专业保护贴心服务 瑞星护卫教育信息安全

——北京市石景山区教委网络防病毒系统案例

一、网络安全形势严峻

随着电子政务建设的推进,政府网络与外界互联网的沟通越来越多。近几年来,挂马、钓鱼网站等非常盛行,病毒感染、传播的途径也变得更复杂、更隐蔽,网络安全形势十分严峻。针对这种情况,瑞星杀毒软件网络版2010扩充和增强了病毒防范和查杀功能,可为用户提供更好的解决方案。

二、安全解决方案整体需求分析

由于教育系统的业务结构相对封闭,因此多采用网络物理隔离等模式来进行控制。但是,随着近年来与外界接口的增加,各种应用和内部各系统间的互联互通等需求的发展,教育系统的安全问题开始跨网络出现。北京市石景山区教委网络为全区教育系统提供服务,用户包括学校、机关等多种类型,网络拓扑结构复杂,网络层次繁多,子网与主机数量庞大,必须经过非常严密的分析才可能提供安全的解决方案。

瑞星公司对石景山教委网络的特点进行详细分析,认为如果采用多种类安全产品混合安装,会有以下几个问题:由于品牌不同,产品之间存在冲突的可能性较大,很可能会产生系统崩溃、资料丢失等严重后果;各个产品之间完全独立,无法实现产品之间的联动,防护效率无法进一步提高;各个产品单独运行会大量占用内存,造成资源效率低下;多种产品组合势必会使产品采购价格上升,而且一旦产品出现问题,无法立刻确定是哪个产品出现问题,使得维护效率低下。瑞星公司可以提供全面的信息安全产品,在反病毒与防黑的结合、多产品之间的兼容和联动、服务的便捷性上有着无法替代的优势。

三、安全解决方案需要考虑的关键因素

1.*多层次和完整性*:现有网络是一个复杂的网络,网络内有不同的操作系统,内部网络有客户机、服务器等,有效的网络防毒体系应该能够支持各种操作系统。

2.*有效的集中管理*:网络防病毒是对整个网络进行病毒预防、监控,由于现在网络规模较大,通过集中管理可以实现快速的防病毒软件的安装维护、病毒定义码和扫描引擎的更新升级、网络防病毒策略的配置、报警的集中管理、定时调度、隔离、实时扫描和监控等。

3.*策略强制执行和用户端保护*:网络内的用户是多样的,为了防止用户删除客户端的病毒监控系统,破坏网络病毒防范的整体性,用户端必须具备防止用户删除和修改策略的保护措施,统一的病毒防范策略才可以实现发现病毒后统一操作。

4.*病毒定义码和扫描引擎的升级、更新*:由于新增病毒的出现频率越来越快。据"瑞星云安全"系统统计,目前每天网上出现的病毒文件数量约为30~50万个。因此,必须能够及时升级病毒库,保证对新增病毒的查杀。

5.*快速和及时性*:由于病毒的发展是破坏性越来越大,杀毒软件必须具有快速的病毒反应速度,能够及时获取最新病毒代码并提供相应的解决方法。

6.*持续性*:杀毒软件必须及时根据新增病毒的出现提供相应的解决方案和软件升级,才可以保证正常使用,这就要求杀毒软件厂家必须具备持续发展的能力。

7.*本地化服务*:计算机病毒的一个显著特征是突发性,某些病毒的突然爆发可能会带来严重后果,能够提供本地化服务可以将这种后果造成的损失降到最低。

四、安全解决方案的实施

1.*应用架构描述*

"防毒+杀毒"结合,以防为主。瑞星防病毒系统在病毒可能流传的各个渠道中都设有监控,结合定时病毒扫描和自动更新,保护系统的安全。同时,结合对应的管理策略,充分发挥瑞星产品在病毒防护集中管理、监控中的优势,在石景山教委的网络中构建有效的病毒监控体系。

2.*设计简述*

该方案贯彻了如下的基本设计思想:第一,全方位、多层次防毒:部署了多层次病毒防线,分别是各种应用服务器防毒(Windows NT/2000,Unix,Linux,NOVELL)和客户端防毒,保证斩断病毒可以传播、寄生的每一个节点,实现病毒的全面防范;第二,集中管理:实现了网络防病毒的集中管理,保证了整个防毒产品可以从管理系统中及时得到更新,同时又使得管理人员可以在任何时间、任何地点通过浏览器对整个防毒系统进行管理,使整个系

统中任何一个节点都可以被管理人员随时管理，保证整个防毒系统有效、及时地拦截病毒。

3.具体实施

瑞星公司在石景山教委网络实施由点及面、全方位网络防病毒产品部署，彻底截断病毒入侵的所有途径，具体产品布置根据不同病毒防范方法采用不同产品。

整体结构为：在石景山教委网络中心内安装一个一级系统中心，在其各下属单位网络中心安装二级系统中心，每个系统中心可以独立运行、管理自己所辖地区网络的全部客户端、服务器端，同时，一级中心和下级各中心可以构建成任意树状结构。如下图所示。

