SECSPACE . COM
北京三思网安科技有限公司

PCI DSS合规和网络信息安全体系建设

2018第三届移动金融安全大会

北京三思网安科技有限公司 CEO
清华大学NISL实验室 高级安全顾问

魏克

2018年11月16日 Friday

Network and Information Security Lab @ Tsinghua University

- **个人简介：**
  - 2000年，加入清华大学网络中心，后进入清华大学网络与安全实验室
  - 2003年，国内第305个CISSP
  - 2007年，成为国内第一个PCI DSS 的高级审核员；同年考取ISO27001主任审核员
  - 在清华期间参与多项国家863，973研究课题；为数十个国内、国际著名企业做过PCI DSS和ISO27001咨询，包括单不限于：
  - 1、First Data
  - 2、中国银联
  - 3、中国工商银行
  - 4、中国银行
  - 5、中航信息
  - 6、支付宝
  - 7、KDDI
  - 8、博报堂
  - 9、澳门通 – 澳门新福利集团
  - 。。。。。。。。
  - 2014年开始创办企业

2015.12何旭东、李国磊、张楠、刘跃、郭云飞。2015.6崔丽娟。2014.6印泰镇。2013.6 李德虎。2013.1 赵宗旭，陈力

陈霖，鲍由之，陆恂，贾皓，张京京，向飞，李硕，许伟林，王若愚，毛骏，汪子菡，赵天，周露崛，毛湘伦，邬骏，崔

项目网站

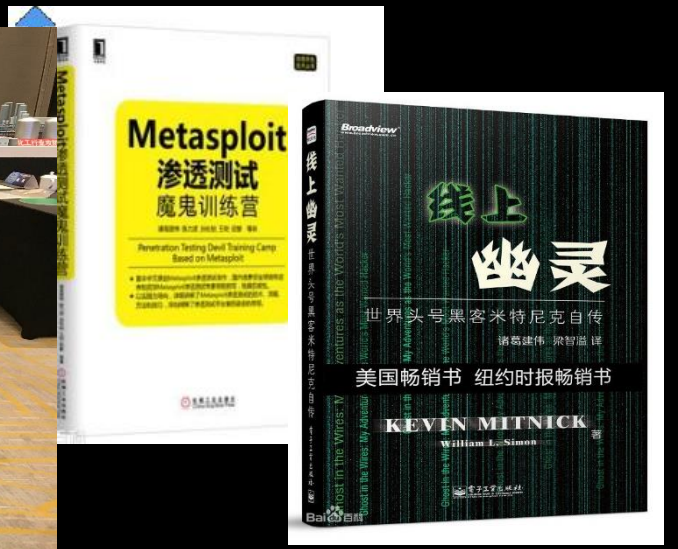
- Hacking技术交流站
- SCAP中文社区
- 共享文档（WIKI）

著名安全与信息安全研究团队和黑客战队

关于CDN攻击的研究获 NDSS ‘16 杰出论文奖

清华大学段海新教授带领博士生陈建军等研究者在美国举行的 学术会议NDSS'16 上发表的论文 “Forwarding-Loop Attacks in Content Delivery Networks” 被评为杰出论文(Distinguished Paper)。NDSS（Network and Distributed System Security Symposium）**是国际公认的网络和系统安全四大顶级学术会议（BIG4）**之一，2016年从 389 篇文章中录取了60篇优秀的研究论文（录取率15.4%），包括本论文在内的4篇论文被评为杰出论文（Distinguished Paper）。本论文**是中国科研机构在网络和系统安全领域国际顶级会议**上获得的**首个杰出论文奖**。

- **Blue-Lotus 蓝莲花(2010-)**
  - 2013年起，中国首次并连续四次入围DEF CON CTF全球总决赛，15排名世界第五，中国大陆最好成绩
  - HITCON CTF、Trend Micro CTF、SIGINT亚军，9447 CTF国际赛
- **0ops(2014-)**
  - 2015年入围DEF CON CTF全球总决赛，排名世界第六
  - CodeGate国际赛冠军，Hack.Lu国际赛亚军
- **2015-2018年全球排名前百强队伍**
  - 0ops (上海交通大学)、Blue-Lotus (清华为主)、Sigma (网络)、* (复旦大学)、ROIS (福州大学)、FlappyPig (多高校)



NISL@TU

1

网络信息安全的目标是保护数据 /信息

企业内机密、敏感和个人隐私数据是敏感数据

网络信息安全的目标是保护“信息”

