信息安全管理
先锋论坛

跟我学信息安全管理

ISO27001条文解析（附录A） 师鑫

信息安全管理专家委员会发布
2016年5月

信息安全管理论坛（http://www.iso27001cn.com）成立于2014年9月，为国内目前最专业的信息安全管理学习和实践交流平台。是学习信息安全管理方法、分享实战经验、提升实践水平的好地方！

关于我们

我们提供

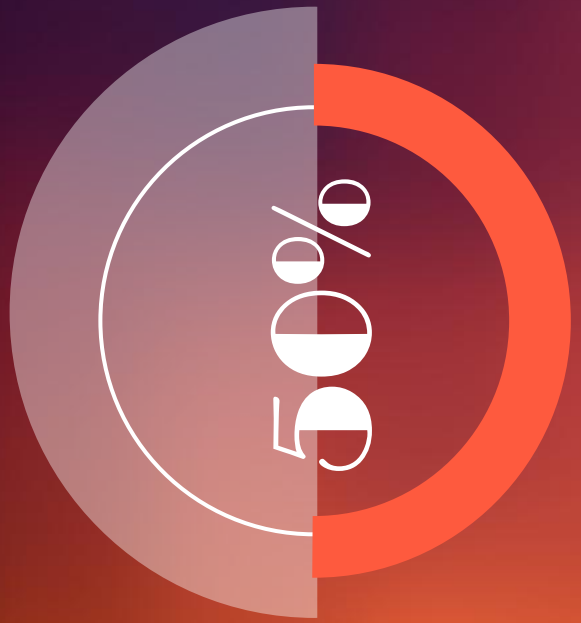
- 最全的信息安全管理资料
- 信安经理高薪工作机会推荐
- 每周专家讲堂（ 每周四晚上8点半YY频道89519382 ）
- 物美价廉的ISO27001课程团购

- 信息安全管理学习实践QQ群 207723402
- 微信 IT管理精英圈 itilxf_(记得有下划线)

欢迎关注

授课专家

师 鑫



师鑫老师在某世界500强外企负责运维工作8年时间，期间信息安全管理是一项重要的工作职责，目前有2年咨询顾问经验，主要负责信息安全体系建设和运维体系建设的研究。 曾在众多项目的开发和实施过程中担任重要角色，并且拥有多年的授课经验。不但拥有知识理论的功底，又有实战与实践的经验，高度的责任感，积极进取，在教育培训中不断的与学员分享与实践。

