Veröffentlicht am: 22. Februar 2007
Medium: InformationWeek

# *USB-Schnittstelle wasserdicht abgesichert*

***von Jürgen Höfling***

***Mobile Speichergeräte wie USB-Sticks oder MP3-Player sind heute allgegenwärtig. Für die Unternehmenssicherheit können diese Geräte eine große Gefahr darstellen. Ein effizientes Schnittstellenmanagement ist deshalb unabdingbar.***

Während Unternehmen etwa ihren E-Mail-Verkehr verschlüsseln oder dafür sorgen, dass Daten auf mobilen Endgeräten wie Notebooks oder PDAs sicher abgelegt sind, kümmern sich bisher nur wenige um den Zugang, über den sich mühelos Gigabytes von Daten in die Firma einbringen und aus ihr herausschaffen lassen: die USB-Schnittstelle. Dabei steht diese Schnittstelle plus Speicherstift exemplarisch für eine stetig wachsende Zahl von leistungsfähigen und deshalb sicherheitskritischen Geräteschnittstellen (PCMCIA, Infrarot, Bluetooth, Firewire, WLAN). Der Vielfalt der Peripheriegeräte und damit den für die Unternehmen nutzbringende Einsatzszenarien in den wertschöpfenden Geschäftsprozessen sind schier keine Grenzen gesetzt. Digitale Kameras und Diktiergeräte, USB-WLAN-Konverter, PDAs mit E-Mail an Bluetooth oder WebCams stehen den Anwendern zur Verfügung. Diese Vielfalt macht deutlich, dass neben den potenziellen Sicherheitslücken hier auch erhebliche Anforderungen an das Systemmanagement gestellt werden. »Sicherheitsbewusste Unternehmen wollen ganz detailliert den Einsatz der Geräte, die Sicherung der Daten und das Management der Speichermedien bis hin zur Inventarisierung oder der Verwaltung des Geräteparks geregelt wissen«, erläutert Ramon Mörl, Geschäftsführer des Münchener IT-Sicherheitsspezialisten itWatch. Damit ist klar, dass man das Problem mit herkömmlichen Windows-Bordmitteln (in Windows XP gibt es ja dafür einige wenige Stellschrauben) nicht in den Griff bekommt. Das ist auch deshalb nicht weiter verwunderlich, weil die durchaus zweischneidigen Segnungen der automatischen Geräteerkennung von Systemen wie Windows XP das Problem zwar nicht geschaffen, aber doch richtig virulent gemacht haben.

**Unterschiedliche Schwerpunkte**

Peripherie-Management ist sehr eng mit Themen wie Rechteverwaltung, Authentisierung und Autorisierung sowie Datenträgerverschlüsselung verbunden (siehe Kasten Seite 32). Die einzelnen Anbieter setzen angesichts der Vielfalt der Segmente unterschiedliche Schwerpunkte. Digitronic aus Chemnitz beispielsweise lässt nur zertifizierte USB-Sticks (Personalisierung der Geräte über die Seriennummer) zu. Matt Fisher, Vice President Marketing des britischen Herstellers Centennial, hält davon nicht viel: »Das Management dieser Sticks dürfte einen erheblichen Aufwand bereiten. Jede Seriennnummer muss ja erst einmal gescannt werden«. Centennial wie auch der Anbieter Msystems aus Israel meinen, das Problem lasse sich mit der Vorgabe, dass nur standardisierte Geräte benutzt werden dürften, lösen. Mit dem Programmpaket Safeguard Advanced Security von Utimaco hingegen lassen sich einem Speicherstift nur bestimmte Laufwerksbuchstaben zuordnen, für die dann beispielsweise nur der Import, aber nicht der Export von Dateien erlaubt ist. Wer den Export von Dateien nicht gänzlich verbieten wolle, könne auch nur das Speichern bestimmter Dateiformate gestatten, erklärt Helmut Dansachmüller, Leiter Produktmanagement bei Utimaco. Zugriffsregeln, die auch auf Inhalts-Ebene bestimmbar sind, bringt Digitronic in der neuesten Version seiner Sicherheitslösung Authention. Und itWatch erlaubt die Klassifizierung von Dokumenten für die USB-Speicherung. Je nach ihrer Sensibilität dürfen Daten von bestimmten Benutzergruppen entweder nur gelesen oder auch verändert und gespeichert werden. Und nur manche Mitarbeiter dürfen sie auch mit nach Hause nehmen.

