高校数据中心的安全防护与审计

于俊清

華中科技大學
HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

斯诺登与棱镜门事件

- 网络与信息安全上升到国家战略

華中科技大學

总统窃听门

❖为了“利益”和“安全”，谁都不放过

十八大指明信息化工作方向

从十八大看今后信息化工作方向

发布日期：2013-05-28 来源：信息化建设 作者：马 龙 浏览次数：3540

在十八大报告中，信息化或信息出现了18次，网络出现了8次，以及信息化标志的“超级计算机”，信息化内容共出现了27次，在“新四化”内容中居核心地位。

党的十八大报告（下称“报告”）提出，“坚持走中国特色新型工业化、信息化、城镇化、农业现代化道路，推动信息化和工业化深度融合、工业化和城镇化良性互动、城镇化和农业现代化相互协调，促进工业化、信息化、城镇化、农业现代化同步发展”，即“新四化”。同步发展的“新四化”中，信息化是新增的内容，这表明信息化已被提升至国家发展战略的高度。

信息化居“新四化”核心地位

在报告中，信息化或信息出现了18次，网络出现了8次，以及信息化标志的“超级计算机”，信息化内容共出现了27次。信息化及相关内容出现在报告的第一、三、四、五、六、七、九、十一共八个部分。

工业化	信息化	城镇化	农业现代化	小计
10	27	10	5	52

高度重视网络安全与信息化工作

中共中央网络安全和信息化领导小组办公室

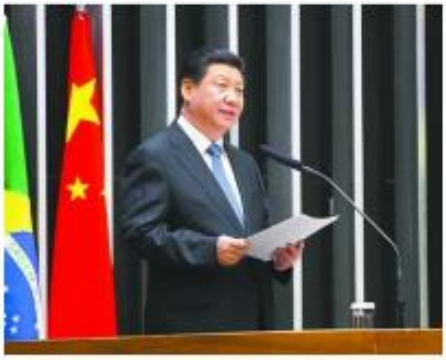
Office of the Central Leading Group for Cyberspace Affairs

WWW.CAC.GOV.CN

5个词读懂习近平的网络安全新主张

新华网 高层 > 正文

学习有方：5个词读懂习近平的网络安全新主张



5个词读懂习近平的网络安全新主张

- 【总体安全】网络安全纳入国家总体安全观
  - 没有网络安全就没有国家安全，没有信息化就没有现代化
- 【技术保障】要有自己的、过硬的信息技术
  - 要制定全面的信息技术、网络技术研究发展战略，下大气力解决科研成果转化问题
- 【法治建设】出台完善网络安全法律法规
  - 要抓紧制定立法规划，完善互联网信息内容管理、关键信息基础设施保护等法律法规，依法治理网络空间，维护公民合法权益

CERNET华中地区网络中心

5个词读懂习近平的网络安全新主张

- 【领导体制】加快完善互联网管理领导体制
  - 面对互联网技术和应用飞速发展，现行管理体制存在明显弊端，多头管理、职能交叉、权责不一、效率不高
  - 坚持积极利用、科学发展、依法管理、确保安全的方针，加大依法管理网络力度，完善互联网管理领导体制
  - 整合相关机构职能，形成从技术到内容、从日常安全到打击犯罪的互联网管理合力，确保网络正确运用和安全

華中科技大學

5个词读懂习近平的网络安全新主张

- 【国际合作】建立多边、民主、透明国际互联网治理体系
  - 在互联网高度全球化的背景下，网络安全的实现，需要内外统筹
  - 本着相互尊重、相互信任的原则，深化国际合作，尊重网络主权，维护网络安全，共同构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的国际互联网治理体系

高校信息泄露和“被黑”事件频发

CERNET华中地区网络中心

高校信息泄露和“被黑”事件频发

搜狐教育 > 新闻

千余高校网站存信息泄露风险，如何破?

