北京大学网络与信息安全防护体系建设

张蓓

北京大学计算中心

2015年11月24日

汇报提纲

一、信息安全形势

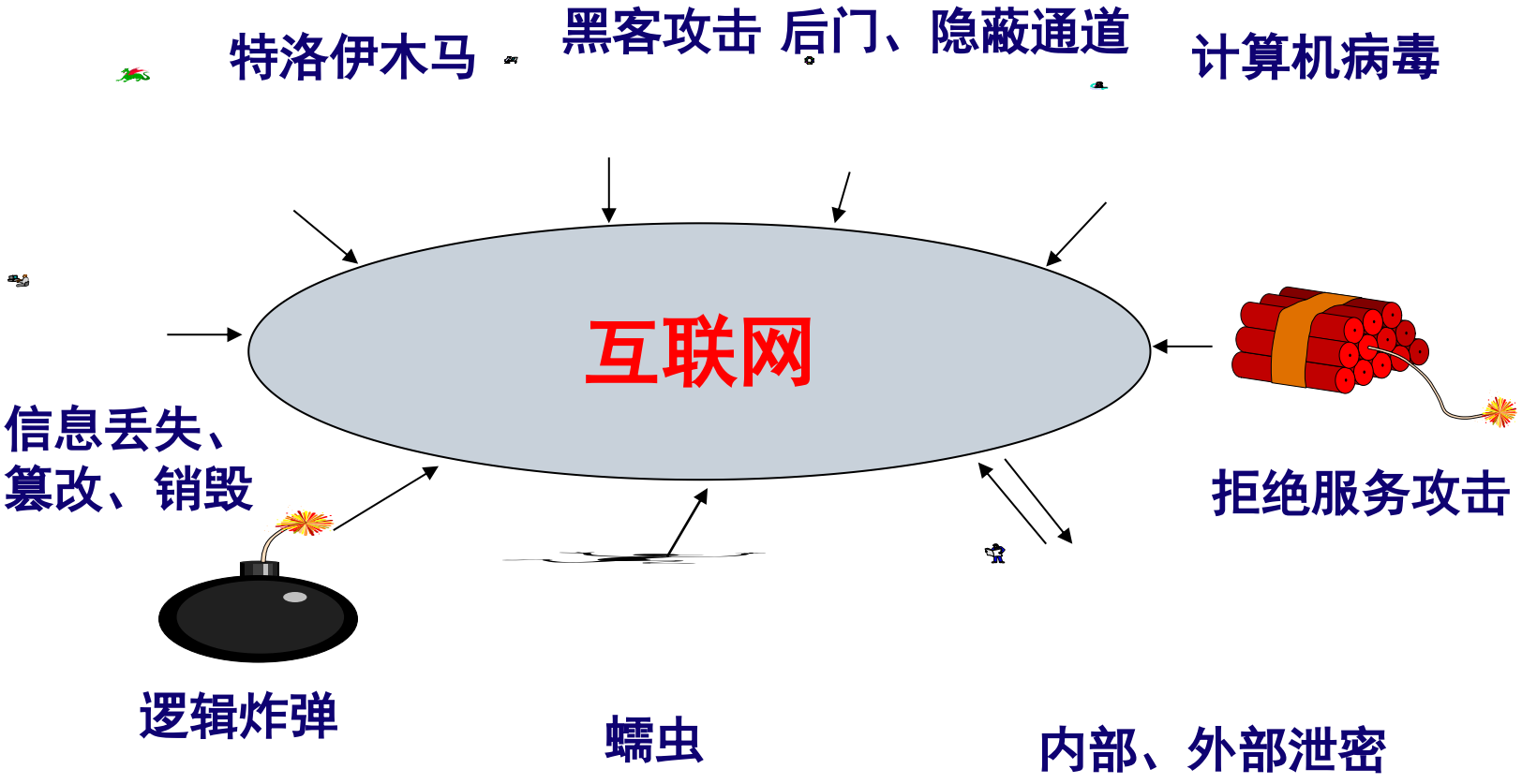
二、基本防护思路

三、安全防护

四、未来努力方向

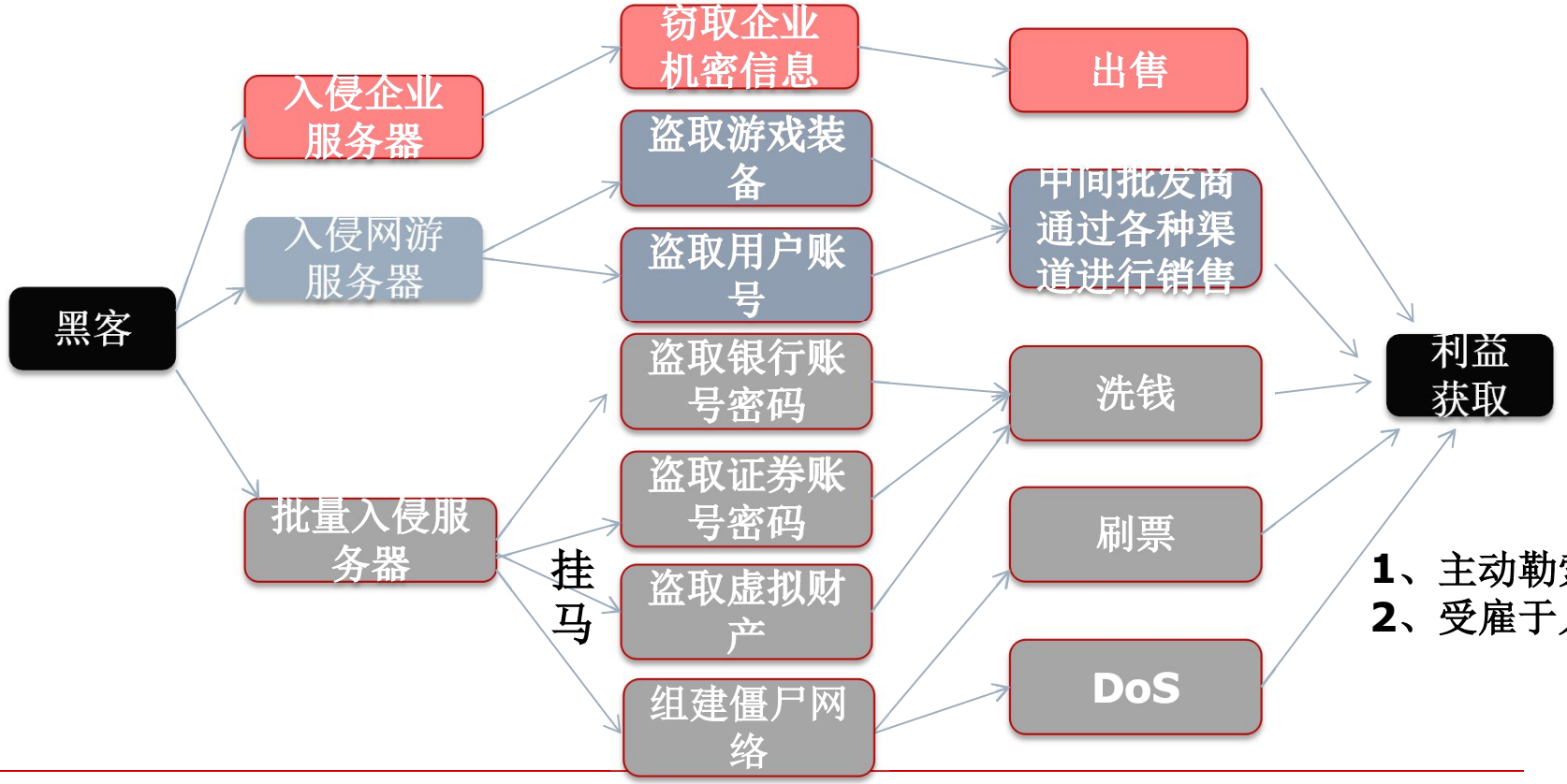
一、信息安全形势

- 恶劣的生态环境：被黑客包围



一、信息安全形势

□ 利益驱动，防不胜防



一、信息安全形势

- 国家战略
  - 网络与信息安全
    - 关系国家安全和主权、社会稳定
    - 随着全球信息化步伐的加快越来越重要
- 党中央高度重视
  - **2014年2月27日中央网络安全和信息化领导小组成立，习近平总书记任小组长**

