LANline

9,– €

Oktober 2010
30. September

ITP VERLAG

IT ■ Netze ■ Infrastruktur www.lanline.de

Sonderdruck für Baramundi Software AG

Cloud Computing und Virtualisierung

Public, Private und Hybrid Cloud

Virtualisierte Anwendungen bereitstellen

Rechtliche Aspekte

Mit Marktübersicht Anbieter von Cloud-Services

Datenschutz im Client-Management

Missbrauch verhindern

Die Arbeitnehmerrechte schützt in vielen Staaten ein eigenes Gesetz – oder zumindest die europäische Datenschutzrichtlinie. Unternehmen haben es aber nicht nur mit dem Wunsch der Mitarbeiter nach Datenschutz zu tun, sondern müssen teilweise sehr strenge gesetzliche Vorgaben einhalten, deren Missachtung strafrechtliche Konsequenzen nach sich ziehen kann. Die eingesetzte Client-Management-Software muss für dieses Dilemma eine Lösung bieten.

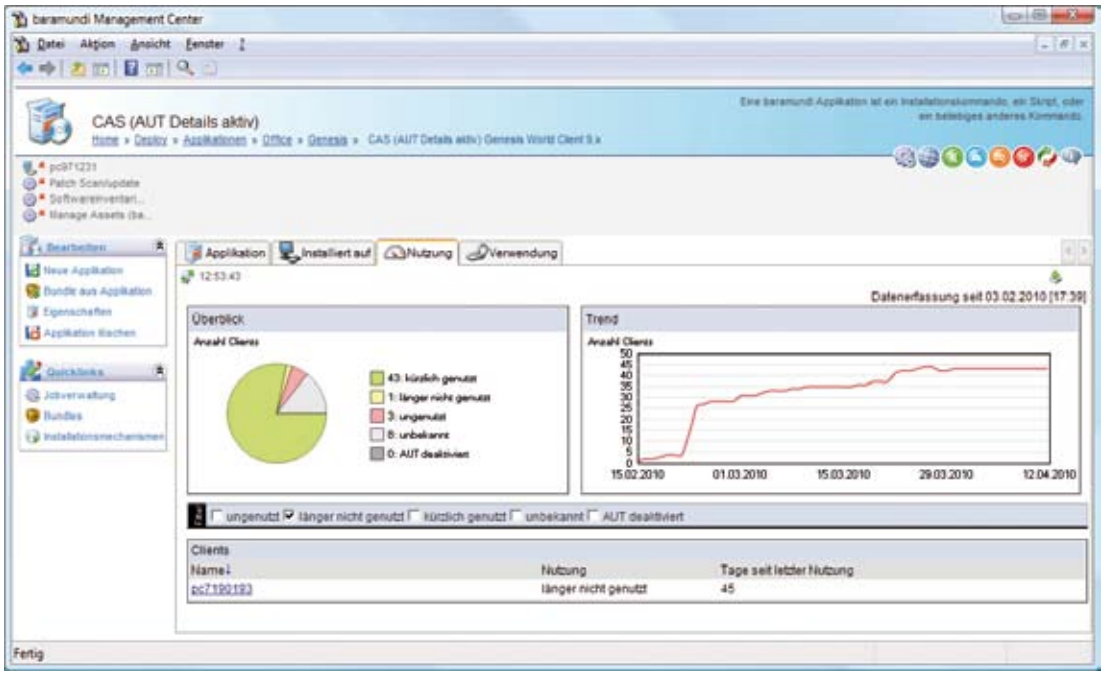
Daten eines Mitarbeiters fallen unter den Datenschutz, wenn dieser ein „schutzwürdiges Interesse" daran besitzt. Diese ungenaue Definition gibt immer wieder Anlass zu Diskussionen und wird in jedem Unternehmen etwas anders gehandhabt; klare gesetzliche Regeln gibt es noch nicht. Generell sind damit aber alle Daten gemeint, die zum Nachteil eines Mitarbeiters verwendbar sind oder im Extremfall sogar zu Gefahr für Leib und Leben führen können. Darunter fallen zum Beispiel Zeiterfassung, Surfgewohnheiten, Gehaltsdaten, Krankmeldungen oder auch die Privatadresse eines Polizisten.