典型项目经验：

中国工程物理 研究院ISO27001项目

微创医疗ISO27001项目

华东凯亚ISO27001项目

中国电信云公司ISO27001项目

ISO27001-2013标准

条文解析

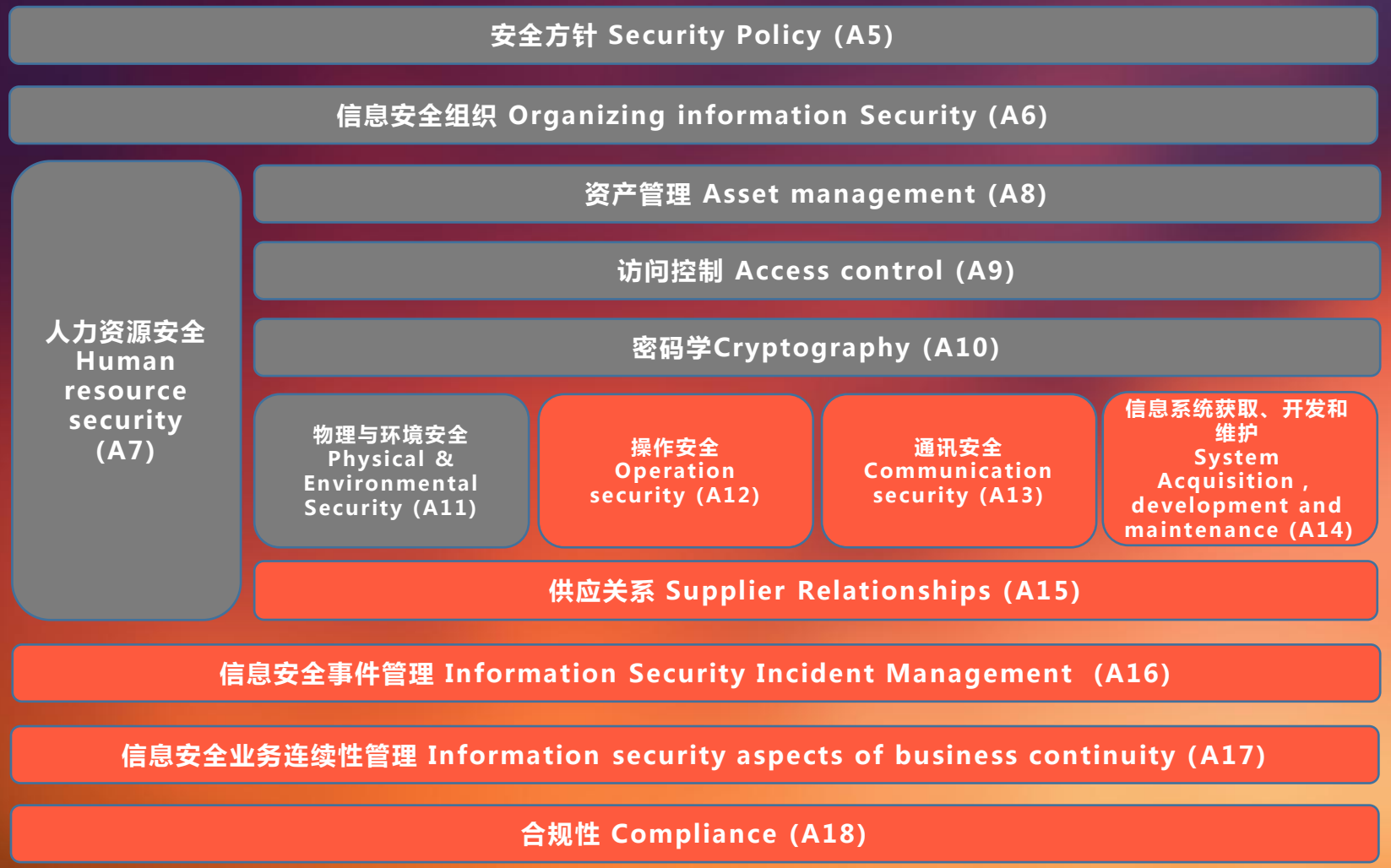
时间安排

- 正文　2016年4月28日　宽恕
- 附录A　2016年5月12日　樊忠林
- 附录A　2016年5月28日　师鑫

ISO 27001 标准正文

ISO 27001标准 附录A

- 本标准包括14个安全控制域，共含有35个主要安全类别和114 项安全控制措施。



A-12 操作安全

- A-12 操作安全
  - A-12-1 操作程序和职责
  - A-12-2 恶意软件防护
  - A-12-3 备份
  - A-12-4 记录和监控
  - A-12-5 操作软件的控制
  - A-12-6 操作脆弱性管理
  - A-12-7 信息系统审计考虑

- A-12-1-1 文件化的操作程序
  - 操作过程应形成文件，并提供给所有需要的用户。
- A-12-1-2 变更管理
  - 对组织，业务流程，信息处理设施和系统的变更应加以控制。
- A-12-1-3 容量管理
  - 资源的使用应加以监视、调整，并作出对于未来容量要求的预测，以确保拥有所需的系统性能。
- A-12-1-4 开发、测试和运行环境分离
  - 开发以及测试环境应与运营环境分离、减少未授权访问和对操作系统变更的风险。

A-12 操作安全

- A-12 操作安全
  - A-12-1 操作程序和职责
  - A-12-2 恶意软件防护
  - A-12-3 备份
  - A-12-4 记录和监控
  - A-12-5 操作软件的控制
  - A-12-6 操作脆弱性管理
  - A-12-7 信息系统审计考虑

- A-12-2-1 控制恶意软件
  - 应实现结合适当的用户提要，使用检测、预防和恢复控制的手段来防范恶意软件。

A-12 操作安全

- A-12 操作安全
  - A-12-1 操作程序和职责
  - A-12-2 恶意软件防护
  - A-12-3 备份
  - A-12-4 记录和监控
  - A-12-5 操作软件的控制
  - A-12-6 操作脆弱性管理
  - A-12-7 信息系统审计考虑

- A-12-3-1 信息备份
  - 根据既定的备份策略备份信息，软件和系统映像，并定期测试。

A-12 操作安全

- A-12 操作安全
  - A-12-1 操作程序和职责
  - A-12-2 恶意软件防护
  - A-12-3 备份
  - A-12-4 记录和监控
  - A-12-5 操作软件的控制
  - A-12-6 操作脆弱性管理
  - A-12-7 信息系统审计考虑

- A-12-4-1 事件日志
  - 应产生记录用户活动、异常情况、错误和信息安全事件的事件日志，并要保持一个已设的周期以支持将来的调查和访问控制监视。
- A-12-4-2 日志信息的保护
  - 记录日志的设施和日志信息应加以保护，以防止篡改和未授权的访问。
- A-12-4-3 管理员和操作员日志
  - 系统管理员和系统操作员的活动应当记录日志，并对其保护和定期检讨。
- A-12-4-4 时钟同步
  - 一个组织或安全域内的所有相关信息处理设施的时钟应使用已设的精确的时间源进行同步。

A-12 操作安全

- A-12 操作安全
  - A-12-1 操作程序和职责
  - A-12-2 恶意软件防护
  - A-12-3 备份
  - A-12-4 记录和监控
  - A-12-5 操作软件的控制
  - A-12-6 操作脆弱性管理
  - A-12-7 信息系统审计考虑

