C3安全峰会
CYBER | CLOUD | COMMUNICATION

新形势下
高校网络安全建设

颜凯

C3

教育之安全
电子科大之安全
未来之安全

C3安全峰会
CYBER | CLOUD | COMMUNICATION

PART/01 教育之安全

聚焦2016安全
信息安全的形势
教育行业的安全

1 2016 安全聚焦

安全问题日益复杂：

新的安全威胁 传统安全问题

安全的法制化

《网络安全法》

《国家网络空间安全战略》

2016 安全聚焦

数据泄露

- **数量大**
  - 俄罗斯邮件5700万
  - LinkedIn 1.17亿
  - 雅虎 15亿
  - 。。。。（数十亿信息泄露）
- **范围广**
  - 高考学生 徐玉玉
  - 总统候选人 希拉里
- **数据精准**
  - 清华大学教授

2016 安全聚焦

网络攻击

- **拒绝服务**
  - 面向基础服务
  - 面向工业控制系统
  - 面向金融系统。。。
- **勒索软件**
  - 黑产利益链
- **网页安全**
  - 网页仿冒
  - 网站后门
  - 网页篡改

2016 安全聚焦

法律法规&政策文件

- 《计算机信息系统安全保护条例》1994.2
- 《全国人民代表大会常务委员会关于加强网络信息保护的决定》2012.12
- 《全国人民代表大会常务委员会关于维护互联网安全的决定》2000.12
- 《国家网络空间安全战略》2016.12
- 《网络产品和服务安全审查办法》2017
- 《国家网络安全事件应急预案》2017.1
- 《个人信息和重要数据出境安全评估办法（征求意见稿）》2017.4
- 《网络安全法》2017.6

2016 安全聚焦

法律法规&政策文件

- 《国家网络安全事件应急预案》2017.1
- 《个人信息和重要数据出境安全评估办法（征求意见稿）》2017.4
- 《网络产品和服务安全审查办法（试行）》2017.6
- 《网络关键设备和网络安全专用产品目录》2017.6

一、列入《网络关键设备和网络安全专用产品目录》的设备和产品，应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。

	设备或产品类别	范围
网络关键设备	1. 路由器	整系统吞吐量(双向)≥12Tbps 整系统路由表容量≥55 万条
	2. 交换机	整系统吞吐量(双向)≥30Tbps 整系统包转发率≥10Gpps
	3. 服务器(机架式)	CPU 数量≥8 个 单 CPU 内核数≥14 个 内存容量≥256GB
	4. 可编程逻辑控制器(PLC 设备)	控制器指令执行时间≤0.08 微秒
网络安全专用产品	5. 数据备份一体机	备份容量≥20T 备份速度≥60MB/s 备份时间间隔≤1 小时
	6. 防火墙(硬件)	整机吞吐量≥80Gbps 最大并发连接数≥300 万 每秒新建连接数≥25 万
	7. WEB 应用防火墙(WAF)	整机应用吞吐量≥6Gbps 最大 HTTP 并发连接数≥200 万
	8. 入侵检测系统(IDS)	满检速率≥15Gbps 最大并发连接数≥500 万
	9. 入侵防御系统(IPS)	满检速率≥20Gbps 最大并发连接数≥500 万
	10. 安全隔离与信息交换产品(网闸)	吞吐量≥1Gbps 系统延时≤5ms
	11. 反垃圾邮件产品	连接处理速率(连接/秒)>100 平均延迟时间<100ms
	12. 网络综合审计系统	抓包速度≥5Gbps 记录事件能力≥5 万条/秒
	13. 网络脆弱性扫描产品	最大并行扫描 IP 数量≥60 个
	14. 安全数据库系统	TPC－E tpsE(每秒可交易数量)≥4500 个
	15. 网站恢复产品(硬件)	恢复时间≤2ms 站点的最长路径≥10 级

