关注企业数据安全十招谨防数据泄露 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/469/2021_2022__E5_85_B3_E6_B3_A8_E4_BC_81_E4_c67_469471.htm 导致网络瘫痪的黑客攻击往往引起人们的极大注意，因此公司对于这些威胁采取了严密的保护措施。不过，如果你的公司只是关注这种安全，还是远远不够的。 不幸的是，预防DDOS攻击、病毒、蠕虫和其它侵害形式的措施并不能解决日益严重的数据流失问题：由于竞争对手的网络间谍活动造成公司数据被窃取。然而你公司的商业秘密泄露给一个竞争者，或者公司的信息被媒体获知，在有些情况下，有可能导致比网络瘫痪更为严重的后果。 那么，为了防止你的数据从公司泄露出去，应该采取哪些措施呢？ 第一招：贯彻执行最少特权的原则 你可以根据两种截然相反的理论观点设置你的网络访问策略。第一种，“ 全面开放 ”策略，假设所有的数据对每一个人都是可用的，除非明确地限制其访问。第二种策略即“ 最少特权 ”策略，即所有的数据禁止所有用户的访问，除非一个用户被明确地给与这种访问权限。后者就像是一个情报机构：除非一个用户拥有所需要的适当证明来访问一个特定的文件，否则就不能访问它。 第二招：将策略写下来形成书面规章制度 你可能会认为你的员工不应复制公司的重要信息，并将其带回家去；在没有经过允许之前，员工也不应该将这些信息通过电子邮件发送到网络之外去。这是很显明的事情。不过，如果你不将这些策略和规则写下来或打印出来，并让员工在其上签字，那么如果他们违反了这些要求，你将很难惩罚他们。不形成规章制度或者未成文的规则是很难实施的。 你的规

则应该具体明确，并举出例子哪些行为应该禁止。员工们可能不理解，除非你清楚地说明之，通过电子邮件将公司的文档以附件的形式发送到公司网络之外（或者发送到其家庭账户上）违反了公司的规则，这与下面的行为是一样的：将这个文档复制到磁盘上或一个USB设备上，然后将其带出公司大门，它们同样违反了公司规则。 不过，对规则的措词应该体现出：加以禁止的行为不限于你所举的例子，一切威胁公司安全的行为都应禁止。 第三招：设计限制性的许可和审计访问 保护数据非常重要的一步就是针对数据文件和文件夹设计恰当的许可。毋庸质疑，Windows网络的关键数据应该存储到一个NTFS分区上，因此你才能运用某种共享许可实施NTFS许可。NTFS许可比共享许可更加精细，并能运用到访问本地计算机和网络数据的用户身上。 要尽可能地给用户最低级的、能完成工作的许可。例如，将“ 只读 ”许可给用户，防止他们修改文件。 你还可以对包含敏感数据的文件和文件夹进行审核，因此就可以看出谁在什么时间访问了数据。 第四招：使用数据加密 将数据存储在NTFS格式的磁盘上的另外一个好处是你可以实施加密文件系统（Encrypting File System (EFS)）的加密。EFS由Windows 2000及以后的操作系统所支持，可以防止其他用户打开文件，即使他们拥有NTFS许可。至于Windows XP/2003及以后的操作系统，可以通过在加密对话框中给其分配特定的许可，实施加密文件夹的共享。窃取数据的一种方法是窃取整台计算机，特别是笔记本电脑等。对于vista 企业版和终极版，为防止万一计算机被窃取的造成的数据丢失，可以利用BitLocker的完全驱动器加密来保护数据。 100Test 下载频道开通，各类考试题目直接下载。详