R1. 问责制和所有权

简介：

对于一个组织来说，传统的数据中心是完全可控的。这个组织可以在逻辑上和物理上保护他们所拥有的数据。一个组织如果选择去使用一个公开的云来托管业务服务，这样会失去对他们自己数据的控制权。这会造成严重的安全威胁，该组织需要认真考虑并解决它。（Pankaj，维奈）

内容：

对于一个组织来说，传统的数据中心是完全被这个组织控制的，这个组织可以在逻辑和物理上保护他们的数据。组织可以选择一个的云提供商来托管他们的业务，但他们这样会失去对自己数据的控制。这可能会造成严重的安全威胁，所以组织需要认真考虑并作出恰当的决策。

威胁的严重程度是由存储在云端的数据的重要性决定的，例如 BLOG、微博、公共新闻以及新闻组信息这些公开的信息就是不敏感的的数据，所以在云中托管这些数据的风险是很低的。相反，像个人健康记录、犯罪记录、信用记录和工资信息是高度敏感的业务数据，如果这些数据被泄露，会导致很严重的商业和法律后果，因此在云中托管这些数据会有非常高的风险。

由于云中的数据由云提供商控制，所以首要的问题是确保存储数据的保密性，加密技术可以被用来确保保密性，如果云提供商使用多租户架构，应当为云中的每个用户提供单独的加密密钥。

云提供商可能会把用户的数据存放在不同的国家，这也会带来一些风险，因为每个国家都会有它自己的法律体系，云提供商运营的业务都要遵循它所在地区的法律体系，某些国家的法律也许会强制云提供商向司法人员提供某些数据和密钥。数据的存放位置也会增加额外的经济成本，如销售订单需要缴纳税点，而且可能无法获得这个国家提供的最低税率的优惠，因为云提供商可能把数据存放在任何国家和地区。

云提供商可能把用户的数据存放在他们的办公场所，或者租用一个基础设施（IAAS）作为提供数据存储的地方。提供商可能采用多租户架构，在一个物理存储中存放许多的云用户数据。这种架构可能缺少必要的控制，以确保云的用户只能访问属于自己的数据，而不会访问到其他用户的数据。如果云用户之间在商业上有竞争关系，那么缺乏这种控制会给用户带来严重的商业风险。

当一个请求要删除一些数据的时候，云提供商可能只是名义上把它删除，并留下可以用来重建原始数据的痕迹。这些数据可能被偷走、并且被滥用，给云中的用户造成严重威胁。

对策：

为了降低各种数据的相关风险，使用云计算来开展服务的组织应当做到以下几点：

1. 明确云提供商是如何确保数据安全，以及是如何去检测和报告一个威胁。
2. 明确数据存储的地理位置，以及确保提供商不会把数据存储在一个受相关限制的国家中。
3. 明确第三方机构或当地政府在什么情况下可以从云提供商处抓取或没收数据，当出现此类事件时提供商应及时提前通知用户。

4. 确保云提供商能基于用户制定的数据分类对数据做适当的保护， 并解决诸如 HIPPA 隐私法的相关问题。

5. 默认情况下提供商拒绝所有对用户数据的访问，用户组织可以给需要访问的对象给予指定和明确的授权。

6. 云提供商要对静态和传输过程中的数据进行加密。

7. 提供商对不同用户的数据进行逻辑上隔离，从而预防任何未经授权的访问、修改或删除数据。

8. 明确云提供商是如何管理不同用户的密钥。提供商应当为每个用户使用一个加密密钥，而不是对所有用户使用相同密钥。

9. 核实云提供商对删除的数据已经进行了彻底的销毁，不能再通过任何方式恢复出来。

10. 如果数据被破坏，确保云提供商承担赔偿。

案例：

2009 年 7 月 15 日，Twitter 透露一个黑客通过劫持 Twitter 员工的邮件账户获取了存储在 Google Apps 上的大量公司数据。尽管这次破坏是由于弱口令和密码重置造成的，不过这一事件已引起新的有关云计算安全和隐私问题更广泛的关注。

