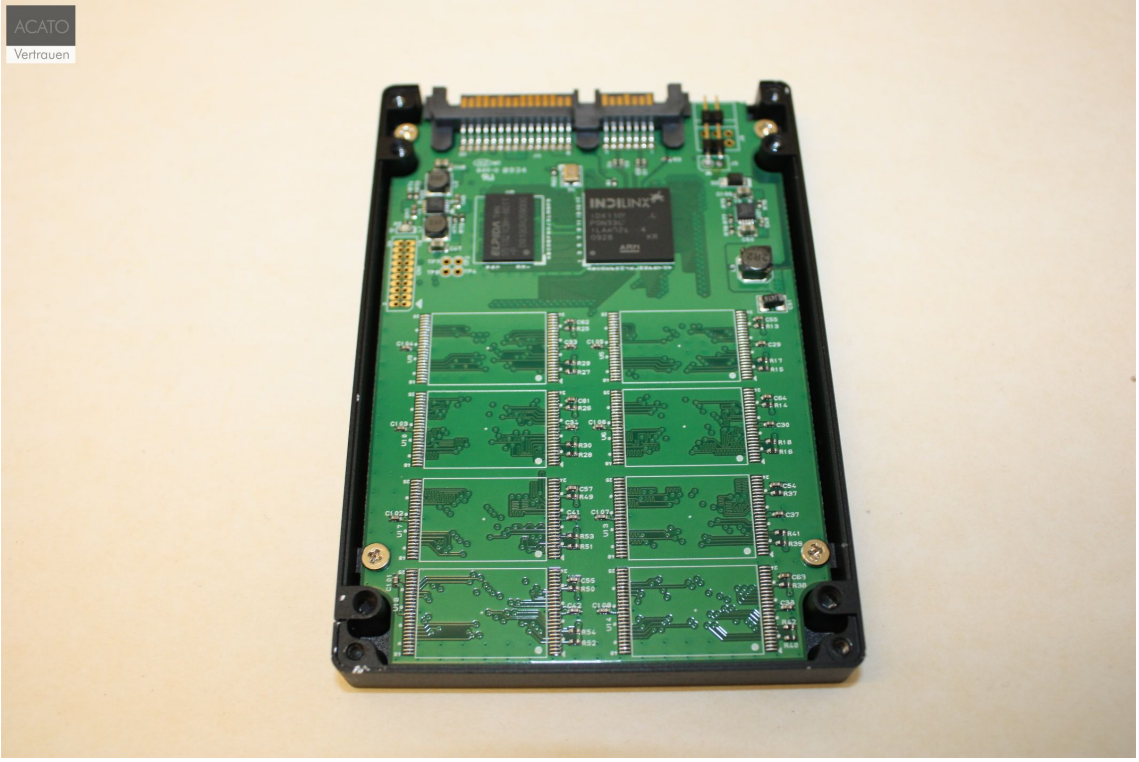
*Typ: Andere*

*Kategorie: Elektronik*

# Wenn Verschlüsselung keinen Mehrwert dem Nutzer bietet...

*Festplatten und mobile Speichermedien mit integrierter Verschlüsselung werden häufig dem Werbeadressaten als wunderbaren Schutzmantel vorgeführt. Wer sich auf blumige Werbeversprechungen verlässt, wird eine Katastrophe über sich selbst herbeiführen.*




*SSD mit Controller, der Daten verschlüsselt ablegt*

Immer mehr Geräte werden mit verschlüsselnden Komponenten angeboten, wobei diese Funktionalität für den Nutzer einen optimalen Schutz vor unbefugten Zugang zu seinen Daten sicherstellen soll. Die Wahrheit über die gekaufte Sicherheit ist ein zweischneidiges Schwert.

Im Folgenden gehen wir auf die jeweiligen Gerätetypen und die Nutzbarkeit sowie Risiken der einzelnen Mechanismen ein.