保护网络

保护主机

保护应用

保护
数据中心

保护IT
基础设施

数据传输

数据处理

数据存储

数据

合规是实现“信息”/“数据”保护的基本途径

- 合规性要求的特点：**体系化、管理和技术并重，全面的要求**
  - ISO/IEC27001：2013 ISMS（信息安全管理体系）
    - 27001：要求
    - 27002：最佳实践
  - PCI DSS：支付卡行业数据安全标准
  - GDPR ：通用数据保护条例（General data protection regulation）
  - 等级保护：信息安全等级保护

ISO 27001

PCI DSS

NISL@TU

2

PCI DSS 支付卡行业数据安全标准

是典型的保护敏感个人支付信息的行业标准

PCI DSS -- 支付卡行业数据安全标准

- **Payment Card Industry (PCI) Data Security Standard**
  - **PCI DSS的核心是保护持卡人数据的 ：**
    - 传输、处理 和 存储 的关键环节

PCI DSS 的维护和制定者

- **PCI安全标准委员会（PCI SSC）：**
  - 由American Express、Discover Financial Services、JCB International、MasterCard Worldwide 和 Visa, Inc.于2006 年共同创立。
  - PCI安全标准协商目前是在美国德拉瓦周（ Delaware, USA ）注册成立的一家有限责任公司（LLC），非盈利性质的公司。

PCI Security Standards Council

PCI DSS 的版本发布

- Release: September 2006， PCI DSS 1.1
  - 到December 31, 2008为止
- Release: October 2008， PCI DSS 1.2
  - October 2008开始实行
- 2009年7月，修订版， PCI DSS 1.2.1
- 2010年10月，PCI DSS 2.0
- 2011年8月，Information Supplement: PCI DSS Wireless Guidelines
- 2011年8月，Information Supplement: PCI DSS Tokenization Guidelines
- 2013年11月，PCI DSS 3.0, 亚太 2014年底
- 2014年，PCI DSS 3.2
- 2015年底，PCI DSS 3.2
- **2018年5月 PCI DSS 3.2.1**

