北京師範大學
BEIJING NORMAL UNIVERSITY

学为人师 行为世范

开展安全评估与规划、实施主动防御 建立安全公共服务平台

—北京师范大学校园网安全建设经验交流

刘臻

北京师范大学信息网络中心

2009年5月26日

学校信息网络安全面临的挑战

学校网络信息安全工作思路

经验与体会

学校信息网络安全面临的挑战

网络信息安全建设不够完善，网络设备、校级服务器、服务器运行系统的安全漏洞情况不够清晰

信息系统未能安全运行，不能保证web网站的健康正常运行

面对信息安全的突发状况，应急服务不够完善

信息网络安全问题

安全意识和安全管理水平不高

缺乏完善的安全管理制度与安全文档

技术人员不具备独立应对网络突发状况的能力

学校网络信息安全建设理念

技术 → 信息 → 理念

1. 应对变化：信息安全范围在扩大，深度在增加
2. 知己知彼：　开展“安全评估”是关键
3. 被动变主动：　开展“加固”，主动防御
4. 资源公共化：　建立校园网安全服务公共支持平台

学校网络信息安全建设工作内容

1. 开展校园网络信息安全评估
2. 制定网络信息安全建设规划和加固措施
3. 完善网络信息安全管理制度
4. 加强网络信息安全人员队伍建设和培训

网络信息安全评估

安全评估

通过工具评估、人员评估、弱点评估、审计评估、综合风险分析等方式对网络设备、安全管理、人员、制度、业务系统等40多台设备、20多类应用进行全方面的安全评估；提出相应的安全建议，指导下一步的信息安全建设

取得效果

明晰了我校目前校园网络设备、校级服务器、服务器运行系统的安全漏洞情况，同时结合相关要求设计切实可行的整改方案，保障信息系统的安全运行，保证web网站的健康正常运行

网络信息安全评估内容案例

Internet访问

WEB网站

信息门户网站

网络信息安全评估--服务器漏洞及脆弱性评估

服务器名称	漏洞数量统计
WEB主站1-202.112.*.*	中风险漏洞： 14个
WEB主站2-202.112.*.*	无
教师邮件系统	高风险21个
学生邮件系统	高风险漏洞：9个；
域名服务系统	高风险漏洞：4个
数字校园应用服务器	高风险漏洞：9个
应用前置WEB服务器	高风险漏洞：1个
师大综合社区服务器	高风险漏洞：4个
数字博物馆系统	高风险漏洞：1个
应用系统服务器	高风险漏洞：1个

Internet访问评估

业务名称	Internet系统					
安全属性 受影响主体	保密性 （泄露 … …）		完整性 （修改、破坏 … …）		可用性 （损坏、中断 …）	
	描述	等级	描述	等级	描述	等级
承载的业务	无影响	1	信息被损害，导致网站系统使用出错	2	网站系统中断	2
单位利益	网站信息为可公开信息，泄漏后无影响	1	信息被破坏，会造成网站发布信息出错，从而导致公众信任丧失，影响单位形象	2	公众无法浏览信息，对单位形象也有一定的影响	2
公众利益	网站信息为可公开信息，泄漏后无影响	1	信息发布数据如果被修改，会影响单位的形象	2	业务中断，公众没有影响	2

取得效果

通过对Internet访问进行了有效的检测与加固，取得了良好效果，不仅提高了Internet访问的安全性，也保证了数据的保密性和业务系统的高可用性

WEB网站评估

业务名称	WEB网站系统					
安全属性 受影响主体	保密性 （泄露 … …）		完整性 （修改、破坏 … …）		可用性 （损坏、中断 …）	
	描述	等级	描述	等级	描述	等级
承载的业务	无影响	1	web网站信息如被修改，会影响到学校形象	2	web网站系统如中断，对学校形象会造成很大影响	3
单位利益	无影响	1	web网站信息如修改，会对学校形象造成损害	2	web网站系统如中断，会损害学校形象	3
公众利益	无影响	1	web网站信息如修改，会对学校形象造成损害	2	web网站系统如中断，会损害学校形象	2

