Flughafen Köln Bonn

Kundenprofil
- Köln Bonn Airport ist mit mehr als 9 Millionen Passagieren und über 750.000 Tonnen Luftfracht einer der größten Verkehrsflughäfen in Deutschland. In seinem Einzugsgebiet, einem der größten in Europa, leben 17 Millionen Menschen. Zahlreiche Messen und Kongresse sowie zahlreiche multinationale Unternehmen verleihen der Region den Status eines wirtschaftlichen Kraftzentrums Deutschlands.

Branche
- Luftfahrt

IT-Umgebung
- Mehr als 1.800 Angestellte

Herausforderung
- Heterogene IT-Landschaft
- Hohe Anforderungen an Compliance und IT-Sicherheit
- Rechteverwaltung und Zugriffskontrollen
- Aggregation und Korrelationen bestehender Daten

Lösungen von McAfee
- Enterprise Security Manager
- Advanced Correlation Engine
- Enterprise Log Manager
- Vulnerability Manager

Ergebnisse
- Erweiterte Optionen bei Security Incident Response- und Forensik-Verfahren
- Ergebnisbezogene Analysen
- Verbesserte Möglichkeiten bei Audit und Compliance Aufgaben
- Automatisches und zielgerichtetes Behandeln von Bedrohungen und Störungen

Flughafen Köln Bonn optimiert seine IT-Sicherheit mithilfe der SIEM-Lösung von McAfee

Für einen internationalen Flughafen gelten strenge Anforderungen. Pünktlichkeit und Sicherheit – sowohl beim Transport von Menschen als auch Gütern – stehen an erster Stelle. Höchste Ansprüche werden auch an die IT gestellt: Sie muss ausfallsicher sein und für einen reibungslosen Ablauf sorgen. Damit dies gewährleistet ist, müssen die Verantwortlichen Netzwerk, Server, Datenbanken und Steuerungssysteme wirkungsvoll, und aus Compliance-Gründen auch nachweislich, vor Angriffen schützen. Hierfür vertraut der Geschäftsbereich Informationstechnologie des Köln Bonn Airport auf Sicherheitslösungen von McAfee®.

Der Köln Bonn Airport zählt mit mehr als neun Millionen Passagieren und über 750.000 Tonnen Luftfracht zu einem der größten Verkehrsflughäfen Deutschlands. In seinem Einzugsgebiet leben 17 Millionen Menschen. Durch zahlreiche Messen, Kongresse und niedergelassene multinationale Unternehmen ist die Region ein wirtschaftliches Kraftzentrum in Deutschland und sorgt so für ein hohes Aufkommen an Geschäftsreisenden. Anders als viele andere Flughäfen, die bereits Engpässe haben, verfügt Köln Bonn über eine beachtliche Reserve an Start- und Landebahnkapazität. Fluggesellschaften können so ihre Slots für einen optimalen Flugplan frei wählen. Das moderne Start- und Landebahnsystem, dessen längste Bahn 3.815 m misst, ermöglicht darüber hinaus Nonstop-Flüge vollbeladener und vollbetankter Jets in alle Welt – nur ein Grund, weshalb beispielsweise UPS seinen Europa-Hub am Köln Bonn Airport betreibt und auch FedEx sein Drehkreuz für Zentral- und Westeuropa am Standort eingerichtet hat.

Sicherheit und Compliance in einer heterogenen IT-Umgebung

Ein Unternehmen dieser Komplexität und mit den besonderen Anforderungen eines Flughafens muss ganz besonders darauf achten, dass in Bezug auf die IT-Sicherheit und IT-Compliance alle Vorgaben erfüllt sind. Im Falle des Köln Bonn Airport war der Nachweis der IT-Sicherheit nicht immer einfach – die IT-Infrastruktur war wie in vielen großen Netzwerken über die Jahre heterogen gewachsen, unterschiedliche Systemarchitekturen mussten miteinander in Einklang gebracht und auch zentral ausgewertet werden können.

Bis vor kurzem brachte dies aufwändige dezentrale Analysen an unterschiedlichen Management-Konsolen mit sich – was in den Augen von René Koch, IT Security Manager am Köln Bonn Airport, unverhältnismäßig viele Ressourcen band. Um eine Risikoanalyse erstellen und Sicherheitsvorfälle aufarbeiten zu können, muss eine IT-Organisation Informationen über Ereignisse im Zusammenhang mit der Rechteverwaltung, den Zugriffskontrollen sowie zu Bedrohungen und Verwundbarkeiten einfach, schnell und verlässlich nachvollziehen können.

René Koch dazu: „Diese Informationen wurden bei uns dezentral generiert und unterschiedlich zeitlich fortgeschrieben. Korrelationen zu bereits bestehenden Information waren nicht möglich." Die IT musste potentielle Schwachstellen zunächst identifizieren und den betroffenen Informationssystemen manuell zuordnen. Eine Aussage zum Grad der Verwundbarkeit war nicht immer kurzfristig möglich, so dass die Einhaltung von Vorgaben der IT-Sicherheit und IT-Compliance nicht immer zweifelsfrei gegeben war. Eine neue Lösung sollte diese Situation verbessern.

