

<<云计算安全>>

图书基本信息

书名：<<云计算安全>>

13位ISBN编号：9787111401391

10位ISBN编号：7111401395

出版时间：2012-12-15

出版时间：机械工业出版社

作者：Vic (J.R.) Winkler

页数：237

译者：刘戈舟,杨泽明,许俊峰,袁春阳

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<云计算安全>>

内容概要

本书从架构到运营（所有环节），从战略到标准，从部署方式（公共云、私有云、社区云、混合云）到服务模式（SaaS、PaaS、IaaS），本书全方位地阐述了构建安全的云计算和云服务的方法与最佳实践，为各种常见的云计算问题提供了解决方案。

全书一共10章：第1章介绍了云计算的一些核心概念和云安全的基础知识；第2章讲解了云计算的架构、部署方式、服务模式和现实世界的云应用场景；第3章讨论了云计算应该考虑的安全问题、法律风险和监管，以及风险评估方法；第4章重点讲解了在设计云计算架构时应该考虑的安全问题；第5章讲解了如何保证云数据的安全；第6章讲解了云计算安全防护的关键战略和最佳实践；第7章和第8章介绍了构建私有云和选择外部云服务提供商的安全标准；第9章讲解了云安全评估的方法和工具；第10章主要探讨了在运营过程中应该注意的安全问题及其解决方案。

<<云计算安全>>

作者简介

Vic (J.R.) Winkler 世界公认的信息安全和网络安全专家，在该领域有30余年的工作经验，曾经以网络安全访问专家的身份为马来西亚政府制定了信息安全策略。

他曾在多家企业从事与安全相关的工作，现担任Booz

Allen

Hamilton公司的高级经理，为客户提供技术咨询，曾经是Sun公司公共云部门的首席安全技术官，同时还是Sun安全技术大使计划（售前安全工程师）的负责人。

他曾经在Planning

Research Corporation公司担任研发部首席研究员，是可信B1 UNIX

OS系统的首席设计师和项目经理，为该公司搭建了早期的网络/主机入侵检测系统。

<<云计算安全>>

书籍目录

- 推存序
- 译者序
- 译者简介
- 作者简介
- 前言第1章云计算和安全概述
- 1.1理解云计算
- 1.1.1云的规模、模式以及运营效率
- 1.1.2协同技巧
- 1.1.3弹性、变形和安全
- 1.2云的IT基础
- 1.2.1云计算作为云服务的基础
- 1.2.2云计算特性
- 1.3底线
- 1.4历史观点：云计算的起源
- 1.4.1分散与扩散
- 1.4.2网络、Internet及Web
- 1.4.3虚拟化
- 1.5安全简明读本：从5万英尺的高度
- 1.5.1术语和原则
- 1.5.2风险管理
- 1.5.3安全必须成为业务的推动力
- 1.6架构简明读本
- 1.6.1系统工程
- 1.6.2IT架构
- 1.7安全架构：简明讨论
- 1.8云推动广泛的变革
- 1.8.1现今的云工程
- 1.8.2有效关注
- 1.9总结
- 第2章云计算架构
- 2.1云参考架构
- 2.1.1重温基本特性
- 2.1.2云服务模式
- 2.1.3云部署模式
- 2.2云模式的安全控制
- 2.3了解云部署
- 2.3.1公共云
- 2.3.2私有云
- 2.3.3社区云
- 2.3.4混合云
- 2.4了解服务模式
- 2.4.1云软件即服务
- 2.4.2云平台即服务
- 2.4.3云基础设施即服务
- 2.5云是怎样构成的以及主要示例

