“思科阴谋”启示:针对性调查应立即展开

在指责美国动不动以“国家信息安全”为由制造贸易保护的同时,中国的“国家信息安全”建设如何完善也被提上了日程。

本报记者 **郭奎涛**

日前,思科希望通过国会遏止华为、中兴进军美国市场的企图遭到曝光,思科产品的安全漏洞及其引发的安全事故也被一并挖了出来。

数据显示,自1994年进入中国的20多年间,思科已经遍布中国金融、航空、固网等各大通信领域,中国市场为思科提供了3%—4%的全球收入和30%的全球利润,但是在思科高昂的产品价格并没有换来中国高度的安全保障。

中国网络安全专家纷纷建言,中国应该立即展开对思科通信系统安全状况的调查工作,并进一步建立完善的通信安全审查制度以及相关法律法规。

思科阴谋遭曝光

10月8日,美国众议院情报委员会发布了一份认定华为、中兴可能危害美国国家安全的报告。这一举动无疑宣告两家公司在美国的多年耕耘即将付诸东流,业内一直猜测市场竞争对手思科就是这一事件的幕后推手。

三天之后,《华盛顿邮报》从接近思科的匿名人士那里获得一份7页的《华为与国家安全》的调查报告,暗指思科以国家安全为由参与游说国会,推动后者开展对华为的审查。

对此,思科高级副总裁兼总法律顾问Mark Chandler发表说明文章,声称上述文件仅根据情报委员会的要求,提供了有关早前思科与华为知识产权诉讼案的公开信息。

不过,这份声明却真实地证实了7页文件的存在,李开复更是在微博上直点思科表述漏洞,“说这篇报道误导(别篇呢?),没有向安全小组游说(别的小组呢?),没有提供某一份市场文件(别的文件呢?)。”

来自《华尔街日报》美国公开政治中心的数据显示,美国525名国会议员之中,有73位投资了思科。非营利机构Opensecrets的统计数据也表明,在美国众议院情报委员会启动对华为、中兴调查的2011年,思科的游说支出创下最高纪录,达到280万美元。

市场人士指出,华为、中兴两家设备商已是全球第二和第四的设备商,假如有问题,美国国会早应在调查报告中指出。作为竞争对手虎视眈眈的思科,也会及时地发现并举报两家设备商可能存在的漏洞。但是,双方至今也没有出具过硬的证据。

不过,美国国会左手拿着“有可能”一词,右手怀揣美国1996新通信法,还是对华为、中兴发起了第二轮调查。

据悉,在最近的十年间,华为和思科的力量正发生着巨大变化:思科的年销售额10年只增长了一倍多,2011年底,市值跌破1000亿美元,不足高峰期的1/5。而华为年销售收入增长了7倍,高达1852亿元人民币(280.6亿美元)。

分析人士认为,假如华为进入美国市场,思科的利润恐将缩水1/3。

安全事件频发

令思科意想不到的是,此事不仅没有查到华为、中兴的安全问题,这一非法竞争反而将自身陷入了众叛亲离的地步,思科编织的安全漏洞及其引发的安全事故也被相继挖了出来。

2005年7月12日,承载着超过200万用户的北京网通ADSL和LAN宽带网,突然大面积中断。对此,北京网通负责人称,网络中断的原因是互联网路由器的原因。而自中国互联网骨干网从架网开始,大部分使用的都是思科的路由器设备,包括硬件和软件。

2010年的黑帽大会上,IBM互联网安全系统公司的研究人员Tom Cross论证说,黑客可轻易地利用思科IOS操作系统中的后门,在忘记密码的情况下,通过恢复系统的出厂配置对路由器进行管理配置,这会将整个网络都置身于不可预知的风险中。

更令人想不通的是,在现有思科路由器产品中,仍然在使用上世纪70年代的加密算法DES(data encryption standard,数据加密标准),这种算法已经被多次证明不再安全,能用穷举搜索法对DES算法进行攻击。即使一台普通的PC机,也能够在10分钟内完成DES算法的破解。

更为糟糕的是,思科居然在OSPF协议设计中也使用了这一极其脆弱的DES算法,来实现协议报文的认证。那么,如果一个人希望看到某个人的账号口令的明文,他只需要在OSPF协议口令设置时,把这个人账号口令的密文件作为OSPF协议的密码,通过在网络上抓包,就能够截获出用户的明文口令,进而造成密码泄露。

