USB Sicherheit

Das braucht man wirklich!

Thorsten Scharmatinat, Key Account Manager itWatch GmbH

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 sowie gefährliche Programme bedrohen die Integrität der Netze und entscheidendes Know-how des Unternehmens kann unerkannt abgezogen und vervielfältigt werden (Data Loss oder Data Leakage).

Die IT-Abteilungen der Unternehmen können das Problem mit Bordmitteln nicht in den Griff bekommen. Viele Lösungen sind am Markt, diese 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 mit der nötigen Information in Echtzeit zu unterstützen.

Das Thema der Endgerätesicherheit (*Endpoint Security*) ist damit viel breiter als nur eine effiziente Zugriffskontrolle für alle Geräteschnittstellen, seien es USB, Firewire, Bluetooth, PCMCIA, Infrarot etc., zu realisieren. In der Folge führen wir eine Bestandsaufnahme durch, was eine Lösung in bestimmten Anwendungsszenarien für die Endgerätesicherheit heute leisten muss, um nicht nur einen Ad-hoc-Bedarf sondern auch die Anforderungen der späteren Projektphasen abzudecken.

Device- und Port-Kontrolle

Wer darf welches Device (Peripheriegerät und fest verbaute Hardware) wann und wo in welcher Situation nutzen? Für eine neue Geräte- oder Schnittstellenklasse darf kein Update vom Hersteller der Sicherheitssoftware nötig werden. Die Nutzung von WLAN oder UMTS ist beispielsweise nicht an bestimmte Nutzer gebunden, sondern abhängig von den erreichbaren

Netzen (*friendly net detection*), den Kommunikationskosten und der Doktrin: „Zu einem Zeitpunkt nur eine aktive Netzwerkkarte“.

Content Kontrolle

Das Lesen von Word- oder PDF-Dokumenten von CD/ DVD mag freigegeben sein, aber es muss sichergestellt sein, dass diese Dokumente keine eingebetteten Schadprogramme enthalten (*embedded executables*). Das vollautomatische Erkennen von Java-Skript in PDF-Dokumenten hätte Anfang diesen Jahres erheblichen Schaden verhindert. Die inhaltliche Analyse muss natürlich auf Archiven (ZIP etc.) und auf verschlüsselten Dokumenten oder Archiven mit den gleichen Mechanismen durchgeführt werden.

Protokollierung und Alerting

Blockieren und Freigeben alleine genügt nicht, vielmehr ist bei den freigegebenen, sicherheitskritischen Aktionen auch die Protokollierung gefordert. Die Beweisbarkeit verschiedener sicherheitskritischer Aktionen ist heute in vielen Umgebungen ein notwendiger Teil der Compliance geworden. Um die Datenflut zu begrenzen, ist ein ausgeklügeltes Filterverfahren mit einfacher Administration notwendig. Bestimmte Ereignisse erfordern eine Echtzeitreaktion, wie etwa ein Alerting per Email oder SMS an einen vordefinierten Verteilerkreis. Sicherheitskritische Aktionen können u.a. sein:

- Datenbewegungen sensibler Daten,
- Nutzung kritischer Hardware (*Devices*) oder Anwendungen (*Applications*),
- der Zugriff von Anwendungen auf sensible Dateien,
- die Trennung der sicherheitsrelevanten Information (z.B. Vergabe eines neuen Schlüssels) von Systemmanagement-Information (z.B. Nichtverwendbarkeit eines USB-Gerätes wegen zu geringer Stromversorgung),
- Sonderfreigaben über Challenge Response oder Selbstfreigabe,
- Ausdruck (*Print*) sensibler Information,
- Netzwerkkontakte mit bestimmten Eigenschaften.

Alle Aktionen sind nach dem jeweiligen Nutzungskontext, etwa Uhrzeit, Wochentag etc., zu beurteilen, um die richtige Einschätzung in Echtzeit treffen zu können.

Benchmark des Risikos

Die Protokollierung gibt die richtige Auskunft über die aktuelle Risikosituation und ermöglicht es, die Risiken anonym oder pseudonym in Qualität und Quantität direkt in das Risiko-Management zu übergeben. So kann immer auf Basis der realen Situation gehandelt werden.