网络安全和信息化是一体之两翼、驱动之双轮
必须统一谋划、统一部署、统一推进、统一实施

一、信息安全形势

- 教育部工作部署
  - **2014年10月** 教育部办公厅：《教育行业信息系统安全等级保护定级工作指南（试行）》
  - **2015年10月** 教育部办公厅：举办**2015**年度教育行业信息技术安全专题培训班
- 信息系统安全等级保护
  - 《中华人民共和国计算机信息系统安全保护条例》（国务院第**147**号令）
  - 《信息系统安全等级保护定级指南》（**GB/T 22240-2008**）
  - 《信息系统安全等级保护实施指南》（**GB/T 25058-2010**）
  - 《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安〔**2007**〕**861**号）
  - 《信息安全等级保护管理办法》（公通字〔**2007**〕**43**号）

二、基本防护思路

- 黑客=小偷
- 最大特点：贼偷方便
- 基本结论：无法杜绝
- 防护思路：制造麻烦
- 防护手段：层层设防
- 关键技术：隔离、躲猫猫
- 防范目标：让黑客少惦记
- 防护法宝：赢在执行

北京大学网络与信息安全防护体系

三个方面

安全防护	防火墙、**Web**应用防火墙、云**WAF**、**IPS**、防病毒、反垃圾邮件、漏洞扫描、安全评估、网站监控、堡垒主机、**VPN**
安全运维	摸清底数—学校网站与信息系统运维系统开发 理顺管理—域名和服务器账号申请、备案和废止流程，完善网站管理制度，清理僵尸域名及网站，每天轮询监控 应急响应—一键断网等
安全服务	为校内各单位提供服务器托管、源代码扫描、安全评估、渗透测试、监控服务、应急响应服务 为个人桌面提供必要的安全服务：杀病毒、**Windows**补丁更新

北京大学网络与信息安全防护体系

校园网边界	防火墙、**IPS**：阻断网络基础性攻击 **Web**防火墙：监控、阻断进入校园网的攻击 流量控制：抑制**P2P**，保障教学、科研 **VPN**：授权用户访问 **IP**控制网关：实名认证	网络服务 前台 后台 技术 网络管理 实时监控 短信报警
信息系统	信息系统安全等保建设 信息系统评测、**Web**网站监控 应急响应(一键断网)	
服务器	防火墙、**Web**防火墙、云**WAF**、 堡垒主机、**PVLAN**、负载均衡、漏洞扫描 垃圾邮件过滤、邮件防病毒	
用户终端	桌面防病毒(**Nod32**) 正版软件平台、**Windows**系统补丁更新 安全认证和接入交换机防**ARP**攻击	

三、安全防护

- 应用安全
- 网络安全
- 数据安全
- 安全运维

三、安全防护：应用安全

1、基础网络防护
2、网站防护
3、网站上线安全检测
4、系统及内容维护安全防护
5、开发环境防护
6、账号安全
7、北大主页安全防护措施
8、传输线路安全
9、数据库安全

三、安全防护：应用安全

1、做好服务器基础网络防护

- 两层包过滤防火墙，最好用不同品牌
  - 出口：粗粒度，阻断基础性网络攻击
  - 服务器群前：细粒度，精细化访问控制
- 开启**PVLAN**：私有**VLAN**
  - 隔离服务器网站间通信，无法侦听同一网段内的其他服务器账号、密码
  - 防范黑客跳板攻击，减少病毒传播
- 阻止未备案服务器上线运行

