

# Prophylaxe gegen Datendiebstahl

## Daten absolut zuverlässig schützen

Ob Konstruktionszeichnung, Personalbogen, Forschungsergebnisse oder Geschäftszahlen – der Schutz wichtiger Daten ist für Unternehmen nicht zu überschätzen, da ein unerlaubter Abfluss von Daten über wohl und wehe von Firmen entscheiden kann. Umso wichtiger ist es, diese zuverlässig vor einem unerlaubten Zugriff zu schützen. Diesbezüglich ist das Unternehmen Identos mit seinen wirksamen Hardware-Lösungen eine absolut empfehlenswerte Anlaufstelle.

Verantwortungsbewusste Unternehmen verhindern mittlerweile mit Zutrittskontrollsystemen, dass sich unbefugte Personen unbemerkt Zutritt in das Firmengebäude verschaffen. Diesbezüglich einen sehr guten Zutrittsschutz bieten Hardwarelösungen mit drahtloser Abfrage einer Chipkarte, die mit einem Fingerabdruck- oder gar einem Irisscanner ergänzt werden können.

Geradezu steinzeitlich geben sich hingegen Zugangssperren, die lediglich ein Passwort oder eine Kennnummer abfragen, da es für Unbefugte mühelos machbar ist, Passwörter in Erfahrung zu bringen.

Beispielsweise ist es eine Tatsache, dass auf internationalen Messen mitunter Mousepads verschenkt werden, die mit einem winzigen,

absolut nicht sichtbaren Code bedruckt sind. Dieser Code ist derart gestaltet, dass beim Überstreichen des Maus-Laserstrahls ein Skript eingelesen wird, wodurch weiterer Code aus dem Netz in den PC überspielt wird, der beispielsweise das Ausspionieren von Passwörtern ermöglicht.

Es ist daher für Unternehmen Pflicht, sich der mannigfaltigen Gefahren bewusst zu werden, die sich mit der Nutzung moderner EDV-Technik ergeben. Es ist daher zwingend eine passgenaue Schutzstrategie für die im Unternehmen eingesetzten Zutrittskontrollsysteme, Kommunikationsmittel und Datenverarbeitungsanlagen auszuarbeiten.

Diesbezüglich bietet das Unternehmen Identos wirkungsvolle Hardwarelösun-



Die Identos GMBH liefert ihre in Deutschland entwickelten und produzierten Produkte weltweit an IT Security-Lösungsfirmen, die solche Sicherheitslösungen vertreiben. Für den deutschsprachigen Markt wird ein Endanwender-Lösungsgeschäft über die Tochterfirma ›Identsmart GmbH‹ mit Sitz in Bad Aibling angeboten.

gen an, an denen sich nicht nur Hacker, sondern auch Geheimdienste vom Schlag eines NSA die Zähne ausbeißen. Beispielsweise vertreibt das

Unternehmen unter dem Namen ›ID50‹ einen USB-Stick, der in der Lage ist, Passwörter zu verschlüsseln und für den Nutzer zur täglichen Arbeit bereitzuhalten. Ein integrierter Chip sorgt für eine Echtzeitverschlüsselung der Daten, sodass der Stick an jedem PC funktioniert. Ein geringer Anschaffungspreis erlaubt es Unternehmen, sehr preiswert jeden Mitarbeiter mit diesem Passwort-Tresor auszustatten.

Sollte einmal ein Exemplar verloren gehen, so sind die darauf gespeicherten Passwörter für den Finder nicht einsehbar, da eine Entschlüsselung erst nach Eingabe einer Pin-Nummer erfolgt, die ausschließlich dem rechtmäßigen Besitzer bekannt ist.

### Stick mit viel Komfort

Der Vorteil dieses USB-Sticks ist, dass man damit in die Lage kommt, sich für den Zugang zu



Mit ›ID50‹ und ›ID60‹ bietet das Unternehmen Identos zwei USB-Sticks an, die Passwörter beziehungsweise Daten sicher verschlüsseln.



Sauber verarbeitete Hüllen lassen iPhone und iPad von Apple zu sicheren Geräten für sensible Daten mutieren.



Die Verschlüsselung der Daten erfolgt nicht per Software, sondern mittels eines speziellen Chips, der auf einer Platine sitzt.

Web-Angeboten aller Art ausgesprochen aufwendige Passwörter auszudenken, die man sich nicht merken muss, da dies der ID50 übernimmt. Der Clou ist, dass der Stick erkennt, welche Internetseite gerade besucht wird und schreibt ohne Zutun die passenden Log-in-Daten in die entsprechenden Eingabefelder. Sollte der Stick einmal verloren gehen, zerstört der Stick alle darauf gespeicherten Passwörter, wenn vier Mal das Schlüsselwort falsch eingegeben wird.

