AirIT
AirITSystems

Final Call!
AirITSystems auf der secIT
6.–7. März 2018 in Hannover

Aktuelle Informationen der AirITSystems

März 2018

NEWS

Günther Gräf *Eric Engelhardt* *Dr. Wolfgang Pelzer*

Liebe Leserinnen und Leser,

effiziente IT-Security besitzt heute für erfolgreiche Unternehmen oberste Priorität. Das Risk-and-Security-Management-Tool von Skybox Security als wichtigstes Werkzeug eines Security Operations Center prüft jede Modifikation an einem Baustein des Kommunikationsnetzwerks hinsichtlich ihrer Auswirkung auf alle anderen Komponenten. So lassen sich potenzielle Sicherheitslücken schließen, lange bevor sie zur Angriffsfläche werden. Wie Sie von einer proaktiven Sicherheitsarchitektur profitieren können, auf deren Transparenz und Frühwarnkapazität auch der Hannover Airport setzt, erfahren Sie auf Seite 4.

Vom 6. bis 7. März findet im Hannover Congress Centrum die erste secIT statt. Auf der neuen Messe für Security-Anbieter und -Anwender geht es um die aktuellen Trends in Sachen IT-Sicherheit. Natürlich sind wir mit einem eigenen Stand vertreten und freuen uns auf Ihren Besuch!

Zum Schluss eine News in eigener Sache: AirITSystems hat sein Produktportfolio mit der Übernahme des Unternehmens Topsonic um die Bereiche Fluglärm- und Flugspurüberwachung ergänzt und ist damit weiter auf Wachstumskurs.

Viel Freude bei der Lektüre!

Inhalt

EU-Datenschutzgrundverordnung war Topthema der Messe

Die it-sa, Europas führende Messe rund um das Thema IT-Sicherheit, wächst weiter: Fast 13.000 Fachbesucher und 630 Aussteller waren vom 10. bis 12. Oktober vor Ort in Nürnberg. AirITSystems informierte die Messebesucher gemeinsam mit dem Partner Skybox Security schwerpunktmäßig zum Security Operations Center (SOC). Das Thema stieß auf reges Interesse.

„Es waren drei spannende Tage mit qualitativ hochwertigen Kontakten und Gesprächen", stellt Artur Michalowitz, Bereichsleiter für Netzwerktechnologien bei AirITSystems, fest. „Wir merken deutlich, dass durch die EU-Datenschutzgrundverordnung das Interesse der Unternehmen an Security-Themen weiter steigt." Tim Cappelmann, Leiter Managed Service, ergänzt: „Die IT-Verantwortlichen fragen vermehrt Risikomanagement-Systeme nach. Das verdeutlicht: Der Trend geht weg vom Vulnerability-Scanner. Unternehmen möchten ihre Angriffsflächen kennen, bevor Angreifer sie ausnutzen." Ein Risk- und Security-Management-Tool arbeitet proaktiv. Der Vorteil gegenüber einem Vulnerability-Scanner liegt darin, dass das System jeden Change im Vorfeld analysiert. Ein Report zeigt auf, welche Auswirkungen etwa Änderungen der Firewall-Einstellungen auf das gesamte Netzwerk haben und wo Sicherheitslücken entstehen können.

SIEM und Risikomanagement-Plattform

Im Jahr 2017 präsentierte AirITSystems vor allem ein Thema: Das SOC der nächsten Generation. Die Experten am Stand gaben Auskunft über die wichtigsten Kernthemen eines zukunftsfähigen SOCs. Sie stellten relevante Tools wie ein SIEM oder eine Risk-and-Security-Management-Plattform vor und gaben Tipps zum organisatorischen Aufbau des SOC. Von besonderem Interesse war für die Standbesucher, wie Unternehmen ein SOC partnerschaftlich mit AirITSystems als Managed Service Partner betreiben können. AirITSystems bietet hier flexible Unterstützung und passgenaue Lösungen, maßgeschneidert auf die Organisation des Kunden. Durch eine Risk-and-Security-Management-Plattform gewinnt ein SOC an Effizienz und wird auch für kleine und mittelständische Unternehmen attraktiv.

