DMK Deutsches Milchkontor sichert Remote Access Mit IDENTIKEY und DIGIPASS

Deutschlands größtes Molkereiunternehmen, DMK Deutsches Milchkontor , setzt beim Fernzugriff auf sein Netzwerk und seine kritischen Daten seit Jahren auf eine starke Zwei-Faktor-Authentifizierung. Im Zuge einer Rechenzentrums-Konsolidierung und des Austauschs der Remote-Access-Hardware entschied das Unternehmen sich, von der bisherigen Lösung auf DIGIPASS-Authentifizierer und den IDENTIKEY Server von VASCO umzusteigen.

Mit 6.240 Mitarbeitern an 24 Standorten und einem Umsatz von 4,4 Milliarden Euro ist DMK das größte Molkereiunternehmen Deutschlands und eines der führenden in Europa. Jährlich verarbeitet DMK 6,6 Milliarden Kilogramm Milch, die das Unternehmen von rund 9.800 aktiven Milcherzeugern bezieht. Die Gesellschaft ist genossenschaftlich orientiert und gehört der Deutsches Milchkontor eG, die im Jahr 2012 aus der Fusion dreier Genossenschaften entstand: der Humana Milchunion eG, der Nordmilch eG und der Molkereigenossenschaft Bad Bibra eG.

FERNZUGRIFF KOMPLETT NEU ORGANISIERT

Im Zuge der Fusion und der Gründung der GmbH entschieden sich die Verantwortlichen, die vorhandenen Rechenzentren in nur einem neuen Rechenzentrum zu konsolidieren. Zudem stand ein Wechsel der Hardware-Plattform für den Remote Access an, da der Hersteller den technischen Support für die bisherige Hardware abgekündigt hatte. Daher entschied sich DMK dafür, den Fernzugriff komplett neu zu organisieren und auch die Authentifizierungslösung neu auszuschreiben, zumal man in Zukunft verstärkt auf Software-Authentifizierer setzen wollte.

Auf Empfehlung ihres langjährigen Systemhauspartners concentrade GmbH mit Sitz in Dortmund implementierte DMK Mitte 2012 eine komplett neue Remote-Access-Plattform, bestehend aus einer Juniper Appliance und dem IDENTIKEY Server von VASCO. concentrade hatte bereits die vorhergehende Lösung installiert und betreut und war auch entscheidend an der Planung und Installation der neuen beteiligt. Während einer Testphase wurden einige Anwender mit Authentifizierern vom Typ DIGIPASS GO 6 ausgestattet, andere mit DIGIPASS for Mobile für die starke Authentifizierung mithilfe der unternehmenseigenen Blackberrys. Nach einer erfolgreichen Testphase wurden dann im November die ersten Anwender komplett auf die neue Plattform umgezogen. Bis April 2013 wurden etwa 300 Anwender auf VASCO-Authentifizierer migriert; spätestens 2015 soll die Umstellung abgeschlossen sein.

KEINE FESTEN ABLAUFZEITEN MEHR

Michael Knipping, Teamleiter Netzwerk bei DMK, begründet die Entscheidung für VASCO vor allem mit dem Ziel, verstärkt auf Software-Authentifizierer zu setzen. „Zudem hatten wir bei unserer bisherigen Lösung das Problem, dass alle Tokens ein festgelegtes Ablaufdatum hatten, unabhängig von ihrem tatsächlichen Zustand“, so Knipping. „Das kostet erstens unnötig Geld, und zweitens ist der Rollout dann ein Problem, wenn man aus Kostengründen die Tokens im 50er-Pack kauft und nun 50 Anwender auf einmal umstellen muss. Bei Vasco gibt es keine derartigen Ablaufdaten, und die mobilen DIGIPASSES muss man überhaupt nicht mehr austauschen.“ Zudem war die VASCO-Lösung laut Michael Knipping auch deutlich günstiger als andere Alternativen.

UMSTIEG IM PARALLELBETRIEB

Den Umstieg auf die neue Lösung gestaltete DMK möglichst einfach durch einen Parallelbetrieb beider Installationen. Die Mitarbeiter werden nach und nach auf die VASCO-Plattform umgestellt und melden sich bis dahin weiter über die noch vorhandene, ältere Lösung im bisherigen Rechenzentrum an. Die Umstellung erfolgt spätestens immer dann, wenn ihre vorhandenen Token ablaufen, möglichst aber früher. Es hätte zwar auch die Möglichkeit gegeben, beide Systeme über eine Proxy-Lösung technisch zu integrieren, aber DMK wollte den Migrationsprozess mit möglichst wenig Komplexität durchführen. Doch auch so hat sich für die Anwender praktisch nichts geändert. Sie arbeiten weiterhin mit den VPN Clients von Juniper und bekommen ihr Einmalpasswort jetzt lediglich von einem neuen Authentifizierer. Daher gab es bei den Anwendern durch die Umstellung auch keinerlei Probleme.

