Software management org

Verarbeitung von personenbezogenen Daten in Software Management Suite

Sehr geehrte Damen und Herren,

Software Management Suite ist ein vollständiges Software Lizenz- und Vertrags-Management System. Es erstellt ein präzises technisches Inventar durch den Scan aller Rechner. Hierbei wird erfasst welche Software installiert ist. In einem kaufmännischen Inventar werden über die von Ihnen erworbenen Softwarelizenzen und Verträge die Nutzungsrechte erfasst. Ziel ist die Gegenüberstellung dieser beiden Inventare in einer Lizenzbilanz als tatsächlichem Abbild der Lizenzsituation Ihres Unternehmens.

Software Management Suite kann bei der Analyse der Computer auch personenbezogene Daten sammeln. In den nachfolgenden Abschnitten gehen wir auf die einzelnen Daten und den Grund ihrer Erhebung und die Möglichkeiten der Abschaltung ein. Bitte leiten Sie das Dokument an Ihren Datenschutzbeauftragten und Betriebsrat weiter, damit Ihr Software Asset Management im Einvernehmen aller Parteien gestaltet werden kann:

(1) zum Zeitpunkt des Scans angemeldeter Benutzer

Der SMOscan wird üblicherweise im Loginscript - oder analog durch Policies - der einzelnen Benutzer ausgeführt. Dabei wird der aktuell angemeldete Benutzer mit dem Loginnamen und Domäne erfasst. Die erhobenen Daten erlauben eine automatisierbare Zuordnung zwischen Arbeitsplatz und Benutzer. Diese Beziehung ist notwendig um personengebundene Lizenzen mit dem Arbeitsplatz zusammenzuführen und die dort gefundenen Produkte mit einer personengebundenen Lizenz abzudecken. Falls keine personengebundenen Lizenzen vorliegen, kann man auf diese Information verzichten.

Sollte die Erhebung dieser Information nicht erwünscht sein, so erlaubt der SMOscan über den Parameter ANONYMOUS=ON eine Abschaltung dieser Sammelfunktion. In Folge dessen müssen Mitarbeiter manuell Arbeitsplätzen zugeordnet werden.

(2) Besitzer einer ausführbaren Datei

In Unternehmen mit Mitarbeiterrichtlinien zum Softwareeinsatz sind allein die Administratoren zu einer Installation von Anwendungen berechtigt. Bei der Installation vermerkt das Dateisystem automatisch an jeder Datei den aktuellen Benutzer als Besitzer. Im Regelfall ist die Gruppe der Administratoren als Besitzer vermerkt. Ist der Besitzer ungleich der Gruppe der Administratoren, so ist dies ein Indikator für eine Installation durch einen Benutzer. Der SMOscan liest den Besitzer aus, jedoch existiert derzeit

Mendelstr. 11
D-48149 Münster

55 Madison Avenue, Suite 400,
07960 New Jersey, USA

Phone +49 (0) 251 – 899 64 - 0
Fax +49 (0) 251 – 899 64 - 99

info@softwaremanagement.org
www.softwaremanagement.org

kein Bericht im SMOmanager zu dieser Information. Sollte der SMOscan unerwünschte Software aufdecken, so ergeht im Regelfall eine Aufforderung zur Deinstallation an alle Mitarbeiter im Unternehmen. Nach unserer Erfahrung kommen die Mitarbeiter der Aufforderung nach und die Situation ist schnell zu bereinigen, ohne dass die gezielte Ansprache einzelner Mitarbeiter notwendig wäre.

Sollte die Erhebung dieser Information nicht erwünscht sein, so erlaubt der SMOscan über den Parameter OWNERSHIP=OFF eine Abschaltung dieser Sammelfunktion. Auch bei ANONYMOUS=ON werden diese Informationen nicht mehr erhoben.

(3) Bezüge zu Webseiten

Der SMOscan kann die Bezüge zu Webseiten (Favoriten oder Links im Startmenü) auslesen. Sollten in Ihrem Hause Produkte mit eigenen Webdiensten im Einsatz sein, so können Sie diese Bezüge einem Softwareprodukt zuordnen, welches dann am Arbeitsplatz erkannt wird.

Sollte die Erhebung dieser Information nicht erwünscht sein, so erlaubt der SMOscan über den Parameter LINKSWEB=OFF eine gezielte Abschaltung dieser Sammelfunktion. Auch bei ANONYMOUS=ON werden diese Informationen nicht mehr erhoben. In Folge dessen können Sie interne Webanwendungen nicht mehr in die Lizenzbilanz einfließen lassen. Sollten die eingesetzten Webanwendungen ein eigenes Lizenzierungsschema z.B. nach Benutzern verwenden, so ist die Ausblendung der Information weniger problematisch. Wegen der möglichen Vermengung von privaten und unternehmensrelevanten Verknüpfungen sollte der Nutzen kritisch hinterfragt werden.

