AMPEG

KWS SAAT SE

70 Länder
auf einen Blick

A Security Lighthouse Case Study

70 Länder auf einen Blick

Je komplexer die technischen und organisatorischen Strukturen einer IT-Landschaft ausfallen, desto aufwendiger wird die Ermittlung des aktuellen Sicherheitsstatus aller Systeme. Das Unternehmen KWS SAAT SE (KWS) löste die Aufgabe bisher durch den manuellen Abgleich umfangreicher Tabellen aus verschiedensten Quellen rund um den Globus. Jetzt erhebt und visualisiert Security Lighthouse von AMPEG die sicherheitsrelevanten Informationen auf Knopfdruck. Sie werden rollengerecht dosiert und nahezu in Echtzeit den eigenen Service Centern und auch verschiedenen IT-Service-Providern zur Verfügung gestellt, die international die Standorte von KWS betreuen.

KWS züchtet seit 160 Jahren landwirtschaftliche Nutzpflanzen. Heute gehört das Unternehmen mit Hauptsitz im niedersächsischen Einbeck zur Spitzengruppe der internationalen Saatgutproduzenten. Rund 5.000 Mitarbeiter sind für KWS tätig, die Standorte verteilen sich auf 70 Länder auf fast allen Kontinenten und reichen von kompletten Niederlassungen unterschiedlicher Größe bis hinab zu kleinen und kleinsten Vertretungen, die im Extremfall lediglich Messdaten von Versuchsfeldern in entlegenen landwirtschaftlichen Regionen übermitteln.

Die Struktur des Unternehmens hat zur Folge, dass sich seine IT mit etwa 3500 Client- und 700 Server-Systemen nicht vollständig zentralisieren lässt. Zwei wichtige Rechenzentren befinden sich am Hauptstandort, aber die weltweit verteilten Vertretungen arbeiten je nach Bedarf mehr oder weniger selbstständig. Sie nutzen beispielsweise eigene Zugänge zum Internet, da eine zentrale Führung der Gesamtkommunikation aufgrund möglicher Übertragungsverzögerungen und mit Rücksicht auf die Konsequenzen des Geo-IP-Konzepts nicht in Frage kommt. Außerdem schlägt zu Buche, dass das Arbeitsfeld von KWS eben nicht primär in den internationalen Metropolregionen liegt, sondern in ländlichen Bereichen mit teilweise nur schmalbandiger Internet-Anbindung.

Sichtkontrolle der Zuckerrübenpflanzen im Nährmedium
Quelle: KWS SAAT SE

Ausgelagerte operative IT

KWS hat seine operative IT weitgehend in die Hände von Service-Providern übergeben. Manche dieser Dienstleister betreuen nur eine Region, andere auch mehrere. Gesteuert werden der IT-Betrieb und die Tätigkeit der Service-Provider von fünf KWS eigenen Service Centern aus, die ebenfalls für unterschiedliche Regionen verantwortlich sind: Deutschland, Westeuropa, Osteuropa, Nordamerika und Südamerika.

70 Länder auf einen Blick

Diese Konstellation verlangt der IT-Leitung und den Sicherheitsverantwortlichen großes organisatorisches Geschick ab, wenn es darum geht, den Sicherheitsstatus der Systeme im gesamten KWS Netzwerk zu prüfen, Schwachpunkte zu erkennen und gezielt zu beheben. Die Einhaltung eines definierten Mindestniveaus in der IT-Security hat für KWS hohe Priorität, denn für die Marktchancen des Saatgut-Anbieters stellen die Ergebnisse seiner IT-gestützten Forschung und Entwicklung einen wesentlichen Faktor dar. Auch der weltweite Vertrieb und die Steuerung der Produktion sind eng mit der IT verzahnt, sodass hohe Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik bestehen. „Unsere IT unterliegt derzeit zwar keinen dedizierten Compliance-Anforderungen von außen", erläutert Andreas Sternberg, IT Security Officer bei KWS, den Stellenwert des Sicherheitsniveaus im Unternehmen, „aber wir definieren unsere eigenen Standards und müssen Wege finden, sie international durchzusetzen und den Erfolg zu messen."

Ersatz für einen manuellen Prozess

Auf der menschlichen Ebene setzt KWS dabei erfolgreich auf Mitarbeiter, die die Kulturen vor Ort kennen und wissen, wie sie die Vorgaben aus der Unternehmenszentrale den jeweiligen Belegschaften und den Dienstleistern an den Standorten am besten nahebringen. Für die Lösung der technisch-organisatorischen Herausforderungen des globalen Security Level Managements fehlte dem Unternehmen allerdings noch ein im gleichen Maße ausgefeiltes Konzept. Vor allem den Prozess zur technischen Statusbestimmung im Bereich IT-Sicherheit wollte man effizienter gestalten. „Wir haben mit regelmäßig übermittelten, umfangreichen Excel-Listen gearbeitet, um den Überblick über den Bestand an IT-Systemen und die darauf installierte Software sowie über Sicherheitswerkzeuge, ausgerollte Patches, Viren-Patterns und andere wichtige Daten zu behalten", berichtet Sternberg und räumt ein: „Dieses Verfahren verschaffte uns jedoch nicht den unmittelbaren Zugriff auf die weltweiten Statusinformationen, den wir uns wünschten." Das Security-Team bei KWS sah die Gefahr, dass das bereits erkannte Delta zwischen der tatsächlichen Sicherheitssituation und den darüber verfügbaren Daten mit dem Wachstum des Unternehmens und seiner IT stetig zunehmen würde.

