Münster Osnabrück International Airport überwacht seine Informationssicherheit mit dem IBM Tivoli Compliance Insight Manager.

Überblick

- ***Die Aufgabe***
  Internationale Richtlinien und Gesetze erforderten stärkere Anstrengungen in Bezug auf Informationssicherheit im Unternehmen. Ein umfangreiches rechtliches Rahmenwerk muß künftig beachtet werden, das den Umgang mit sensiblen Daten und Logfiles regelt.
- ***Die Lösung***
  Einsatz des IBM Tivoli Compliance Insight Managers zur Kontrolle des IT-Netzwerkes in Echtzeit.
- ***Die Vorteile***
  Automatisch aufspüren, analysieren und bewerten von Aktionen im Netz. Überprüfung der Benutzer-Aktivitäten in Echtzeit.

Flughafen im Aufwind

Der Münster Osnabrück International Airport (FMO) verbindet Nordrhein-Westfalen und Niedersachsen mit den großen Geschäftszentren in Europa. Mehr als 1,6 Millionen Passagiere pro Jahr nutzen mittlerweile die internationalen Anbindungen des Flughafens. In den vergangenen Jahren verzeichnete der Airport ein stetiges Wachstum und reagierte auf die wachsende Zahl von Flugbewegungen mit dem Ausbau neuer Terminals und einer für 2009 geplanten Verlängerung der Start- und Landebahn.

Dank einer attraktiven Mischung aus Linienflügen, Touristik- und Billigflugverkehr steigen auch die Passagierzahlen des FMO stetig an. Insbesondere im anspruchsvollen Geschäftsreisesegment wurden 2007 überproportionale Zuwächse erreicht.

Mit den Umsatz- und Passagierzahlen wuchsen auch die Ansprüche an Sicherheit und Integrität der IT-Infrastruktur. Deshalb setzt der Airport seit Herbst 2005 auf den Tivoli Compliance Insight Manager von IBM.

Compliance und Auditing

Internationale Richtlinien und Gesetze erfordern von IT-Administratoren immer stärkere Anstrengungen in Bezug auf die Informationssicherheit im Unternehmen. Auch die IT-Abteilung des Münster Osnabrück International Airport hat ein umfangreiches rechtliches Rahmenwerk zu beachten, das den Umgang mit sensiblen Daten und Logfiles regelt. „Auditing ist zwingender Bestandteil eines umfassenden Risk-Managements und für uns daher unvermeidbar“, erklärt Francisco Rodríguez, CIO des Flughafens.

> *„Nachdem wir die Lösung von IBM gesehen hatten war uns sofort klar, dass es auf dem Markt kaum vergleichbare Produkte gibt. Das Preis-Leistungs-Verhältnis und die Handhabung des Produktes waren für uns von Anfang an sehr überzeugend.“*
>
> *– Francisco Rodríguez, Leiter IT- und Kommunikationsmanagement (CIO)*

Bislang konnten die Administratoren des Airports nur punktuell überprüfen, ob die Sicherheitsrichtlinien im Unternehmen tatsächlich eingehalten wurden. Eine vollständige Kontrolle der Informationssicherheit war dadurch nicht möglich. Insbesondere das größte Sicherheitsrisiko für den Flughafen – dass strategische Dokumente oder vertrauliche Informationen in die Hände Unbefugter gelangen – konnte ohne umfassendes Auditing nicht kontrolliert werden.

Daher ist die Überwachung bedrohlicher Aktivitäten innerhalb des Netzwerkes für das IT-Management ebenso wichtig wie die Abwehr von Risiken, die das System von außen bedrohen.

Umfassendes Sicherheitsmanagement mit IBM Tivoli

Für den CIO kam dazu schon nach kurzer Marktsondierung nur ein Produkt in Frage:

„Nachdem wir die Lösung von IBM gesehen hatten war uns sofort klar, dass es auf dem Markt kaum vergleichbare Produkte gibt", resümiert Francisco Rodríguez. Auch der Funktionsumfang überzeugte: „Nach mehreren Gesprächen mit den IBM-Fachleuten und nach Vorführungen des in Frage kommenden Produktes war uns klar, dass InSight genau dem entspricht, was wir uns vorstellen". Die umfassende Funktionalität, das Preis-Leistungsverhältnis und die Handhabung des Systems überzeugten IT-Abteilung und Management gleichermaßen.

Beim Rollout entschied sich das Unternehmen bewusst gegen einen ausführlichen Testlauf: „Wir waren überzeugt, dass wir diese Phase überspringen könnten. Natürlich sind einige Vorbereitungen nötig – anhand der von IBM gezeigten Referenzen und des am FMO vorhandenen Know-Hows haben wir uns jedoch für eine sehr kurze (5 Tage) Probephase entschieden. Dies hat sich am Ende auch als sinnvoll und richtig erwiesen", erklärt Rodríguez.

Weitreichende Kontrolle und verbesserte Transparenz

IBM Tivoli Compliance Insight Manager verfügt über Funktionen, um verdächtige Aktionen von Benutzern innerhalb des Netzwerkes automatisch aufspüren, analysieren und bewerten zu können. Das System stellt den einzelnen Anwender in den Mittelpunkt und überprüft in Echtzeit die Aktivitäten von Benutzern sowie die daraus resultierenden Auswirkungen auf geschäftskritische Unternehmensprozesse: „Die Lösung ermöglicht uns einen genauen Nachweis darüber, wer zu welchem Zeitpunkt auf bestimmte Ressourcen zugegriffen hat.

Nur so können wir im Falle eines Sicherheitsverstoßes eine schnelle Aufklärung schaffen und die Einhaltung unserer Richtlinien überprüfen", so Rodríguez.

Ein weiterer Pluspunkt für den Airport ist die verbesserte Transparenz von IT-Administration und Informationssicherheit: dank umfangreicher Berichtsfunktionen können Sicherheitsprozesse und Systemintegrität nun übersichtlich für das Management dargestellt werden. Die IT stellt für die Unternehmensführung somit keine undurchschaubare „Black Box" mehr dar, sondern kann aktiv mit den Prozessen und strategischen Zielsetzungen des Unternehmens koordiniert werden.

Ausblick: Weiterer Ausbau des Risk Managements

Nach mehreren Monaten im Produktiveinsatz hat Tivoli Compliance Insight Manager den CIO voll überzeugt: ein weiterer Ausbau des Security Information Managements ist fest eingeplant. Rodríguez will weitere IT-Syteme in den Tivoli Compliance Insight Manager integrieren. „Dadurch wird die IT-Sicherheit schrittweise erhöht ohne die Prozesse am Flughafen durch schnelle Änderungen zu stören."

Fakten zu IBM Tivoli Compliance Insight Manager

- *Umfangreiche Funktionen für Auditing und Compliance*
- *Features für Monitoring, Analyse und die Erstellung von Berichten zur Überwachung der Systemintegrität*
- *Nahtlose Integration mit einer Vielzahl von Sicherheitssystemen wie Firewalls, Antivirus- und Intrusion Detection-Systemen*
- *Überwachung der Aktivitäten von Anwendern und „Trusted Users"*
- *Unterstützung standardisierter sowie maßgeschneiderter Sicherheitsrichtlinien*
- *Automatisch generierte Berichte für ständigen Überblick über den aktuellen Sicherheitsstatus*
- *Für Netzwerkumgebungen mit heterogenen Plattformen geeignet*

IBM Deutschland GmbH
70548 Stuttgart
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

IBM Form GK12-4388-00 (09/2008)