三、安全防护：应用安全

2、网站防护：基于WAF

- **WAF**：通过执行一系列针对**HTTP/HTTPS**的安全策略来专门为**Web**应用提供保护

两层WAF架构，防护全校网站

- 校园网边界：硬**WAF**，粗粒度，阻断确定漏洞
- 核心服务器群前：硬**WAF**，细粒度，精细化
- 分散独立网站：云**WAF**，细粒度，精细化
  - 跨越校园网：防护校内二级单位网站
  - 跨互联网：防护校外单位网站

三、安全防护：应用安全

3、网站上线安全防护：容易被忽视的环节

- 源代码白盒扫描，有问题整改到位
- 黑盒扫描：系统、**Web**漏洞，有问题整改到位
- 配置域名，配置网络防火墙和**Web**防火墙
- 加入网站监控队列
- 建立相关账号

□ 严格准入

三、安全防护：应用安全

4、系统维护、网站内容维护安全防护

- 校内：必须通过堡垒主机访问服务器
- 校外：通过专用**VPN**组进入校内，再登录堡垒主机访问服务器
- 服务器前防火墙设置
  - 只开**80**等**web**服务端口
  - 只允许堡垒主机访问

三、安全防护：应用安全

5、开发环境安全防护：容易忽视的重要环节

- 威胁
  - 开发和测试服务器中有测试用真实数据
  - 防护薄弱的开发计算机，可以成为黑客的跳板
- 措施
  - 开发服务器有单独的网段，与运行服务器隔离
  - 开发PC机、服务器均做IP/MAC绑定
  - 设立专用的开发VPN组，分配专有的IP地址
  - 防火墙保证专有的IP地址访问开发测试网段
  - 开发人员必须通过VPN访问开发测试服务器

三、安全防护：应用安全

6、用户账号安全防护

- 安全威胁
  - 用户名、密码：过于简单，失窃危险性大
  - 个人隐私泄露
  - 利用正常账号发送大量垃圾邮件，被封禁
- 实施用户弱口令限制
- 应用管理员账户安全防护：重要
  - 使用**USB Key**：职能部门嫌麻烦，难推广
  - 目前：用户名+密码+验证码：简便、可行

三、安全防护：应用安全

7、主页安全防护措施

- 采用静态页面：关键技术措施
- 独立的CMS：关键技术措施
  - 中文主页、英文主页、二级网站群：独立CMS
- 部署主页防篡改系统
- 选用安全可靠的CMS系统

三、安全防护：应用安全

8、传输线路加密

- 关键网站通过**https**访问
  - 购置受信**CA**证书：**VeriSign**
  - 门户网站、用户认证、邮件、**VPN**等
- 重要服务器之间通过**SSL**加密传输

9、数据库安全防护

- 数据库审计：操作可追踪、可回放
- 数据库加密：攻进来也拿不走
- 数据库**IP**访问控制：限制访问数据库的**IP**地址

三、安全防护：网络安全

- 校园网出口万兆防火墙
  - 阻断基础性攻击，如：不完整会话，TCP分片攻击
  - 会话数控制：单IP并发连接数
  - IP黑名单：迅速阻断攻击IP转发
  - IPS和Anti-DDoS：影响性能，关键时期打开
- 流控设备
  - 按时间策略压制P2P：优先保证教学、科研用网
- IP控制网关
  - 实名认证。攻击报文不能到达未登陆的主机。