Treffpunkt der Branche

Die it-sa gilt weltweit als eine der wichtigsten Fachmessen zur IT-Sicherheit. Der Anteil der ausländischen Fachbesucher lag bei 53 Prozent. Unter den Ausstellern gab es Beteiligungen aus 24 Ländern. Erstmals begleitete ein Kongressprogramm die Messe. Bei Congress@it-sa stand vor allem die neue EU-Datenschutzgrundverordnung im Fokus. Auf vier Vortragsbühnen und bei 320 Vorträgen in offenen Foren bot die it-sa reichlich Informationen über die aktuellen Trends der IT Security.

Ihr Kontakt:
Diana Schatka
Tel.: +49 511 977-4011

secIT 2018

Neue Messe rund um das Thema IT Security

Vom 6. bis 7. März 2018 öffnet im Hannover Congress Centrum die secIT zum ersten Mal ihre Pforten. Die neue Veranstaltung richtet sich in erster Linie an Security-Anwender und -Anbieter. Im Mittelpunkt stehen die neuesten Trends, Methoden, Lösungsansätze sowie aktuelle Softwarelösungen und Produkte aus dem Bereich IT-Sicherheit. AirIT-Systems ist mit einem eigenen Stand vor Ort.

Auf rund 2.000 Quadratmetern stellen sich die wichtigsten Unternehmen der IT-Sicherheitsbranche vor. In mehr als 25 Vorträgen bekommen die Besucher Informationen zu den Schwerpunktthemen Digitalisierung, Internet of Things, Industrie 4.0, EU-Datenschutzgrundverordnung und Cybersecurity. Auch Tim Cappelmann, Leiter Managed Services bei AirITSystems, wird als Sprecher auftreten. Am 6. März gibt er von 9:20 Uhr bis 9:40 Uhr Einblicke ins Thema „Security Operations Center (SOC). Aufbau, Betrieb, Referenzprojekt".
Informieren Sie sich über die aktuellen Trends in Sachen IT Security und besuchen Sie unsere Experten am Stand Nr. 4. Wir vergeben 30 Freitickets für die secIT. Melden Sie sich einfach telefonisch bei Diana Schatka (siehe Infobox).

Ihr Kontakt:
Diana Schatka
Tel.: +49 511 977-4011

AWARO®

AWARO mit integriertem 3D-CAD-Viewer

Frankfurt, im Februar 2018. – Der Geschäftsbereich AWARO Collaboration Solutions der AirITSystems hat zur Unterstützung der Anwender des Projektraums AWARO in BIM-Projekten einen leistungsstarken 3D CAD-Viewer integriert.

Mit dem 3D-CAD-Viewer können 3D-Modelle direkt im Browser auf dem PC oder auf einem mobilen Gerät betrachtet werden.

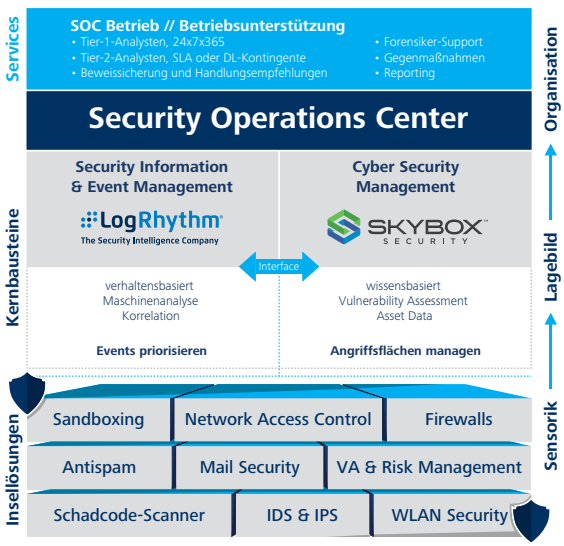
Damit kann der Anwender ohne Installation zusätzlicher Software IFC 3D-Modelle direkt im Browser auf dem PC oder einem mobilen Gerät betrachten. Darüber hinaus unterstützt der Viewer aber auch zahlreiche 2D-CAD, Office- und Bildformate. Durch die Möglichkeit, auch mehrere Teilmodelle in einer Gesamtansicht zu zeigen, ist der Viewer ein hilfreicher Baustein in Koordinationsbesprechungen, um beispielsweise Schnittstellenprobleme zu diskutieren.
Da die Oberfläche konform zu Microsoft Office gestaltet ist, ist eine Bedienung einfach und intuitiv möglich. Durch ein serverseitiges Rendering der Geometrien und die Nutzung von HTML-5-Technologien ist die Visualisierung, aber auch das Drehen oder Vergrößern selbst bei komplexen 3D-Modellen leistungsfähig und flüssig. Die einzelnen Bauteile können ausgeblendet, freigestellt oder vermessen werden. Ist eine aussagekräftige Ansicht des Modells gefunden, so lässt sich diese abspeichern und wieder aufrufen.
AWARO vernetzt alle am Bauprojekt Beteiligten wie Bauherr, Architekt, Fachplaner und ausführende Unternehmen über eine zentrale Kooperationsplattform, die die Anwender über Webbrowser ohne Softwareinstallation nutzen. So können die Nutzer überall auf die Informationen zugreifen, für die sie autorisiert sind. Durch Qualitätsvorgaben im Dokumentenmanagement und systematische Aufgabenverfolgung bietet AWARO optimale Voraussetzungen für die Projektsteuerung.

