Praktisches Teufelszeug

Umgang mit USB-Sticks in der betrieblichen Praxis

USB-Speicher sind gleichermaßen praktisch wie riskant. Angesichts der immensen Verbreitung dieser handlichen Systeme sollte jede Organisation die zugehörigen Risiken ergründen und Vorsichtsmaßnahmen für den eigenen Gebrauch treffen.

Von Rainer W. Gerling, München

USB-Sticks haben die Diskette als Speichermedium nahezu komplett abgelöst. Durch den enormen Preisverfall und die Verfügbarkeit selbst bei Lebensmitteldiscountern sind sie enorm verbreitet. Im Unternehmen muss man deshalb immer damit rechnen, dass Mitarbeiter auch mal einen privaten USB-Stick mitbringen und in den dienstlichen Rechner stecken, was unter Umständen eine Gefährdung der internen Systeme und Daten bedeutet.

Doch auch offiziell eingesetzte USB-Medien stellen einen Risikofaktor dar: einerseits für die darauf gespeicherten Daten (Verlust, Ausspähung), aber auch als „Store-and-Foward"-Schnittstelle ins interne Netz sowie als Micro-Plattform für (evtl. unerwünschte oder gefährliche) Software. Selbst spezifische Hacker-Tools existieren mittlerweile für die handlichen Systeme.

Formatfragen

USB-Sticks bestehen im Wesentlichen aus einem elektronischen Speicherbaustein (z. B. Flash-Speicher), der mittels Stecker mehr oder weniger direkt an einen Port des Universal Serial Bus (USB) angeschlossen werden kann. Die Datenübertragung zwischen PC und USB-Gerät erfolgt mit 1,5 MBit/s (low speed), 12 MBit/s (full speed) oder 480 MBit/s (high speed, ab USB Version 2.0). Die Speichergröße der Sticks reicht von 16 MByte (im Kostenbereich von Werbegeschenken) bis hin zu mehreren Gigabytes. Derzeit sind Speicher-Sticks mit 1 GByte die gängigsten; die Speichermöglichkeiten übersteigen damit die Kapazität einer CD-ROM um fast 50 Prozent.

USB-Sticks können sich gegenüber dem Betriebssystem entweder als „Superfloppy" oder als Festplatte zu erkennen geben. Bei dem Superfloppy-Format besitzt der Datenträger nur einen Bootsektor ohne Partitionstabelle (wie eine Diskette), im anderen Fall hat er wie eine Festplatte einen Masterbootrecord und eine Partitionstabelle. Dies ist auch der Grund, warum manche USB-Sticks unter Windows mit Wechseldatenträgersymbol und manche mit dem Festplattensymbol dargestellt werden.

Die Unterschiede zwischen den Formaten haben übrigens nichts mit der Hardware zu tun, sondern resultieren ausschließlich aus der Formatierung. Mit dem USB Disk Storage Format Tool von HP kann beispielsweise ein USB-Stick unter Windows als Festplatte formatiert werden (http://h18000.www1.hp.com/support/files/serveroptions/us/download/20306.html).

Beim Anschluss von USB-Speichern an Windows-Systeme laufen – je nach Systemkonfiguration und Inhalt des Datenträgers – verschiedene Vorgänge automatisch oder nach kurzer Bestätigung durch den Benutzer ab, um betriebssystem- (Plug&Play, Treiber, ...) oder applikationsgesteuerte Vorgänge anzustoßen. Auch das Booten eines PCs ist vom USB-Stick möglich: Ob das funktioniert, hängt nicht zuletzt vom BIOS des Rechners ab. Neuere BIOS-Versionen können in der Regel von beiden erwähnten Formaten booten, ältere sind jedoch häufig auf eines festgelegt; hier hilft im Zweifel nur Ausprobieren.

Zur Beschränkung der allgemeinen Nutzung oder der erlaubten Funktionen von USB-Speichern (und anderer Plug&Play-Hardware) gibt es eine Reihe von Windows-Einstellungen (Gruppenrichtlinien etc.) und spezifische Sicherheitssoftware zur Device-Verwaltung, die entsprechend einer Unternehmens-Policy eingerichtet und genutzt werden sollten.

