ChannelPartner

Link: https://www.channelpartner.de/a/haendler-fragen-die-ssd-experten-von-samsung-antworten-teil-2,3042226

**Sicherheit und Verfügbarkeit von Daten**

# Händler fragen – die SSD-Experten von Samsung antworten (Teil 2)

Datum: 05.05.2014

**Solid State Drives (SSD) begeistern viele Anwender durch schnelle Zugriffszeiten und die damit verbundene Zeitersparnis im Arbeitsalltag. Doch können Fachhändler ihren Kunden die neue Technologie bedenkenlos empfehlen? Wie sicher sind Flash-Speicher? Die CHANNELPARTNER-Redaktion hat Fragen von Händlern gesammelt und den SSD-Experten von Samsung vorgelegt. Lesen Sie hier die Antworten rund um die Themen Sicherheit und Verfügbarkeit von Daten auf SSD.**

## Sind meine Daten auf SSD genauso sicher wie auf einer Festplatte?

Datensicherheit ist das Ergebnis einer Vielzahl unterschiedlicher Faktoren. Wie sicher die Daten eines Unternehmens sind, das hängt zum einen von der eingesetzten Technologie ab. Mindestens ebenso wichtig ist jedoch der sicherheitsbewusste Umgang mit den genutzten Tools und Technologien. Je komplexer die Infrastruktur eines Unternehmens, desto wichtiger ist es, dass die unterschiedlichen Sicherheitsmechanismen optimal aufeinander abgestimmt sind und konsequent genutzt werden. Bezogen auf das Speichermedium als solches, sind vor allem zwei Aspekte entscheidend:

- Der Schutz der Daten vor unberechtigtem Zugriff, Diebstahl, Manipulation und Zerstörung.
- Fehlerfreies Ablegen der Daten auf dem gewählten Speichermedium.

Wer seine Daten vor unbefugtem Zugriff schützen will, kann sowohl beim Einsatz von HDD als auch von SSD aus einer breiten Palette an Softwarelösungen auswählen. Wird dieser Zugriffsschutz in Form der Datenverschlüsselung ausgeführt und per Software realisiert, ergibt sich - unabhängig vom jeweiligen Speichermedium - immer eine gewisse Leistungseinbuße beim Ver- und Entschlüsseln der Daten während der Lese- und Schreibvorgänge. Diese Leistungseinbuße kann dadurch eliminiert werden, dass man Laufwerke mit integrierter Hardwareverschlüsselung einsetzt. Solche im Datenträger integrierte Tools kommen sowohl in Enterprise-Festplatten als auch in Solid State Laufwerken wie der 840 Pro und EVO Serie von Samsung zum Einsatz. Hier besteht kein Unterschied hinsichtlich der Datensicherheit, da diese hauptsächlich von der Stärke der gewählten Verschlüsselung abhängt.

Betrachtet man den Begriff "Datensicherheit" unter dem Aspekt des fehlerfreien Speicherns, dann hängt dies in nicht unerheblichem Maße von den Fehlerkorrekturmechanismen im Speichermedium ab. Sowohl bei Festplatten als auch bei SSDs können sogenannte CRC-Fehler auftreten, was bei Festplatten meist auf einen oder mehrere kaputte Sektoren hindeutet. Um solchen Fehlern vorzubeugen, kommen bei Samsung SSDs Fehlerkorrekturverfahren wie ECC zum Einsatz, die in der Lage sind, 1-Bit-Fehler zu erkennen und sofort zu korrigieren.

Ein weiterer Aspekt der Sicherheit von Daten auf SSD ergibt sich aus ihrer Bauweise: Da sie keine mechanischen Bauteile enthalten, sind sie im Unterschied zu HDD weitgehend unempfindlich gegenüber Stößen.

## Wie sinnvoll ist der Einsatz von SSDs in Verbindung mit einer Festplattenverschlüsselungssoftware?

Hier kommt es darauf an, welches Verschlüsselungsverfahren und welche Verschlüsselungsart der Anwender nutzt. Wird die Verschlüsselung per Software (wie etwa TrueCrypt) durchgeführt, dann ist immer mit einer Beeinträchtigung der Performance unabhängig vom verwendeten Datenträger zu rechnen, da die Geschwindigkeit dieses Vorgangs direkt von der Leistungsfähigkeit der CPU abhängt. Daher ist die Nutzung der Hardware-Verschlüsselung vorzuziehen, wie sie bei den Samsung SSDs der 840 Pro und 840 EVO Serie zum Einsatz kommt. Dieses Verfahren zeichnet sich dadurch aus, dass der Verschlüsselungsvorgang, in diesem Fall mit AES 256-Bit, unabhängig von Systemressourcen wie CPU und RAM vorgenommen wird und direkt im Controller der SSD stattfindet. Dies geschieht für den Nutzer vollkommen transparent und weder die Leistung des Systems noch die Geschwindigkeit der SSD wird hierdurch beeinträchtigt. Die guten Testergebnisse der SSD 840 Pro und EVO-Serie in bekannten Magazinen wurden mit aktivierter Verschlüsselung erzielt.

## Muss die Hardware-Verschlüsselung genutzt werden, oder kann man sie auch abgeschalten?

Die Hardware-Verschlüsselung ist bei den SSDs der Serien 840 Pro und 840 EVO immer aktiv. Ein Abschalten ist nicht möglich. Da die Hardware-Verschlüsselung jedoch für den Anwender komplett transparent im Controller der SSD erfolgt und hierfür keinerlei weitere Systemressourcen benötigt werden, ist dies für Anwender nicht bemerkbar. Aus Security-Sicht entspricht dieses Verfahren der Ablage von Daten in einem Tresor, der zwar eine Türe besitzt, aber kein Schloss, sodass jedermann auf die dort abgelegten Daten Zugriff hat. Um diesen Tresor abzuschließen, muss daher noch vom Anwender ein Schloss angebracht werden. Dies erfolgt in Einzelplatz-Umgebungen entweder durch die Aktivierung der HDD-Security / ATA Passwort Option im BIOS/UEFI oder durch den Einsatz einer Software nach dem TCG/OPAL-Standard.

---