浙江移动安全管理平台案例介绍

SOC 事业部

网御神州科技有限公司

1 项目背景

作为在纽约证券交易所上市的企业，中国移动需要通过 SOX 法案对 IT 审计的严格要求。2006 年，中国移动集团公司、中国移动浙江分公司（下简称“浙江移动”）都提出了针对 ERP、统一信息平台的日志审计要求，要求必须按照集团和分公司关于 SOX 内控的规定做整改，符合 SOX 的要求。同时为确保浙江移动管理信息系统环境和所有应用的稳定运行，分析系统的运行状况，统计系统的运行信息以及防范非法入侵和访问，需要对重要系统日志按照规范要求进行审核，将问题防范于未然。

2 需求分析

浙江移动由于网络规模庞大、设备和应用系统众多，如果采用人工的方式，费时、费事、代价昂贵、准确性和时效性都很差。浙江移动希望通过一套综合审计系统，集中采集网络设备、安全设备、主机、应用系统和数据库等的日志，按照集团公司的规范和 SOX 对于 IT 审计的要求进行安全审计，定期生成相关的审计报告。通过审计发现可疑行为和违规操作，进行必要的调查和整改。

浙江移动的业务系统是企业信息安全防护最核心的部分，但是目前的业务系统往往会面对很多的威胁而无从解决，这些威胁和问题包括：

外部人员对业务系统业务专网资源的未授权访问；业务系统内部用户的违规行为；缺乏对网络通讯的监测和审计，对网络连接是否正常无法判断；缺乏对重要服务器与数据库的运行和访问状态的集中监测；缺乏对已部署的各种安全系统（防火墙、入侵检测系统、防病毒系统）的集中监测，对安全事件是否发生，是否需要处理不能准确判定；缺乏对业务系统各种应用系统的集中监测；缺乏对业务系统内部的各种桌面系统的集中监测；缺乏有效的技术手段，建立安全事件责任认定与跟踪机制。

3 案例解决方案

网御神州采用先进的安全管理平台，将用户 ERP 系统、统一信息系统平台的多个应用、中间件、管理系统、主机、网络安全设备等日志统一采集、统一存储、统一分析，提供实时告警和审计报表，满足用户需求。采集企业信息化部的重要主机（包括 Windows、Linux、

Unix 系统主机)、中间件（WebSphere、WebLogic 等)、应用系统和数据库系统的日志，并将其进行归一化，生成统一的内部格式的事件，传送给事件分析服务器。系统可利用多种展现方式展现事件（包括列表、统计图、统计表、事件图、地图信息图等)，事件分析处理器根据预定义的规则对事件进行分析，可以触发报警（如控制台、邮件、短信等）和预定义的响应动作（执行系统命令、预定义脚本或设备联动等)。所有接收的事件被保存到数据库中。实施中针对浙江移动和 SOX 要求定制了报表模版，创建了相应的报表任务，可定期生成所需的审计报告，并将报告发送给指定的接收人。

基于浙江移动网络安全审计需要解决的问题，网御神州的具体解决方案如下：

1、采集多种类型的日志数据

采集浙江移动网络中各种操作系统的日志，防火墙系统日志，入侵检测系统日志，网络交换及路由设备的日志，各种服务和应用系统日志。并根据用户需要定制开发相应的日志收集模块以便收集用户的应用环境中所特有的日志数据。

2、日志集中存储、管理和查询

自动将采集到的各种操作系统、数据库和网络设备的日志信息经过转换后集中存放到同一个数据库中，统一进行分析处理和报表，便于对各种复杂日志信息的统一管理与处理，方便管理员的日常维护和管理工作。支持以多种方式查询网络中的日志记录信息，以报表的形式显示。

3、事件关联分析

使用多种内置的相关性规则，对分布在网络中的设备产生的日志及报警信息进行相关性分析，从而检测出单个系统难以发现的安全事件。系统内置完善的入侵检测知识库，可以根据知识库对日志数据进行分析，识别出多种可能的入侵行为，如异常登录、攻击 Web 服务器、缓冲区溢出攻击、系统异常等。知识库可以进行升级，以便检测出最新的攻击手段。

4、自动生成安全分析报告和可视化分析

根据日志数据库记录的日志数据，分析浙江移动网络或系统的安全性，并输出安全性分析报告。报告的输出可以根据预先定义的条件自动地产生、提交给管理员。根据用户的要求，系统通过对数据库中历史数据的深入分析，使用系统预设的各种模板，能够从不同角度（按网络设备、系统、事件类型等）生成日志分析结果，以直观、清晰的可视化图表予以显示。分析涵盖了对事件的归类统计及事件的变化发展趋势。

5、多种事件响应方式

在浙江移动网络中一旦识别出入侵或者越权行为，或者日志收集代理和日志服务器之间的连接中断时，或者数据备份失败时，可以进行告警。告警方式包括屏幕打印告警信息、将告警信息写入数据库、在页面上显示、电子邮件告警等多种方式。不同类型的告警信息可以发送给不同的管理员。

4 项目效益

浙江移动企业信息化部就安全审计系统项目进行了公开招标，经过激烈的竞争，网御神州的产品和方案最终胜出，得以承建浙江移动企业信息化部的安全审计平台。

中标后，项目启动的时间已经落后用户预定的时间，而集团要求完成的时间不变，这给项目的实施带来很大的困难，尤其是项目进度控制上。网御神州从硬件的采购和生产，设备调查，开发环境搭建等多方面投入大量的人力，将工作并行展开，为赢得时间而努力，克服重重困难，准时完成项目的要求，完全达到了预定的目标。

项目实施后，极大地提高了浙江移动企业信息化部的安全预警和安全审计能力，使用户可以及时发现攻击行为和违规操作，为调查取证提供详实的审计数据，为企业的 IT 合规管理提供了有效的技术手段。该项目的实施，帮助浙江移动企业信息化部顺利通过移动总部的 IT 审计检查和审计公司对公司的 SOX 外审。浙江移动企业信息化部领导给我们的评价是：产品功能强大、人员技术高超、服务质量过硬、把用户利益放在第一位，急用户之所急，想用户之所想，下次合作还找网御神州！

欲获取更多信息，请即联系网御神州科技（北京）有限公司
全国统一热线服务电话：010-87002000（7×24 小时）
E-mail：service@legendsec.com（5×8 小时）
网站地址：www.legendsec.com
网神安全管理博客地址：http://blog.sina.com.cn/legendsec
传真：010-62972896
通信地址：北京市海淀区上地信息产业基地开拓路 7 号先锋大厦 2 段 1 号
邮政编码：100085