**Sichere Datenhaltung**

Auch in punkto sichere Aufbewahrung der Daten auf den mobilen Speichergeräten haben die unterschiedlichen Hersteller verschiedene Lösungsangebote. Utimaco etwa bringt über seine

Kompetenzen in der Verschlüsselung ganzer Festplatten von Haus aus entsprechende Mechanismen mit, kann aber nur den ganzen Speicherstift mit jeweils einem Schlüssel chiffrieren. ItWatch bietet mit PD Watch die Möglichkeit, einzelne Verzeichnisse anzulegen und verschiedene Schlüssel selbst zu wählen. Digitronic und Msystems haben derzeit keine Verschlüsselung. Es empfiehlt sich bei diesen Systemen auf jeden Fall die Verwendung von mTrust Ready-Speicherstiften, die einen Kryptochip eingebaut haben (bei Msystems ist mTrust sogar vorgeschrieben).

**Überwachungs- und Steuerungsmechanismen**

Gerade durch den Einsatz von Betriebssystemen mit automatischer Geräteerkennung ergibt sich ein erheblicher Bedarf an Überwachungs- und Steuerungsfunktionen, da der Plug&Play-Kern von Windows XP (und übrigens auch von Vista) keine hochwertigen netzweiten Managementfunktionen anbietet. Die Lösung Device Wall von Centennial liefert laut Angaben des Herstellers einen vollständigen Überblick über die Geräte, die ans Netzwerk angeschlossen wurden. Auch Safend hat mit Auslieferung der Version 3.0 seines Safend Protector nachgezogen. Ein zentraler Management-Leitstand soll eine einheitliche Verwaltung von Richtlinien, Logs und Protector-Clients gewährleisten. Auch Msystems betont, mit dem mTrust Manager den gesamten Lebenszyklus mobiler Speichermedien im Griff zu haben. Doch Anforderungen wie automatisierte Inventarisierung, Inventar-Management aller mobilen Geräte oder die Inventarisierung und Bereitstellung von Treibern auf Bedarf erfüllen nur wenige Sicherheitslösungen.

Übergreifende Sicherheitslösung gefragt »Manche Produkte unserer Wettbewerber mögen wohl in einzelnen Features besser sein«, räumt Matthias Kirchhoff, Geschäftsführer und Gründer des Chemnitzer Unternehmens Digitronic, ein. »Was aber die Ganzheitlichkeit der Sicherheitslösung angeht, dürften wir wohl ziemlich deutliche Vorteile besitzen«, so Kirchhoff. Die Lösung Authention führt die Komponenten »Logon, SafeMode Block, Single Sign On, Virtual Private Drive, Crypted Group Share, Universal Device Block, Extended Device Block« und ein Token-Management-System zusammen. itWatch bietet ebenfalls eine ganze Produktsuite an, und zwar DeviceWatch (Gerätesicherheit), PDWatch (Verschlüsselung), XRayWatch (Contentkontrolle, Patternprüfung, Shadowing), DEvCon (Systems Management) und CDWatch (medienbasierte Sicherheit).

Überzeugungsarbeit unabdingbar

Was die Sensibilität der Anwender für die Sicherheitsproblematik der USB-Schnittstelle anlangt, geben die befragten Hersteller recht unterschiedliche Eindrücke zu Protokoll. Kirchhoff von Digitronic meint, dass sich das Thema nur über Umwege, sprich über das Angebot einer Komplettlösung für ein ursprünglich anderes Security-Leck, verkaufen ließe. Utimaco klingt dagegen geradezu euphorisch. Noch vor zwei Jahren habe man die Unternehmen bekehren müssen, jetzt kämen sie von allein, meint Helmut Dansachmüller. »Unsere Kunden wissen um die Notwendigkeit, die Kontrolle über das Endgerät zurück zu erlangen«, ist sich Gil Server von Safend, sicher. Thorsten Scharmatinat von itWatch wiederum ist eher über das Abwarten der Unternehmen besorgt: »Viele scheuen beim Peripherie-Management vor der Vielfalt der zu verwaltenden Geräte zurück«