导语

云端数据存储不仅操作方便，而且应用免费，所以深受用户的喜爱。但在充分享受云存储带来便捷的同时，随之而来的云端数据存储安全也让人感到十分担忧，例如云端敏感数据对外泄露、上传数据被恶意修改复制等。为了让云端数据安全更有保障，本文提供了多种应对措施，用户不妨依照自身实际情况，来有选择性地采用。

让云端数据安全更有保障

■天津　张岩

云端数据面临安全隐患

伴随着虚拟化应用越来越普及，用户数据的存储位置、存放方式发生了很大变化，用户可以随时随地通过网络获取数据，这就使得传统的数据安全管理方案已经无法应对云环境下的安全问题。云端数据安全面临新的安全隐患，数据安全防护也要转换思路，更加有效地识别相关人及设备。

目前，云环境下用户的各类应用以及重要数据都集中保存在云端，由于云端自身合法原因（例如为了达到预防灾难目的，进行的不同位置备份），或不合法的原因（云平台有强制复制用户数据的权利），造成的云环境下数据可控性问题以及隐私外泄问题显得极为突出。重要数据集中保存在一个位置，容易吸引外网恶意用户和内网不怀好意人员偷偷窃取，例如与云端数据相关的云服务商、云平台、存储管理员以及第三方服务商对隐私数据的非法访问，上传到云端的重要数据被云平台厂商备份及利用，而且有的云平台在用户上传了数据后，连用户基本的彻底删除操作权限也被取消了，这让用户在想保护自己隐私数据时，显得无能为力。所以，在不影响单位或个人正常工作的情况下，确保云端重要数据不被无关人员非法访问，已经成为亟需解决的问题。

图1 美国FedRAMP

保护云端数据安全措施

虽然云端数据存储的出现给用户带来了极大的便利，但是用户在使用的过程中，可能还会遇到一些比如数据丢失、密码被盗等安全方面的问题。在此，本文为用户们提供了几种简单的应对措施，可以有效地保护云端数据的安全。

1. 选用安全可信平台

为了保护云端数据安全，单位用户必须要从云端平台产品的信誉度、安全性、易用性以及性价比等方面，选用安全可信平台。首先要关心云端平台服务提供商的信誉。可以先调查云端平台服务提供商的技术水平、服务历史以及相关软硬件产品的市场影响。同时还要调查它们的市场表现、客户评价以及服务能力，毕竟优秀的云平台服务商都有不错的市场影响，试着上网寻找有关的用户使用评论，有利于用户选择合适的云平台服务厂商。此外，对于追求7*24小时安全机制的用户来说，管理服务能力是又一重点考察对象。

其次要关心云平台服务提供商的安全认证能力。主要考

察云平台服务提供商有没有提供通过专业认证的技术，相关技术有没有获得厂商的官方支持，这些细节因素都会关系到云端数据存储的安全性。例如，美国的 FedRAMP 就是一个强制性的政府机构（如图 1 所示），它规范了云端存储认证的安全评估，能够通过该机构认证的云平台服务提供商，提供的云端存储服务自然也是安全可信的。

要提醒大家的是，很多著名的云端存储服务提供商都没有通过 FedRAMP 的认证，而在国内，可信云服务认证工作已由官方部门开启，阿里、腾讯、百度等厂商的云平台产品都顺利通过了这方面的安全认证，当然也有部分厂商的产品没有通过这种可信云服务认证。因此，用户一定要依照自身实际情况，选用通过官方认证的云平台产品。

第三要考察云平台的易用性。一些云平台无法让普通用户彻底删除相关重要数据，这往往会让他们感到十分不安，因为这意味着数据控制权的丢失。还有一些云平台产品包含有开源项目，可以让用户直观看到内部执行的过程，但是它的技术门槛很高，有时不适合中小规模的企业用户。

第四要关注产品的性价比。无论哪一种产品，不能单纯看产品价格，还要看所选购平台的功能和技术支持水平。要是云平台服务提供商为用户提供了价格相当低廉的云端存储服务，那企业用户应该更加关注它的服务细节和技术水平，以保证对方的服务能够真正落到实处。

2. 做好重要数据备份

当用户尝试将重要数据传输到云端平台之前，必须认真考虑当云平台服务提供商破产或用户决定退出该服务时，会有什么样的后果可能发生。最严重的后果自然就是无法找回自己的数据。为了避免这种问题的出现，最有效的办法就是及时对自己的重要数据进行备份，而且确保不管在什么时候什么地方都可以轻松获取备份内容。及时备份重要数据是帮助有着重要数据存储需求的用户解除数据丢失担忧的最佳途径。

3. 严肃认真对待密码

相信这样的建议，用户已经听过若干次，但显然并没有引起足够重视，所以还是要不厌其烦地提醒。大家知道，不法分子想要访问用户的隐私数据，必须要想方设法去窃取用户的账号和密码。但不少用户都有一个不良的习惯，不管什么情况，不管在什么位置，都喜欢使用相同的登录账号，甚至连登录密码都设置的一样，这自然就加大了登录密码对外泄露的可能。