<<云计算安全>>

- 2.5.1使用虚拟化构成云
- 2.5.2使用应用程序或服务构成云
- 2.6真实世界的云应用场景
 - 2.6.1虚拟化构成的云
 - 2.6.2应用程序/服务构成的云
 - 2.6.3混合云模式
- 2.7总结
- 第3章安全顾虑、风险问题以及法律方面
 - 3.1云计算：安全顾虑
 - 3.1.1近距离观察：虚拟化
 - 3.1.2近距离观察：服务开通
 - 3.1.3近距离观察：云存储
 - 3.1.4近距离观察：云运营、安全与网络
 - 3.2评估你的云计算风险承受能力
 - 3.2.1评估风险
 - 3.2.2信息资产与风险
 - 3.2.3隐私与保密性顾虑
 - 3.2.4数据所有权与场所顾虑
 - 3.2.5审计与取证
 - 3.2.6新兴的威胁
 - 3.2.7这样就安全了吗
 - 3.3法律和监管问题
 - 3.3.1第三方
 - 3.3.2数据隐私
 - 3.3.3诉讼
 - 3.4总结
- 第4章云安全防护：架构
 - 4.1架构的安全需求
 - 4.1.1物理安全
 - 4.1.2云安全标准和策略
 - 4.1.3云安全需求
 - 4.2安全模式和架构元素
 - 4.2.1纵深防御
 - 4.2.2蜜罐
 - 4.2.3沙盒
 - 4.2.4网络模式
 - 4.2.5配置管理数据库的重要性
 - 4.2.6线缆模式
 - 4.2.7弹性与优雅
 - 4.2.8为变化做规划
 - 4.3云安全架构
 - 4.3.1云成熟度以及它与安全的相关性
 - 4.3.2Jericho论坛
 - 4.3.3代表性的商业云架构
 - 4.3.4代表性的云安全架构
 - 4.4规划安全运营的关键战略
 - 4.4.1将数据和系统分类

