

李雨航：信息安全的云卫士

文/本刊记者 裴媛

李雨航，云安全联盟全球总顾问/大中华区主席，中国云安全联盟常务副理事长。



随着云计算等新兴技术的发展，云安全问题受到越来越多人的关注，新兴技术及其业务模式的发展不仅带来便利和富足的物质生活，也带来了严峻的信息安全问题。西方媒体曾做过一项调查，76%的人会因为个人信息泄露而减少网络活动，而在中国这一比例只有20-30%，这充分说明目前我们对个人信息安全的重视程度远远不够。故本刊特邀云安全联盟大中华区主席李雨航教授，请他为我们介绍当今网络安全形势及云安全行业发展现状。

网络安全形式严峻

“个人信息安全正处于十分严峻的时代，数据泄露事件不断发生。”对于云计算大数据的信息泄露，李雨航介绍道：“这类新兴技术，基于数据信息中央存储的形式，数据一旦丢失，损失非常大，会加剧信息丢失的严重性。”对于个人的信息泄露，李雨航认为最主要的原因在于国家针对个人隐私问题的法律在推出和实施上还没有细化。

据李雨航介绍，云安全有两个含义：一个是保障云服务的安全，另一个是利用云计算来增强安全能力。一方面，云计算的计算能力和存储能力非常强大，黑客能够进攻它，也能够利用它的力量来强化攻击技术。另一

方面，云计算可以成为安全专家和安全防护人员的武器，安全防护人员可以用云计算大数据的力量来打造新的安全服务，把这些安全服务利用云技术传递给用户。这个概念在云安全范畴里，称为安全云或者安全云服务。

对于企业来说，随着云计算、大数据等新兴技术的产生，面临的数据安全问题更加严峻。“云计算是把企业的计算资源作为一种服务，放在云计算中心，由云服务商来提供传统的IT服务。企业从先期购买IT资源变成到云服务商那里租用IT服务的用户，企业的数据就已经从隔离保护的边界里出去，不再由企业掌控。另外云计算采用了大量虚拟机等技术，这些技术的安全性如何，还需要时间来验证。在这种情况下，如何对数据进行安全保护成为更大的难题。”李雨航介绍道。

李雨航做了一个比喻，企业数据以往在自己“家”里非常安全，周围有安全门、防盗锁等一系列完备的安全防护措施。由于企业需要发展，数据被搬到一个公共环境——云计算中，云计算类似于一个新环境，在这种环境下数据面临更多的风险和威胁，数据的保护方式与传统手段截然不同。在传统方式中，黑客要进攻企业数据资产，他会采用物理方式，通过门禁系统进来，或者通过防火墙外部进来。在云计算的环境中，攻击者也可以购买一个服务，他可能跟企业共享一个虚拟机，这样威胁系数直线上升。“你在自己家里，入侵者如果想进来，他需要破坏你的报警和防御系统。如果你处于一个公共环境，你身边可能处处是敌人，黑客要攻击你就容易了，这种威胁程度是不一样的。”李雨航强调，“数据在云端遭遇的攻击面更大，黑客可以变成一个租户从侧面进攻，甚至黑客会收买云服务商的管理



这些新兴技术引入了太多变量，太多攻击面，我们防守者很难保护。因为攻击者只需要攻破一个点，能够进来就攻击成功了。而防守者却需要面面俱到，把所有的点都堵住，这对防守者来说十分困难。



员，从背后或内部攻击企业数据。”

李雨航认为目前我们面临的安全形势紧张，未来更有挑战性。“我们的对手，黑客和攻击者他们也在想尽各种方法增强自身的实力。而且还存在一些特殊组织，他们会高额投资技术来专门做攻击，攻击手段更是层出不穷。”李雨航提到，“这些新兴技术引入了太多变量，太多攻击面，我们防守者很难保护。因为攻击者只需要攻破一个点，能够进来就攻击成功了。而防守者却需要面面俱到，把所有的点都堵住，这对防守者来说十分困难。”

多种手段共同维护信息安全

“维护信息安全，需要结合法律手段、管理手段和技术手段，同时还要注重公民教育，仅从一个局部下手无法从根本上解决问题。”李雨航解释道。

“法律在其中起决定性作用。法律是源头，没有法律的约束，黑色产业会越来越猖獗。”李雨航强调，“其他手段只是修修补补，法律是核心。”2015年，国家推出《国家安全法》，首次把网络安全写进国家安全；2016年国家推出网络安全领域的基本法律《中华人民共和国网络安全法》。这

一系列法律政策让网络安全有法可依，表明了国家对数据信息的保护越来越重视。

管理手段是法律手段的补充，法律法规在具体实施上需要通过管理和技术手段来帮助落实。如政府结合国内外安全行业形势颁布了安全行业标准，要求企业和服务商做对应的防护措施；美国政府和云安全联盟合作推出了RAMP STAR认证；云安全联盟结合安全产业形势对服务商发布了行业的云安全标准。政府和行业都会制定安全标准，这些标准是对云服务商和企业的一种管理手段。“如果不提要求，有些云服务商可能会偷懒，毕竟安全投资需要大量资金。”李雨航说。