Ein Windows-PC sammelt automatisch zahlreiche Daten über seine Verwendung: Wer meldet sich wann an, welche Anwendungen werden gestartet, welche Dokumente geöffnet, welche Webseiten aufgerufen? Da ein PC meist direkt einem Mitarbeiter zuzuordnen ist, lassen sich darauf bei Auswertung durch einen IT-Profi Rückschlüsse auf das Nutzungs- und Arbeitsverhalten des Mitarbeiters ziehen. Daher greift bereits hier der Datenschutz: Analysiert also beispielsweise der Vorgesetzte den PC eines Mitarbeiters, ohne diesen vorher darüber zu informieren, verstößt er gegen das Datenschutzgesetz.

Client-Management

Eine Client-Management-Lösung sammelt ebenfalls zahlreiche Daten, zum Beispiel: Wie ist der Patch-Status, welche Software ist installiert, ist der Rechner online, ist der Benutzer online? Hinzu kommen Informationen über Dateien, die ein Anwender öffnet, auf externe Datenträger kopiert oder ins System einspielt, sowie Angaben dazu, welche Applikationen er wann und wie verwendet. Diese Daten werden zudem über einen längeren Zeitraum gesammelt und in einer Datenbank dauerhaft gespeichert. Damit birgt jedes Client-Management die Möglichkeit des Datenmissbrauchs: Der Arbeitgeber könnte die für die Funktion des Client-Management-Systems nötigen Daten anderweitig auswerten und gegen einen Mitarbeiter verwenden. Für jedes Unternehmen empfehlen sich daher erstens ausführliche Information der Mitarbeiter oder der Mitarbeitervertretung über Missbrauchsmöglichkeiten und zweitens klare Richtlinien für die Administratoren.

Gerade Administratoren haben teilweise domänenweit uneingeschränkten Zugriff auf alle Computer im Unternehmen. Für die Auswahl und Kontrolle von Administratoren müssen somit besondere Kriterien gelten. Client-Management bietet hier interessante Möglichkeiten, indem man den eigentlichen domänenweiten Zugriff auf das Tool verlagert und sich die jeweiligen IT-Beauftragten



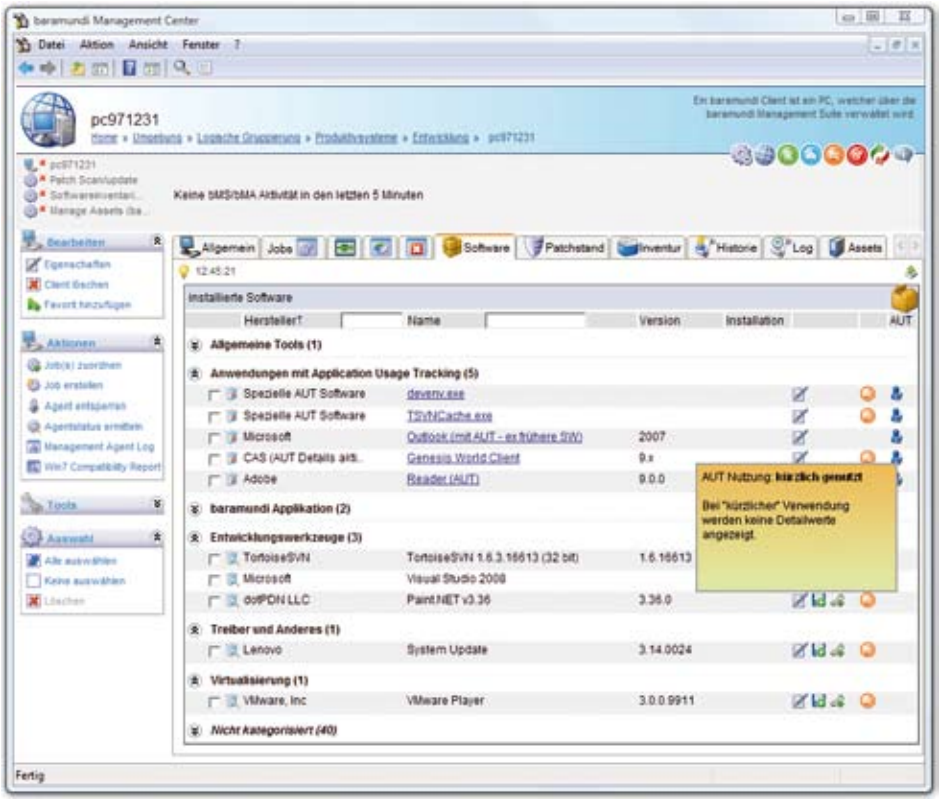
Ansicht einer Applikationsverwendung: Auf pc7190193 wird diese Software nicht genutzt und lässt sich somit einsparen. **Bild: Baramundi Software**