参考：

无

R2. 用户身份统一

简介：

当企业需要转移服务和应用到不同云服务提供商时，他们保持对自己的用户身份控制是非常重要的，而不是让云服务提供商创建多个不同的身份，这会导致管理变的越来越复杂。用户应当具有一个可在不同的云服务提供商间通用的唯一的身份验证（如 SAML），这样用户即可不需要管理众多账号和证书，很好的提高了用户的使用体验。这使得后端数据在不同云提供商之间的整合变得更加容易。（维奈，Pankaj）

内容：

无

对策：

无

案例：

无

参考：

无

R3. 合规性

简介：

复杂的合规性说明。数据在一个国家可能被认为是安全的，在另一个国家可能被认为是不安全的，这是因为不同的国家或地区的监管法律是不同的。举例来说，欧盟有非常严格的隐私法，因此存放在美国的数据可能不符合欧盟的法律条款。（尚卡尔，奥雅纳）

内容：

用户最终为了安全和遵从监管法规，把他们自己的应用托管在云中。数据服务和应用所有者必须及时到位的提出审计计划，确保用户对托管在云提供商处的应用和基础设施有适当的控制权。不少公司在计划采用云技术（如 SaaS，Iaas，Paas 等），必须确保他们的云提供商了解各自的角色和职责（RACI 等），从而帮助用户遵从适当的监管法规和标准（政府和商业）。IT 经理可能会害怕把数据给云提供商而失去对数据的控制，因为缺少透明的机制运提供商可能为了符合监管法规而在用户不同意的的情况下改变他们的底层技术和实现。IT 组织应当分析是否应该将风险管理框架包括数据保护和合规性要求应用到云中，并确认通过数据保护，可用性和密钥管理等方式更好的界定服务水平协议的可行性。

对策：

无

案例：

无

参考：

[1].Anthes, G（2009 年 1 月），saas 的现实，计算机世界 43(1), 21-22.，摘自 2009 年 8 月 9 日，ABI/ INFORM Global.(文件编号：1626575741)。

[2].Business：Pain in the aaS；计算机安全（2008 年 4 月），经济学家，387（8577），86。 取自 2009 年 8 月 9 日，ABI 公司/ INFORM Global.。 .(文件编号：1469385981)

[3].Gartner: 七大云计算安全风险：
http://www.cio.com/article/423713/Gartner_Seven_Cloud_Computing_Security_Risks?page=1&taxonomyId=1419

[4].Google：云计算比传统 IT 技术更安全：http://www.computerweekly.com/Articles/2009/07/21/236982/cloud-computing-more-secure-than-traditional-it-says.htm

[5].云计算安全问题 TOP5：http://www.computerweekly.com/Articles/2009/04/24/235782/top-five-cloud-computing-security-issues.htm

[6].云安全联盟：http://www.cloudsecurityalliance.org/csaguide.pdf

[7].奥沙利文, D. (2009) 互联网云的一线希望 英国行政管理杂志。

[8].Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009).云中的数据控制：外包数据而非外包控制，论文发表在 2009 年 CCSW：云计算安全， 2009 年美国芝加哥，伊利诺伊州，ACM 研讨会论文集

[9].Getgen, K. (2009, October) 2009 加密和密钥管理的行业标准的报告，Trust Catalyst 白皮书 数据保护中的风险管理.

R4. 业务持续性和灵活性

简介：

业务持续性是用来确保 IT 组织的业务在遇到灾难的情况下可以正常运行的活动。当一个组织使用了云服务之后，维护业务持续性的职责便要授权给云服务提供商。这有可能会让组织产生一个失去业务持续性控制的风险。(Pankaj，尚卡尔)。关于服务的持续性和服务质量（QoS），首先要确保有关的云计算拟议的合同解决方案，以及服务等级协议。（卢多维奇）

