中国信息化周报/2017 年/8 月/28 日/第 007 版
趋势

我国网络空间安全态势分析与应对

中国工程院院士　方滨兴

当前,网络空间安全已经成为国家安全的核心组成部分,并在经济和社会发展的关键环节和基础保障方面发挥日益重要的作用。和我国网络空间快速发展形成鲜明对比的是网络空间安全保障能力的不足,人民群众对网络社会进一步发展的迫切需求和现阶段网络空间安全治理能力有限之间的矛盾已经成为影响国家安全和经济社会发展的重大问题。

当前网络安全事件的态势

目前,各种网络安全事件频发,令人疲于应对,网络安全态势逐渐趋向恶化。

1.大规模攻击日趋频繁。大规模攻击的形式主要包括拒绝服务攻击(DDoS)、域名解析服务器(DNS)劫持等。如今最大的 DDoS 攻击规模已比几年前高一个数量级,因 DDoS 攻击而导致的大规模网络瘫痪事件日益严重。针对 DNS 进行劫持攻击,可导致两方面的危害,一是网页无法正常打开,另一方面攻击者将正规网站劫持到钓鱼网站上,诱骗用户登录,既可以造成个人的信息泄露乃至财产损失,也可以对被攻击网站造成经济损失和相应厂商的名誉损失。

2.大量用户信息数据被窃取。大型企业特别是互联网企业拥有巨量的客户数据,一旦系统被入侵,很容易造成大规模的客户隐私信息泄露事件,不仅会对用户的财产安全和隐私安全构成威胁,也将对企业的声誉造成负面影响。近年来,大规模的用户隐私泄漏事件频频发生,其手段多样且结果严重。同时,大部分的用户隐私信息在窃取之后被卖给地下市场,从而造成更大的安全隐患。

3.涉密内网主机屡见被植入后门。CNVD 曾发现 D-LINK、Cisco、Linksys、Netgear、Tenda 等多家厂商的路由器产品存在后门,黑客可由此直接控制路由器,进一步发起 DNS 劫持、窃取信息等攻击,直接威胁用户网上交易和数据存储安全,使得相关产品变成随时可被引爆的安全"地雷"。很多企业内部的重要机密也可以通过这样简单的方法实现窃取。

4.重要网站内容持续被篡改或者被攻击。境外"反共黑客"长达五年持续不断地每三天攻击一个具有中国政府背景的网站,并将反攻标语涂改在被攻击的网站页面上,以求达到诋毁中国共产党的政治影响。

5.网络安全高危漏洞频现。网络设备、计算机系统,甚至智能联网设备的安全漏洞问题严重,修复进度未跟上步伐,黑客可以绕过访问控制来从中获利,甚至进行金钱敲诈。风靡一时的"想哭"勒索病毒利用的就是已经公开的安全漏洞,中招的就是那些没有及时打补丁的用户。

6.移动互联网恶意程序数量仍大幅增长。大量移动恶意程序的传播渠道转移到网盘或广告平台等网站,应用软件供应链安全问题凸现,导致人们常常因下载应用软件而感染上恶意代码。

7.网页仿冒事件数量暴涨。仿冒事件主要是利用钓鱼网站来进行欺诈。目前来看,针对金融支付的仿冒页面数量上升最快,其通过仿冒某一金融机构的主页,诱惑用户点击,从而可以盗取用户银行账号、密码以及其他信息。

未来可能成为热点的安全事件

随着网络空间安全形势不断恶化,各种新的网络攻击形态也将会不断涌现,一些新的攻击模式将会变成热点,需要人们加以警惕。

1.路由扰乱致瘫威胁。针对路由器的攻击方式主要分为两大类,一类是利用漏洞或后门获取路由器系统权限后种植僵尸木马;另一类是获取路由器管理权限后篡改默认的 DNS 服务器设置,实现 DNS 劫持。另外,攻击者还可以发布错误的路由信息,造成回路、重定向等错误路由,从而降低了网

