Aussicht auf Übersicht: IT-Management für das Internet der Dinge

Device Management, Software Asset Management, Lizenzierung, Inventarisierungslösung, Patchmanagement, Business Continuity

www.deskcenter.com

Christoph A. Harvey ist Chief Executive Officer der **DeskCenter Solutions AG**. Die DeskCenter Solutions AG ist ein international agierender, deutscher Softwarehersteller mit Sitz in Leipzig. Ihre technologisch führenden SAM 4.0-Lösungen für Unternehmen, öffentliche Organisationen und Cloud Service Provider bilden den gesamten IT-Management-Prozess ab.

IT-Manager müssen schon seit längerem mit inhomogenen Systemlandschaften zurechtkommen – und das Internet der Dinge verschärft die Situation durch eine Vielzahl sehr unterschiedlicher, internetfähiger Geräte, die im Rahmen der Beschaffung von Fachabteilungen Einzug in das Unternehmen halten. Zu diesen gehören eine Reihe von Devices, darunter medizintechnische Apparate in Krankenhäusern, Industrie-PCs oder Automobile im Fuhrpark – und die meisten von ihnen werden aktuell außerhalb des Radars der IT betrieben. Ähnlich verhält es sich beispielsweise bei Zutritts-Management-Systemen oder Schließanlagen von Gebäuden.

Warum sie die im Fachbereich angeschaffte Hard- und Software unter den Einflussbereich der IT-Abteilung stellen sollten, ist für viele Mitarbeiter zunächst nicht ersichtlich. Jedoch: Größtmögliche Sicherheit, Compliance und Business Continuity können ohne ein umfassendes IT-Management heute nicht mehr erreicht werden – dies ist wesentlicher Eckpfeiler einer modernen Geräte- und Systemverwaltung.

Lizenzrechtliche Prüfung

Ein erster Aspekt für das IT-Management betrifft die Lizenzierung. Zwar sind die meisten Geräte im Internet of Things mit OEM-Lizenzen ausgestattet. Viele Fachbereichsmanager und sogar einige IT-Leiter sind daher der Meinung, sie wären damit lizenzrechtlich automatisch auf der sicheren Seite. Doch das Gegenteil ist der Fall: Auch die serverseitige CAL-Lizenzierung (Client Access License) muss geprüft werden. Unter diesem

Aspekt zählt jedes Gerät, das auf den Server zugreift, also jede Maschine, jeder mobile Scanner und auch jedes „Connected Car“. Da inzwischen immer mehr Apps Verbindungen mit dem Unternehmensnetzwerk initiieren, sind die lizenzierten CALs oft rasch erreicht.

Aber je mehr Geräte sich im Netz eines Unternehmens anmelden, umso schwieriger wird es für die IT, sämtliche lizenzrechtlichen Anforderungen nachzuhalten. Der Versuch, dies manuell und mit Hilfe von Listen zu bewerkstelligen, ist zum Scheitern verurteilt – und kann teuer werden. Denn im Fall einer Plausibilisierung eines Softwareanbieters drohen hohe Nachzahlungen. Vermeiden lassen sich diese nachträglichen Forderungen am besten mit einem Software-gestützten Lizenzmanagement. In diesem Fall stellt eine automatisch erzeugte Lizenzbilanz auf Knopfdruck alle vorhandenen und genutzten Assets den bestehenden Lizenzen gegenüber. Ein Bedarf zur Nachlizenzierung wird so zuverlässig erkannt.

Flexible Inventarisierung

Die Einhaltung von Lizenzvereinbarungen geht einher mit einer effektiven Verwaltung aller Geräte, die sich im Netzwerk des Unternehmens anmelden. Kein einfaches Unterfangen, denn je nach Art und Funktion eines Geräts läuft die Beschaffung über die Fachbereiche und ohne unmittelbare Beteiligung der IT. Darüber hinaus werden für die Lizenzverwaltung Informationen benötigt, welche Software und welche Treiber auf den Devices installiert sind.

Mit einer leistungsstarken Inventarisierungslösung lassen sich diese Daten managen, bis zu 3.500 Systeminformationen pro Gerät können damit erfasst werden. Dabei spielt es keine Rolle, ob ein Gerät ständig im Netzwerk ist oder sich nur sporadisch einloggt: Je nach Gerät und Nutzungsart kommen unterschiedliche Inventarisierungsmethoden zum Zug.

So greifen bei einem agentenlosen Verfahren im Netzwerk verteilte Dienste nach festgelegten Zeitplänen remote auf die jeweiligen Devices zu und geben die ermittelten Daten an die Asset-Management-Datenbank weiter. Doch die agentenlose Methode erfasst nur Systeme, die zum Zeitpunkt des Scans im Netzwerk angemeldet sind. Für Infrastrukturen mit einem hohen Anteil an mobilen Endgeräten ist sie daher nicht ausreichend. In diesem Fall kommt zusätzlich die agentenbasierte Inventarisierung zum Einsatz, für die ein Softwareagent lokal installiert wird.

Auf Devices in Entwicklungsumgebungen, auf hochsensiblen Steuerungsanlagen in der Produktion oder bei Energieversorgern darf in der Regel keinerlei Fremdsoftware installiert werden. Diese Geräte sind aus Sicherheitsgründen auch nicht über das Firmennetzwerk erreichbar. Hier sollte die Inventarisierung „offline", beispielsweise über einen USB-Stick, erfolgen. Die erhobenen Daten speichert der Stick zwischen und überträgt sie später in die Asset-Management-Datenbank.