三、安全防护：网络安全

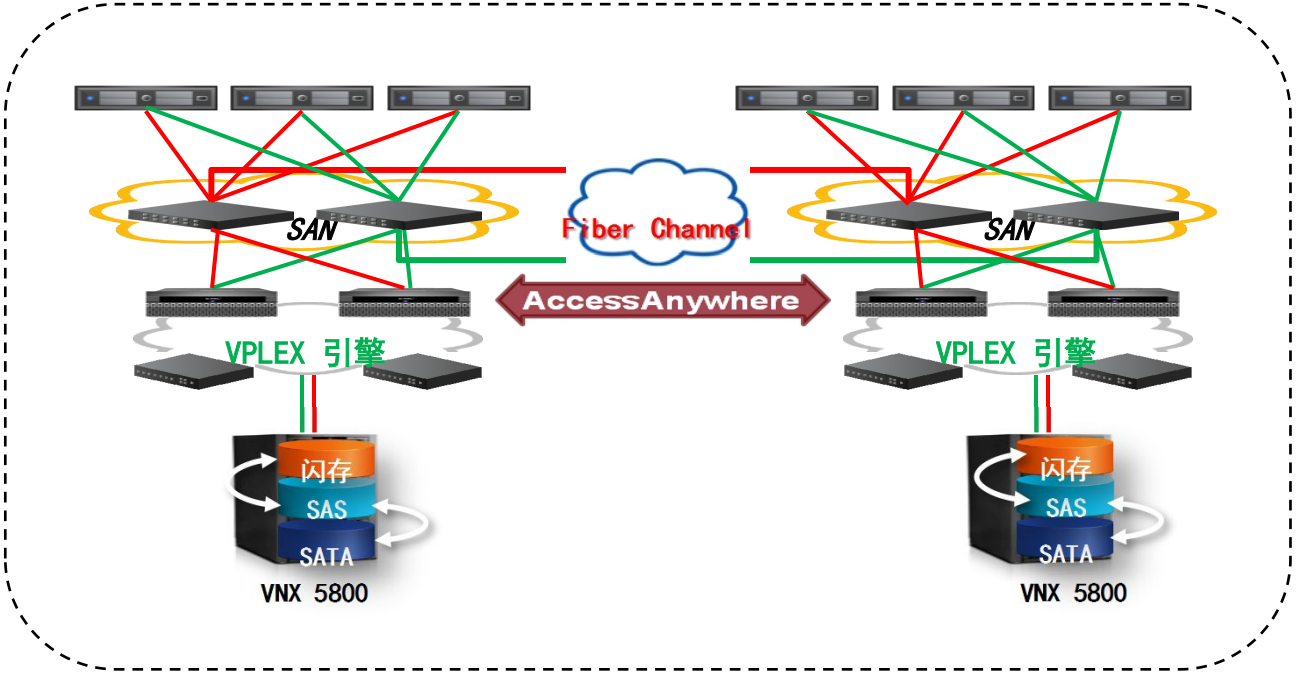
- 校园网出口路由器
  - 建立黑名单**ACL**，随时根据需要，封禁校内或校外攻击地址；
- **IP**网关实现一键封禁功能，在紧急情况下值班人员可以直接封禁；
- 核心/汇聚路由器
  - 对于有问题的**IP**，直接指向路由黑洞**Null0**；
  - 对所有用户网段，源地址检测、设置**ACL**，用于简单安全防护

三、安全防护：网络安全

- 接入层设备
  - 支持**arp detection**、**DHCP snooping**等
  - 防止**arp**攻击、私设**DHCP**
- 部署**SSL VPN**，实现入校园网访问安全
- 网络设备的配置管理实现**AAA**认证登录
- 网络设备和安全设备的日志实现统一接收、分析
- 无线网开启准入认证