Jeder kann in einen Laden für Computer und Multimedia Geräte eine wahre Vielfalt an Speicherkarten finden. Manche Kunden gehen bei der Kaufentscheidung nach ihnen bekannten Marken, dem für sie attraktivsten Preis oder dem Bauchgefühl. Kaum ein Hobbyfotograf fragt an der Theke nach der Sicherheit des von ihm gewählten Datenträgers. Nicht jeder Händler kann oder will die Risiken der verschlüsselnden Controller aufzeigen, denn auch auf des Verkaufsverpackung findet man keine Erwähnung des verwendeten Controllers.

Der Controller ist eine besondere Baukomponente. In Speicherkarten und USB Sticks arbeiten die weltweit verbauten Controller für NAND Chips bzw. Flashspeicher extrem unterschiedlich von einander. Während einige Controller einfach gestrickt sind und die Daten seriell auf den Speicherchips ablegen, gehen andere zur Verschleissminderung dazu über Inversion als auch Zufallsverteilung bei der Verteilung der Daten auf die einzelnen Speicherzellen anzuwenden. Jede Speicherzelle hat nur eine begrenzte Lebenszeit, die durch die Anzahl der Schreib- und Lesezugriffe begrenzt ist. Damit aber diese Zellen möglichst lange verwendbar bleiben, muss der Controller seine Wahl der zu verwendenden Zellen optimal streuen.

Auch Controller in höherwertigen Speicherkarten und USB Sticks haben einen Plan-B. Dabei werden in der Regel

mindestens 3 Zellen als Ersatzzellen in jedem Zellenblock reserviert. Erst wenn eine aktive Zelle ihre Lebenszeit erreicht hat, wird diese deaktiviert und durch eine Ersatzzelle kompensiert. Dabei verlagert der Controller die gespeicherten Daten auf die neue Zelle. Ist eine Verlagerung der Information nicht möglich, bekommen die betroffenen Dateien ein Konsistenzproblem.

Wie wirkt sich die Tätigkeit der verschlüsselnden Controller in Speicherkarten aus?

Controller mit integrierter Verschlüsselung kann man meist durch eine Recherche im Internet identifizieren. Die Hauptvertreter dieser Controller sind Sandforce (SF-xxxx) und SanDisk (SDxxxx) Controller. Auch OCZ und Kingston setzen vereinzelt verschlüsselnde Controller in der Produktreihe SSD, jedoch nicht bei Speicherkarten ein.

Wer keine Verschlüsselung erwerben will, sollte auf andere Marken setzen als SanDisk. Warum eigentlich?

Bei einem extremen Defekt des Controllers kann nur noch der Weg über die Demontage des Speicherchips zu den Daten führen. Damit kann man keine Daten ohne spezielle Laborausrüstung zurückbekommen.

Wenn ein Controller die Daten stark verschlüsselt ablegt, liegen die Daten selbst in nicht wieder erkennbaren Mustern. Hat der Speicherchip ebenfalls interne Schäden so kann der Experte auch hier keine Brücke über defekten Segmente hinweg bauen.

Es gibt aber auch Controller anderer Hersteller, die eine leicht zu brechende Verschlüsselung verwenden. Hier kann der gut ausgebildete Experte die Logik im Schrittmodell per re-engineering von hinten nach vorne rekonstruieren. Dadurch lassen sich am Ende mit einer recht guten Datenquote Fälle erfolgreich abschliessen.

Auf der anderen Seite sollte man sich aber fragen, was diese Verschlüsselung dem eigentlichen Käufer bietet. Wenn eine solche Speicherkarte gestohlen wird, kann der Dieb trotz Verschlüsselung problemlos und ohne Spezialsoftware auf die Daten zugreifen, denn das Gerät ist ja unbeschädigt. Es existiert also kein Zugriffsschutz in diesem Szenario.

Wo ist der Mehrwert für den Kunden?

Wenn aber die gestohlene Speicherkarte beim Diebstahl beschädigt wird, kommt der Dieb nicht an die Daten heran. Was aber wenn die Speicherkarte nicht gestohlen, sondern per versehen vom Nutzer verbogen wird? Dann kommt er in den meisten Fällen nicht mehr an seine Daten. Wir sprechen von "meistens", weil die Verschlüsselungsmethoden einiger SanDisk Controller in Fachkreisen bekannt sind und daher in ca. 5 bis 10% der Fälle zur Freude des Kunden fast alle Daten intakt extrahiert werden können. Dennoch muss man bei Speicherkarten mit verschlüsselnden Controllern die Verschlüsselung stark in Frage stellen.