Tarnen und Täuschen

Zudem ist „der Feind" oft nur schwer zu erkennen: Die Bauformen von USB-Systemen sind extrem unterschiedlich. Neben den einfachen Sticks gibt es Armbanduhren, Stifte und sogar Taschenmesser mit integriertem USB-Speicher. Fast wirken solche Devices wie Film-Gadgets eines Geheimagenten. Gibt es im Unternehmen ein Verbot privater Speichermedien, das unter Umständen sogar durch den Werkschutz kontrolliert wird, so „helfen" derart getarnte USB-Sticks beim Ein- oder Ausschmuggeln deutlich dabei, die Regeln zu umgehen. Selbst bei Taschenkontrollen sind sie nur schwer zu entdecken (vgl. Abb. 1).

Eine weitere Erschwernis ist die Größe, beziehungsweise Kompaktheit besonders kleiner USB-Sticks: Die kleinsten sind derzeit die Sony Micro Vault Tiny mit einem Gewicht von 1,5 g und einer Größe von knapp 15 x 3 x 30 mm. Trotz dieser geringen Ausmaße reicht die Speicherkapazität bis zu 2 GByte. Solch eine kleiner Stick lässt sich naturgemäß gut verstecken!

Abbildung 1: USB-Sticks sind heutzutage in verschiedensten Bauformen, als miniaturisierte Varianten oder auch Systeme mit eingebautem Fingerabdruck-scanner erhältlich.

Schreibschutz und Verschlüsselung

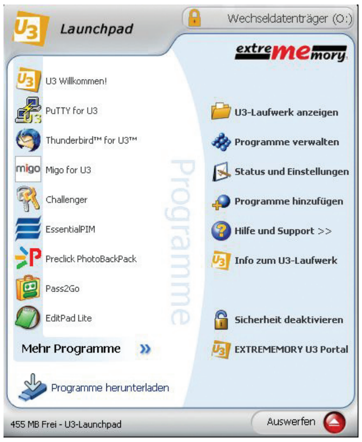
Die einfachste Schutzfunktion ist bei einigen USB-Sticks ein Schreibschutz-Schieber, mit dem sich der Speicher vor einem versehentlichen Löschen schützen lässt. Außerdem verhindert man so, dass Dateien unbeabsichtigt verändert werden.

Darüber hinaus gibt es heute USB-Sticks mit integriertem Finger-abdruck-Scanner; richtig implementiert bietet dies eine große Sicherheit. Bei allen solchen Sticks wird eine Software mitgeliefert, mit der der Fingerabdruck erstmalig eingelesen und dann im Stick gespeichert wird (Enrollment). Leider gibt es diese Enrollment-Programme in der Regel nur für Microsoft Windows. Zur späteren Nutzung wird der Fingerabdruck vom Stick autark, ohne Softwareunterstützung auf dem „Host“-System geprüft; nach der Initialisierung kann der Stick also plattformunabhängig eingesetzt werden.

Zur Signalisierung an das Betriebssystem gibt es dabei zwei Möglichkeiten: Manche Sticks melden, dass kein Wechselmedium eingelegt sei, andere wiederum behaupten der Datenträger sei nicht formatiert. Es hängt nun vom Betriebsystem ab, was nach dem Einscannen des Fingerabdrucks und der Freigabe der Daten geschieht: Mit dem Einlegen eines Wechselmediums kommen alle klar, mit dem plötzlichen nachträglichen „Formatieren“ des Medium haben jedoch einige Betriebssysteme Probleme.

Selbstverständlich lassen sich Daten auf einem USB-Stick auch verschlüsselt speichern; einige Hersteller liefern Verschlüsselungssoftware

Abbildung 2: So genannte U3-Sticks haben ein eigenes Startmenü und arbeiten als „Mikroplattform“, deren Software keine Installation auf dem Gast-PC erfordert. So lassen sich Software-beschränkungen und Installationsverbote eventuell leicht umgehen.



gleich mit. Besser ist es aber, ein klares Betriebs-Konzept im Unternehmen zu erstellen und gegebenenfalls in allgemeinere Verschlüsselungslösungen zu integrieren, die im Einsatz sind. Stellt man technisch durch eine transparente Verschlüsselung sicher, dass Daten nur verschlüsselt auf einem USB-Stick gespeichert werden können, so ist das Kopieren der Daten erheblich erschwert. Es gibt auch bereits Lösungen, die den notwendigen Krypto-Schlüssel im Trusted Platform Module (TPM) des Gast-PCs speichern – dann kann der USB-Stick auch nur an diesem Rechner wieder ausgelesen werden.

