

sds etabliert mit CA Access Control einheitliche Sicherheitsstrukturen nach ISO und erhöht dadurch seine Wettbewerbsfähigkeit.



Kundenprofil

Branche: Informations- und Kommunikationstechnologie
Unternehmen: sds business services GmbH (an ACS company)
Mitarbeiter: rund 160
Umsatz: 29,6 Mio. € (FY 2009)

Nutzen für die Organisation – Übersicht

Business:

sds als deutsche Landesgesellschaft der ACS gehört zu den führenden Anbietern von IT-Dienstleistungen in Deutschland. In seinen Rechenzentren betreut sds zentral über 20.000 internationale Anwender. Zum Angebot gehört das vollständige Spektrum des RZ-Betriebes sowie das komplette Netzwerk-Management. Hinzu kommen Software-Entwicklung sowie die System- und Software-Integration.

Challenge:

Die Sicherheit der Kundendaten sowie Compliance haben bei sds höchste Priorität. Um den Anforderungen seiner Kunden gerecht zu werden, suchte sds nach einer einheitlichen Sicherheitslösung für alle betriebenen Plattformen. Gefragt war eine breitgefächerte Lösung, mit der sich sowohl die unterschiedlichen Sicherheitspolicies der Kunden, als auch die hauseigenen Sicherheitsbestimmungen von sds umsetzen lassen.

Solution:

Die Wahl fiel wegen ihrer hohen Flexibilität und der fein abgestuften Mechanismen für die Zugangskontrolle auf CA Access Control in Verbindung mit CA Audit. Mit beiden Lösungen konnte sds die geforderte ISO 27001-Zertifizierung erreichen. Die CA-Lösungen vereinfachen die Administration sowie die Einrichtung von Policy Groups und personalisierten Zugriffsrechten über alle Plattformen hinweg.

Result:

CA Access Control vereinfacht die Identifizierung der Benutzer sowie die Protokollierung der Aktionen. Darüber hinaus können gewachsene Konzepte problemlos übernommen werden. Unter dem Strich bedeutet das eine höhere Flexibilität, mehr Transparenz und nicht zuletzt die Erfüllung aller Anforderungen an Compliance. Der Einsatz von CA Access Control hat die Abläufe in den sds-Rechenzentren deutlich verbessert und beschleunigt.

Business

Durchgängiges Sicherheitskonzept auf allen Plattformen

sds business services GmbH ist einer der führenden "Full-Service IT-Provider" in Deutschland. Zum Portfolio gehört die IT-Infrastruktur ebenso, wie das Hosting, die Softwareentwicklung und der Betrieb von SAP-Systemen und Oracle Datenbanken. sds wurde 1969 als Unternehmen der Stinnes AG gegründet und gehört heute zur Affiliated Computer Services, Inc. In seinen Rechenzentren in Mülheim an der Ruhr sowie in Duisburg betreibt das Unternehmen rund 700 Server, wobei der Schwerpunkt auf IBM pSeries und Intel-basierten Fujitsu Siemens Servern der Primary-Familie liegt. Im Netzwerkbereich dominieren Cisco-Komponenten, die mit den entsprechenden Tools verwaltet werden. Zu den Kunden gehören namhafte Unternehmen, wie DB Schenker, toom BauMarkt GmbH, Brenntag Holding GmbH oder die Saint-Gobain Building Distribution Deutschland GmbH, um nur einige zu nennen.

Challenge

Compliance ist ein wichtiges Thema

Die Einhaltung der mit den Kunden vereinbarten Service Levels garantiert bei sds ein proaktives Monitoring, das sämtliche Abläufe in den Rechenzentren überwacht. Die Service Levels entsprechen den individuellen Anforderungen der Kunden und orientieren sich an deren Servicelandschaft sowie den jeweiligen Applikationen.

„Verstärkt kommt aber jetzt auch das Thema Compliance auf den Tisch, das alle Unternehmensgrößen betrifft“, berichtet Jörg Ortmann, bei sds verantwortlich für den SAP-Basisbetrieb. „Hand in Hand damit geht bei nahezu allen Kunden zudem der Wunsch nach mehr Sicherheit, getrieben durch höhere Revisionsanforderungen. Immer häufiger wird dabei die Zertifizierung nach ISO 27001 für alle vom Dienstleister erbrachten Services nachgefragt.“

Als 2007 der Vertragsabschluss mit einem großen Unternehmen von der ISO 27001 Zertifizierung abhängig gemacht wurde, suchte sds nach einer breitgefächerten Lösung, die auf sämtlichen Plattformen des Rechenzentrums eingesetzt werden kann. sds wollte zudem ein Sicherheitssystem, das die individuellen Sicherheits-Policies der unterschiedlichen Kunden und die hauseigenen Bestimmungen gleichzeitig umsetzt. „Auf keinen Fall wollten wir Insellösungen, die nur auf einzelnen Servern laufen und nur bestimmte Bereiche abdecken“, berichtet Jörg Ortmann. Darüber hinaus musste eine Lösung gefunden werden, die schnell verfügbar und implementierbar war.

