

Windows IT Pro

Das Magazin für den Windows-Administrator

Sonderdruck für Prosoft

USB-Flash-Laufwerk mit Hardwareverschlüsselung

Tresor in der Tasche

von Frank-Michael Schlede

Die USB-Sticks haben definitiv Disketten und CDs als Speichermedien „für jeden Tag“ abgelöst. In allen Farben und Formen und mit einem Speichervolumen von bis 64 GByte stehen diese Medien zur Verfügung. Doch gerade im professionellen Einsatz bergen sie Gefahren: Zu leicht ist ein USB-Stick mit seinen Daten verloren. Die hier vorgestellte Lösung soll helfen.

Für Systemadministratoren und IT-Verantwortliche hat der Einsatz von USB-Sticks eindeutig auch eine Schattenseite. Die große Kapazität gepaart mit der handlichen und unauffälligen Bauform machen sie zu idealen Werkzeugen für den unauffälligen Datendiebstahl: So können die Daten eines Exchanges-Servers problemlos in der Hosentasche eines Angestellten die Firma verlassen. Noch viel größer ist häufig jedoch der Angst vor Verlust der Daten auf einem derartigen Medium durch Unachtsamkeit: Wie schnell geht ein USB-Stick verloren, wird an einem Rechner in einer anderen Firma oder im Internet-Cafe vergessen – dann sind sämtliche Daten durch einfaches Anstecken an ein anderes System zugänglich.

Sicherheit auch auf externen Medien: Verschlüsselung ist gefordert.

Um dieses Horrorszenerario zu vermeiden, werden USB-Medien immer häufiger Teil

der übergreifenden Sicherheitsrichtlinien in den Firmen: Das reicht bei fantasielosen IT-Verantwortlichen vom totalen Verbot der Medien bis hin zu ausgeklügelten Strategien, die sicherstellen, dass die Daten nur verschlüsselt auf den USB-Sticks abgespeichert werden. Hier kommt unter anderem häufig die freie Software Truecrypt zum Einsatz. Der Nachteil beim Einsatz derartigen Lösung besteht darin, dass sie bei allen guten pragmatischen Ansätzen, die beispielsweise gerade Truecrypt für den Einsatz auf USB-Sticks mitbringt – zunächst einmal installiert und entsprechend konfiguriert werden muss. Zudem muss der Administrator dafür sorgen, dass die nötigen Updates und Patches für die Software ebenfalls immer auf allen Geräten rechtzeitig eingespielt werden.

Aus diesen Gründen bieten eine ganze Reihe von Herstellern spezielle Lösungen für USB-Flash-Laufwerke an, die eine Ver-

schlüsselung bereits an Bord haben. Dabei gibt es verschiedene Ansätze: Einige Anbieter tun nichts weiter, als normale USB-Sticks mit einer zusätzlichen Software auszuliefern, die sie zuvor konfiguriert und auf das Medium gespielt haben. Viele bieten auch Kombinationen aus Hard- und Software an, die häufig daran krankt, dass die benötigte Software immer zunächst auf dem PC installiert werden muss, an dem der Anwender das Medium dann einsetzen will.

Hardwareverschlüsselung inklusive.

Es gibt aber auch Hersteller, die sich auf reine Hardwarelösungen konzentrieren und auf diese Weise versuchen, nicht nur die Angriffsfläche der Lösung zu verringern, sondern auch das Handling für Anwender und Administratoren deutlich zu vereinfachen. Zu diesen Anbieter gehört auch die schwedische Firma Blockmaster, die sich laut eigener Aussage auf diese Art von Gerä-

ten spezialisiert hat. In Deutschland werden diese Lösungen unter anderem von Prosoft vertrieben. Von diesem Distributor wurde uns auch ein SafeStick Secure USB Flash Drive mit einer Speicherkapazität von 4 GByte zur Verfügung gestellt. Das Gerät traf in einer kleinen Plastikverpackung in der Redaktion ein und wirkte wie ganz normaler zudem kleiner USB-Stick. Die Bauart als schmalere, kleiner Stick wird gerade von Profis bevorzugt, und wer jemals versucht hat, einen der „modernen“ USB-Drives in entsprechend voluminöser Form mit einem der eng beieinander sitzenden USB-Anschlüsse eines Notebooks oder gar eines der Netbook-WinZlinge zu verbinden, wird diese Form ebenfalls zu schätzen wissen. Denn gerade für diesen Bereich, den mobilen Anwender, der seine Daten auf einem derartigen Medium regelmäßig sichert, sind diese USB-Medien laut Distributor auch gedacht, der als einen wichtigen Vorteil dieser Lösung hervorhebt, dass durch ihren Einsatz die mobilen Daten vollständig passwortgeschützt und verschlüsselt abgelegt werden.