an der Konsole des Client-Managements anmelden. Dies kann so eingerichtet werden, dass es keinen domänenweiten Account mehr gibt. Vor allem bei großen Netzwerken mit mehreren Verwaltungs-Levels kann das Client-Management dafür sorgen, dass jeder Administrator nur die zur Erfüllung seiner Aufgaben tatsächlich benötigten Rechte besitzt.

Die zahlreichen gesammelten IT-Daten wecken bei Controllern und Vorgesetzen immer wieder den Wunsch, diese auch zur Leistungsbeurteilung ihrer Mitarbeiter zu verwenden. Hier gilt der Grundsatz: Die Leistungsbewertung muss im Voraus klar definiert und kommuniziert werden, jeder betroffene Mitarbeiter muss darüber informiert sein. In Call-Centern etwa werden dazu oft Ticketsysteme mit eingebauter Zeitmessung verwendet. In gehobenen IT-Umgebungen ist diese Überwachung aber eher unüblich, da sie von Mitarbeitern nur wenig akzeptiert wird und ihre Ergebnisse in der Regel nur schlecht Rückschlüsse auf die tatsächliche Leistung eines Mitarbeiters ermöglichen.

Bereits beim Entwurf der Funktionalität für ein Client-Management-System sollte der Hersteller Datenschutzkriterien beachten. Denn Datenschutz lässt sich nicht im Nachhinein in ein Produkt hineinentwickeln, sondern muss konsequent in allen Phasen der Entwicklung berücksichtig sein. Einige Hersteller von Client-Management-Systemen sammeln möglichst viele Nutzungsdaten über Mitarbeiter. Man kann aber davon ausgehen, dass dies zukünftig nur noch selten geduldet wird und zu erheblichen Wiederstand der Mitarbeiter führt. Hat sich erst einmal Wiederstand gebildet, steht die komplette Einführung eines Client-Management-Systems vor großen Problemen. Dabei sollte eigentlich die IT-Qualität verbessert werden und nicht die IT in den Verruf kommen, Mitarbeiter auszuspionieren.

Richtig ausgewählte und korrekt eingesetzte Client-Management-Systeme eröffnen nicht neue Missbrauchsmöglichkeiten, sondern eliminieren vielmehr bereits vorhandene Schwachstellen. So ist es beispielsweise möglich, die Domänen-Administratorenrolle komplett dem Client-Management zu überlassen. Administratoraufgaben, die höhere Rechte benötigen, werden über den zentralen Server abgewickelt. Die Client-Management-Lösung – und nur diese – kennt den relevanten Administrationskontext, was ein hohes Maß an Datenschutz und Sicherheit erlaubt.