麦可思研究 2015-05-22 11:48:09 信息 数据 问题 阅读(525) 评论(0)

据媒体报道，中国高校或成为信息安全泄漏的重灾区，千余高校网站存信息泄漏风险。学校网站掌握着大量集中性人群的个人信息，高校像是信息汇聚的心脏，一旦发生意外，血液般的信息骤然涌出，就会给师生带来无尽隐患，导致高校“大出血”。

很多高校网站的信息安全漏洞都非常低级，一旦不法分子利用这些漏洞，就可以轻而易举地入侵邮件系统，获取科研项目和领导机密，篡改网页，植入任意内容，控制大量电脑并侵入校园网络，窃取账号密码等个人信息等。在信息化时代，高校应该如何应对信息安全问题呢？

新闻链接

CERNET华中地区网络中心

高校信息泄露和“被黑”事件频发

新闻中心

千余高校网站存信息泄漏风险 多所顶级学府上榜

2015年05月20日01:54 经济参考报

我国高校或成为信息安全泄漏的重灾区。《经济参考报》记者日前对补天漏洞响应平台的数据梳理发现，自2014年4月至2015年3月的12个月间，补天平台上显示的有效高校网站漏洞多达3495个，涉及高校网站1088个。其中，高危漏洞2611个，占74.7%；中危漏洞691个，占19.8%；低危漏洞193个，占5.5%。

在上述漏洞中，至少有384个漏洞可能造成教职员工或学生个人信息泄漏，一旦这些漏洞全部被恶意利用，至少会导致837万以上的教职员工及学生个人信息泄漏。令人担忧的是，过去一年间，在被告知网站存在漏洞后，会修复漏洞的高校网站只有35个，仅186个漏洞被修复，96.8%的高校网站完全无视安全漏洞的存在，94.6%的高校网站安全漏洞未被修复。

高校信息泄露和“被黑”事件频发

360：黑客攻陷[ ]官网 植入假淘宝钓鱼页面

2014年06月05日 14:36 来源：中国新闻网 参与互动(1) 0

中新网6月5日电 高考来临，上[ ]是每个考生梦寐以求的目标，上北大官网却要当心。根据360安全中心检测，近期北大官网遭黑客入侵篡改，网站被植入假冒淘宝的钓鱼页面。如果网友在此页面购物，网银账户将被黑客盗取。

高校信息泄露和“被黑”事件频发

[ ]网站被黑 黑客捏造新闻报道

2008-08-25 10:00:50 来源:Solidot 作者: 点击:1257

清华大学网站被黑，黑客宣称现行的大学教育制度就是“在往学生们的脑子里灌屎”。

清华大学网站被黑，黑客宣称现行的大学教育制度就是“在往学生们的脑子里灌屎”。黑客捏造了一篇清华大学校长顾秉林接受采访的新闻报道，批评现行教育制度：顾秉林校长表示，在二十世纪初至40年代，可以说是中国教育界的黄金时期，在这段时间以内中国的大学为社会培养出了大批的优秀人才，他们中有伟大的思想家、 教育家，有革命义士、抗日英雄，有科学骨干、民族精英。而这种盛况自从解放后尤其是九十年代开始衰落。现在的各高校，包括清华与北大在内，已经没有将培养人才作为大学教育的目标。

严重的学术腐败，枯燥且与社会脱节的课程，死记硬背的教育方式，将导致学生们的思想僵化，对课程失去兴趣，对大学乃至整个中国的教育失去信心，退学正是表达他们对大学教育失望的最极端方式.....顾秉林先生表示，中国的高等教育体制改革势在必行，“应该停止再扼杀人才了!应该停止再向学生们的脑子里灌屎了!”

