



Kontrolle über Geräte und Schnittstellen

Mobile Datenträger wie USB-Sticks oder MP3-Player sind zu einer Selbstverständlichkeit geworden – auch im Geschäftsalltag. Damit sind jedoch enorm grosse Sicherheitsrisiken verbunden. Die Gefahr, schädliche Dateien (Malware) über mobile Datenträger in das Firmennetzwerk einzuschleusen, wächst kontinuierlich – wie auch der schnelle und unbemerkte «Datenklau» von sensiblen Daten.

Trojaner, Würmer, interne wie externe Mitarbeitende können eine ernsthafte Bedrohung sein. Der Schaden, der durch Verstösse (bewusst und unbewusst) gegen die Sicherheitsbestimmungen innerhalb eines Unternehmens selber verursacht wird, übersteigt bei weitem die Bedrohung durch Aussenstehende. Externe Datenträger werden immer kleiner und die Speicherkapazitäten werden immer grösser. So ist es ein Leichtes, grosse Mengen von sensiblen Daten vom Firmennetzwerk herunterzuladen und unter Umständen missbräuchlich zu verwenden.

Unternehmen sehen sich heute mit zwei Arten von Sicherheitsrisiken durch «Insider» konfrontiert: eingeschleppte Malware und unautorisiertes und unkontrolliertes Kopieren von kritischen Daten. Beide Sicherheitsrisiken sowie zusätzliche Produktivitäts- und Stabilitätsprobleme sind auf den missbräuchlichen Zugriff auf Datenträger und Daten zurückzuführen.

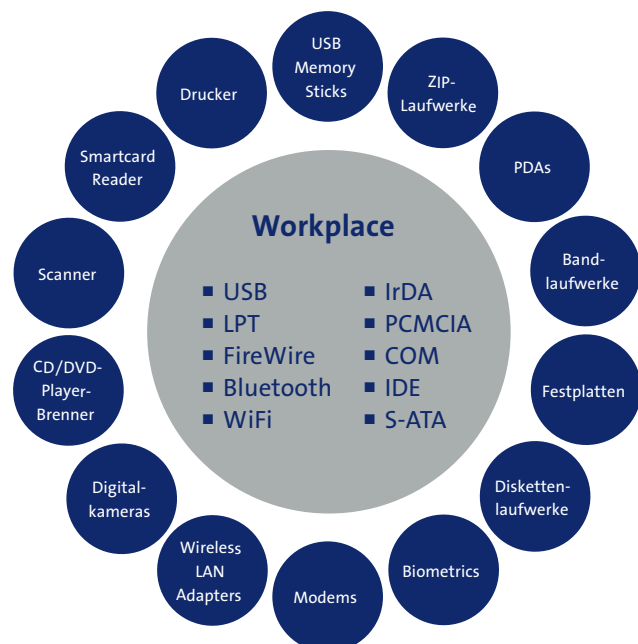
Lösung

Der Device Control Service ermöglicht die Steuerung und Kontrolle von Zugriffen auf so genannte Plug&Play-Geräte und Anschlüsse. Nach dem Grundsatz des möglichst restriktiven Zugriffs wird für alle Nutzer der Zugriff auf nicht freigegebene Geräte standardmässig verweigert – nur Geräte, welche erfasst und freigegeben wurden, können durch die Benutzer verwendet werden.

Mit dem Device Control Service lassen sich die meisten Gefahren verhindern,

welche Insider durch den Missbrauch von Netzwerkressourcen und geschäftskritischen Informationen verursachen können. Diese Sicherheit wird erzielt, indem der Zugriff auf Endanwender-Geräte wie DVDs, serielle, parallele und USB-Devices und weitere Geräte kontrolliert wird.

Durch die Implementierung der Gerätezugriffskontrolle mit Device Control werden ebenfalls die Gefahren des elektronischen Diebstahls geistigen Eigentums und weiterer sensibler Geschäftsinformationen weitgehend gebannt.



Leistungsmerkmale

Der Service Device Control zeichnet sich durch folgende Funktionen aus:

- Kontrolle über alle gängigen externen Geräte-Typen (Devices) inkl. interner Laufwerke
- Zentrale Verwaltung der Benutzer und der eingesetzten Geräte
- Zugriffsrechte unterliegen einer Zugriffskontrollliste; in dieser wird festgehalten, wer auf welche Geräte zugreifen darf
- White-List-Konzept: Nur Geräte, welche erfasst und freigegeben wurden, können verwendet werden; standardmässig sind alle Geräte gesperrt
- Zeitlich eingeplanter und befristeter Zugriff (Lese- und Schreibzugriff) möglich
- Eindeutige Kennzeichnung und Zulassung bestimmter Wechselmedien
- Erkennung von Plug&Play-Geräten und Anwendung der Zugriffskontrollliste im laufenden Betrieb
- Nachvollziehbarkeit (Auditing) gewährleistet
- Schutz bleibt auch im Offline-Betrieb bestehen
- Beschränkungsmöglichkeit der zu kopierenden Datenmenge

Leistungsumfang

- Integrationsberatung und -konzeption
- Bereitstellung und Integration der server- und clientseitigen Device-Control-Funktionalitäten
- Betrieb und Wartung des Services über den gesamten Produkt-Lifecycle

Ausprägungen

Standard:

- Betrieb, Wartung und Support der Server- und Clientseitigen Device-Control-Funktionalitäten
- Garantierte Leistungen gemäss SLA Premium:
Zusätzlich zu den Standardleistungen höhere Skalierbarkeit und somit Nutzung in Umgebungen mit hoher Anzahl an Anwendern
- Betrieb eines dedizierten Applikations-Servers ist inklusive

Ähnliche Services/ Komplementäre Services

- Information Rights Management
- Workplace Antivirus

Nutzen

- Durchsetzen der internen Sicherheitsrichtlinien
- Erhöht das Sicherheitsniveau
- Verhindert den «Datenklau» auf externe Datenträger
- Reduziert massiv die Gefahr des Einschleppens von Malware
- Zentrale Kontrolle und Steuerung aller eingesetzten Geräte
- Kontrolle über Ein- und Ausgang von Unternehmensdaten
- Leistungsstarke Audit-Fähigkeiten