



[PR]

Thementag „Security Operations“ in Hannover

Next Generation SOC – So geht Security Management heute

Pressekontakt

Diana Schatka

Unternehmenskommunikation

Tel. 0511 /977-4011

Fax 0511/977-4100

d.schatka@airitsystems.de

AirITSystems GmbH
Benkendorffstraße 6
30855 Langenhagen
www.airitsystems.de

Thementag „Security Operations“ in Hannover

Next Generation SOC – So geht Security Management heute

Die IT Security Branche in Deutschland ist im Aufwind. Hacker-Angriffe, beispielsweise durch Ransomware, sind inzwischen immer häufiger medial präsent. Nicht zuletzt deshalb hat sich inzwischen auch in kleinen und mittelständischen Unternehmen ein Bewusstsein für die Bedeutung von IT-Sicherheit entwickelt. Viele IT-Abteilungen stehen jedoch vor der gleichen Herausforderung: Die Heterogenität der vorhandenen Lösungen verhindert einen umfassenden Blick auf die potenziellen Angriffsflächen. Der Thementag „Security Operations“ von AirITSystems stellte am 9. August 2017 am Flughafen Hannover deshalb das Next Generation SOC ins Zentrum der Veranstaltung. Auf zwei parallel verlaufenden „Tracks“ brachten die Referenten von AirITSystems, Skybox Security und LogRhythm dem Publikum aus IT-Spezialisten aus Unternehmen und Behörden die Grundpfeiler eines modernen Security Operations Center (SOC) näher. Der „Technik Track“ zielte vor allem auf die technischen Bausteine eines SOC, wie Risk- und Vulnerability Management bzw. SIEM ab. Im „Management Track“ stand der organisatorische Aufbau im Vordergrund.

Ein SOC macht heute mehr Sinn denn je

Tim Cappelmann, Leiter Managed Services bei AirITSystems, betonte zunächst die Aktualität des Themas SOC: „Cyber-Vorfälle stehen auf der Liste von Unternehmensrisiken ganz oben – Tendenz steigend.“ IT-Entscheider fragten sich jedoch, wie sie ein SOC wirtschaftlich und effektiv umsetzen können. Tim Cappelmann plädiert hier für die Schaffung einer eigenen Organisationseinheit „Security Operations Center“. „Ein SOC sollte sich gezielt auf wenige Aufgaben mit einem hohen Qualitätsanspruch fokussieren, getreu dem Motto: do a few things well“, betont Cappelmann. Die Kernaufgabe des Teams ist

PR-Mitteilung

AirITSystems GmbH

9. August 2017
Seite 3 von 4
Ca. 3100 Zeichen

es dabei, CERT Meldungen zu verarbeiten, Incidents zu bearbeiten und die Risikolage zu bewerten. Um eine Ende zu Ende Sicht auf die Sicherheitslücken eines Unternehmens zu erlangen, ist der Einsatz eines Risk-Management-Tools unerlässlich. Neben dem SIEM der wichtigste Baustein auf technischer Seite: „Ein Unternehmen hat heute keine Möglichkeit mehr, ein SOC ohne SIEM zu betreiben“, so Cappelmann weiter.

Den Überblick behalten

Jörg von der Heydt, Channel Director DACH bei Skybox Security, stellte zu Beginn seines Vortrags den Zuhörern die Frage: „Wissen Sie, was Sie alles in Ihrem Netzwerk haben?“ Denn das sei die Voraussetzung dafür, überhaupt für IT-Sicherheit sorgen zu können. „Ich muss wissen, was ich habe, sonst kann ich nicht wissen, was ich schütze“, so von der Heydt weiter. Ein obligatorischer Bestandteil eines SOCs sollte deshalb ein Risk-Management-Tool sein, das alle Netzwerkkomponenten und deren Korrelation erfasst. Ebenso unerlässlich ist ein SIEM. Richard Quignon, Sales Engineer bei LogRhythm, wies in seiner Session auf Faktoren hin, die eine schnelle Erkennung von Bedrohungen erschweren: Alarmmüdigkeit, Analysen auf mehreren UIs oder die fehlende Automatisierung sind nur einige davon. „Genau das wollen wir vermeiden und alle Informationen auf einem Bildschirm bündeln“, erklärt Quignon. Ein leistungsstarkes SIEM bietet dem Nutzer einen schnellen Überblick über aktuelle Bedrohungen.

Mit den Thementagen verfolgt AirITSystems das Ziel, IT-Verantwortliche in Unternehmen und Behörden zeitlich verdichtet über aktuelle Trends und Notwendigkeiten der IT-Security-Welt zu informieren. Die Veranstaltungsreihe fand in Frankfurt und Hannover statt, um lange Reisewege und hohe Zeitaufwände zu minimieren.

PR-Mitteilung

AirITSystems GmbH

9. August 2017
Seite 4 von 4
Ca. 3100 Zeichen

Über die AirITSystems GmbH

AirITSystems wurde 2001 als gemeinsame Tochter der beiden Flughäfen Frankfurt und Hannover gegründet, um hier hochkarätige Kompetenzen zu bündeln. Jede IT- und Kommunikations-Leistung, die am Flughafen Hannover erbracht wird, ist mit AirIT geplant, entwickelt und realisiert. Im Bereich Sicherheit setzt das Unternehmen auf eine ganzheitliche Betrachtung und sorgt für Gebäudesicherheit, Informationssicherheit und IT-Sicherheit. AirIT-Lösungen sind für alle Unternehmensgrößen und Branchen skalierbar - sie zeichnen sich durch ein Maximum an Stabilität, Sicherheit und Innovation aus.

Pressekontakt

riske & jorns

Nadine Riske

FON 0531 390 76 75 1

MOBIL 0170 321 51 61

nadine.riske@riske-jorns.de

AirITSystems GmbH

Diana Schatka

FON 0511 977 40 11

D.Schatka@airitsystems.de