Automatisiertes Patchmanagement

Mit einer vollständig inventarisierten IT-Infrastruktur erzielen Unternehmen nicht nur die nötige Compliance. Sie begegnen auch erfolgreich Sicherheitsrisiken. Denn zu einem umfassenden Schutz gehört auch das zeitnahe, möglichst automatisierte Einspielen aktueller Patches und Updates auf sämtlichen betroffenen Geräten. Nicht umsonst zählt das Bundesamt für Sicherheit in der Informationstechnik, kurz BSI, das Patchmanagement zu den Top-10-Maßnahmen für Cybersecurity.

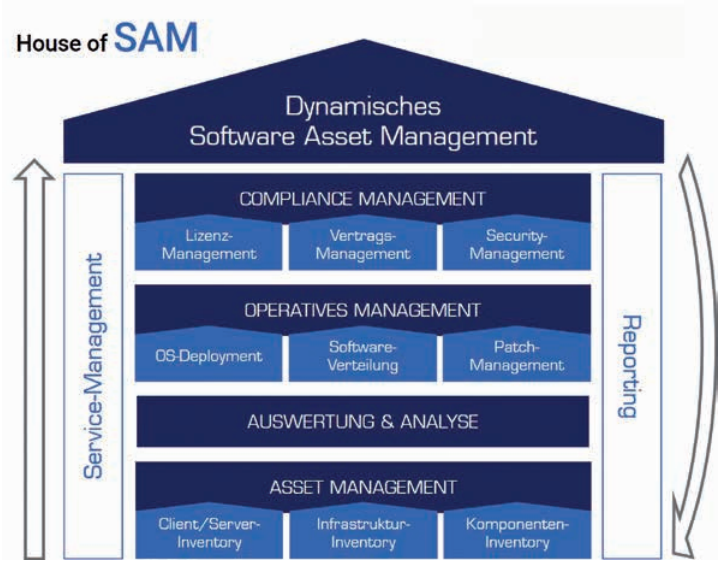
Intelligente, ganzheitliche Lösungen für IT und Software Asset Management (SAM), vereinen Lizenzmanagement, Inventarisierung sowie Softwareverteilung und Patchmanagement. Sie sind deshalb auch in der Lage, alle Anwendungen tagesaktuell mit einer Sicherheitsdatenbank abzugleichen und potentielle Sicherheitsrisiken aufzulisten. Direkt aus dieser Übersicht heraus sollte anschließend die neue Software verteilt beziehungsweise veraltete Software deinstalliert werden. Dabei müssen für jedes Gerät die Compliance-Vorgaben berücksichtigt und spezielle Wartungsintervalle eingehalten werden.

Werden diese eingehalten, sollten sich Bedrohungen durch Cyberkriminelle wie beispielsweise die WannaCry-Angriffe, die erstmals im Mai 2017 in die Schlagzeilen gerieten, weitgehend vermeiden lassen. Denn diese Attacke war nur dann erfolgreich, wenn Unternehmen auf die im März 2017 veröffentlichten Windows-Sicherheitspatches verzichtet hatten – ein Umstand, der für viele weitere Fälle von Internetkriminalität gilt.

Abgesicherte Business Continuity

Ein weiterer Aspekt, der sich unmittelbar auf die Produktivität von Unternehmen auswirkt, muss an dieser Stelle ebenfalls zur Sprache kommen: Werden Systeme mittels Sensoren und Aktoren laufend überwacht, lassen sich kritische Zustände von Produktionsanlagen bereits im Vorfeld erkennen und zuständige Techniker können rechtzeitig eingreifen. So kommt es erst gar nicht zu einer Leistungsreduktion oder einem Stillstand. Voraussetzung für diese Kontrollmöglichkeit ist ein leistungsstarkes Service Management, basierend auf einem entsprechenden Incident Management. Prozesse, die aus dem IT Service Management schon lange bekannt sind.

Praxisbeispiele zeigen, wie sehr sich das IT-Management diesbezüglich geändert hat: weg von einem Tool-bestimmten Ansatz hin zu abteilungsübergreifenden Abläufen. Gleichzeitig wurde der Verantwortungsbereich der IT zunehmend erweitert. So hatte sie zuvor einen Überblick über die eingesetzten IT-Systeme in einer heterogenen Systemumgebung, nicht aber über die darauf installierte lizenzpflichtige Software. Durch den Einsatz einer modernen Suite für IT und Software Asset Management kann dagegen heute die komplette IT-Infrastruktur des Konzerns abgebildet und die IT-Planung- und Verwaltung erheblich vereinfacht werden.



Erprobte Werkzeuge
für die digitale Transformation im Unternehmen
© DeskCenter Solutions AG

Fazit

Mit dem Management von Geräten des (Industrial) Internet of Things erweitert die IT ihren Verantwortungsbereich um ein geschäftskritisches Aufgabenfeld. Dank ihres langjährigen Service-Know-hows ist sie mit ihren Prozessen bereits bestens darauf vorbereitet. Die Herausforderungen, die eine rasant wachsende Anzahl unterschiedlichster Devices mit sich bringt, lassen sich mit Lösungen für das IT- und Software Asset Management der nächsten Generation, kurz SAM 4.0, meistern. Denn diese vereinen bereits die vier essenziellen Bausteine Discovery, Automation, Cybersecurity und Compliance. So erleichtern sie einem Unternehmen den Weg der digitalen Transformation – und die IT liefert damit einen wesentlichen Wertbeitrag für das gesamte Unternehmen.