个人隐私的泄露已经成为整个行业的痛点，因此企业和学术界做了大量前沿性的研究工作，在隐私技术方面产生了很多新兴技术。从账号管理体系、身份认证体系、访问控制体系到审计体系等，都取得了不菲的成绩。李雨航举了一个例子：现在被苹果引用的差分隐私技术是由微软科学家发明的，当个人隐私在被传到中央服务端时，差分隐私技术通过对个人隐私加一些噪声，达到保护统计后隐私信息的目的。在大量隐私信息被传到中央储存的情况下，黑客识别不出哪些是个人的，所以隐私能够得到保护。“在技术上，我们能做的事非常多，但技术是要有成本投入的。”李雨航说，“如果法律有这方面的要求，比如要保护隐私，那么相应的技术手段会得到投资。”如欧盟在2016年颁布的《通用数据保护条例》是一个典型例子，如果企业达不到这个要求，将会受到非常重的处罚，罚款最高甚至可以达到全球营业额的4%。在这种情况下与欧盟业务相关的企业，他们就愿意投资有关隐私保护的技术。

除此之外，公民教育也是很重要的一种手段。李雨航提到云安全这类新兴技术，知识更新非常快，无法及时进入课堂，导致目前我国安全产业人才匮乏。“现在有了非常大的转变，我们国家意识到网络安全是非常重要的领域，所以从去年开始把网络空间安全列为了一级学科，跟计算机学科是并列的，授权很多大学来开展这个学科的教育。”李雨航提到，“但是我觉得从长期来讲，国内教育还有许多工作要做，给学生提供更多实践经验。我希望有更多的高校和云服务或云安全公司进行合作，共同致力于网络安全人才的培养。”

除了上述几种手段以外，李雨航认为，为了应对未来网络安全不断恶化的形势，云服务商和云安全公司需要摆脱传统防御的思维来做一些创新，化被动为主动，针对新环境开发新技术。新技术不仅可以带来威胁和风险，也可以用来增强安全能力。李雨航介绍，云安全联盟在这方面做了很多创新性工作，“我们有一个方案是让攻击者看不见攻击目标，不管攻击者再厉害，系统应用的漏洞再多，你看不见我，就没法进攻，这种叫做隐身术，我们有不少这样的方案。”李雨航认为，“我们行业需要思考怎样利用新兴技术来做安全工作。不只是防御，还有到检测，再到数据自我保护。不管环境是否安全，有无漏洞，核心数据资产都能够自我保护，受到攻击后能够快速地进行自我识别、自我恢复。”

云安全联盟——网络安全的领跑者

云安全联盟（CSA）2009年在RSA安全大会上正式成立，目前有美洲区、欧非区、亚太区及大中华区。在李雨航的努力促成下，云安全联盟大中华区在2017年依托中国云安全联盟开始进行专

业化运作。李雨航担任国际云安全联盟CSA大中华区主席兼全球战略总顾问。联盟向企业会员提供服务，现在会员大约有300家来自全球500强的科技公司和安全公司，比如亚马逊、微软、谷歌、腾讯云、华为等。

中国云安全联盟是独立、中立、专业、权威、具有公信力的中国非盈利组织，也是国际产业组织（如国际云安全联盟CSA）在华的运营单位。中国云安全联盟使得国际安全业务在中国自主可控，为中国引进来、走出去搭建国内外认可的国际通道，为中国网络安全产业在国际发声。

对于企业会员，CSA一般采用定制化的合作。企业与CSA一起制定标准，做人才培训和研究安全技术等工作。

“通常企业会提出一个特定的问题或需求，云安全联盟帮助企业整合资源，由企业作为工作组长，一起对问题做研究。比如在华为，我们成立了两个工作组，一个针对云安全管理项目，还有一个针对云安全产品组件安全项目。”李雨航介绍到。

对于个人会员，CSA会提供很多活动机会，帮助他们了解最新技术知识和发展趋势，甚至包括新技能培训。“安全人才的储备是我们与攻击者较量中最重要的一环，如果我们没有足够的后备力量，很难打赢这场安全战争。云安全联盟创立了认证培训计划，开设有关云安全专业的培训课程，通过考试的专家可以拿到证书，他可以向业界证明他掌握了一定的安全知识技能，这是联盟的工作之一。”李雨航提到。

CSA有近千位业界资深安全专家，以安全研究为基础，对所有新兴技术的安全进行前期探索及研究工作，安全专家在30多个工作组里做30多个安全研究项目。很多的安全研究成果被业界广泛

认可，例如CSA云安全指南、STAR认证、CCSK等。

针对数据在云上面临的威胁，CSA在2017年发布了最新版本的《12大顶级云安全威胁：行业见解报告》，帮助用户梳理和认识云计算中12个比较大的威胁。为了帮助产业更好地应对云安全威胁，CSA在2016年发布了《云计算安全技术标准》；2017年发布了《云计算关键领域安全指南》第四版；2017年年底发布了《物联网安全技术标准》、《大数据安全技术标准》等一系列安全指南和安全标准。

云安全联盟在构建受信任的云生态系统方面已经取得了巨大进展，李雨航表示未来云安全联盟将继续对物联网等相关领域进行研究，以解决市场需求，并加速努力，进入下一代安全构建模块领域，例如人工智能、区块链和雾计算。“国际云安全联盟作为一个非盈利机构，可以为中国网络信息安全产业的发展提供帮助。我们会把国际的先进经验和先进技术介绍到中国来，当然最终要靠企业将技术产业化。”李雨航最后说道。