Auch Freeware-Lösungen zur Verschlüsselung auf einem USB-Stick sind verfügbar: als empfehlenswert können hier TrueCrypt (www.truecrypt.org) und Axcrypt (www.axantum.com/AxCrypt/) gelten. Axcrypt verschlüsselt einzelne Dateien mit einem Benutzer-Passwort; die Bedienung ist einfach, erfordert aber relativ viel Benutzerinteraktion. TrueCrypt nutzt hingegen eine transparente Container-Datei oder Partitionsverschlüsselung: Auf einem als Harddisk formatierten USB-Stick kann dann eine verschlüsselte Partition eingerichtet werden. Auf jedem Rechner, auf dem TrueCrypt installiert ist, kann man nach Eingabe des Schlüssels auf die chiffrierten Dateien transparent zugreifen. Der so genannte Traveller-Modus ermöglicht den einfachen Zugriff auf die verschlüsselten Dateien auch auf fremden Rechnern, da die notwendigen Treiber mit auf dem USB-Stick liegen. Um TrueCrypt im Traveller-Modus zu starten, sind allerdings Administrator-Rechte erforderlich. TrueCrypt ist für Windows XP/200x sowie Linux ab Kernel 2.6.5 verfügbar.

Mikroplattformen

Ein vergleichsweise junges System ist die U3-Technik zur Absicherung von USB-Sticks (vgl. www.u3.com). Nahezu alle Hersteller bieten ihre Speicher auch als U3-Sticks an; diese sind nur unwesentlich teurer als normale Geräte (weniger als fünf Euro).

Ein U3-Stick meldet beim Betriebssystem zwei Datenträger an: eine circa 6 MByte große CD-ROM und ein Wechselmedium mit dem restlichen Speicher. Über die Windows-Autostart-Funktion des CD-ROMs wird eine Anwendung gestartet, die ein Passwort abfragt. Nur nach richtiger Eingabe ist das Wechselmedium mit seinen Daten zugänglich. Es gibt die U3-Umgebung derzeit nur für Windows. Andere Betriebssysteme können auf den Stick nur zugreifen, wenn der Zugriffschutz zuvor unter Windows deaktiviert wurde.

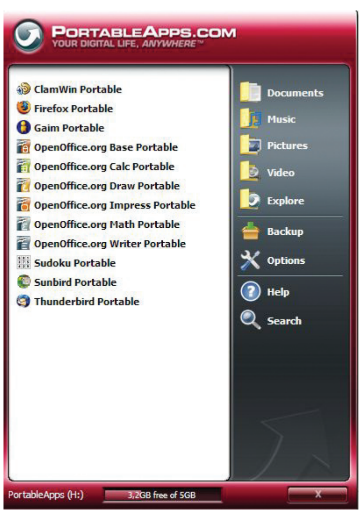
Gleichzeitig stellt die Autostart-Anwendung eine Menüoberfläche zur Verfügung, mit der die auf dem Stick installierte Software gestartet werden kann (s. Abb. 2); Software für praktisch alle Bereiche findet man auf dem U3-Portal (http://software.u3.com). Das besondere ist, dass U3-angepasste Software nicht auf die Festplatte des Rechners zugreift: Sie arbeitet also, ohne Spuren auf dem Gast-Rechner zu hinterlassen. Das hebelt Verbote aus, Software zu installieren, die in der Nutzerordnung festgelegt sind.

