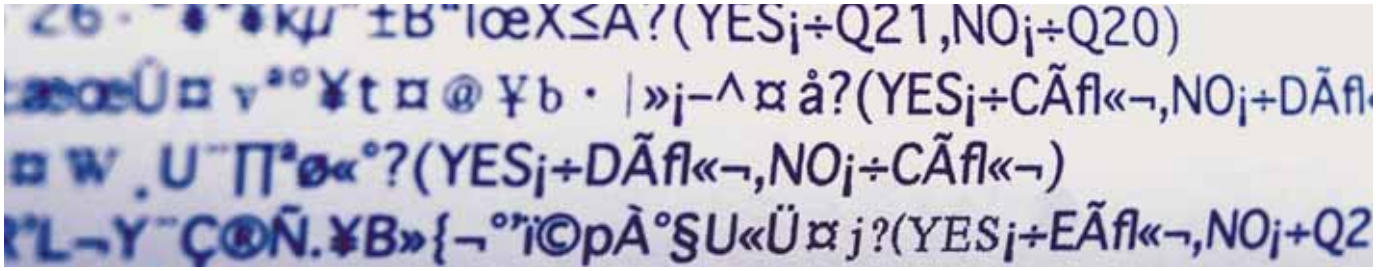


Den Fluss der Information überwachen

Geräte-Kontrolle – Fortschrittliches Device-Management unterstützt Unternehmen bei Standardprozessen und bringt Funktionen für Service-Desk und das Systems-Management gleich mit. Und es kontrolliert, wie die Daten im Netz fließen.

Der USB-Port und die daran angebundenen Memory-Sticks sind exemplarisch für die stetig wachsende Zahl von Geräten und Schnittstellen. Ein moderner Desktop oder Laptop bringt daneben noch PCMCIA-, Infrarot-, Bluetooth-, Firewire- und WLAN-Interfaces mit. Der Vielfalt interessanter Peripheriegeräte und dem nutzbringenden Einsatz in den Geschäftsprozessen sind keine Grenzen gesetzt. Digitale Kameras, Diktiergeräte, USB-WLAN-Konverter, PDAs mit E-Mail an Bluetooth, USB oder WLAN, Webcams und viele weitere »Devices« helfen den Nutzern und dem Unternehmen, Zeit und Geld zu sparen. Die IT-Leiter sind gefordert, alle diese Peripheriegeräte zentral zu verwalten.

Sie haben mehrere Aufgaben zu lösen – Sicherheit ist nur einer davon. Denn der Einsatz des scheinbar komfortablen Betriebssystems Windows und seiner Plug&Play-Mechanismen verursacht einen erheblichen Bedarf an Kontroll- und Steuerungsfunktionen. Allein deshalb, weil der Kern des Microsoft-Betriebssystems - übrigens auch Vista - keine hochwertigen netzweiten Managementfunktionen anbietet.

Firmen haben dieses Problem bereits erkannt, begnügten sich aber zuerst mit der Kontrolle darüber, wer welches Gerät wann an welchem PC nutzen darf. Diese Funktionalität wurde in der vergangenen Ausgabe beschrieben und mit einem Marktüberblick einiger Startups angereichert. Heute genügt diese Funktionalität gerade großen Unternehmen nicht mehr.

Hat die Firma nämlich die Sicherheit im Griff, müssen die Devices auch im täglichen Betrieb einfach verwaltet werden. Um diese Anforderung zu erfüllen, gilt es mehrere Disziplinen zu beherrschen. Dazu zählen die automatische Inventarisierung, Asset-Management aller volatilen Geräte, das Device-Driver-Management on Demand und viele weitere Features.

Denn nur die automatische Nutzung und die effiziente Einbindung in die Geschäftsprozesse der Unternehmen erlauben einen kostengünstigen Einsatz, und sei es durch die Reduzierung der Calls im Help-Desk. So hat beispielsweise die Polizei Bayern das Einsparpotenzial aus der automatischen Verarbeitung digitaler Fotos am Tatort mit den Produkten »DeviceWatch«, »XRayWatch« und »DEvCon« von IT-Watch umgesetzt. Trotzdem konnten die durch das Justizministerium vorgegebenen hohen Sicherheitsanforderungen voll erfüllt werden. Die Einsparungen durch die Umstellung von Polaroid auf digitale Fotografie ließen sich nur realisieren, indem die Fotos vom Entstehungsort über die Kamera bis zur gerichtlichen Verwertbarkeit ohne weitere Interaktion durch den einzelnen Nutzer automatisch verarbeitet werden.