- A-12-5-1 操作系统软件的安装
  - 应建立流程对操作系统软件安装进行控制。

A-12 操作安全

- A-12 操作安全
  - A-12-1 操作程序和职责
  - A-12-2 恶意软件防护
  - A-12-3 备份
  - A-12-4 记录和监控
  - A-12-5 操作软件的控制
  - A-12-6 操作脆弱性管理
  - A-12-7 信息系统审计考虑

- A-12-6-1 技术脆弱性的管理
  - 应及时得到现用信息系统技术脆弱性的信息，评价组织对这些脆弱性的暴漏程度，并采取适当的措施来处理相关风险。
- A-12-6-2 限制软件安装
  - 应建立流程对操作系统软件安装进行控制。

A-12 操作安全

- A-12 操作安全
  - A-12-1 操作程序和职责
  - A-12-2 恶意软件防护
  - A-12-3 备份
  - A-12-4 记录和监控
  - A-12-5 操作软件的控制
  - A-12-6 操作脆弱性管理
  - A-12-7 信息系统审计考虑

- A-12-7-1 信息系统审计控制
  - 设计对运行系统核查的审计要求和活动，应谨慎的加以规划并取得批准，以便最小化造成业务过程中断的风险。

携程网瘫痪超8小时

2015-05-29 07:57:59　来源: 网易科技报道

网易科技讯 5月29日讯 今日凌晨1：30分，携程官方称，经携程技术排查，确认此次事件是由于员工错误操作导致。从5月28日上午11:09，发现携程官网及APP出现故障，到28日23:29全面恢复，整个过程耗费12个多小时。

另外携程还称，由于携程涉及的业务、应用及服务繁多，验证应用与服务之间的功能是否正常运行，花了较长时间。携程官方网站及APP已于28日23:29全面恢复正常。对用户造成的不便，携程再次深表歉意。

对于本次事件的排查结果，简要原因说明：

1、事件发生原因

经携程技术排查，确认此次事件是由于员工错误操作，删除了生产服务器上的执行代码导致。

2、为什么恢复时间那么长

一般来说，类似携程这样的大型网站承载着繁多业务，其后台是一个由SOA（面向服务）架构组成的庞大服务器集群，看似简单的一个页面背后由上千个应用子系统以及上千个Web Service组成，而每个应用子系统和每个Web Service之间都存在着相互调用的依赖关系。

发生事件后，携程的技术人员除了需要恢复生产服务器上的执行代码以外，还需要做的是恢复并确保每个应用子系统以及每个Web Service的功能正常，同时确保应用子系统与Web Service间的调用关系得以正常执行。

这种验证性的操作需要携程的工程师及运维人员通力合作，尽快恢复生产代码并通过反复地、持续性地调试以确保应用子系统与Web Service功能的正常运行。

携程再次保证，数据和数据库并未受到此次事件的影响，用户订单数据也完整无损，请用户放心并继续使用携程网站及App。

3、如何杜绝此类事件的再次发生？

携程在系统上做了改进，规范并杜绝技术人员错误删除生产服务器上代码的操作。

.cn根域名服务器遭遇有史最大的DDOS攻击

2013年8月25日，中国互联网络信息中心(CNNIC)发表声明，国家域名解析节点与8月25日凌晨时许受到拒绝服务攻击，到凌晨3时服务恢复正常。期间大量.cn域名和.com.cn无法解析，受影响的包括新浪微博和一批以.cn为域名的网站。事后查明是由于黑客利用僵尸网络攻击某游戏私服导致。　几天后，国家互联网应急中心CNCERT/CC运行管理部处长王明华透露，策划该事件的黑客已经在山东青岛被抓获。

飓风熊猫本地提权工具

2014年10月，CrowdStrike发现飓风熊猫这个本地提权工具，飓风熊猫是主要针对基础设施公司的先进攻击者。国外专业人士还表示，该攻击代码写的非常好，成功率为100%。我们知道飓风熊猫使用的是“ChinaChopper”Webshell，而一旦上传这一Webshell，操作者就可试图提升权限，然后通过各种密码破解工具获得目标访问的合法凭证。该本地提权工具影响了所有的Windows版本，包括Windows7和WindowsServer 2008 R2 及以下版本。

赛门铁克揭秘间谍工具regin

2014年11月24日，赛门铁克发布的一份报告称，该公司发现了一款名为“regin”的先进隐形恶意软件。这是一款先进的间谍软件，被称为史上最为复杂的后门木马恶意软件。该软件被用于监视政府机关、基础设施运营商、企业、研究机构甚至针对个人的间谍活动中。

关于JBoss网站蠕虫再次大规模爆发的情况通报

时间：2013-03-05

缩小字体 放大字体

国家互联网应急中心（CNCERT）抽样监测发现，JBoss网站蠕虫在继2012年第三季度大规模爆发后，在今年2月26日凌晨1:50左右再次出现大规模的攻击情况。该蠕虫具有传播速度快、影响范围广等特点，对网站用户信息安全和业务运行安全构成严重的威胁。现将有关情况通报如下：