取得效果

通过对WEB系统进行了有效的检测、评估、分析与加固，提高了web系统的安全性，保证了业务系统的高可用性

信息门户网站评估

业务名称	信息门户网站系统					
安全属性 受影响主体	保密性 （泄露 … …）		完整性 （修改、破坏 … …）		可用性 （损坏、中断 …）	
	描述	等级	描述	等级	描述	等级
承载的业务	会造成重要信息泄密	1	信息如果被损害，会导致相关业务正常运行	2	系统中断，会严重影响相关业务的正常运行	3
单位利益	会造成重要信息泄密	2	信息门户网站信息如损害，会使得学校业务出错，影响单位业务的执行，会造成一定的延迟	2	信息门户网站系统如果中断，会降低单位内部办公的效率，从而导致单位业务处理延迟	3
公众利益	会造成重要信息泄密	2	信息如果被损害，影响相关业务的开展	2	信息门户网站系统如果中断，会降低个人办公的效率，从而导致个人业务处理延迟	2
社会利益	无影响	1	无影响	1	无影响	1
国家利益	无影响	1	无影响	1	无影响	1
单一安全属性	对保密性的要求较低	2	对完整性的要求较低	2	对可用性的要求较高	3
综合安全属性	对保密性、完整性要求较低，对可用性的要求较高 等级：3					

