Gut besuchte Vorträge im Saal REGER des Hotel Maritim.

Deutschland digital fit machen

Oberst i.G. Armin Fleischmann, Leiter Programmbeirat AFCEA Bonn e.V.

Die AFCEA-Fachausstellung mit über 110 Ausstellern aus dem In- und Ausland und das begleitende Symposium haben sich seit 1986 als eine Art grüne IT-Leitmesse zum führenden Treffpunkt der IT-Community für Führungsunterstützung, Nachrichtengewinnung und Aufklärung, Geoinformationssysteme, IT-Sicherheit, Ausbildung, Logistik und SASPF entwickelt. Die 32. Ausstellung steht unter dem Motto „Digitale Zukunft gestalten – Intelligent. Vernetzt. Sicher". Dieser Blick ist wichtig: Werden Entwicklungen längst nicht mehr durch den Bedarf der Landes- oder Bündnisverteidigung definiert. Das Militär und andere Bereiche der öffentlichen Sicherheit müssen sich den bestehenden Entwicklungen stellen und Wissen aufholen.

Oberst i.G. Armin Fleischmann, Kommando Cyber- und Informationsraum.

Bereits 2017 hatte sich AFCEA mit dem Thema „Innere und äußere Sicherheit 4.0 – Schlüssel zur digitalen Souveränität" und deren zunehmenden Verzahnung von Produktion mit moderner Informations- und Kommunikationstechnologie beschäftigt. Aufgrund der Umsetzung aktueller Technologietrends wächst auch die Bedrohungen hinsichtlich der Möglichkeiten digitaler Angriffe. Zweifelsohne geht mit Industrie 4.0 aufgrund der zunehmenden Vernetzung ebenfalls die Notwendigkeit erhöhter Sicherheitsstandards hinsichtlich der inneren und äußeren Sicherheit (4.0) einher. Die klassische Trennung zwischen innerer und äußerer Sicherheit ist in unserer vernetzten Welt nicht mehr durchgehend möglich.
Innere und äußere Sicherheit stellen damit den Schlüssel zur digitalen Souveränität Deutschlands dar. Neben der technologischen Betrachtung müssen sich auch rechtliche Rahmenbedingungen und gesellschaftlicher Umgang mit den neuen Chancen und Risiken ändern, um zu einer neuen Form der Souveränität – einer digitalen Souveränität – zu gelangen.
2018 nun „Digitale Zukunft gestalten – Intelligent. Vernetzt. Sicher." Längst geht es bei neuen technischen Lösungen für die öffentliche Verwaltung nicht mehr nur um Vernetzung, sondern auch um die sichere Nutzung und andere gemeinsame Gestaltungsfelder der Zukunft. Vor allem intelligente und auch autonome Systeme bieten neue Chancen, bergen aber auch neue Herausforderung. Aktuelle Entwicklungen und Innovationen werden auch längst nicht mehr durch den Bedarf von Streitkräften oder anderer staatlicher Institutionen bestimmt. Militär und andere Bereiche der öffentlichen Sicherheit müssen sich den bereits stattgefundenen Entwicklungen stellen, Wissen aufholen und neue Kompetenzen erwerben. So erfahren Streitkräfte und Sicherheitsbehörden durch die Digitalisierung und Automatisierung, im Friedensbetrieb wie im Einsatz, massive Veränderungen, sei es beim Waffeneinsatz, in der Logistik, in der Führung oder in der Aufklärung. Maßgebliche technische Entwicklungen wie etwa soziale Medien sind Treiber gesellschaftlicher Entwicklungen geworden, die vom Staat eine neue normsetzende Rolle abverlangen. Gleichzeitig entwickeln Manipulationen in den Sozialen Medien massiven Einfluss auf demokratische Entwicklungen. Künstliche Intelligenz und autonome Maschinen werden den Staat noch stärker fordern, sowohl in regulatorischer Hinsicht als auch in der Förderung disruptiver Technologieentwicklungen.
AFCEA Bonn e.V. wird deshalb mit dem Jahresthema „Digitale Zukunft gestalten – Intelligent. Vernetzt. Sicher." auch aktuell seiner traditionellen Rolle als Plattform für die Kommunikation mit den federführenden Stakeholdern in Deutschland gerecht. Auf der 32. AFCEA Fachausstellung wird der Bestsellerautor Marc Elsberg am 11. April in Bonn die Frage diskutieren, wie Deutschland sich für die digitale Zukunft rüsten kann.

