，TDA 的作用和细节上的所有功能都得到了全面的发挥。在部署 TDA 之前，如果出现终端感染事件，网络数据传输可能因异常流量出现延迟，或因其它原因出现中断、停顿或数据错误现象，从而使得业务系统出现延迟、停顿或中断。技术工程师要对所有机器逐个进行筛查，才有可能解决问题，这会给用户和证券公司造成非常大的损失。”中原证券对这 3 台 TDA 的部署和应用都十分满意，并且对网站、交易系统、内部办公平台的性能提升和稳定性，以及证券公司网络安全制度的落实都显得非常关键。

据了解，由于高级持续性威胁（Advanced Persistent Threat，APT）的广泛出现，极可能造成证券企业数据中心业务数据泄露，因此越来越多的金融和证券企业开始对 APT 高度关注。中原证券及时对 TDA 的引入，有效地避免了员工和高级主管个人电脑被恶意代码植入的风险，在第一时间将这些威胁“扼杀在摇篮之中”，从而降低了交易网和数据中心的风险防御压力。

IT 服务持续改进　TDA 纳入运维流程

中原证券在对自身安全体系不断加强的同时，IT 标准化运维的项目也在加紧实施过程中。在 IT 标准化运维中（如：ITIL、ITSM、BSM），安全服务等级、事件流程、控制台中都缺少不了预警和监控系统的支撑。由于 TDA 可以实现将预警和报表信息都纳入到中原证券的 IT 服务流程中，一旦出现预警信息便会立即启动设计好的事件流程。因此，TDA 便可起到了“关键岗位、关键人”的作用。同时，由于中原证券整体的安全产品都配合使用了趋势科技提供的 PSP 服务（专属咨询服务），一旦发现未能处理的信息和可疑的流量，中原证券都会得到趋势科技技术客户经理（TAM）的电话和现场支持，服务水平和应急能力也得到了进一步提升。

随着中国证监会和相关指导部门的组织协调，中原证券和相关单位正在筹措私有云和虚拟化进程，其中虚拟化应用已经部署在非核心业务服务器上，而虚拟化防毒和数据中心威胁防护也在进一步测试当中。在私有云和虚拟化进程中，趋势科技凭借 Deep Security 在虚拟化防毒领域的技术优势，已经被中原证券列为重点关注的产品。与此同时，下一阶段中原证券将与趋势科技联手，对证券行业中不同网络和系统的安全等级设定进行深入研究，并将其研究结果付诸于实践。