Wozu bauen Hersteller wie Sandforce und SanDisk ihre Controller mit Verschlüsselung?

Hier geht es einzig und allein um den Schutz des geistigen Eigentums der Hersteller. Mit extrem aufwendigen Forschungsprojekten, versuchen diese Hersteller die Alterung der Speicherchips zu bremsen. Dieses spezielle Wissen über die ausgeklügelten Speicherverfahren, möchte man aber der Konkurrenz nicht auf dem goldenen Tablett präsentieren. Dabei muss man sich aber fragen, ob nicht dann die Verschlüsselung wieder kontraproduktiv wirkt. Da man auch keine Hintertür für Werksspionage bieten will, geben diese Hersteller auch keinen Generalschlüssel oder charchen-typischen Schlüssel an die kleinen und großen Datenrettungsunternehmen heraus.

Ähnlich der ärztlichen Verfügung für lebenserhaltende Maßnahmen, muss der Kunde beim Kauf einer Speicherkarte berücksichtigen wie sehr er im Falle eines Geräteausfalls die Wiederbeschaffung der Daten benötigt. Nicht an mehreren Orten gespeicherte Daten sollten daher nicht auf Speichermedien mit verschlüsselnden Controllern abgelegt werden.

Wie verhält sich dies bei dem art-verwandten USB Stick?

Speicherkarten und USB Sticks unterscheiden sich meist nur in der Anschlusstechnologie und dem verfügbaren Platz

für die Steuerungskomponenten. In einem USB Stick findet man meist größere Bauteile, weshalb USB Sticks häufiger günstiger sind als Speicherkarten, wenn man sie nach dem Verhältnis Speicherplatz zu Preis. Dennoch ist Speicherkarte nicht gleich Speicherkarte. Die von Profifotografen verwendeten Compact Flash CFII verwendeten Karten haben eine extrem hohe Speicherkapazität und Geschwindigkeit, da die mehr Raum zur Verfügung haben als die gewöhnliche SDHC Speicherkarte.

Derzeit kann der schnellste Speicherchip eine Datenausgabegeschwindigkeit von 7 bis 10 MB pro Sekunde erreichen und deshalb können Kartenleser mit USB 3.0 derzeit nicht ihre volle Wirkung erreichen. Gerade bei der Datenrettung beeinflusst diese begrenzte Geschwindigkeit den Auslese- und Analyseprozess.

Intelligente fortschrittliche Systeme verfolgen eine einmalige Extraktion und sind dann in der Lage die Daten für eine analytische Untersuchung aufzubereiten. Daher wird die Datenrettung bei immer moderneren USB Sticks immer komplexer. Das beginnt bereits bei der Demontage der Speicherchips, denn meist können die mittlerweile extrem dünnen Speicherchips durch ungeeignete Verfahren beschädigt werden. Heißluftpistolen ohne Wärmeregulierung zerstören sofort die Speicherchips. Ältere Speicherchips sind nicht so empfindlich.

Die Folge dieser Entwicklung ist, dann man übergehen muss zu hochwertigen Reworkstationen. Die im Internet angepriesenen chinesischen Reworkstationen beschädigen jedoch die empfindlichen Komponenten, da sie zu breitflächig und ungenau arbeiten. Eine professionelle Reworkstation kostet in der Vollausstattung ca. 25.000 EUR, weshalb man auch nachvollziehen kann, dass ein Gerät für 800 EUR aus China niemals in ein professionelles Labor gehört.

Wie bereits bei den Speicherkarten aufgezeigt, hat ein verschlüsselnder Controller auch bei USB Sticks keinen Mehrwert für den Nutzer. Wer spezielle Sicherheitsanforderungen an einen USB Stick hat, greift auf die blauen USB Sticks von Kingston zurück. Die ACATO GmbH erhielt von Kingston mehrere der DataTraveller Vault Pravacy USB Sticks zum testen der Datensicherheit unter Laborbedingungen.

