So klein und schon eine Sicherheitslücke?

Verschlüsselte USB-Sticks im Vergleich

Einfache USB-Sticks können Sie beim Discounter für wenig Geld kaufen, oder sie werden als Werbegeschenke verteilt. Entsprechend weit verbreitet sind sie im Privatbereich. Hat man sich einmal an die praktischen Datenträger gewöhnt, möchte man sie im Arbeitsalltag nicht mehr missen. Doch ohne vorbeugende Maßnahmen landen schnell personenbezogene oder andere vertrauliche Daten auf einem Stick. Wenn der dann verloren geht, kann das für das Unternehmen unangenehme Konsequenzen haben. Hier sei etwa an den § 42a BDSG erinnert – die Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten.

Verschlüsselungssoftware für USB-Sticks gibt es wie Sand am Meer. Bei der großen Masse handelt es sich um Container-Verschlüsselungen für das Betriebssystem Windows. Häufig besteht ein solcher USB-Stick dann aus zwei Laufwerken:

1. einem unverschlüsselten Laufwerk für die harmlosen Daten und
2. einem verschlüsselten Laufwerk für die sensiblen Daten.

Kontrollieren Sie stichprobenartig

Die Entscheidung, auf welchem Laufwerk gespeichert wird, trifft der Mitarbeiter. Setzt das Unternehmen eine solche Lösung ein, sollten Sie daher regelmäßig Stichproben machen und so den richtigen Umgang mit den USB-Sticks kontrollieren. Beachten Sie dabei die Mitbestimmung durch den Betriebsrat!

USB-Sticks am Rechner lassen sich auch nachträglich nachweisen

Ob schon einmal ein USB-Stick am Rechner des Mitarbeiters angeschlossen war, lässt sich mit Tools wie USBdeview (*http://www.nirsoft.net/utils/usb_devices_view.html*) leicht kontrollieren.

Da Windows die komplette Historie der verwendeten USB-Sticks seit der letzten Neuinstallation speichert, sieht man alle jemals angesteckten USB-Sticks. Auch bei dieser Kontrolle gilt: Denken Sie an die Mitbestimmung.

Die Hardwareverschlüsselung ist teuer, aber sicher

Vielen Problemen mit USB-Sticks lässt sich aus dem Weg gehen, wenn man nur hardwareverschlüsselte USB-Sticks einsetzt. Sie können nicht unverschlüsselt benutzt werden. Allerdings müssen dazu spezielle USB-Sticks beschafft werden; ein Nachrüsten der Funktionalität mittels Software ist nicht möglich.

Und wegen der besonderen Qualität lassen sich die Hersteller diese Sticks sehr gut bezahlen: Mit rund 80 bis 100 Euro für einen 4-GByte-USB-Stick müssen Sie bei diesen hochsicheren Sticks schon rechnen.

Besonders wichtige Daten auf jeden Fall hardwareverschlüsseln!

Damit eignen sie sich für eine Massenanwendung im Unternehmen zwar nicht – aber zumindest die sensiblen Daten des Unternehmens – quasi die Kronjuwelen unter den Daten – sollten hochwertig geschützt werden.

Schutz der Daten mit Passwort und 256-Bit-Schlüssel

Das Funktionsprinzip ist bei allen Sticks gleich. Von einer kleinen CD-ROM, die der Stick virtuell zur Verfügung stellt, wird eine Software zur Eingabe des Passworts gestartet. Sobald das Passwort korrekt eingegeben wurde, steht das eigentliche Laufwerk zum Speichern der Daten zur Verfügung.

Alle Sticks verschlüsseln die Daten hardwaremäßig mit 256 Bit AES. Betriebssystemabhängige Software wird nur für die Passworteingabe und die Konfiguration des Sticks benötigt.