取得效果

信息门户网站进行了有效的检测、评估、分析与加固，提高了信息门户网站的安全性、完整性和保密性，同时也有力保证了业务系统的高可用性

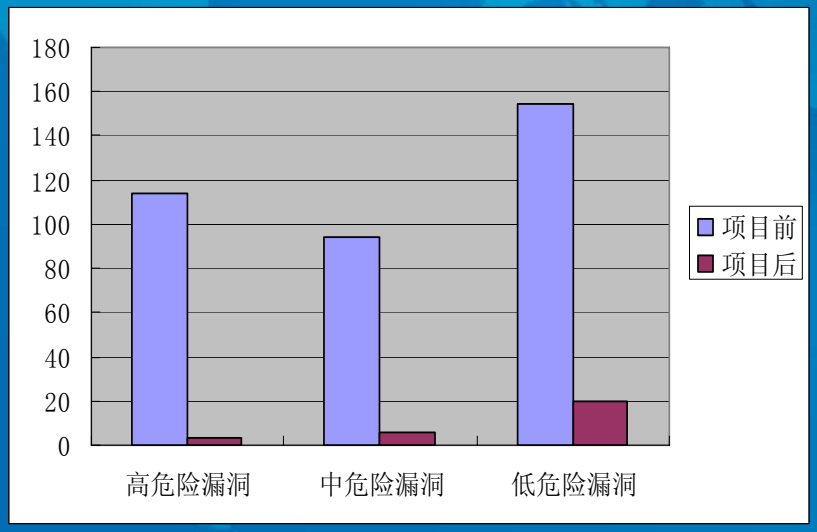
安全加固

对信息系统、网络系统、一卡通进行安全加固

安全加固

针对信息系统安全评估发现的高中风险漏洞，对我校的信息系统进行了安全加固工作，其中，针对操作系统的加固有21个，针对应用类的加固有40个

取得效果



- 信息系统存在的高、中风险漏洞比之前大大降低，提高了信息系统的安全水准。
- 我校准备以后进行周期性安全评估加固服务工作，使信息系统始终维持较高的安全水平

备注：由于升级补丁需要重启服务器造成业务中断，造成部分服务器还存在高危险漏洞

开展的部分网络信息安全建设工作

建设统一身份认证系统

建设统一网络杀毒软件系统

建设高端网络防火墙

部署邮件反垃圾网关

部署流控系统

建设网络信息安全咨询服务与应急服务项目

应急服务项目建设

应急服务

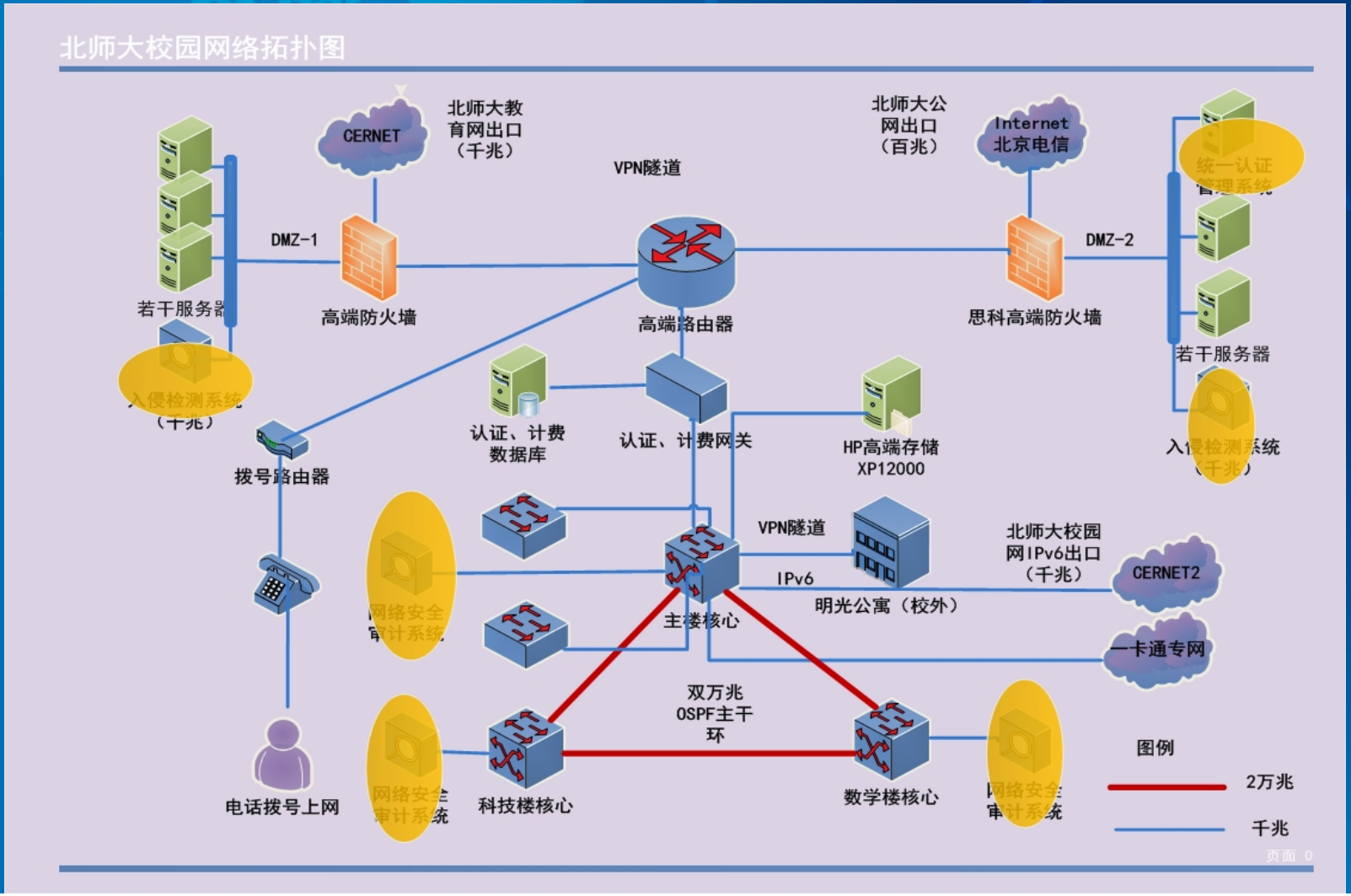
网络发生安全事件时，依靠自己的技术力难以得到有效解决时，可向专业安全公司提出应急响应服务的要求；安全公司在接到紧急事件报告后，会启动应急响应服务体系，提供安全专家紧急出动响应服务，协助恢复网络运行

取得效果

尽可能快的恢复网络的正常工作，并协助检查入侵来源，提供及时、全面的安全问题解决方案

北师大信息系统网络安全规划—全局网络部署视图

北师大信息系统安全技术体系建设贯彻纵深防御的思想，拟从网络基础设施建设、边界保护、局部计算环境保护、业务应用保护以及安全支撑设施来开展信息安全技术措施的建设。



北师大信息系统网络安全规划—安全系统建设

网络信息安全
设备建设规划

网络运行监控体系建设、网页防篡改系统

流量控制建设规划

终端安全防护建设规划

1. 不断完善安全建设的疏漏之处
2. 变被动为主动，加强事前监控优于事后补救
3. 针对业务系统的流量进行有效监控，提高网络整体运维效率
4. 加强终端安全防护的建设；降低由终端带来的安全风险

