

行业中国(2013-08-05)



数据越重要 越要提升安全意识

2013-08-05 行业中国

随着互联网技术、移动终端发展迅速，全球每日的数据流量不断提升，不论是浏览网站，或者是使用各Apps程序，都有可能留下用户的行踪及隐私。不少企业担心重要的数据外泄，对企业形象及实际利益带来重大损害。因此，我们必须提高网络安全意识，保障网络数据安全。

数据迈向消费者主导

留存在网络上的数据越多、越细致，越能反映使用者的日常习惯、行为，就像许多人每天必定使用的微博、微信以及Gmail等云平台或应用程序，背后都收集了大量的用户数据，从而优化使用者体验。例如微博能通过关注与粉丝的情况，实现好友推荐与淘宝的商品推荐；而Gmail则会根据用户的电邮内容，显示针对性的广告，可见网络数据的重要性不断提高。

之前网络的安全泄漏事故，多数是黑客所为；然而如今智能手机、移动终端，以及社交平台日益普及，许多数据、隐私都会不经意地从这些地方外泄，让不法份子有机可乘。



培养检查网络安全习惯

其实网络应用是中性的，有人利用它成为网络警察；也有人以此来欺凌其他受害者，最重要还是用户如何管理自己的隐私，培养检查网络安全习惯。个人用户应

尽量避免使用不熟悉的网络平台，或设定隐私限制，一般网络平台默认的安全模式为中等程度，用户可视乎自己的需要来调整安全程度。

企业应设立更加严谨的网络安全制度，保护商业机密数据，例如定期使用软件测试网络安全、定期更新网络安全软件；并且使用防火墙来加强安全程度。即使在云端环境下，也可选择以硬件或虚拟化软件来加强网络安全。

在保护数据方面，企业可以将网络服务器、数据库分开储存，避免一次性遗失所有数据。比如，关乎企业命脉的安全数据，可以存放在企业自己的机房里，而一些非核心部门的数据，则借助一些云存储平台。比如第一线集团的云端数据中心，也是可以考虑的。同时，企业可以使用密钥加密技术(Key Encryption Technology)，为重要数据进行加密，用户需拥有指定的密钥才可开启档案，即使数据外泄也不会轻易被破解。

避免在公用网络处理重要数据

除了一般的网络外，不少人喜欢使用智能电话、移动终端上网，许多户外地点也有提供免费Wi-Fi服务。由于这些公用网络多数没有为数据进行加密，所以用户使用这些网络时便要格外留神，避免处理重要数据。例如处理财务交易，或下载企业机密档案，避免黑客利用不同工具盗取这些数据。另外，移动终端用户也应安装及定期更新防毒软件，防止黑客入侵。