网络安全防护中的“标杆管理”

——趋势科技携手淄博矿业集团构建全球领先的防病毒体系

“标杆管理”是站在全行业、甚至更广阔的全球视野上寻找基准的方法论，同时它也是企业管理活动中支持企业不断改进和获得竞争优势的最重要的管理方式之一，其核心驱动力在于不断完善和持续性改进。标杆管理的引入在网络安全防护工作中的意义非凡，因为企业要不断完善网络安全架构的合理性和完整性，从而应对实时变化的威胁入侵。

淄博矿业集团有限公司（简称“淄矿集团”）在近5年里，持续利用趋势科技的OfficeScan网络版防病毒软件、网络病毒墙NVWE、防毒墙控管中心TMCM、主动式威胁发现设备TDA，以及网关Web病毒和内容过滤设备IWSA，在网关、网络接入、内网安全监控与终端防护上形成坚不可摧防护罩，层层排除隐患，为网络平稳运行提供了有效保障。

企业内网一样存在“蝴蝶效应”，制度不能是一纸空文

淄博矿业集团有限公司（简称“淄矿集团”）具有上百年的开采历史，是一个以煤为主、多业并举的跨地区、跨行业、跨所有制的大型现代企业集团。作为全国企业500强之一，淄矿集团把信息化建设作为企业发展战略的重要组成部分，有效地发挥了以信息化建设带动企业发展的作用。随着近十年来的信息化持续建设，企业内部的计算机终端逐渐增多，其数量已经超过了3000台，而担任核心业务的服务器也达到了30多台，在庞大的终端用户面前，网络安全已经成为淄矿集团领导层关注的议题。

淄矿集团信息中心于先生表示：“防病毒工作一直以来是我们在网络安全中最基本的，也是最为重要的一个环节。尤其是近两年互联网出现的恶意代码千变万化，每天在我们信息中心的办公室里，感染病毒和杀毒的话题就没有停止过。并且，由于终端安装的应用软件越来越多，而这些软件使用规模群体越大，安全性缺陷所带来的威胁就越严重。加上内网中隔离防范措施不如外界那样严格，一台终端感染病毒，就很有可能在全网产生‘蝴蝶效应’。”

据了解，除明确了国家对计算机网络使用法律法规的条款外，淄博矿业集团信息中心还详细划分落实了网络用户责任制，详细规定了个人IP地址、用户账号和密码的管理及使用守则，对不遵守上网规定、感染病毒、攻击服务器，恶意登录他人计算机，转接转让用户IP地址等22种行为明确了处罚规定。然而，于先生和信息中心的其他同事对《制度》表示了另外的看法：“这些安全制度的制定本身并没有问题，但如果没有配套的产品和服务支撑，很可能就成了挂在墙上的白纸了。因此，为了确保淄矿集团的业务连续性、避免病毒对企业网络带来威胁，我们需要在趋势科技提供的OfficeScane网络防病毒系统基础上，对防病毒系统进行升级。”

从趋势科技NVWE网络病毒墙准入控制入手，持续导入威胁发现设备TDA等多层防护

趋势科技提供的OfficeScan为客户端提供了良好防毒品质以及优秀的杀毒功，但对于移动性较强的笔记本用户来说，由于长期出差或不在OfficeScan保护范围内（员工个人物品），一旦缺少重要的补丁更新携带了病毒，也会严重影响网络的正常访问。为实现 “网络安全主动出击”的目标，淄矿集团的IT系统在近5年当中持续升级OfficeScan的同时，继续采购了趋势科技NVWE网络病毒墙和主动式威胁发现设备TDA，并与OfficeScan进行了整合操控，从而有效地避免了网络协议2至7层所有的安全事件，

据介绍，淄矿集团是在4年前购置的趋势科技NVWE网络病毒墙产品，主要用于预防ARP恶性病毒在网络中的存留。NVWE作为网络层的威胁防御设备，可隔离和清除无保护设备（移动PC等），并当其进入网络时快速完成健康标准检查。当新采购的计算机以及移动PC用户连接到内部网络时，NVWE会通过TCP的5091端口，侦测计算机是否已经安装NVWE代理程序，如果计算机尚未安装代理程序，位于网络骨干上的NVWE就会拒绝计算机连接到外部网络，这时候开启浏览器，会自动转接到NVWE的警告画面，并提示使用者通过浏览器下载代理程序安装。而至于NVWE的代理程序，淄矿集团信息中心的工程师在安装趋势企业版的OfficeScan终端上，可自动利用Plug-in Manager进行安装，因此部署工作非常方便。

近期，随着淄矿集团对网络运维标准化观念的引入，网络安全工作更注重主动发现、主动预防和绩效评估等量化工作。信息中心也将“标杆管理”付诸于实践，在网络中加入了全球网络安全技术中最先进的主动式威胁发现系统——趋势科技TDA（Threat Discovery Appliance）。TDA采用了离线配置模式，旁路连接在淄矿集团信息中心的核心交换机上，同时对淄矿集团办公区和家属区的网络流量进行扫描。据于先生介绍：“之前我们对于异常流量的监控主要依靠IDS和其他抓包软件，需要手工分析攻击类型，而现在使用TDA可以快速、高效地抓到高危客户端并识别攻击型态，并利用趋势科技的TMCM将NVWE、OfficeScan、TDA整合起来使用，第一时间发现、阻断、修复病毒源。另外，我们将TDA注册到趋势科技的云安全（Secure Cloud）后，趋势科技TMSP 智能分析平台会定期自动为我们提供威胁评估报表。TDA报表可以全面展现集团网络整体威胁状况和危险等级，并给出安全建议。我们也借助趋势科技提供的一系列产品，将所有的《安全制度》逐一进行了落实。”

信息安全管理，永无止境

据了解，趋势科技与淄矿集团双方的合作正在延续，另一款专门针对Web病毒防护的IWSA安全网关也在部署实施中。IWSA将部署在淄矿集团家庭区网络的主交换机和上层路由器之间，对内部用户的Web应用进行综合性防护和控制，包括：HTTP/FTP协议实时防病毒、Web信誉评估服务、防间谍软件、防网络钓鱼、恶意URL阻止、URL过滤、Java Applet＆ActiveX插件过滤等等。

趋势科技携手淄矿集团对原有的防病毒解决方案进行升级，建立起一个多层次、全方位、系统化并易于管理的网络防病毒体系，双方对于网络安全管理的看法相同，这就是：“安全没有终点”。那么，永远没有终点就意味着要不停地发展，而发展就是要求我们不断总结实践经验、不断创新管理理念和管理方法，永远掌握安全管理的主动权，永远利用最先进的技术，在与病毒和黑客的较量中取胜。