Dabei wurden mittels des Sicherheitssystems Testdaten auf die USB Sticks gespeichert und den darin befindlichen Container anschliessend geschlossen. Die USB Sticks wurden dann demontiert und versucht über Re-Engineering wieder an die Daten heranzukommen. Damit konnte erwiesen werden, dass diese Art von USB Sticks einen Schutz bieten, der im Einklang mit dem Schutzbedürfnis der Unternehmenskunden steht. Hierbei geht es dem Geschäftskunden in erster Linie nicht um eine "Rettbarkeit" sondern zu verhindern, dass die transportierte Kopie eines Betriebsgeheimnisses im Falle eines Diebstahls auch mit unwissender Beteiligung eines Labors nicht möglich sein darf.

Bei solchen USB Sticks finden wir folglich einen Mehrwert beim Einsatz einer Verschlüsselungstechnik.

Und wie steht es mit SSD Festplatten?

Wozu brauchen wir dort verschlüsselnde Controller? Aus dem selben bereits erwähnten Wunsch nach dem Schutz des geistigen Eigentums, werden solche verschlüsselnde Controller eingesetzt. Teilweise erreichen diese SSDs eine höhere Geschwindigkeit zum Preis eines möglichen unumkehrbaren Datenverlustes.

Auch hier findet man vereinzelt leicht verschlüsselnde Controller, die bei kompletter Demontage einer SSD mit SATA oder Bladetechnologie trotzdem entschlüsselt werden können. Es gibt einige Hersteller von SSDs, die gelegentlich versucht haben durch Zukauf von Sandforce Controllern ihre Geräte noch leistungsfähiger zu machen. Leider vergessen sie dabei den Kunden vollumfänglich über die Risiken aufzuklären. Wenn erst einmal der Totalverlust eingetreten ist, beginnen Kunden sich umzuorientieren. Der Marktvergleich zeigt, dass fast alle SSD Hersteller irgend wann einmal mit verschlüsselnden Controllern einzelne Produktreihen eingeführt haben. Dabei wird die integrierte Verschlüsselung unter einem eher positiven Aspekt dargestellt.

Die Frage nach den sicheren SSD Herstellern ohne verschlüsselnde Controller wird daher immer schwerer zu beantworten. Im Prinzip kann man bei Kingston, Crucial, intel und Samsung relativ gut einkaufen. Man muss aber trotzdem in den Datenblättern nach dem Schlüsselbegriff "Verschlüsselung" suchen, damit man auch dort keine

Fehlentscheidung trifft. Für den Nutzer, der sowieso keine Daten ausser Systemdaten auf einer SSD ablegt, für den ist diese Wahl fast immer irrelevant. Nur wer von seinem kompletten Server mit SSD Technologie in einer Ausfallsituation sowohl System als auch Nutzerdaten rettet sehen will, muss äusserst vorsichtig bei der Beschaffung sein.

Bei Betrachtung der vorangegangenen Erläuterungen über die Flashspeichertechnologie und den verbauten verschlüsselnden Controllern, bestätigt sich der fehlende Mehrwert für den Nutzer, denn bei einem Ausfall hat nicht die Geschwindigkeit sondern die zu rettende Datenmenge oberste Priorität.

Man darf trotzdem nicht generalisieren, wenn es um die Datenrettung aus SSD Festplatten der Hersteller mit Controllern der verschlüsselten Art geht. Es lassen sich in vielen Fällen Daten retten, jedoch bei zu starker Beschädigung dieser Controller kann eine Transplantation der Speicherchips auf eine gesunde SSD Platine auch nur ein fragwürdiger Akt sein. Jedenfalls würden die meisten Kunden für diese aufwendige Prozedur kaum bereit sein zu zahlen. Es ist einfach langfristig günstiger schon beim Kauf an die zukünftigen Gefahren zu denken.

Letztendlich aber entscheidet der Kunde wie er sein Verhältnis zum Risiko gestaltet.



Kontakt
ACATO GmbH
Christian Bartsch
Heimeranstr. 37
80339 München
Tel.:08954041070
E-Mail:presse@acato.de
Web:http://www.acato.de