Das braucht man wirklich!

Endgerätesicherheit muss die steigenden Anforderungen aller Geräteklassen erfüllen

Die Sicherheitsdefizite durch die generische Plug & Play-Pforte für Peripheriegeräte wie USB Memory Sticks, Flash Pens, digitale Kameras, Scanner, Modems etc. sind seit Langem bekannt: Unerwünschte Inhalte und gefährliche Programme bedrohen die Integrität der Netze, und entscheidendes Know-how des Unternehmens kann unerkannt abgezogen und vervielfältigt werden (Data Loss oder Data Leakage).

Das Tempo der Innovationen in der IT-Branche ist hoch, und das Wachstum der Möglichkeiten im IT-Sektor steigt rasant. So ist es kein Wunder, dass mehr und mehr Unternehmen aller Größenordnungen auch ihre wertschöpfenden Prozesse auf den Einsatz von innovativen mobilen Lösungen rund um die Peripheriegeräte ausrichten. „Volatile" Peripheriegeräte und immer mehr schnurlose Schnittstellen kommen zu den „festen" Geräten wie Maus, Tastatur und Drucker in einem Ausmaß hinzu, das bis vor ein paar Jahren unvorstellbar war. So haben Memory Sticks, PDAs, Flash Pens und digitale Kameras auf Basis von Innovationsdruck und Kosteneffizienz mittlerweile ihren festen Platz in den IT-Umgebungen. Alle diese neuen Geräte müssen inventarisiert und ggf. personalisiert werden, damit weiterhin Überblick herrscht, welche Geräte wann und wo welchen Nutzen bringen. Der IT-Manager wird aber nicht in gleichem Maße Personal- oder Zeitzuwachs erhalten haben, sondern muss weiterhin in einem identischen Zeitrahmen die erhöhten Anforderungen an die IT-Umgebung bedienen.

Die IT-Abteilungen der Unternehmen können das Problem zudem mit Bordmitteln nicht in den Griff bekommen. Auch die von Microsoft vorgestellten Betriebssysteme Windows Vista, Windows 7 oder Windows 2008 Server bieten hier keine Lösung an. Viele Lösungen am Markt decken aber häufig nur einen Teil der Problematik ab. Zu den Interessen aus der IT-Sicherheit kommen noch die Anforderungen des Betriebes nach Effizienz und Kostensenkung sowie die Notwendigkeit, den Benutzer bei komplexeren Einsatzszenarien zu unterstützen.

Das Thema der Endgerätesicherheit (Endpoint Security) ist damit viel breiter, als nur eine effiziente Zugangskontrolle für jedwede Geräteschnittstelle, sei es USB, Firewire, Bluetooth, PCMCIA, Infrarot etc. zu realisieren. Eine umfassende Lösung für die Endgerätesicherheit muss heute vieles leisten.

Abb. 1: Vorsicht Datenklau: Schützen Sie sich vor Hackern und machen Sie Ihr System einbruchsicher.

Die Herausforderungen

- Device Kontrolle – Wer darf welches Device (Peripheriegerät und fest verbaute Hardware) wann und wo nutzen? Natürlich darf für eine neue Geräteklasse oder Schnittstellenklasse kein Update vom Hersteller nötig werden.
- Verschlüsselung der mobilen Datenträger – Die Verfahren der Vergangenheit (z.B. Partitionsverschlüsselung) haben ausgedient, da der Bedarf an Vertraulichkeit zunehmend von den Dateiinhalten und ihrer Sensitivität abhängt und nicht mehr alle Daten einheitlich klassifiziert und behandelt werden können.
- Personalisierung von Datenträgern – Günstige Datenträger verfügen über keine eigenen Merkmale wie Seriennummern. Die Verwendung von Datenträgern in besonders kritischen Bereichen (Vorstand, Akquisition, Stabsabteilungen etc.) erfordert es aber aus Gründen der Compliance, wesentliche Datenbewegungen beweisbar abzulegen. Die Personalisierung von Datenträgern für Nutzer oder Projektgruppen ist hier Voraussetzung.
- Kontrolle der Anwendungen – Die Unterscheidung zwischen erlaubten und nicht erlaubten Anwendungen erfordert aus praktischen Gründen den Einsatz von Whitelists UND Blacklists. Z.B. muss der Einsatz „kleiner" Programme auf einigen Rechnern des Unternehmens spontan möglich sein, indem durch Blacklisting in Echtzeit neue Anwendungen an eine zentrale Stelle gemeldet werden, die eine sofortige Entscheidung auslöst.
- Protokollierung aller verwendeten Geräte und ausgetauschten Dateien – Blockieren und Freigeben allein genügt heute schon lange nicht mehr. Die Beweisbarkeit von Datenbewegungen ist in vielen IT-Umgebungen zum kritischen Faktor geworden. Die Begrenzung der Protokollvolumina durch geeignete Verfahren ist hier zwingend – insbesondere, wenn die gesamten Dateninhalte (also nicht nur Dateinamen) protokolliert werden müssen.
- Kontrolle der verwendeten Netze – Durch die Unterscheidung zwischen erlaubten und nicht erlaubten Netzen kontrolliert die IT-Abteilung die Kontakte. Entsprechend des erkannten Netzes muss die Security Policy in Echtzeit eingestellt werden – z.B. Heimarbeitsplatz, Firmenzentrale, Standort Produktion, Schulung etc.
- Alerting – Die Benachrichtigung der bereits etablierten Intrusion-Detection-Verfahren, also die unkomplizierte Integration in Drittprodukte, ist hier genauso wichtig wie die Möglichkeit, Echtzeitreaktionen auf kritische Ereignisse zu konfigurieren.
- Management Information, Reports und Quota-Management (Datenmengen-Management) geben historische oder Echtzeit-Auskunft über die Nutzung und den Netzzustand nach Standorten, Abteilungen oder anderen Kriterien.

Abb. 2: In kritischen Bereichen ist die Personalisierung von Datenträgern unverzichtbar.

Diese Anforderungen an die Endgerätesicherheit sind natürlich alle in Echtzeit, an allen Geräteschnittstellen (USB, Firewire, Bluetooth, WLAN etc.), für alle Geräteklassen, für alle Benutzer und für alle Dateien oder Informationen zu leisten.

Bei dem Blick auf die bestehenden Softwarelösungen im Markt zeigt sich, dass die Lösungen auf der Systems-Management-Seite kaum Funktionen in der IT-Sicherheit haben, die über das Blockieren und Protokollieren hinausgehen. Die Produkte aus der Sicherheitswelt haben aber fast alle keine Mehrwerte im Systems Management.

Zwischen den unabhängigen „Welten" Systems Management, IT-Sicherheit, einfache Nutzbarkeit für Endanwender und Administratoren, Compliance, Applikationskontrolle und Security Awareness der Nutzer müssen also effektive Brücken gebaut werden, welche zudem hohe Kosteneinsparpotentiale ausnutzen durch ein einfaches Rollout mit einer automatisierten Integration in alle vorhandenen Prozesse. Einzige Ausnahme ist hier die Endpoint Security Suite der itWatch, die zusätzlich zu den umfassenden Sicherheitsfunktionalitäten auch alle Wünsche aus dem Systems Management erfüllt.

Kontakt:
Dipl.-Inform. Ramon Mörl
Geschäftsführer
itWatch GmbH, München
Tel.: 089/62030100
info@itWatch.de
www.itwatch.de