

Datensicherheit

Der Feind in meinem Netz!

Wer kennt sie nicht die beliebten USB-Sticks, mit denen man eine große Zahl von Informationen in kürzester Zeit von PC zu PC transportieren kann. Unbemerkt von der Geschäftsleitung können somit wichtige Daten von z.B. potenziellen Kunden zum Mitbewerber gelangen. Neben dem USB-Stick als komfortabelste Lösung gehören auch iPods, digitale



Foto: TGZ

USB-Sticks als Massenspeicher sind notwendig, bergen aber auch Gefahrenpotenzial. Umso wichtiger ist eine einheitliche Sicherheitsstrategie.

Kameras oder CDs/DVDs zu der Kategorie Massenspeicher, die durch Vorteile wie einfache Mobilität und Verwendbarkeit an jedem beliebigen Computer glänzen. Eine zweite Gefahrenquelle ist die Einschleusung von Viren und Trojanern – vorbei an der Firewall in das Unternehmensnetzwerk. Niemand unterstellt dabei seinen Mitarbeitern, dass sie potenzielle Datendiebe sind oder dass sie wissentlich, gar

vorsätzlich, Viren und Trojaner in das Firmennetzwerk importieren. Leider sieht die Realität anders aus. Aktuelle Studien belegen, dass IT-Abteilungen vor allem mit der Gefahr externer Speichermedien kämpfen. Dabei können Speichermedien nicht gänzlich verboten werden. Ferner müssen im ersten Schritt Richtlinien für den Umgang festgelegt und an die Mitarbeiter kommuniziert werden. Im zweiten Schritt, zur Kontrolle der Umsetzung der Richtlinien und zur Gewährleistung der Sicherheit im Unternehmen, ist der Einsatz einer einfachen und effizienten Technologie gefragt. Diese muss mit wenig Aufwand und leichter Bedienbarkeit die Administration optimal unterstützen.

Software reglementiert Gerätezugriffe

Der USB-Blocker PLUS vom Institut für System-Management aus Rostock ist so eine einfache Lösung. Er reglementiert an den Clients, wer wann auf welche Geräte zugreifen darf. Dabei benötigt der USB-Blocker keine Datenbank, da er auf den vorhandenen Gerätemanager aufbaut. Die Verwaltung der zu sperrenden oder zuzulassenden Geräte erfolgt über die Erstellung von Benutzergruppen im

Active Directory bzw. Novell Directory System. Die zu sperrenden Speichergeräte können mit Hilfe des integrierten Admin-Tools von der Klasse (USB-Stick) über den Hersteller bis hin zur eindeutigen Kennung (ID) unterschieden werden. Sämtliche Schnittstellen wie USB, Firewire, PCMCIA, Bluetooth oder interne Laufwerke wie CD/DVD, Diskettenlaufwerke und Flashcardreader können kontrolliert werden. Unabhängig von der Anzahl der Benutzer, von einigen wenigen bis hin zu mehreren Tausend, kann der USB-Blocker eingesetzt werden.

Sicherheitskonzept muss sein

Abschließend ist festzustellen, dass mobile Endgeräte in unserer technikaffinen Welt im Geschäftsalltag zwar nicht mehr wegzudenken sind, aber zur Minimierung der bereits beschriebenen Risiken Schutzmaßnahmen, wie eine Sicherheitssoftware, umgesetzt werden müssen. Dieses Sicherheitsprogramm funktioniert ohne Probleme. Doch auch wenn alle Schnittstellen des PCs abgesichert werden, liegt es doch am Ende am Benutzer selbst, wie er mit den für ihn autorisierten Speichermedien umgeht.

Abstract

Nobody wants to shelter his employees being a potential data theft or importing dangerous software like viruses and trojans intentionally to company's network. Unfortunately in reality, things are different. Current studies show that CIOs mainly cope with the risk of external storage media. There-with these storage media cannot be forbidden completely.

Furthermore at the first step there have to be defined guidelines for the handling and these have to be communicated to the employees, of course. At the second step the deployment of a simple and efficient technology is necessary in order to realize the guidelines and consequently to guarantee the security in the company.

The required technology has to support the administration by high usability and without causing considerable expenditure. The USB-Blocker of the Institut für System-Management is such a simple but efficient technology.

ISM-Institut für System-Management GmbH

Marco Laß
Oldendorfer Straße 12
D-18147 Rostock
Tel.: +49(0)381 375730
Fax: +49(0)381 3757329
www.usb-blocker.de
marco.lass@secu-sys.de