声音

网络安全需要扎紧“围栏”

访派拓网络大中华区总裁陈文俊

“十四五”以来，数字中国建设进入了快车道。中国信通院发布的《中国数字经济发展报告（2022年）》显示，2021年，我国数字经济发展取得新突破，数字经济规模达到45.5万亿元，千行百业的数字化在带来经济效益的同时，也使得数据呈现爆炸式增长，大量的应用数据被产生、传输、公开、共享。数字化在让社会更加智能的同时，也让安全变得更加“脆弱”。

成立于2005年的Palo Alto Networks（派拓网络 NASE: PANW）是全球网络安全领导者，凭借行业领先的威胁情报（是指某种基于证据的知识，包括上下文、机制、标示、含义和能够执行的建议）和先进自动化技术，为全球各行各业成千上万的客户提供下一代网络安全平台和服务，在Gartner模拟象限里，派拓网络连续12年处于领导者的位置。随着全球数字化转型的深入，派拓网络把整个解决方案从网络安全防火墙拓展到云安全和安全应用上，包括零信任网络的访问，漏洞管理、扩展和响应，安全编排自动化，云安全、攻击面管理，对很多未知威胁提供更好的防御。

数字经济时代，网络安全面临哪些新的威胁？对企业和个人会造成哪些影响？国内外对于网络安全的认识差异性如何？近期，《中国经营报》记者专访了派拓网络大中华区总裁陈文俊。

在后疫情时代，混合式办公可能会成为一个新常态，众多的应用、数据加速上云会导致网络受攻击面不断扩大。

网络安全边界转移到云上

随着数字化转型，远程办公，逐渐上云。只在城堡边缘设立的防火墙被打破了，边界已经跨到云上，通过云再回到办公室。

《中国经营报》：数字经济时代企业所面临的网络安全与传统经济时代有什么区别？

陈文俊：比较早的时候我们做网络安全，像在一个城堡里，有护城河去保护城堡。一般会设置一些防火墙，在企业的出口做城墙的保护，我们在城堡里面工作就相对比较安全，这是最早对网络安全的定义。

随着数字化转型，实现远程办公，逐渐上云。只在城堡边缘设立的防火墙被打破了，边界已经跨到云上，通过云再回到办公室。如果是居家或者在咖啡厅办公，这个边界也可能扩展到家里和咖啡厅，那么这些场所也可能成为攻击面，进而攻击进企业内部。现在越来越多的IoT设备，如摄像头、智能冰箱、智能灯泡、微波炉都是联网的，这些IoT设备都可能成为黑客进入的目标。

举个形象的例子，以前家周围的围栏只需要50～100厘米高，现在要加高到3米，黑客就很难进来了。因为对他们来说，攻击的机会很多，成本也不高，他们会选择容易的地方攻击。

近几年，网络攻击越来越迅猛，2021年中国受到勒索攻击的数量在全球排第16位，亚太排第4位，网络攻击事件在过去几年里不断增加。

《中国经营报》：遭受网络攻击会对企业造成什么影响？

陈文俊：无论在中国还是在全球，每天都有很多网络攻击事件发生。2022年黑客勒索的罚金比2021年多了100%，2022年黑客勒索的罚金每笔30万～50万美元，最高甚至到了几千万美元。黑客攻击的主要目的是盈利，发起的攻击中有一个成功，就可能获得高额的罚金。黑客行业已经成为一个产业链，他们可以共享攻击手段和工具，也可以租用云上设备进行攻击，这需要大家提高警惕。

网络威胁趋势呈指数级增长

目前，国内外的企业都非常接受零信任的概念，采用这个架构做保护，在边界、云上、移动终端上，都能更好地提供保护，这也是比较主动地对威胁进行防御。

《中国经营报》：虽然防御手段持续升级，但网络威胁趋势反而呈指数级增长的原因是什么？

陈文俊：派拓网络发布的《2022 年Unit 42网络威胁趋势研究报告》显示，尽管防御手段持续升级，但近年来网络威胁趋势不仅没有放缓，反而呈指数级增长。仅在2021年，对Log4Shell（软件安全漏洞的一种）的利用就高达数百万次。不仅攻击数量显著增加，而且基于文件的威胁恶意比例较前一年几乎翻了一番。