Dies wird durch den Einsatz eines Intel-8051-Prozessors erreicht, der in den

USB-Stick integriert wurde. Dieser Onboard-Prozessor verwendet laut Anbieter eine 256-bit AES-Verschlüsselung für die Daten auf dem Medium, während die Kommunikation von und zum Flash-Drive mittels RSA1024 abgesichert wird. Da dies alles in der Hardware geschieht, soll einem eventuellem Angreifer so auch wenig Möglichkeit geboten werden, hier

eine Lücke zu finden. Zudem werben Hersteller und Distributor damit, dass keinerlei Softwareinstallation am PC notwendig ist: Einzige Voraussetzung für den Einsatz des USB-Sticks ist ein Windows-System ab Windows 2000 mit Service Pack 4. Alle neueren Windows-Systeme mit Windows XP und Vista werden laut Hersteller unterstützt. Linux- und MacOS-Systeme können laut diesen Aussagen nur durch die Unterstützung einer virtuellen Maschine von Vmware auf diese Lösung zugreifen.

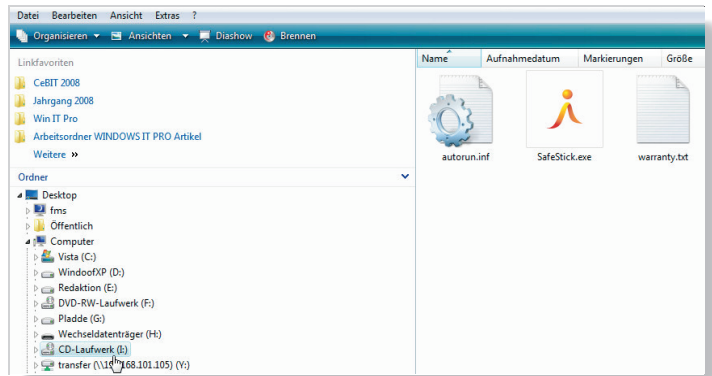


Bild 1. Kann zunächst verwirrend sein: Der SafeStick meldet sich mit zwei Geräten am System an, wobei auf dem „CD-Laufwerk“ die Anwendung zum Login gestartet wird – wenn Autorun nicht deaktiviert ist.

und hier auch mit den USB-Sticks beherrschen. Aber wie viele dieser Medien, die mit einer Verschlüsselung arbeiten, stellt sich das Bild beim ersten Gebrauch solcher Lösungen etwas anders dar: Der SafeStick meldet sich nach der üblichen Benachrichtigung, dass nun neue Systemtreiber installiert seien, mit zwei Laufwerken am System an, wobei das eine Laufwerk wie üblich als Wechseldatenträger und das andere als CD-Laufwerk gekennzeichnet ist (Bild 1). Bei dem Wechseldatenträger han-

SafeStick USB-Flash-Drive

Hersteller:
Blockmaster

Vertrieb in Deutschland:
Prosoft
Tel: 08171/405-200
http://www.prosoft.de

Preis:
in der von uns getesteten 4 GByte-Version (es stehen 512-MByte- sowie 1- bis 32-MByte-Modelle zur Verfügung, 64-MByte-Modelle sind angekündigt) zur Zeit als Schnupperpreis 69,90 Euro; der Anbieter gewährt günstigere Konditionen bei Bestellung einer größeren Anzahl der USB-Sticks.

- Pro:
- transparente Sicherheitslösung mit Hardwareverschlüsselung
 - keine Installation von Software nötig
 - kann an allen aktuellen Windows-Version eingesetzt werden

- Kontra:
- rudimentäre Beschreibung kann unerfahrene Anwender verwirren

Installation und Bedienung: Zunächst nicht selbsterklärend.

