## 华云数据：如何构建企业上云安全防护体系

来源：华云公众号 2019-02-28

链接: https://www.huayun.com/news/573.html

随着云计算业务的快速发展，国内外云计算企业的专利之争也愈发激烈。在云计算这样的技术领域，专利储备往往代表着企业最新的技术实力。华云数据本期“智汇华云”专栏将针对“如何构建企业上云安全防护体系”，与大家共同分享云计算领域的发展趋势。

随着云计算业务的快速发展，国内外云计算企业的专利之争也愈发激烈。在云计算这样的技术领域，专利储备往往代表着企业最新的技术实力。华云数据本期“智汇华云”专栏将针对“如何构建企业上云安全防护体系”，与大家共同分享云计算领域的发展趋势。

当前，网络数字化、智能化快速发展，网络威胁加速渗透，网络安全面临重大风险和挑战。大量分散数据集中到云内，这些数据中包含的巨大信息和潜在价值吸引了更多的攻击者，针对云上安全防护的需求也与日俱增。云安全的建设需要充分保证租户业务安全与数据安全，要求云服务提供商能够提供持续运营安全服务。

在数字化时代，由于云计算风险集中，导致大规模安全风险的出现，让网络安全形势更加严峻。那么，企业上云安全该如何建设，如何才能拥有一套成熟的安全体系？华云数据作为中国云计算、大数据独角兽企业，积极助力数字中国网络安全体系建设，助推网络安全生态健康发展。

2019年2月28日，华云数据集团售前方案经理屈崇凯分享了云上安全合规的解决方案及探索与实践，助力企业开启安全、可控的上云之路。

精彩言论

1、当前，网络数字化、智能化快速发展，网络威胁加速渗透，网络安全面临重大风险和挑战。严峻的行业背景下，网络安全技术与实践应用、网络安全体系及生态建设备受业界关注。互联网是关系国民经济和社会发展的重要基础设施，深刻影响着全球经济格局、利益格局和安全格局。基于互联网协议第四版（IPv4）的全球互联网正面临网络地址消耗殆尽、服务质量难以保证等问题。下一代的互联网协议第六版（IPv6）应运而生。

2、2017年11月26日，中央办公厅、国务院办公厅印发《推进互联网协议第六版（IPv6）规模部署行动计划》（以下简称《行动计划》），对各行业IPv6迁移过渡提出明确安排和时间要求。作为国家经济运行的重要支撑，金融行业应积极开展IPv6技术的试点研究与探索，为其全面部署落实奠定基础。2019年1月10日，中国人民银行发布关于金融行业贯彻《推进互联网协议第六版(IPv6)规模部署行动计划》的实施意见。《行动计划》要求在未来5~10年间实现下一代互联网IPv6自助产业技术体系和产业生态，并在经济社会各领域深度融合应用，金融机构网络将首先完成互联网环境的IPv6规模部署。

3、对于企业而言，云安全建设需求主要有三点，其一是业务牵引，包括业务安全的积极预防，云及混合云环境是否能够防患于未然，提前感知威胁；业务自身及环境安全，业务上云，如何保障云平台安全、数据安全、应用安全；业务安全的持续监测，如何检测云上业务系统面临的各类安全威胁；业务安全的处置手段，云环境中，出问题后如何快速定位，止损溯源。其二是技术牵引，建设云安全体系。在云环境下，原有的隔离原则将会失效，原有可信的边界日益模糊，攻击平面增多。软件定义安全成为趋势，越来越多的安全软件化、虚拟化，并支持可编程式的控制。用云方式解决安全问题会越来越普及。其三是合规快速响应，能否一站式解决新技术和新合规要求。

4、  虚拟化会带来一些安全风险，比如虚拟机逃逸，正常情况下，同一虚拟化平台下的客户虚拟机之间不能互相监视、影响其他虚拟机及其进程，但虚拟化漏洞的存在或隔离方式的不正确可能会导致隔离失效，使得非特权虚拟机获得 Hypervisor 的访问权限，并入侵同一宿主机上的其他虚拟机。对于虚拟化平台而言，也存在一些安全风险。虚拟机迁移时，需要先迁移虚拟机的内存等状态信息，并传输虚拟机副本到新的物理机上恢复运行，攻击者有较多的时间截取敏感信息。虚拟机镜像、快照恢复的时候，由于缺乏及时的系统补丁，造成新创建的虚拟机极易受到攻击。

5、  云资源可以灵活调配，击破传统安全域的便捷。同一物理机上虚拟机（业务系统）间的网络流量无法使用传统网络设备进行检测。内部病毒爆发引起的互相感染攻击无法通过边界安全设备控制。传统安全策略无法感知、跟随虚拟机的迁移。虚拟机之间的隔离主要通过虚拟化层软件实现，无法控制同一宿主机中的其它租户安全防护能力如果攻击者利用一台虚拟机获得宿主机的所有资源，导致其他虚拟机没有资源可用，将造成虚拟化环境下的拒绝服务攻击，“邻居”失火殃及“自己”。

6、  虚拟网络存在风险，一方面传统的安全域被打破，东西向流量不可见，同一宿主机中不同业务系统间的通信（东西流向），传统（南北流向）物理安全设备无法检测，另一方面，在超大的二层虚拟网络中，被攻击者攻破的通道很多，攻击危害性都远远超过了它们在传统网络中的影响。因此，也带来了安全管理方面的风险。运维人员通常使用远程管理平台对虚拟机进行管理，如VMware的vCenter、Citrix的XenCenter。集中管理降低了管理复杂度，但可能带来如跨站脚本攻击、SQL注入等危险。

7、云计算有安全强制规范，公安部发布了《网络安全等级保护条例》，对于大型云计算平台，应将云计算基础设施和有关辅助服务系统划分为不同的定级对象。传统安全手段无法满足云等保合规的要求。在云环境下，云安全责任模型需要建设端到端整体安全体系，治理层次清、权责界限清，核心理念是智慧云安全，以等保合规为基础，安全组件齐全，安全资源池满足快速交付，日志集中审计和存放，三权分立。以软件定义安全为架构，开放的整体架构，南向支持第三方安全组件集成，东西向，支持不同的云平台对接，北向开放接口支持被集成。以安全运营为核心，资产同步、租户同步，服务编排，事件监测、报警和处置，计量计费，安全服务。