教育行业 信息安全的形势

重要讲话

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- 2014年2月27日，中央网络安全和信息化领导小组成立，国家主席习近平亲自担任组长，对网络发展和网络安全的高度重视，并指出：“**没有网络安全，就没有国家安全，没有信息化就没有现代化**”，强调“**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**”。

- 2014年11月19日，首届世界互联网大会在浙江乌镇召开，习近平主席在致辞中指出，“**互联网发展对国家主权、安全、发展利益提出了新的挑战**，迫切需要国际社会认真应对、谋求共治、实现共赢”。

- 2015年12月16日，第二届世界互联网大会，习近平主席在致辞中指出，“**安全和发展是一体之两翼，驱动之双轮。安全是发展的保障，发展是安全的目的。**”

重要讲话

C3安全峰会
CYBER | CLOUD | COMMUNICATION

- 2016年4月26日，国家主席习近平在网络安全和信息化工作座谈会上的讲话
- 正确处理安全和发展的关系“**网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进**”。
- 要求“**树立正确的网络安全观**”、“**加快构建关键信息基础设施安全保障体系**”、“**全天候全方位感知网络安全态势**”“**增强网络安全防御能力和威慑能力**”。
- 强调“**今年是十三五开局之年，网络安全和信息化工作是十三五时期的重头戏**”。

政策文件

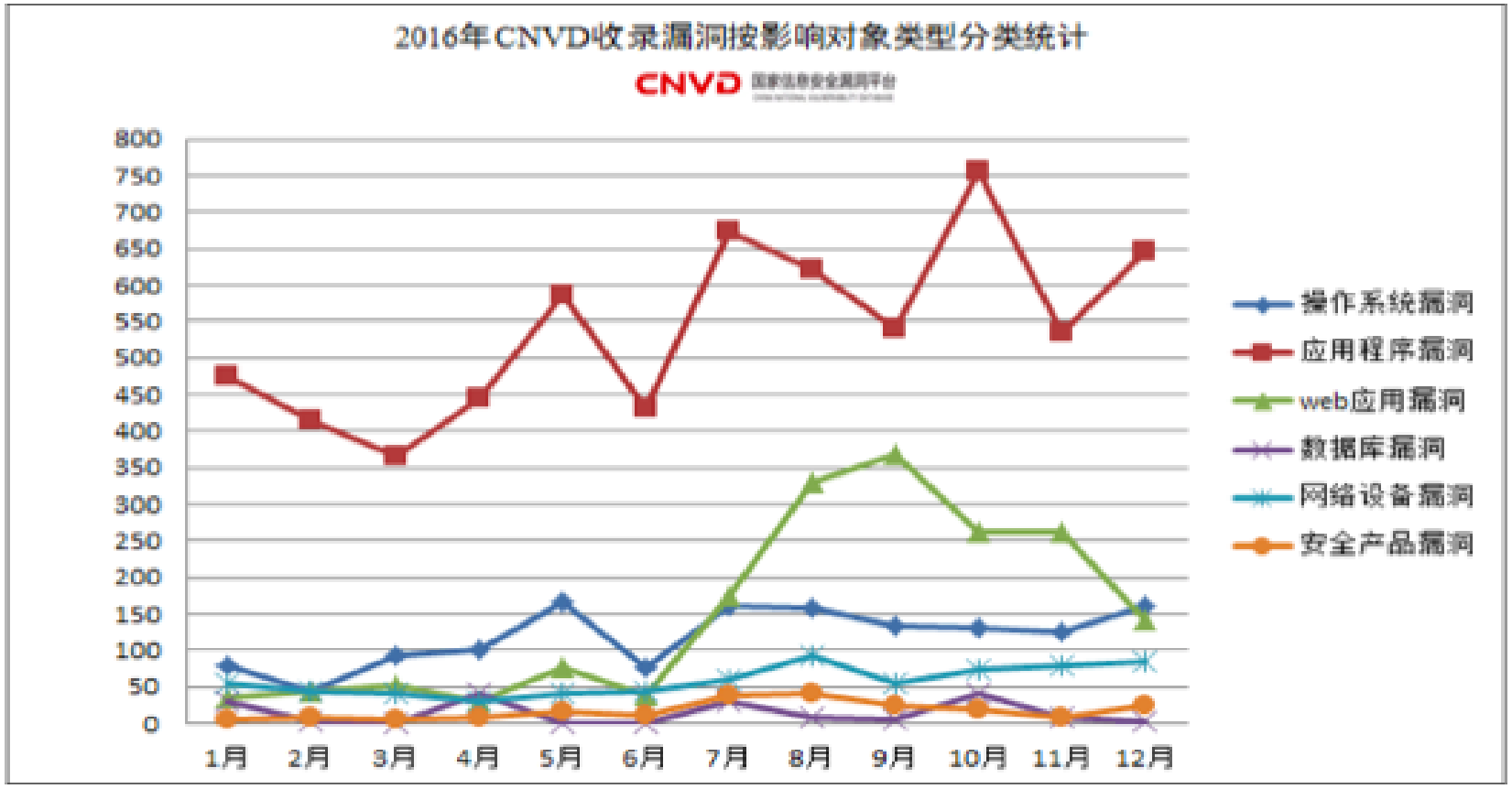
- 国家网络空间安全战略（2016.12）
- 国家信息化发展战略纲要
- “十三五”国家信息化规划
- 党政机关、事业单位和社会组织网上名称管理暂行办法
- 党政机关网站开办审核、资格复核和网站标识管理办法
- 关于加强党政部门云计算服务网安全管理的意见（中网办发文【2014】14号）
- 关于信息安全等级保护工作的实施意见（公通字【2004】66号）
- 信息安全等级保护管理办法（公通字【2007】43号）
- 信息安全等级保护备案实施细则（公信安【2007】1360号）
- 政务信息资源共享管理暂行办法（国发【2016】51号）
- 关于加强网络安全学科建设和人才培养的意见（中网办发文【2016】4号）