一、情况分析

根据CNCERT抽样监测结果，从2月26日1:50左右开始，JBoss网站蠕虫再次活跃，仅截止到27日12点已感染网站服务器203个，其中境内网站有58个。这些被JBoss网站蠕虫成功入侵的服务器，还会自动扫描其他网站服务器，利用JBoss漏洞对之进行攻击从而传播自身。截至27日12点，被扫描攻击的网站数量高达90.7万个，其中境内网站有35.7万，涉及大量政府网站、金融行业网站、新闻类网站及科研院所网站等重要网站。

JBoss网站蠕虫主要攻击存在“JBoss企业应用平台JMX控制台安全绕过漏洞”（编号：CNVD-2010-00821）的网站服务器，并通过服务器开放的JMXInvokeServlet服务，在网站上植入.JSP类型的网站后门文件以及相关恶意程序，常见后门文件有：zecmd.jsp、idssvc.jsp、iesvc.jsp、wstats.jsp、invoker.jsp。由于感染JBoss网站蠕虫的都是网站服务器，而并非普通的用户个人计算机，且受感染的大量网站能够形成一个受到黑客远程集中控制的僵尸网络，所以JBoss网站蠕虫危害十分严重，需引起高度重视。

A-13 通信安全

- A-13 通信安全
  - A-13-1 网络安全管理
  - A-13-2 信息传输

- A-13-1-1 网络控制
  - 应管理和控制网络以保护系统和应用程序中的信息。
- A-13-1-2 网络服务的安全
  - 所有网络服务的安全机制，服务水平和管理要求，应予以明确并列入网络服务协议中，无论这些服务是否由公司内部提供还是外包。
- A-13-1-3 网络隔离
  - 应在网络中隔离信息服务、用户以及系统信息。

A-13 通信安全

- A-13 通信安全
  - A-13-1 网络安全管理
  - A-13-2 信息传输

- A-13-2-1 信息传输的策略和程序
  - 应建立正式的传输策略，流程和控制措施，以保证所有类型的通信设施间的信息传输安全。
- A-13-2-2 信息传输协议
  - 应建立组织与外部放传输商业信息的安全传输协议。
- A-13-2-3 电子消息
  - 涉及电子消息的信息应适当保护。
- A-13-2-4 保密或不泄露协议
  - 应确定组织信息保护需要的保密性或不泄露协议的要求，定期审查并记录。

黑客入侵亚马逊网上鞋店Zappos盗取2400万客户资料

2012年01月17日 14:22

来源：深圳特区报 作者：吴炎

深圳特区报讯 据英国媒体16日报道，亚马逊网上鞋店Zappos．com日前表示，黑客已窃取其2400万客户的个人信息，包括顾客姓名、电邮地址、收货地址、电话号码和信用卡的最后四位数字。所幸由于完整的信用卡号码存放在另外一个服务器内，所以未被黑客盗取。

据网店声明称，黑客是通过肯塔基州一个服务器入侵系统的。目前，警方正在调查这一案件。

在致客户的公开信中，网店首席执行官表示，为了保护顾客信息不被非法使用，客户原密码已被取消，并要求客户重设密码。 （吴炎编译）

美国通过互联网监听从事工业间谍活动

- 美国国家安全局监听计划的揭露给2014年的整个IT界和各国政府都蒙上了一层阴影。可以说，今年一月爱德华·斯诺登声称的以民主堡垒自居的美国通过互联网监听从事工业间谍活动是最令人不寒而栗的事件之一。
- 斯诺登称，美国的工业间谍活动所针对的不仅仅只是限于“国家安全问题”，而且还包括任何可能对美国有价值的工程和技术资料。他以德国工业巨头西门子为例说:“如果西门子的信息符合美国的国家利益，即使这些信息与美国的国家安全没有半毛钱关系，他们照样还是会拿取这些信息。”
- 和今年的其他安全事件一样，斯诺登的言论毫无疑问地引起了很多关于将敏感信息存储在云端是否符合其背后逻辑的质疑。

法国被曝用海底电缆监听世界

2015-07-04 19:54:23　来源: 新华网

分享到：

707

这个夏天，一场监听大戏在大西洋两岸上演。先是，维基揭秘网站曝光，美国国家安全局监听三任法国总统。美国“致歉”，法国“震惊”。接着，维基揭秘再爆料，美国监听包括财政部长在内的多名法国政要和大型企业，法国再度“震惊”。最新一集的剧情颇有点反转：法国媒体报道，法国情报机构同样在利用海底电缆监听世界，其中自然包括美国。