Sowohl Hersteller als auch Anbieter des SafeStick scheinen sich ihrer Sache sehr sicher zu sein, wenn sie von der Einfachheit der Bedienung reden: Anders ist es nicht zu erklären, dass der Kunde den USB-Stick in der erwähnten Plastikverpackung erhält, die als „Anleitung“ nur ein Stück Pappkarton enthält, auf dem neben den „Benefits & Features“ und der „Linited Warranty“ in mikroskopisch kleiner Schrift nur drei magere Statements zum Betrieb des USB-Sticks zu finden sind. Diese weisen den Anwender an, den Stick in den USB-Anschluss einzustecken, 30 Sekunden zu warten und dann „zu genießen“ (Enjoy). Etwas kleiner darunter findet der Anwender dann auch einige Hinweise, was er zu tun hat, wenn nach dieser Prozedur nichts passiert: Nach dem obligatorischen Entfernen und Wiederverbinden des Sticks mit dem System soll der Anwender das „Login SafeStick“-Volumen anwählen und auf dieses klicken.

Nun kann man sicher von einem Systemadministrator oder auch von einem routinierten Anwender erwarten, dass er den Umgang mit externen Speichermedien



Bild 2. Eingabe des Passworts: Die Lösung achtet darauf, dass der Anwender ein Passwort eingibt, dass gewissen Sicherheitskriterien entspricht. Es kann nur unter Datenverlust zurückgesetzt werden, wenn nicht das zusätzlich Recovery-Tool zum Einsatz kommt.

```

Eingabeaufforderung
T:\tmp>set PLSCSI=\\.\I:
T:\tmp>plscsi -v
x 00000000 12 00:00:00 24 00 "R@@@#@"
x 00000000 00:80:00:01 1F:00:00:00 42:40:20:20 20:20:20:20 "@@@A @@@BM"
x 00000010 53:61:65:65 53:74:69:63 6B:20:42:45 20:20:20:20 "SafeStick BE"
x 00000020 31:2E:31:30 "SafeStick BE" "1.10"
set PLSCSI=\\.\I: // @ BM SafeStick BE i.10
// 0 = plscsi.main exit int

T:\tmp>plscsi -vx "25 00 00:00:00:00 00 00:00 00" -i 8
x 00000000 25 00 00:00:00:00 00 00:00 00 .. .. .. "x@@@@@@@@@"
x 00000000 AE:AE:AE:AE AE:AE:AE:AE "....."
x 00000000 70:00:02:00 00:00:00:0A 00:00:00:00 3A:00 .. "p@b@@@@J@@@@@"
// x 2 3A sense // 8 residue
// -x0102 = -258 = plscsi.main exit int

T:\tmp>plscsi -vx "28 00 00:00:00:10 00 00:01 00" -i x800
x 00000000 28 00 00:00:00:10 00 00:01 00 "(@@@P@@@@"
x 00000000 AE:AE:AE:AE AE:AE:AE:AE AE:AE:AE:AE "....."
x 00000000 70:00:00:00 00:00:00:0A 00:00:00:00 00:00 .. "p@@@@@J@@@@@"
// x 0 sense // x800 (2048) residue
// -x0102 = -258 = plscsi.main exit int

T:\tmp>

```

Bild 3. Einbruchversuch: Es gelang uns zwar mit dem Freeware-Programm „Plscsi“ grundsätzlich auf den Stick zuzugreifen, wir hatten jedoch während des kurzen Testzeitraums keinen Erfolg bei dem Versuch so an die verschlüsselten Daten zu kommen.

delt es sich um die Partition des Sticks, die dann später die verschlüsselten Daten beinhaltet. Versucht der Anwender auf diese zuzugreifen, so bekommt er die wenig aufschlussreiche Fehlermeldung präsentiert, dass sie kein Datenträger im entsprechenden Laufwerk befindet. Vom Hersteller ist die Installation so geplant, dass die zweite offene Partition als CD-Laufwerk über einen Autostart automatisch das „SafeStick“-Programm ausführt, das dann den Anwender zur ersten Eingabe des Passwortes auffordert (Bild 2). Dies funktionierte in unseren Tests auch sowohl unter Windows XP (SP 3) als auch unter Windows Vista (SP 1) – allerdings nur solange, wie die Autoplay-Funktion der CD-Laufwerke nicht abgeschaltet ist. Da wir das aber den meisten Systemen aus Sicherheitsgründen (schnell ist eine CD/DVD im Laufwerk vergessen und führt dann beim nächsten Start ein vielleicht unerwünschtes Programm aus) immer so halten, passiert natürlich zunächst einmal nichts. Leider konnten wir auf dem Vista-System auf diese Weise so reproduzierbar einen Fehler erzeugen, da das System nicht vorhandenen Datenträger mit der Fehlermeldung „Windows –Kein Datenträger“ monierte und dabei eine „Exception Processing Message“ anzeigt, die erst nach mehrmaligem Klicken wieder vom Bildschirm verschwindet. Hat der Anwender aber das CD-Laufwerk mit dem SafeStick-Programm gefunden und es mit einem Doppelklick gestartet, so kann er in einer aufgeräumten Maske sein Passwort eingeben, wobei das Programm bestimmte Voraussetzung an das Passwort

