基于校园环境的网络安全解决方案

周晓虹[1,2]
(1.厦门大学 福建 厦门 361000;2.厦门交通职业学校 福建 厦门 361000)

摘要:简单分析了目前互联网安全问题的现状,针对校园网的特点,总结了目前学校网络安全中经常面对的主要安全隐患,提出五种措施来加强校园网络的安全管理。

关键词:校园网络;安全管理;防火墙;IDS

1.引言

近年来互联网上发生了越来越多的大规模网络安全事件,各种攻击手段层出不穷,比如蠕虫、非法访问、拒绝服务器攻击等,使得大量重要数据被破坏,造成巨大的损失。随着我国校园信息化进程的推进,计算机网络已经成为学校重要的基础设施,校园网上运行的应用系统越来越多,信息系统变得越来越庞大和复杂,如果校园网络的安全运行受到威胁,必将严重影响学校的正常工作。

2.校园网络中的安全隐患

一般的校园网络总体上分为校园内网和校园外网。如图 1 所示,校园内网主要包括教学局域网、图书馆局域网、办公自动化局域网等。校园外网主要指学校提供对外服务的服务器群、与 CERNET 的接入以及远程移动办公用户的接入等。

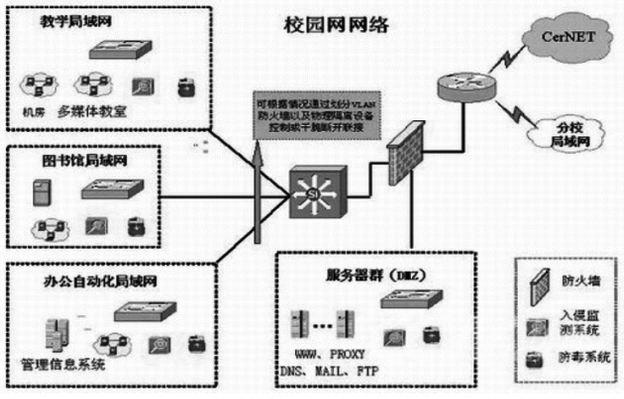

图 1 一般校园网络拓扑结构图

校园网络中的安全隐患多且复杂,主要有以下几个方面:

(1)校园网几乎时刻与 Internte 相连,也就时刻面临遭遇攻击的风险。

(2)由于内部用户对网络的结构和应用模式都比较了解,而且现在黑客攻击工具在网上泛滥成灾,学生的年龄和心理特点决定了他们利用这些工具进行攻击的可能性。

(3) 校园网的网络服务器安装的操作系统一般有 WindowsNT/Windows2000、Unix、Linux 等,这些系统本身也存在着一些安全隐患。

(4)随着校园内计算机应用的大范围普及,特别是学生宿舍和教职工家属接入校园网后,接入校园网的节点数日益增多,而这些节点大部分都没有采取安全防护措施。

(5)内部用户对 Internet 的非法访问以及下载文件可能将木马、蠕虫等病毒程序带入校园内网;内外网恶意用户可能利用一些工具对网络及服务器发起 Dos/DDos 攻击。

3.针对校园网络特点的安全解决方案

针对校园网络的特点并对其主要安全隐患进行分析,本文认为基于校园网络的安全解决方案应该将防护重点放在以下方面:网络信息过滤、网络安全隔离、网络监控措施、网络安全漏洞扫描、网络病毒的防范等。

3.1 正确设置路由器[1]

路由器、防火墙和核心交换机构成了校园网的核心,也就是我们平常说的网络中心,网络中心性能的好与坏将直接影响整个校园网的性能。路由器处在网络中心的最顶层,它直接与互联网连接,同时内连校园网中的防火墙,可以滤掉被屏蔽的 IP 地址服务。同时,路由器也可以过滤一些服务协议,进一步减少其他协议带来的安全隐患。在实际操作中,下面的几种配置路由器的方法能够对校园网起到一定的保护作用:

(1)修改默认的口令:大部分的突破事件是由薄弱的口令引起的。最好把默认的口令更改,避免使用普通的口令,并且使用大小写字母混合的方式作为更强大的口令规则。

(2) 禁用 HTTP 设置和 SNMP (简单网络管理协议): 路由器的 HTTP 设置部分对于一个繁忙的网络管理员来说是很容易的, 但是这对路由器来说也是一个安全问题。如果你的路由器有一个命令行设置,那么禁用 HTTP 方式并且使用这种设置方式;如果你没有使用你的路由器上的 SNMP,那么你就不需要启用这个功能。

(3)关闭 IP 直接广播(IPDirectedBroadcast):Smurf 攻击是一种拒绝服务攻击,在这种攻击中,攻击者使用假冒的源地址向你的网络广播地址发送一个 "ICMPecho"请求,这要求所有的主机对这个广播请求做出回应,这种情况至少会降低你的网络性能。以思科路由器为例,此时我们可以通过 "Central(config) #noipsource- route"这个指令关闭它的 IP 直接广播地址。

(4)封锁 ICMP(互联网控制消息协议)ping 请求:黑客能够利用你的路由器上启用的 ICMP 功能找出可用来攻击你的网络的信息。通过取消远程用户接收 ping 请求的应答能力,你就更容易避开那些无人注意的扫描活动或者防御那些寻找容易攻击的目标的 "脚本小子"(scriptkiddies)。

(5)禁用来自互联网的 telnet 命令:在大多数情况下,你不需要来自互联网接口的主动的 telnet 会话, 如果从内部访问你的路由器设置会更安全一些。

(6) 关闭 IP 源路由和 IP 重新定向:IP 协议允许一台主机指定数据包通过你的网络的路由,用于诊断连接故障。但是,这种用途很少应用。这项功能最常用的用途是为了侦察目的对你的网络进行镜像,或者用于攻击者在你的专用网络中寻找一个后门。除非指定这项功能只能用于诊断故障,否则应该关闭这个功能。

3.2 部署防火墙 防火墙作为一种将内外网隔离的技术, 普遍运用于校园网安全建设中。一个防火墙(作为阻塞点、控制点)能极大地提高一个内部网络的安全性,并通过过滤不安全的服务而降低风险。[2] 在防火墙设置上我们按照以下原则配置来提高网络安全性:

(1)根据学校网络安全策略和安全目标,规划设置正确的安全过滤规则,严格禁止来自公网对校园内部网不必要的、非法的访问。

(2)将防火墙配置成过滤掉以内部网络地址进入路由器的 IP 包,这样可以防范源地址假冒和源路由类型的攻击; 过滤掉以非法 IP 地址离开内部网络的 IP 包,防止内部网络发起的对外攻击。

(3)为每个内网用户设置可使用流量最大值,控制内网用户访问 Internet 时间。

(4) 在防火墙上建立内网计算机的 IP 地址和 MAC 地址的对应表,防止 IP 地址被盗用。

(5)在局域网的入口架设千兆防火墙,并实现 VPN 的功能,在校园网络入口处建立第一层的安全屏障,VPN 保证了管理员在校外也能够安全接入数据中心。

(6)定期查看防火墙访问日志,及时发现攻击行为和不良上网记录。

(7)允许通过配置网卡对防火墙设置,提高防火墙管理安全性。

3.3 在入侵检测系统(IDS)的基础上架设入侵防御系统(IPS) IDS(IntrusionDetectionSystems)[3]是一个监听设备,主要用来监视和记录网络的流量,根据定义好的规则来过滤从主机网卡到网线(下转第 58页)