标准规范

- GB/Z 20986-2007《信息安全事件分类分级指南》
- GB 17859-1999《计算机信息系统安全保护等级划分准则》
- GB/T 22239-2008 《信息安全技术 信息系统安全等级保护基本要求》
  GB/T 22240-2008《信息安全技术 信息系统安全等级保护定级指南》
- GB/T 31167-2014《信息安全技术 云计算服务安全指南》
- GB/T 31168-2014 《信息安全技术 云计算服务安全能力要求》

安全问题到底在哪里

- 逐渐从程序漏洞，SQL注入，跨站脚本转向框架
- 逐渐从中心扩展到边缘



高校安全问题的原因

- 网站建设和管理不统一、基数大
  - 高校内部网站数量多，建设单位杂，安全管理困难
  - 政府网站由2017年8万缩减到4万，教育行业edu.cn活跃就是11万，还有教育机构58万家
  - 网站日常维护缺失，高校网站重建设、重功能，日常安全维护较差，一些已公布的安全漏洞修复不及时，孤站僵尸网站数量多
- 对安全重视高度不够，数据价值高
  - 由于高校网站的公益性 ，被入侵和篡改网页造成的损失不太明显，网站安全往往得不到重视
  - 有大量老师和学生的个人信息，海量数据，敏感度高
- 网站信息保护意识差
  - 弱口令、信息泄露随处可见
- 系统漏洞
  - 信息系统众多，通用性软件，技术能力不足或者服务商能力不足，服务器端安全服务差
  - 软件或系统漏洞没有及时打补丁或更新