Wichtige Software, die es als U3-Version gibt, sind beispielsweise der E-Mail-Client Mozilla Thunderbird, der Browser Mozilla Firefox, das Instant-Messaging-Programm Trillian, die Telefonie-Software Skype (!), die Sicherheits-Tools WinSCP und Putty sowie ein kleiner Mobile-Web-Server, der Dateien vom USB-Stick im Netz anbieten kann. Hinzu kommt verschiedenste Verschlüsselungssoftware. Eine Besonderheit der U3-Umgebung: Zieht man den Stick ab, werden alle laufenden U3-Anwendungen sofort beendet („The boss is coming“-Funktion). Der Passwortschutz des U3-Sticks schützt somit nicht nur die Daten, sondern auch installierte Programme vor ungewolltem Zugriff.

Der Inhalt der rund 6 MByte großen „CD-ROM“ lässt sich zudem aktualisieren: Findige Leute haben den zugehörigen Mechanismus geknackt und es ist nun möglich ein eigenes „CD-Image“ zu installieren. Damit kann über den CD-Autostart-Mechanismus eines U3-Sticks beispielsweise auch Schadsoftware eingeschleust werden; hierzu sind bereits fertige Programmpakete erhältlich.

Doch selbst für Nicht-U3-Sticks gibt es Software, die ohne Installation auf dem „Host“ arbeitet: Die Web-Seite PortableApps beherbergt solche Anwendungen (http://portableapps.com). Ausgesprochen

Abbildung 3: Auch für Nicht-U3-Sticks gibt es umfangreiche Software, die ohne Installation auf dem Host-System arbeitet (Bild: Startmenü der PortableApps-Suite).



interessant ist beispielsweise die PortableApps Suite (Standard Edition), bestehend aus einer Menü-Oberfläche, einem Backup-Programm sowie dem Viren-Scanner ClamWin, dem Browser Mozilla Firefox, dem Instant-Messaging-Programm Gaim, dem Paket OpenOffice, einem Sudoku-Spiel, dem Kalender Mozilla SunBird und dem E-Mail-Programm Mozilla Thunderbird. Benötigt wird lediglich ein beliebiger USB-Stick mit mindestens 512 MByte. Für Individualisten gibt es alle Komponenten auch einzeln sowie zum Beispiel das Paket XAMPP (Apache, mySQL, PHP, phpMyAdmin) zum Betrieb eines Web-Servers vom USB-Stick.

Attacke!

Der Albtraum eines USB-Stick-Nutzers ist das Tool USB-Dumper: Es läuft unbemerkt im Hintergrund von Windows-Systemen und kopiert den kompletten Inhalt eines eingesteckten USB-Sticks heimlich auf die Festplatte. Die aktuelle Version 2.2 des USB-Dumpers geht noch einen Schritt weiter: Sie kann auch unbemerkt Dateien *auf* den Stick kopieren und alle darauf gespeicherten Word- und Excel-Dateien mit einem Autostart-Makro versehen (potenziell Malware). Die Konfiguration des Hacker-Tools ist bequem über eine grafische Oberfläche möglich (s. Abb. 4).

Der sicherheitsbewusste Anwender benötigt daher regelmäßig zwei USB-Sticks: Einen „öffentlichen“, den er auch mal an einen fremden Rechner steckt, um eine Datei dorthin zu kopieren, und einen persönlichen, den er nur mit eigenen Rechnern verbindet. Daten, die Dritte nicht sehen dürfen, kommen nur auf den persönlichen Stick – im betrieblichen Einsatz empfiehlt sich eine entsprechende Regelung in den Policies.

Einen anderen Ansatz hat das Hacker-Projekt „USB Switchblade“: Es versucht durch geschickte Anwendung von Autorun- beziehungsweise U3-Mechanismen fremde Rechner auszuspionieren. Auf normalen USB-Sticks wird dazu eine simple autostart.inf-Datei verwendet:

```
[autorun]
icon=folder.ico
action=Gefährlichen Trojaner
       öffnen
shellexecute=\trojaner\
       tr.exe
```

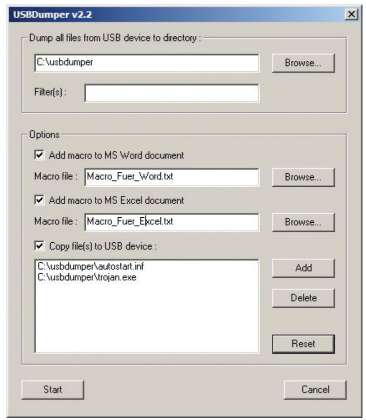


Abbildung 4: Die Konfiguratonsoberfläche des USBdumper 2.2

Standardeinstellungen auf dem „gastgebenden“ Windows vorausgesetzt, erzeugt man damit nach dem Einstecken des USB-Sticks die Dialogbox aus Abbildung 5. Dieser