2012年7月2日,一位匿名用户在科技资讯网站slashdot上发布讯息称,思科Linksys路由器产品E2700、E3500、E4500三种设备远程更新固件,监控用户网络使用情况。

网络安全专家、中国工程院院士方滨兴认为,一般来说,与电脑软件类似,只要是连在网络上的设备,包括计算机、服务器、路由器等网络上的运行设备,如果留有“后门”,那就会有风险。通过“后门”,可以将网络设备中的信息自动获取,并发送给后台。

实际上,在网络世界“后门”无处不在。比如微软操作系统的“自动更新”功能,正是通过“后门”程序来实现的。不同的是,微软的这种“后门”是得到用户认可和公开进行的,而思科的这种“后门”则是在用户根本不知情的状况下暗中进行。

国家信息安全待加强

在思科产品设备存在安全隐患的背后,则是从1994年进入中国至今,在金融行业,中国四大银行及各城市商业银行的数据中心全部采用思科设备,思科占有中国金融行业70%以上的份额;在海关,公安、工商、教育等政府机构,思科的份额则超过了50%;在铁路,思科的份额达到了60%;在民航,空中管制骨干网络全部为思科设备……

尤其重要的是,中国电信163和中国联通169是中国最重要的两个骨干网络,两者承担着中国互联网80%以上的流量。思科一家占据了70%以上的份额,把持着所有的超级核心和互联互通节点。

“如此高的市场份额掌握在一家美国公司手中,这意味着国家信息和公众信息安全对思科来说几乎是透明的,这对于整个国家战略信息安全更是致命的。”业内人士评论说。

近年来,随着我国信息化进程不断加快、信息基础设施进一步扩展、信息系统、通信网络应用日益普及,关系国计民生的行业、部门、机构越来越依赖于信息网络系统。这也对中国如何加强国家网络安全建设、提高国家网络安全意识,提出了更高要求和新的挑战,而美国封杀华为事件,无疑为我们敲响了“国家网络安全”的警钟。

“如为网络安全立法、对现有网络设备的更替以及对现有网络的安全审查等,都是可行的方法。比如这次联通公司对江苏无锡节点思科设备的成功搬迁,虽然只是一个节点,但也是一个良好的开始。”互联网专家方兴东这样评价中国联通无锡节点搬迁工程。

近日,中国联通成功完成联通China 169骨干网江苏无锡节点的核心集群路由器搬迁工程,这是业界首次对思科CRS集群路由器的搬迁工程。

美国是世界上最早建立和使用计算机网络的国家,也是信息产业发展最为迅速的国家,信息安全一直居于美国国家安全战略的高度。早在十年前美国便公布了《网络安全国家战略》以及《确保信息安全的国家战略》,确定了3个战略目标和5项优先行动,并通过为信息安全立法,来完善保障信息安全法规体系。据悉,近年来美国相继制定了《信息自由法》、《总统档案法》、《联邦信息资源管理法》、《国家信息基础设施保护法案》、《反电子盗窃法》、《计算机犯罪强制法》等一系列法律法规,以确保国家安全。

在中国,国外软件可以用在哪儿、什么地方必须使用国产软件、什么机构除了做好网络安全还需要物理隔离,对于这些问题的管理策略,国内目前还没有机构对此类问题做出统一规定。因此,保障通信安全应建立审查制度,从设备采购为始,对设备进行严格的审查,以长期监管维护为终,进行系统的定期审查,才能保障中国网络信息安全,毕竟高价代表不了绝对的高安全。

中国政法大学副教授吴丹红指出,中国在保护国家利益和本土的经济利益时比较软弱,缺乏应有的重视,在关系国家网络和信息安全问题上,不应再拖延,应立即开展对思科相应的调查工作。

社址:北京海淀区紫竹院南路17号 邮编:100048 账号:10282000000248270 开户行:华夏银行北京车公庄支行 户名:《中国企业报》股份有限公司 电话:68485798(总编室)68701500(办公室)68425077(地方工作部) 工人日报社印刷厂印刷