Arbeiten an in vitro Zuckerrüben Kultur unter dem Mikroskop
Quelle: KWS SAAT SE

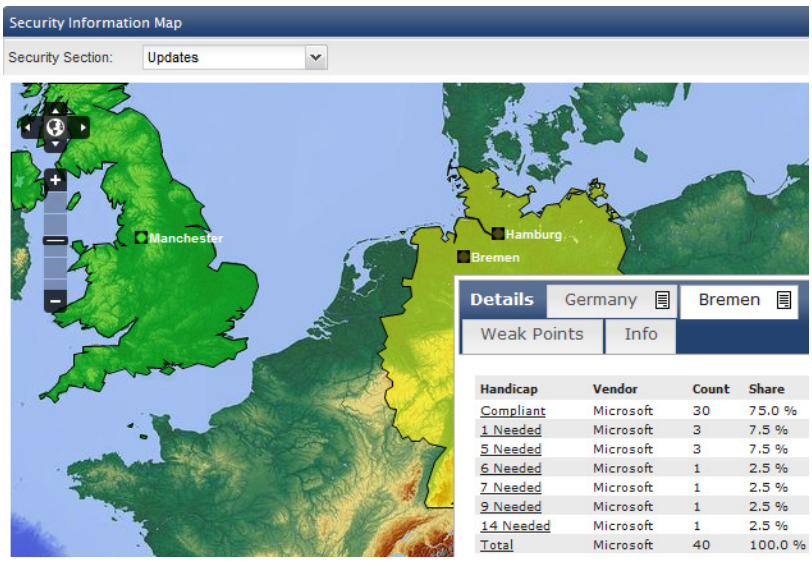
Statusinformationen auf Knopfdruck im Dashboard

KWS suchte vor diesem Hintergrund nach einer Lösung, die den Status der Sicherheitsinformationen aus den System-Management- und Security-Tools in einem Dashboard zusammenführen und jederzeit einen aktuellen Überblick liefern sollte – automatisiert und verzögerungsfrei auf Knopfdruck, also auch unabhängig von eventuellen Daten-Aufbereitungsprozessen in den unterschiedlichen Zeitzonen.

70 Länder auf einen Blick

Die Sicherheitsverantwortlichen entschieden sich für AMPEG Security Lighthouse als Monitoring-System. Das Produkt koppelt sich mit „Kollektoren" an die Sicherheitssysteme im Netzwerk an, erhebt und korreliert die dort gewonnenen Daten nahezu in Echtzeit und gleicht sie mit den unternehmensinternen Sicherheitsvorgaben ab. Die Ergebnisse bereitet das System unter anderem auf einer Weltkarte visuell auf und symbolisiert den Sicherheitsstand einzelner Lokationen anhand von Ampelfarben. Zeigen sich an einem Standort Unstimmigkeiten oder Fehler – nicht ausgerollte Viren-Patterns, fehlende Software Updates, ausgelassene Patches oder verspätete System-Rückmeldungen – kann der Operator den Problemen per Mausklick sofort auf den Grund gehen. Er kann zu jeder Zeit detailliertere Informationen vom Netzwerksegment hinab bis zu den einzelnen Systemen abrufen.

„Mit der Genauigkeit und Aktualität der Daten wuchs auch die Zielsicherheit unserer Reaktionen", erzählt Sternberg. Ergaben die vorher genutzten Tabellenauswertungen zum Beispiel, dass sich ein kritisches System längere Zeit nicht bei einem bestimmten System-Management-Tool gemeldet hatte und somit auch nicht auf dem neuesten Stand sein konnte, kontaktierte das Security-Team das zuständige Service Center. Dieses wiederum beauftragte den zuständigen Service-Provider damit, das Problem zu beheben. „Manchmal kam dann dabei heraus, dass das System geregelt abgeschaltet und ersetzt worden war oder dass es sich in der Zwischenzeit wieder gemeldet hatte", blickt Matthias Helmke, Head of Infrastructure bei KWS, zurück. Solche „False Positives" verursachten unnötige Aufwände, die Security Lighthouse nun zu vermeiden hilft.



