两会特别报道

■ 本版撰文 本报记者 季春红

编者按:当前,随着互联网经济的蓬勃发展,网络信息安全事件时有发生。习近平总书记在中央网络安全和信息化领导小组第一次会议上提出"没有网络安全,就没有国家安全";李克强总理在今年的政府工作报告中提到,要"依法保护企业和个人信息安全"。网络信息安全问题已被提升到国家安全的战略高度。

今年全国两会期间,网络信息安全也成为代表委员们热议的关键词。实际上,维护网络信息安全也是每年全国两会保障工作的重要一环。

全息时代网络安全成两会热点

信息化产业高速发展的中国正面临着网络安全带来的潜在风险和困扰。2014年几次大规模的网络数据泄露事件,更加引发了民众对网络安全的担忧。有观点认为,随着互联网市场规模和用户数量的持续放量增长,以及移动电子商务、网上支付、社交网络等应用平台的快速发展,潜藏在互联网繁荣背后的风险将更加突出。

某种程度上讲,在云计算和大数据快速发展阶段,破解上述问题或成为中国信息产业化发展的重要步骤。记者获悉,在今年召开的全国两会上,多位代表和委员就网络安全展开了热烈讨论并提交了具体议案和提案。全国人大代表、老百姓大药房连锁有限公司董事长谢子龙在两会上表示,在智能手机、移动互联广为发展的今天,加强网络个人信息安全管理已迫在眉睫。

对于中国人来讲,在网络安全层面,2014年是一个黑色的发展之年。这一年,无论是商业服务机构还是智能手机制造商,无论是教育机构的学生信息还是铁路部门的官方订票网站,都毫无例外地成为网络黑客的攻击目标,并由此引发了大规模的个人信息泄露事件。

除了上述个人信息泄露以外,来自黑客的频频攻击,也让一些机构的官方网站处于被动压制的尴尬境地。来自国家工信部网站的消息称,2015年,全国网络安全形势比较严峻,可能发生有组织的大规模网络攻击,金融、能源、航天、运输等关键领域发生大规模、持续性的网络攻击行动,窃取敏感信息数据、瘫痪或摧毁重要目标的网络安全风险加大,网络安全事件将呈现上升态势。

而在个人信息安全领域,针对安卓设备的网络攻击持续增加,移动支付将可能成为网络攻击的新目标。同时,BYOD(自带移动设备)的兴起将带来更多针对企业或机构内部网络的攻击。这就意味着,无论是个人还是企业,以及政府部门,在2015年将迎来非常艰巨而复杂的网络安全形势。

十八大报告明确提出"要健全信息安全保障体系"的战略目标。今年2月27日,中央网络安全和信息化领导小组第一次会议提出要全面建设"网络强国",并明确指出"没有网络安全,就没有国家安全;没有信息化,就没有现代化"。个人信息安全作为网络安全的重要组成部分,已成为关系到信息消费发展、人民生活幸福、社会和谐稳定的战略问题。

在个人网络信息保护方面,谢子龙代表在两会议案中指出,首先要完善网络个人信息安全保护的制度体系;其次要制定严厉的处罚措施,增加违法成本和提高全社会的个人信息保护意识;再次,加强行业规范和监管,明确个人信息的保护主体。同时,他还呼吁全社会参与网络安全防范。

我们生活在一个全新的互联网信息时代,互联网已经成为多数人生活和工作的依赖。一方面,互联网的空间具有一定的隐私性。另一方面,由于网络的开放性和信息的安全监管问题,个人信息处于完全裸露的状态下。全国人大代表、广州佳都集团董事长刘伟在今年两会上以发生在自己身上的故事为例,向媒体道出了企业在信息安全问题上的尴尬与被动,并以此向大会提交应尽快制定《网络安全法》的议案。

从事IT行业多年的刘伟不曾想到,去年,因为一个网络信息数据被人非法窃取,公司蒙受了经济损失。然而,他在启动了追责调查程序后,却发现法律维权在互联网中非常薄弱甚至无力。

记者了解到,在刘伟的这份议案中,既隐藏着对网络攻击的愤怒,也隐藏着对现行网络法律法规立法存在短板的无助。他认为,网络安全不仅影响到企业正常生产和网民的生活秩序,也威胁到国家安全。构建良好的互联网监管体系和完善相关法律法规,才能营造和构建健康和谐的网络发展环境。换句话说,互联网的立法是中国信息产业化发展的必由之路和重要支撑。

从全国两会网络安全保障透视科技创新活力

远江盛邦公司召开会议落实两会网络安全保障工作

全球关注的中国两会正在北京召开,威武雄壮的武警雪豹突击队以及代表委员们的议案提案给民众留下了深刻印象。然而,除了我们看得见的大量军警和安保人员在为两会提供保障,还有一群人正在另一个看不见的战场,守护着两会的网络安全。