Auch die Mitarbeiter in der IT sind mit der neuen Lösung sehr zufrieden. „Die Installation und die Tests verliefen ohne größere Probleme“, so Michael Knipping, „und auch der Rollout der Authentifizierer stellt keine große Herausforderung

dar. Zudem haben wir während des gesamten Projekts eine hervorragende Betreuung von concentrade genossen und konnten so von deren Erfahrung aus anderen Projekten profitieren."

Ziel

Ablösung einer existierenden Authentifizierungs-Lösung für Remote Access im Rahmen einer Rechenzentrums-Konsolidierung. Zudem sollten verstärkt Software-Authentifizierer eingesetzt werden.

Herausforderung

Die Migration musste im laufenden Betrieb erfolgen, ohne die Sicherheit des Remote Access zu beeinträchtigen.

Lösung

DMK entschied sich für die Kombination aus dem IDENTIKEY Server und den Authentifizierern der DIGIPASS-Familie von VASCO. Die Umstellung von der bisherigen Lösung erfolgt Schritt für Schritt im Rahmen eines Parallelbetriebs.

Über Deutsches MilchKontor

DMK Deutsches Milchkontor ist mit 6,6 Milliarden verarbeiteten Kilogramm Milch Deutschlands größtes Molkereiunternehmen. Hinter DMK stehen rund 9.800 aktive Milcherzeuger. Die Milch wird an 24 Standorten mit Hilfe von 6.240 Mitarbeitern unter anderem zu Milchbasisprodukten und Käse, Markenprodukten wie MILRAM Gewürzquarks oder Ravensberger Desserts über milchbasierte Inhaltsstoffe als Ingredients für weiterverarbeitende Lebensmittelhersteller bis hin zu Humana Babynahrung, Eiskrem und sanotact Gesundheitsprodukten. verarbeitet. Mit 4,4 Milliarden Euro Umsatz gehört das Unternehmen auch europaweit zu den Top Ten der Milchindustrie.

Über concentrade

concentrade ist renommierter Lösungsanbieter für den Bereich IT-Sicherheit und Netzwerkkommunikation mit Sitz in Dortmund. Das Unternehmen ist 1997 als Gesellschaft mit beschränkter Haftung (GmbH) gegründet worden und ist seither inhabergeführt. Unser Ziel ist die Sicherstellung eines störungsfreien Netzwerkbetriebs und die wirksame und kosteneffiziente Minimierung von Sicherheitsrisiken für unsere Kunden.

Über Arrow ECS

Arrow mit Sitz in Fürstenfeldbruck bei München wurde im Jahr 1988 gegründet. Das Unternehmen beschäftigt heute ca. 200 Mitarbeiter in Fürstenfeldbruck und im Logistikzentrum in Neuenstein. In Deutschland hat sich Arrow auf die Produktbereiche Server, Storage, Networks & Security, Desktop Delivery, Virtualisation sowie Services fokussiert. Darüber hinaus bietet Arrow ein einzigartiges Cloud Portal „Arrow-Sphere", das Resellern den Vertrieb von Cloudlösungen auf Basis eines eigenen Webportals ermöglicht.

Über VASCO

VASCO ist ein führender Anbieter von Lösungen für Strong Authentication sowie digitale Signatur und hat sich auf Internet-Sicherheits-Anwendungen und -Transaktionen spezialisiert. VASCO konnte sich weltweit als Software-Unternehmen für Internet-Security etablieren und beliefert etwa 10.000 Unternehmen in mehr als 100 Ländern, darunter mehr als 1.700 internationale Finanzinstitute. Die wichtigsten Märkte für VASCO sind der Finanzsektor, Unternehmens-Sicherheit, e-Commerce und e-Government.

www.vasco.com

BRUSSELS (Europe)
phone: +32 2 609 97 00
email: info-europe@vasco.com

BOSTON (North America)
phone: +1 508 366 3400
email: info-usa@vasco.com

SYDNEY (Pacific)
phone: +61 2 8061 3700
email: info-australia@vasco.com

SINGAPORE (Asia)
phone: +65 6323 0906
email: info-asia@vasco.com