高校信息系统服务器安全管理规范探讨

王明宇,史 娜
(黑龙江林业职业技术学院信息中心,黑龙江 牡丹江 157011)

摘 要:本文根据高校信息系统服务器维护经验,总结了一些安全管理的要点,提出了管理员应遵循的服务器部署要求及厂商工程师维护管理要求,是形成高校信息系统服务器安全管理规范的主要内容。

关键词:网络安全;服务器;管理制度
【DOI】10.12231/j.issn.1000-8772.2021.01.107

1 引言

高校信息系统服务器主要采用两种方案:一是虚拟化平台(国内主要厂商华为、深信服等,国外主要厂商 vmware 等);二是实体机服务器。无论采用哪种方案,单纯依靠技术不能解决所有的安全问题,必须配套相应的管理手段。安全管理规范是必要而且非常重要的辅助手段。

2 人员安全管理

配备专职的系统管理员可以让管理工作落实到专人上,可以更高效的开展安全管理工作。识别出关键事务岗位,对这些关键岗位配备多人进行共同管理,以防止疏忽,并且建立起约束和监督机制。对安全工作的开展情况进行审核和检查可以及时、有效的督促安全制度和安全技术的执行、运作情况,减少安全疏忽,及时发现并解决问题,使安全工作日常化、制度化。

系统管理员要做到:(1)每周进行安全检查,检查内容包括系统日常运行、系统漏洞和数据备份等情况;(2)每季度进行全面安全检查,检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等;(3)每次检查都要制定安全检查表格实施安全检查,汇总安全检查数据,形成安全检查报告,并对安全检查结果进行通报;(4)将上述工作要求写入《安全审核和检查管理制度》,用以规范安全审核和安全检查工作的频率等重要内容。

3 服务器部署管理

无论采用虚拟化平台还是实体服务器进行系统部署,安装可靠的操作系统是服务器安全的基本保障。高校服务器常见操作系统类型主要有 centOS 和 windows server。官网下载可以保证资源的完整性、可用性和安全性;Centos 官网地址为 https://www.centos.org。windwos server 操作系统可以从官方网址下载,也可以到网站 https://msdn.itellyou.cn/下载。不能使用网上任意搜索到的镜像安装,无法保证系统的可靠性。系统管理员最好能够按照厂家的要求进行操作系统安装,或监督软件厂家工程师进行安装,做到心中有数。操作系统安装完毕,要进行以下配置才能够进行应用系统的安装:(1)操作系统防火墙配置。充分利用操作系统自身的防火墙功能,配置禁止全部入栈、出站通信,只开放应用系统所用到的端口,实现服务器间横向的隔离。(2)用户配置。账号和密码保护可以说是服务器系统的第一道防线,目前网上大部分对服务器系统的攻击都是从截获或猜测密码开始。对服务器系统管理员的账号和密码进行管理是保证系统安全非常重要的措施。禁用 root、administrator 等系统默认管理员账户,根据不同权限等级,设置不同管理员账户,并做到一机一密码,避免使用弱密码。(3)常用端口修改。修改远程桌面默认端口 3389;修改常用数据库默认端口,如 sql server 端口 1433,mysql 端口 3306,oracle 端口 1521 等。并在操作系统防护墙配置中开放新设置的端口。(4)系统补丁。不论是 Windows 还是 centOS,任何操作系统都有漏洞,及时的打上补丁避免漏洞被黑客利用,是服务器安全最重要的保证之一。如果配备了终端响应检测平台(Endpoint Detection and Response)将为系统维护提供极大的便利,除了可以进行病毒扫描外,还可以自动对系统进行漏洞扫描,自动安装补丁程序。服务器应尽量避免与外网直接通讯,必要时可以手动安装补丁程序,国家安全漏洞共享平台 https://www.cnvd.org.cn/中可以查到最新的漏洞补丁信息。(5)关闭不需要的服务。服务器操作系统在安装时,会启动一些不需要的服务,这样会占用系统的资源、增加系统的安全隐患。应该关闭不需要的服务,如 Telnet 等。以上配置完成后,再允许软件厂商工程师安装应用系统,可在调试过程中发现哪些端口使用了默认端口没有修改,避免厂商工程师为了方便调试,使用开放的环境。(6)日志管理。日志提供了有关网络活动的第一手信息。服务器要保存 60 天以上的系统运行日志和用户使用日志记,以便进行问题分析和攻击溯源。

4 软件厂商工程师维护管理

应用系统的安装离不开软件厂商工程师,但工程师水平不一、工作不规范,如果不进行严格规范的管理,很多漏洞往往来自安装过程中。如:非法使用 U 盘、随意下载软件依赖程序等。要求软件厂商工程师做到:(1)系统安装只能通过管理机或堡垒机访问远程服务器进行安装。要访问远程服务器,设置 SSH 密钥身份验证。它比密码更安全。(2)所有安装程序包要经过病毒和木马扫描。(3)软件依赖程序必须在官方网站下载。如 dot net 框架程序、jar 文件、c++ 库等。(4)不能随意开放 vpn 账号。软件厂商工程师流动性比较大,虽然 VPN 账号只能访问特定系统,但往往给工程师分配的都是管理员账号,为安全带来隐患。尽量在管理员监督下使用管理机进行维护,只能使用 VPN 时,用完就关闭账号。

5 防火墙与 WAF 安全设置

操作系统自身的软件防火墙起到了服务器间横向隔离的作用。硬件防火墙则起到了纵向隔离的作用,在硬件防火墙中要按照一服务一策略的详细配置,细化到源 IP、源端口到目的 IP、目的端口的设置。安装 Web 应用防护系统(WAF)可以对访问请求进行控制,可以主动识别、阻断攻击流量,可以防范 WEB 攻击、DDOS 攻击、SQL 注入攻击等。

6 结束语

安全管理是一个系统工程,有的单位购买了大量防护设备,过了等级保护测评依然受到了攻击,遭受了损失,原因还是规范不到位,制度没有落实。只有科学合理制定规范、严格执行才能保证系统的安全、稳定运行。

参考文献

[1]信息安全技术网络安全等级保护基本要求.GBT22239-2019.
[2]网络安全等级保护条例.2018.

本论文为黑龙江省教育厅 2019 年度高等职业教育教学改革研究项目《网络安全等级保护 2.0 制度下智慧校园网络安全防护措施与制度建设研究》(课题编号:SJGZZ2019030)阶段性成果