Verschlüsselung sensibler Information

Die Angriffe im ersten Quartal 2010 haben die Unsicherheit vieler selbstverschlüsselnder Memory-Sticks gezeigt. Die häufig verwendete Partitionsverschlüsselung hat wesentliche Nachteile, da ein einziger Schlüssel große Datenbereiche unwiderruflich frei gibt und die Daten für sogenannte USB-Dumper vollständig offen liegen. Der Bedarf an Vertraulichkeit ist zunehmend von den Dateiinhalten und ihrer Sensitivität abhängig. Deshalb sind moderne Verfahren mit Unternehmensschlüsseln und privaten Schlüsseln ausgestattet, die je nach Berechtigung des Anwenders und der Sensitivität der Daten zu einer optionalen oder zwangsweisen Verschlüsselung der Inhalte mit den richtigen Schlüsseln führen. Die zwangsweise Verschlüsselung mit einem Firmenschlüssel reduziert das Risiko des Datendiebstahls (Data Loss) auf null Prozent.

Kontrolle der Anwendungen

Das Monitoring aller Anwendungen, deren Start überhaupt versucht wurde, mit den authentischen Merkmalen der Anwendung und weiteren Attributen, gibt den permanenten Überblick. Die Unterscheidung zwischen erlaubten und nicht erlaubten Anwendungen erfordert aus praktischen Gründen den Einsatz von Whitelists UND Blacklists, je Benutzer, PC oder Netzwerk. So kann z.B. Skype im Hausnetz verhindert, aber im Hotel über WLAN freigegeben werden. Den Anwendungen können eigene vom Benutzer unabhängige Rechteräume zugewiesen werden. Dadurch wird definiert, unter welchen Umständen welche

Applikation auf welche Nutzdaten zugreifen kann. So kann jede Anwendung sicher berieben werden – auch alte Legacy Anwendungen ohne Änderung der Anwendung.

Kontrolle der verwendeten Netze

Die Netzwerk-, UMTS-Karten, WLAN-Geräte oder andere Zugangsmöglichkeiten zu weiteren Netzen, wie etwa Modems in PDAs, verbinden den Rechner mit potentiell gefährdeten Netzen. Durch die Unterscheidung zwischen erlaubten und nicht erlaubten Netzen kontrolliert die IT-Abteilung diese Kontakte. Entsprechend des erkannten Netzes wird die gültige Security Policy in Echtzeit eingestellt – (Heimarbeitsplatz, Firmenzentrale, Standort Produktion, Schulung, etc.), so dass der PC netzbasiert die richtige Sicherheitseinstellung durchsetzt und die Rechte nicht mehr am Anwender hängen müssen.

Schutz gegen Spyware

Angreifer nutzen Schwachstellen in Programmen aus und schleusen so Schadcode vom Benutzer unbemerkt in das Unternehmen ein. Dieser wird unter Nutzerrechten im Hintergrund ausgeführt und überträgt die sensiblen Daten unbemerkt verschlüsselt ins Internet. Durch eine Integritätsprüfung der Applikationen und die Überprüfung der Zugriffsrechte der Anwendungen kann diesen Angriffen wirksam entgegen getreten werden.

Kontrolle der verwendeten Netze

Die Netzwerk- und UMTS-Karten, WLAN-Geräte oder andere Zugangsmöglichkeiten zu weiteren Netzen, wie etwa Modems in PDAs, verbinden den Rechner mit potentiell gefährdeten Netzen. Durch die Unterscheidung zwischen erlaubten und nicht erlaubten Netzen kontrolliert die IT-Abteilung diese Kontakte. Entsprechend des erkannten Netzes wird die gültige Security Policy in Echtzeit eingestellt – (Heimarbeitsplatz, Firmenzentrale, Standort Produktion, Schulung, etc.), so dass der PC netzbasiert die richtige Sicherheitseinstellung durchsetzt und die Rechte nicht mehr am Anwender hängen müssen.