内容：

维护业务的持续性是一个公司或组织必须具备的操作预案，以确保一些关键的业务功能对客户、提供商、监管机构和其他必须能够访问这些功能的实体是可用的。这些活动包括许多常规操作如项目管理、系统备份、控制更改和帮助台(helpdesk)。灵活性是系统必须具备的一个特征，这使系统本身能够适应自然或人为事件所造成的灾难性故障后果。

在非云端环境下，保证业务的连续性是公司或者组织的职责。公司或者组织理应制定计划，执行业务连续性。因为公司或组织拥有完备的 IT 基础设施，它有能力和资源开发有效的业务连续性计划。

在使用云的情况下，企业维护业务持续性的责任必须授权下放给云提供商。组织失去了制定和执行业务连续性计划的控制权。因此在万一出现灾难的情况下，在大的灾难发生时没有足够能力保证业务连续性的公司或组织可能会出现危险。

对策：

为了减轻这种风险，公司或组织在使用云的时候，应该遵循下面几点：

1. 确保完全理解客户恢复时间目标(Recovery Time Objectives :RTOs)被云提供商理解并将其明确的写到合同关系中。
2. 确认云提供商已经实施了由其董事会董事核准的业务连续性性策略。
3. 检查一下云提供商是否已经具备有效的管理支持和对业务连续性定期的审查程序。
4. 确认一下云提供商的业务连续性程序是否已经经过认证并且/或者能够符合国际公认的标准比如 BS25999.

然而，除了考虑以上的危险以外，如果一个公司或者组织自身就缺乏因为连续性的策略，那么如果使用了具备良好业务连续性策略的云提供商提供的服务的话，该组织将从云的使用中受益。

案例：

windows Azure，微软的云计算平台，在 2009 年 3 月的曾经中断服务一个周末。如果你的公司使用了该服务，那么这次中断服务对你的公司的运营造成什么影响？微软有职责去解决这个问题，而不是你们公司的 IT 团队。

参考：

无

R5. 用户隐私与数据的第二用途

简介：

用户个人数据从使用社交网站开始就已经存储在云端了。大多数的社交网站对于如何处理用户的个人数据都是模糊不清的。此外，大多数的社交网站采用默认共享所有（或者很少的限制）的策略来建立用户。例如通过 LinkedIn、twitter、Facebook 等是非常容易推断个人的详细信息的。（维奈）

你需要确定你的数据是否能够被云服务提供商用于其他目的。包括能够直接从提供商获得的用户数据和间接基于用户行为分析出来的数据（点击次数，链入链出的网址等）。许多社交应用提供商挖掘用户的数据来进行二次使用，比如做针对性的广告等。因此，当我们使用 Gmail、hotmail 或 yahoo 把我们的假期计划告诉给朋友时，就马上会看到靠近我们目的地的旅店或者航班的广告也就不用奇怪了。（维奈，奥雅纳）