比较内容 / 方案名称	SAP 合同数据进入 OA 系统的方式	优点	缺点
方案一	录入完毕，SAP 调用 COM，对 OA 进行推数据操作，并调用 OA 中的代理进行数据初始化	效率高、实时性高、对服务器负载要求低、流程顺畅。	SAP 开发量有所增加，需要调用 COM 来进行推数据操作，以及驳回和通过对标识位修改的 RFC 开发。
方案二	录入完毕，SAP 通过 COM，调用 OA 中的代理执行 SAP 中应搜索新合同的 RFC 函数，获取需要审批的合同信息，并在 OA 中新建新的审批流程。	SAP 开发量比方案一少一点，需要对 COM 调用 OA 代理、搜索新合同、驳回修改标识和完成修改标识进行 RFC 开发、实时性较高、对服务器负载要求低、流程顺畅。	由于触发需要 2 步走，效率相应较低。
方案三	SAP 将合同信息导入具体 Excel 中，FTP 到 OA 服务器指定目录，由 OA 中设置定时代理，获取需要审批的合同信息，并在 OA 中新建新的审批流程。	SAP 开发量较少，需要对搜索新合同、驳回修改标识和完成修改标识进行 RFC 开发。	实时性低、服务器定时代理，因此负担比较大、接口稳定性低，特别是 FTP、网络因素对系统影响大
方案四	SAP 生成对应合同信息文件，由专人在 OA 中新建新的审批流程，嵌入合同信息。	开发量最少	审批过程驳回和通过都由专人对 SAP 进行维护修改、自动化程度低、人为因素突出、实用性差
方案五	OA 中设置定时代理，通过对应搜索新合同的 RFC 函数，获取需要审批的合同信息，并在 OA 中新建新的审批流程。	SAP 开发量较少，需要对搜索新合同、驳回修改标识和完成修改标识进行 RFC 开发。	实时性低、服务器定时代理，因此负担比较大、接口稳定性较低

图 3.1 本系统设计方案比照表

3.2 方案选择与确认

分析上述的五个方案，在理论分析上来看，方案一是最好的，实时性好、对服务器负载也低。但是在测试过程中发现，由于采用一种推的方式将合同提交到 OA，需要经过三层（sap- com- Notes 代理- Notes 文档）才能到达 Notes 文档，中间层的 com 对于用户是完全不可见的，即使发生错误消息也很难捕捉、反馈。而 Notes 代理在这个调用过程中也不能进行调试等工作，由此产生的问题就是：对于 SAP 用户来说就无法知道是否将合同成功提交至 OA，从而就很难确认是否该在 SAP 中锁定合同信息。另一个问题就是：执行这一个过程所需时间比较长，如果碰到网络连接等问题时易发生提交失败的现象。

方案二存在类似问题。

方案三操作就更加繁琐了

方案四手工式操作太多

最后观察方案五；该方案采用拉的方式，SAP 端写好所有的 RFC 之后，大部分操作都在 OA 端，充分利用 OA 系统中工作流的机制，对于执行结果可以进行很好的监控和信息捕捉。对于该方案中提到的缺点可以通过增大定时代理执行时间和一定程度上的“隐藏式手动操作”（比如在用户进入该系统时后台进去操作），可以大大改善效果。

综上所述我们最终采用的就是方案五。

综合上述分析，笔者在仔细分析考虑 OA 与 ERP 整合的各种因素后，提出了 OA 系统与 ERP 系统集成的五种方案，基于充分利用原有 OA 系统工作流技术的出发点，而且考虑到该企业运用 OA 系统进行公文流转已经非常成熟，因而选择了在目前技术条件下最佳的 SAP 与 OA 通讯技术方案。科

参考文献

[1] 张洪波. 工作流管理在 ERP 系统中应用研究. 企业管理信息化，2005.9,9~10.
[2] 康英杰,王玉善.浅析 ERP 中控制流的实现与作用.南京理工大学学报（社会科学版）,2004.8,17 卷第 4 期,59~61.
[3] 宋文津,李广莉.OA 系统中的工作流技术及其新的模式.办公自动化杂志,2006,8.11~12.
[4] 夏定元,周曼丽.基于知识管理的 OA 系统开发与应用[J].计算机工程与应用,2002,9:252~256.
[5] 林琪,王宇,卢昱.办公行文自动化管理系统的开发.微机发展[J],2000,10(5):48~50.
[6] 周源.ERP 和 OA“二重奏”.IT 经理世界,2006.12,72.
[7] 郭应中,宛延闿,韩伟.基于工作流的 OA- ERP 集成.微计算机应用,2003,3.24 卷第 2 期.65.

