中国地质大学（北京）

信息网络中心文件

信息网络中心　　2013.5.15

学校主页信息安全管理

一、技术层面

1、系统架构

学校主页网站采用目前主流的J2EE技术架构（Struts2+Spring+Hibernate）。基于J2EE的应用程序具有平台独立性特点，即不依赖任何特定操作系统、中间件、硬件，网站系统只需开发一次就可部署到各种平台。

由于平台无关，网站系统部署在安全性更好地Linux操作系统（CentOS）环境下，相较于Windows系统，Linux操作系统下漏洞、病毒、木马较少，具有更高的安全性和稳定性。

应用服务器采用Tomcat RAC集群，Tomcat RAC使用Tomcat自带的cluster方式，由两个节点组成，两个节点同时运行提供服务，实现负载均衡和冗余，当一个节点出现故障，不会影响应用服务器的正常运行。

Web服务器采用ApacheHTTP Server（简称Apache），它

是Apache软件基金会的一个开放源码的网页服务器，可以在大多数计算机操作系统中运行，由于其多平台和安全性被广泛使用，是最流行的Web服务器端软件之一。

2、网站与数据库分离

为了保证数据库的安全，采用网站系统和数据库分离的方式，网站系统部署在前端，数据库由独立的数据库服务器在后端提供服务。数据库服务器设置有严格的防火墙过滤规则，仅限于管理员的IP登陆访问。网站系统和数据库之间采用私有地址连接，当网站被攻击或入侵时，由于网站系统和数据库分离，能够较好的防范数据库被攻击，防止数据泄露。

3、HTML 静态化

网站访问时，效率最高、消耗最小的是纯静态化的html页面，为了提高性能，主页网站上的页面大部分采用静态页面来实现。由于学校网站主页内容较多并且需要频繁更新，由信息网络自举开发了Cms系统来实现信息的发布与管理，Cms系统可以实现最简单的信息录入自动生成静态页面。网站静态化有如下优点:

（1）静态网页化之提高速度

主页网站JSP动态程序需要读取调用数据库内容，才能显示数据，相对于流量比较大，就增加了数据库的读取次数，占用很大的服务器资源，影响网站速度。而采用网站做成静

态的，直接除去了读取数据库的操作，减少了环节，提高了网站反映速度。

（2）静态网页化之搜索引擎

从网站优化来分析，搜索引擎更喜欢静态的网页，静态网页与动态网页相比，搜索引擎更喜欢静的，更便于抓取，搜索引擎SEOpaiming更容易提高。

（3）静态网页化之网站稳定

从安全角度讲，静态网页不宜遭到黑客攻击，除开源程序采用的是开源Cms，如果黑客不知道你网站的后台、网站采用程序、数据库的地址，静态网页，更不容易受到黑客的攻击。

从网站稳定性来讲，如果程序、数据库出了问题，会直接影响网站的访问，而静态网页就避免了如此情况，不会因为程序等，而损失网站数据，影响正常打开，损失用户体验，影响网站信任度。

4、虚拟化与主备镜像

为保证主页网站的稳定运行，尽量减少服务器故障率和对外服务宕机时间。主页网站部署在VMware虚拟化服务器上，当主页网站所在虚拟机的物理服务器出现故障时，虚拟机可以在物理服务器之间漂移，这样可以避免出现系统宕机。

另外，主页网站还配置有一台备用镜像服务器，当主页网站出现故障或网页内容被篡改导致无法恢复时，立即启用

备用镜像服务器，恢复学校网站系统的正常运行，以尽量减小学校网站的对外服务宕机时间。

5、定期扫描、安全分析、加固

采用绿盟漏洞扫描系统定期对主页网站漏洞进行安全扫描，根据扫描结果对网站进行安全性评估，分析主页网站的安全隐患，找出相关的解决办法，对服务器进行防护加固，如果是网站系统代码漏洞，修改相关代码，对漏洞进行修复。

6、网站监测

采用绿盟网站安全监测系统主动发现网站的风险隐患，并及时采取修补措施，则可以降低风险、减少损失。该系统能够根据站点管理者的监管要求，通过对目标站点进行不间断的页面爬取、分析、匹配，为客户的互联网网站提供远程安全监测、安全检查、实时告警，是构建完善的网站安全体系的最好补充。其特点有：