KWS schaut auch bei der IT-Sicherheit genau hin: in der Security Information Map des Security Lighthouse wird der aktuelle Sicherheitsstatus in nahezu Echtzeit eingesehen

Bei KWS schloss man eine Vielzahl von System-Management- und IT-Security-Tools an das Produkt von AMPEG an – darunter den Virenschutz, das Patch- und Vulnerability-Management, das Inventory, die Verwaltung der Festplattenverschlüsselung, das Active-Directory und andere Quellen, um durch Korrelation auch Inkonsistenzen in den Meldungen der Systemwerkzeuge auswerten zu können. „All diese Sicherheitsbereiche können beim Security Lighthouse ‚out of the box' angekoppelt werden", erklärt Michael Hänsel, zuständiger Projektmanager bei AMPEG, „und nach der Ankopplung stehen sofort alle Auswertungen für die Analyse des Sicherheitsniveaus zur Verfügung."

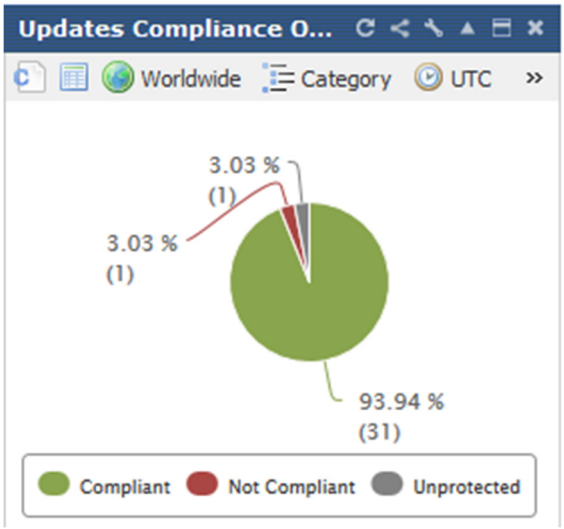
70 Länder auf einen Blick

Bei KWS dauerte die Installation für die Proof-of-Concept-Phase unter diesen Voraussetzungen nur drei Tage. In die anschließend ohne großen Aufwand implementierte produktive Lösung konnte das Security-Team die Konfigurationsdaten aus dem PoC-System direkt übernehmen.

„AMPEG reagiert überdies schnell auf Anfragen aller Art und setzt Kundenwünsche prompt um", ergänzt Sternberg die positive Erfahrung aus der Einführungsphase: „Die langen Wartezeiten, die wir von manchen anderen Dienstleistern kennen, gibt es hier nicht. Auswertungen, die uns fehlten, ergänzte der Anbieter innerhalb von nur zwei bis drei Wochen." Die gute Ausstattung mit Kollektoren einerseits und die Kommunikationsbereitschaft von AMPEG andererseits sind aus seiner Sicht auch im Hinblick auf die Flexibilität bei zukünftigen Investitionen wichtig: „Wenn wir beispielsweise einmal unser Virenschutz-System wechseln sollten, können wir sicher sein, dass sich Security Lighthouse problemlos und mit sehr geringem Migrationsaufwand auch ans neue Produkt koppelt."

Rollenmanagement als Anforderung

Eine wichtige Anforderung bei KWS war ein gut durchdachtes Rollenmanagement für den Zugriff auf die Status-Dashboards. Dieser Eintrag im Pflichtenheft resultierte aus der organisatorischen Besonderheit, dass die Behebung eventueller Mängel bei einzelnen Systemen im Verantwortungsbereich unterschiedlicher KWS Service Center und letztlich in den Händen verschiedener Dienstleister liegt. Security Lighthouse bietet eine entsprechende Zugriffssteuerung: „Jeder Service-Provider bekommt aufgrund seiner Rollendefinition genau den Bereich zu sehen, für den er zuständig ist", beschreibt Sternberg die neue Situation, „und wir können sicher sein, dass er über seine jeweils aktuellen Tasks auch tatsächlich informiert ist."



Das weltweite Sicherheitsniveau auf einen Blick

AMPEG Security Lighthouse macht sich auch bei der Kommunikation mit anderen Abteilungen im Unternehmen positiv bemerkbar. Das Management etwa schätzt die gelungene Visualisierung der Sicherheitslage. Matthias Helmke weist auf einen weiteren Punkt hin: „Wenn Wirtschaftsprüfer einen Blick auf unser Sicherheitsniveau werfen wollen, können wir dieses sofort und in bemerkenswert anschaulicher Form anbieten. Auch Reports lassen sich schnell und zielgruppengerecht erstellen. All dies erleichtert Audits erheblich."

70 Länder auf einen Blick

„Wir sehen, wo wir stehen, können eventuellen Detailfragen unmittelbar auf den Grund gehen und schnell Abhilfe schaffen“, fasst Andreas Sternberg das Resultat der Produkteinführung zusammen. Die Qualitätssicherung in der IT-Sicherheit erfolgt nun zeitnah und auf der Basis stets aktueller Informationen.

Die Lösung wurde realisiert bei:

KWS SAAT SE
Grimsehlstrasse 31
37555 Einbeck, Germany
http://www.kws.com/

Mit Unterstützung von:

AMPEG GmbH
Stavendamm 22
28195 Bremen, Germany
https://www.ampeg.de/