（上接第 55 页）上的流量，而 IPS(IntrusionPreventionSystem)是一种主动的、智能的入侵检测、防范、阻止系统,简单地理解，IPS 的检测功能类似于 IDS，但 IPS 检测到攻击后会采取行动阻止攻击，可以说 IPS 是一种基于 IDS 的、建立在 IDS 发展基础上的新生网络安全产品，架设一个 IPS 是非常必要的。[4]

3.4 漏洞扫描系统 采用先进的漏洞扫描系统定期对工作站、服务器、交换机等进行安全检查，并根据检查结果向系统管理员提供详细可靠的安全性分析报告，为提高网络安全整体水平产生重要依据。另外，要求每台主机系统必须正确配置，为操作系统打够补丁、保护好自己的密码、关闭不需要打开的端口，例如:如果主机不提供诸如 FTP、HTTP 等公共服务，尽量关闭它们。

3.5 部署网络版杀毒软件 在整个局域网络内可能感染和传播病毒的地方采取相应的防病毒手段。同时为了有效、快捷地实施和管理整个网络的防病毒体系，应能实现远程安装、智能升级、远程报警、集中管理、分布查杀等多种功能。一般实现方法如下：

在学校网络中心配置一台高效的 Windows2000 服务器，安装一个网络版杀毒软件系统中心，负责管理校园网内所有主机网点的计算机，在各主机节点分别安装网络版杀毒软件的客户端。安装完杀毒软件网络版后，在管理员控制台对网络中所有客户端进行定时查杀毒的设置，保证所有客户端即使在没有联网的时候也能够定时进行对本机的查杀毒。网络中心负责整个校园网的升级工作。为了安全和管理的方便起见，由网络中心的系统中心定期地、自动地到杀毒软件网站上获取最新的升级文件(包括病毒定义码、扫描引擎、程序文件等)，然后自动将最新的升级文件分发到其它各个主机网点的客户端与服务器端，并自动对网络版杀毒软件进行更新。

采取这种升级方式，一方面确保校园网内的杀毒软件的更新保持同步，使整个校园网都具有最强的防病毒能力；另一方面，由于整个网络的升级、更新都是有程序来自动、智能完成，就可以避免由于人为因素造成网络中因为没有及时升级为最新的病毒定义码和扫描引擎而失去最强的防病毒能力。

4.结束语

除此之外，校园网络的管理者还需要建立一套校园网络安全管理模式,制定详细的安全管理制度,如机房管理制度、病毒防范制度等,并采取切实有效的措施保证制度的执行从而更有效地保障校园网络的可靠运行。随着新的安全问题的不断涌现，校园网络的管理者还必须根据不断变化的形势和现有管理办法中暴露出的问题，对已有的校园网安全解决方案进行及时的维护和更新，保证校园网络的正常使用和良性发展。科

参考文献

[1] 张志钢.路由器安全管理技术[J].天津城市建设学院学报.2003.9(4):284- 286.
[2] 何泾沙.Linux 防火墙[M].北京：机械工业出版社.2006.
[3] 高光勇，迟乐军.联动防火墙的主机入侵检测系统的研究[J].微计算机信息.2005.7.
[4] 李小平，王意洁，王勇军.入侵防御系统的研究与设计[J]，微计算机信息.2006.11(3).

作者简介：周晓虹(1980.1-)，女，福建人，中学一级教师。