Abbildungen © StefanVeres

Das MARITIM Hotel Bonn ist erneut Veranstaltungsort.

32. AFCEA-Fachausstellung Informations- und Kommunikationstechnik

Das diesjährige Motto: „Digitale Zukunft gestalten – Intelligent. Vernetzt. Sicher."

Jürgen K.G. Rosenthal

In diesem Jahr haben sich circa 130 Aussteller zur 32. AFCEA-Fachausstellung angemeldet. Die AFCEA-Fachausstellung findet auch in diesem Jahr wieder im MARITIM Hotel Bonn-Bad Godesberg statt. Das Thema in diesem Jahr lautet: „Digitale Zukunft gestalten – Intelligent. Vernetzt. Sicher."
Die 32. Fachausstellung wird wieder durch ein Symposium an beiden Tagen begleitet, das im Motto das Jahresthema von AFCEA Bonn 2018 aufnimmt.

Längst geht es bei neuen technischen Lösungen für die öffentliche Verwaltung nicht mehr nur um Vernetzung, sondern auch um die sichere Nutzung und andere gemeinsame Gestaltungsfelder der Zukunft. Vor allem intelligente und auch autonome Systeme bieten neue Chancen, bergen aber auch neue Herausforderung und werden den Staat in regulatorischer Hinsicht zukünftig stärker fordern.
Aktuelle Entwicklungen und Innovationen werden auch nicht mehr durch den Bedarf staatlicher Institutionen bestimmt. Militär und andere Bereiche der öffentlichen Sicherheit müssen sich

den bereits stattgefundenen Entwicklungen, als auch der Förderung disruptiver Technologieentwicklungen stellen, Wissen aufholen und neue Kompetenzen erwerben. So erfahren Streitkräfte und Sicherheitsbehörden durch die Digitalisierung und Automatisierung, im Friedensbetrieb wie im weltweiten Einsatz, massive Veränderungen, sei es beim Waffeneinsatz, in der Logistik, in der Führung oder in der Aufklärung. Maßgebliche technische Entwicklungen wie etwa soziale Medien sind Treiber gesellschaftlicher Entwicklungen geworden, die vom Staat eine neue normsetzende Rolle abverlangen. Gleichzeitig entwickeln Manipulationen in den Sozialen Medien massiven Einfluss auf demokratische Entwicklungen, die es zu erkennen gilt.

Symposium zur 32. AFCEA-Fachausstellung

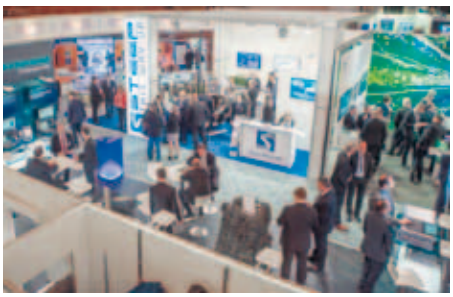
11. April 2018 – Erster Tag des Symposiums

10.00 Uhr	Begrüßung und Eröffnung der 32. AFCEA-Fachausstellung Generalmajor a.D. Erich Staudacher, Vorsitzender AFCEA Bonn e.V. und General Manager AFCEA Europe
10.20 Uhr	Grußwort der Stadt Bonn tbd. – Vertreter der Stadt Bonn
10.30 Uhr	Vortrag Klaus-Hardy Mühlec Abteilungsleiter Cyber- und Informationstechnik und CIO im BMVg
11.20 Uhr	Vortrag Ministerialdirigent Andreas Könen Leiter der Stabsstelle „IT- und Cybersicherheit, sichere Informationstechnik“ BM des Inneren
14.00 Uhr	Diskussion über die digitale Zukunft Deutschlands Marc Elsberg Bestsellerautor, unter anderem „Black-out – Morgen ist es zu spät“ (Stromausfall) und „Zero – Sie wissen, was du tust“ (Big Data/Datenschutz)
16.00-17:45 Uhr	Young AFCEANs Leadership Forum im Saal REGER Das Young AFCEANs Leadership Forum ist eine Gesprächsrunde für junge Führungskräfte mit Spitzenvertretern aus Bundeswehr, Verwaltung, Wissenschaft und Industrie, die Einblicke in ihren Lebenslauf gewähren und Karrieretipps geben. Im Mittelpunkt steht der Erfahrungsaustausch.
18.00 21.00 Uhr	Get-together AFCEA-Fachausstellung Im Ausstellungsbereich – Foyer I und II des MARITIM Hotel Bonn