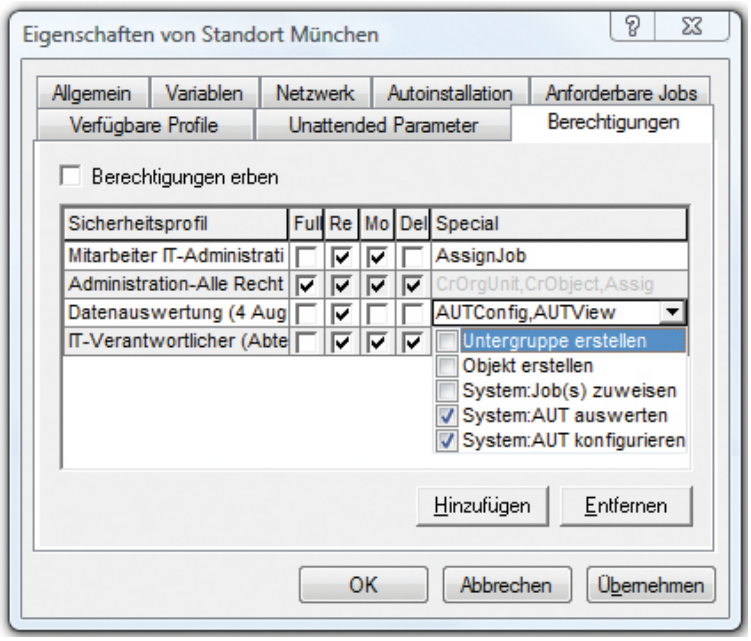
Ansicht einer Softwareinventur für einen Client: Angezeigt wird hier auch „kürzlich genutzt". Der Anwender verwendet diese Software also. **Bild: Baramundi Software**

Von den Clients sammelt das Client-Management Daten wie Patch-Stand, Hardwaredetails, installierte Software und Applikationsverwendung. Der Patch-Stand ist meist kein schützenswerter Gegenstand; hingegen ermöglicht zum Beispiel das Prüfen des Hardwarebestands das Erkennen eines unerlaubten Ein- oder Ausbaus von Hardware. Das Entnehmen eines Speicherriegels könnte einem Mitarbeiter als Diebstahl angelastet werden, obwohl er diesen vielleicht nur in einen anderen PC verbaut hat. Ist den Mitarbeitern jedoch diese Form der Überwachung bekannt, stellt sie meist kein Problem dar.

Die Überwachung der installierten Software ist hingegen öfter ein Streitpunkt. Haben die Mitarbeiter die Möglichkeit und das zugesicherte Recht, auf ihrem PC Software nach Belieben zu installieren, so ist auch die Überwachung meistens unerwünscht. Die Abmahnung eines Mitarbeiters wegen Installation unerlaubter Software ist ohnehin nur möglich, wenn die Überwachung vorher klar kommuniziert wurde. Für echtes Client-Management ist es aber wichtig, dass die installierte Software bekannt ist. Um auch in sensiblen Umgebungen die Inventur zu ermöglichen, ohne Mitarbeiter unerlaubt zu überwachen, kann bei manchen Tools die Inventur auf jene Applikationen eingeschränkt werden, die der Systemverwalter selbst verteilt hat.

Application Usage Tracking

Mit Application Usage Tracking (AUT) lässt sich automatisiert feststellen, welche Anwendungen wann und wie oft verwendet werden. Unternehmen nutzen sie oft, um Software korrekt zu lizenzieren und ungenutzte Applikationen zu entfernen. Viele Betriebsräten sehen AUT allerdings kritisch. Doch auch hier kommt es darauf an, welche Daten wie erhoben und ausgewertet werden. Es gibt bekannte Lösungen, die zahlreiche schützenswerte Daten



Über die Definition verschiedener Rechtestufen lässt sich der Zugriff auf einzelne Objekte regeln.
Bild: Baramundi Software

des PC-Nutzers sammeln. Zum Beispiel erfassen sie alle gestarteten Anwendungen mit ihrer tatsächlichen Nutzungszeit, oft sogar bis zur Anzahl der getätigten Tastenanschläge oder Mausklicks.

Unternehmen verwenden AUT in der Regel, um ungenutzte Software aufzuspüren. Dies bringt oft erhebliche Einsparungen durch geringeren Lizenzierungsumfang oder komplette Entfernung ungenutzter Anwendungen – es führt aber auch zu einer klassischen Konfrontation zwischen Unternehmer und Arbeitnehmer, wobei der Datenschutz eine klare Richtung vorgibt: „Nur so viel Daten speichern, wie zur Erfüllung notwendig."