USB-Stick und Herstellerkontakt	Beriebssystem(e)	Passwortmanagement
Blockmaster Safestick *http://www.prosoft.de/produkte/safestick/*	Win, Mac, Linux	Ja
Ironkey Basic *https://www.ironkey.com/basic*	Win, Mac, Linux	–
Ironkey Enterprise *https://www.ironkey.com/enterprise*	Win, Mac, Linux	Ja
Kingston DataTraveler Vault – Privacy Edition *http://www.kingston.com/deroot/flash/dtvaultprivacy.asp*	Win, Mac	–
SanDisk Cruzer Enterprise *http://www.sandisk.de/Enterprise/*	Win	Ja
takeMS MEM-Drive Crypto AES *http://www.takems.de/products.php?categ=usb&prod=MEM-Drive_Crypto_AES*	Win	–

Hardwareverschlüsselte USB-Sticks und die Betriebssystemunterstützung sowie die Verfügbarkeit eines zentralen Passwortmanagements im Vergleich

Wählen Sie die Sticks passend zum Betriebssystem

Unter Windows können Sie den Autorun- bzw. Autostart-Mechanismus nutzen. Unter Mac OS und Linux müssen Sie das Anmelde-Programm manuell starten – sofern es überhaupt eine Mac-OS- oder Linux-Version gibt. Die Auswahl des konkreten Sticks für das Unternehmen hängt also ganz wesentlich vom Support für die im Unternehmen eingesetzten Betriebssysteme ab.

Beachten Sie, dass – je nach Hersteller – gewisse Funktionen nur unter Windows möglich sind. Der Zugriff auf die verschlüsselten Inhalte ist mit den in der Tabelle angegebenen Betriebssystemen möglich. Das erstmalige Setzen eines Passworts und das Ändern des Benutzerpassworts funktionieren unter Umständen nicht unter allen Betriebssystemen!

Testen Sie die Managementumgebung

Da es immer mal wieder vorkommt, dass Nutzer ihr Passwort vergessen, muss es eine Möglichkeit geben, das Passwort zurückzusetzen, ohne dass die Daten auf dem verschlüsselten USB-Stick verloren gehen. Es versteht sich von selbst, dass dieser Mechanismus entsprechend abgesichert sein muss, damit er keine Sicherheitslücke darstellt. Das Testen der Managementumgebung ist daher der wichtigste Teil der Produktauswahl.

Die USB-Sticks von Blockmaster, SanDisk, TakeMS und Kingston

Prüfen Sie: Hat jemand das Passwort auf den Stick geschrieben?

Durch ein zentrales Policy-Management lassen sich Vorgaben über die Mindestanforderungen an die Passwort-Qualität durchsetzen. Was sich technisch aber nicht verhindern lässt, ist, dass das Passwort ganz trivial auf den Stick geschrieben wird.

Hier helfen nur regelmäßige visuelle Inspektionen der Sticks, wobei Sie wieder an die Mitbestimmung denken müssen.

Aktualisieren Sie ältere Sticks

Die im Dezember 2009 von der Firma SySS gefundene Sicherheitslücke in den Krypto-Sticks von SanDisk und Kingston ist durch Firmwareupdates behoben. Sollten ältere Sticks dieser Firmen im Einsatz sein, ist eine Kontrolle der Firmwareversion erforderlich. Gegebenenfalls müssen die Sticks dann aktualisiert werden.

Die sicherste Variante: sensible Daten hardwareverschlüsseln

Hardwareverschlüsselte USB-Sticks sind alles in allem also die beste Lösung für den Einsatz von Speicher-Sticks in Bereichen, in denen sensible Daten verarbeitet werden.

Mit Softwarelösungen, die nachträglich auf normale USB-Sticks installiert werden, ist eine vergleichbare Sicherheit im Allgemeinen nicht zu erreichen. Ein zentrales Passwort- und Policy-Management wie bei der Hardwareverschlüsselung ist unverzichtbar.

Prof. Dr. Rainer W. Gerling

Rainer W. Gerling ist Datenschutz- und IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft und Honorarprofessor für IT-Sicherheit an der Hochschule München.