12. April 2018 – Zweiter Tag des Symposiums

10.00 Uhr	Vortrag Oberstleutnant i.G. Frank Werner Trettin Leiter Aufbaustab „Agentur für disruptive Innovationen in Cybersicherheit“
14.00 Uhr	Vortrag Generalarzt Dr. Michael Zallet Abteilungsleiter B im Kommando Sanitätsdienst der Bundeswehr

Begrüßung und Eröffnung durch Generalmajor a.D. Erich Staudacher, Vorsitzender AFCEA Bonn e.V. und General Manager AFCEA Europe



Kritische Geoinformation für militärische Evakuierungsoperationen

Wie Kartenmaterial – aufbereitet durch moderne GIS-Technologie – ressortübergreifend als gemeinsame Planungs- und Durchführungsgrundlage genutzt werden kann

Für militärische Evakuierungsoperationen (MilEvakOp) deutscher Staatsbürger im Ausland verfügt die Bundeswehr über speziell ausgebildete Kräfte. Die erfolgreiche Planung, Durchführung und Nachbereitung solch zeitkritischer Operationen erfordert, dass Spezialisten unterschiedlicher Fachgebiete eng miteinander zusammenarbeiten und ihren Informationsraum genau kennen.

Vom Planungsstab, über die eingesetzten Kommandosoldaten, bis hin zur medizinischen Versorgung befreiter Bürger – die Integrität und Aktualität der Informationskette muss hierfür stets gewährleistet werden. Auf der diesjährigen AFCEA zeigt Esri, welche Möglichkeiten dank intelligent genutzter Geoinformationen für MilEvakOp entstehen. Die Karte fungiert hierbei ressortübergreifend als gemeinsame Planungs- und Durchführungsgrundlage, um in Krisensituationen ad hoc zu handeln.
Moderne GIS Technologie von Esri stellt Entscheidungsträgern passgenaue Informationen zum Einsatzraum bereit – zu jeder Zeit, überall und geräteübergreifend. Beispiele missionskritischer Informationen für eine Evakuierung:

- Potentielle Evakuierungsrouten und ihre Verfügbarkeit
- Zugangswege für einen Zugriff
- Hochaktuelle Satelliten- und Drohnenaufnahmen
- Lageinformationen eigener Kräfte (Blue Force Tracking)
- Meldungen zu fremden Kräften
- Lage und Status umliegender KRITIS
- Politische und ethnologische Verteilungen.

Die ArcGIS Plattform ermöglicht der Bundeswehr den gemeinsamen Informationsraum bis in die letzte Meile aufzuspannen, und auch in Offline-Szenarien handlungsfähig zu bleiben.
Wir freuen uns, mit Ihnen auf der AFCEA 2018 die technischen Innovationen rund um das MilEvakOp zu beleuchten.
Besuchen Sie uns am Esri Deutschland Stand M26 im Saal Maritim.

www.esri.de

Großes Interesse am Esri Deutschland Stand auf der AFCEA 2017.
© HHK / StefanVeres

Deutsche Telekom zum Thema Cybercrime: Darauf müssen wir uns 2018 einstellen

Stärker, ausgeklügelter, schneller – Cyberangriffe kennen in den vergangenen Jahren keine Abwärtskurve. Und auch im neuen Jahr wird der Cyberhimmel nicht rosarot aussehen, prognostizieren die Sicherheitsexperten der Telekom. Fünf große Trends bei Cyberangriffen sehen sie für das kommende Jahr: Und die bedeuten, dass Privatnutzer und Unternehmen noch mehr auf der Hut vor Erpressungs-Software sein, ihre Passwörter mit viel Bedacht auswählen und auf vernetzte Geräte Software-Updates regelmäßig aufspielen müssen, um nicht Opfer von Cyberkriminellen zu werden.

