广东核电病毒防护体系建设

步建华　陈双平　赵志中　彭少华　高 伟
(大亚湾核电运营管理有限责任公司 信息技术中心 518124)

1 引言

McAfee ePO 产品能完成从反病毒软件安装、配置到管理的全部工作的反病毒系统管理调度软件,它不仅可以管理不同厂商的防病毒软件,甚至还可以管理防火墙、入侵检测等安全产品,使它们形成了一个完整的安全体系。可以管理不同厂商的安全产品。这一点很重要,目前企业界并购和重组事件时有发生,一旦涉及两家企业信息系统的整合,很有可能就会出现两家企业用的是不同厂商的产品。因此,McAfee ePO 对不同产品在管理上的兼容性将起到投资保护的作用。

2 EPO 的特点

2.1 McAfee ePO (McAfee ePOlicy Orchestrator) 具有可伸缩能力

其功能包括全方位的策略管理、详细的图形报表以及软件部署功能。McAfee ePO 能够使系统管理员更有效地确保系统的病毒防护能力,包括防御各种新型病毒和管理病毒防护策略。根据反病毒产品中的数据,McAfee ePO 可以生成详细的图形报表,并在企业内部所有的工作站和服务器上部署病毒防护,还可为个别小组或终端用户机配置特别策略,从而为系统管理员节省大量时间。McAfee ePO 服务器可管理的范围突破了单个部门的局限,扩大到整个企业内部,可管理的最大节点数达到了 25 万个。此外,McAfee ePO 还确保了移动用户可以在他们每次建立网络连接或者互联网连接的时候更新其病毒样本库。使用 McAfee ePO 所提供的各种预定制报表,用户可以轻易地追踪到病毒发作的源头,或确定出病毒安全策略的效能,通过 McAfee ePO 提供对防御体系中每一层次覆盖级别的报表,用户可随时掌握病毒安全的最新信息。此外,McAfee ePO 还可以对报表进行用户化,使它们能更好地满足自己的特殊需要。

2.2 McAfee ePO 的安装很简单。

如果小型企业使用原有的硬件,那么其安装过程不会超过一小时。大型企业则可以因 McAfee ePO 的管理功能而获得效率上的提升。一旦 McAfee ePO 安装完毕,用户就可以在企业内部的任何一个地方使用远程控制台对所有的操作进行管理。系统管理员可从不同的防护级别为每一台电脑或者每一个小组制定各种病毒防御策略,从更新频率到可以扫描的文件类型,甚至试探式扫描的设置,都可以根据系统管理员的需要随意设置。McAfee ePO 的报表功能使频繁的策略审查变得简单易行,用户所要做的不过是轻点鼠标,使反病毒策略生效。

2.3 高效率的升级体系

在信息技术中心建立了升级服务器,定期、自动地接受 NAI 病毒升级站点 ftp. nai. com 的最新的病毒定义码和扫描引擎;安装 SecureCast ,接收从 Back-Web 推送来的数据;负责向 McAfee 反病毒紧急响应小组 AVERT 提交下级行提交上来的病毒样本,并根据 AVERT 的建议,采取相应的措施。一级行负责分发、管理、配置、安装和升级辖区内的防病毒软件,集中收集辖区内的病毒报警事件,采取相应的措施,比如是否进行病毒定义码的紧急更新等,从而形成高效率的升级体系。

3 广东核电防病毒体系的建立

3.1 产品选择

在广东核电的多重病毒防护体系中,充分考虑到保护原有的投资,原来第二核电用的是 SYMANTEC 的防病毒系统,而广东核电的其他公司与总部使用的是 MCAFEE 的防病毒系统,防病毒系统的管理具有相当大的难度。因此在防病毒管理解决方案中考虑到六

个重要的因素：防病毒管理体系对硬件的要求、通过管理软件可以查出哪些安全漏洞、管理软件对带宽的要求、企业级 Internet 的架构以及客户端实施的简单性，能提供详细的病毒情况的报告。

基于以上的六点考虑，我们最终选择了 MCAFEE 的 EPO 做为防病毒管理系统的控制中心。McAfee ePO 也充分发挥了它的能力：通过 EPO 的分发功能我们在 WindowsXp 和 Windows2000 以上版本的服务器和客户端计算机上，升级安装了 VirusScan7 的企业版软件防病毒软件，在 Windows9x 的计算机上我们安装了 symantec 的防病毒软件，防止病毒的内部传播；在 Exchange 服务器上，安装了 GroupShield 选件，提供邮件服务器的病毒防护。同时 Mcafee EPO 也具有强大的报表分析能力。

3.2 EPO 功能

（1）EPO 将所有的防病毒产品统一管理起来，协调各部分的功能。这些防病毒软件的协同部署对公司整个系统架构的安全起到至关重要的作用。任何一个方面的不足都可能导致病毒“趁虚而入”。更何况整个防病毒体系是一个不断升级的动态系统，它使系统的管理尤为重要。McAfee ePO 自动做到软件的部署与升级，对用户来说是透明的，是用户在毫无觉察间使他的电脑得到了最新的安全保护。

