风险管理提上日程 “所见即所得”的威胁消除能否实现？

——趋势科技TDA服务于“中石油长庆油田公司第七采油厂”内网安全

能源企业需要依靠信息网络技术来提升管理效率、提高安全水平和帮助企业节约成本，可以说，一旦数字化信息网络系统瘫痪，企业所造成的损失难以估量。因此，目前多数大型能源企业均把网络安全保障看作是企业发展的根本，中石油长庆油田公司第七采油厂（以下简称第七采油厂）拥有这样一支专业的信息网络管理团队，为数字化油田的稳定运转保驾护航。

第七采油厂的网络基础平台承载着企业绝大多数的业务系统，一直以来厂部高层领导非常重视信息安全基础建设。针对信息安全中的风险管理，IT团队利用趋势科技提供的威胁发现设备（Threat Discovery Appliance，以下简称TDA），通过镜像方式部署在核心交换机上，形成了全面威胁发现的统一平台，并通过监控网络层的可疑活动定位恶意程序，让集成“云安全”技术的TDA充分结合到了风险评估管理工作中。

内部威胁成为安全“短板”

第七采油厂开采区域横跨陕西、甘肃两省，目前矿权面积为4000余平方公里，是长庆油田公司建成的第一个百万吨数字化采油厂。第七采油厂厂机关与两个前线指挥部“三地”地域跨度大，网络接入端分散等现实条件，造成了网络架构松散、统一管理难度较大。从2009年末开始，第七采油厂进行了大规模的网络改造项目，最终实现了统一网络汇聚的格局，并形成近20台服务器、1000台客户终端的网络规模。

第七采油厂的信息网络业务围绕着数字综合管理平台展开，其中包括了OA协同办公、外网和内网电子邮件、视频监控、安全监控、生产管理、视频会议系统等多个子系统。为了保证这些系统的安全稳定运行，IT管理人员不但安装了防毒软件、防火墙等必需的安全设备，还对照重要等级，把信息系统进行了多次安全评估。但随着信息系统和终端用户数量的不断增加，IT管理人员发现，为应对黑客入侵，都把重要的安全设施集中在核心机房、网络入口处，在这些设备的严密监控下，来自网络外部的安全威胁大大减小了，然而，来自网络内部的安全威胁却渐渐地突显出来。能够在内网中存活的恶意软件数量和漏洞的载体越来越多，包括：服务器、桌上型与笔记本电脑，传统电子邮件客户程序、企业与个人网页式邮件、网页浏览器、协同作业环境、企业与个人移动装置、实时通讯客户端、USB 和手机储存装置等等。尤其是办公网络的相对开放性，使得下一步将开展的网络风险评估工作，会出现异常繁琐的情况。

第七采油厂信息管理人员认识到：“针对客户端的安全级别往往难以保证，这对于现在这样的规模，以及内网用户数量众多的同行业单位更为如此。使用版本陈旧的操作系统、长时间不更新个人防火墙和杀毒软件、安装具有潜在安全漏洞的软件，这些都将成为局域网安全中的‘短板’。因此，要进行内网安全建设，首当其冲要全面了解系统存在的漏洞，评估系统安全性，认识到自己的风险所在，从而才能迅速、准确的解决内网安全问题。”

“有证可依”提升网络健康水平

风险源于周围进行的操作决定和结果的不确定性，“不确定性”会将我们陷入安全管理的泥潭。通过介绍，我们了解到，第七采油厂在网络升级之后的一段时间里，因为厂有些同事反应计算机变慢和上网速度变慢，网络管理人员通宵进行网络监控查找原因，想了解是什么威胁造成了厂网络及计算机变慢。通过对多台样机进行分析，终于发现是由于Worm_Down 蠕虫病毒感染造成的，虽然已经处理了几台计算机，但是感染的情况还是没有有效解决。那么，第七采油厂的网络内到底还有哪些威胁呢？他们自己心理也没有底，不知道何时又会出现这种高危事件的感染，这必然让大家加班不断，烦恼不断。

其中一位网络工程师表示：“由于追查每一种最新感染源的工作非常繁琐，同时我们发现网络安全的早期设计是‘外刚内柔’型的，所以，随时随地的搞清楚网络里面到底跑着什么诡异的东西，是我们马上要开展的工作。我们之前做过一些安全评估工作，对趋势科技和其他安全厂商咨询之后，发现TDA在安全评估和威胁管理上，都可以帮助我们将计划落实。”

据了解，第七采油厂在对市场上的安全产品调研时发现，趋势科技TDA的基本功能是检测企业内部网络中的安全威胁和破坏，但最能符合“风险评估”的因素有两个：一个是由于采用了独有的云安全技术，因而对于 TDA 的日志可以配合各项信誉服务，进行交叉分析，这为IT部门提供更精准的分析内容。另外一个是报表服务，发现隐藏威胁，提供精准的威胁报告，定位感染源，事故分析以及威胁建议。这几大功能，都可以将信息安全工作量化，符合了近期和未来发展的需求。

数字化信息中心表示：“采油七厂不能停留在出现问题、解决问题这个层面上，我们开始尝试引进PDRR安全模型，动态的管理网络，形成信息安全周期的管理。为了摆脱采用头痛医头，脚痛医脚的方式，TDA的报表功能在PDRR的四个组成部分都能起到至关重要的作用。通过近半年时间，我们严格的把报表中的威胁一一排除，病毒感染的频率正在逐渐减少，这些都能看在眼里，行动出来，最后把主动权牢牢抓在自己手中。”据了解，第七采油厂数字化信息中心提到的PDRR模型，是由4个英文单词的头字符组成的缩写，这包括：Protection（防护）、Detection（检测）、Response（响应）、Recovery（恢复），这四个部分构成了一个动态的信息安全周期，如今已被很多企业采用。

针对第七采油厂的成功经验，趋势科技xxx认为：“风险管理是确定威胁的存在，并决定如何应对的过程。对于特定企业的生产系统（第七采油厂的生产和数字管理平台）更容易被他们的 IT 环境问题所影响，而导致服务中断，因此我们所讲的风险管理变得越来越重要。按照行业安全流程的文字规定，自觉的执行一套完善的安全风险防范管理系统，是非常困难的一件事情。但不能否认，我们已经进入到一个风险管理的时代，TDA正是可以帮助、督促你去执行这套策略的工具。”