华中科技大学

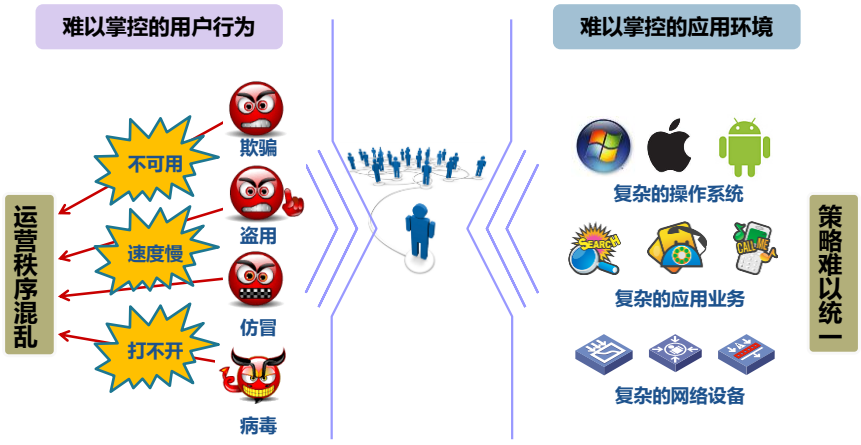
高校信息泄露和“被黑”事件频发

数据安全将成为我们关注的核心

过去：争抢建机房和数据中心

出了问题：推脱责任

现实困难与挑战



- 引不进、留不住，技术人员严重短缺

现实困难与挑战

- 运营商的围追堵截
- 师生的抱怨
- 待遇低、工作强度大，员工的不满意
- 人才流失严重，技术人才缺乏
- 设备更新快，经费投入不足
- ……

现在：希望ITS什么都做？

- 我们该做什么？
- 我们能做什么？
- 我们做什么才能保证数据安全？
- 我们可以保证什么安全？
- ……
- 敢问路在何方？

目 录

信息化的目标与定位

- 提高管理服务水平
- 提供科学决策支持
- 促进学科发展

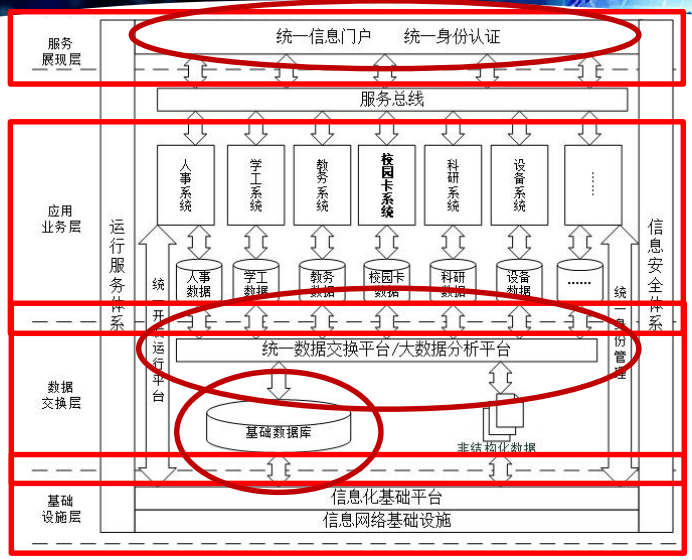
工作机制

- 领导机制
  - 体制机制、游戏规则（领导小组的作用）
- 统筹机制
  - 信息化的制度、规范、发展规划、项目管理（网信办）
  - 基础设施建设与运维（信息技术中心）
- 责任分担机制
  - 职能部门、院系
- 合作机制
  - 银行、运营商、设备提供商

信息技术中心（ITS）职责

- 校园计算机网络建设和运行维护管理
- 学校信息化基础平台建设和运行维护管理
  - 数据中心的硬件和软件
- 学校信息系统的综合集成及安全管理
  - 统一门户、统一身份认证
- 学校基础数据库的建设管理
  - 基础数据库、数据共享与交换平台
- 信息安全技术支持与服务

信息化的技术架构



应用系统的开发与管理

- 鼓励优先采购安全、成熟、应用面广和售后服务优良的商业软件
- 没有相应商业软件，或商业软件不适应我校实际管理需求时，可以通过软件开发（包括定制软件开发）建设应用系统

