企业防病毒体系的建立

Construction of Enterprise Anti – virus System

陈平仲　（广东外语外贸大学教育技术中心 510420）

摘要：本文论述了防治病毒的常识，详细介绍了如何分层建立企业网络病毒防护体系，并对企业防护体系提出了一些注意事项。

关键词：网络 病毒技术 病毒防护 病毒库

1 前言

随着网络建设的不断深入，基于网络的业务系统的开展，企业对网络的依赖性越来越高，网络系统或其相依的业务系统的瘫痪，都将对企业造成极大的挫伤甚至可能造成致命的打击，如何提高系统的高可用性以及不停机时间，对企业来说是极其重要的，那么如何提高系统的可用性？除了有良好的软硬件环境和认真到位的网络管理体系外，很重要的一个方面是病毒的防护体系。

目前，不少的企业所做的病毒防护措施仅是在客户端上安装单机版的防病毒软件，而单机版的防病毒软件系统，像金山毒霸、诺顿等，它跟局域网中的其他主机没有必然的联系，员工只要管理好自己的“一亩三分”地就不错了。有的企业甚至单机版的防病毒软件都不是统一品牌，每一个员工自己使用一套杀毒软件。其实单机版防病毒软件系统不但不便于管理，而且保护的能力也非常有限。从防病毒发展的角度来讲，单机版的防病毒软件系统已经越来越显露出其不足之处。

现在的新型病毒，已大不同于以往了，首先是病毒更加智能化了。新型病毒，比如像 Worm . Sobig 就自己带着 SMTP 引擎。这样它自己直接就可以转发邮件，一台机器被感染之后，就开始大规模的转发这种病毒邮件，如此循环往复，形成大规模的网络风暴。另一个智能的表现是：有一些病毒它自己带有口令字典，用它挨个去试，如果有一个口令对得上，就可以进入你的服务器操作系统。其次，传播方式多元化和混合化。现在的病毒大部分是混合型病毒，很难分清这种病毒是一种纯病毒还是一种攻击行为。像“爱情后门”，它虽然属于蠕虫病毒，但本身却同时具有蠕虫、黑客、后门等多种病毒特征，不但会通过发送带毒邮件进行传播，还会通过局域网感染其他的计算机；另外，还会给系统开一个后门，直接对用户电脑进行控制。

2 企业所面临的问题及解决方法

现在，企业的网络几乎每天都会遭到新的病毒或旧的病毒变种的入侵。企业网络怎样才能避免或大幅度削弱病毒的入侵呢？

企业网络所连接的电脑可能是几十台、几百台甚至上千台，只要网络中有一台计算机被病毒感染，那么，病毒会立即在企业内部网中扩散，造成全网中毒，并还有可能向外扩散。怎样才能找到最先感染的机器并迅速将其隔离呢？

人工完成病毒码更新、防病毒软件的更新或安装补丁程序，都无法跟上病毒在网络上传播的速度，而且，遇到周末、节假日又怎么办呢？并且，在企业网络中员工的安全意识太薄弱，他们的计算机水平参差不齐，有的只会上上网，用用 Word、Excel 等 Office 软件，什么杀毒软件，有的人根本就没装！有的装了，也不会升级。确实，客户端的使用者计算机水平、网络水平、对安全的认识一日不提高，网管员就得天天解决这些本可以避免的问题。所以，一个企业要具有安全的防病毒系统，具体要从以下几个方面来确保。

首先，防毒一定要实现全方位、多层次的防毒部署。为了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，网关防毒是整体防毒的首要防线。企业必须将网关防毒作为最重要的一道防线来部署，全面消除外来病毒的威胁，使得病毒，病毒邮件不能再从外网传播进来，对内部网络资源和系统资源造成消耗。还有针对上网下载的文件，如果文件里含有恶意代码，他有可能在机器上开一个后门或放一个木马，这种情况都必须在网关上过滤掉。

第二个层次，文件服务器的保护。病毒的传播方式是多种多样的，比如内部文件的共享和从软盘拷贝等方式是不经过网关的，网关就不能将这部分漏洞补上。如果不在网关部署相应的防毒产品，只在文件服务器安装防病毒系统也是不完全的。假如有大量的垃圾邮件进来，如果不在网关上处理，它就会全部跑到服务器上去，虽然服务器可以把这些垃

圾邮件屏蔽掉,但服务器的资源比较有限,用大量资源去处理这些垃圾数据包,其他正常工作的响应速度就会很慢。

第三个层次,邮件服务器的保护。虽然在网关将病毒邮件和垃圾邮件都过滤掉了,但是在邮件服务器还是需要保护的。假如两个人都在公司里面,我给他发一封邮件,是从我的机器到邮件服务器,再从邮件服务器到他的机器上,而不经过外面的网关,这样的话,假如我机器染上病毒,然后再把大量的病毒传播出去,网关这一端是观察不到的。

