INFORMATION SECURITY SOLUTIONS

PRIVILEGED IDENTITY MANAGEMENT

Hochprivilegierte Berechtigungen sicher und zugleich effizient verwalten

Der Umgang mit Benutzerberechtigungen in IT-Systemen rückt in den Fokus von Wirtschaftsprüfern, Unternehmensrevisionen und der Finanzaufsicht. Unternehmen reagieren und führen Identity & Access Management-Systeme ein. Oft vernachlässigen oder vergessen sie dabei aber Benutzerkonten mit besonders hohem Risikopotenzial. Dazu zählen die hochprivilegierten IT-Administratorkonten. Die Folgen reichen von Compliance-Verstößen bis hin zu Datenverlust durch Sabotage. Sopra Steria Consulting zeigt Ihnen den Weg zu einem sicheren und zugleich effizienten Umgang mit diesen Berechtigungen.

„Privileged Identities" – was ist das überhaupt?

Unter „Privileged Identities" versteht man im Allgemeinen hochprivilegierte Benutzerkonten, die oft keiner natürlichen Person direkt zugeordnet sind und über die höchsten Berechtigungen innerhalb eines Systems verfügen. Meistens handelt es sich dabei um in den Systemen zwingend vorhandene Benutzerkonten, die nicht gelöscht oder deaktiviert werden können. Man spricht auch von „Superusern".

Beispiele zur Veranschaulichung:

- User „root" in Unix-Systemen
- User „dba" in Oracle-Datenbanken
- User „sa" in Microsoft SQL-Servern
- User „rwa" in Cisco-Systemen

Nachlässigkeit ist die Realität

In vielen Unternehmen wird die Verwaltung hochprivilegierter Benutzerkonten immer noch vernachlässigt. Oftmals arbeiten ganze Abteilungen – zum Teil sogar mehrere Abteilungen – auf dem gleichen IT-System, der Einfachheit halber unter einem einzigen Benutzerkonto, das mit vielen Privilegien ausgestattet ist.

Die Passwörter dieser Benutzerkonten sind häufig weitläufig bekannt und werden selten bis gar nicht geändert. In vielen Fällen wird dasselbe Passwort für die hochprivilegierten Benutzerkonten mehrerer Systeme verwendet.

Warum führt das zu Schwierigkeiten?

Wird in Unternehmen wie oben beschrieben gearbeitet, ist es nicht mehr möglich nachzuvollziehen, welche Tätigkeiten auf welchem System, von welchem Mitarbeiter durchgeführt wurden, da alle unter der gleichen User-ID protokolliert werden.

Diese Nachvollziehbarkeit wird aber immer stärker gefordert, z. B. vom Gesetzgeber, aber auch von Branchenverbänden zur Erreichung von Compliance. Dabei müssen die Unternehmen sicherstellen, dass ihre Mitarbeiter auf den IT-Systemen nur über die Rechte verfügen, die sie für die Ausübung ihrer Tätigkeiten wirklich benötigen.

Es ergibt sich aber auch noch ein ganz praktisches Problem: Wenn Mitarbeiter immer mit höchsten Berechtigungen arbeiten, können auch kleine Fehler verheerende Auswirkungen haben. So kann ein an der falschen Stelle abgesetztes Löschkommando ungewollt ganze Datenbestände vernichten und das Unternehmen in wirtschaftliche sowie rechtliche Probleme stürzen.

Privileged Identity Management – was kann man sich darunter vorstellen?

Privileged Identity Management (PIM) stellt deshalb eine äußerst wichtige Ergänzung des klassischen Identity and Access Managements (IAM) dar. Während sich IAM hauptsächlich um die Verwaltung von Benutzerrechten persönlicher und technischer Benutzer kümmert, steht bei PIM die Verwaltung hochprivilegierter Benutzerkonten im Fokus.

PIM beginnt bei der Erfassung sämtlicher hochprivilegierter Benutzerkonten aller Systeme (z. B. durch Integration mit einer CMDB). Es setzt sich bei der Vergabe und Verwaltung individueller Passwörter pro System fort. Zuletzt werden die nötigen Zugriffsrechte für die Mitarbeiter vergeben und Freigabeprozesse definiert, mittels derer Zugriffe protokolliert und auditiert werden können.

Um schnelle Erfolge mit möglichst geringem Aufwand zu erzielen, empfiehlt sich ein schrittweises Vorgehen. Dies ist durch den modularen Aufbau von PIM-Lösungen problemlos möglich.

Welche Anforderungen werden an Privileged Identity Management gestellt und welche Vorteile bietet es?

Im ersten Moment mag es einem Systemverantwortlichen widersinnig und riskant erscheinen, die Passwörter aller hochprivilegierten Benutzer aller Systeme an einer zentralen Stelle zu speichern. Aber nur so ist es möglich sicherzustellen, dass die Passwörter auch für alle Systeme im Notfall zur Verfügung stehen.

Hieraus ergeben sich einige Anforderungen an PIM:

- Sehr hohe Datensicherheit
- Logischer und physischer Zugriffsschutz
- Durchgängige Protokollierung und ggf. Alarmierung
- Verfügbarkeit des Systems auch im Notfall

Damit Unternehmen zusätzlich zur deutlich erhöhten Systemsicherheit und der Erfüllung von Compliance-Anforderungen noch einen möglichst großen wirtschaftlichen Nutzen aus einer PIM-Lösung ziehen, ist Automatisierung ein entscheidender Faktor.

Durch die Integration einer PIM-Lösung in vorhandene Prozesse und Verfahren zur Bereitstellung, Änderung und Außerbetriebnahme von IT-Systemen reduziert sich der manuelle Arbeitsaufwand der Administratoren erheblich. Zudem wird sichergestellt, dass die Datenbestände immer aktuell sind.

Für Ihre Administratoren ergibt sich zusätzlich zur Arbeitsentlastung noch ein weiterer Vorteil: PIM versetzt Sie in die Lage, die Verwendung hochprivilegierter Benutzerkonten direkt nachzuvollziehen und einzelnen Personen zuzuordnen. Somit können Ihre Administratoren im Falle von Sicherheitsereignissen einen möglichen Missbrauchsverdacht zuverlässig entkräften.

Unser Anspruch – Ihr Nutzen

Durch jahrelange Erfahrung im IAM- und PIM-Umfeld besitzt Sopra Steria Consulting die nötige Expertise für die Analyse, das Design sowie der technischen Einführung einer PIM-Lösung.

Sprechen Sie uns an, wir beraten Sie gerne!

A4_18040_1504-SEC-d

Tel.: +49 40 22703-0
www.soprasteria.de