虽然攻击技术不断迭代，但旧版的恶意软件并未完全退出市场。在去年检测到的恶意软件中，Barber是最常见和最主流的，而其早在2004年就被首次发现。

不仅如此，网络攻击速度也越来越快，手段越来越复杂；此外，只是靠某一端点的产品很难抵御现在的网络攻击。很多客户对网络安全非常重视，但是仍然缺乏安全感。因为不同网络安全产品之间存在差异化，保护的级别可能也不一样，最后导致黑客利用不同产品之间的差别发起攻击。

《中国经营报》：不同体量的企业对网络安全的认知有什么不同？

陈文俊：只有大公司才需要特别关注网络安全问题，小公司就不需要，这是一个错误观念；很多中小公司认为，只有大公司才能有更多的人员、更好的基础设施进行网络安全保护，这也是误解。黑客会广撒网，进行各种各样的攻击，像钓鱼一样，只要有人上当，他们就可能产生收益，同时成本又非常低。各种安全事件都会给各类企业造成压力，而不仅仅是大企业。

企业对于网络安全的投入，要基于对风险的承受度、对合规要求的满足、企业内部IT架构的成熟度等各方面因素综合考虑。如何分配资源，每个企业情况不一样，需要结合实际情况做出评估。总而言之，网络安全是大中小企业都需要关注的问题。

《中国经营报》：国内的企业与海外的企业对于网络安全的重视程度是否相同？

陈文俊：在网络边界逐渐消失以后，黑客可以从网络端、终端、IoT、移动设备进入企业内部。从法律层面上来看，欧美起步早一些，无论是金融监管机构还是信息保护监管机构。比如欧洲有GDPR（通用数据保护条例），如果出现问题，罚单是营业额的4%以内。近期，我国《网络安全法》完善了相关的处罚要求，要求处以营业额的5%以下，或者100万～5000万元之间的罚款，国内企业也会在这部分加强保护，特别是一些上市公司，金融业也受到监管，相信国内企业也会慢慢加强网络安全。

零信任代表了新一代的网络安全防护理念，它的关键在于打破默认的“信任”，用一句通俗的话来概括，就是“持续验证，永不信任”。默认不信任企业网络内外的任何人、设备和系统，基于身份认证和授权重新构建访问控制的信任基础，从而确保身份可信、设备可信、应用可信和链路可信。基于零信任原则，可以保障办公系统的三个“安全”：终端安全、链路安全和访问控制安全。

目前，国内外的企业都非常接受零信任的概念，采用这个架构做保护，在边界、云上、移动终端上，都能更好地提供保护，这也是比较主动地对威胁进行防御。

转换网络防御策略

云将会成为一个非常需要保护的地方，我们也是全方位地提供云原生的安全保护，特别在云上要做合规，在云上的开发，容器的保护，在开发阶段就能保护起来，在开发应用APP的时候，把安全植入，在开始阶段把安全做得更好。

《中国经营报》：如何建立起新时期的网络“护城河”？

陈文俊：过去我们采用被动式的防御，但现今已经无法适应网络攻击的速度，我们需要转换成积极主动的防御策略。过去城堡的方式已经不能满足这个要求，我们需要以一种全新的方式做预防、检测，应对各种载体的攻击。