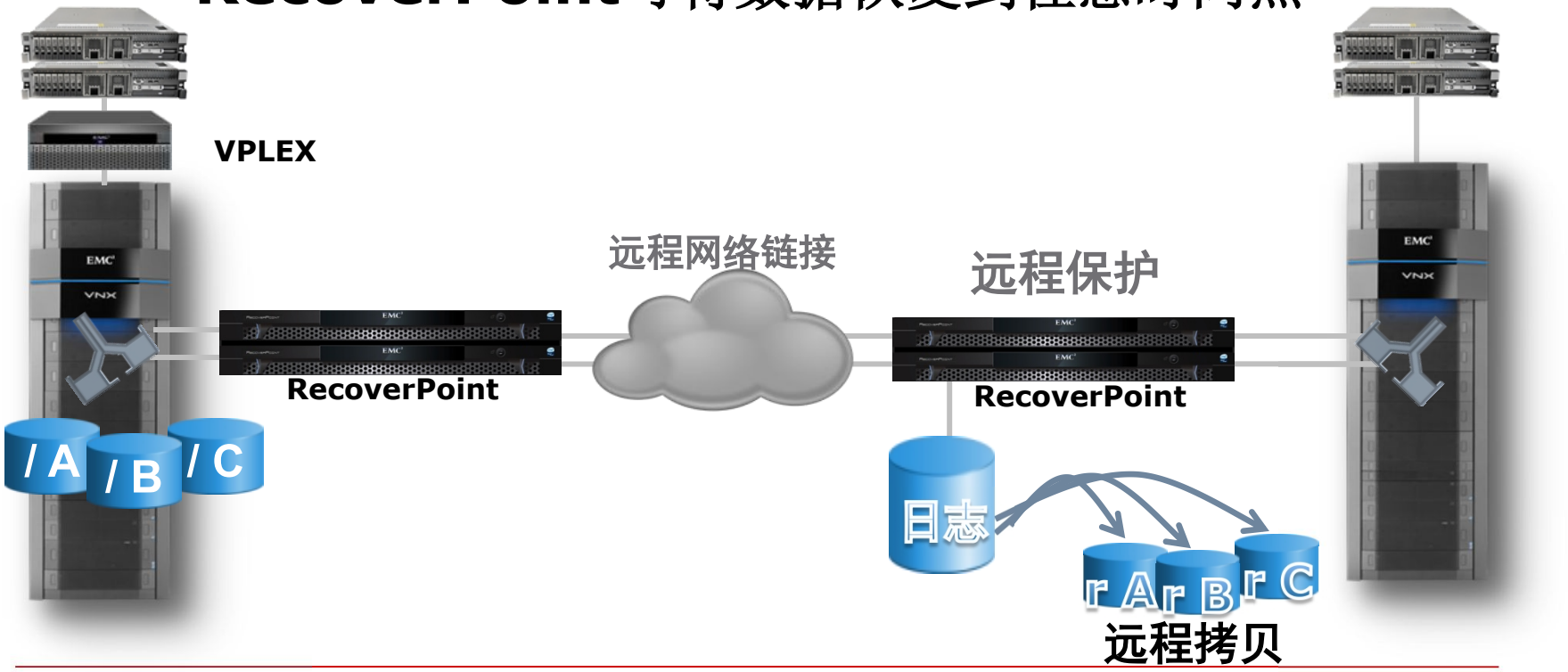
三、安全防护：数据安全

- 数据存储双活
  - 一台存储失效不影响业务，零恢复时间
  - 机房物理位置调整不中断业务



三、安全防护：数据安全

- 数据中心灾备
  - 实现连续性数据保护(CDP)，灾备容量: 500TB
  - RecoverPoint可将数据恢复到任意时间点



三、安全防护：数据安全

- 数据备份
  - 建立完善的系统级备份、恢复机制
  - 定期备份：完整+增量
    - 数据库
    - 物理机
    - 虚拟机

三、安全防护：安全运维

1、摸清家底
2、定期进行操作系统漏洞扫描
3、部署网站监控系统
4、多种手段监控Web网站安全
5、关键时期果断关闭高危网站
6、应急响应：一键断网
7、对高危网站做主动渗透测试
8、完善机制，严格落实

四、未来努力方向

- 进一步提高认识，提高责任感和紧迫感
- 进一步健全机制，建立信息安全责任体系
- 进一步加强建设，提高信息安全防护能力
- 逐步消灭二级出口，将互联网出口汇集在网络中心统一管理，实现统一安全策略和管控
- 逐步消灭二级域名，实现统一安全监测管控
- 购置专业安全服务，对重点网站、信息系统定期进行专业性主动渗透测试

四、未来努力方向

- 对重要信息系统定期进行安全等级保护
- 个人用户**IP**地址全面私有化
- 消灭小路由
- 加强容灾备份环境建设
- 备份数据的恢复性演练：定期
- 加强信息安全技术队伍建设，提高核心能力
- 推广云**WAF**：为兄弟院校提供安全服务
- 信息安全与信息技术伴生发展
- 且行且努力，永远在路上

敬请指正，谢谢！