看起来，全世界的间谍和情报机构干的活儿都差不多。难怪法国《新观察家》周刊1日在报道法国这一秘密监听项目时语气平淡，标题甚至不乏自嘲：《法国如何也在监听世界》。

这篇报道说，早在2008年，时任法国总统尼古拉·萨科齐授权情报机构国外安全总局利用海底电缆监听全球通信。这一项目耗资7亿欧元(约合7.7亿美元)，为期5年。国外安全总局在法国马赛等地安装海底电缆“拦截站”，监听欧洲与世界的通信。

按照这家媒体的说法，在通信运营商的“帮助”下，2008年至2013年间，法国情报机构监听至少五条海底电缆通信，涉及国家和地区包括美国、印度、东南亚和西非。

德国联邦情报局再陷“监听门”

发布时间：2016-03-02 07:38:00　来源：人民日报　作者：冯雪珺　责任编辑：罗伯特

德国《明镜》周刊近日披露，德国联邦情报局对盟友的窃听行为“显然没有丝毫限制”。《明镜》周刊从政府相关渠道获得的信息显示，为窃取欧盟外交政策情报，在凯瑟琳·阿什顿2009年担任欧盟外交和安全政策高级代表、欧盟委员会第一副主席后，德国联邦情报局一直在监视其电话和邮件，直到2013年秋季才终止这一行动。德国新闻电视台表示，若消息属实，这将是一起严重的外交事件，会使德国和欧盟之间产生不信任，德国在欧盟的主导地位也将受到冲击。此外，多位欧洲国家领导人和美国国务卿克里也在窃听名单上。

德国联邦情报局去年10月就曾被曝出监听盟友丑闻，欧盟委员会、法国等盟国驻德大使馆以及欧洲航空防务及航天集团、欧洲直升机公司等都在德国的“监听名单”中。奥地利内政部去年甚至就德国监听事件提出了司法指控。

德国“每日新闻”网站2月24日披露，尽管德国联邦情报局是一个对外情报部门，但在其“怀疑即侦查”的宗旨下，德国本国公民也未能逃离监听。报道批评称，这是公然“忽视公民基本权利保护”的行为。据悉，2月中旬，德国联邦情报局将一份机密文件交送至被称为“G10”的秘密会议在联邦议院分设的办公室，文件主要内容涉及对德国公民的监听。德国联邦情报局监听本国公民的行为已长达10多年，这一行为由德国总理府办公室授权，依据“职能部门理论”的规定，只要德国公民为外国机构工作，且不在谈论私人事务，其通话及邮件就可以被监听。

A-14 系统获取、开发和维护

- A-14 系统获取、开发和维护
  - A-14-1 信息系统的安全要求
  - A-14-2 开发和支持过程中的安全
  - A-14-3 测试数据

- A-14-1-1 安全需求分析和规范
  - 在新的信息系统或增强已有的信息系统的业务需求陈述中，应规定对安全控制措施的要求。
- A-14-1-2 保护公共网络上的应用服务
  - 公网上应用服务中传输的信息应被保护，以免遭受欺诈、合同纠纷，未经授权的披露和修改。
- A-14-1-3 保护应用服务交易
  - 应用服务传输中所涉及到的交易信息应加以保护，以防止未经授权的消息改变，不完整的传输，路由错误，未经授权披露，未经授权的消息复制或重放。

A-14 系统获取、开发和维护

- A-14 系统获取、开发和维护
  - A-14-1 信息系统的安全要求
  - A-14-2 开发和支持过程中的安全
  - A-14-3 测试数据

- A-14-2-1 安全开发策略
  - 应制定以及应用关于软件和系统的开发规则。
- A-14-2-2 变更控制程序
  - 公网上应用服务中传输的信息应被保护，以免遭受欺诈、合同纠纷，未经授权的披露和修改。
- A-14-2-3 操作平台变更后对应用的技术评估
  - 当操作平台发生变更时，应对业务的关键应用进行评审和测试，以确保对组织的运行和安全没有负面影响。
- A-14-2-4 软件包变更的限制
  - 应对软件包的修改进行劝阻，只限于必要的变更，且对所有的变更加以控制。
- A-14-2-5 系统开发程序
  - 应建立安全系统开发流程，记录，维护并应用到任何信息系统开发工作。

A-14 系统获取、开发和维护

- A-14 系统获取、开发和维护
  - A-14-1 信息系统的安全要求
  - A-14-2 开发和支持过程中的安全
  - A-14-3 测试数据

- A-14-2-6 安全的开发环境
  - 组织应建立并适当保护开发环境安全，并集成涵盖整个系统开发周期的工作
- A-14-2-7 外包开发
  - 组织应监管和监督外包的系统开发工作
- A-14-2-8 系统安全性测试
  - 在开发过程中，必须测试功能的安全性
- A-14-2-9 系统验收测试
  - 在建立新系统，升级系统和更新版本时，必须建立验收测试程序和相关标准

