网络安全产业的再思考

杜跃进
2019-05-24

网络安全正在变得越来越重要。网络安全产业和人才，是网络安全能力的两大基础。因为有了丰富的优秀人才，才可能有持续的技术创新，而有了繁荣的产业，才能让创新的技术成为产品和服务真正发挥作用，也才能让网络安全形成良好的可持续发展的生态。然而我国的网络安全产业经过二十多年的发展，尽管很多专家学者或者业界精英一直在不断大声疾呼和持续努力，到今天为止却依然发展得不尽人意。这背后到底是什么原因、我们的思路是否有需要调整的地方，可能需要重新思考。

一、 我国网络安全产业的几个现象

1、关于产值。有一组数字比较有趣。一般认为，我国网络安全产业到目前为止大概在300亿到500亿人民币左右的规模；我国每年黑灰产的“产值”至少达到1000亿人民币。根据以前的调研结果估算，黑灰产每获取1元钱，其造成的损失在10-30倍左右。也就是说，每年我国黑灰产造成的损失是万亿级别的。这几个数字放在一起就比较耐人寻味了：如果每年有万亿级别的损失，为什么网络安全产业才能做到百亿级别？网络安全产业界能帮助客户挽回多少损失？

2、关于产业构成。全球网络安全市场中主要收入来源于安全服务，而我国的网络安全市场安全硬件是主要收入来源。这个现象反映的是我国网络安全用户依然认为可以看到的“盒子”才是货真价实的，而对更具安全保障实效的软件、运营和服务缺乏重视。

3、关于安全现状。我国的网络安全现状不容乐观。以数据安全为例，过去几年，在数据安全能力成熟度模型（DSMM）的试点推广过程中我们进行了大量的测评，数据表明，从数据安全的视角来看绝大部分企业或者组织的能力非常欠缺，全社会的数据安全保护能力比较低。各类不断出现的数据安全事件也从另一个侧面验证了这一点。然而我国传统网络安全产业在满足今天不断增长的数据安全需求方面却还存在很大不足。

从以上现象我们看到，网络安全产业存在几种矛盾交织的现象：一是网络安全问题很突出、客户损失很大，二是客户对安全的理解存在偏差，三是网络安全产业在帮助客户减少损失方面似乎或者有劲使不上，或者心有余而力不足和。

二、 我国网络安全产业存在问题的重新思考

1、网络安全产业需要真正从满足客户需求出发，才能实现良性可持续发展和繁荣。政策扶持可以起到早期技术突破或者产业孵化的作用，但是长远的发展或者产业做大还是要依靠真正给客户带来价值。整个世界都在进入快速变化和不

确定的第四次工业革命时代，我国目前是数字经济发展最快的国家，也是数字经济最发达的国家之一，因此我国也是网络空间安全遇到问题最多最复杂的国家，对网络安全产业界来说这也意味着全球难得的机会。我国的网络安全产业是否需要调整自己，找准当前时代的客户的安全痛点？面对那万亿级别的损失，或者黑灰产千亿级别的“收入”，网络安全产业界能做些什么？

2、网络安全产业需要服务广大社会客户。当我们说到国家关键信息基础设施安全、说到一些特定重要信息系统安全的时候，我们很容易理解网络安全关系到国家安全。但是这不等于说网络安全产业的客户就仅仅是和国家安全相关的党政军等部门。因为如今的数字时代网络安全和每一个行业都开始发生深刻关联，每个部门、机构、企业甚至个人都将有网络安全需求。一方面，这些需求关系到每个企业和普通百姓的利益，这也是网络安全产业界应该肩负的责任，另一方面，这种市场需求也是网络安全产业生存和发展的基础。所以，满足人民群众日益增长网络安全需求是网络安全产业责无旁贷的任务，也是产业生存和发展的动力源泉。

3、网络安全更多地变成内需，才能让网络安全产业健康持续发展。传统的思路习惯于制定网络安全法律法规或者标准要求，然后用检查和处罚的方式“逼迫”客户进行网络安全投入，进而带动网络安全产业发展。这种方式是一定历史

时期的必然，在今天一些特定场景下也依然存在必要性，但无法保证网络安全产业的健康持续发展。因为这种思路下，客户只是被动执行、以实现合规免责为目标，而不是从保护自身利益、以实现安全风险可控为目标。面对不断变化的安全对抗，前者比较机械和表面功夫，后者才能适应自己的情况、适应对抗的变化和解决客户问题。由于网络安全中的不少威胁类型会直接给企业带来严重损失，越来越多的企业其实不需要别人替他着急，自己就会有强烈需求，而这部分需求会成为网络安全产业最有活力的部分。当然，网络安全十分复杂，从让我做，变为我要做，使网络安全更多地变成内需，需要一个持续教育和发展的过程。

4、简单化的处罚政策无助于网络安全，需要更加细分。有一种观点认为网络安全产业做不起来是因为处罚不够大，这是一个过于粗放的结论。既然网络安全是和攻击者之间的对抗，那么我们就都理解“没有百分之百的安全”，也理解“魔高一尺、道高一丈”和攻防相长的道理。因此，简单化地施行“谁出事谁挨罚”的结果就是，谁今天刚被攻击者狠砍了一刀后，明天就要再被处罚一遍。这就如同家里孩子被坏人欺负了之后，家长不问缘由就再把孩子打一顿，这个逻辑是不是有点问题？或者换句话说，如果被攻破的企业使用了某个网络安全公司的产品，这个罚款就由这个网络安全公司来承担？中国今天大约五千万家企业，80%估计都能很容易被

攻破，如果只是处罚的话，今天这 80%的企业要被关门，一年后可能 90%要关门，因为攻击者的能力又增长了。因此，处罚政策需要细化，参考阿里巴巴平台治理的做法，就是“帮助弱的、纠正错的、处罚恶的”。现实中大量的企事业单位是因为不具备足够的资源和条件来完成必要的安全能力建设，对他们应给予帮助，寻找更适合的方案来应对安全威胁。还有一些企事业单位是存在理解或者认知错误，对他们应提供更好的教育或者支持，让他们提早升级适应安全的变化。只有那些故意做恶的或者不作为的企事业单位，才应该是受到严重处罚的对象。谁去帮助那些需要帮助的对象呢？就是网络安全产业界。

5、满足广大中小企事业单位的网络安全需求是重大的挑战和难得机遇。在今天广泛互联融合的数字化时代，网络安全能力相对薄弱的中小企事业单位会成为网络攻击者更“偏爱”的洼地，也会是网络安全威胁的重灾区，同时也会成为攻击者绕过大企业大机构安全防线达到攻击目的的路径。可以说在今天这个时代，不要说各企业、机构，甚至连