内容：

隐私是本地的，可是数据流向的云端确实全球的。现在个人和规章都希望和要求他们本地的预期值能够在共享/全球的云上汇合。

什么是隐私数据？

能够唯一标识一个人和他/她的行为和活动的数据。不同的国家和地区有着不同的隐私条例。

Google 和其他社交网站收集隐私数据并利用它。

它会导致什么损失？

用户根本不知道这一切是怎么发生的

谷歌的隐私策略。

数据不再存放在企业的物理意义上的场所内，因此也就不再会有有效的网络边界控制。这种转变表明我们需要云服务提供商(CSP)提供数据中心的安全模型和扩展的可信边界的必要性。另外，隐私和管理的服从要求 CSP 扩展和驱动更强的内部安全控制比如萨班斯法案，支付卡行业以及健康保险流通与责任法案。随着网络空间和使用社交媒体的合作的指数级增长，安全讨论方面的焦点集中在隐私关注方面。然而企业的领导希望在不改变风险偏好的情况下，能够享受到云计算带来的好处。企业的领导必须权衡自我拥有的低成本和改善的功能，即时的市场优势和对隐私和数据的保护需求。本文会提供当企业采用了云计算之后，如何管理安全和隐私风险的信息和方法。在云计算中，一个最大的挑战是最小化企业的风险。第一步是评估和审视云基础设施中数据管理的隐私需求。 CSP 的隐私评估需要考虑安全控制是否存在，包括物理存储和数据跨云的分发。工作于不同的安全方案，作者们必须设计一个使用“隐私安全矩阵”的评估方法。这个矩阵映射 PII 数据元素到对应的区域做安全控制。将 CSPs 的安全和隐私需求以及协议转换为 SLAs，并督促提供商对其进行实现。同样，企业可能需要更新隐私策略，与用户社区进行沟通（公司的律师和 HR 可能并不喜欢这么做）。最后，对正在进行的风险管理和顺从，云提供商扩展一个有效的监控和可审计的程序是非常必要的。程序流程应该有明确和可的量化的标准，保证隐私和安全程序的有效性。总的来说，作者在评估 CSPs 的安全隐私风险以及他们开发的方法中的亲身体会是它会帮助潜在的和正在使用云计算的用户，当使用云的时候，学会如何有效的管理安全和隐私风险。

对策：

无

案例：

无

参考：

[1] . http://www.privacyconference2007.gc.ca/workbooks/pres_infosession1_01_abrams_e.pdf

R6. 服务和数据传输安全

简介：

组织必须确保它们的私有数据在终端用户和云数据中心之间进行传输的过程中是得到充分的保护的。所有的组织都应当考虑数据在传输过程中被截取的问题，因为当数据通过互联网上传输时，组织利用云计算模式存在更大的风险。在传输过程中，不安全的数据是容易遭到窃听和篡改的。（尚卡尔，奥雅纳）

内容：

Gartner 公司发布了大量的关于云服务中间商即所谓的云服务经纪人(cloud services brokerages)的研究。这项研究提高和丰富了云服务的性能并对云能够被正式通过有一定帮助。

云服务提商必须向正在计划采用云服务的消费者保证他们的私有数据数据是收到充分的保护的。就像终端用户和云数据中心通过 internet 进行数据传输。云计算模型增加了数据在传输过程中被窃听的风险，尽管这种风险并不仅仅局限于云。云提供商必须使用 SSL 和/或更加严格的加密协议来保证数据在传输过程中的安全。日益复杂的集成度和云计算中的动态数据是及时诊断和解决事故——比如通过恶意软件的检测和及时的入侵响应来缓解影响——的重要挑战。

对策

无

案例

无

参考

[1].Babcock, C. (2009 年 9 月). Hybrid Clouds. InformationWeek,(1240), 15-19. 取自 2009 年 12 月 20 号, from ABI/INFORM Global.（文件编号：1865633581）.

[2].Byrne, T. (2009, April). Clouding Over. EContent, 32(3), 37. Retrieved December 20, 2009, from ABI/INFORM Global. (Document ID: 1675328451). de Assuncao, M. D., di Costanzo, A., & Buyya, R. (2009). Evaluating the cost-benefit of using cloud computing to extend the capacity of clusters. Paper presented at the HPDC '09: Proceedings of the 18th ACM International Symposium on High Performance Distributed Computing, Garching, Germany. 141-150.

[3].Hoover, J. (2009, April). 通用电气公司提出向云模型试验，信息周刊，（1226），32-33。取自 2009 年 12 月 20 号，来自 ABI/INFORM Global。（文件编号：1682898981）。

[4].Gupta, R., Prasad, K. H., Luan, L., Rosu, D., & Ward, C. (2009). Multi-dimensional knowledge integration for efficient incident management in a services cloud。发表在 SCC'09(2009 年 IEEE 国际服务计算会议论文集)的论文， 57-64。

[5].Christodorescu, M., Sailer, R., Schales, D. L., Sgandurra, D., & Zamboni, D. (2009). 云安全不（仅仅）虚拟化安全：一个发表在(CCSW'09) 美国伊利诺伊州芝加哥 2009 年 ACM 云计算安全研讨会论文集中简短的论文。