Ihr Kontakt:
Marc Beißler
Tel.: +49 69 430536-22

Success Story

Maximale Effizienz im Security Operations Center (SOC)

IT-Sicherheit ist für jedes Unternehmen ein Thema mit höchster Priorität. Um seine IT-Landschaft optimal abzusichern, setzt der Hannover Airport auf die AirITSystems GmbH. Sie betreibt ein Security Operations Center für den Flughafen, das den reibungslosen Betrieb aller IT-Gewerke gewährleistet. Wichtigstes Werkzeug: das Risk-and-Security-Management-Tool von Skybox Security.



Sicherheit managen - Security Operation Center (SOC) by AirITSystems

Die Herausforderung: Sicherheit für eine kritische Infrastruktur

Der Hannover Airport ist der größte Flughafen Niedersachsens. Rund 5,8 Millionen Fluggäste pro Jahr nutzen die Möglichkeit, von Hannover aus in den Urlaub zu fliegen oder eine Geschäftsreise anzutreten. Der Flugbetrieb findet an 24 Stunden pro Tag statt. Für die Region Hannover und Niedersachsen ist der Airport mit seinen 8.000 Beschäftigten ein wichtiger Wirtschaftsfaktor. Eine funktionierende und absolut sichere Informations- und Kommunikationstechnik ist für einen so wichtigen Knotenpunkt wie den Flughafen unerlässlich.

AirITSystems ist langjähriger Partner des Flughafens, wenn es um die Sicherheit und den Betrieb der IT-Infrastruktur geht. Der IT-Sicherheitsspezialist betreibt unter anderem das Security Operating des Airports. Das bewährte Security Information and Event Management (SIEM) des Flughafens sollte nun durch ein Risk-and-Security-Management-System von Skybox Security ergänzt werden.

Die Vorteile: Angriffsflächen erkennen, bevor sie entstehen

Für die Spezialisten des SOC ist das Tool von Skybox Security eine echte Bereicherung. Es bildet die komplexe Kommunikationsmatrix des Airports vollumfänglich ab und setzt sämtliche IT-Komponenten in Kontext. Schwachstellen sind so bereits sichtbar, bevor sie tatsächlich angreifbar werden. Für die IT Security bedeutet das effizienteres Arbeiten. Jede noch so kleine Änderung, etwa an den Firewall-Regelwerken, prüft das System auf deren Auswirkung auf die übrigen Netzwerkkomponenten. Durch die Änderung entstandene neue potenzielle Angriffsflächen sind nun auf einen Blick ersichtlich.

„Das Netzwerk ist eine der wichtigsten Lebensadern des Airports. Unsere Anforderungen an IT-Sicherheit und Verfügbarkeit sind deshalb sehr hoch. Die effiziente IT-Modellierung von Skybox Security im SOC von AirITSystems hat uns wirklich beeindruckt."
Jan Oodes, Corporate Infomanagement des Hannover Airports