<<云计算安全>>

4.4.2定义云人员及客户的有效角色

4.5总结

第5章云安全防护：数据安全

5.1云计算数据安全综述

5.1.1数据控制与公共云经济

5.1.2机构责任：所有权与保管权

5.1.3静态数据

5.1.4动态数据

5.1.5云数据安全的常见风险

5.2数据加密：应用及限制

5.2.1密码技术综述

5.2.2数据加密的常见失误或错误

5.3云数据安全：敏感数据分类

5.3.1认证及身份

5.3.2访问控制技术

5.3.3数据分类以及数据标签的使用

5.3.4静态数据的加密应用

5.3.5动态数据的加密应用

5.3.6在云中加密技术的障碍

5.3.7数据删除

5.3.8数据屏蔽

5.4云数据存储

5.5云锁定

5.5.1元数据

5.5.2避免云锁定

5.6总结

第6章云安全防护：关键战略及最佳实践

6.1总战略：有效管理风险

6.2安全控制综述

6.2.1云安全控制必须符合你的需要

6.2.2美国标准与技术研究所对安全控制的定义

6.2.3非机密模式

6.2.4机密模式

6.2.5云安全联盟的方法

6.3安全控制的限制

6.3.1安全性暴露会随时间而变化

6.3.2漏洞攻击是不会光明正大进行的

6.4最佳实践

6.4.1云计算最佳实践：基本原理

6.4.2云社区的最佳实践

6.4.3云计算的其他最佳实践：云服务客户

6.4.4云计算的其他最佳实践：云服务提供商

6.5安全监测

6.5.1安全监测的目的

6.5.2转换事件流

6.5.3安全监测的保密性、完整性及可用性的需求

6.5.4MaaS的机遇

<<云计算安全>>

6.6总结

第7章安全标准：构建内部云

7.1私有云：动机和综述

7.1.1安全启示：共享资源与专用资源

7.1.2实现成本节约的考虑

7.1.3私有云：城堡要塞

7.1.4支持架构决定的分析

7.2确保私有云的安全标准

7.2.1网络考虑

7.2.2数据中心考虑

7.2.3运营安全考虑

7.2.4监管

7.3总结

第8章安全标准：选择外部云提供商

8.1选择云服务提供商：保证综述

8.1.1提供商的声明与独立验证

8.1.2选择云服务提供商：提供商的透明度

8.2选择CSP：风险综述

8.2.1风险会因客户和CSP而改变

8.2.2评估风险因素

8.3选择CSP：安全标准

8.3.1安全标准：重温纵深防御

8.3.2安全标准：其他考虑

8.3.3其他安全相关标准

8.4总结

第9章评估云安全：信息安全框架

9.1评估云安全

9.2评估云安全的清单

9.2.1基础安全

9.2.2业务考虑

9.2.3纵深防御

9.2.4运营安全

9.3清单指标

9.4总结

第10章云运营

10.1从架构到有效安全的运营

10.1.1规划的范围

10.1.2物理访问、安全以及持续成本

10.1.3逻辑和虚拟访问

10.1.4人员安全

10.1.5从物理环境到逻辑

10.1.6引导安全运营

10.1.7程序及流程随时间完善

10.1.8效率和成本

10.2安全运营活动

10.2.1服务器构建

10.2.2业务持续、备份与恢复

<<云计算安全>>

- 10.2.3运营环境中的变更管理
- 10.2.4信息安全管理
- 10.2.5漏洞和渗透测试
- 10.2.6安全监测与响应
- 10.2.7最佳实践
- 10.2.8运营弹性
- 10.3总结

章节摘录

版权页：插图：将安全控制与认知风险类别联合起来的另一种方法来自国家安全信息领域。第5章在关于数据标签以及如何处理分类方面，我们提出了使用这样的信息分类方法（非机密、机密、秘密、绝密、隔离）。

但这里的安全控制一般是与在信息系统内保护此类数据相关联的。

这个领域的安全要求和技术控制的细节大多是保密的，还有几个安全控制截然不同。

正如第5章讨论的，信息分类的实施是通过添加新的结构和机制获得的，操作系统使用这些结构和机制添加标签以及执行隔离。

从某种意义上说，这模仿了由机构实施的、用以处理文件或其他物理信息表示的严格策略和文档控制。

一种形象化描述这些控制如何运行的方法是：它像单个容器那样，根据信息的最高等级贴上标签，信息都位于这些容器中。

虽然单个元素或文件可以标记以介质访问控制（Media Access Control, MAC）样式的标签，但随着单个文件添加到容器（例如，一个目录）中，容器将浮动到高级别的标签以反映整体容器机密水平的提升。

聪明的读者会好奇信息如何才会降级：只有具有特殊权限的用户可以实施降级操作，通常都是例外情况。

在非常严格的安全策略执行中如何实施有用的工作，虽然在这方面涌现出许多很棘手的情况，但实际上这种多等级的可以胜任的系统能够通过单一实施取代多个单独的系统。

多等级系统在策略执行能力范围方面更加复杂和先进，但是对于一般用户而言比较难以理解。

如果用户界面以及用户工具允许更加简单的操作，这种技术的应用会更加广泛。

有时会在机密世界中使用另一组安全控制，它是与“创建者控制”数据的概念相关的。

例如，原始发件人将一封电子邮件发送给一组可信任的收件人，然而原始发件人可能希望控制再将这些邮件发送给其他潜在收件人的行为。

这是难以实施的，但可以为那些想要系统执行关于信息限制的人提供重要的手段。

对于国家安全数据的强调是基于严格程度的，这种严格程度要求根据不同数据的机密水平进行分隔，使得只有经放行和授权的个体才能对这种数据进行访问。

商业领域也要迅速行动，采用相似的严格方法，从而在所需之处维护数据的保密性。

6.2.5云安全联盟的方法 云安全联盟开发了控制矩阵，它是由近100个不同的控制指标组成的框架。

云安全联盟控制矩阵强调业务的信息安全控制，其形式是提供框架结构以及符合云行业需求的信息安全具体内容。

云安全联盟控制矩阵的范围和控制情况如图6.4所示。

云安全联盟控制矩阵的工作还很新（版本1.0在2010年4月发布），我们可以预期这项工作随着时间推移还会发展。

这是个好的开始，它将作为本书在第9章中构建的模型之一。

<<云计算安全>>

编辑推荐

《云计算安全:架构、战略、标准与运营》是一本系统、全面、务实的云计算安全指南，从架构到运营（所有环节），从战略到标准，从部署方式（公共云、私有云、社区云、混合云）到服务模式（saas、paas、iaas），《云计算安全:架构、战略、标准与运营》全方位地阐述了构建安全的云计算和云服务的方法与最佳实践，为各种常见的云计算问题提供了解决方案。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>