核心提示

□据 新华网(记者 罗争光 俞菀 周慧敏)

近日，国内最大的开发者社区600余万个用户邮箱账号和密码被泄露，现实版“黑客帝国”引发网络安全集体恐慌。此后不久，天涯论坛、新浪微博、人人网、开心网……众多知名网站相继陷入“密码疑云”。

专家指出，接入互联网的数据信息，理论上都有遭到技术破解的风险，但此次互联网公司数据信息集体“走光”，直接拉响了互联网公司信息安全的“红色警报”。网络信息安全可否绝地反击筑起更多“防线”？记者就此展开调查。

现实版“黑客帝国”引发网络安全集体恐慌

“密码疑云”下，网络安全“防线”缘何轻易“溃堤”

绘图 玉明 吴芳

【陷落】 知名网站集体陷入“密码疑云”

12月21日，国内最大的开发者社区CSDN.NET用户密码遭黑客泄露，涉及600余万个注册邮箱账号和密码，CSDN官方确认并公开道歉。

然而，CSDN仅仅是一个开始。此后不久，包括人人网、开心网、多玩、世纪佳缘、珍爱网、美空网、百合网等10多家国内知名网站也被报道存在类似泄密问题，超过5000万个用户账号和密码在网上被公开扩散。尽管人人网、开心网、7K7K等均对此予以否认，但密码外泄的“流感”一时使互联网服务公司和用户人人自危。网友“小龙变肥龙”说：“用户密码只是拿去发垃圾邮件也就算了，如果去干坏事，那后果真是难以想象！”

12月26日，天涯社区被报道约有4000万个用户的密码遭泄露，天涯社区随后发布致歉信证实了部分用户隐私遭黑客泄露的事实。

新浪微博用户密码亦疑遭泄露。根据网友提供的信息，泄露文件显示的用户数据涉及4765896名微博用户，随即验证其中的用户名、密码的确可以正常登录新浪邮箱或新浪微博。新浪公司很快对此予以否认，并紧急提醒用户进行账号安全设置。

随着疑似泄密的范围扩大，多数用户被网站要求重新设置密码。一些网民开始尝试“回避”风险，希望注销自己在各网站上的账号，却发现想要彻底注销还真是件难事，很多网站都没有“注销账号”这项服务。

【分析】 网络安全“防线”缘何轻易“溃堤”

“这次意外事件，虽然不是针对我们一个网站，但给整个互联网行业都敲响了警钟，提醒大家要重视网络安全，同时也提醒用户及时更新数据，加强自我保护。”业内人士初蒙说，互联网公司集体“落难”，说明互联网安全还有很大漏洞，安全隐患普遍存在。

那么，网络安全“防线”到底能不能发挥作用？国家信息安全工程技术研究中心主任文仲慧坦言：“随着网络应用环境日趋复杂，企业核心数据被盗、用户数据丢失等事件频发，互联网用户信息被盗可以说已经司空见惯，甚至许多人信息被盗了还浑然不觉。”

在专家看来，互联网用户账号、密码信息被盗现象在全球范围内屡有发生。今年4月，日本索尼公司约1亿名PlayStation Network网络账户遭到黑客攻击，该公司被迫关闭PlayStation Network近1个月，引起全球高度关注。在国内，黑客利用网站服务器的安全漏洞侵入，盗取用户数据库等信息，然后私下进行传播、倒卖，已形成“灰色产业链”。

互联网安全企业“奇虎360”公司副总裁石晓虹介绍，互联网的技术漏洞理论上始终是存在的，互联网公司数据一旦接入网络，相应的安全意识和安全措施不健全，就会增大泄密风险。目前一些大型网站普遍采用加密存储技术，数据即使被盗取也难以破解；而一些中小型网站则相对缺少防范意识，网站一旦被黑客攻破并窃取数据，就有可能引起严重的安全问题。

上海泛洋律师事务所高级合伙人刘春泉分析，互联网公司需要承担降低用户数据信息泄密的主要责任。“互联网公司首先必须做好员工管理工作，坚决杜绝内部员工主动泄密的情形，刑法修正案加入‘非法获取公民个人信息罪’，对此能起到一些警示作用；其次则是要做好用户信息数据的安全防护工作，包括技术投入和数据管理，提升数据保密层级。”刘春泉说。

【借鉴】 网络安全将筑更多“防线”

专家指出，网络信息遭遇黑客攻击，是一个世界性难题。不过，从国外关于网络信息安全的一些举措来看，或可为我国互联网行业提供一些借鉴。

比如，我国互联网企业在收集用户信息时太过随意，应当借鉴发达国家的“最少信息收集”理念，尽量减少对用户(客户)信息的收集。刘春泉介绍，韩国也曾发生过知名网站用户信息被大规模泄露的情况。事后，韩国政府要求，个人或企业使用用户身份信息时，需事先获得批准。只有在必要的时候，才可以进行信息注册和登记。这不仅降低了用户信息被盗的风险，也增强了事后追责的可操作性，企业在收集和保管这些信息时也会更加谨慎。

“而美国在处理类似事件时，往往倾向于惩罚性赔偿。”刘春泉说，“企业为了避免打官司，尽量不收集用户信息，即使最后发生了泄露事件，也会及时向社会发布相关情况，以减少更多损失。”

上海律师协会信息网络与高新技术业务委员会主任商建刚介绍，美国从今年起开始尝试推行《网络空间可信身份国家战略(草案)》，希望建立一个“允许用户在线交易时创建可信身份”的系统，保护个人信息安全。

“这其实就是建立一种‘身份属性供应商’渠道，犹如电子商务领域的第三方交易平台，当用户在网站进行登记、注册时，不需要直接向网站提供个人身份信息，而是由第三方提供身份证明，这样就减少了网络公司对用户信息的收集和保管，无疑降低了用户信息泄露的风险。这个过程中，网站实际上只需提供一个公共接口，让‘身份属性供应商’的信息能够接入，为用户提供身份验证即可。”商建刚说。