第四层就是客户端的保护了。所有进入到网络里面的计算机还有其他的网络设备,都要求安装防病毒的客户端,让它实时监控进出本机的数据,并定期扫描自己硬盘上的文件,并且这些计算机系统必须安装最新的软件补丁包。在 2003 年 8 月,遭遇 MSBlaster 病毒攻击的计算机在几十秒内自动重启,所有未保存的资料会全部遗失。在疫情爆发的 24 小时内,有些企业被迫打补丁,或要求员工暂时不用网络,造成许多不便。2004 年 5 月 1 日历史重演, Sasser 如出一辙的手法同样将目标不仅锁定服务器也瞄准个人用户,让一般打补丁的动作不勤快的个人用户,成为防疫漏洞。

第五层就是必须有防毒的中央控制管理系统。没有集中管理的防毒系统是无效的防毒系统,中央控管软件定期自动进行全网络的病毒查杀,自动的更新病毒码和扫描引擎,自动的生成全网络的病毒日志,分析报表,并且通过日志查找网络中的病毒源头等。所有这一切都是通过位于中心的中央控管软件自动进行。上述五层可以用图 1 表示。

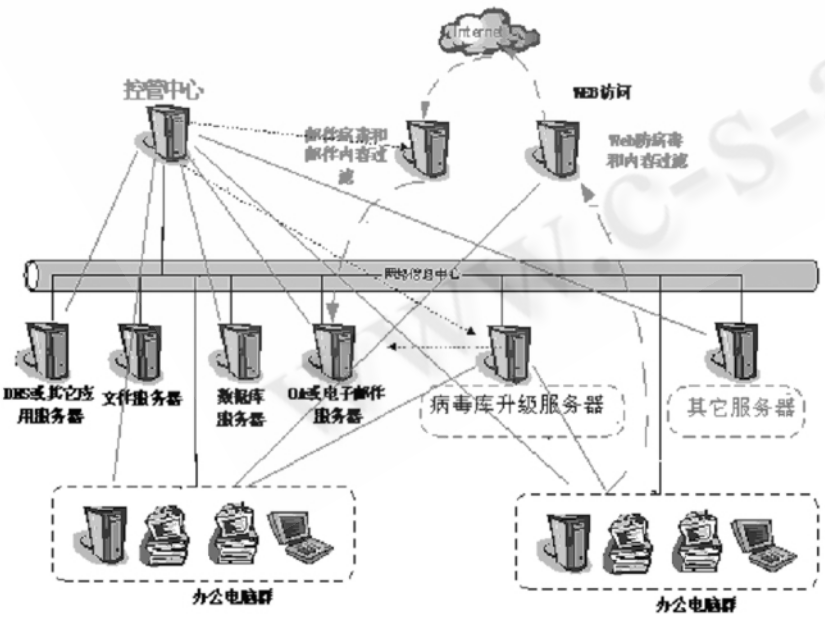

图 1

最后一层就是防病毒软件公司的服务。服务是整体防毒系统中极为重要的一环。防病毒系统建立起来之后,能不能对病毒进行有效的防范,与病毒厂商能否提供及时、全面的服务有着极为重要的关系。这一方面要求厂商要有全球化的防毒体系为基础,另一方面也要求厂商以及本地服务商能有足够的本地化技术人员作依托,不管是对系统使用中出现的问题,还是用户发现的可疑文件,都能进行快速的分析和方案提供。在防病毒软件使用过程中出现异常时能及时派技术人员到场提供技术支持。

3 总结

防毒之道,主动防御比被动查杀更重要,虽然事后的治疗是必须的,但更有效的是事先的一种防御。首先对安全漏洞进行诊断或漏洞扫描,通过这样的工具可以发现,哪些系统没有打上最新的杀毒系统的补丁,没有安装最新的病毒代码,哪些系统容易受到病毒系统的攻击,哪些系统已经受到了病毒的攻击,目前,很多病毒主要攻击系统的漏洞,因此,用户有必要用补丁管理或修补程序管理的产品为网络筑起一道安全防御的体系。另外,就是安全规章制度。最好与员工签定一项协议,协议里列出:你要保证你的计算机不能染上病毒,如果出现什么问题,个人有什么样的责任。如果有这样一套健全的制度,那么大家的思想意识方面知道哪些事情可以做,哪些不能做,哪些做了之后会影响其他同事和公司的网络安全,大家有这样的意识之后,基本可以杜绝病毒的入侵。我们强调的依然是要提高安全意识,如果使用的是单机版的产品要有按时升级的意识,如果企业网络规模越来越大,要有更换产品的意识,有了合适的产品和解决方案后,还要有正确实施的意识,因此安全问题,最终都可以归结到“意识”这两个字上来。

参考文献

1 计算机病毒防治与网络安全手册, 梅筱琴、蒲韵、廖凯生著, 海洋出版社, 2001.6。
2 计算机病毒原理及防治,卓新建著,北京邮电大学出版社, 2004.1。
3 计算机病毒与木马程序剖析, 张又生、米安然著 , 北京科海电子出版社, 2003.3。