Auch hier kann man vorsorgen, indem die Software nur die tatsächlich relevanten Daten wie Installationsdatum und letzte Verwendung sammelt. Natürlich sollte sie nur Angaben zu jenen Applikationen erheben, die per AUT zu überwachen sind. Sammelt sie Daten auf Tagesbasis, sind auch keine Rückschlüsse auf Tagesarbeitszeiten möglich. Zusätzlich lassen sich die Daten bei der Anzeige noch weiter abschwächen, sodass zum Beispiel der Tag der letzten Verwendung für den Administrator nicht mehr erkennbar ist. Wird beispielsweise eine „Nicht verwendete Applikation" nach 30 bis 90 Tagen angezeigt, so kann man in den meisten Fällen davon ausgehen, dass der Anwender die Software tatsächlich nicht benötigt. Der konkrete Zeitpunkt der Verwendung ist für die Erfüllung der Aufgabe nicht relevant und sollte deshalb nicht ersichtlich sein.

Datenmissbrauch wie eine unerlaubte Leistungsmessung durch Vorgesetzte ist aufgrund der langen Zeitspanne und fehlender Tagesarbeitszeiten somit kaum denkbar. Client-Management-Systeme, die dies schon im Design berücksichtigen, sollten auch auf ausreichende Akzeptanz in der Belegschaft stoßen – vorausgesetzt, die Mitarbeitervertretung ist frühzeitig informiert.

Vier-Augen-Prinzip

Welche Daten schützenswert sind, zeigt sich meist in der Diskussion mit Mitarbeitervertretern. Beinahe jedes Unternehmen entwickelt hier seine ganz eigene Vorgehensweise. Die Bandbreite reicht von „Kein Thema!" bis zur Beachtung jeder Kleinigkeit. Um Client-Management-Systeme auch im Rahmen sehr strenger innerbetrieblicher Datenschutzbestimmungen einsetzen zu können, ist ein ausgefeiltes Berechtigungssystem Voraussetzung. Gute Client-Management-Lösungen bieten ein eigenes Rechtesystem. Damit kann man im Detail festlegen, wer welche Daten des Systems einsehen, Aufgaben definieren und Aufgaben auf Clients durchführen darf. Einige Systeme räumen dem Datenschutz bei AUT sogar ein eigenes Recht ein. Für Daten, die als besonders kritisch gelten, empfiehlt sich das Vier-Augen-Prinzip: Daten sind nur von mindestens zwei Personen gemeinsam einsehbar, zum Beispiel von einem Unternehmensvertreter und einem Betriebsrat. Das Rechtesystem stellt diese Vorgehensweise sicher: Man richtet einen speziellen Benutzer für den Zugriff auf die zu schützenden Daten wie zum Beispiel der AUT-Angaben ein. Dieser Benutzer erhält ein mehrteiliges Passwort, von dem jeder Beteiligte nur einen Teil kennt. Dies stellt sicher, dass die Daten nur dann einzusehen sind, wenn alle Inhaber der Passwortteile das Passwort gemeinsam vollständig eingeben.

Fazit

Vor allem große Unternehmen und Behörden müssen oft mit jeder Art von Client-Management sehr vorsichtig umgehen. Denn schnell wird der Unternehmensleitung oder der Administration ein Eingriff in die Persönlichkeitsrechte der Mitarbeiter unterstellt. Will man PC-Systeme auf unerwünschte Hardware- und Softwareänderungen überprüfen, ist dies unbedingt vor Einführung des Tools zu kommunizieren. Wenn jeder Anwender noch selbst Herr über seinen PC ist und ein schutzwürdiges Interesse anmelden kann, empfiehlt es sich, die Softwareüberprüfung mit der Mitarbeitervertretung abzustimmen.

Auf ein automatisches Abmahnwesen auf Basis einer Client-Management-Lösung sollte man in jedem Fall verzichten. Bereits ein Einzelfall würde ausreichen, um das gesamte System in Misskredit zu bringen und effizientes Client-Management im Unternehmen unmöglich zu machen. Wird die geplante Einführung derartiger Systeme rechtzeitig und ausführlich mit dem Betriebsrat diskutiert, lassen sich Bedenken meist ausräumen.

Stefan Kuhn/wg

Stefan Kuhn ist Produkt-Manager bei Baramundi Software in Augsburg.

■ Info: Baramundi Software AG
Tel.: 0821/56708-0
Web: www.baramundi.de