云计算的“中场战事”

走过风云激荡的 2019 年，时代进入 21 世纪的 20 年代，一些曾被刻意隐藏的故事如今可以透露一二了。

大约一年前的这个时候，某知名互联网公司连续遭受了两次 DDoS 攻击，其中一次攻击流量峰值竟然高达 710Gbps！要知道，4 年前 DDoS 攻击的流量世界纪录才是 400Gbps，当时拖垮了包括维基解密在内的 78.5 万个网站。

幸运的是，为该公司提供云服务的腾讯云对于解决客户超大流量 DDoS 攻击富有经验，在遭遇攻击时能智能调度防护节点来抵抗攻势，两次都在不到一分钟之内解决了战斗，让客户网站和大量用户在无意识中度过了危机。

尽管如此，据刚刚发布的《2019 云安全威胁报告》显示，2019 年中约 2/3 的网络 DDoS 攻击事件都以云平台 IP 作为攻击目标。除此之外，当下云平台还面临着包含存储、网络、管理等在内的安全威胁，任何攻击都有可能对整个云上用户造成灾难性影响……

种种表明，在今天的云端世界，人们所感受到的“岁月静好”，都不过是各条战线上的安全团队们为各界负重前行，而云服务提供商应该、也正在成为云安全防护的主力。

■新快报记者 郑志辉

关注“如何上云”，更关注“如何安全上云”

近年来，在政府、产业的双重推动下，云计算技术在我国得到迅速推广。据中国信息通信研究院的数据显示，2018 年中国云计算产业规模达到 962.8 亿元人民币，预计未来几年将保持稳定增长，到 2022 年市场规模将达到 2902.9 亿元。

与此同时，任何以互联网为基础的应用都存在着一定危险性，云计算也不例外，安全问题从云计算诞生那天开始就一直受人关注，其产生的危害和影响远比传统安全事件要大得多。正如篇首案例所呈现的，如今规模越来越大的 DDoS 攻击事件频繁出现，恶意程序增多，未知威胁所带来的危害程度持续升级。面对日益复杂的安全需求，传统软硬件的安全防护体系和模式开始力不从心，而代表未来趋势的云安全，顺理成章成为云时代的刚需品。

2019 年 8 月，中国信息通信研究院发布了《云计算发展白皮书（2019 年）》，白皮书认为，随着我国云计算应用的日益普及，用户不再仅仅考虑“如何上云”，而更关注“如何安全上云”，受近些年云安全事件频发的影响，用户对云上的安全需求越发迫切。

同时，《网络安全法》等法规政策的出台强化了企业安全合规的要求，进一步推动了我国云安全市场的快速发展。一方面，云计算厂商在强化自身安全能力的同时，纷纷将自身安全能力产品化输出；另一方面，安全厂商积极布局云计算安全解决方案，将积累的丰富安全经验适配于云环境。

中国云安全市场快速崛起

与全球云计算市场发展格局类似，中国云计算领域也呈现出市场份额进一步向头部厂商聚拢的现象。在中国厂商里，阿里云对标 AWS 在全球市场的发展轨迹，优势明显。腾讯云厚积薄发，背靠腾讯系生态，近年来增长极快；过去四年，腾讯云的营收规模均保持了三位数增长。日前，腾讯云又宣布，年度收入在第三季度已经突破 100 亿元，进入全球云计算厂商百亿俱乐部之列。

中国电信在渠道及技术上借助合作伙伴力量，主攻传统政企市场；金山云的优势在于成立之初抓住了公有云领域视频和游戏这两个最大的应用场景，跻身于四强席位。

与之相伴的中国云安全市场目前仍处于起步阶段，但整体市场规模将随着云计算市场规模的增长而快速崛起。根据赛迪统计，2018 年中国云安全服务市场规模达到 37.8 亿元，同比增长 44.8%，处于爆发式增长阶段，预计到 2021 年市场规模将突破百亿元，未来三年年均增长率为 45.2%。

虽然中国的云安全服务市场增速喜人，但实际上并不是太多企业和个人真的了解它，比如说，什么是安全的云？评判标准是啥？

这一现象在 2019 年 9 月 1 日后无疑会大大改善。国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部共同制定并发布的《云计算服务安全评估办法》（以下简称“办法”），将于此日起施行。

