趋势科技护航东风悦达起亚实现合资企业网络安全管理

东风悦达起亚汽车有限公司（DYK）是由东风汽车公司、江苏悦达投资股份有限公司、韩国起亚自动车株式会社共同组建的中外合资轿车制造企业。作为合资制造企业典型代表，DYK的网络跨越了国内的各个省份并与韩国KIA总部进了国际专线联接，解决了大型制造企业中的流程管理复杂、异地数据传输、业务系统众多、客户端分散等等一系列的安全管理难题。同样网络安全软件及服务领域的全球领导者——趋势科技，深入剖析合资企业跨国管理和制造行业管理的特点，并结合了云安全2.0(Smart Protection Network)全球防毒架构，携手DYK一起解决了安全运维中难题。

一切为了高品质的产品

DYK公司对 IT 基础架构进行大量的投资，为加速新型车辆的设计和研发，完善生产流程，进一步提高DYK 汽车的质量。据管理部朱部长介绍：“DYK对于业务系统信息平台建设，一直都将安全放在首位，公司从开始构建IT构架平台时，就把平台安全作为首要问题。例如：双路由、双线路、数据传输过程严格加密、备份磁带库以及马上要建立的异地容灾系统等等。然而公司的网络结构非常复杂，这对防止病毒和黑客攻击非常不利。DYK现在由近300台服务器和数千台客户端组成，并划分了生产网络、办公网络，分别连接各个分支机构，以及远在韩国的产品研发中心。‘三网合一’，在满足网络应用特点同时，都能提供统一标准安全策略，消除安全隐患，显得十分重要。”

据了解，DYK已经实现了每小时44台新车下线的生产能力，公司在产品设计、营销网络、库存管理、配件订单以及售后维修等方面，都依靠网络才能展开。数千台的客户端，随时都可能出现的病毒事故,保障正常业务有序运行的难度比较大。DYK的网络在前几年也没有逃脱ARP病毒的侵扰，通过Web途径涌入病毒、木马、恶意插件和垃圾邮件的事件也逐年递增。因此，如何防止这些威胁进入到网络、进入后如何发现、遇到紧急事件如何处理，种种难题始终困扰着IT中心。

在朱部长的带领下，IT中心INFRA的同事一起制定出详细的安全管理规划，并且已经逐步落实,从网络隔离，到SSL VPN和邮件加密传输等等。朱部长表示，整个规划的核心目标就是：“提升服务品质和管理效率，将公司所有的信息系统进行整合管理，不能让IT安全问题影响到公司的业务。”

“四大任务”唯有趋势“能行”

相对于其它行业来说，由于DYK具有了合资企业和制造企业的特点，产品设计和汽车电子控制程序都在韩国进行。本土生产厂和韩国的设计部门需要及时沟通，对数据的实时性和安全性要求非常严格，网络中细微的变化都可能影响更新程序的正常传输。

为了解决每一个生产网络和办公网络客户端的安全问题，IT中心在尝试了几款防毒产品之后，从技术、管理、服务等多方面进行评选，最终选择了趋势科技的OfficeScan。此外，为了坚持“分毫不差”的管理理念，进一步完善安全防御体系，提升工作效率，优化管理。朱部长又提出了四个要求：第一，在网关层先行过滤，防止Web和邮件病毒进入；第二，即使有“漏网之鱼”，在客户端遭到病毒侵袭之后，能第一时间发现威胁、预警与隔离；第三，是客户端能够相关关联，在第一个人发现恶意网站和木马后，别人“不再犯同样的错误”；最后，在遇到入侵或者一些极端安全事故的时候，得到专家团队全面的技术支持。要想完成DYK制定的这四项任务，就需要将“多层防护、主动防御、统一管理、响应及时”的目标逐一落实下去。

为此，IT中心对INFRA的员工进行动员，咨询多位业内专家、资深人士，并考查了各个安全厂商提供的整体方案。朱部长表示：“真是百里挑一，这其中‘唯有’趋势科技能够提供对应的整套产品和服务。”DYK有针对性地选择了趋势科技的一系列产品：可以在云安全架构中实现客户端全面统一管理的OfficeSan；能够支持DYK这样大型网络的高性能邮件网关安全设备IMSA5000；分别负责生产网和办公网、第一时间发现威胁设备TDA（Threat Discovery Appliance）；以及应对威胁和反病毒所需的完整生命周期的TMES（TrendMicro Exper Service）服务体系。

纵深防御加强 破解安全难题

利用趋势科技的产品和服务，DYK网络运维已经在之前坚固的IT 基础结构上，建立起了无坚不摧的防御体系，安全难题被逐个击破。

利用IMSA5000，公司从之前对垃圾、病毒、钓鱼邮件以及恶意URL连接的防御中完全解脱出来，成果非常显著。而被俗称为“一揽子式”邮件安全解决方案的IMSA，其融合了防病毒网关、防垃圾邮件设备、防间谍软件设备等功能，可以替代若干台安全设备，因此朱部长对IMSA功能和性能都非常满意。通过IMSA提供数据统计功能，技术人员可以对每天、每月处理的邮件数量、正常邮件和垃圾邮件数量一目了然。

对TDA和OfficeScan的结合应用效果，朱部长深有感触：“之前，我们虽然对TDA的功能了解不少，但在实际应用中，我们发现TDA对于生产网、办公网和300台服务器实现统一管理的效果，超出了我们的预期。对于无法被网关端阻挡病毒、内部发起的攻击、网络流量的异常行为和担忧产品研发数据外泄，TDA的作用超出了数十人的IT团队在24小时内不间断监控网络的结果。”由于TDA集成了趋势科技云安全2.0中的“多协议关联分析技术”，可全面支持检测2-7层的恶意威胁。在两个网络都部署TDA之后，发生在DYK每一个网络中的Web攻击、网络钓鱼行为、病毒攻击点和高危网络通讯行为都在第一时间得到解决，这也就杜绝了向外界泄露数据或从僵尸网络控制中心接收命令的木马行为，这是传统IDS和IPS安全产品所无法办到的。此外，由于OfficeScan也集成了趋势科技云安全2.0中独创的“云客户端文件信誉（Cloud-Client File Reputation，CCFR）”技术，通过云端服务就可以实现IMSA在网关层、TDA在网络层、OfficeScan在终端层进行统一的管理和联动，将DYK网络安全策略 “落地”。

对于建立企业网络安全管理机制的必要性，朱部长认为：“同东风悦达起亚汽车有限公司一样，很多大型的合资公司，避免不了生产地分散的情况发生，因此单独只有产品的支撑并不能实现放心的管理，而趋势科技提供的TMES对整个反病毒周期的动态管理机制，使得趋势原厂服务体系和客户IT人员在整个周期中都能及时、迅速地发现、界入和处置病毒问题，实现真正意义上有效的IT防毒管理。尤其是安全评估和应急响应，来帮助我们处理各种管理方面的问题，特别是现在需要降低成本的同时，网络威胁又变得更加复杂的时候，‘服务’显得更为重要。”