



# 大连理工大学校园网站安全与管理

李先毅  
大连理工大学 网络与信息化中心

2017年05月05日

# 汇报内容



问题提出

技术安全

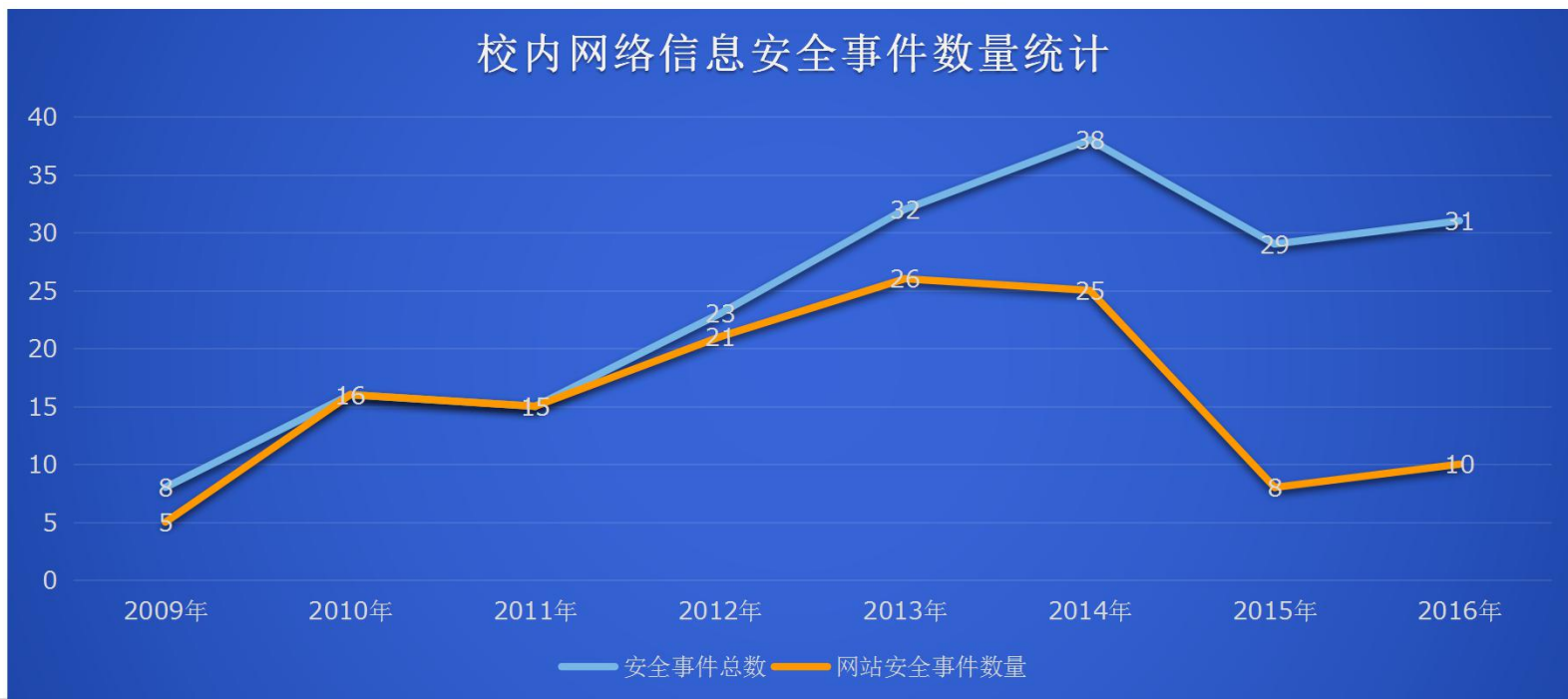
管理安全

未来设想

# 问题的提出

## ❖ 网站安全-高校信息安全重要组成

- 高校信息化建设：基础设施、信息系统、网站
- 传统高校网站：易攻击、影响大、占比高、不好管
- 新形势、新法规、新要求





# 问题的提出

## ❖ 学校网站建设发展

- 逐步认识并完善网站安全建设与管理

## ❖ 2002年以前-“散养”阶段

- 缺资源，鼓励建
- 开放的互联网IP地址；域名登记（1998年）

## ❖ 2002~07年-“大跃进”阶段

- 二级单位、实验室、课题组、个人、项目……
- 网络中心开始提供资源，以服务为主
- 数据中心（IDC）-64台1U服务器-虚拟主机、托管
- 物理机瓶颈；网站安全问题初现

**安全问题以病毒防控为主**

# 问题的提出

## ❖ 2007年~2013年-虚拟化阶段

- 虚拟化环境，解决物理机问题，对安全有一定帮助
- 提供资源，服务+管理-以学校主页、二级主页为主
- 技术规范；09、11网站评比；09网络信息安全工作

## 安全问题突显，网站安全尤为突出

## ❖ 2013年至今-云平台阶段

- 2013年建设网站群-学校主页、二级主页
- 2015年-会议网，2016年-教师个人主页平台
- 2016年站群升级-校内所有WEB网站要求迁移到网站群
- 提供通用平台，统一管理+服务

