·科技工作大家谈·

文/杨义先

# 全球信息安全的六大战略错误

科学家被认为是人类最聪明的群体之一。而在人数众多的科学家群体中,信息安全专家则被认为最善于彼此"对抗"。但正是这批"人精",在保卫信息安全方面,却常常"好心"办"糊涂"事,使得赛搏空间秩序大乱,日甚一日"危机四伏"(注:赛博空间,Cyberspace,是哲学和计算机领域中的一个抽象概念,指在计算机以及计算机网络里的虚拟现实)。

据此,笔者列举了全球信息安全界的6个代表性"战略"错误:

**(1)最基础的错误——忽略了"返祖"现象。**构成赛搏空间的所有要素(计算系统、存储系统、传输系统、采集系统等)都是人类文明精华的最先进成果,按惯性思维,自然认为赛搏空间最"文明"。然而,实事上,赛搏空间可能是最"返祖"的样板,在这里,文明社会的最基本准则(道德准则、关系准则、秩序准则)被打乱,"弱肉强食"变得司空见惯,"损人利己"貌似天经地义,"损人不利己"甚至"损人损己"的事情也比比皆是。

因此,要想保卫赛搏空间的"生态"安全,必须返璞归真,由"丛林法则"开始,踏踏实实地重建赛搏社会的"生态"文明。

**(2)最致命的错误——过度信任用户。**当今,所有信息安全技术的建立都以"用户是好人,一定会遵纪守法"为初衷与前提,只有当确认某款软件干了"坏事"后,才把它定为恶意代码,才开始对其进行封杀或补漏;只有当某个用户已被证明危害了安全后,才将其定为黑客,才开始对他进行应急处置等。如果这种"挽救"式的思路与做法得不到根本改观,那么,全球信息安全专家们将永远处于疲于奔命和被动挨打的状态。

当然,由于历史欠账太多,我们也不可能一夜之间就把思路调整为"人之初,性本恶"的有罪推论,毕竟现在的绝大部分信息安全技术和手段都主要处在"亡羊补牢"的"消防队"的阶段。

**(3)最受累的错误——网民被"水涨船高的怪圈"绑架。**当前信息安全界的逻辑是:当个别黑客的"魔"高一尺时,全体网民的"道"就必须再高一丈,如此循环往复,永无止境。犹如全体网民都被逼进了"露天电影场",因为有人"站立",便导致后面的人永远要比前面的人站得高。为什么网民们不能舒服地坐着享受电影呢?我们也许会罗列许多理由来辩解这种无奈现象,比如,信息系统越来越复杂、黑客技术越来越先进等,网民必须为信息安全付出应有的代价。猛听起来,这种"叫屈"好像有道理,但在现实社会中,确实存在一些案例能够打破这种"水涨船高"的效应。

但愿网民们不再夜夜为自己的信息安全"做恶梦",但我们真能打破"水涨船高怪圈"吗?必须承认,我们至今还无计可施,但世上无难事,杜绝"露天电影效应"的办法有2个,其一,"放映"效果足够好,使每个人都能清晰地享受,这样就不会有"站立者"了;其二,对"站立者"严惩不贷。

**(4)最"仁慈"的错误——未组建信息安全别动队。**现在信息安全界就像选用了一个股民来担任"美联储"主席,灾难性的后果可想而知。事实上,当前,国内外信息安全领域"攻"与"守"几乎都是同"一伙人"。"矛"与"盾"成了摆设,这更加剧了各利益方的"博弈",殃及全体网民。如果有一支网络"联合国维和部队",恪守中立、不辱使命,尽心尽力、一视同仁地为全世界信息系统"保驾护航",那网民们的安全指数将倍增。

所幸,这样的"别动队"现在已经开始活跃于赛搏空间的某些局部,比如,出现了SAAS概念,即,信息安全即服务。希望这支"部队"更加训练有素,日益壮大。

**(5)最具体的错误——黑名单管理。**当前,赛搏空间行事规则是:非禁止,即允许。该规则在信息安全的攻防双方是通行的,好处是极大扩展了各自的创新空间,但是,却耗费了对抗双方难以数计的人力、物力和财力等资源。如果把安全规则修改为"白名单"管理方式,即,未被允许的指令均为禁令,那么,理论上,只需要由权威机构,在给定环境下,预先测试某些操作的安全性,然后,将安全操作写入"白名单"中就可。

当然,要想马上、全面启动"白名单",似不现实,但从局部起步,针对某些关键系统的核心操作,采用"白名单"管理模式值得尝试。

**(6)最机械的错误——动态性不足。**如同现实社会,赛搏空间的"人"(实体)和"事"(进程)瞬息万变,网络社会的移动性、隐蔽性、不定性尤为凸显,因此,既不能简单机械地用身份认证的方法,把用户分为"好人"或"坏人";也不能把各种操作,简单机械地定为"合法"或"非法";更不能"以不变,应万变",必须要综合考虑时间、空间、事件等因素。当然,要想提高动态性,一定得付出足够的努力和相应的"代价"。

因此,针对一些特定的信息系统,在特殊情况下,完全可以借用现实社会中的思路,用时间的动态性、空间的动态性、事件的动态性等来"换取"赛搏空间的安全性。

客观公允地说,以上6个错误不能完全归咎于信息安全界,因为,IT界的"过度"创新和"失误"留下了太多的遗憾和急需弥补的漏洞,使得我们仓促上阵,马不停蹄,只得头痛医头,脚痛医脚,没有足够的时间和精力来更加精细地运筹帷幄,统筹战略。作为信息安全专家,我们没有能力和机会介入赛搏基础设施的起步阶段,致使建设与安全始终是"两张皮"。对于如何纠正上述6个错误,也绝不仅仅是某一部分人的责任,更重要的是全体IT专家必须行动起来。"纠错"将是长期难题,但不能另起炉灶,目前的切入点,是在特定情况下,从局部改起。

**作者简介**　杨义先,北京邮电大学信息安全中心主任,教授、长江学者。

本栏目专门刊登就促进科学技术发展提出的意见和建议,欢迎国内外科技工作者投稿。

(编辑　祝叶华)