建立云上网络安全的“第一道防线”

根据《办法》中规定的云计算服务安全的重点评估内容，我们可以以近年来致力于云上安全建设的腾讯云为例，深入了解何谓“安全的云”，云服务厂商该如何建立起云上网络安全的“第一道防线”。

作为一家云厂商，首先要具备运营大规模基础设施的经验，才能持续提供高速、稳定、安全的云服务。据了解，目前腾讯全网服务器总量已超过 100 万台，带宽峰值突破 100T，基础设施覆盖全球五大洲 25 个地区，曾为多家知名企业化解过 T 级 DDoS 流量攻击。

威胁情报被视为网络攻防的第一关卡，已被大量政企、机构作为风险预知的“报警器”。拥有 20 余年网络安全经验的腾讯云，结合多年黑灰产对抗经验，可对海量安全数据进行过滤和自动识别，形成威胁情报库。在某次大型网络攻防演练活动中，腾讯云曾依托威胁情报中心，成功阻断主动攻击 3 万余次，分析上报安全事件上千次，检测到新型网络武器攻击数十次。

威胁情报只是腾讯云三大核心安全技术之一，其他两大技术能力是安全攻防和“大数据+AI 能力”。

安全攻防是安全技术硬实力的体现，包括了对云上漏洞的挖掘和收敛，突发事件的紧急响应，对黑客攻击的溯源等等。腾讯云的安全攻防团队，在内部采取红蓝对抗的方式，不断磨练提高团队的攻防技术、收敛云上的安全漏洞。在 2018 年举行的贵阳大数据及网络攻防演练上，获得过攻与防的双料冠军。

AI+大数据的能力则为租户的业务安全提供了更多保障。蒙牛就曾在 2018 年世界杯期间，依托腾讯安全的黑灰产大数据、AI 风控模型，实现精准识别、实时判断和分级处理三层营销风控保障，快、准、狠地拒绝“羊毛党”掠夺。

举生态之力，共担安全责任

独行快、众行远。云计算打破了传统的网络边界防护，一家企业或机构的安全规划与建设，很难由单一一家安全企业提供完整技术能力来解决。伴随产业互联网的发展，以及增量安全需求的复杂性，加快安全生态协同共建，已经迫在眉睫。为此，腾讯过去几年来一直在倡导构建安全生态云环境。

据了解，目前腾讯与合作伙伴共同打造的安全联合解决方案超过 20 个，这些联合解决方案占腾讯安全全品类销售比例达到 26%，而在 2019 年上半年，腾讯安全产品通过渠道伙伴销售的增速达到 200%。基于良好的合作实践，腾讯正在与 P17 等安全生态伙伴探索“生态资源共享、能力互补、生态共建”的协同机制，共享产业安全红利。

P17 是由腾讯安全 2017 年发起，汇聚天融信、卫士通、启明星辰、美亚柏科、拓尔思、蓝盾股份、任子行、北信源等国内安全上市企业领袖的安全领袖圆桌，主要探讨产业互联网背景下的安全产业发展新趋势，达成“生态资源共享、能力互补、生态共建”全新合作机制，共同承担产业互联网安全发展责任。

在产业互联网的融合安全市场中，不仅需要长期深耕网络安全行业的“老玩家”带队，也需要专注各个细分场景的新锐力量，让网络安全行业变得丰满和体系化，从而满足各种量级政企用户的多样化安全需求。

由腾讯安全和知道创宇 2018 年联合发起的 FP50（安全新锐力量）俱乐部，持续性聚合优秀的安全行业新锐力量企业，不断吸引安全新秀企业加入，2019 年就有厦门服云信息、江苏敏捷科技、全知科技、深圳万物安全、北京天际友盟等新锐安全企业加入，更集结成员企业的“网络安全解决方案”优秀案例，汇编成为《FP50 优秀网络安全解决方案白皮书》，展示了安全行业新锐力量的优秀实力，推动行业内核心技术创新突破，助力安全行业新担当的迅猛腾飞。