我们需要更多的自动化，利用更多大数据和机器学习做自动化，更快地应对攻击。我们也相信大型的厂家，因为他们提供平台式或者整体解决方案，帮助客户主动应对未来的攻击。

国家的法律法规也在不断完善，自2017年施行《网络安全法》以来，《数据安全法》《个人信息保护法》《密码法》《关键信息基础设施安全保护条例》等相继施行。近期，《网络安全法》迎来首次修改，调整违反《网络安全法》的行政处罚种类和幅度，大幅提高罚款金额，同时拟完善关键信息基础设施运营者有关违法行为的行政处罚规定，新增网络信息安全其他违法行为的法律责任规定。从行业角度看，能够搜集大量个人数据的企业，比如关键基础建设，像运营商、交易系统、输电等，这些都需要保护以免受到攻击。

《中国经营报》：如何提高企业的防护意识？

陈文俊：很多企业也意识到信息安全是很重要的，他们意识到风险的存在后，会寻找一些方案来解决这个问题。比如受到病毒感染之后在电脑上安装杀毒软件等，但这些是远远不够的。由于服务器里都是客户和交易信息，在受到攻击的时候企业的正常运转就会受到影响，对企业声誉等各方面也都会造成不可挽回的影响。信息和网络安全问题也变成企业运行的风险，这就使得企业越来越关注网络安全问题，主动按照法律法规要求去完善。与此同时，我们需要不断地跟客户或者更多的企业互动，以后能够尽量减少受到黑客的攻击。

《中国经营报》：派拓网络在网络安全中扮演什么样的角色？

陈文俊：我们公司在2005年成立，2007年出产品，非常值得一提的是开创了下一代防火墙的领域。我们做的防火墙和传统防火墙不一样，我们通过减少攻击面做更好的防御。经过这几年的努力，我们成功实现了三大目标：网络安全转型、云原生安全、安全运营。我们新一代防火墙的硬件做得很成功，我们把硬件成功的经验拓展到软件和现在非常流行的SASE，在网络接入安全的部署上面，能够帮助客户在网络安全上转型成为零信任的安全。对客户来说，可以在数据中心里部署，也可以在云上部署，这是我们讲的网络安全转型。

云将会成为一个非常需要保护的地方，我们也是全方位地提供云原生的安全保护，特别在云上要做合规，在云上的开发，容器的保护，在开发阶段就能保护起来，在开发应用APP的时候，把安全植入，在开始阶段把安全做得更好。

安全运营，对未知的攻击威胁做演练和保护，我们想黑客下一次攻击的时候会做什么，我们利用大数据和机器学习，对未知威胁进行防御，针对黑客攻击的手段预先做一些保护，更好地对未知威胁做一些防御。

老板秘籍

1 不同体量的企业对网络安全的认知有什么不同？

只有大公司才需要特别关注网络安全问题，小公司就不需要，这是一个错误观念；很多中小公司认为，只有大型公司才能有更多的人员、更好的基础设施进行网络安全保护，这也是误解。黑客会广撒网，进行各种各样的攻击，像钓鱼一样，只要有人上当，他们就可能产生收益，同时成本又非常低。各种安全事件都会给各类企业造成压力，而不仅仅是大企业。

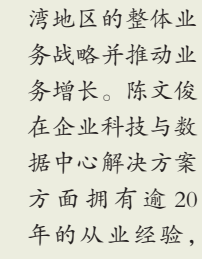
企业对于网络安全的投入要基于对风险的承受度、对合规要求的满足、企业内部IT架构的成熟度等各方面因素综合考虑。如何分配资源，每个企业情况不一样，需要结合实际情况做出评估。总而言之，网络安全是大中小企业都需要关注的问题。

2 如何建立起新时期的网络“护城河”？

过去我们采用被动式的防御，但现今已经无法适应网络攻击的速度，我们需要转换成积极主动的防御策略。过去城堡的方式已经不能满足这个要求，我们需要以一种全新的方式做预防、检测，应对各种载体的攻击。