PCI DSS 的适用目标

- PCI DSS 的核心是保护持卡人数据的 – 传输、处理 和 存储

服务提供者

卡组织网络

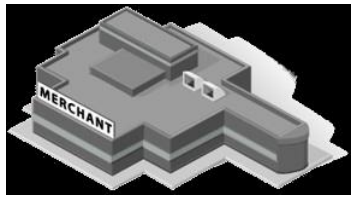
服务提供者

发卡机构

收单机构/行

服务提供者

持卡人



商户

服务提供者

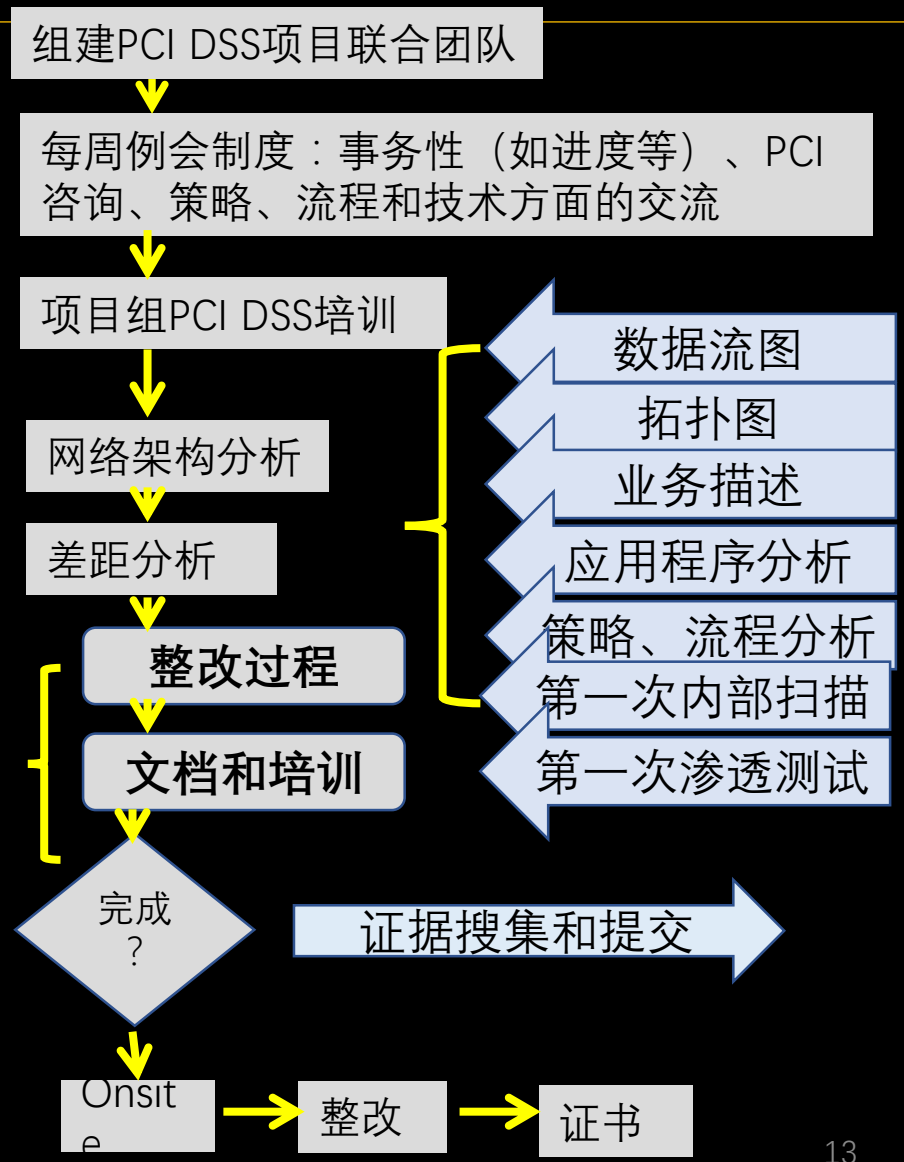
PCI DSS 的评估范围

PCI DSS 要求企业有完整的网络信息安全管理体系和技术体系架构

建立并维护安全的网络和系统	1、安装并维护防火墙配置以保护持卡人数据 2、不要使用供应商提供的默认系统密码和其他安全参数
保护持卡人数据	3、保护存储的持卡人数据 4、加密持卡人数据在开放式公共网络中的传输
维护漏洞管理计划	5、为所有系统提供恶意软件防护并定期更新杀毒软件或程序 6、开发并维护安全的系统和应用程序
实施强效访问控制措施	7、按业务知情需要限制对持卡人数据的访问 8、识别并验证对系统组件的访问 9、限制对持卡人数据的物理访问
定期监控并测试网络	10、跟踪并监控对网络资源和持卡人数据的所有访问 11、定期测试安全系统和流程
维护信息安全政策	12、维护针对所有工作人员的信息安全政策

PCI DSS 合规历程

- 启动项目Kick off
  - 项目组团队建设
  - PCIDSS安全标准培训
  - 网络体系架构分析
- 差距分析与系统整改
  - 差距分析
  - 系统整改与修复服务
- 文档建设与培训服务；
  - 安全策略与流程文档建设
  - 安全策略与流程培训
  - 应急相应培训
  - 员工安全意识培训；
- 技术服务；
  - 外部扫描
  - 外部渗透
  - 内部漏洞扫描服务（包含无线扫描）；
  - 内部渗透测试；
- PCIDSS审查服务；
  - 远程验证及证据提交；
  - PCIDSS Onsite审查验证；



3 构建满足PCI DSS要求的网络信息安全的体系架构

是保护信息/数据安全的基础

网络信息安全领域的对抗 —— 是非对称的

1

防守方

企业面临的是非对称威胁

- “敌强”，我弱
- “敌众”，我寡
- 我明，“敌暗”

防守方木桶效应突出

- 万无一失 – “难”