Ein weiteres Anwendungsbeispiel »Dienstbeginn des Chefarztes« verdeutlicht die Verbindung aus Kostensenkung, Usability und Sicherheit: Vollautomatisch und revisionssicher werden die relevanten Patientendaten der vergangenen Nachtschicht auf seinen PDA oder Handheld geladen. Der Chefarzt legt dazu lediglich den PDA neben den Computer. Die Synchronisation über Bluetooth startet automatisch, wobei Randbedingungen wie die korrekte Verschlüsselung des PDAs, die Authentifizierung an allen beteiligten Geräten und viele weitere Systemzustände automatisch vorab geprüft werden.

Datenströme überwachen

Neben der obligatorischen Gerätekontrolle ist es wichtig, die firmeneigenen Informationen auf ihrem Transportweg zu kontrollieren und vor Missbrauch zu schützen. Dies birgt ein altbekanntes Problem: Der Benutzer kann zwar die Sensibilität der Information selbst am besten einschätzen, hat aber weder Wissen im Umgang mit Verschlüsselungstechnologien, noch die Zeit für eine »Sonderbehandlung« der Information. Vor allem große Unternehmen fordern, dass sie die Verschlüsselung schützenswerter Daten auf dem Transportweg mit nur wenigen Mausklicks erzwingen können.

Sie fordern zudem die Personalisierung und Individualisierung von externen Datenträgern. Diese beiden Funktionen unterstützen das Arbeiten in kleinen (Vorstand und Sekretariat) oder

großen Gruppen (Projekte) mit besonders vertraulichen Informationen. Das Auslagern und der Zugriff auf individualisierte Medien werden wiederum je nach Inhalt und berechtigtem User unterstützt, so dass auch Projektrollen wie die Zuständigkeiten für Finanzen oder Patente technisch abgebildet werden.

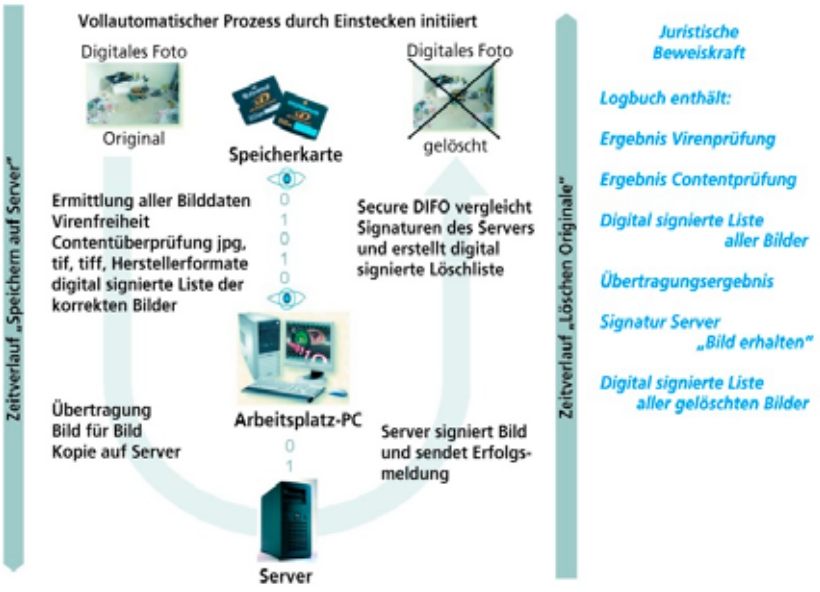
Auf größere Konzerne trifft ferner zu, dass sie weit mehr Gesetzesvorgaben wie HIPAA, Bundesdatenschutzgesetz, SOX oder KonTraG einhalten müssen. Ein Device-Management-System muss diese Bedingungen also nicht nur technisch unterstützen, sondern auch beweissicher umsetzen. Ein börsennotiertes Allfinanzunternehmen hat seine Compliance-Anforderungen auf 40000 Notebooks im Außendienst daher mit dem Produkt »PDWatch« von IT-Watch umgesetzt.

