成都电子政务 SOC 案例介绍

SOC 事业部

网御神州科技有限公司

1 建设背景

成都作为全国信息化建设的试点城市一直在政务信息化建设上走在全国前列。成都市政府非常重视信息化建设的发展，早在 03 年就制定了《成都市信息化建设管理暂行规定》使成都的信息化建设有法可依。并依照“五大体系”、“四个公开”、“四项措施”、“两手体现”的原则制定了《成都市信息化标准体系》，形成完整的理论体系。

成都市电子政务外网是成都市信息化建设的关键，随着政府部门信息化程度的提高，对信息系统的依赖程度越来越高。同时，整个电子政务外网的信息系统所面临的各种安全风险也日益严重，如何更好地为成都市电子政务外网和电子政务信息系统提供安全保障，确保电子政务外网的安全运行和信息化的健康发展是成都市电子政务网络和信息系统建设所面临的一个主要问题。

今年，成都市政府采购服务中心受成都信息化技术应用发展中心的委托，对成都市电子政务外网安全管理平台项目进行了公开招标，邀请国内多家顶级网络安全服务商参加投标。经过数月的综合测试，网御神州 SOC 平台安全解决方案以完整的安全管理系统架构、强大的事件关联引擎、丰厚的安全领域知识积淀和企业级的分布处理战胜诸多强手而最终胜出。成都市也成为首个将电子政务安全管理平台付诸实施的省级城市。

2 信息化建设现状

成都市电子政务网络是由成都城南、城西、城北节点等核心节点和 14 个远郊区县骨干节点共同组成的大型网络系统。政府各机关单位通过成都市电子政务外网进行高效、快捷的网络信息交换，并通过互联网向企事业单位、社会公众提供透明和公开的政务服务。成都市电子政务外网现有出口电信 100M、网通 10M、移动 10M。电子政务外网接入市级党政部门 70 余个，20 个区（市）县电子政务网络，共计约 15000 台终端；电子政务外网已承载多个大型重要应用系统，如卫生防疫、新农合、城乡救助等系统受众面广、使用率高、影响大；更且各区（市）县政务服务中心网站、各市级部门网站共约有 100 多个在利用外网互联网出口提供访问服务。

3 迫切需要解决的问题

目前对这些设备采用的是分散管理，使得外网的实际运行状况，与国家对电子政务网的安全等级保护建设要求、中心领导的期望以及中心的安全目标，还存在较大的差距，这些差

距主要体现在以下几个方面：

安全管理的问题：电子政务外网的安全管理制度是否得到了有效贯彻，安全产品和服务厂家所能提供的服务运作流程是否有效实施，无法衡量到底处理、解决了多少安全事件；

海量数据的问题：不同品牌的防火墙、IDS、服务器等日志信息，每天多达数以百万计，淹没了真实的安全信息，使我们无法对众多的日志进行审计；

设备孤岛的问题：各种安全设备间缺少信息层互通能力，降低了系统整体的运作效率，延长了安全事件的发现时间和响应时间；

实时监控的问题：在现有的监控条件下，不能实时地查看每个安全设备和应用系统的日志，对整个网络的安全威胁和安全漏洞情况、安全状况和综合风险无法提供实时的分析数据；

持续改进的问题：安全管理需要不断对已处理的安全事件进行总结，不断更新安全知识库，不断改进安全运维流程，以及不断完善安全管理制度等，因而需要有效的管理手段来实现持续改进。

设备高可用性问题：据日常维护管理记录数据，外网出口所在政务服务中心路由器、防火墙等设备出现故障造成外网出口瘫痪是出口中断的主要原因。目前出口设备是从路由器、防火墙、流量管理和防攻击设备串接所联，设备的任何单点故障都会造成出口动荡，很多出口功能都集中在一台防火墙上实现，防火墙已不堪重负。通过两台路由器、防火墙等设备实现出口的负载均衡和设备之间的高可用性，出、入流量负载均衡和冗余切换，链路负载的高可用性，核心设备的高可用性，综合域名解析和地址管理等功能模块实现出口的链路保护和负载均衡功能保障出口稳定。