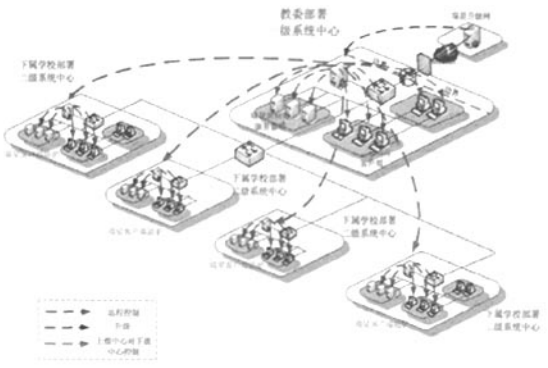

图 石景山教委网络防病毒体系整体结构

上下级系统中心通过 HDLS、VPN、拨号等方式进行通讯。通过这种多级系统中心的模式可以实现：上级中心可以对下级进行管理，并接收由下级中心传送过来的数据；下级中心接收到上一级中心系统发出的命令，并将命令转发给本级的所有客户端；定时收集本中心系统的病毒信息，在分析处理后上传到上级中心，以便上级得到下级的病毒信息，及时做出相应的处理。这样既避免了由于过度的信息传输给网络资源造成的影响，又能够及时让管理员得到最新的病毒分布情况。

通过该系统，可实现反病毒的统一管理和分级管理，统一管理表现为由上级中心统一发送查杀病毒命令，下达版本升级提示，并及时掌握全部系统中心(包含下级中心)的病毒分布情况等；分级管理表现为下级中心既可以在收到上级中心的命令后做出响应，又可以管理本级，并主动向上级中心发送请求和汇报信息。可见，多级中心系统支持大型的、多层级的、复杂的网络。这样即使是下级的任何一个客户端出现病毒，一级系统中心都可以及时发现。

五、结束语

瑞星除了针对用户需求提供定制研发方案之外，在方案实施过程中，从安装调试到技术支持，都提供了详细、周到的服务，在方案实施之后，瑞星的售后服务体系在系统的稳定运行与完善实施方面又做了细致的工作。瑞星的所有软件产品都具有完全自主的知识产权，且产品用模块化进行开发，不但保证了系统本身的安全，而且可扩充性也非常好。事实证明，整个方案是科学、有效的，开始设定的目标都得到了完满的解决。

附：瑞星研制出全球最快反病毒虚拟机

近日，瑞星宣布，世界上最快的专业反病毒虚拟机已经研制成功，并被应用于瑞星杀毒软件网络版 2010，以及瑞星“云安全”平台的病毒自动处理系统之中。实验室评测数据表明，这款由瑞星研制的专业研究型虚拟机，比原来的传统虚拟机运行速度高 200 倍。专家表示，该虚拟机的研制成功，可以把国内反病毒行业的整体技术水平向前推进一大步。

据介绍，虚拟机是反病毒行业的核心技术之一，目前世界上的主流杀毒软件，为了提高查杀能力都集成了虚拟机技术。但虚拟机具有占用系统资源、运行效率低的天生缺陷。针对这一业界难题，瑞星成立了专门的研究团队，经过长达 5 年的技术攻关，终于取得了飞跃性的技术突破。新一代瑞星虚拟机应用分时技术和硬件 MMU 辅助的本地执行单元，在纯虚拟执行模式下，可以在 CPU 为 P4 3.0 的机器上，每秒钟执行超过 2000 万条虚拟指令，结合硬件辅助后，更可以把效率提高 200 倍。由于虚拟机运行效率的提高，集成虚拟机的瑞星杀毒软件 2010 版不但杀毒能力强，而且占用的系统资源更少，运行更快。

瑞星反病毒专家介绍说，虚拟机的运用主要是两个方面：第一，虚拟机可以集成在杀毒软件中，当遇到加壳、变形等难以查杀的病毒时，可以将其置入虚拟机中运行，病毒在其中恢复原形运行，就会被杀毒软件杀掉，这样可以大大提高杀毒软件的查杀能力，有效查杀各种复杂恶性病毒及木马。第二，虚拟机可以用在病毒样本的自动处理当中。由于瑞星云安全系统每天需要处理百万量级的样本，虚拟机效率的提高，可以让系统处理新样本的时间减少，还可以大大节约服务器资源。在瑞星“云安全”系统应用新一代虚拟机技术之后，一个新木马从出现在互联网上，到被分析完成彻底查杀，只需要 5 分钟。

业内专家分析说，杀毒软件是我国仅有的几个具有国际竞争力的高科技领域之一，而随着互联网的发展，信息安全在国际竞争中拥有越来越重要的意义。瑞星专业虚拟机的研究成功，不但可以推动整个反病毒行业的技术发展，更对我国高科技企业参与国际竞争有着重大意义。◉

(郭凤珍)