软件采购与开发安全管理

- 业务管理部门撰写需求分析报告，明确详细的功能和性能需求
  - 如果是购买商业软件，还需考察并确定一个或多个候选商业软件提供商
- 信息技术中心负责软件所需的数据中心资源、协助制定技术方案
  - 包括硬件、运行平台软件和基础数据等
- 信息办组织对技术方案进行论证和审批，确定信息安全保护等级

软件采购与开发安全管理

- 购买商业软件
  - 业务管理部门根据论证和审批通过后的方案按照学校相关规定采购和实施
- 委托开发
  - 业务主管部门在学校认定的软件系统开发商中，按照学校相关规定委托一家软件系统开发商开发
- 自主开发
  - 若业务管理部门具有应用系统开发维护能力，可自行组织开发

CERNET华中地区网络中心

软件采购与开发安全管理

- 学校认定的软件系统开发商
  - 由信息技术中心按照学校相关规定，采用公开招标的方式遴选资质和信誉良好的软件企业，以提高软件的安全性和可维护性
- 业务管理部门为应用系统的主管部门
  - 应指定专门人员负责系统的建设、运行维护和安全管理
  - 制定应用系统运维和安全管理方案，明确运行维护部门
  - 应用系统原则上由业务管理部门运维，特殊情况可委托网络与计算中心运维

華中科技大學

队伍建设

- 拟建设一支30-50人的开发与运维队伍
  - 三分之一核心人员：学校引进、不唯学位和出身
  - 三分之一服务外包：以服务的形式购买软件公司的技术人员
  - 三分之一业务部门的IT运维人员：财务、人事、教务、图书馆、远程教育

目 录

数据中心的任务与面临的问题

- 主要任务
  - 为学校信息化建设提供稳定安全可靠的运行环境
  - 为学校应用系统的互联互通提供基础条件和技术保障
    - 三大平台、通讯平台等基础信息系统
- 面临问题
  - “以应用需求为核心”和“应用数据大集中”对信息化基础设施提出了更高的要求
  - 可靠性、安全性、可用性、随需应变
  - 信息化基础设施运维与应用系统运维的边界问题
  - 信息化基础设施的日益复杂与人手短缺的矛盾

安全威胁

- WEB应用攻击
  - 据统计，目前Web应用（HTTP 80/HTTPS 443端口）已替代 Microsoft-DS（445端口）成为黑客攻击的目标首选
- 弱密码利用
  - 远程桌面、SSH、网站、ftp、数据库
- 操作系统、应用软件漏洞利用
  - 远程代码执行，提升权限，安装后门

安全威胁

- **现实问题**：攻击无法避免
- **根本原因（苍蝇不盯无缝的蛋）**：各种安全隐患长期存在
  - **管理因素**：单位没有相关管理制度，造成网站或服务器的基本安全维护工作缺失，导致服务器长期存在各种漏洞
  - **人员因素**：管理员和普通用户计算机技术及安全意识薄弱（使用弱密码、主动安装恶意软件等）
  - **技术因素**：很多网站和应用服务在设计实现时就存在各种应用逻辑漏洞

信息安全保障：数据安全

- 敏感数据 “**看不见**”
- 核心数据 “**拿不走**”
- 运维操作 “**能审计**”

信息安全保障：数据安全

- 数据泄露的原因、方式及应对措施
  - 专业网络罪犯
    - 网络隔离、安全扫描、防火墙、入侵检测、及时更新安全补丁
  - 合作伙伴（开发商、运维服务商）
    - 建立系统交付规范、运维服务规范、签署保密协议等管理制度来加强管理，合理的权限分配、审计管理
  - 善意的内部人员
    - 建立安全管理制度，加强安全管理意识和进行安全技术培训
  - 恶意的内部人员
    - 加强内部人员管理，建立完善的分权机制（安全员、系统管理员、审计员进行人事分工）
    - 采用先进的技术手段（Oracle Database Vault、Oracle Advanced Security、DB Firewall等软件）

安全域的划分与隔离

- 同一安全域中的系统应该具有相似的安全防护需求
- 每个安全域具有完全独立和封闭的物理及逻辑网络
- 安全需求高的安全域应只具有唯一出口与外网相连，且与外网的联系方式越简单越好
- 每个安全域都应在所有出口上根据实际情况设计并实现完整的网络访问控制策略控制