C3安全峰会
CYBER | CLOUD | COMMUNICATION

PART/02 电子科大之安全

- 2017安全工作整体情况
- 安全工作保障

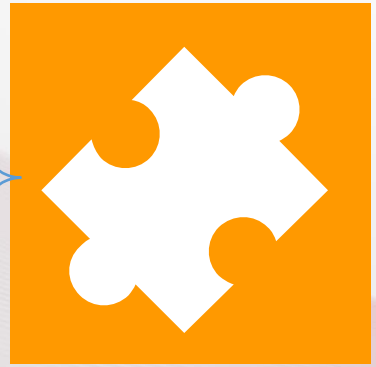
2017安全工作整体情况

《网络安全法》
网络安全综合治理
行 动（3-8月）

重要时期的保障工 作
“零报告”工作

1-6月
安全漏洞79件

- 教育部通报 17
- 教育行业漏洞平台 25
- 漏洞盒子 21
- 补天平台 4
- CNVD 8
- WebSoc 3



3月7日 StrutsS2-045
StrutsS2-046
5月12日 勒索病毒
6月15日 暗云木马
震网三代

电子科大之安全保障

等级保护

所有系统都定级备案
评测整改

机构设置

网络信息安全领导小组
网络信息安全工作小组

制度建设

《电子科技大学网络信息服务管理办法（试行）》
《电子科技大学信息技术安全管理办法（试行）》
《电子科技大学信息中心网络与信息安全类突发事件应急处置预案》
《电子科技大学网络与信息安全类突发事件断网处理流程》