A-14 系统获取、开发和维护

- A-14 系统获取、开发和维护
  - A-14-1 信息系统的安全要求
  - A-14-2 开发和支持过程中的安全
  - A-14-3 测试数据

- A-14-3-1 测试数据的保护
  - 测试数据应被仔细筛选，保护和控制。

公安部物证鉴定中心网站遭入侵 黑客留言调侃

http://news.QQ.com 2010年01月04日01:12 京华时报 苗慧 我要评论(278)

公安部物证鉴定中心网站首页

CSDN首页 > 移动开发

XcodeGhost爆发 中国APP开发者遭遇严重水坑攻击

发表于 2015-09-24 15:49 | 47次阅读 | 来源 新闻资讯 | 0条评论 | 作者 新闻资讯

摘要：9月18日，苹果iOS被曝出安全漏洞，黑客利用经过篡改的开发工具Xcode向300余款千万量级的热门APP注入了木马病毒，致使上亿用户的手机配置信息被第三方提取，并随时存在用户隐私信息泄漏、Apple ID账密泄漏、网银及第三方支付账户被盗等风险。然而，在苹果的安全神话被彻底粉碎之后4天，知名游戏引擎...

9月18日，苹果iOS被曝出安全漏洞，黑客利用经过篡改的开发工具Xcode向300余款千万量级的热门APP注入了木马病毒，致使上亿用户的手机配置信息被第三方提取，并随时存在用户隐私信息泄漏、Apple ID账密泄漏、网银及第三方支付账户被盗等风险。然而，在苹果的安全神话被彻底粉碎之后4天，知名游戏引擎Unity及Cocos-2d也被曝出以同样的手法遭到篡改，瑞星安全研究院对该事件进行了重点关注和研究，并发现《愤怒的小鸟2》、《叫叫超级医生》等知名手游都已遭到XcodeGhost攻击。瑞星安全研究院院长刘思宇指出，本次攻击事件的发生绝非偶然，这是一次蓄谋已久的针对APP开发者的"水坑攻击"，其危害之大、范围之广，史无前例，也很大程度上挑战了iOS以及苹果APP生态链的安全性。

A-15 供应商关系

- A-15 供应商关系
  - A-15-1 供应商关系的安全
  - A-15-2 供应商服务交付关系

- A-15-1-1 供应商关系的信息安全策略
  - 对于减少与供应商相关的信息安全风险或信息处理设施的信息安全要求应被记录。
- A-15-1-2 供应商协议中的安全
  - 应建立于信息安全相关的要求并获得供应商的认可，包括处理，存储，沟通或提供组织IT基础设施的信息。
- A-15-1-3 ICT供应链
  - 与供应商的协议应包括解决信息、通信技术服务、产品供应链相关信息安全风险的要求。

A-15 供应商关系

- A-15 供应商关系
  - A-15-1 供应商关系的安全
  - A-15-2 供应商服务交付关系

- A-15-2-1 监测和审查供应商服务
  - 组织应定期监测，审查和审核供应商的服务。
- A-15-2-2 供应商服务变更管理
  - 应管理供应商提供服务的变更，包括维护、改进现有的信息安全策略、程序和控制，应将商业信息的关键性，系统、流程和风险的重新评估考虑在内。

上海数十万条新生儿信息遭倒卖 卫生局：系外包数据公司所为

2012-08-30 13:52 来源：中国广播网 打印本页 关闭

中广网上海8月30日消息（记者周洪）今天（30日），有上海媒体报道数十万条新生儿信息遭倒卖。卫生局表示此事系外包数据公司所为。

今天记者就此事采访上海市卫生局，卫生局表示出生系统数据库由卫生局外包给一家数据公司，然而这家公司的管理松懈，犯罪嫌疑人张某甚至可以在家中采集数据库，无人监管。

据悉，30岁的张某到案后，交代了其利用开发、维护市卫生局出生系统数据库的职务便利，于2011年初至2012年4月，每月两次非法登录该数据库，下载新生儿出生信息累计达数十万条，并出售非法获利3万余元。

