

企业面对的网络安全威胁呈几何级数量增长——

# 产业互联网急需安全新“铁闸”

本报记者 陈 静



钓鱼、木马、病毒……对个人用户而言，来自互联网的安全威胁可能仅仅停留在这个层面。然而，随着“互联网+”战略的持续推进，越来越多的企业也面临着网络安全挑战。如何在“云”端保障自己的数据安全、降低被黑客攻击的风险，成为产业互联网发展面临的又一个考验

网络安全不仅仅是钓鱼木马、短信诈骗，对于正在拥抱互联网的传统企业来说，它同样是安身立命的根本。亚信集团董事长田溯宁坦言：“过去10年，互联网应用主要针对消费者，但在未来的5年到10年，互联网的应用、技术和市场，必将从消费领域走向传统产业，这意味着在产业互联网时代，网络安全将面临更大挑战。”

业内安全专家们有一个形象的比喻，过去企业的网络安全只需筑起高墙，守好一扇门，但如今这道高墙上却开了很多扇窗。在“互联网+”大背景下，传统企业如何为自己安上安全新铁闸？

## 守护安全要未雨绸缪

“从技术背景来看，云计算、大数据这些新技术、新应用的出现，使网络安全的形势变得越来越复杂。”北京邮电大学互联网治理与法律研究中心副主任崔聪坦言。

这种复杂性的根本，在于网络攻防的不对称。中国工程院院士邬江兴表示：“当前网络安全现状不平衡，面对未知的漏洞、攻击等安全威胁，静态、相似、确定的IT系统架构成为网络空间最大的安全黑洞，需要针对未知的风险及威胁提供安全防护机制。”360企业安全沈阳研发中心总经理陶耀东也表示：“传统企业‘触网’打破了传统安全可信的控制环境，网络攻击可以从外向内渗透，对于制造业来说，网络化协同、服务化延伸、个性化定制等新模式新业态的出现也对网络安全提出了更高要求，但根据调研，95%以上的企业只能通过外部通报或看到显著损失后才能发现其自身正在面临的网络威胁。”

今年1月份发布的《信息产业发展指南》中，同样将产业互联网的网络安全防护作为重点之一，提出“建立健全工业信息安全政策和标准体系，完善工业信息安全检查评测和信息共享机制，推动开展安全检查、漏洞发布、信息通报等工作。



作，营造安全的工业互联网环境”。

产业互联网的网络安全从何而来？亚信安全CTO张伟钦对人工智能抱有厚望。他认为人工智能通过机器学习，能够对过去的病毒和攻击方式作出分析，从而预测未来的攻击，真正提高防御能力。“在下一个病毒还没有来袭之前，甚至连它长什么样都不知道，依然可以拦截。”锐捷网络安全与应用交付产品事业部解决方案部经理蔡铮鸣则表示，随着海量数据不断在企业中流动，进入企业内部网络的途径会越来越多，这为黑客定向攻击提供了更多途径。

“但大量数据的流动变化，也让不断创新的大数据安全技术成为可能，可以做到‘听其声、辨其形’，而网络安全‘态势感知’将成为抵御未知威胁的锋利武器。”

中央网络安全和信息化领导小组办公室副主任庄荣文表示，产业互联网和工业互联网的网络安全，还需要建立起一套安全机制，要加快健全完善设备内嵌安全机制，动态网络安全防御机制，信息和功能安全融合机制。

## “云”上安全需协同合作

来自普华永道的数据显示，包括香港和内地在内，2016年检测到的企业信息安全实践平均数量达到2577家，与2014年相比攀升了969%，普华永道安全咨询顾问江玮认为，企业面对的网络安全威胁正在呈几何级数量增长。

对于传统企业来说，不得不面对的另一安全考验是“上云”。江玮表示，“拿金融企业来说，有47%的客户表示其服务是通过云端来实行交互的，最多的是IT服务，还有财务、市场与销售、售后和运营。他们也希望利用云技术在培训、政策、大数据方面有更多的收益。”安全厂商文签网络CEO李旭阳也坦言，随着企业将业务迁移到云，就不能再依靠传统的防火墙来保证数据安全。

在张伟钦看来，这就意味着安全厂商也必须基于云提供解决方案。“包括可口可乐在内，过去的IT预算值已经不见了，规定将可能更多地走公有云，也就是用一个小时付一个小时钱。在今年我们也会推出一个纯粹基于公有云的安全防护平台，本身就‘活’在亚马逊、腾讯这样的公有云平台上。”

不过，企业上云，也意味着安全防护不再是一家之事。崔聪告诉记者，2016年11月份，《中华人民共和国网络安全法》通过，计划于今年6月1日起施行。“其中重要的亮点之一，就是确立了协同保障安全的治理体系，需要政府、企业、行业的共同参与，包括安全时间、威胁、漏洞和缓解的措施都需要共享，这正是针对现在的网络安全态势。”崔聪说。

基于联合与分享的安全共同体由此提上日程。腾讯信息安全执委会主任杨鹏认为，伴随着互联网更深层次的融合

与开放，不同领域的企业跨界合作机会增多、程度加深，安全产业与其他行业交相辉映，逐渐建立起联动联通的生态战略体系。从运作思路来分析，开放输出核心技术资源的方式，与产业链参与者结成战略联盟，是未来纵深合作形式的一大主流。陶耀东也表示，“对于工业互联网安全来说，我们也需要以协同的方式来解决安全问题。在工业互联网产业联盟的指导下，我们正式推出了工业互联网协同安全防护体系，通过众多工业互联网安全企业、区域检测与响应中心、工业互联网威胁情报中心与响应中心的多级协同，为工业互联网企业提供安全检测与响应服务”。

在国际领域，同样需要加强合作。安恒信息首席安全官刘志乐表示：“中国企业应该加入到更多的国际组织，比如说云安全联盟，加入后不仅能作出贡献，而且可以享受其标准，进一步提升国内云安全水平。”

在国际领域，同样需要加强合作。安恒信息首席安全官刘志乐表示：“中国企业应该加入到更多的国际组织，比如说云安全联盟，加入后不仅能作出贡献，而且可以享受其标准，进一步提升国内云安全水平。”

在国际领域，同样需要加强合作。

安恒信息首席安全官刘志乐表示：“中国企

业应该加入到更多的国际组织，比

如说云安全联盟，加入后不仅

能作出贡献，而且可以享

受其标准，进一步提升国内

云安全水平。”

在国际领域，同样需要加强合作。

安恒信息首席安全官刘志乐表示：“中国企

业应该加入到更多的国际组织，比

如说云安全联盟