记者了解到,今年两会除了在新会风上有了较大改进外,还充分利用互联网优势,建立两会专用APP和媒体资料查询网络窗口,以期最大程度地提高工作效率和信息传播速度。代表委员们可以通过APP进行交流、讨论、查询会议通知和相关新闻。在提高代表委员们开会效率的同时,也有效节约了会议用纸。

然而,在充分利用信息化为我们带来便利的同时,网络威胁也如影随形。为了应对可能出现的信息安全事件,相关部门在今年两会期间组织了非常细致的信息安全保障工作。由于信息安全战场的特殊性,在参与两会安保的队伍中,除了国家的有关部门,许多从事信息安全服务的高科技企业也扮演了非常重要的角色。

3月8日,《中国贸易报》记者见到了正为今年两会提供网络安全保障的远江盛邦公司CEO权小文,并就当前网络安全监控的复杂性和危害性等问题进行了采访。

权小文告诉记者,全国两会是我国政治领域最高级别的活动,网络安全保障成为大安保系统的重要组成部分。鉴于当前互联网安全事件频发带来的不良社会危害,对重大事件进行信息安全保障早已成为常态。事实证明,这样做也是完全必要的。来自卡巴斯基的统计数据显示,2014年,针对安卓设备的攻击是2013年的4倍。有机构预测,2015年,针对安卓设备的恶意软件数量将是2014年的2倍。

互联网带来的便利和看不见的安全隐患将在相当长的一段时间内同时存在。具有重大影响力的网络传播活动需要更为严谨和密集的安全检测手段和应对突发事件的处理能力。据了解,去年在乌镇召开首届世界互联网大会当天,会址所在地某县级检察院网站就被黑客攻击并篡改了网站主页,留下了大量违法言论信息。远江盛邦作为承担信息安全保障任务的主要机构,通过其WEB监控系统在3分钟内便发现了问题,并进行了高效的应急处理,避免了不良影响的扩大。

因为这次成功的安全保障工作,该公司当地负责人徐进被当地政府评为"2014年度互联网安全管理工作先进个人"。"这件事使我们更加了解自己所从事的工作对于国家和人民的意义,更加坚定了我们深耕网站安全防护这一领域的信心和决心。"权小文这样对记者说。

网站安全已经成为网络安全的焦点,这与网站在当代社会所扮演的重要角色密切相关。通过网站提供公共服务的是互联网企业,比如门户网站、社交网站等,而随着它们对人们生活方式的影响日益深入,大量的传统商业企业也纷纷开始向互联网转型,从旅游、零售,到医疗、金融,几乎商业社会的整体版图都在向互联网搬移。与此同时,政府部门和公共机构也纷纷开发了自己的网站主页。到2014年底,中国开通门户网站的政府部门累计接近7.7万。正是由于网站在社会生活中扮演着极其重要的角色,才使得对网站的攻击日益增多,与网站相关的安全事件也往往会造成非常严重的经济损失和非常恶劣的社会影响。

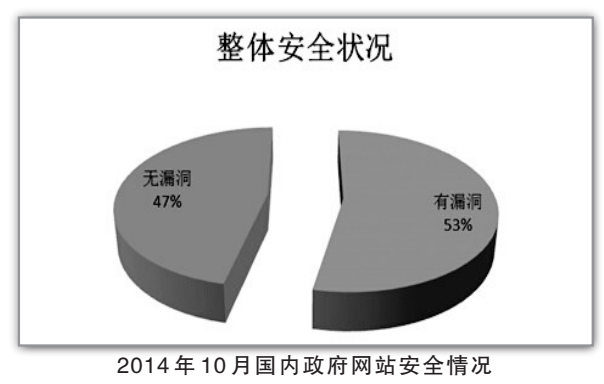
权小文向记者介绍,针对网站的攻击从大的维度划分为三类:一类是拒绝服务类攻击,即通过大流量访问,致使对外提供服务的网站瘫痪,这对于购票、医疗、电商等网站是非常致命的攻击。比如近来针对淘宝、京东、12306等网站的攻击。第二类是网页篡改,即不法分子通过攻击手段修改网站页面原始内容,添加恶意内容。比如我们所熟知的"跨站攻击"就是非常典型的篡改类攻击。当然,通过修改网站主页,添加各种违法言论也是篡改类攻击的主要表现。第三类,也就是最严重的一类网站攻击就是数据盗窃类。随着大数据技术的发展,网站或者各个关系国计民生的机构往往拥有大量的个人隐私数据和商业机密数据,数据泄露会带来极其严重的损失。例如2014年5月,美国著名电商网站EBAY发生的数据泄露事件就直接导致全球1.28亿名用户受到影响。而在2014年12月,中国发生的12306用户信息泄漏事件,由于适逢春运,更是在全国造成了不良影响。

根据国家互联网应急中心发布的报告,仅在2015年1月,中国境内被篡改网站就多达10455个,其中被篡改政府网站数量为376个;被植入后门的网站数量为3976个,其中政府网站237个。