安全域的划分与隔离

- 访问控制策略的设计原则
  - 无需提供服务的监听端口一律关闭
  - 无需对全网提供服务的监听端口就一定进行严格的访问IP地址范围

几点经验

- **必须坚持的经验：有所不为**
  - 不要大包大揽，不做保姆
  - 不要唯命是从，凡事以安全为重
- **建立规则、守护好规则（依法治国，立法更要守法）**
  - 规则的好坏是水平问题，守护规则是品质问题
- **转变观念**
  - **优质服务**求生存、**服务创新**求发展

几点经验

- **不要大包大揽，不做保姆**
  - 安全的问题是复杂的，就算给计算机系统加上了铜墙铁壁，也难以防止从内部开始的瓦解
  - 对用户的行为必须加以严格规范，制定完善的安全管理及操作规定，发生问题时要有据可查
  - 权责一定要划分清晰，对于不属于亲自管理的计算机系统就一定不能负责到底，并且制定相关规定，有据可查

CERNET华中地区网络中心

几点经验

- **不要唯命是从，凡事以安全为重**
  - 规定就是规定，安全的原则不能因为领导的一句话或者用户的一个请求就轻易放弃，因为那样会后患无穷
  - 商量沟通后，采取其它变通的安全方式实现
    - 外网通过VPN的方式远程登录校内计算机系统，而不是向外网完全开放
  - 如果确实没有其它可变通的方式，又无法拒绝时，请一定让当事人或单位留下书面承诺书，出现问题时有据可查

華中科技大學

目录

安全审计

安全审计

- 审计是模拟社会监察机构，在计算机系统中用来监视、记录和控制用户活动的一种机制
  - 使影响系统安全的访问和访问企图留下线索以便事后分析和追查
- 审计系统是现代信息安全系统必不可少的组成部分
  - 在身份鉴别、访问控制、数据加密等多种安全措施基础上，进一步增强系统安全性

安全审计的重要性

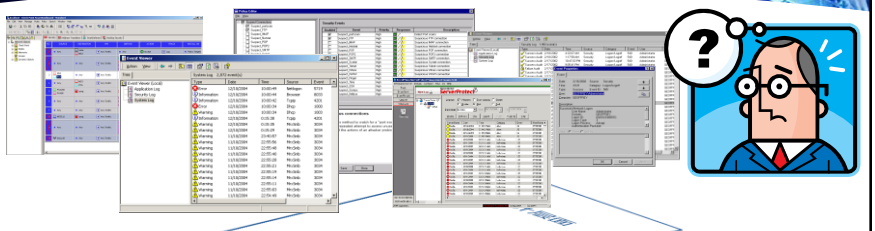
- 完备的审计系统对攻击者具有强大的威慑作用
  - 所有安全防线被攻克，只有通过审计系统进行事后追查
- 国家信息安全等级保护条例中，对审计功能具有明确的技术要求
  - 网络安全审计——应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录
  - 主机安全审计——审计范围应覆盖到服务器上的每个操作系统用户和数据库用户
  - 应用安全审计——应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计

安全审计的现状

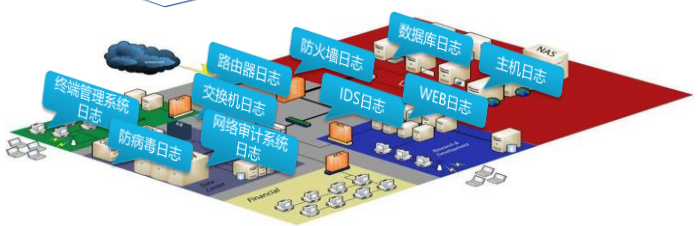
- ❖设备种类繁多，审计日志记录分散，格式不统一
- ❖日志记录量大（每日审计数据上百G）