Vernetzte Geräte werden vermehrt für Angriffe missbraucht

Haushalts- und Bürogeräte wie Fernseher, Kühlschränke und Sicherheitskameras sind mittlerweile so leistungsstark wie kleine Rechner – und oft mit dem Internet verbunden. Immer häufiger kapern Kriminelle diese vernetzten Geräte und nutzen sie dazu, weitere Ziele anzugreifen. Meistens, ohne dass der Besitzer dies überhaupt merkt. So kann es kommen, dass die Server eines Unternehmens unter massenhaften Anfragen zusammenbrechen und die Webseiten dieses Unternehmens nicht mehr erreichbar sind. Und der eigene Fernseher oder die Aufzugssteuerung in einem Unternehmen ist Bestandteil dieses Angriffs.

„Patchen, patchen, patchen heißt die Lösung", sagt Thomas Tschersich, Leiter Cybersecurity bei der Telekom. „Wenn man immer die aktuellste Software auf seinen Geräten betreibt, liegt die Chance, nicht erfolgreich angegriffen zu werden, bei über 90 Prozent." So rät der Experte, bei vernetzten Geräten immer die AutoUpdate-Funktion zu aktivieren.

Cyber-Erpressung wird immer gewiefter

Durch Abhandenkommen und anschließender Veröffentlichung von Angriffswerkzeugen von Geheimdiensten und Staaten, erhalten auch Cyberkriminelle Zugang zu mächtigen Werkzeugen zur Verbreitung ihres Schadcodes: Anstatt nur eine Mail mit einem verseuchten Anhang zu senden, schleusen Cyber-Kriminelle jetzt über diese Werkzeuge zunehmend Schadcode ein, der sich selbst verbreiten kann. Ist innerhalb eines Netzwerkes einer Firma etwa ein Rechner infiziert, greift die Schadsoftware auf weitere Rechner über.

„Das bedeutet eine neue Qualität von Angriffen über Erpressungstrojaner, die wiederum neue Schutzmaßnahmen nötig macht: Bisher gingen die meisten Unternehmen und Privatnutzer davon aus, von dienstlichen oder staatlichen Cyberangriffen nicht betroffen zu sein. Nun sind die Werkzeuge für solche Angriffe Allgemeingut geworden – und jeder muss sich vor ihnen schützen", kommentiert Thomas Tschersich.

Besonders bei Unternehmen sei die Frage nicht mehr, ob sie erfolgreich angegriffen werden, sondern wann. „Deshalb wird es immer wichtiger, sich auf einen erfolgreichen Angriff vorzubereiten und dafür zu sorgen, dass dessen Auswirkungen möglichst gering bleiben." Hier bedarf es gut geschulter Experten, die man sich entweder im eigenen Haus, oder über einen spezialisierten Dienstleister vorhalten sollte, so Tschersich.

Identitätsdiebstahl verstärkt sich und erschwert Aufdeckung von Angriffen

Die meisten Dienste im Internet funktionieren heute mit Passwort. Viele Menschen machen es sich leicht und nutzen ein Passwort für zahlreiche Dienste und Anwendungen: Die Anmeldung zum Mailaccount ist dieselbe wie für den Online-Shop, das Banking-Portal und das Kundencenter des Telefonanbieters. Das Problem dabei: Gelangen die Kriminellen an einer Stelle an die Daten eines Nutzers, testen sie diese bei verschiedenen Diensten – und bestellen im Zweifelsfall mit einer gestohlenen Identität im Shop, buchen Leistungen und Geräte auf Telefonverträge oder spionieren weitere Daten aus.

Schwierig wird es in diesen Fällen, Missbrauch nachzuweisen: Die Transaktionen, die die Kriminellen mit der gestohlenen Identität ausführen, erscheinen auf den ersten Blick legitim – Banking, Bestellen unter einer tatsächlich existierenden Identität sind gewöhnliche Aktionen in der online-Welt. „Hieran zeigt sich eine neue Entwicklung in der Aufdeckung von Cyberkriminalität. Gut versus Böse reicht längst nicht mehr aus zur Bewertung. Die neuen Kategorien lauten „plausibel versus nicht plausibel". Dahingehend verschiebt sich aktuell die gesamte Cyber-Analyse", erklärt Sicherheitschef Thomas Tschersich. Dem Einzelnen rät er, sichere Passwörter zu nutzen und vor allem nicht dasselbe Passwort für alle Anwendungen und Dienste zu nutzen.