Integration in Geschäftsprozesse

Um den Sicherheitsanforderungen an das Plug&Play gerecht zu werden, muss ein modernes Device-Managementsystem mehrere Funktionen beherrschen, die es allerdings auch zentral zu verwalten hat. Zu den Basiseigenschaften zählen:

- Präventives Blockieren von Geräten und Dateien, die natürlich nicht nur an deren Namen erkannt, sondern durch eine kundenspezifisch erweiterbare Patternprüfung individuell gefiltert werden,
- Verschlüsselung mobiler Datenträger nach zentralen Richtlinien,
- Automatische Verarbeitung von CDs und DVDs außerhalb des Benutzerrechteraums,
- Erkennung von ungewöhnlichem oder der Unternehmensrichtlinie widersprechendem Verhalten oder auch Angriffen in Echtzeit durch Intrusion-Detection und geeignete Schnittstellen zu Drittsystemen,
- Maßnahmen der Beweissicherung wie Logging und Shadowing und das Aufbereiten der Auditdaten für die Revision.

Der Hersteller IT-Watch hat diese Anforderungen in seiner Lösung bereits berücksichtigt. Das Tool »DeviceWatch« sorgt für die Gerätesicherheit, »PDWatch« verschlüsselt die Daten, »CDWatch« überwacht die Medien-Sicherheit, während »,XRayWatch« die Contentkontrolle, Patternprüfung und das Shadowing übernimmt. »DEvCon« deckt alle Anforderungen aus dem Systems-Management ab. Diese Werkzeuge werden über eine zentrale Administrationskonsole verwaltet.



Dem Kontrollverlust durch Plug&Play sollten Unternehmen aber nicht nur durch Maßnahmen aus der IT-Sicherheit begegnen. Die Integration in die Unternehmensprozesse, sei es die PDA-Synchronisation, ist ebenso wichtig. Unternehmensprozesse finden nicht nur auf den PCs statt, sondern auch in Form von Change- und System-Management. Im Change-Management ist es beispielsweise wichtig, komplexere Änderungen der Security-Policy in der produktiven Infrastruktur nur getestet durchzuführen. Diese Änderungen sind dann aus der Testumgebung automatisiert zu übernehmen. Einfache Export- und Import-Funktionen sind deshalb wesentlich für einen Langzeitbetrieb. Auch vorbereitende Werkzeuge für Erstellung einer Security-Policy sind hilfreich. Der »DeviceWatch Scanner« ermittelt dazu den Bestand der bisher im Unternehmen verwendeten Devices, ohne auf den PCs eine Veränderung vorzunehmen. Dadurch ist die Sicherheitspolicy für den Ist-Stand des Unternehmens konzipiert und enthält keine überflüssigen Elemente. Noch wichtiger ist die Möglichkeit, die Policy-Regeln »sanft« in Betrieb zu nehmen. Dazu sind Benutzernachrichten in Echtzeit sowohl beim Anstecken eines verbotenen als auch beim Anstecken eines »noch« erlaubten Gerätes notwendig. In den Nachrichten der »noch« erlaubten Devices wird darauf hingewiesen, dass sich die Regelung in Zukunft ändert - der Text kann jeweils individuelle Handlungsanweisungen mit zeitlicher Gültigkeit und anderen Möglichkeiten enthalten.

Neben diesen Beispielen für die Prozessintegrationen ist auch den aktuellen Themen Applikationskontrolle und »Information-Leakage-Prevention« Rechnung zu tragen. Denn anspruchsvolle Kunden aus den Bereichen Militär, Nachrichtendienst, Dax und NYSE lösen diese Probleme bereits heute mit technischen Maßnahmen. Aber auch der Mittelstand profitiert von diesen Funktionen. Sie erlauben es einem Unternehmen, in nur fünf Minuten zu definieren, welche Information die Mitarbeiter auf mobilen Datenträgern nutzen dürfen. So lässt sich beispielsweise das Einbringen von ausführbaren Dateien über CDs, DVDs, Memorysticks oder Flashkarten mit nur wenigen Mausklicks effizient verhindern. Das Device- und Schnittstellenmanagement nimmt so den nächsten Entwicklungsschritt hin zur tatsächlichen Endpoint Security mit Content-Kontrolle.

Irmgard Bähr, Sios