（1）综合运用Web应用信息重整化（Web Profile）等多种领先技术，自动、高效、及时准确地收集监测站点的所有信息；

（2）专业的Web应用扫描模块，可以自动化进行Web应用、Web 服务及支撑系统等多层次全方位的安全漏洞扫描，简化安全管理员发现和修复 Web 应用安全隐患的过程；

（3）多项网页木马检测专利技术，提供最为准确的检

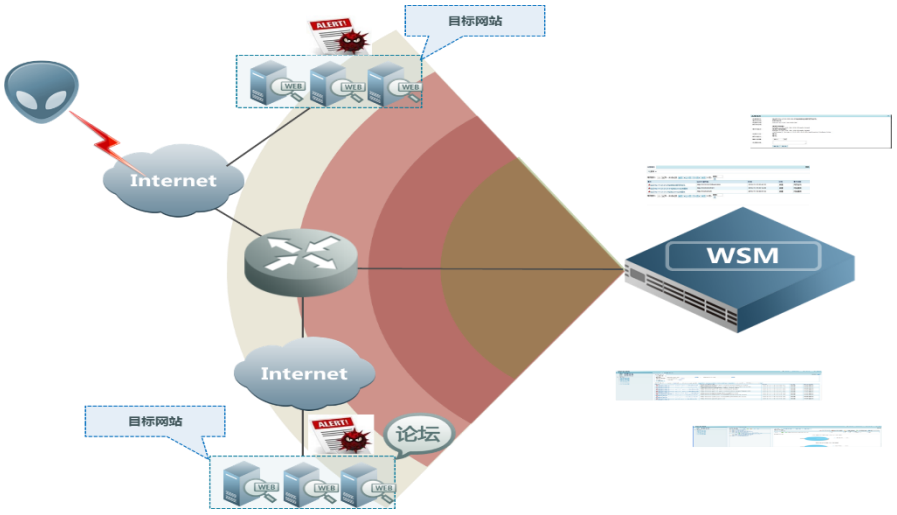
测效率；

（4）先进网页篡改检测技术，有效保护网页安全；

（5）高效的网页敏感信息检测技术

（6）基于DOM结构进行页面细粒度分析，对篡改事件提供准确的检测；

（7）灵活、可扩展的架构设计，满足监测站点高频率的监测要求，并能够对监测的目标站点形成统一的风险对比、及趋势分析。



二、管理层面

1、值班

网络中心制定有一套规范的值班制度，根据值班安排，值班人员内需定期对学校网站进行监控，如果发现异常情况，及时联系相关技术人员进行处理。

2、紧急处理

➢ 网站受攻击时的紧急处置措施

当发现网站被攻击时，如访问速度慢、网页内容被篡改、系统不稳定等情况

（1）检查校园网运行状态，排除因网络故障引起的不正常情况。

（2）立即将被攻击的服务器等设备从网络中隔离出来，同时向领导汇报情况。

（3）将重要数据从被攻击服务器中备份到其他介质上，启用反病毒软件对这些数据进行杀毒处理，如发现反病毒软件无法清除病毒，应立即向领导报告

（4）分析日志文件，查找网站被攻击的原因；如果是操作系统漏洞，对操作系统进行补丁升级，修复系统漏洞；如果是软件系统漏洞，查询相似的被攻击情况和解决方案，进行修补工作

➢ 软件系统遭受破坏性攻击的紧急处置措施

（1）重要的软件系统平时必须存有备份，与软件系统相对应的数据必须有多日备份，并将它们保存于安全处。

（2）立即向技术人员、网络管理员报告，并将系统停止运行。

（3）启动备用网站系统，立即进行软件系统和数据的恢复。，尽量减小学校网站的对外服务宕机时间

（4）查找软件遭受破坏性攻击原因，一旦查明，找出解决方案，并记录在案。

- **硬件故障的紧急处置措施**

（1）一旦硬件故障，应立即向技术人员、网络管理员报告，并将系统停止运行。

（2）启动备用服务器，立即进行网站系统的恢复，尽量减小学校网站的对外服务宕机时间

（3）联系厂家硬件维修

- **数据库安全紧急处置措施**

（1）各数据库系统要至少准备两个以上数据库备份。

（2）一旦数据库崩溃，应立即向技术人员报告，同时暂缓上传数据。

（3）利用数据库备份，恢复数据库

（4）如因第一个备份损坏，导致数据库无法恢复，则应取出第二套数据库备份加以恢复。

（5）如果两个备份均无法恢复，应立即向有关厂商请求紧急支援

（6）数据库在本地和异地均要有备份