CONSULTING4IT

FALLSTUDIE

AKTIV GEGEN WIRTSCHAFTSSPIONAGE – Antriebsspezialist SEW-EURODRIVE optimiert Berechtigungsmanagement und Datenschutz mit Varonis

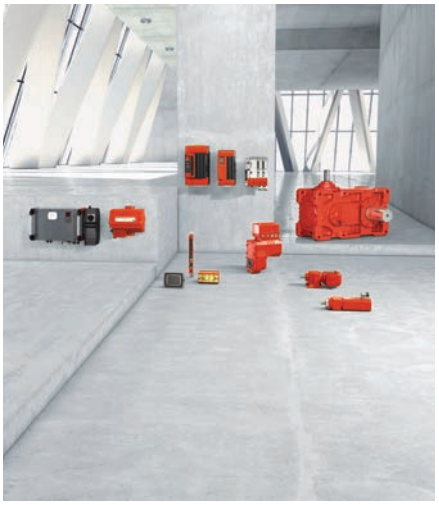
SEW-EURODRIVE, Familienunternehmen in der mittlerweile dritten Generation, ist eines der international marktführenden Unternehmen für Antriebstechnik und Antriebsautomatisierung mit über 16.000 Beschäftigten.
15 Fertigungswerke und 77 Drive Technology Center verteilen sich auf 51 Länder weltweit.
Zu den Kunden gehören kleine Unternehmen genauso wie Konzerne. SEW-EURODRIVE versteht sich zudem als einer der Treiber von Industrie 4.0. Die Logistik des Unternehmens ist in vielen Bereichen bereits seit längerem stark automatisiert. Das erworbene Know-How verkauft SEW-EURODRIVE mittlerweile als eigene Dienstleistung.

Die IT ist überwiegend zentral organisiert. Die Rechenzentren stehen am Hauptstandort in Bruchsal. Das macht es in Sachen IT-Sicherheit etwas einfacher. Bernhard F. Haungs ist IT-Compliance & Information Security Verantwortlicher und gleichzeitig Datenschutzbeauftragter. „Das klingt überraschend kommt aber in der Praxis immer häufiger vor. Konflikte sehe ich nicht, eher ergänzen sich die beiden Bereiche."

Industriespionage? Ist Fakt

2005 war SEW-EURODRIVE mit einem schweren Fall von Industriespionage konfrontiert. Auf der HANNOVER MESSE entdeckte man eigene Produkte auf einem anderen Messestand. „Zwar noch nicht ausführbar, aber schon als Produkt. Da spätestens war uns klar, dass wir unbedingt etwas tun müssen", so Haungs.

Untätig war die SEW-EURODRIVE in Sachen IT- und Informationssicherheit bis dato nicht gewesen. Neben den Anforderungen des BSI (Bundesamt für Sicherheit in der Informationstechnologie) hatte man bereits die BS 7799-1 umgesetzt. 2006 führte das Unternehmen als eines der ersten überhaupt die ISO/IEC 27001 ein. Die ISOs bringen etliche Anforderungen mit, wenn es um Verfügbarkeit, Vertraulichkeit und Integrität geht. Dennoch ließen sich viele Fragen immer noch unzureichend oder nur mit einem enormen Zeitaufwand beantworten.



2005 war SEW-EURODRIVE mit einem schweren Fall von Industriespionage konfrontiert. Auf der HANNOVER MESSE entdeckte man eigene Produkte auf einem anderen Messestand. Zwar noch nicht ausführbar, aber schon als Produkt. Da spätestens war uns klar, dass wir unbedingt etwas tun müssen.

Bernhard Haungs, IT Compliance & Information Security Verantwortlicher und Datenschutzbeauftragter SEW-EURODRIVE GmbH

CONSULTING4IT

Consulting4IT GmbH
Im Ermlisgrund 6
D - 76337 Waldbronn

Telefon: +49 7243 - 2058 - 500
Telefax: +49 7243 - 2058 - 502
Web: www.consulting4it.de
E-Mail: info@consulting4it.de

Mehr Fragen als Antworten

Die Initialzündung für die Einführung eines Berechtigungsmanagements war schließlich ein Managementmeeting. Dabei kamen die Fragen auf: Wie und wo sind die Daten gerade gespeichert und wer hat worauf Zugriff?
„In so einem Moment stehen Sie als Verantwortlicher für die Informationssicherheit einsam da. Sie können zwar viel sagen. Aber letzten Endes wissen Sie es eben auch nicht ganz genau“, erinnert sich Haungs.