Integriertes Steuercockpit für die IT-Sicherheit

Diese neue Lösung musste vor allem zwei Dinge erfüllen: die Transparenz erhöhen und die IT-Landschaft zentral steuerbar machen. Die Security Spezialisten um René Koch wollten den Status der IT-Sicherheit in nahezu Echtzeit bestimmen können. Auch sollten alle Informationen die IT-Sicherheit betreffend über ein integriertes „Steuerungscockpit" teilweise automatisiert kontrolliert, beeinflusst und dokumentiert werden können.

Protokollierte Informationen mussten dabei vollständig, fälschungssicher und im Nachhinein unveränderbar sein, um die Beweiskraft der Berichte sicher zu stellen. Außerdem musste die Lösung in der Lage sein, die heterogenen Informationen für ein Gesamtlagebild zu normalisieren und es dem Team ermöglichen, sehr einfach einzelne priorisierte Vorgänge aus der Menge aller Ereignisse filtern zu können. Auch in Bezug auf die Zugriffsrechte sollte die Lösung eine granulare Steuerung ermöglichen.

Der Köln Bonn Airport entschied sich letztlich für die Security Information und Event Management (SIEM)-Lösung „McAfee Enterprise Security Manager". Diese erfüllte nicht nur die Vorgaben hinsichtlich des Reportings, sie bietet den Security Spezialisten auch die Möglichkeit, zeitnah und fundiert auf Sicherheitsvorfälle reagieren zu können. Weil das System eine risikobasierte Priorisierung von Maßnahmen erlaubt, können Aufgaben zur Schwachstellen- und Bedrohungsbekämpfung intelligent gesteuert und nachgehalten werden.

SIEM-Individualiserung für passgenaue Sicherheit

Heute kann der Geschäftsbereich Informationstechnologie des Köln Bonn Airport relevante Ereignisse produktunabhängig und angepasst an die jeweiligen Bedürfnisse der verschiedenen Fachteams betrachten. „Das spart uns nicht nur im laufenden Betrieb Zeit – auch das Training können wir nun auf eine Lösung fokussieren", so René Koch. "Unsere Analysen liefern übergreifende Ergebnisse, losgelöst von den architekturabhängigen Ereignismeldungen der jeweiligen Competence Center. Durch die Integrierung mit McAfee Vulnerability Manager und McAfee ePolicy Orchestrator® (McAfee ePO™), sind wir nun in der Lage, Bedrohungen und Störungen unserer IT-Landschaft zielgerichtet zu behandeln."

So ergänzen beispielsweise die Penetrationstests um eine dauerhafte Schwachstellenanalyse potentieller Gefahren und Verwundbarkeiten. Dabei werden die Ereignisse und Informationen aktiver und passiver Komponenten permanent ausgewertet und in einer integrierten Sicht zentral aufbereitet. Abweichungen und Verstöße von den definierten Regeln lösen automatisch Benachrichtigungen aus. So sind die Administratoren stets über mögliche sicherheitsrelevante Vorfälle informiert.

Die Security Spezialisten begannen zudem sofort damit, eigene Messkriterien aus den Analysen und Störmeldungen abzuleiten und im SIEM-System zu hinterlegen – beispielsweise in Bezug auf Veränderungen des Datenvolumens, welches in der Netzlandschaft verarbeitet wird. Werden Messwerte auffällig, erhalten die verantwortlichen Systemverantwortlichen automatisiert Benachrichtigungen. Auch die zahlreichen Regelwerke innerhalb der McAfee Correlation Engine können vom Team individuell angepasst werden. „Die hierdurch geschaffene Möglichkeit des integrierten Alarmierungs- und Berichtswesens bietet einen Vorteil gegenüber anderen Lösungen am Markt", erklärt René Koch.

Eine übergreifende Lösung für das Management von Sicherheitsinformationen und Events vereinfacht die Steuerung komplexer IT-Infrastrukturen erheblich. Je besser integriert und intelligenter dabei die Lösung, desto mehr Kontrolle bietet sie den Verantwortlichen. Als Teil des McAfee „Security Connected"-Ansatzes integriert sich der McAfee Enterprise Security Manager nahtlos in McAfee ePO, McAfee Risk Advisor sowie in McAfee Global Threat Intelligence und liefert den notwendigen Kontext für eine autonome und adaptive Verwaltung von Sicherheitsrisiken.

„Die Sicherheit hat am Flughafen oberste Priorität – und McAfee ist in Bezug darauf ein wichtiger Partner für uns. Vor allem helfen uns die Sicherheitslösungen dabei, Transparenz zu schaffen und unsere IT nachweislich den Vorgaben entsprechend zu steuern. Dank des zentralen Managements können wir unsere Ressourcen nun äußerst gezielt einsetzen."

— René Koch
IT Security Manager
Köln Bonn Airport

McAfee
An Intel Company

McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de

61209cs_airport-cologne_0714