R7. 多租户和物理安全

简介：

多重租赁的云服务意味着在多个客户端之间共享资源和服务（CPU 资源、网络带宽、空间容量、数据库、应用程序池）。它需要加入对逻辑的隔离和其它控制等可靠的功能来确保一个用户不能有意或无意地妨碍其他用户保密性、整体性、可用性等方面的安全。（维奈，Pankaj）

内容：

云中多租户指共享资源和服务来运行软件，来服务大量用户和组织(租户)。它指物理资源(如计算、网络、存储)和服务共享，而且管理功能和支持和可以共享。对云提供商来说，在多用户中共享和重新使用资源来降低成本是一个大的利益驱动。

在一个多用户的环境中，更多的安全取决于逻辑的(在应用层面上)而不是资源的物理隔离，一些云供应为了多个用户，可能不允许某个特别的用户在共享的结构中审计和评估。

1、 不适当的逻辑安全控制：物理资源(CPU、网络、存储/数据库、应用栈)在多用户中共享，也就是说依赖逻辑的隔离和其他控制来保证某个用户无法妨碍其他用户的安全(保密性、完整性、可用性)。

2 恶意的或者无知的用户：如果供应者(如软件)在多用户中存在比较弱的不合理的控制，那么某个恶意的或者无知的用户可能降低其他用户的安全性。

2、 共享资源可能成为故障点：如果供应者没有很好地构建共用服务，这样由于 某个用户错误或者滥用共有服务，很容易成为单一故障点；

3、 不协调的变更控制和错误配置，当多用户正在共享底层结构时，所有的变更均需要协调和测试；

4、 混合用户数据：为了减少成本，提供者可能把多个用户的数据存储在相同的数据库单元和备份单元。尤其是如果用户数据存储在共享的媒介里(如数据库、备份空间、案卷保管处)，一旦数据毁坏，多用户均面临挑战；

5、 性能风险：某个用户对服务大量应用，会影响其他用户应用该服务的质量；

6、 Xaas 特殊风险：

1 Saas(software-as-a-service):多个客户端(租户)可能共享一个应用软件栈(数据库、app/web 服务器、网络)。那意味着多用户的数据可能存储在同一个数据库，可能一起备份和一起存档，可能移向共同的网络设备(未加密的)，而且被共同的程序处理。这就更加强调了在应用软件之间的逻辑安全构建，来分离本用户和其他用户。

2 Paas(Platform-as-a-service): 多个用户共享平台栈。攻击平台栈可能会导致用户之间共享数据备份和存档的质量问题；

3 Iaas(Infrastructur-as-a-service)：交叉虚拟机器的攻击，交叉网络通信的监听。这会发生经常处于低安全性状态的设备，这会发生经常在不被关心它们主机的硬件和系统补丁的低安全性状态的设备上面。特别是当这些主机被攻击和控制时，会存在这种风险。

对策：

1、 对多用户进行构建：提供者需要提供多用户的架构，而不是单纯使用那些不是为多租户设计的服务。多用户的构建应该考虑合理的划分，加强通用的服务和故障单点，同时给消费者(用户)提供更多的透明度。

2、 数据加密：对数据进行加密以及对各个用户的数据进行隔离。要求用户的密钥管理对数据进行加密、在一个虚拟的环境中这意味着每个用户的密钥管理在每台虚拟机进行加密，而不是提供者进行加密。

3、 变更控制管理：需要对所有的变更(尤其是通用共享的服务变更)进行很好的计划，快速释放使用资源使用户进入新的基础设施。对于 SaaS 提供商(或者 SaaS 模式)来说，用户需要日益的想新的基础设施融合，(对这些行为，提供者需要计划额外的资源)提供者需要有多用户到基层资源和服务的映射表，以至于基层资源的任何变更均被很好的计划。

4、 透明性/管理审计：用户需要知道管理者有权访问它们的资源/服务。其中之一的办法就是允许具有审计能力的管理者访问栈的各个层(操作系统、网络、应用软件、数据库)，这些层是可以被用户审计的。提供者可能仍在管理，但是在很严格的可审计环境中进行管理；