进展情况

提高意识
摸清家底
规范操作
落实职责

机构设置

网络安全是一把手工程，中央网信领导小组组长是习近平总书记，教育部网信领导小组组长是陈宝生部长。

网络信息安全领导小组

网络信息安全工作小组

网络信息安全领导小组

- 主要负责人负总责

网络信息安全工作小组

- 分管负责人牵头抓

机构设置

明确职能部门、技术支撑机构，做到职责明确、分工协作

谁主管谁负责
谁运维谁负责
谁使用谁负责

主管

信息系统的责任单位对系统的安全负主要责任和管理责任

运维

信息系统的运维单位根据主管单位的要求，做好信息系统的安全运维和技术防护

使用

对系统操作、提供的数据和信息负直接责任，应该严格按照信息系统的操作和管理规范使用

制度建设

制度：

《电子科技大学网络信息服务管理办法（试行）》
《电子科技大学信息技术安全管理办法（试行）》
《电子科技大学信息中心网络与信息安全类突发事件应急处置预案》

相关表格：

《电子科技大学网络信息安全工作责任书》
《电子科技大学网络信息服务备案表》
《网络安全与保密协议》
《统一身份认证平台接入申请表》

制度建设—网络信息服务管理办法

C3安全峰会
CYBER | CLOUD | COMMUNICATION

《电子科技大学网络信息服务管理办法（试行）》

1、总则

介绍管理办法的制定背景，对相关名词进行了定义

2、网络信息安全领导小组及职责

明确领导小组的组成、职责和职权

3、网络信息服务审批和备案

明确信息中心是网络信息服务的审批、等级、备案管理单位，规定网络信息服务的备案管理的细则

4、网络信息服务的管理

规定提供网络信息服务的原则和要求

制度建设—信息技术安全管理办法
《电子科技大学信息技术安全管理办法》

1、总则

介绍管理办法的制定背景和依据，对基本原则进行阐述，对名词进行了定义，规定校内各单位的安全责任

2、信息系统与互联网网站安全管理

明确网站技术安全管理、网站内容安全管理的规定，对数据安全和电子公告服务安全管理的规定

3、电子邮件安全管理

明确电子邮件系统安全防护责任，规定学校各单位、师生员工电子邮箱使用的安全要求

4、人员安全管理

确定岗位安全责任制度，给出人员管理的一般性安全规定以及关键岗位人员的安全规定

制度建设—信息技术安全管理办法

《电子科技大学信息技术安全管理办法》

5、信息安全应急管理

确定信息安全应急管理的统筹管理、技术支撑保障单位，规定安全事件报告与处置，明确师生员工对于信息安全事件的报告责任

6、信息安全检查监督

规定信息安全自查、检查、整改、报告的基本要求

7、信息安全责任追究

明确信息安全责任追究的基本原则

8、附则

对涉密信息系统的补充规定

等级保护

2014年10月27日 教技厅函[2014]74号教育部办公厅关于印发《教育行业信息系统安全等级保护定级工作指南（试行）》的通知

学校信息系统可分为重点建设类高等学校信息系统（I类）、高等学校信息系统（II类）、中小学校（含中职中专院校）信息系统（III类）。

以等级保护建设为契机，推动教育安全保障的体系建设

进展概要

- 摸清家底
- 健全制度
- 落实职责
- 体系建设

变 “被动” 为 “主动”

- 事件响应—被动（界限模糊，忙于处理各类事件）
- 安全治理—主动（实现责任分担，有序进行安全防范）

PART/03 未来之安全

- 建立教育的安全生态圈

新技术面临新新形势

人防

人员配比

人员要求

- 71% 高校投入安全工作人数 ≤ 2人
- 16% 没有相对固定安全人员投入
- 44% 未明确设立网络信息安全岗位

数据来源：

《2015高校网络信息安全工作调查分析报告》

http://sec.edu-info.edu.cn/120

技防

安全设备

安全技术

安全没有短板

- 新技术：大数据、云服务、虚拟化、移动终端
- 安全域的划分，漏洞扫描/漏洞管理/补丁管理，安全加固，数据备份，应急预案/应急演练

建立安全生态圈

C3安全峰会
CYBER | CLOUD | COMMUNICATION

多方合作共赢

全国

教育部 安全监测通报平台
高校网络信息安全工作组
高校 IPDB
http://ipdb.sec.edu-info.edu.cn/ipdblogin/
竞评演练

四川省

城域网联盟
四川教育信息化安全工作委员会

学校

整合校内学科资源
培养学生团队（白帽子）
宣传与培训
攻防演练

建立安全生态圈--全国

C3安全峰会
CYBER | CLOUD | COMMUNICATION

EDU IPDB 登录 排行榜 关于

排行榜

排名	地区	注册单位数量	注册联系人数量	未注册单位数量	完成百分比	单位总数
1	广东省	151	192	35	0.81	186
2	浙江省	109	183	37	0.75	146
3	重庆市	43	69	37	0.54	80
4	吉林省	41	56	49	0.46	90
5	四川省	72	110	99	0.42	171
6	青海省	7	19	12	0.37	19
7	天津市	28	43	47	0.37	75
8	安徽省	48	59	91	0.35	139
			80	95	0.35	146
			56	77	0.33	115

教育行业漏洞报告平台（Beta） 首页 漏洞列表 排行榜 礼品中心 关于 注册 登录

最新漏洞

时间	标题	等级	作者
2017-06-23	北京化工大学存在SQL注入漏洞	高危	hu5ky
2017-06-23	上海外国语大学存在敏感信息泄露	高危	hu5ky
2017-06-23	吉林师范大学博达学院存在弱口令	中危	hwan
2017-06-23	北京交通运输职业学院存在SQL注入漏洞	高危	hackbar
2017-06-23	山东大学存在SQL注入漏洞	高危	铭心
2017-06-23	伊犁师范学院存在SQL注入漏洞	中危	铭心
2017-06-23	同济大学存在弱口令	低危	ChamPion
2017-06-23	兰州大学存在弱口令	低危	ChamPion
2017-06-22	湖南警察学院存在SQL注入漏洞	高危	闭关修炼的_令狐少侠
2017-06-22	长沙民政职业技术学院存在SQL注入漏洞	中危	闭关修炼的_令狐少侠