„Kunden, die global agieren, benötigen ein zuverlässiges Sicherheitskonzept, das sich an internationalen Standards orientiert. Das ist der Grund für die steigende Nachfrage nach einer ISO 27001 Zertifizierung.“

Jörg Ortmann

Teamleiter SAP Basis, sds business services

„Die CA-Lösung optimiert unsere internen Prozesse, erleichtert die Arbeit unserer Administratoren und schafft Transparenz auf ganzer Linie.“

Jörg Ortmann
Teamleiter SAP Basis, sds business services

Solution

Einheitliches Sicherheitskonzept überzeugt

Nach einer vergleichsweise kurzen Evaluierung des Marktes zogen die Verantwortlichen bei sds, die Lösung CA Access Control in die nähere Auswahl. CA kannte man bereits aus der Zusammenarbeit in anderen Bereichen. Mit den Produkten hatte man gute Erfahrungen gemacht.

Auch das Leistungsspektrum von CA Access Control konnte schnell überzeugen, beispielsweise durch seine plattformübergreifende Einsatzmöglichkeit, eine Option die viele andere Lösungen nicht bieten. „Es handelt sich um eine breitgefächerte Lösung, die es uns ermöglicht, den zertifizierten Sicherheitsstandard ohne großen Aufwand plattformübergreifend in der gesamten Serverlandschaft einzuführen“, begründet Jörg Ortmann die Entscheidung für die CA Access Control.

Als CA zum ersten Inhousegespräch gleich seinen Partner NEAM mit an die Ruhr brachte, war die endgültige Entscheidung zugunsten von CA Access Control schnell gefällt. NEAM verfügt über ein umfassendes ISO-Know-How, führt selbst ISO 27001 Zertifizierungen durch und implementiert seit Jahren erfolgreich CA Software. In das ISO 27001-Projekt bei sds konnte der CA-Partner zudem bereits bestimmte Regelsätze, Best Practises und Dokumentationen einbringen, was die Implementierungsphase deutlich verkürzte. Diese Kompetenz war ein maßgebliches Kriterium für die kurzfristige Einführung von CA Access Control im Rechenzentrum von sds.

Die Lösung wird eingesetzt, um Bereiche mit unternehmenskritischen Applikationen der Kunden durch fein abgestimmte Sicherheitsmechanismen gegen unautorisierte Zugriffsversuche zu schützen. „Wir haben aber den Einsatz von Access Control im Rahmen des Projektes auf zunächst 20 Server beschränkt“, erzählt Jörg Ortmann. Sukzessive wird die Lösung auf weiteren Systemen implementiert.

Die wichtigste Funktion von CA Access Control in Verbindung mit CA Audit ist für sds die Möglichkeit, die individuellen Sicherheits-Policies seiner Kunden in sogenannten Policy-Groups hierarchisch zu strukturieren.

Gewachsene Konzepte eines Kunden können problemlos übernommen werden, was einerseits die Flexibilität und die Transparenz steigert, gleichzeitig aber auch zu einer deutlichen Qualitätsverbesserung führt. sds muss die Security-Einstellungen der Server nicht mehr individuell verwalten, sondern kann diese automatisch den relevanten Policy Groups und deren individuellen Regeln zuordnen. Darüber hinaus können mit CA Audit zentral und einheitlich Security-Logs überwacht werden.

„CA Access Control ist State-of-the Art und die bei sds implementierten Regeln gewährleisten einen hohen Sicherheitsstandard nach ISO 27001“, sagt Jörg Ortmann. „Unseren Kunden können wir damit eine Out-of-the-Box-Lösung anbieten, die von Haus aus bestimmte Best-Practise-Standards enthält und mit der ein Grundgerüst bereitgestellt wird, das bei Bedarf ausgebaut werden kann. Neukunden wird das System als Standard angeboten“.

„Durch den Einsatz von CA Access Control können wir die geforderten Security Policies auf unseren Servern heute innerhalb weniger Stunden implementieren. Die Security-Anforderungen unserer Kunden können schneller und damit kostengünstiger umgesetzt werden.“

Jörg Ortmann

Teamleiter SAP Basis, sds business services

Result

Kunden profitieren von einheitlichem Konzept

Durch den Einsatz von CA Access Control konnte sds seine Sicherheitsstandards weiter vereinheitlichen und Prozesse zentralisieren. „Die Vorteile, die wir erzielen, können wir zwar nicht in Euro und Cent beziffern“, schmunzelt Jörg Ortmann. „Allerdings zeigt sich der Nutzen in optimierten Arbeitsabläufen und in einer deutlich höheren Transparenz der Prozesse.“

Davon profitiert sowohl sds als auch die Kunden. Dank CA Access Control konnte sds:

- Sein Security Management vereinfachen
- Die Arbeit der Administratoren dank der Policy Groups optimieren
- Konfigurationsprozesse von mehreren Tagen auf wenige Stunden reduzieren
- Kosten reduzieren.

„Gerade beim Setup spielt CA Access Control seine volle Stärke aus“, betont Jörg Ortmann. „Während wir früher für die Serverkonfiguration mehrere Tage brauchten, ist dieser Job heute in zwei bis drei Stunden erledigt. Dem Kunden steht die Infrastruktur schneller zur Verfügung, gleichzeitig reduzieren sich die Implementierungskosten.“ Dadurch konnte sds die Kundenbindung weiter erhöhen und seine Position im Wettbewerb stärken.

Wenn Sie weitere Informationen dazu erhalten möchten, wie CA Sie bei der Umstellung Ihres Unternehmens unterstützen kann, besuchen Sie unsere Website ca.com.