CERNET华中地区网络中心

安全审计的现状



日志分散　日志格式不统一　日志量大



華中科技大學

安全审计的现状

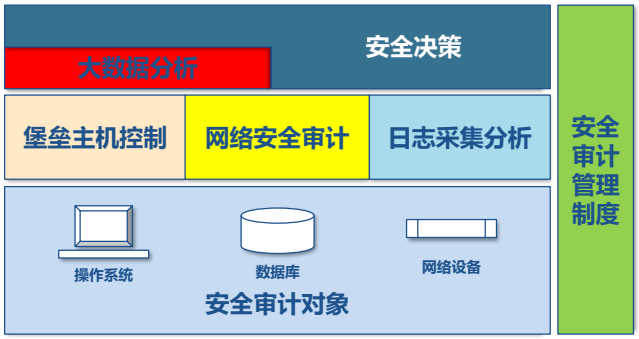
- 设备审计功能非强制开放，审计信息不全
- 设备审计记录缺乏保护，对超级管理员缺乏约束
- 设备审计信息相对孤立，缺乏有效的审计事件关联分析手段
- 无专职安全审计员，多由管理员兼任
- 安全审计管理制度不健全

安全审计系统建设目标

- 有效监控可能影响信息安全的用户和管理员行为
- 建立有效的安全事件预警、追踪平台
- 对分散的日志数据进行集中存储，建立统一的安全审计监控平台
- 建立日志信息大数据分析平台
- 健全安全审计管理制度

安全审计系统建设目标

- 建立以堡垒主机控制、网络安全审计、日志采集分析为技术手段，以安全审计管理制度为政策保障，以大数据分析为决策支持的安全审计中心



目 录

日志采集

- 主要功能
  - 自动采集各类设备产生的运维日志
  - 对各类日志进行集中存储和分析
  - 通过关联分析追踪安全事件

CERNET华中地区网络中心

日志采集

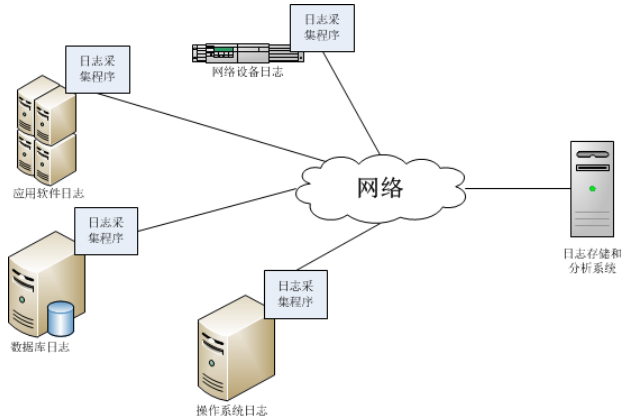
- 应用场景
  - 安全事件追溯
  - 日志综合分析
  - 安全预警
  - 系统管理员操作监督

華中科技大學

日志采集

❖部署方式

- 灵活部署，网络可达即可



日志采集

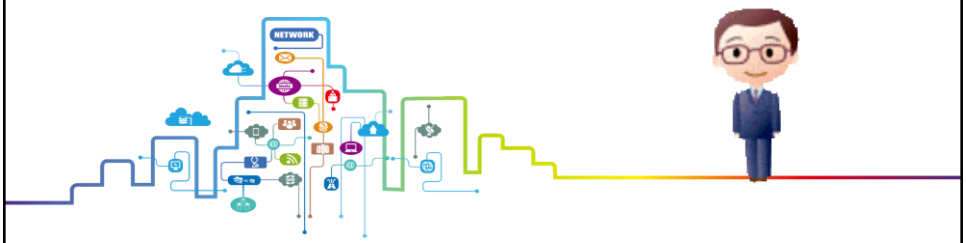
❖相关产品

- 启明星辰TSOC-SA泰合安全日志审计系统
- 明御综合日志审计平台
- HP ArcSight
- Splunk日志分析系统

日志大数据分析平台

- Splunk、Hadoop、Spark

致 谢



Email: yjqing@hust.edu.cn