我们需要更多的自动化，利用更多大数据和机器学习做自动化，更快地应对攻击。我们也相信大型的厂家，因为他们提供平台式或者整体解决方案，帮助客户主动应对未来的攻击。

我们国家的法律法规也在不断完善，自2017年施行《网络安全法》以来，《数据安全法》《个人信息保护法》《密码法》《关键信息基础设施安全保护条例》等相继施行。近期，《网络安全法》迎来首次修改，调整违反《网络安全法》的行政处罚种类和幅度，大幅提高罚款金额，同时拟完善关键信息基础设施运营者有关违法行为的行政处罚规定，新增网络信息安全其他违法行为的法律责任规定。从行业角度看，能够搜集大量个人数据的企业，比如关键基础建设，像运营商、交易系统、输电等，这些都需要保护以免受到攻击。



简历

陈文俊，拥有中欧国际工商学院（China Europe International Business School, CEIBS）EMBA学位，以及香港中文大学计算机科学学士学位。现任Palo Alto Networks（派拓网络）大中华区总裁一职，负责领导公司在内地、香港及台湾地区的整体业务战略并推动业务增长。陈文俊在企业科技与数据中心解决方案方面拥有逾20年的从业经验，在技术领域经验丰富。在加入Palo Alto Networks（派拓网络）之前，陈文俊供职于NetApp公司长达16年之久，先后担任多个高级领导职位，直至成为NetApp公司大中华区总裁。在此期间，他创造了将大中华区业务提升至数亿美元的出色业绩。

深度

网络安全发展趋势是平台化

目前，在数字经济向更多新领域渗透，以及5G、物联网等数字经济核心技术应用加速的助推下，AI、智能驾驶、元宇宙等新场景新需求不断涌现，无论是企业还是个人，正处在一个万物互联，“天高任鸟飞，海阔凭鱼跃”的开放网络世界，但若缺乏安全保障，毫无底线的“自由”就会变成“潘多拉魔盒”。

近几年，网络安全事件不断升级，攻击手段越来越先进，影响范围迅速扩大，给国家经济和社会造成的影响越发严峻。网络攻击行为已经不再是互联网初期的黑客炫技或者偶发事件，而是针对重要高价值目标的有组织、成规模的持续性威胁。

企业一旦遭受攻击，将造成不可挽回的损失。派拓网络发布的《2022年Unit 42事件响应报告》显示，勒索软件攻击的中位停留时间（即攻击者被检测到之前在目标环境中花费的时间）为28天。赎金高达3000万美元，实际支付800万美元，而且越来越多的攻击者开始使用双重勒索，如果不支付赎金就会公开企业敏感信息。

层出不穷的网络安全事件也在催促企业愈加重视网络安全。但是，在传统的数据安全建设模式中，多以单点安全解决方案为主，企业无法将大量的数据信息关联起来，从而不得不在多个防御系统之间疲于奔命。数据安全监测技术难、体系化规划难成为企业数据防护中的普遍痛点，企业转而寻求一体化数据安全解决方案，客户对数据安全厂家全面防御的要求提升。

网络安全市场需要以派拓网络为代表的众多企业能够持续创新，防范网络威胁于未然。

在陈文俊看来：“未来网络安全防护发展趋势应该是平台化的，需要更多的自动化，利用更多大数据和机器学习做自动化，更快地应对攻击。”

研究机构Gartner在《2021数据安全技术成熟度曲线》上，给出数据安全平台（DSP）的明确定义，就是以数据安全为中心的产品和服务，旨在跨数据类型、存储孤岛和生态系统集成数据的独特保护需求。

陈文俊认为：“多种方式如果整合在一个平台上，对客户来说可以更好地管理。平台方面的保护都是互相关联，通过一个平台的方案可以减少多个产品的投入，降低运营和维护费用，更敏捷地面对新环境。用一个平台的方案可以帮助企业更好地应对威胁，同时支持业务灵活、网络安全、降低成本。”

（本版文章均由本报记者秦枭采写）

印刷：人民日报印务有限责任公司（北京市朝阳区金台西路2号）