5、 虚拟个人云(VPC):它是私人云存在于一个公共的或者共享的云中。一个 VPC 是把一公共云分割成孤立的虚拟基础设施和链接方法，通过加密的网络链接来回到多用户的内在资源。

6、 第三方评估：可以轮流评估或契约，如果每个消费者由于安全考虑而要求审计，但提供者有不允许时除外。

7、 隔离用户：用户能一直想云提供商协商或要求拥有它们自己的隔离物理基础设施，数据库、存储、网络，……在安全领域，隔离起来重要作用，但是他确实增加了用户/客户的成本。

案例：

2010 年 6 月 WordPress 平台 大面积不能访问，覆盖高端的博客站点(例如 CNN Techcrunch)的 WordPress 系统，3 个数据中心(1300 个服务器，千万博客)发生了损坏，这仅仅是由于程序员修改了配置(数据库)，这对云博客服务的大量用户造成了冲击。

参考：

[1]. http://chucksblog.emc.com/chucks_blog/2010/01/thoughts-on-secure-multitenancy.html

[2]. http://aws.amazon.com/vpc/

[3]. http://www.elasticvapor.com/2008/05/virtual-private-cloud-vpc.html

[4]. http://blogs.gartner.com/thomas_bittman/2009/01/08/virtual-cloud-privacy-is-gray/

[5]. http://people.csail.mit.edu/tromer/papers/cloudsec.pdf

[6]. http://www.cloudsecurityalliance.org/csaguide.pdf

[7]. http://smoothspan.wordpress.com/2010/06/11/wordpress-and-the-dark-side-of-multitenancy/

[8]. http://techcrunch.com/2010/06/10/wordpress-gives-us-the-vip-treatment-goes-down-on-us-again/

[9]. http://hakre.wordpress.com/2010/06/14/wordpress-outage-feedback/

[10]. http://en.blog.wordpress.com/2010/06/14/downtime/

[11]. http://www.enterpriseirregulars.com/14980/security-risks-of-multi-tenancy/

[12]. http://salesforcechannel.com/video/Multitenant-Magic-Under-the-Cov

[13]. http://natishalom.typepad.com/nati_shaloms_blog/2010/03/multitenancy-does-it-have-to-be-that-hard.html

R8. 影响范围分析和法律支持

简介：

发生信息安全事件时，在同一个云提供商上部署的应用程序和托管服务可能难以追查记录，因为日志记录可能分散到多台主机和数据中心，这些不同的主机和数据中心可能位于不同的国家，因此受不同的法律管制着。 此外，由于属于多个客户的日志文件和数据可能共同位于相同的硬件和存储设备，因此，需要加强对执法部门和取证恢复技术的关注。(尚卡尔，奥雅纳)

内容：

无

对策：

无

案例：

无

参考：

无

R9. 基础设施安全

简介：

发生信息安全事件时，在同一个云提供商上部署的应用程序和托管服务可能难以追查记录，因为日志记录可能分散到多台主机和数据中心，这些不同的主机和数据中心可能位于不同的国家，因此受不同的法律管制着。 此外，由于属于多个客户的日志文件和数据可能共同位于相同的硬件和存储设备，因此，需要加强对执法部门和取证恢复技术的关注。(尚卡尔，奥雅纳)

内容：

虽然上述条目的细节必须被视为高度敏感的信息，但是也有理由期望客户愿意去了解高层次的细节也是情有可原的。提供商必须愿意提供这些信息。

基于应用的数据安全完全取决于构成基础设施的组件构成的应用程序平台的安全性。未能采取“最佳实践“考虑的后果可能导致的数据，名誉，或可用性损失，甚至有可能带来监管/法律的后果。

1. 系统和网络设备的默认配置。刚出厂的系统，应用或网络设备很可能运行的是软件的旧版本，并没有进行最新的安全更新。而且，标准配置，密码，漏洞等是众所周知的，这些细节在互联网上自由传播，这意味着这些系统将更容易被利用。