Für die lokal vorgehaltenen Daten - zum Teil auf den über 1.000 iPhones in Bruchsal - sind die Besitzer verantwortlich. Den internationalen Sicherheitslevel gibt die ISO 27001 am Standort Bruchsal vor, die weltweit angesiedelten Standorte werden dementsprechend zertifiziert.

Anders, als bei den lokalen Daten, sieht es in den zentralen Rechenzentren in Bruchsal bei den strukturierten und unstrukturierten Daten aus. Dabei sind die unstrukturierten Daten die größere Herausforderung für SEW-EURODRIVE.

Insbesondere weil sie mit inzwischen 180 Terabyte den größten Teil der von SEW-EURODRIVE erzeugten Daten repräsentieren. Und diese Datenmenge wächst jährlich stark an. Das sorgte für Intransparenz unterhalb der obersten Hierarchieebene von File- und SharePoint-Servern sowohl für die IT-Abteilung als auch das Management.

Die im Rechenzentrum gespeicherten unstrukturierten Daten verteilten sich auf Exchange/Outlook, diverse Fileserver sowie SharePoint beziehungsweise Intranet.

Die geforderte Transparenz herzustellen war mit Bordmitteln nicht möglich. Es musste also eine Lösungen gefunden werden, welche im Wesentlichen zwei Dinge sicherstellt: Konsolidierung der Berechtigungen sowie die vollständige und transparente Einsicht in alle Ereignisse.

Berechtigungen konsolidieren, Zugriffsaktivitäten nachvollziehen

Der Grundgedanke eines sicheren Austauschs von Dateien ist der, dass Benutzer nur auf diejenigen Informationen zugreifen können, die sie für ihre Arbeit brauchen - und nur auf diese Informationen.

Bei der Suche nach einer Lösung wurde das Unternehmen auf DatAdvantage von Varonis aufmerksam. „Uns ist sehr schnell klargeworden, dass DatAdvantage alle Anforderungen erfüllt, die wir vorab definiert hatten“, erklärt Haungs.
Die Lösung kann vor allem die beiden wichtigsten Anforderungen, Konsolidierung von Berechtigungen und Transparenz über Zugriffsaktivitäten, mit Hilfe seiner Kernfunktionen erfüllen.

Über eine bidirektionale Sicht auf die Filesystemberechtigungen, erhält man zum Beispiel darüber Einsicht, welcher Benutzer auf welche Dateien und Ordner zugreifen kann.

„Uns ist sehr schnell klargeworden, dass DatAdvantage alle Anforderungen erfüllt, die wir vorab definiert hatten.“

Die Lösung kann vor allem die beiden wichtigsten Anforderungen, Konsolidierung von Berechtigungen und Transparenz über Zugriffsaktivitäten, mit Hilfe seiner Kernfunktionalitäten erfüllen. Über eine bidirektionale Sicht auf die Filesystemberechtigungen, erhält man zum Beispiel darüber Einsicht, welcher Benutzer auf welche Dateien und Ordner zugreifen kann.

Bernhard Haungs, IT Compliance & Information Security Verantwortlicher und Datenschutzbeauftragter SEW-EURODRIVE GmbH

Consulting4IT GmbH
Im Ermlisgrund 6
D - 76337 Waldbronn

Telefon: +49 7243 - 2058 - 500
Telefax: +49 7243 - 2058 - 502
Web: www.consulting4it.de
E-Mail: info@consulting4it.de

Bereinigen aber wie?

Für einen wirksamen Data-Governance-Prozess braucht man den Kontext zu seinen Daten, die sogenannten Metadaten. Das sind besonders User- und Gruppeninformationen, Informationen zu den Berechtigungen, Zugriffsaktivitäten sowie Hinweise auf sensible Inhalte und wo sich diese befinden.

Bei der Rückspiegelung der Daten sind sämtliche Fileserver nach Bereichen ausgewertet und folgende Ergebnisse ermittelt worden:

- Welche Ordner sind für „jeden“ zugänglich?
- wer (Nutzer/Gruppe) greift auf welche Ordner zu?
- Welche Ordner sind über einen bestimmten Zeitraum hinweg überhaupt nicht geöffnet worden?
- Wo sind Anomalien und von der definierten Norm abweichende Aktivitäten auf den Fileservern zu beobachten?

In der Praxis

Bevor DatAdvantage eingesetzt wurde, war bei SEW-EURODRIVE nicht immer genau klar, wer alles auf welche Dateien zugreift. Somit waren auch genaue Angaben über einen Zugriff wie zum Beispiel über ausgeführte Aktivitäten, Datum, Uhrzeit oder IP-Adresse nicht möglich. Seit dem Einsatz ist dies jederzeit transparent.

