精译版

IaaS：云安全的下一篇章

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	IaaS: The Next Chapter In Cloud Security		
原文作者	Kaushik Narayan	原文发布日期	2017 年 2 月 24 日
作者简介	Kaushik Narayan 是云安全公司 Skyhigh Networks 的联合创始人和首席技术官，负责 Skyhigh 的技术愿景和软件架构。 http://www.darkreading.com/author-bio.asp?author_id=1862		
原文发布单位	Darkreading		
原文出处	http://www.darkreading.com/cloud/iaas-the-next-chapter-in-cloud-security/a/d-id/1328202?		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

IaaS：云安全的下一篇章

Kaushik Narayan

2017 年 2 月 24 日

采用 IaaS 的企业必须使用共享责任模型来更新其安全方法。

从制造业，金融服务到公共部门的各行业的公司信任云提供商，依靠他们的服务存储关键数据。SaaS（软件即服务）应用程序（如 Office 365 和 Salesforce）的快速增长就依赖于这种信任关系。但是，直到 IT 专家确信云提供商可以提供与传统软件相当或更好的安全性，SaaS 才得以广泛应用。然而，企业仍然面临着严峻的挑战；Gartner 预测 95%的云安全事件将会源于客户的错误。

现在，第二波云应用浪潮正在迅速蔓延，企业边界将会融入 IaaS（基础架构即服务）产品。要想应用 IaaS，企业必须使用共享责任模型来更新其安全方法。

更新 IaaS 的共享责任模型

青睐云的公司使用 SaaS 工具实现不同的功能：Office 365 用于协作，Workday 用于人力资源配置，Salesforce 用于客户关系管理。每个企业都为员工，客户和合作伙伴开发了内部应用程序，数量从几个到数千个不等。企业正在消除其数据中心，并将这些专有应用程序大量迁移到 IaaS 云产品中，导致 IaaS 的增长速度是 SaaS 的两倍。

即使采用主动 SaaS 安全方法的公司也必须重新评估其在 IaaS 平台上托管应用程序的能力。SaaS 和 IaaS 平台在不同的共享责任模式下运行，在云提供商和客户之间分配不同的安全能力。SaaS 提供商处理安全漏洞的责任会落在托管于 IaaS 服务上的应用程序的客户的肩膀上。

此外，企业面临快速迁移的压力，这意味着安全团队可能不会监督 IaaS 安全，开发团队没有额外的资源来更新预定迁移到云的内部应用程序的安全功能。专有应用程序没有 SaaS 应用程序那样的专有安全解决方案，也没有与安全产品集成的 API。过去，我们认为创业公司和云服务提供商负责保护 AWS，Azure 或 Google Cloud Platform 的安全。但是今天，世界 2000 强公司都面临着在云中保护应用程序的挑战。

IaaS 安全威胁来自企业内外。黑客攻击企业 IaaS 账户以窃取数据或计算资源。他们可以通过窃取凭证、获取错误的访问密钥或利用配置错误的服务设置来利用此向量。一位研究人员在 GitHub 上发现了超过 1 万个 AWS 凭证。被黑客入侵的账户可以用于挖掘比特币或勒索赎金，托管公司 Code Spaces 就是最糟糕的前车之鉴了。

在企业内部，能够访问 IaaS 账户的恶意员工可能会窃取，更改或删除该平台上的数据，造成巨大的损失。人为错误和疏忽可能会将公司数据和资源暴露给攻击者。医疗保健公司 CareSet 发生了一个配置错误，导致黑客利用其 Google Cloud Platform 账户对其他目标发起了入侵攻击。几天后，该问题仍然没得到解决，于是 Google 暂时关闭了该公司的账户。企业不能想当然地认为 IaaS 环境是安全的。在上述案例中，云提供商都无力处理客户的漏洞。

IaaS 安全行动计划

要想保护 IaaS 平台上的专有应用程序中的数据，我们需要比 SaaS 安全措施更进一步：保护计算环境本身。保护 AWS，Google Cloud Platform，Microsoft Azure 或其他 IaaS 平台首先要进行配置审查。以下是保护 IaaS 平台的四个至关重要的措施：

1. **多因素身份验证：**对于存储着敏感企业信息的任何应用程序（特别是暴露于互联网的云应用程序）来说，多因素身份验证是一个必要的措施。公司应为 root 账户和身份和访问管理用户启用多因素身份验证，以降低账户泄露的风险。这种身份验证可能需要用户在提交操作（例如删除 S3 存储桶）之前进行其他登录步骤。

2. **检查无限制访问：**不必要地暴露 AWS 环境会增加各种攻击威胁，包括拒绝服务、中间人攻击、SQL 注入和数据窃取。检查对 Amazon Machine Images（亚马逊机器映像），Relational Database Service（关系数据库服务）和 Elastic Compute Cloud（弹性计算云）的无限制访问可以保护知识产权和敏感数据，以及防止服务中断。

3. **删除非活动账户：**非活动和未使用的账户会对 IaaS 环境造成不必要的风险。审查和删除非活动账户可以防止账户泄露和滥用，对公司的运作也没什么影响。

4. **安全监控：**将计算迁移到云中，最大的担忧之一是失去可视性和取证问题。启用审查追踪（如 AWS 的 CloudTrail 日志记录）可以创建一个行为监控工具，用于监控威胁和取证调查。这也是对所有大型公司提出的基本合规性要求，该要求可能会成为公司将应用程序迁移到 IaaS 的阻碍。

在这四个措施中，安全监控是最复杂和最可靠的。机器学习工具可以被调谐，以检测威胁信标。API 可以根据会话位置，过度活动或强制登录启用监控功能。乍一看，将应用程序迁移到云可能会失去控制。然而，使用主动的基于云的安全策略，IaaS 上的应用程序可以与企业内部程序一样安全，甚至更安全。