络性能。

2.云计算平台所存在的安全问题。在云计算平台发挥巨大作用的同时,也引发了新的安全问题。一是计算平台的安全问题,主要表现在云平台自身的冗余度与鲁棒性不够而引发的灾难性崩溃。二是云计算平台被黑客攻击的问题,主要表现在虚拟机安全方面。攻击者通过突破虚拟机管理中间件来获得宿主机操作系统的权限并实施控制。三是云服务商自身的可信问题,主要表现在数据安全方面。由于云服务商的内控手段不足,而云计算平台管理者的流动性较强,从而具有侵害云计算平台用户利益的动机,有可能擅自收集云用户的信息。四是云计算平台被恶意滥用问题,主要表现在内容安全方面。这是因为云计算平台缺乏对云租户的管理手段,使不法租户利用云计算平台来做恶,将之作为有害信息和垃圾信息的传播渠道,给国家安全带来新挑战。

3.互联网流量容易受到外部监控。目前流量劫持手段已经形成多样化的态势,攻击者可能会通过监控某一个企业的通信行为来为其将要进行的 APT 攻击进行前期的信息采集,该类攻击组织的目的也不仅仅是金钱,还将包括窃取政治机密、科研秘密等。

4.瘫痪工业控制系统。随着工业控制系统与互联网+的结合,其安全问题也逐渐浮出水面。工业控制系统主要存在以下问题:一是传统安全手段不适用于工控网络;二是网络工程师与工控工程师的融合困难;三是针对工控系统的攻击的防御点不是工控防火墙,而是在 PC 侧,是在上位机;四是难以保障物理隔离的有效实施,内部有意无意的配合将是更大的风险所在。

5.基础网络 IP 化和智能化导致工作异常或瘫痪。IP 网络各种各样缺陷的不断地累积,网络的节点数和拓扑数量越高,其薄弱点也就越多,潜在的风险就越大;同一网络承载多业务,导致安全风险的互相影响;网络和业务的分离,导致业务层面不能全面考虑网络资源而滥用网络资源。

6.大数据安全问题将会引起社会的关注。大数据安全主要涉及的是隐私保护,具体表现在三个方面:一是数据发布过程中的匿名保护不够到位,攻击者可利用多种渠道获取数据;二是数据自身安全带来的信息泄露问题,传统安全产品所用的技术手段在大数据环境下不能有效发挥作用;三是大数据技术的挖掘能力使得用户隐私无处逃遁。

建设新一代国家级网络安全应急体系

没有网络安全,就没有国家安全,构建新时期中国网络空间安全事件应急体系已经成为当务之急。

1.指导思想。建立完善的应急响应体系,要从治理、管理、技术等角度全面提升应急保障的核心能力。一是从治理角度来说,要建立必要的应急组织,包括常设的国家级的应急协调机构;要解决机构分散,职责重叠交叉缺位,缺少统一协调管理的问题;要建立多方参与的协作机制,吸引各种社会团体参与应急响应工作。二是从管理角度来说,要尽快完善网络安全相关的法制制度,形成有效的网络安全法律规章制度体系;三是从技术角度来说:要加速基础技术与相关标准的研究,加快网络核心信息技术装备国产化的步伐。

2.法律规范。国家应该尽可能地在政策、资金、税收等方面促进具有民族网络产业的快速发展,为国产网络设备和软件开发打好基础,从本质上防范网络安全事件的发生;建立防止数据泄密的信息安全保障制度,建立网络信息安全审查制度和反恐监控制度。

3.工作体制。一是要建设完备网络安全应急组织体制,包括成立国家层面的应急指挥协调机构;二是要加强网络安全应急队伍的建设,成立网络安全应急人才培训基地;三是要加强社会教育,加大对社会的网络安全应急宣传普及教育力度。

4.技术措施。要构建应急处置的技术体系框架,建设自动化、智能化的主动防御体系。要加强应急响应技术研究,包括操作系统加固优化,网络陷阱及诱骗、阻断、入侵检测,事件隔离与快速恢复等技术;要加强网络应急安全演练工作,构建网络安全应急的商业模式。

(本文根据方滨兴院士的演讲内容整理而成,未经本人确认。)