Unser Angebot: maßgeschneidertes Security Operating

Ein Security Operations Center (SOC) ermöglicht einen ganzheitlichen Blick auf die aktuelle Bedrohungslage. Doch nicht jedes Unternehmen ist in der Lage, ein eigenes SOC-Team zu stellen. Sind die Kapazitäten beziehungsweise Kompetenzen, die ein SOC fordert, nicht vorhanden, lassen sich Teilbereiche gut als Managed Services umsetzen. AirITSystems kann auf weitreichende Erfahrungen in diesem Umfeld zurückgreifen. Die Services erbringt das Unternehmen für alle Marktsegmente. Der Leistungsumfang ist entsprechend den individuellen Anforderungen und der Unternehmensgröße skalierbar. Dabei steht es Unternehmen frei, einzelne Bereiche wie das Firewall Operating oder auch das gesamte Security Operating als Managed Services betreiben zu lassen. Das Risk-and-Security-Management-Tool von Skybox Security ist in Verbindung mit einem SIEM das wichtigste Standbein eines von AirITSystems betriebenen SOCs.

Ihr Kontakt:
Tim Cappelmann
Tel.: +49 511 977-4071

Agieren statt reagieren

Die neue EU-Datenschutzgrundverordnung (EU-DSGVO) tritt im Mai 2018 in Kraft. Inzwischen ist sie im Bewusstsein der IT-Sicherheitsverantwortlichen angekommen und ein vieldiskutiertes Thema. Wer pokert und hofft, dass bestehende Systeme schon ausreichen werden, bewegt sich auf dünnem Eis.

Eine der Neuerungen der EU-DSGVO ist die Meldepflicht von Datendiebstahl an die Aufsichtsbehörden. Gelingt es Cyber-Angreifern, personenbezogene Daten abzuziehen, müssen Unternehmen dies umgehend mitteilen. Versäumen sie es, drohen Bußgelder. Jedes Unternehmen sollte sich also die Frage stellen, wie gut seine IT gegen Angriffen von Cyber-Kriminellen geschützt ist. Wer sich darauf verlässt, dass die IT-Sicherheit im eigenen Haus schon gegen die Cyber-Kriminellen gewappnet sei, spielt mit dem Feuer.

Denn es drohen nicht nur Bußgelder seitens der Aufsichtsbehörden. Auch ehemalige Kunden könnten im Schadenfall klagen. Denn das in der EU-DSGVO verankerte sogenannte ‚Recht auf Vergessen' nimmt Unternehmen in die Pflicht, personenbezogene Daten auf Wunsch des Kunden zu löschen. Kommt ein Unternehmen dem nicht nach und die Daten geraten illegal nach außen, kann das einen hohen monetären Schaden bedeuten.

Dieser entsteht ebenfalls, wenn durch Cyber-Attacken Schäden an Hardware oder in der Produktion entstehen. Es lohnt sich also, einen prüfenden Blick auf die eigenen Systeme zu werfen. Sind die Compliance-Vorgaben umfassend genug oder stehen Nachbesserungen an? Systeme wie etwa ein Security Information and Event-Management (SIEM) sind in der Lage, das Abfließen von Daten zu erfassen. Unternehmen, die ein SIEM betreiben, können demnach schnell erkennen, wenn es zu einem Sicherheitsvorfall kommt. Ein solches System gibt aber im Vorfeld keine verlässliche Einschätzung dazu, ob die Daten ausreichend gesichert sind.

Die EU-DSGVO fordert jedoch, dass Unternehmen das Risiko des Datendiebstahls so gut es geht minimieren. Besonders für kleine Unternehmen ist das eine Herausforderung. Sie können die Voraussetzungen für gewisse Standards, wie sie etwa ein Information Security Management System (ISMS) verlangt, nicht immer erfüllen. Ist ein ISMS aus wirtschaftlichen Gründen nicht umsetzbar, sollte zumindest eine IS-Leitlinie existieren.

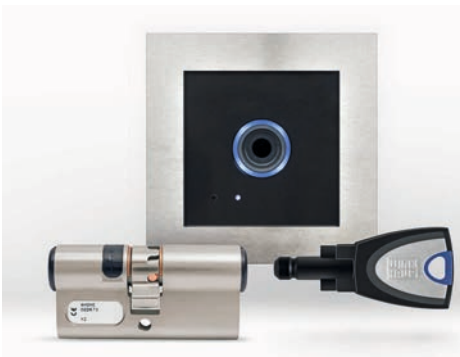
Viele am Markt verfügbare Monitoring-Tools können problemlos an bestehenden Systemen anknüpfen. Spezielle Risk-and-Security-Management-Plattformen, wie sie etwa Skybox Security anbietet, können Sicherheitslücken erkennen, bevor sie entstehen. Grundsätzlich ist es ratsam, Sicherheitsthemen im eigenen Haus zu belassen. Nicht immer ist es jedoch möglich, alle Maßnahmen zur IT-Sicherheit intern abzudecken. Dann sollten Unternehmen auf Leistungen von Managed-Service-Anbietern zurückgreifen.