(4) Terminal Sessions

Wenn ein Terminal Server über Terminal Sessions den Zugriff auf Softwareprodukte erlaubt, so ist im Microsoft Umfeld die Nutzung pro Endgerät zu lizenzieren. Folglich muss der SMOscan die aktive Nutzung der Anwendung protokollieren. Wir haben dabei analysiert, dass nur eine einmalige Nutzung einer Anwendung protokolliert werden muss, um dem Lizenzrecht des Herstellers gerecht zu werden d.h. der erste Start einer Anwendung von einem Endgerät wird protokolliert. Alle nachfolgenden Starts werden nicht mehr aufgezeichnet.
Somit ist dem Lizenzrecht und dem Schutz der Mitarbeiterinteressen vollständig Rechnung getragen, weil eine Ableitung von Produktivitätskennzahlen oder Ähnlichem ist auf dieser Datenbasis nicht möglich ist.
Nun könnte man argumentieren, dass auch der einmalige Bezug zum Mitarbeiter nicht relevant ist, weil eine auf das Endgerät bezogene Auswertung ausreicht um dem Lizenzrecht des Herstellers zu genügen. Allerdings hat Microsoft ausdrücklich weitere Sparpotentiale eingeräumt, wenn es möglich ist nachzuweisen, dass für den Benutzer innerhalb von 90 Tagen ein Hauptarbeitsplatz existiert hat. In

diesem Fall sind alle Nebennutzungen an anderen Arbeitsplätzen nicht lizenzpflichtig. Um dieses Sparpotential ausschöpfen zu können, wird der Loginname als Nutzer-Information benötigt.

Nachvollziehbarkeit für den Betriebsrat

Für den Betriebsrat ist es jederzeit möglich das Protokollverhalten des SMOscan zu überprüfen. Alle vom SMOscan erzeugten zip-Dateien enthalten Klartextdateien, welche mit dem Notepad geöffnet werden können. Dadurch kann der Betriebsrat jederzeit überprüfen, ob die mit der IT-Abteilung vereinbarte Parametrisierung in der SMOscan.ini eingehalten wurde.

zip-Dateien des SMOscan:
pcAinB.zip => Arbeitsstation oder Server mit Name A in Domäne B
taAinBonCinDfromE.zip => Nutzung in Terminal Session durch Benutzer A in Domäne B auf Terminalserver C in Domäne D ausgehend vom Endgerät E.

Darin finden sich Dateien mit folgender Endung:
.sw => vorgefundene bzw. in einer Session einmalig genutzte Software
.hw => vorgefundene Hardware
.ev => vorgefundene Einträge im Ereignisprotokoll

Wir halten es für eine gute Vorgehensweise die oben genannten Eigenschaften an Betriebsräte und Datenschutzbeauftragte heranzutragen, damit diese eigene Stichproben vornehmen können um sich von der korrekten und dem Zweck angemessen Arbeitsweise zu überzeugen.

Einbindung des Betriebsrats in Entscheidungsprozesse

Betriebsrat und Geschäftsführung sollten gemeinsam Prozesse für folgende Situationen definieren:

- Entdeckung nicht autorisierter Software: es wird eine Rundmail ohne die gezielte Ansprache einzelner Mitarbeiter empfohlen. Zunächst sollten Mitarbeiter sensibilisiert werden, dass sie nicht einfach beliebige Software installieren bzw. verlangen. Eine solche Vorgehensweise hat in der Regel negative Folgen für das Unternehmen in Form von unnötigen Kosten, Produktivitätseinbußen bis hin zu Sicherheitsproblemen. Derartige Software sollte im Nachgang entweder entfernt oder aber autorisiert werden.

- Entdeckung von Lizenzüber- oder Unterdeckungen: Arbeitsverträge weisen Führungskräften üblicherweise die Verantwortlichkeit für die korrekte Lizenzierung von Software zu. Sollte durch Software Asset Management (SAM) eine Lizenzüber- oder Unterdeckung aufgedeckt werden, so sollte die Verhältnismäßigkeit gewahrt bleiben. War es der Führungskraft wegen nicht beeinflussbarer

Rahmenbedingungen (kein Budget für SAM etc.) nicht möglich für Transparenz im Lizenzbereich zu sorgen, so sollte dies bei der Erwägung von Konsequenzen gewürdigt werden. Es sollte verhindert werden, dass Führungskräfte gegen die SAM Manager arbeiten, weil sie negative Konsequenzen befürchten müssen. Hier sollten die Ziele des SAM, wie Transparenz und die Möglichkeit zukünftige Beschaffungen günstiger zu gestalten, viel höher gewichtet werden. In diesen Zielen stecken die eigentlichen Motive des SAM und das sollte den betroffenen Führungskräften auch kommuniziert werden.

Durch eine verbindliche Definition der Entscheidungsprozesse können Geschäftsleitung und Betriebsrat eine Blockadehaltung ihrer Mitarbeiter verhindern und sie gleichzeitig vor unangemessenen Härten schützen.

Auf der Seite der Informationserhebung kann durch eine verbindlich vereinbarte Parametrisierung des SMOscan dafür gesorgt werden, dass unangemessene Eingriffe in die Privatsphäre der Mitarbeiter verhindert werden. Auf diese Weise wird den verfolgten Zielen des Software Asset Management bzw. der Lizenzverwaltung und den möglichen Bedenken im Vorfeld Rechnung getragen.

Mit freundlichen Grüßen

Holger Schmeken
Dipl.-Wirtschaftsinform.

Softwaremanagement.org ITS

Email: HolgerS@Softwaremanagement.org
Tel: +49(0) 251 / 899 64 43