那么存储有重要数据的云平台登录密码在设置方面有什么要求呢？怎样才能为云端存储加上一把牢固的锁呢？正常来说，在云端平台系统完善不存在安全漏洞的情况下，恶意用户通常会使用密码字典、暴力破解等方式破译密码，非法访问他人重要数据。想要给云端数据提供安全保护，那么就要让恶意用户不能轻易突破密码验证机制。换句话说，就是只要设置足够“强壮”的密码，那么不法分子就不会轻易破解密码了，除非云端系统自身有重大安全漏洞。如果用户在设置“强壮”密码的基础上，再使用二次验证，那么安全防护效果就会更好。

那么，怎样才能设置好足够“强壮”的密码呢？第一要增强密码复杂程度。类似生日、名字这样的密码内容，很容易被破解，只有将各种类型的字符混杂起来使用，才能增加黑客暴力破解密码的难度，例如用感叹号代替数字 6，￥符号代替数字 2 等，密码内容组合越复杂、位数越长，那么它被成功破解的几率就会越小。而且，在设置密码内容时，不要让密码位数低于 12 位，不要使用

与登录账号关联的密码，不要以英文单词作为密码，不要使用连续相同字符的密码，不要将单位管理者个人信息作为密码。

第二，要定期修改密码内容。强度再高的密码也容易被人偷窥到，定期修改密码内容，可以避免偷窥带来的安全风险。一般来说，如果用户有经常更换强密码的习惯，被破解的可能性可见是极低的。但扪心自问一下，有多少人会自觉定期修改密码内容呢？而到了必须调整密码内容的时间，是不是有用户仅仅调整个别字符来应对密码策略的强制要求呢？对于单位来说，要强制员工定期修改密码，必须加强对他们进行培训，让他们意识到强壮密码的重要性，以及定期调整密码内容的原因。作为密码策略的一部分，单位管理者也能借助第三方工具，来禁止员工使用相同或相近的密码应付密码策略强制要求。

第三，要注意不同场合使用不同密码。不要在任何场合下，让一个密码“走天下”，这样在遇到安全威胁时，可能会带来连锁反应。现在用到密码的场合很多，用户不能图一时方便，而将所有密码内容都设置成一样的，不然的话恶意用户在一处得手，那么在其他地方就会一路绿灯，这是因为恶意用户会首先用已窃取到的密码，去破译其他位置处的密码内容。

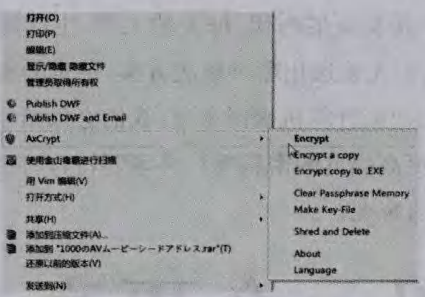

图 2 AxCrypt 工具

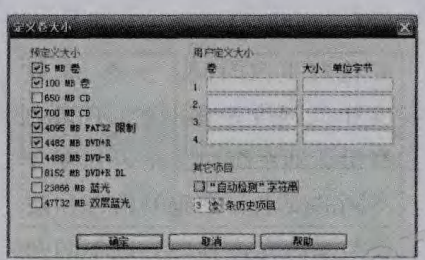

图 3 设置界面

4. 善于使用加密措施

不管这种措施是否可行，它都是目前为止保护数据安全最直接的方法。一般情况下，当用户需要上传重要数据到云端平台时，可以借助专业工具为目标数据文件创建密码，之后将设置了密码的数据文件传输到云端平台，这样在云端的数据如果没有用户的访问密钥，别人是打不开的，这就相当于为数据文件多加了一份保障。例如，用户可以在“AxCrypt”专业工具的帮助下，通过如图 2 所示菜单中的“make key-file”命令为重要数据生成密钥文件，再通过“GnuPG”工具为密钥文件加密，最后将数据文件和密钥文件分别上传到不同的服务平台中，这种加密方式至今为止无人能够破解，但它也有明显缺陷，操作起来相当麻烦。

此外，用户也能选择可信第三方对用户颁发证书，用户对重要数据文件进行数字签名加密后，传输到云端平台，确保其他人无法对其解密。该加密方式虽然也很安全，但是它的加密解密速度较慢，加密灵活性也比较差，无法对不同数据文件采用不同密钥内容。

值得注意的是，一些证书企业制作数字证书的过程不很透明，证书企业在生成并交付用户私钥的过程中，存在偷偷备份证书私钥的可能，因此大家在选择证书颁发机构时，必须要选用值得信任的机构，例如可以选用大多数企业首选的 VeriSign 数字证书。