Schleusenfunktion lokal

Die Entschlüsselung und Dekomprimierung erfolgt in einer lokalen Quarantäne. Erst dann können die Inhalte im Klartext geprüft werden. Je nach Ergebnis, werden die Dateien geblockt und sicher gelöscht, zur Prüfung an Dritte weitergeleitet oder freigegeben. Der Rechner kann nicht durch Schadcode infiltriert werden – zusätzliche Hardware und lange Wege sind unnötig.

Personalisierung von Datenträgern

Günstige Datenträger verfügen über keine eigenen Merkmale wie Seriennummern. Die Verwendung von Datenträgern in besonders kri-

tischen 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. Den „unternehmenseigenen Datenträger“ erstellt man am besten durch Personalisierung auf die Gruppe der Domänenbenutzer mit zwei Mausklicks und vermeidet dadurch aufwändige Verfahren der Pflege von Seriennummern und den Einkauf teurer Hardware.

Ereignisgesteuerte Reaktion

Die unkomplizierte Integration in die bereits etablierten Verfahren, z.B. Intrusion Detection oder Help Desk, ist hier genauso wichtig wie die Möglichkeit Echtzeitreaktionen auf kritische Ereignisse zu konfigurieren, um z.B. mit dem untrainierten Anwender sofort in den Dialog zu treten und Security Awareness in Echtzeit beweisbar umzusetzen.

Security Awareness in Echtzeit

Die Belange des Datenschutzes und der lokal gültigen Datenschutzgesetze sowie anderer branchentypischer Auflagen sind für den Endanwender nicht immer einfach zu verstehen. Zentrale Schulungen verpuffen oft, weil zu viele Inhalte, die nicht täglich angewendet werden, den Anwender überfordern.

E-Learning-Systeme werden häufig nicht geeignet wahrgenommen. Die beste Lösung ist alle Vorteile miteinander zu kombinieren und die Lerninhalte oder bestimmte elektronische Willenserklärungen (z.B. Zustimmung zur Protokollierung für Compliance) direkt an die kritische Aktion zu koppeln und die Zeitspanne bis zur Wiederholung des Anwenderdialogs in der Security Policy zu verankern um eine Häufung zu vermeiden.

Reports und Management Information

Beweisbare Compliance auf Knopfdruck reduziert die Zeit der Prüfung, spart Geld und erlaubt es die Kernfrage „Wie sicher sind wir?“ spontan und präzise zu beantworten. Revision, Auditoren, Risiko Management und die Manager des Unternehmens haben mit historischer und Echtzeit-Auskunft über alle Ereignisse, nach Standorten, Abteilungen oder anderen Kriterien sortiert, echte Mehrwerte im Betrieb und können die Unternehmensressourcen zielsicher steuern.

Diese und viele weitere Herausforderungen löst die Endpoint Security Suite der itWatch auf mehreren Millionen PCs täglich mit Freigaben für *NATO-restricted*, *Verschlusssache NfD* und *Geheim*. Sie skaliert nicht nur technisch für jede Unternehmensgröße, sondern auch für jedes Budget.

Weiterführende **Literatur** finden Sie unter ***Downloads*** auf **itWatch.de:**

- **„Data Leakage Prevention - Jeder Anfang ist schwer.“**
- *„Endpoint Security leicht gemacht - Management von Anfang an“*
- *„DLP – IN DEUTSCHLAND ANDERS?“*
- *„IT-Sicherheit ist nicht nur Gesetz und Compliance, sondern vor allem Unternehmenskultur“*
- *„Null Administration, Volle Sicherheit“*
- *„Endgerätesicherheit - Anforderungen und Lösungen“*
- *„Verschlüsselung beim Transport von Daten“*
- *„SecuritySolution - Den Fluss der Information überwachen“*
- *„Security Awareness in Echtzeit – on demand!“*
- *„LanLine - Daten sicher transportieren“*
- *„Einsatzbericht der Polizei Bayern“*

itWatch GmbH
Tel.: +49 (0) 89 620 30 100
Email: Info@itWatch.de
www.itWatch.de