Nach dem gleichen Prinzip arbeitet der »ID60«. Unter diesem Namen vertreibt das Unternehmen einen USB-Stick, der bis zu 50 GB große Files auf der Festplatte des PCs verschlüsselt. In diesen Datentresor können sensible Konstruktionszeichnungen, interne Unternehmenskorrespondenz, Geschäftspläne oder andere, nicht für fremde Augen be-

stimmte Daten abgelegt werden. Der Datenschutz basiert auf einem angriffssicheren Verschlüsselungsverfahren, das mittels eines auf dem Stick verbauten Chips funktioniert. Da die Verschlüsselung des virtuellen Laufwerks in Echtzeit über diesen Chip auf dem eigenen PC erfolgt, kann nicht einmal ein personell und technisch bestens ausgestatteter Geheimdienst an die Daten ran.

Daher ist es eine Überlegung wert, die Cloud mit allen ihren Vorteilen hinsichtlich der Datenausfallsicherheit zumindest für weniger wichtige Daten zu nutzen, da die Verschlüsselung auch in der Cloud funktioniert, die Daten demnach dort für fremde Augen ebenso unlesbar lagern, wie auf dem eigenen PC.

Die Handhabung der Daten mithilfe des Sticks ist denkbar einfach: Sobald der Stick am PC angesteckt wird, wird das ver-

schlüsselte, virtuelle Laufwerk sichtbar und die Daten stehen zur Bearbeitung bereit. Interessant ist, dass einzelne Dateien und Dateistrukturen problemlos auf andere Laufwerke kopiert werden können, von wo sie direkt für andere Personen zur Weiterbearbeitung zugänglich sind. Sobald der Stick abgezogen wird, werden Daten, aber auch Programme, die sich auf dem virtuellen Laufwerk befinden, wieder unsichtbar.

Sollte dieser Stick verloren gehen, so dient ein bei der Erstellung des virtuellen Laufwerks automatisch generiertes Passwort als Notfallschlüssel, mit dem der Datentresor auch ohne Stick wieder sichtbar gemacht werden kann. Dieses Passwort muss selbstverständlich an einem sicheren Ort verwahrt werden, da ohne dieses Passwort bei fehlendem ID60-Stick der Zugang zu dem nach AES 256 Bit, Tweak 128 Bit oder SHA256 verschlüsselten Laufwerk nicht mehr möglich ist. Hohe Sicherheit muss demnach mit hoher Sorgfalt einhergehen!

Besonders hervorzuheben ist, dass ID50 und ID60 in Deutschland entwickelt und produziert werden. Das Unternehmen Identos garantiert, dass keine Hintertüren existieren, die es etwa Geheimdiensten ermöglichen würden, bequem auf die Daten zuzugreifen. Eine entscheidende Aussage, die gerade vor dem

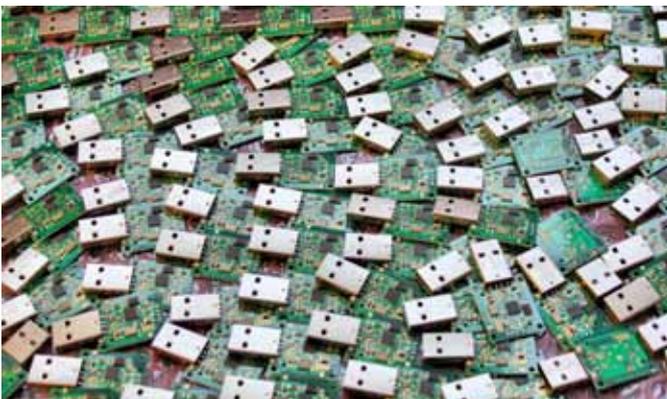
Hintergrund des NSA-Skandals nicht hoch genug gewichtet werden kann. Die beiden Sticks sind daher insbesondere für agile Unternehmen interessant, die innovative Produkte entwickeln.

Doch hat Identos noch mehr zu bieten, wenn es um die Sicherheit von Daten geht. Beispielsweise werden unter dem Namen »Cryptoterminal« für das iPhone sowie das iPad von Apple Hardwarelösungen angeboten, die dafür sorgen, dass Daten verschlüsselt über das Funknetz übertragen werden. Die Kommunikation mit Krankenkassen, Behörden oder der eigenen Firma wird dadurch auf eine sichere Basis gestellt. Ein Fingerabdruckscanner sorgt dafür, dass fremde Personen mit einer gestohlenen oder verlorenen Hardware nichts anfangen können.

Um firmenbezogene Anwendungen für die Kommunikation und Datenerfassung zu erstellen, wird von Identos ein SDK bereitgestellt. Die nötige Hardware gibt es in verschiedenen Ausprägungen. Wer es ganz bequem haben möchte, greift zu einem formschönen Gehäuse, in dem das iPad beziehungsweise das iPhone sich optimal einfügt. Damit bietet Identos einen sicheren Datenschutz, der auch dem Auge schmeichelt.



[www.identsmart.com](http://www.identsmart.com)



Jeder Stick ist ein Unikat. Somit existiert kein Duplikat, mit dem die Verschlüsselung umgangen werden könnte.