Auf dieser Grundlage werden auch die Berechtigungen vergeben. So konnten Altlasten wie zum Beispiel der Zugriff aller Mitarbeiter auf geschäftskritische Ordner der „Entwicklungsabteilung Motoren“ behoben werden.

Um Abweichungen vom Sollzustand zu entdecken nutzt man auch die Fähigkeit von DatAdvantage mit Hilfe von lernenden Algorithmen Anomalien zu identifizieren.

Zum Beispiel konnte bei einem vermeintlichen Datendiebstahl schnell Entwarnung gegeben werden. Man hatte beobachtet, das große Datenmengen abgezogen worden waren. Doch es handelte sich um ein Großprojekt in Singapur, bei dem ein ganzer Datenbereich für den Vor-Ort-Einsatz verlagert wurde.

Bevor DatAdvantage eingesetzt wurde, war bei SEW-EURODRIVE nicht immer genau klar, wer alles auf welche Dateien zugreift. Somit waren auch genaue Angaben über einen Zugriff wie zum Beispiel über ausgeführte Aktivitäten, Datum, Uhrzeit oder IP-Adresse nicht möglich. Seit dem Einsatz ist dies jederzeit transparent. Auf dieser Grundlage werden auch die Berechtigungen vergeben.

Consulting4IT GmbH
Im Ermlisgrund 6
D - 76337 Waldbronn

Telefon: +49 7243 - 2058 - 500
Telefax: +49 7243 - 2058 - 502
Web: www.consulting4it.de
E-Mail: info@consulting4it.de

2016: Und jetzt auch für Sharepoint...

In SharePoint gab es eine ganze Reihe von Problemen. Die Vererbung von Rechten in Gruppen und Berechtigungsstufen ist einigermaßen komplex und entsprechend aufwendig ist es die Berechtigungen zu überprüfen.

Ebenso war unklar, ob die Site-Owner oder diejenigen, die eine Zugriffsberechtigung beantragt hatten - zum Beispiel nach Umstrukturierung - noch immer die richtigen Ansprechpartner sind.

Mithilfe von Varonis wird SharePoint jetzt wie ein Fileserver inventarisiert, sämtliche Zugriffsaktivitäten protokolliert sowie Nutzer und Administratoren automatisch benachrichtigt.

Bei bestimmten, definierten Vorfällen erzeugt die Software automatisch ein Reporting und bei einem abweichenden Verhalten löst sie sofort einen Alarm aus.

Fazit

Bernhard F. Haungs: „Mit einem Entwicklungsteam von 700 Mitarbeiter kann niemand Industriespionage zuverlässig ausschließen.

Wir haben jetzt eine Lösung, die uns das Datenmanagement und das Nachvollziehen sämtlicher Zugriffsaktivitäten und Ereignisse erlaubt.

Das Reporting bietet uns wertvolle Analysedaten. Das hat die Datensicherheit und den Datenschutz im gesamten Unternehmen nachhaltig verbessert."

Projektsteckbrief

Kunde:
SEW-EURODRIVE GmbH & Co KG

Ort:
Bruchsal, Deutschland (Hauptsitz)

Branche:
Einer der internationalen Marktführer im Bereich Antriebstechnik/ Antriebsautomatisierung

Herausforderung:
Die Menge an nutzergenerierten Daten stieg auch bei SEW-EURODRIVE kontinuierlich an. Den Überblick darüber zu behalten, welche Berechtigungen vergeben worden waren, wer über welche Zugriffsrechte verfügte und wie er sie nutzte sowie Zugriffsaktivitäten und Ereignisse nachzuvollziehen erwies sich als aufwendig bis unmöglich.

Die Lösung:
Varonis DatAdvantage für NetApp, Windows, Active Directory und SharePoint

Vorteile:
- Langfristig konsolidierte Berechtigungen
- Zugriffsaktivitäten und Ereignisse transparent nachvollziehen
- Automatisiertes Benachrichtigungsmanagement & Reports
- Stellt Compliance her und verbessert den Datenschutzlevel im gesamten Unternehmen

Partner:
Der betreuende Partner der SEW-EURODRIVE ist Consulting4IT GmbH

GOLD PARTNER

Consulting4IT GmbH
Im Ermlisgrund 6
D - 76337 Waldbronn

Telefon: +49 7243 - 2058 - 500
Telefax: +49 7243 - 2058 - 502
Web: www.consulting4it.de
E-Mail: info@consulting4it.de