Ihr Kontakt:
Thomas Wimmer
Tel.: +49 511 977-4073

Elektromechanische Schließanlagen

Allrounder für die intelligentere Gebäudezutrittsorganisation

blueSmart von Winkhaus ist die eigenentwickelte elektronische Zutrittsorganisation für die zeitgemäße Verwaltung komplexer Gebäudestrukturen. Mit Hilfe vernetzter elektromechanischer Schließzylinder lassen sich Zutrittsberechtigungen komfortabel verwalten. Das System kommuniziert in einem virtuellen Netz. Durch die umfangreichen Systembausteine lassen sich individuelle, auf das Objekt zugeschnittene Konzepte realisieren.



blueSmart verknüpft auf innovative Weise die Vorteile von Offline- und Onlinelösungen. Maximaler Komfort und besonders hohe Flexibilität für den Anwender stehen im Fokus der elektronischen Zutrittsorganisation. Einmalig ist die Kombination eines schlüsselbetätigten Systems mit den Leistungsmerkmalen eines Onlinesystems. Die Realisierung erfolgt mittels eines virtuellen Netzwerkes. Die Technologie kann auch in bestehende Systeme wie Gebäudeleittechnik, Kantinenabrechnung oder Alarm- und Energiemanagement eingebunden werden.

Komponenten bilden virtuelles Netz

Das virtuelle Netzwerk von blueSmart funktioniert offline und drahtlos zwischen den installierten elektronischen Komponenten, die miteinander kommunizieren. Im Gegensatz zu konventionellen Netzen entfallen aufwendige Verkabelungen, eine Vielzahl von Umsetzern oder störanfällige Funkstrecken. Mit blueSmart können Schließanlagen mit bis zu 195.000 Komponenten realisiert werden. Dabei ist die Anlage schnell und unkompliziert installiert, denn bei Nutzung des virtuellen Netzwerks von Winkhaus ist nur der Aufbuchleser konventionell zu verkabeln.

Passiver Schlüssel

Informationen zwischen den elektronischen Zylindern überträgt das System schnell und kabellos. Überträger ist der blueSmart-Schlüssel. Der aus Hochtemperatur-Kunststoff gefertigte Schlüssel ist wasserdicht (IP 68) sowie wartungsfrei und trägt einen RFID-Chip im Inneren, der sowohl programmierte Transaktionen als auch aus Türkomponenten ausgelesene Daten transportiert.

Nutzen in der Praxis:

- Flexible Vergabe von Berechtigungen
- Keine Anpassung an vorhandene Türen notwendig
- Bei Schlüsselverlust ist eine komfortable Sperrung möglich
- Geringer Administrationsaufwand
- Kostengünstiger Betrieb (geringer Wartungsaufwand)
- Nachvollziehbarkeit von Berechtigungen (Revisionssicherheit)

Kompakte Zylinder

Die elektronischen blueSmart-Zylinder haben die gleichen Maße wie mechanische Zylinder und brauchen nicht verkabelt zu werden, so dass bei der Installation aufwendige Umbauten von Türen entfallen. Auch lassen sie sich wie traditionelle mechanische Zylinder bedienen. Der elektronische blueSmart-Schlüssel wird in den Zylinder hineingesteckt und gedreht. Lange Batteriestandzeiten gewährleisten den dauerhaften, zuverlässigen elektronischen Betrieb. Daher ist der Wartungsaufwand sehr gering. Ein Zusatzelement ist der Ereignisspeicher. In diesem werden die letzten 2.000 Schließereignisse dokumentiert. Im Falle eines Diebstahls können die Nutzungsdaten im Nachgang eingesehen werden.