4 案例解决方案

4.1 网御神州 SOC 平台方案目标

通过安全管理平台，对现有的各种安全产品进行资源整合之后，成都电子政务外网的安全管理能够达到以下目标：

- 动态地协调和管理现有的安全产品，发挥它们应有的作用。
- 在现有人力资源的情况下，使安全管理人员全面实时地掌握系统内的安全状况，及时地发现安全风险和事故。
- 对信息安全政策的执行情况进行有效的监督与审计；对所有非法访问形成审计、跟踪、分析、处理、报告的完善流程。

- 对安全威胁进行及时地处理，减少安全事故造成的损失。

4.2 网御神州 SOC 平台功能和服务

统一管理网络设备

安全管理（SOC）平台可以收集各种网络设备的日志，集中、实时地监控网络安全状态。它可以管理的设备包括交换机、IPS（入侵防御）、IDS（入侵检测）、天融信等厂家的防火墙以及各种服务器，解决了安全管理过程中分散、非实时的问题，实现了统一、协调管理，大大地提高了工作效率。

划区域、分等级管理信息资产

按照信息安全等级保护内容和要求，SOC 平台中的信息资产主要是指网络区域、应用系统服务器和主机。SOC 平台可以将资产划分成安全区域，并借鉴已经发布的关于安全等级保护的制度和实施办法，根据资产的重要程度，将它们划分成不同的安全等级，并且将资产的安全等级和事件的危险程度结合起来，使资产管理更好地为安全管理服务。

有效地发现安全事件

SOC 平台在对日志信息解析和标准化的基础上，可以针对实际的网络环境，配置适合本网的多种过滤、归并和关联规则，使每天的事件数量大大地减少，并结合资产的安全等级，挖掘出最具威胁的网络攻击，有效地利用日志信息，发现安全事件，解决了海量数据的问题。

方便、实时监控、预警和响应

SOC 平台提供了统一的窗口，可以以表格和多种图形方式，同时监控来自多台设备的安全事件，并且安管人员可以方便地查询感兴趣的事件。

SOC 平台还可以通过控制台、短信和邮件等方式自动进行 7*24 小时的预警。

已有的安全管理人员、流程和制度，通过 SOC 平台提供的用户和工单管理得以实现，完成对安全预警的响应和处理工作，为有效地执行安全管理制度和流程提供了可能。

报表和知识库

通过 SOC 平台集中的数据分析，对一段时间内的各种网络安全状况，提供事件分析报告和安全趋势报告，为安全审计提供依据，帮助成都电子政务外网提前做出安全防御准备或者动态地调整安全策略。

在使用 SOC 平台时，对各种事件的处理方法和处理流程，最终会成为知识库中的文章，从而使安全管理经验不断得到累积，使安全管理工作更容易延续下去。而且，可以把收集来

的关于信息安全管理的文章加入知识库，便于安管人员不断地学习。

5 项目收益

信息安全是一个长期而复杂的系统工程，它不但涉及到了安全产品的应用，更为重要的是它还需要长期、优质的安全服务，如果没有不间断的安全服务，则信息安全就无法得到保障。所以，网御神州为用户提供了全方位的服务，来保障客户的安全服务工作。包括产品定期升级、培训、咨询等。客户也可以利用 SOC 平台为电子政务外网的区市县各级部门提供集中安全管理的外包服务。

通过以上安全管理平台的案例分析，网御神州 SOC 安全管理平台的引入能够更好地发挥现有政务外网的安全产品的作用，节省人力资源及信息安全建设的资金投入，是成都电子政务外网安全运行和管理的基础，同时也是政务外网安全保障的十分重要的技术平台。网御神州 SOC 安全管理平台为信息安全管理者提供了十分有效的技术和管理手段，使成都电子政务外网的安全管理水平提升到一个新的高度，为其他地区电子政务系统的安全管理提供了新的思路和示范。

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