**学校主页一直采用静态发布方式，未出现安全问题**



# 问题的提出

## ❖ 提出校园网站管理原则与目标（2013年后）

- 保障安全
  - 在目前安全形势及相关要求下的首要任务
  - 页面、后台、数据的安全
- 统一管理
  - 集中管理，便于监控，简化操作
  - 校内不再允许自建对外服务网站
- 数据共享
  - 数据资产的重要组成部分
- 信息公开
  - 信息的严肃性、权威性、持续性

# 技术安全

## ❖ 技术手段-SaaS云平台，分类实现

- 将网站按功能分类，通过不同类型的平台实现，不再单独进行网站建设
- 网站类平台：
  - 信息发布类-网站群
  - 会议类-会议网<http://meeting.dlut.edu.cn>
  - 个人主页类-教师中英文主页<http://faculty.dlut.edu.cn>



# 技术安全

## ❖ 网站群平台安全管理

### ■ 网站群平台安全

- 静态web网页，严格限制动态组件的使用；开启防篡改
- 等保情况

### ■ 服务器安全

- 开发、管理、发布三套独立服务器分开-安全、负载
- 访问控制
  - 开发、管理服务器严格限制访问；发布服务器仅开80
- 管理服务器-集群，保证负载能力和可扩展性
  - 集群分区：学校主页、新闻网
- 发布服务器-多节点，根据内容、访问量、重要性分类
- 开发服务器-独立的；计划定期清理



# 技术安全

- 严格区分用户权限-网站开发、网站管理人员
  - 开发人员-开发平台权限，临时账号，非统一身份认证
  - 网站管理员-管理平台权限，统一身份认证
  - 网站开发、修改原则上都在开发服务器，完成后由平台管理员导入管理服务器并发布
- 平台运维人员
  - 网信中心、第三方
  - 堡垒机
    - 服务器运维
    - 应用发布-WEB、PLSQL

# 技术安全

## ❖ 配套安全保障

- 网络安全
  - 访问控制-对外仅开放web服务端口，对内关闭敏感端口
- 数据中心安全
  - 虚拟化层的HA保障
  - 部署统一虚拟化防护平台，包括杀毒、主机防火墙、虚拟补丁、日志审查
  - 部署waf
- 备份策略
  - 虚拟化层的整机备份
  - 平台的网站备份-可快速独立恢复网站

# 管理安全

## ❖ 组织机构及人员保障

- 学校信息化建设领导小组（2008）
- 学校网络安全与信息化委员会（2016）
  - 网络与信息安全工作组
  - 信息化建设工作组
- 信息化队伍-各单位
  - 信息化负责人、信息化专干
- 网信中心专人负责网站平台
- 网站登记明确各网站的负责人、管理员
- 人员更新机制-年审

# 管理安全

## ❖ 管理规定-制度保证

- 校内域名管理办法（2014）
- 学校主页管理办法（2014）
  - 主页改版，明确权责，网信中心与相关部门各司其职
- 二级主页管理办法（2014 已废止）
  - 推进二级主页迁移
- 信息化数据管理办法（2015 已废止）
- 信息化建设管理办法（2016）
  - 明确校内各部门信息化建设权责、管理建设模式
- 校内网站管理办法（2016）
  - 确定校内网站建设管理模式；全部网站迁移到网站群
- 信息化数据资源管理办法（2017）
- 网络信息技术安全管理办法（试行）（2017）



# 管理安全

## ❖ 推行

- 服务支撑与推广力度并重
  - 做好服务；坚持原则（领导的支持）
- 开展多次培训宣传
  - 网站群专项培训6次，信息化主题宣讲3次以上
  - 建立qq群等日常交流手段
  - 第三方的支持
- 切中要害的推广
  - 制度出台后，跟着会发布具体实施通知，立即行动
  - 以安全为抓手-用户IP关闭对外服务；安全检测报告
  - 讲策略：教师主页-招生
- 基本实现技术、管理安全措施推行

# 目前情况

## ❖ 网站类平台建设：

- 网站群-190+
- 会议网-25
- 教师主页-1700+

## ❖ 信息系统类平台-参考网站平台

- 活动类-校内活动管理平台<http://huodong.dlut.edu.cn>
- 投票类-调查问卷系统<http://survey.dlut.edu.cn>
- 视频会议类-视频会议管理<http://emeeting.dlut.edu.cn>
- 本地会议类-无纸化会议<http://paperless.dlut.edu.cn>
- 存储类-云盘服务<http://emeeting.dlut.edu.cn>

# 目前情况-安全情况

## 校内网络信息安全事件数量统计





# 未来方向

## ❖ 移动端的支持

- 网站移动版-H5
- 移动应用平台-微信企业号、APP、QQ校园公众号
- 移动安全-极其严峻!

## ❖ 筹划制定的管理制度

- 网络信息技术安全事件处理流程-应急响应
- 信息化项目建设流程、规范

## ❖ 信息化建设方向

- 基础平台+应用平台+核心业务系统
- 更多的应用类平台：网上办事大厅，轻应用平台
- 科研、教学的支撑：学术期刊、学术成果展示……



谢谢大家!

Lxy at dlut.edu.cn