Ihr Kontakt:
Heiko Leßmann
Tel.: +49 511 977-4848

Neues Tochterunternehmen

AirITSystems erweitert Produktportfolio

Der Spezialist für IT- und Sicherheitslösungen AirITSystems erweitert sein Portfolio: Mit dem Tochterunternehmen Topsonic zählen nun auch Fluglärm- und Flugspurüberwachung zum Leistungsspektrum des Flughafenbetreibers.

Die neue Tochter von AirITSystems, die Topsonic Systemhaus GmbH mit Sitz in Würselen bei Aachen, ist auf hochwertige Messtechnik im Bereich der Flug-, Bau- und Industrielärmüberwachung sowie der Radardatenverarbeitung spezialisiert. Topsonic bietet seinen Kunden wartungsarme Hard- und Software für das Monitoring kritischer Systeme in Echtzeit. Zum Angebot des Unternehmens gehören darüber hinaus die Auswertung der Überwachungssysteme, das IT-Hosting und das Leasing der Messanlagen.

„Durch den Zusammenschluss von AirITSystems und Topsonic nutzen wir wertvolle Synergien. Die Expertise von Topsonic im Feld der Fluglärm- und Flugspurüberwachung ergänzt unsere Kompetenzen im Monitoring. Mit Topsonic als Tochter möchten wir im Markt wachsen und an die internationalen Kontakte des Unternehmens anknüpfen“, erläutert Eric Engelhardt, Geschäftsführer der AirITSystems GmbH.

„Der Schulterschluss mit AirITSystems ist für uns eine Win-win-Situation. Mit AirITSystems an unserer Seite werden wir bestehende Technologien weiterentwickeln und unseren hohen Sachverstand ausbauen“, sagt Topsonic-Geschäftsführer Bernd van Lier.

Die Topsonic Systemhaus GmbH wurde im Jahr 1996 gegründet und gehört zu den weltweit führenden Anbietern im Geschäftsfeld der Entwicklung von Fluglärmüberwachungssystemen. Das Unternehmen beschäftigt derzeit 15 Mitarbeiter/innen und wurde zum 01.07.2017 Tochterunternehmen der AirITSystems GmbH.

Ihr Kontakt:
Diana Schatka
Tel.: +49 511 977-4011

AirITSystems erlangt McAfee Managed Services Specialization

Neue Produkte und ein flexibles Preismodell: Kunden von AirITSystems profitieren ab sofort vom neuen Partnerstatus mit McAfee. Das US-amerikanische Unternehmen stellt Software und Hardware rund um das Thema Computersicherheit her.

In der Vergangenheit war AirITSystems bereits Silver Partner des Antivirus-Spezialisten McAfee. Mit der Managed-Services-Spezialisierung sind wir in der Lage, unseren Kunden nun weitere Produkte und Services anzubieten. Besonders das Angebot aus dem McAfee Web Gateway hat sich erweitert. Die Vorteile: Das „pay as you use“-Modell ermöglicht eine flexible und hochskalierbare Preisgestaltung. Darüber hinaus profitieren Kunden von unserem umfangreichen nachgelagerten Expertensupport.

Ihr Kontakt:
Tim Cappelmann
Tel.: +49 511 977-4071

Hannover
AirITSystems GmbH
Benkendorffstraße 6
30855 Langenhagen
(Hannover Airport)
Postfach 42 01 62
30661 Hannover
Telefon: +49 511 977-4000
E-Mail: info@airitsystems.de

Frankfurt
Speicherstraße 49–51
60327 Frankfurt am Main
Telefon: +49 69 430536-22

Frankfurt Fraport
Fraport AG
60329 Frankfurt am Main
Telefon: +49 69 380784501

Berlin
Rosenthaler Straße 34–35
10178 Berlin
Telefon: +49 30 2332905-10

München
Elsenheimer Straße 65
80687 München

AWARO®
Telefon: +49 89 2000526-60

Netzwerktechnologie
Telefon: +49 89 2190959-66

Impressum
AirITSystems GmbH
Benkendorffstraße 6
30855 Langenhagen
www.airitsystems.de
E-Mail: info@airitsystems.de
Telefon: +49 511 977-4000
Geschäftsführung:
Eric Engelhardt, Günther Gräf,
Dr. Wolfgang Pelzer
Grafik/Layout: www.steindesign.de

HANNOVER · FRANKFURT · BERLIN · MÜNCHEN