Truecrypt ist sicher

Truecrypt ist sicher, wenn man es richtig anwendet. Heise zitiert heute einen Polizisten, der das Passware Kit Forensic eingesetzt haben will:
Heute gelang mir der Zugriff auf eine Truecrypt-Partition in einem sehr wichtigen Fall. Alle relevanten Informationen für den Fall waren darauf gespeichert. Andere Produkte hatten zuvor versagt.

Ich sehe hier keine zwei unabhängige Quellen, die heranzuziehen für eine solch windige These Journalisten in der Pflicht sind, sondern nur eine nicht nachprüfbare Propaganda-Behauptung des Software-Herstellers. Selbst wenn das wahr sein sollte, handelt es sich um ein nachvollziehbares Szenario, wie im Heise-Forum ganz richtig angemerkt wird:

„If the target computer with the encrypted volume is powered off, encryption keys are not stored in its memory, but they could be possibly recovered from the hiberfil.sys file, which is automatically created when a system hibernates.

NOTE: If the target computer is turned off and the encrypted volume was dismounted during the last hibernation, neither the memory image nor the hiberfil.sys file will contain the encryption keys. Therefore, instant decryption of the volume is impossible. In this case, Passware Kit assigns brute-force attacks to recover the original password for the volume.

Das heißt: Ein Angriff ist unter Umständen möglich, wenn ein Truecrypt-Container *nicht* per *dismount* geschlossen, sondern der Rechner nur heruntergefahren wurde, also dann, wenn der Nutzer sind fahrlässig verhalten hat.

Sorry, aber das *muss* in einen solchen Artikel, sonst ist das reine Panikmache.