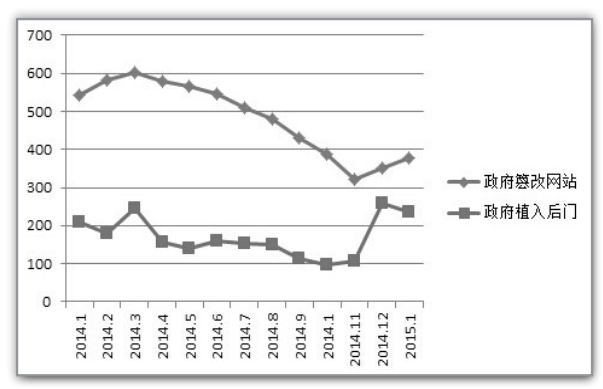
另据权小文介绍,在2013年公安部组织的一次针对政府网站的专项检查行动中,远江盛邦承担了总共12700个政府网站的检查任务,占总比例的25%。经过持续3个月的检查,结果显示,70%左右的网站存在不同程度的安全漏洞,其中有40%左右的网络漏洞可以被攻击和利用(意味着可以控制网站、修改网站网页等任意行为)。2014年10月,360公司通过全球互联网安全监测中心发现,全部的76981个政府网站中,有漏洞的网站仍然高达41080个。

同样,在国家互联网应急中心的安全通告中,政府类网站篡改每月有数百起,并且针对政府类网站后门植入有所增加。

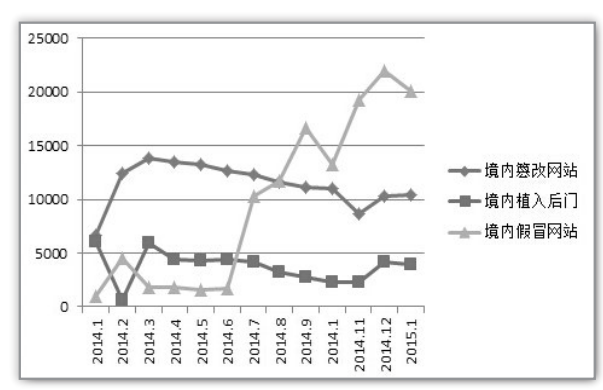
针对这一严重情况,党和国家都给予了高度重视。2014年网信办成立伊始,就发布了《关于加强党政机关网站安全管理的通知》。该文件明确指出必须强化党政机关网站应用安全管理(第四条),并且强调要运用"网页防篡改、网站防攻击"等先进技术为党政机关网站提供安全保护措施(第七条),该文件从安全的角度,分析党政机关面临的问题,并给出了解决问题的明确方法。



2014年10月国内政府网站安全情况



2014年政府网站被恶意入侵趋势图



2014年国内网站被恶意入侵趋势图
(数据来源:CNCERT/CC国家互联网应急中心,360公司)

记者管窥

活力在民间 创新有后劲

信息安全领域的竞争是高科技的竞争,是人才的竞争,更是国家产业的竞争。在这个战场上活跃着很多力量,其中有大型国企,也有高校、研究院等科研机构,还有许多上市的大型企业,它们构成了我们今天信息安全战场的中坚力量。毋庸讳言,在与欧美发达国家的竞争中,我们今天在技术能力上仍然处于相对落后的位置,导致这种局面的一个重要原因就在于,市场的参与主体太少,创新能力严重不足。依靠少数"国家队"和上市公司无法为我们带来足够的创新能力。这一点在美国硅谷也得到了证明,大量的创新都是来自于中小规模的初创企业而不是传统意义上的行业巨头。这些创业企业对用户需求非常敏感,而且具备非常强的学习能力和极强的创新能力。他们的创新成本和试错成本都远远低于大型企业和机构,而创新的节奏又远远超出了传统企业,凭借着快速的迭代开发,往往可以令其产品以极快的速度成长起来。

中国人从来都不缺聪明才智,我们拥有世界顶级的科学家和工程师,在信息安全领域更是如此。全世界排名靠前的安全企业中活跃着大量的中国人,他们也往往扮演着核心角色。现在,国家鼓励自主创新,制定了大量的优惠政策,都在为远江盛邦这样的小型企业提供便利,并且通过各种基金进行大力扶持。正如权小文所说,"我们有信心做出国际一流的产品,我们自己也要成为国际一流的公司,打造国际一流的安全品牌。"

一群"70后"和"80后"年轻人,正怀着极高的创业热情,投身到科技创新和产业报国的伟大理想实践中。应该说,权小文和他的同伴们,只是众多创业青年的一个代表,他们拥有的是科技时代推动变革的伟大力量。目前,在北京中关村乃至全中国,这样的创业型安全团队还有很多。虽然他们大多规模较小,名不见经传,但他们才是中国网络安全领域创新力量的源泉。我们必须充分发挥中国在智力资源方面的优势,尽可能地创造有利条件,让他们充分释放创新能力和创业激情。只有如此,我们才能够凭借创新、凭借自主可控的产品和技术,打造我们在信息安全领域的新的长城。