Abbildung 5: Mit der im Text angegeben autostart.inf-Datei wird diese Dialogbox beim Einstecken eines USB-Sticks angezeigt (Windows-Default-Einstellungen vorausgesetzt). Bei geeigneter Wahl von Icon und Text der ersten Zeile sind somit durch eine Kombination aus Technik und Social Engineering erfolgversprechende Angriffe möglich.

Angriff ist eine Mischung aus Technik und Social Engineering: Icon und Text der ersten Zeile (bzw. der autostart.inf) sind natürlich „geeigneter“ zu wählen. Es versteht sich von selbst, dass der Einsatz solcher Tools unter den Straftatbestand des Ausspähens von Daten fällt.

Hackergruppen arbeiten zudem an einer Kombination von USB-Dumper und den U3-Autostart-Mechanismen. Das Ziel ist es, auf einem fremden Rechner den USB-Dumper zu installieren und die Inhalte aller nachfolgend angesteckten USB-Sticks per verschlüsselter E-Mail an den Angreifer zu schicken. Dieses Projekt läuft unter dem Namen „USB Hacksaw“.

Unter den genannten Gesichtspunkten sind somit auch fremde USB-Sticks am eigenen Rechner nicht unkritisch. Zumindest sollte der Windows-Autostart für alle Laufwerke deaktiviert sein, damit solche Software nicht ohne Weiteres starten kann.

Fazit

Der sichere Umgang mit USB-Sticks im Unternehmen erfordert zwei Mechanismen: eine Policy sowie technische Schutzmaßnahmen. Die Benutzerordnung kann leicht erstellt werden (siehe Kasten). Zur technischen Sicherheit bieten etliche Hersteller Softwarepakete an, die den Zugriff auf angesteckte USB-Geräte unterbinden oder einschränken. Sollen personenbezogene, vertrauliche oder anderweitig schutzbedürftige Daten auf einem USB-Stick gespeichert werden, so muss eine Verschlüsselung als obligatorisch gelten. ■

Prof. Dr. Rainer W. Gerling ist Datenschutz- und IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft.

USB-Stick-Policy

Die folgenden Punkte sollten in einer Nutzerordnung beziehungsweise Betriebsvereinbarung geregelt sein:

- Die Nutzung privater USB-Sticks im Unternehmen ist nicht erlaubt.
- Das Starten nicht-freigegebener Software von einem USB-Stick ist nicht erlaubt.
- Sind auf dienstlichen USB-Sticks personenbezogene oder andere vertrauliche Daten gespeichert, so muss der USB-Stick am Arbeitsplatz verbleiben und bei Nichtnutzung weggeschlossen werden.
- Werden auf dienstlichen USB-Sticks personenbezogene oder andere vertrauliche Daten transportiert, so sind die gespeicherten Daten zu verschlüsseln.
- Dienstliche USB-Sticks mit personenbezogenen oder anderen vertraulichen Daten dürfen nicht an unternehmensfremde Rechner angeschlossen werden.
- Zum Anschluss an unternehmensfremde Rechner ist ein seperater USB-Stick zu nutzen. Dieser muss über einen Schreibschutzschalter verfügen und darf nur öffentliche Daten enthalten.
- Für die Einhaltung der Regeln ist der Mitarbeiter verantwortlich, dem der Stick zur dienstlichen Nutzung überlassen wurde.
- Ein Verstoß gegen diese Regeln hat arbeitsrechtliche Konsequenzen.

Erhält eine Mitarbeiterin oder ein Mitarbeiter einen dienstlichen USB-Stick, so sollten diese Regeln mit Übergabe des USB-Sticks schriftlich ausgehändigt und gegebenenfalls unterschrieben werden. Der Anschluss unternehmensfremder USB-Sticks an Rechner im Unternehmen ist in der allgemeinen Policy zu regeln.