2

攻击者

为生存而战，动机明确

- 行走在地下世界，“风险小”，“收益大”
- 黑客也是人，也要养家糊口

理解网络信息安全的基本概念 -- CIA

网络/系统无法使用

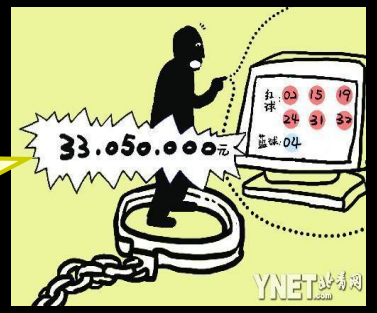
可用性：保证合法用户对信息和资源的使用不会被不正当地拒绝

机密信息泄露

机密性：是指网络信息不被泄露给非授权的用户

数据被篡改

完整性：指在传输、存储信息或处理数据的过程中，确保信息或数据不被非授权用户篡改



可用性

机密性

完整性

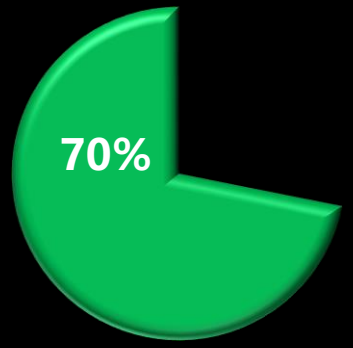
信息安全基本三要素

1、 安全意识的培养：企业面临的各种各样的安全危险

2、建立基本的网络信息安全管理理念：安全管理很重要

管理层负责

1. 成立企业网络信息安全管理委员会，明确职责
2. 制定企业的网络信息安全政策、策略和流程
3. 建立应急响应处理机制和流程



安全问题70%的的管理问题

技术也很重要

30%的技术问题

3、数据分类很重要：保护有价值的数据

信息所有者的责任

基本数据分类

- 机密数据
- 敏感数据
- 私有数据
- 可公开数据

保护机密/敏感数据

不同的数据

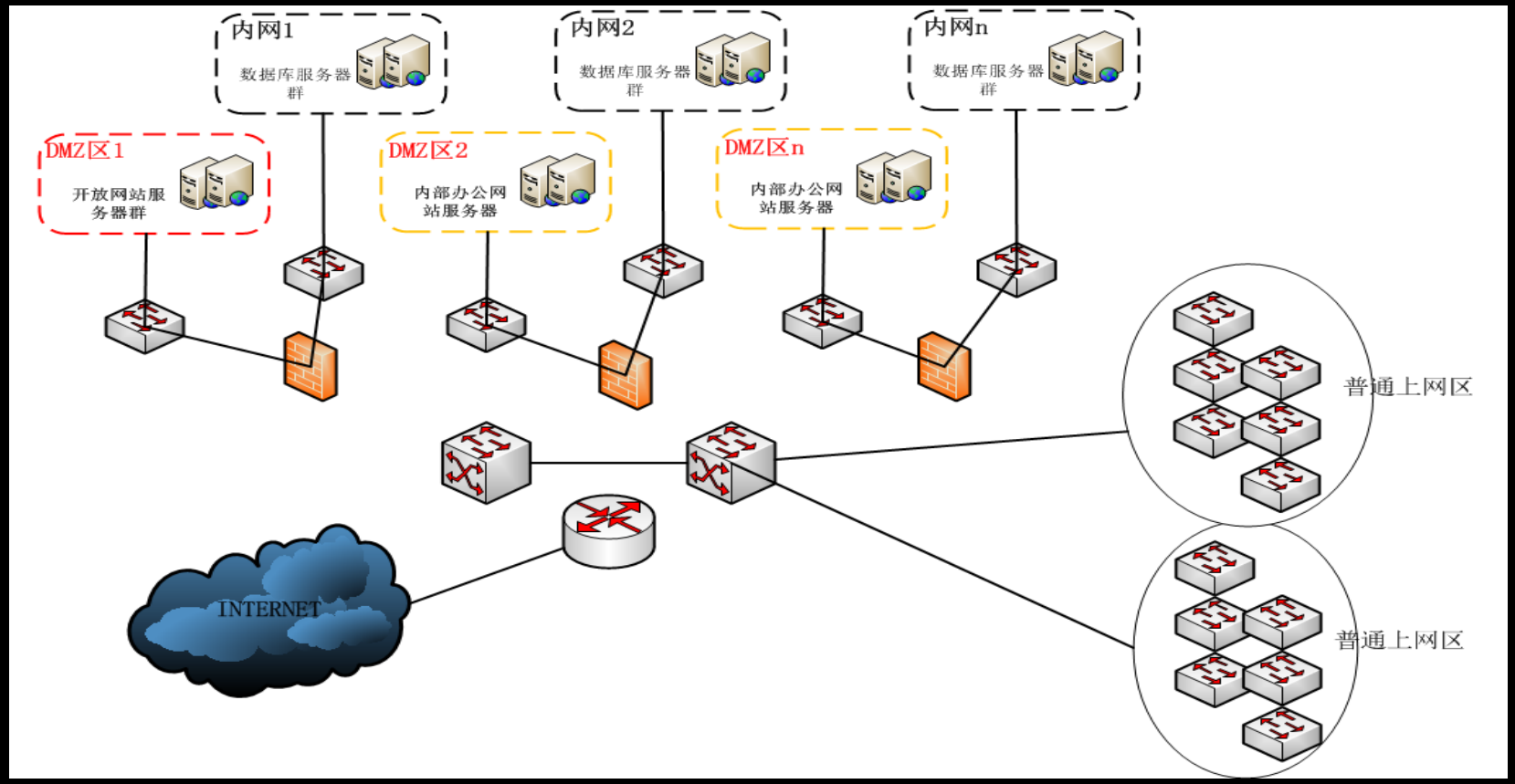
不同的传输、处理和存储措施

4、网络架构的安全很重要 -- 不要让设备厂商给“忽悠了”