stellt (Bild 1). So gut es ist, dass dieses Programm kein Passwort zulässt, das nicht mindestens Klein- und Großbuchstaben sowie Zahlen enthält, so unverständlich scheint es, dass es bereits ein acht Zeichen langes Passwort als gültig und sicher akzeptiert. Danach wird der Datenträger automatisch am Windows-System montiert und steht als normales Laufwerk zur Verfügung. Die Anwendung „SafeStick“ wandert als Icon in die Tasktray des jeweiligen Systems, installiert aber keine Software auf dem Rechner. Mit ihrer Hilfe kann der Anwender dann jederzeit das Laufwerk „verriegeln“ und wieder von System abmelden. Auch die „brutale“ Methode, bei der der USB-Stick einfach ohne Abmeldung und vorherige Maßnahmen von System abgezogen wurde, überstand die Lösung in unseren Tests schadlos. Danach kann der Anwender den Stick an einem beliebigen anderem System wieder anstecken, sein Passwort eingeben und weiterarbeiten. Wir haben das Gerät während des Testzeitraums von ungefähr vier Wochen an diversen unterschiedlichen Notebook- und Desktop-Systemen unter Windows XP und Vista ohne Problem einsetzen können. Die Geschwindigkeit war bei der uns zur Verfügung stehen 4-GByte-Version angenehm und reichte für die normalen Arbeiten aus, auch wenn wir die vom Distributor auf dem Webseite versprochenen Geschwindigkeiten von bis zu 22 Mbyte/s beim Lesezugriff und bis zu 19 MByte/s beim Schreiben nicht erreichen konnten. Mit dem freien Tool H2testw in der Version 1,4 konnten wir an unterschiedlichen Sys-

temen eine Schreibrate von circa 7 MByte/s und eine Leserate von knapp unter 16 MByte nachmessen.

Zum Abschluss unseres Tests haben wir das System noch einer kurzen Prüfung mit der Software Plscsi (<http://members.aol.com/plscsi>) unterzogen. Dieses Werkzeug erlaubt es, ähnlich wie früher mit dem AT-Befehlen beim Modems, von der Kommandozeile direkte Befehle an SCSI-Devices abzusetzen. Der Gebrauch solcher Programme ist nur mit größter Vorsicht möglich, da es bei ihren Einsatz auch problemlos möglich ist, den Inhalt eines Speichervolumens unbrauchbar zu machen. Nach der Beschreibung auf der Webseite gelang es uns zwar grundsätzlich auf die Partition auf dem USB-Stick zuzugreifen, allerdings haben wir es nicht geschafft, die dort befindlichen Information in irgendeiner Weise auszulesen. Wie das Bild 3 zeigt, gelang es dem Programm zwar die Bezeichnung des Geräts auszulesen, aber dann wurde nur immer wieder die Zeichenfolge „AE“ ausgegeben, was laut Aussagen der Webseite anzeigt, dass hier kein Auslesen möglich war. Damit ist sicher nicht ausgeschlossen, dass es nicht doch noch einen Weg gibt, mit einem derartigen LowLevel-Programm Zugang zu den Daten auf dem Stick zu erhalten, wir konnten es bei unseren kurzen Tests nicht schaffen.

Vor allen Dingen der unkomplizierte Einsatz, der es erlaubt, den Stick jederzeit an jedem System zu verwenden, hat uns gut gefallen. Für Administratoren ist es allerdings wichtig, die nicht so erfahrenen Anwender zunächst mit der Anwendung einer solchen Lösung und hier vor allen Dingen mit dem Vorhandensein von zwei unterschiedlichen Laufwerken vertraut zu machen. ●



Buergermeister-Graf-Ring 10
D-82538 Geretsried
Tel.: +49 8171 405-219
Fax: +49 8171 405-400
eMail: Robert.Korherr@ProSoft.de