当然，如果用户嫌上述加密措施操作起来麻烦，也可以直接选用一些云平台自身提供的本地加密【下转第114页】

导语 现在我们生活在一个身份验证的时代，每天的工作、生活都离不开身份验证。而身份验证的解决方案也是越来越多，但无论选用哪种解决方案，基本的密码／账号组合验证方式不可或缺。为了增强被非认证的用户或计算机破译难度，我们必须给密码一个更高的“强度”。不过，哪种类型的密码才能看成是更高强度的密码呢？必须要符合哪些条件呢？我们该怎样避免由于密码内容过于复杂而容易遗忘呢？

给密码一个更高“强度”

■江苏 孙秀洪

高强度只是个神话

所谓密码强度是指一个密码被破译的难易程度，密码强度可以分为低强度或高强度。低强度密码包括系统默认密码、常见的密码以及其他一些短密码，这些密码一般由某些具有固定特征的词组成，比如人的姓名、字典里的单词等，这些内容容易被轻易猜出或快速破解。高强度密码一般长度足够长，排列随机，猜出或破解需要花费更多时间。当然，高强度和低强度是相对的，不同的身份认证系统对于密码强度有不同的要求。密码的猜译和破解与系统允许客户尝试不同密码的次数、是否熟悉密码主人等因素相关；然而，即使强度再高的密码也有可能被猜译和破解。

为了增强猜译和破解难度，用户在设置密码时，一般都喜欢遵循字符复杂化原则。按有关标准要求，一个高强度、复杂化的密码所包含字符应该不少于12个，管理员级别的密码字符数尽量要达到15个字符。很多人或许会对这样的字符长度感到头疼，不过这已经是最近几年来美国国家标准与技术研究所推荐的长度中最短的了，所有长度不达要求的密码都会被认为是不安全的。

【上接第113页】 和解密服务。换句话说，就是用户可以尝试使用云平台自身服务加密重要数据文件，然后安全地将加密数据上传到云端平台进行存储，这将为用户的云端数据安全添加一份更为可靠的保障，因为连云平台提供商也不能轻易访问加密数据。

5. 重要数据碎片存储

所谓碎片存储，就是使用外力工具，将重要数据分割成若干个碎片文件，再将不同的碎片文件上传到不同的云端平台进行存储，例如一个存放到腾讯云，另外一个存放到百度云中。这样，即使其中某个云平台服务提供商想非法访问用户的重要数据，它只能获取到不完整的碎片文件，不能访问到具体的数据内容，这样用户就不用担心重要数据被人私下使用、备份、拷贝、编辑了。

将特定数据分割成碎片文件，操作其实很简单，只要通过常见的“WinRAR”程序就能轻松做到。只要在压缩数据文件时，进入“WinRAR”程序的压缩设置对话框，点击“默认卷大小”按钮，切换到如图3所示的设置界面，在这里输入适当的数字即可。一般来说，输入的数字大小与被分割数据的尺寸有直接关系，正常将数据文件分割成三个碎片文件，每个文件大小应该为原始数据尺寸的1/3。N

阅读此文的还阅读了：

1. 如何保障云数据安全?
2. 有备无患 数据安全有保障
3. 安全治理云数据——安华金和保障云端安全
4. 我存在云端的数据安全吗？
5. 你的“云端”还安全吗?
6. 云端数据存储安全
7. 江南天安助力阿里云保障云端安全
8. 用持续改进以保障数据安全
9. 保障小型数据库的安全
10. 云端数据存储安全
11. @欢乐的云端之上:#机务人员人身安全保障#
12. 备份——数据安全的有效保障
13. 云端数据治理初探
14. 无云端读取本地数据
15. 云端数据存储安全
16. 存在“云端”的数据牢靠吗
17. 保护云端数据安全的三种方式
18. 让云端数据安全更有保障
19. 你的“云端”安全吗？
20. @欢乐的云端之上：#机务人员人身安全保障#
21. 数据未来智胜云端
22. 让云端数据更安全
23. 保障移动“云”中数据的安全
24. 一种面向云端存储的大数据安全审计框架
25. 云端数据库安全问题

26. 数据砌成的安全保障

27. 门禁系统为医院保障数据安全

28. 后棱镜时代对云端数据安全的思考

29. U盘加密又隐藏 数据安全有保障

30. 云端数据治理初探①

31. 浅析企业让云端数据更安全的解决方案

32. 大数据的基础安全保障

33. 会计电算化下的数据安全保障

34. 安全可控在云端

35. 为什么要把公共安全数据存入云端

36. 云计算环境下的数据安全保障

37. 我存在云端的数据安全吗？

38. 北森iTalent捍卫用户云端数据安全

39. “用大数据保障数据安全”

40. 硬盘播出系统的数据安全与保障

41. BakBone保障重钢数据安全

42. 保障IIS数据安全

43. 保障数据安全四法

44. 四招保障数据安全

45. Imperva:保障大数据时代数据安全

46. 基于云端服务的数据安全与防护

47. 云环境下企业如何保护云端数据安全

48. 保障企业数据安全更给力

49. 门禁系统为智慧医疗保障数据安全

50. 浅谈基于数据备份保障数据安全