CIO的教训：加密数据也不可认为是安全的 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/236/2021_2022_CIO_E7_9A_84_E6_95_99_E8_c40_236266.htm CIO们应从此次TJX黑客事件中吸取什么教训呢？即便是已加密的数据，也不可就认为其是安全的。 TJX在过去18个月内有将近4600万信用卡用户数据泄漏。在TJX提呈SEC（证券交易委员会）的一份文档中有披露此次事件一些相关细节。电子周刊主任编辑埃里克。卢坤思（Eric Lundquist）表示：看过这份文档后，我个人认为此次黑客对TJX计算机系统的攻击极为老道也很成功，采取不法行为的时间极为适当，很巧妙地跨过了TJX安全加密系统。至于此次消费者信息泄漏事件，虽然电子周刊的埃文。舒曼（Evan Schuman）已作了很好报道，但当政府调查员及TJX聘的私人公司来查看该公司安全程序以试图了解事情发生的原因时，却发现一部分数据泄漏的细节已丢失了。而这份SEC文档中标题为“ 计算机入侵 ”的章节倒是提供了额外的细节，内容有关于从2005年7月初次入侵直到2006年12月，这么久一段时间计算机入侵者是如何大范围地渗透进该公司的系统中。 TJX在这份文档中陈述道：“ 2006年12月18日，我们发现在我们的计算机系统中有可疑软件。我们立即着手进行了一次调查，并且在第二天就邀请了在计算机安全及事件响应方面处于领先地位的通用动力公司（General Dynamics Corporation）及IBM来协助进行调查。最后他们在2006年12月21日正式确认，我们的计算机系统已被入侵且入侵者还存在我们的计算机系统中。 卢坤思还表示：我认为这名黑客应曾是个专业人士，为什么？有三大原因。 一、入侵时间长

。18个月对于进行非法访问来说是一段很长时间。二、入侵者做了很好工作来掩盖他们的痕迹，这可从以下这份文档的陈述可得以表明，“此外，入侵者所用技术使得我们到目前为止都无法确定我们认为在2006年已被窃取所有文件中大部分文件的内容是什么。对于此次计算机入侵事件中包括的业务范围和区域、计算机系统还有时间进度，我们的调查已要求有个明确到日期的时间范围，且我们的调查仍未完成。我们还将继续调查以确认这次计算机入侵中被盗的信息具体有哪些，不过除了以下所提供信息以外，我们也许永远无法能再确认其它大部分被认为已被窃的信息。”三、尽管TJX有采取一些适当的加密和数据擦除策略（至少据SEC文档中显示是如此），但入侵者十分精通计算机，足以知道在什么时间系统中所运行数据是未加密数据。以下内容来自这份SEC文档，“通过我们的调查，我们已确认有近100个文件是在这段时间内入侵者从我们位于弗雷明汉市的系统中所窃取的（我们相信很大一部分是入侵者自己创建的），而且我们怀疑其中包含有消费者数据。不过，由于入侵者所采用的一些技术，使得我们并不能确认这些文件中所包含信息的种类及范围。尽管在2006年我们就已在位于弗雷明汉市的系统中加入了诸多隐蔽及加密措施，但同年入侵者却利用一些技术在支付卡发行商批准过程期间从我们位于弗雷明汉市的系统中窃取支付卡数据，因为在这个时间段数据（包括第二磁道数据）都是未加密直接传输给支付卡发行商的。此外，我们相信入侵者已能使用解密工具来破解TJX所用的加密软件。”最后，卢坤思还指出：首席信息官们及信息安全主管们的底线是永不能放松你们的安全防护。你们可分割你们的数据、擦

除你们的数据以及加密你们的数据，但这并不意味着你们的数据是安全的可免遭入侵。要时刻不放松对你系统的保护，要保持系统上你的安全程序有一直运行，要有工作人员时刻关注你的系统，这些是维护计算机安全所应付的代价。如果你不愿付出这些代价，那么也许某天你会发现自己上了每日头条。 FTI咨询公司执行总监马克。拉希（Mark Rasch）也表示：“ 加密技术仍是一项至关紧要的工具，只是人们必须认识到它只是诸多安全工具之一。 ”他表示。“ 人们往往将密钥与所保护数据保存在同一台设备上，这是及其错误的。理想来说，密钥应保存在单独硬件设备上，并且仅在需要时使用。经常有人把密钥保存在系统的某个地方。这就也比使用的是真正的好锁却将钥匙藏在垫子下。 ”