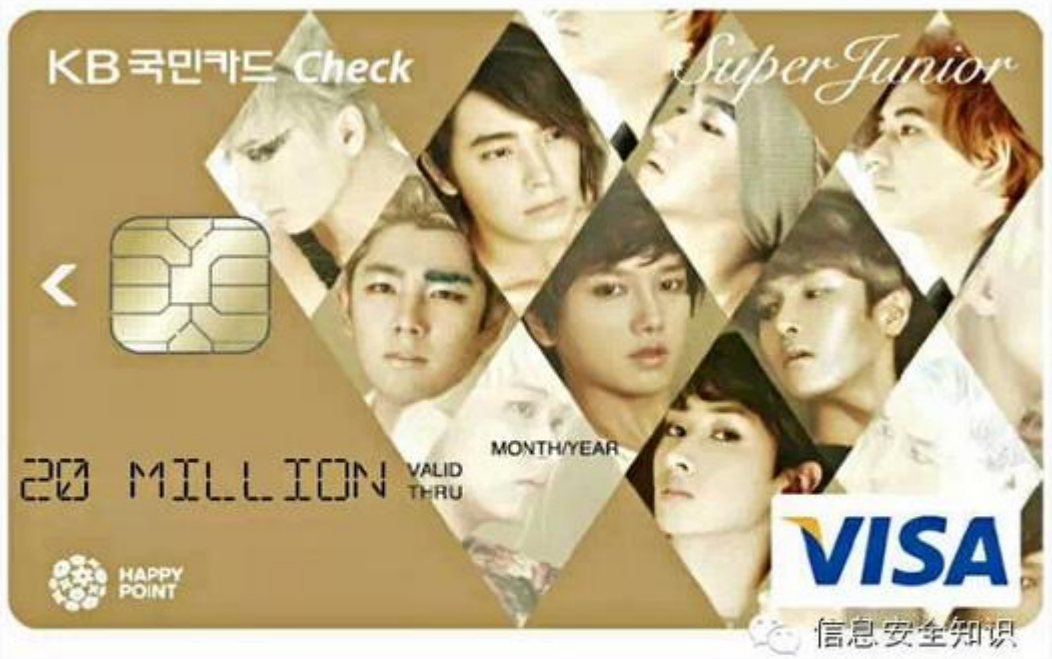
目前，为避免数据库信息再次发生泄露，市卫生系统已经采取措施，规定外包服务方必须在指定的卫生系统地点进行数据维护，并有专人予以全程陪同。

今年央视“3?15”晚会曝光了罗维邓白氏公司非法买卖公民个人信息事件，上海警方在控制5名公司高管后，经过数月的追踪调查又先后抓获了48名犯罪嫌疑人，查获近2亿条被倒卖的公民个人信息。

上海警方昨日表示，在被抓的犯罪嫌疑人中，有些与本市卫生系统和保险行业有紧密接触，其中有几十万条新生儿出生信息遭倒卖。目前，所有涉案犯罪嫌疑人均已移送检察机关审查起诉。

警方提醒市民，如发现个人信息遭泄露 并被非法使用的情况，应及时向公安机关报案。

一、韩国信用局



今年一月，据透露韩国信用局2700万条记录被盗，包括姓名、居民身份证号码和信用卡详细信息，波及韩国人口的40%。一家负责韩国信用局信用评分系统的计算机承包商，因在超过一年半的时间里滥用访问权限秘密复制数据到外部驱动器，而成为该事件的罪魁祸首。目前该承包商已经被确认并逮捕，一起被逮捕的还包括在信息传播中发挥作用的15人。当局仍在试图确定泄露记录的分布情况，调查还没有结束。

三、美国塔吉特连锁店

同样今年二月，塔吉特宣布，某受信第三方供暖和空调承包商对这起历史上最大的数据泄露事件负责。在这起内部事件中，塔吉特连锁店顾客的4000万客户信用卡和借记卡号码连同7000万条包含姓名、地址、电子邮件和电话号码的记录被泄露。此次泄露事件仍在接受联邦调查，目前塔吉特正在处理由受影响银行和信用联盟提请的诉讼。

四、美国杜邦

今年三月，美国杜邦公司宣布，其用于纸品和塑料清洁生产的白色颜料专有配方被盗，并在市场上以140亿美元的价格卖给了一家有竞争力的中国公司。杜邦公司某承包商以2800万美元的合同价售出了该配方。承包商被判经济间谍罪、窃取商业机密罪、干预证人罪、虚假陈述罪等22项罪名。

A-16 信息安全事件管理

- A-16 信息安全事件管理
  - A-16-1 信息安全事件管理和持续改进

- A-16-1-1 职责和程序
  - 应建立管理职责和程序，以确保快速、有效和有序地响应信息安全事件。
- A-16-1-2 报告信息安全事态
  - 信息安全事态应尽可能快的通过适当的管理渠道进行报告
- A-16-1-3 报告信息安全弱点
  - 应要求信息系统和服务的所有员工、外部方人员记录并报告他们观察到的或可以的任何系统或服务的安全弱点。
- A-16-1-4 信息安全事件的评估和决策
  - 信息安全事件应当被评估与决策，如果他们被归类为信息安全事件。

A-16 信息安全事件管理

- A-16 信息安全事件管理
  - A-16-1 信息安全事件管理和持续改进

- A-16-1-5 信息安全事故的响应
  - 信息安全事件应按照程序文件响应。
- A-16-1-6 回顾信息安全事故
  - 从分析和解决信息安全事故中获取知识，减少未来事故的可能性和影响。
- A-16-1-7 收集证据
  - 组织应制定和应用程序，用于鉴定，收集，获得和保存可作为证据的信息。

