http://www.cww.net.cn/tech/html/2016/6/1/201661845229573.htm
NetEvents2016：cloud computing platform security is vital
01/06/16

NetEvents2016：云计算平台安全至关重要

通信世界网　　作者：郄勇志　　2016年6月1日 08:45　　云计算 云安全 稳捷网络 Wedge Networks　　分享

通信世界网消息(CWW) 紧随云计算、云存储之后，云安全也出现了。“云安全”是“云计算”技术的重要分支，已经在反病毒领域当中获得了广泛应用。云安全通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，推送到服务端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。整个互联网，变成了一个超级大的杀毒软件，这就是云安全计划的宏伟目标。5月26日在新加坡举行的NetEvents亚太地区记者和分析师会议上，与会专家就云计算平台的安全问题进行了深入的讨论。

恶意软件流行倒逼安全云计算平台诞生

云环境面对的威胁中有很多都与传统企业网络面对的威胁相同，但由于有大量数据存储在云服务器上，云提供商便成为了黑客很喜欢下手的目标。万一受到攻击，潜在损害的严重性，取决于所泄露数据的敏感性。个人财务信息泄露事件或许会登上新闻头条，但涉及健康信息、商业机密和知识产权的数据泄露，却有可能是更具毁灭性的打击。

一旦发生数据泄露，公司企业或许会招致罚款，又或者将面临法律诉讼或刑事指控。数据泄露调查和客户通知的花费也有可能是天文数字。其他非直接影响，比如品牌形象下跌和业务流失，会持续影响公司长达数年时间。

同时，一旦恶意软件进入系统，就无法阻止它扫描密码、银行账户信息，或其他敏感的知识产权。对消费者和企业来说，这是一个可怕的真实入侵。这些恶意软件攻击的范围很大，2015年美国联邦调查局FBI收到2,453宗有关恶意软件网络攻击的投诉，FBI表示这让受害者付出了超过2400万美元的代价。

根据 NSS实验室首席架构师Jayendra Pathak（NSS实验室是位于德州奥斯汀的顶级科技安全分析公司）表示，这些恶意软件攻击在美国和欧洲最为普遍，但也正在快速渗透亚太地区。

在这方面，全球权威专家给出了自己的建议-。例如稳捷网络（Wedge Networks）首席执行官James Hamilton，Menlo安全公司欧洲中东和非洲解决方案架构师Jason Steer，和Cylance 亚太地区区域总监Andy Solterbeck均对现代最大的安全威胁隐患提出他们的建议“关键是预防”，毫无疑问，云计算平台安全问题肯定是全球性，并且正在迅速蔓延到世界各地，特别是亚太地区。

云计算安全平台从网络防御开始

云平台上的管理访问都是通过互联网，而不是传统数据中心模式中坚持的受控制的和限制的直接或到现场的连接，这自然会增加风险和暴露，所以就要求对系统控制和访问控制限制的变化进行极为严密的监控。

传统云安全的防护主要体现在对病毒的恶意程序检测上面，它主要依赖于安装在用户计算机上的威胁特征码数据库，这意味着，每台计算机上的威胁特征码数据库只有在更新并包括新威胁的特征码之后才能提供最新的防护。也就是说在对待安全威胁的处理上，存在着时间的延迟。这种办法无法有效地处理日益增多的恶意程序。因为来自互联网的主要威胁正在由电脑病毒转向恶意程序及木马而这样就会造成对被感染文件的干预延迟，从而造成安全隐患。

快速变化的网络威胁与传统企业网络的解体使得中小型企业几乎不可能靠自己来维持强健的网络安全。在网络的云层安全运营是必要的，但大多数企业缺乏熟练的资源、云基础设施，和资本预算来靠自己实现安全的这一层。幸运的是，由通信服务提供商（CSP，communications service providers ）发起的新的基于云的安全即服务举措，承诺了以风险降至最低而提高商业案例的方式为服务提供商来解决这个市场的需求。

就在上周，随着在新加坡推出网络安全卓越中心（COE，Centre of Excellence），StarHub宣布稳捷网络为创始生态系统合作伙伴之一。StarHub COE作为网络安全生态系统的枢纽，汇集了处理网络威胁的专业处理方式，这些网络威胁给企业和经济带来严重的风险。

StarHub分析和网络安全副总裁Woo Lip Lim博士指出“随着StarHub建立了新加坡的网络安全卓越中心，我们相信基于云的安全并提供安全即服务的好处给我们的客户将是至关紧要的。与如稳捷网络的行业领导者合作，放大了我们提供网络犯罪预防与为我们的客户提供有价值服务的卓越能力。”

稳捷网络亚太区董事总经理Gary Tate强调了作为一个基于云的平台来支持亚太地区创新的规模和胃口，稳捷CND日益增长的地区重要性，他解释说“该地区几乎每一家主要的服务提供商都在评估或计划为他们的客户提供基于云的安全即服务。利用云基础设施提供安全与性能、规模和效率，而不需要专门的硬件，是一笔巨大的资产。基于云的方法降低了投资风险，最终让他们加快新的和动态的服务。”

云安全企业发展前景光明

旨在为企业跨云应用提供安全解决方案的云安全初创企业 vArmour 近日获得了 4100 万美元的 D 轮融资。目前 vArmour 在全球拥有 165 家客户，涵括金融、政府、医疗保健、零售以及电信运营商等行业，管理的虚机达到了 10 万个，且在去年已经实现现金流为正，其目标是今年将客户数增长到 450 家。

此轮融资的领投方包括 Redline Capital 等战略投资者以及新的投资方澳洲电信。澳洲电信将会利用这层关系拓展其托管服务，并与 vArmour 达成合作关系在亚太区推销数据中心安全服务。对于 vArmour 来说，加上 2014年 获得的B 轮和 C 轮，至此其总该融资额已达 8300 万美元。

无独有偶，以色列云安全创企Avanan获1490万美元A轮融资，由Greenfield Cities Holdings领投，前投资者Magma VC和StageOne Ventures续投。Avanan所提供的云安全平台可以保障安全服务的云安装，包括恶意软件防护、反病毒程序、数据泄露防护、端点安全检查、行为监控、邮件安全、防止网络钓鱼、数据加密以及其他服务。

而在国内，云计算安全问题也备受瞩目。第八届中国云计算大会于2016年5月18日在北京国家会议中心正式拉开帷幕，云安全问题再次成为参会各方热烈讨论的话题。新致软件的云计算事业部总经理田奎认为：在安全审计方面，应该建立安全审计系统，进行统一、完整的审计分析，通过对操作、维护等各类日志的安全审计，提高对违规溯源的事后审查能力。

最近的一份来自ABI研究的报告发现大数据和云计算是管理空间威胁隐患主要的增长因素，这份调查询问了150名来自各个行业的企业IT安全专家，询问了他们在不久的将来采用SDN的计划，63%的受访者说网络安全业务在过去的两年里变得更加困难。此外，调查发现，69%的受访者目前运行着私有云，使用公有云服务，或者两者都有，他们表示仍在学习如何将安全策略应用到混合云基础设施中。换句话说，在云安全方面尽管已经取得了巨大的成就，但安全操作和流程仍然不足，部分原因在于网络复杂性正在上升。