Aschauer Str. 30
D-81549 München
Tel.: +49 89 62030100
Fax.: +49 89 620301069
http: //www.itWatch.de
e-Mail: info@itWatch.de

München, 18.11.2020

Passwortlisten und Kontoauszüge auf vermeintlich leeren USB-Sticks- mit itWatch wäre das nicht passiert

Bei nicht sicherem Löschen droht Schaden und Verletzung von Geheimhaltung und Datenschutz

Eine Untersuchung gebrauchter, vermeintlich leerer USB-Sticks an der Abertay University ergab, dass Daten von zwei Drittel der USB-Sticks von den Vorbesitzern nicht korrekt gelöscht worden waren. So konnten rund 75 000 der gelöschten Dateien wiederhergestellt werden. Darunter befanden sich höchst sensible Daten wie Listen von Passwörtern, Kontoauszüge und Verträge. Mehr zu den Untersuchungsergebnissen finden Sie auch auf heise online.

Betriebssystemeigene Löschfunktionen löschen nicht tatsächlich, sondern lediglich den belegten Speicher für die künftige Nutzung freigeben. Die Daten bleiben somit auf dem Datenträger, ob mobil oder die Festplatte eines PCs, lesbar. Gelangen Datenträger in fremde Hände so können gelöschte Dateien mit frei verfügbaren Tools wiederhergestellt und missbraucht werden beispielsweise zur finanziellen Bereicherung direkt über Kontodaten und Passwörter oder gar durch Erpressung mit der Drohung, heikle Daten andernfalls preis zu geben. Insbesondere auch Dokumente, die der Geheimhaltung unterliegen, müssen zwingend unwiderruflich gelöscht werden, um Geheimhaltung auch in juristischer Hinsicht gerecht zu werden. Ebenso geht sicheres Löschen mit der rechtlichen Verpflichtung des Datenschutzes einher- ein Aspekt, der oft vernachlässigt wird.

Mit dataEx als Modul der **itW**atch **E**nterprise **S**ecurity **S**uite (itWESS) wird auf der Basis der vorhandenen Berechtigungen das sichere Löschen von Dateien beziehungsweise Ordnern und deren Metainformationen realisiert, so dass diese auch mit den besten forensischen Werkzeugen nicht mehr rekonstruiert werden können.

Unabhängig davon sollten sensible Daten generell verschlüsselt abgespeichert werden, sodass auch im Falle des Verlustes eines Datenträgers die Inhalte der abgespeicherten Daten für Unbefugte nicht lesbar sind. So kann man sich auch gegen schadcodebehaftete Controller schützen, wie sie z.B. unter dem Namen BadUSB bekannt sind, worüber Geschäftsführer Ramon Mörl 2015 mit dem Vortrag „BadUSB- vergleichbare Exploits und sinnvolle Verteidigungsstrategien“ auf dem IT-Sicherheitskongress des BSI referierte. Für weitere Informationen zu diesem Thema lesen Sie auch „BadUSB, aktuelle USB Exploits und Schutzmechanismen“.
Mit PDWatch (**P**rivate **D**aten) der itWatch GmbH, ebenfalls ein Modul der **itW**atch **E**nterprise **S**ecurity **S**uite (itWESS), lassen sich Dateien verschlüsseln. Die Verschlüsselung kann beim Export von Dateien auf beliebige Datenträger erzwungen oder auch benutzerabhängig optional zur Verfügung gestellt werden.

Nähere Informationen finden Sie unter www.itWatch.de