2017 © 主办：中国高等教育学会教育信息化分会 联系邮箱：contact@src.edu-info.edu.cn
联合主办：网络安全研究国际学术论坛

CNVD 国家信息安全漏洞共享平台 CHINA NATIONAL VULNERABILITY DATABASE

漏洞盒子

补天 漏洞响应平台

中国高等教育学会教育信息化分会
网络信息安全工作组
Education Information Security Working Group

教育行业漏洞报告平台（Beta）

123	13658	9	2516
待审核漏洞	全部漏洞	待发货礼物	用户总数
查看详情	查看详情	查看详情	查看详情

建立安全生态圈--四川省

四川

四川省计算机信息安全行业协会

IWC 教育信息化工作委员会 Education Information Work Committee

- 主要职责：组织开展网络信息安全业务，借助专家资源，规范信息系统安全管理体系；为教育行业网络信息安全建设提供技术支持以及相关培训服务工作。
- 本会宗旨：遵守国家的法律、法规和政策，弘扬社会道德风尚。搭建网络信息监管部门与院校之间的沟通桥梁，规范和加强网络信息安全保护工作，提高网络用户的安全意识，促进信息技术的社会化和产业化的健康发展。

建立安全生态圈—学校

育人和安全工作相结合
网络空间安全一级学科 29所

参加“安全运维挑战赛”
以赛促建
以赛促学
以赛代练

高校IT管理技术人员+在校优秀大学生

组成联合安全团队

统计数据覆盖范围106所高校

《2015高校网络信息安全工作调查分析报告》

规模	计算机专业		信息安全专业		软件工程专业	
无	13	9.70%	51	38.06%	22	16.42%
0~50	8	5.97%	19	14.18%	10	7.46%
50~100	21	15.67%	18	13.43%	28	20.90%
100~200	36	26.87%	12	8.96%	31	23.13%
>200	49	36.57%	15	11.19%	32	23.88%
未答	7	5.22%	19	14.18%	11	8.21%

高校甲方安全团队和安全部门普遍缺失

资源整合　提高高校安全防范
多维度合作 共同培养安全人才

建立安全生态圈—学校

C3安全峰会
CYBER | CLOUD | COMMUNICATION

2017年7月~12月举办 2017全国高校网络信息安全管理运维挑战赛

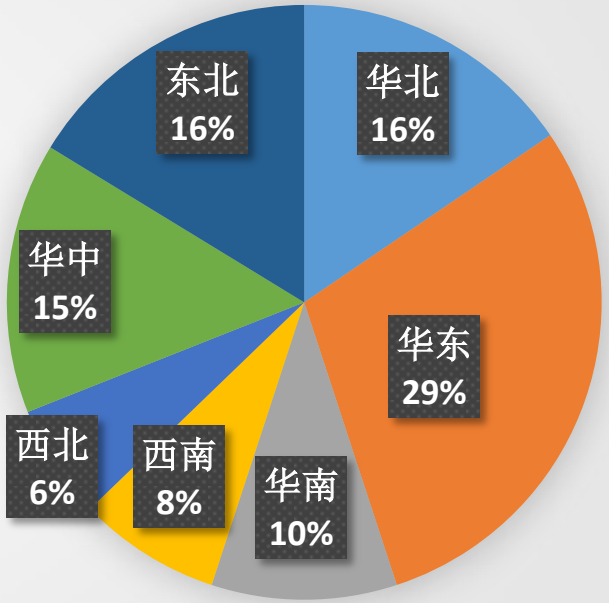
（http://sec.sjtu.edu.cn ）

- 以高校为基本单位组织参加
  每个参赛队由1~3名教师 + 1~3名学生组成，另设领队一名（安全分管领导）

1）**安全理论部分**： 标准化测试（选择题），3小时。允许多个团队成员参加，最后取其中最好成绩（折合为百分制）。

2）**动手实践部分**： CTF(Capture The Flag)竞赛模式，8小时。以团队为单位参加，取最后总得分（折合为百分制）。考察点包含但不限于以下内容：

每个团队理论与实践成绩累加，满分为200分。



- 全国分为七大赛区

129 支高校团队/511 名参加人员

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Thank You