网络运行监控体系建设

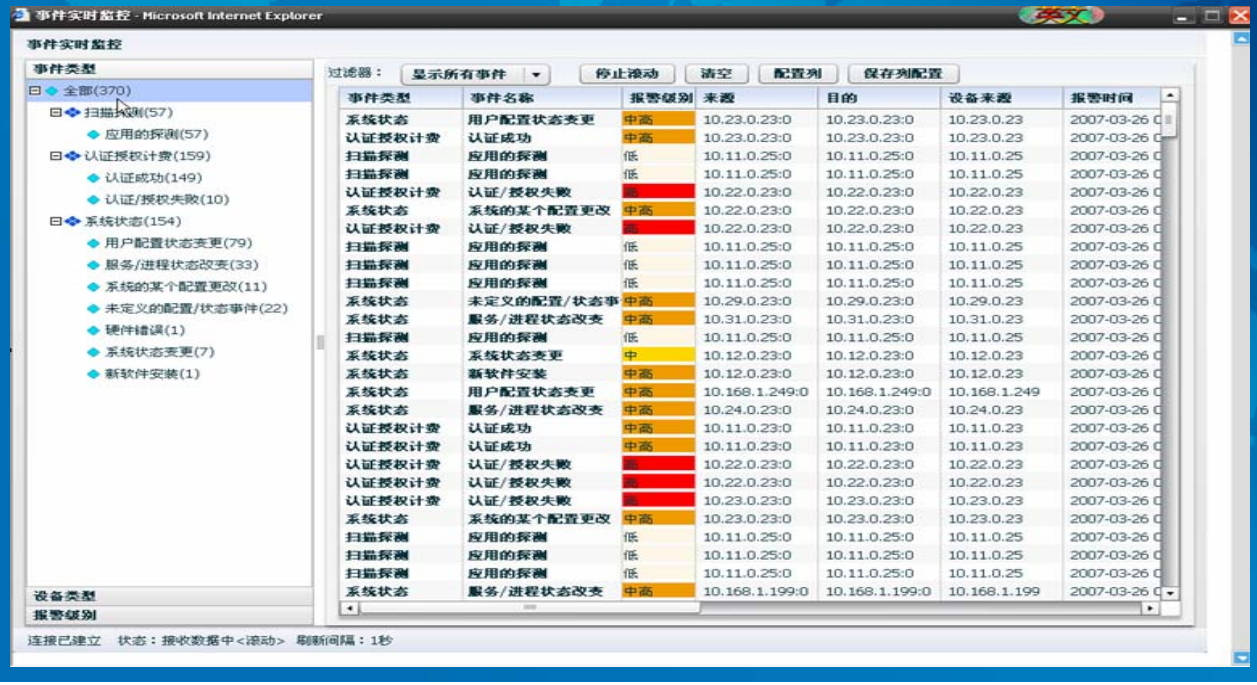
需求

网络运行
监控体系建设

建设规划

完善机房视频监控系统，对机房内访问行为进行记录和审计，网络中没有入侵检测机制，无法准确及时的定位网络安全事件

在核心交换机上部署入侵检测和防护系统；完善视频监控系统



流量控制建设规划

需求

没有全面的流量监控软件，不能对流量的变化做出判断和预测，网络出现故障无法迅速诊断，不能及时了解网络拥塞情况，无法及时发现异常为快速处理问题争取时间；带宽资源有限，须对内网的下载、在线视频等行为进行控制，避免下载应用占用大量带宽，影响正常业务的运行

通过具有流量分析、控制功能的安全类产品对带宽占用行为进行有效管控，从而保证优质网速，避免因网速影响而出现宕机、业务中断的危险

建设规划

终端安全防护建设规划

需求

某一终端出现病毒后，迅速在网络中蔓延
内部终端的未授权访问
内部终端滥用网络
IT资产管理不清晰

建设规划

通过建设具备终端管理能力的安全设备使终端各项安全指标达到预设的安全管理标准和效果，从而有效解决终端安全问题，达到规范终端安全防护的目的

完善安全管理制度

制度文档

安全与应急管理文档、信息分级与保密文档，技术设施文档、应用系统文档、机房环境文档、设备管理文档、信息监控文档

取得效果

建设了具有统一指导意义的安全策略和安全管理制度，建立起完善、系统、全面的安全管理组织机构，为合理有效的规范了信息安全管理流程，有利于在全校范围内推行统一安全策略

完善网络信息安全管理制度

制定场地安全管理制度

制定设备安全管理规范

制定系统安全管理规范

制定和实施信息监控规范

制定应急服务方案与信息报送流程规范

人员建设及培训

- 从08奥运开始，建立起分层、分级的网络信息安全监控梯队和安全情况“零问题”报送机制：以学校信息网络中心为核心，院系二级网管教师为支撑、学生兼职网管员为协助。

- 强化培训工作，提高网络技术人员的网络信息安全应急处理技能；通过专题演讲、典型事例宣传等方式，提高了学校师生的网络信息安全意识。

安全培训

安全培训

通过现场培训、集中专业培训两种方式培养学校自己的安全工程师。以充分提高技术人员的动手能力和安全分析能力。

取得效果

通过安全咨询项目的培训使我校技术人员的知识系统化，提高了技术人员的技术实力，同时培养了独立度思考自身网络配置及面临的安全威胁能力。使得我们技术人员的整体技术实力上一个台阶，为今后顺利地开展工作奠定扎实的基础。也提高了师生的网络安全意识。

经验与体会

1. 预防为主，检测与纠正并举的安全控制措施，定期开展安全评估
2. 安全问题发生的阶段越靠后，解决安全问题付出的代价越高
3. 虽然不能消除所有的风险，但是可以管理所有风险

要明确安全目标 ，有效进行整体安全规划，合理的配置网络设备，从而有效规避危害较大的安全事故。

加强业务系统管理人员安全管理意识

——“预防为主　响应为辅”　“主动多于被动”

谢谢！