安全区域划分：分级、明确服务对象和安全需求

基本数据分类：保护敏感、机密数据的传输、处理和存储

- 网络基础架构的安全
  - DMZ：提供公共服务。
  - 内网：仅供内部使用，数据库只能放在内网。
- 安全设备
  - 防火墙，WAF，IDS/IPS
  - 日志服务器
  - 防病毒
  - 文件完整性监控：防窜改



5、“技术体系”和“管理体系” --》 都很重要

网络信息安全技术

- 防病毒软件：不可缺少
- 防火墙：边界防护，标配设备
- WAF：有一定作用
- IDS/IPS：标配设备

安全即服务（Security as a service）

网络信息安全管理策略

- 安全策略和流程：等保要求，安全规划
- 漏洞管理流程
- 周期性安全检查策略：
  - 渗透测试服务
  - 漏洞检测
  - 安全加固（基线建设）
  - 日志监控（FW/IDS/Syslog等）
  - 基线检查。。。

安全技术平台

安全服务集合

4 网络信息安全工作面临的挑战

挑战 -- 安全团队缺人是关键

- **重要**：绝大多数企业的主要业务不是IT，但IT系统是成为了基础业务支撑系统
- **专业**：网络信息安全问题是**专业领域问题**，普通IT运维难以从专业的角度处理信息安全问题
- **复杂**：网络信息安全涉及**网络安全**、**系统安全**、**数据库安全**、**应用安全**等各个方面（需要各领域安全人员相关配合）
- **昂贵**：网络信息安全成本高，安全设备多种多样，安全技术复杂多变
- **其他问题**：学校缺少信息安全专业氛围，安全人员流失；安全设备多种多样；安全事件影响重大；安全标准繁多

企业IT环境的复杂性和安全的不确定性

一般而言，企业的IT环境是由**多种业务服务器**（包括WEB服务器、邮件服务器、数据库服务器等）、**网络基础设施**（包括接入路由器、核心交换机等）和**网络安全设施**（包括防火墙、防病毒服务器、日志系统、入侵检测或防护系统等）等组成。

面对复杂的IT运行环境和广泛存在的攻击行为，一般企业在部署了各类网络安全设备/系统后，依然无法解决安全问题。保障安全需要有**专业的**安全团队对IT系统进行**周期性**的安全评估和配置检测，对系统日志进行**持续的**分析和审核，对各种系统组件进行**持续的**监控和升级，这些繁重的安全保障工作需要花费大量的人力、物力。

安全缺位的法律风险

网络安全法 – 法律风险：

自从网络安全法在2017年6月1日正式实施后，已经有百度、微信、BOSS直聘、某高校等众多企事业单位受到处罚。网络信息安全的**责任主体**明确到**网络的所有者**、**管理者**和**网络服务的提供者**。

一旦发生网络信息安全事件，不但会对企业的正常运作造成严重的影响，造成巨大的经济损失， 企业等单位**的管理者**还要面临违法的风险。然而，现今在大多数的企、事业单位等**缺少专业的网络安全管理和技术团队**，因此网络信息安全管理不到位，网络信息安全防护技术力量弱，重视网络信息安全却又力不从心！无法应对网络信息安全风险。

网络信息安全托管服务

- **安全服务提供商：安全托管服务就是**通过为**一系列的、持续的安全技术和管理服务**，来保障客户IT系统的安全，从而达到**让客户安心、省心、放心，省人、 省事、 省钱**的目的。
- **有了安全托管**：客户的IT系统***平时有人打理，出事有人处理，安全有人管，责任有人担！***

NetDefender安装管理综合运营平台

正确理解网络信息安全托管服务： P – D – C – A

组织

安全策略和流程

技术

效果评估

发布/实施/检查

选型/实施/运行/检查

漏洞/威胁/风险/处置/检查

周期性安全服务

外部组织/专家

制定安全策略和流程

安全技术体系架构

风险评估/标准/攻击防御

加固/渗透/扫描/日志审核

内部安全组织

咨询，培训，协调，沟通

规划/推进

1

2

3

4

改进

NISL@TU

SECSPACE.COM
北京三思网安科技有限公司

致谢！ CIO各位同仁

Thank You!

魏克：weike@tsinghua.edu.cn
电话：13811578231