A-17 信息安全方面的业务连续性管理

- A-17 信息安全方面的业务连续性管理
  - A-17-1 信息安全连续性
  - A-17-2 冗余

- A-17-1-1 规划信息安全连续性
  - 组织应确定其在不利情况下的信息安全和信息安全管理连续性要求，如危机或灾难。
- A-17-1-2 实现信息安全的连续性
  - 组织应建立，记录，实施，维护流程、程序、控制项，以保证在不利情况下要求的信息安全连续性等级。
- A-17-1-3 验证、评审和评估信息安全的连续性
  - 组织应每隔一段时间合适其建立和实施的联系安全连续性控制，以确保他们在不利情况下是有效和生效的。

A-17 信息安全方面的业务连续性管理

- A-17 信息安全方面的业务连续性管理
  - A-17-1 信息安全连续性
  - A-17-2 冗余

- A-17-2-1 信息处理设施的可用性
  - 信息处理实施应当实现冗余，以满足可用性需求。

武汉同济医院电脑系统出现故障 患者无法看病(图)

发布时间：2013-04-25 09:54:56 来源： 楚天都市报 【关闭】

看病系统出现故障，不少患者等候

楚天都市报讯 记者 张皓 摄影：记者 李响

昨日上午，同济医院电脑系统出现故障，前来看病的患者们苦等了一个多小时才能正常看病。有患者质疑，离开电脑就不能看病了吗？为什么不能建立应急预案？

突发：医院停电患者干等近2小时

独家：宁夏银行7月发生数据库故障 业务中断37小时

2014年08月04日 09:12 新浪财经 我有话说(133人参与) 收藏本文

新浪财经讯 8月4日消息，金融数据，钱事关天，国内金融业信息安全有待加强。新浪财经独家获悉，宁夏银行2014年7月1日下午15时37分至7月3日5时40分核心系统数据库出现故障，导致存取款、网银、ATM等业务全部中断长达37小时，期间只能依靠手工办理业务。

资料显示，宁夏银行是宁夏唯一一家股份制商业银行，宁夏财政厅持股18.5%，为第一大股东。截至2013年末，宁夏银行资产总额797亿元，各项存款余额658亿元，贷款余额426亿元，2013年净利润13.3亿，同比增16%，资本充足率14.23%。

银监会银行二部(主要监管全国股份制银行和城商行)(2014)187号文下发全国，通报了宁夏银行的数据库故障事件。

据悉2014年7月1日，宁夏银行核心系统数据库出现故障，导致该行(含异地分支机构)存取款、转账支付、借记卡、网上银行、ATM和POS业务全部中断。

经初步分析，在季末结算业务量较大的情况下，因备份系统异常导致备份存储磁盘读写处理严重延时，备份与主存储数据不一致，在采取中断数据备份录像操作后，造成生产数据库损坏并宕机。

因宁夏银行应急恢复处置机制严重缺失，导致系统恢复工作进展缓慢，业务系统中断长达37小时40分钟，其间完全依靠手工办理。

A-18 符合性

- A-18 符合性
  - A-18-1 符合法律和合同的要求
  - A-18-2 信息安全评审

- A-18-1-1 识别使用的法律和合同的要求
  - 对每个信息系统和组织而言，所有相关的法令、法规和合同要求，以及为满足这些要求组织所采取的方法，应加以明确的定义，形成文件并保持更新。
- A-18-1-2 知识产权（IPR）
  - 应实施适当的规程，以确保在使用具有知识产权的材料和具有所有权的软件产品时，符合法律、法规和合同要求。
- A-18-1-3 文档化信息的保护
  - 按照法律，法规，合同和业务需求保护文档化信息，以免遭受损失，破坏，篡改，未经授权的访问和擅自发布。

A-18 符合性

- A-18 符合性
  - A-18-1 符合法律和合同的要求
  - A-18-2 信息安全评审

- A-18-1-4 隐私和个人信息的保护
  - 应按照相关的法律、法规和合同条款的要求，确保隐私和个人信息的保护。
- A-18-1-5 密码控制措施的监管
  - 使用密码控制措施应遵从相关的协议、法律和法规。

A-18 符合性

- A-18 符合性
  - A-18-1 符合法律和合同的要求
  - A-18-2 信息安全评审

- A-18-2-1 信息安全的独立审查
  - 组织管理信息安全的方法以及实施（例如信息安全的控制目标、控制措施、策略、过程和规程）应按照计划的时间间隔进行独立评审，当安全实施发生重大变化时，也要进行独立评审。
- A-18-2-2 符合安全政策和标准
  - 管理者应定期审查其职责范围内的信息处理和规程被正确的执行，以确保符合安全策略、标准和其他安全要求。
- A-18-2-3 技术符合性检查
  - 信息系统应被定期检查是否符合组织信息安全策略和标准。

Thank you

信息安全管理先锋论坛

师鑫
微信：baggio_xin
QQ: 20256150

特别鸣谢

北宙咨询 North Universe

Trendsetting Consulting

艾拓咨询 AituoXianfeng Consulting

特别鸣谢

ITIL 先锋论坛