（2）McAfee ePO 使各个杀毒软件成为了一个整体解决方案，可以协同作战，达到效果最佳化。广东核电做到了安全策略与具体的防病毒技术有机结合。从目前的世界防病毒产品来看，防病毒技术是相当成熟的，而安全策略的缺口却是病毒入侵的关键。策略大于一切，有资料显示，目前有 76% 的大型企业制订了防病毒策略，但只有将这些策略实施 95% 以上，企业才能得到真正的保护。根据调查，25% 的企业 1 年以上检查 1 次，9% 的企业半年检查一次，19% 的企业一个季度检查一次，21% 的企业不知道多长时间检查一次，只有 13% 的企业能够做到一周检查一次。这些数据表明很多企业内的防病毒体系的应用漏洞百出，这也导致历次大规模病毒发作时，总有一大批企业遭受到很大的损失。有人对经济损失做统计后称，去年尼姆达病毒发作带来的经济损失甚至超过了 9·11 事件的损失。但这种损失并没有像世贸中心的倒塌那样悲怆，当然也没有它那样引人关注。然而，这种病毒带来的损失是可以降低到最低限度的，其关键在于整体防病毒策略的实施。‘千里之堤，溃于蚁穴’这就是绝大部分企业在面对病毒时遇到的主要问题。当一个企业网络被病毒侵入，它很可能利用网络内部的一些共享机制和内部用户的权限无所顾忌地进行传染，过去一段时间内爆发的很多病毒通过这种方式使大批电脑陷于‘毒手’。因此，堵住每一个‘蚁穴’是 McAfee ePO 防病毒策略中最重要的一环。不仅如此，一些反病毒专家称，这种病毒与黑客技术相结合将会是未来病毒发展的重要趋势，它迫使防病毒技术与网络整体安全管理并肩作战。

（3）在防病毒产品的分发安装、升级等一系列的管理工作中，McAfee ePO 将分发功能集成在了一起，为广东核电的防病毒体系提供了一个优秀的分发工具，更为重要的是它无须占用太多的网络带宽，还可以提供 SQL2000 数据库服务器报告。McAfee ePO 将系统报告生成 SQL 数据库保存与绝大多数防病毒管理软件生成文本日志的方式形成了鲜明的对比。这种日志管理策略也使 McAfee ePO 为用户提供了更加强有力的功能：由于采用 SQL 数据库来保存防病毒系统的记录，它可以容纳大规模的数据量，使得系统运行的每一个细节都有信息保存。此外，数据库保存方式也使用户可以按照标准的数据查询方法方便地进行快速查询。事实上，McAfee ePO 在此基础上为用户提供了一系列更为直观的图形报表，使管理员一眼便知系统的安全状态。

（4）长期以来，杀毒软件一直都处于被动地位，直到病毒出现以后才去想办法解决，而系统中存在的大批漏洞又使其更加被动。如何增强防病毒产品的主动性成为整个防病毒的关键，即变被动为主动。同样的在这些方面 EPO 提供给网络管理员病毒警报，使网络管理员可以第一时间得到病毒到达和发作的报警，以便及时地做出应变。

（5）从近年病毒发展的趋势来看，越来越多的病毒开始带有黑客技术，而黑客技术主要是通过系统中存在的漏洞和弱点来进行攻击的。NAI 以 McAfee ePO 为核心推出了完整的 AVD（动态病毒防护体系），它可以主动地去寻找系统中存在的漏洞，并堵住这些‘蚁穴’。另一方面，在 AVD 的病毒查杀中，NAI 引进了

（下转第 46 页）

(上接第 87 页)

基于行为的智能查毒技术,它通过对代码所做的操作来确认是否是病毒。这种方式改变了以往只有病毒出现后才能通过病毒特征码的提取实现查毒的传统做法,实现了未知病毒的查杀。在国际权威机构的检测中,McAfee 的杀毒软件对未知病毒的查杀达到了 80% 。这一技术目前在世界上仍属领先。由此,尽管计算机体系结构的限制使完全解决病毒防范的被动性不太可能,但在某些情况下主动地寻找可能出现问题的地方和代码却是可行的——正如对待犯罪一样,在犯罪以前,我们没办法断定他是否会犯罪。但公安机关可以通过一系列的排查工作来提前发现治安隐患,避免事后补救可能造成的损失。Mcafee 的 E500 防病毒网关与防火墙紧密的结合起来,扩大了病毒的防范范围,从而增强了广东核电的防病毒的预防和侦测能力。

4 显著效果

通过使用美国网络联盟的整体防病毒解决方案,广东核电部署了成功的防病毒系统,切断电子邮件、网络访问、移动介质等所有病毒传播途径和消除发作机会,从而使广东核电大大降低因病毒传播和发作引起的资料损失、性能损失、人工损失,简化防病毒体系的管理,从而节省操作成本,能够及时获得病毒告警和事件报告,能够动态快速更新病毒特征数据,能够容易地扩展升级并迁移到新的防病毒技术。自从去年上半年利用 McAfee EPO 部署全广东核电的防病毒系统部署以来,成功的抵御了包括红色代码、Nimda、求职信、振荡波等各种病毒的攻击,确保了广东核电网络系统的正常运行。