2. 所有的服务，甚至活跃而未使用的，都有可能包含潜在被利用的安全相关的漏洞，而恶意组织正通过互联网进行主动的扫描。这些服务的运行，即使实际上是毫无目的的，也会因此而不必要地增加组织基础设施成为漏洞利用目标的可能性。

3. 被利用的服务如果不被控制，则可能成为到别的服务的跳板。例如，如果 web 层能够直接访问数据库，那么一旦 web 服务被利用，则可能导致后台数据库也被入侵。

4. 活跃的网络协议和开放端口，即使没有在解决方案体系结构中使用，也可能被利用。

5. 管理访问可能被滥用，或者通过管理员或者通过被利用的管理帐号。此外，管理访问可能会导致意外的中断

6. 所有代码（应用程序，操作系统，网络）会包含安全相关的漏洞，配置也可能包含配置错误，这些都能够被利用。

对策：

1. 对操作系统，应用程序和配置进行加固。目的在于通过减少有漏洞的系统服务，应用程序，未使用的或不安全的默认账户等风险，来减少被入侵的风险。

2. 分层解决方案的架构。解决方案的分层架构将意味着一个直接暴露在 Internet 的系统更不可能被攻击者作为进入组织网络的跳板。“扁平“的网络——例如处理 Internet 业务的系统能够直接访问后端数据库服务器——需要重新审核。

3. 分离的基础设施组件，例如，通过使用 ACL 网络，以减少

4. 基于角色的管理者访问和受限的管理者权限。每个组织应该将对资源的管理访问权限限制在有限范围之内，并确保角色进行了明确定义。例如，如果数据库管理员，系统管理员和网络管理员都清楚界定及区分角色界限，那么通过单一角色所进行的恶意行为或者产生的意外错误，其风险就能够降低。

5. 定期脆弱性评估。每个组织都应该对其基础设施定期进行风险评估，并对其开发的代码进行脆弱性评估。凡顾客/客户/合作伙伴相关的信息，组织应该认为，其他各方也有兴趣知道他们的数据是如何受到保护的；而只有独立的第三方评估/审核机构才比较可能被信任和接受。

案例：

无

参考：

[1].Center for Internet Security (CISecurity) http://www.cisecurity.org

[2].SANS Institute - Reading Room: http://www.sans.org/reading_room/

R10. 非生产环境暴露

简介：

一个开发应用软件的 IT 组织内部采用了非生产环境来进行设计、开发和测试活动。而非生产环境一般都没有和生产环境一样程度的安全措施。如果组织为其非生产环境采用云服务，那么就会存在非授权访问、信息篡改和窃取等高风险的威胁。（潘卡序，奥雅纳）

内容：

在开发应用软件的 IT 组织的内部，采用了一系列用于设计，开发和测试活动的非生产环境。这些非生产环节，其安全程度一般都不会与生产环境相同。这是方便和促进开发和测试周期的需要。这些非生产环境不只是组织成员可以访问，外包厂商也可以访问。在非云环境中，非生产环境位于数据中心的组织内部，并组织对其具有完全所有权。因此，组织应该可以适当控制这些环境的访问。

如果组织为其非生产环境采用了云提供服务，则该组织失去了控制权。既然云是公开访问的，那么就存在的高风险就在于，未授权用户可能会访问到非生产环境。恶意用户可能会改变这些环境，使其不可用。或者更糟的是，恶意用户可能会完全删除环境。

非生产环境可能使用通用的认证证书。在非生产环境中使用的密码可能不符合该组织的标准密码策略。在这种情况下，未经授权访问变得非常容易。

组织可以通过从相应的生产环境中复制数据的方式来构建一个非生产环境。在这种情况下，未经授权用户能够窃取敏感的生产数据，例如信用卡和社会安全号码。

对策：

为了降低非生产环境的暴露风险，组织应考虑以下几点：

1. 确保访问非生产环境所使用的认证证书是健壮的，符合与生产环境相同的标准。

2. 非生产环境中所使用的数据不是生产环境的数据拷贝。

案例：

无

参考：

无