Beeinflussung über Fake News und Microtargeting nehmen zu

Spätestens seit den US-Wahlen sind „Fake News" zum geflügelten Wort geworden. Sowohl bewusst falsche Nachrichten in der Breite, als auch das Streuen von Nachrichten an passgenau ausgewählte Zielgruppen werden ebenfalls weiter zunehmen und zur Verunsicherung von Menschen führen. Entsprechende Angriffe werden immer zielgerichteter und sind längst nicht mehr in gebrochenem Deutsch verfasst. Und Fake News verbreiten sich über soziale Netzwerke wie Lauffeuer. Dadurch steigt die wahrgenommene Glaubwürdigkeit, und ein „Dagegenhalten" wird zunehmend herausfordernder.

Kryptowährungen werden zunehmend korrumpiert

Mit fortschreitender Verbreitung von Kryptowährungen steigt die Gefahr, dass Kriminelle die Systeme privater Nutzer zum Schürfen von Kryptowährungen missbrauchen. Bereits heute beobachten die Telekom-Experten einen Anstieg von Kryptomining in Browsern. Diese Entwicklung wird sich 2018 fortsetzen. Eine weitere Gefahr ist, dass Nutzern ihre bereits vorhandene Kryptowährung durch Malware oder Schwachstellen gestohlen wird. Parallel zu den fünf Haupttrends beobachten die Telekom-Experten, dass Cyberkriminelle ständig neue Vehikel entwickeln, um Schadcode zu platzieren. Jüngstes Beispiel ist ein Einschleusen über Dynamic Data Exchange (DDE), einem Feature zum Austausch von Daten innerhalb von Microsoft Windows. Über DDE können Kriminelle Schadcode auf Rechner übertragen, ohne dass der Betroffene dafür Makros in einem Microsoft Office Dokument aktivieren muss. Thomas Tschersich: „Auch das ist eine neue Qualität eines Angriffs, gegen den die meisten Unternehmen noch nicht gerüstet sind."

Um die aktuellsten Entwicklungen von Cyberangriffen zu verfolgen, die eigene und die Infrastruktur von Kunden noch besser zu schützen, und um Vorhersagen zur weiteren Entwicklung von Angriffen und möglicher Abwehr zu treffen, hatte die Telekom jüngst ihre Cyberabwehr ausgebaut: In Bonn entstand ein neues Cyber Defense und Security Operations Center, in dem die Cyber-Aktivitäten der Telekom zentral gesteuert werden.

Deutsche Telekom AG
Corporate Communications
www.telekom.com

Thales zeigt die Funksysteme SYNAPS und Jammer zum Schutz gegen funkgesteuerte Sprengfallen

Jürgen K.G. Rosenthal

Thales ist seit Jahrzehnten bei Ausrüstung und Service von Mobilen Taktischen Kommunikationssystemen Partner der Bundeswehr und der NATO. Durch ein hochmodernes, einsatzerprobtes Portfolio steht Thales als Systemanbieter der Bundeswehr bei der Umsetzung des Programms „Mobile Taktische Kommunikation" (MoTaKo) mit Beratung, Entwicklung, Design, Inbetriebnahme und Service zur Seite.

SYNAPS Radio Network Solution zur Führung und Kommunikation.

Das Produktportfolio kann dem einsatzbedingten Kommunikationsbedarf modular angepasst werden. Die moderne Systemarchitektur ermöglicht eine nahtlose, medienbruchfreie Kommunikation. Moderne Funksysteme wie die neu entwickelte Software-Defined-Radio-Produktfamilie SYNAPS bietet leistungsfähige Kryptologie- und Schlüsselmanagementlösungen, während moderne SOTM-Systeme die notwendigen Kommunikationsplattformen die Gewährleistung eines „Quality of Services" sicherstellen.

Der tragbare Jammer von Thales für die Bundeswehr.

Die Bundeswehr wird künftig bei ihren Auslandseinsätzen mit tragbaren Jammern von Thales ausgerüstet sein und damit besser gegen funkgesteuerte Sprengfallen geschützt werden.

Die Jammer schützen die Soldaten beim Verlassen ihrer Fahrzeuge vor improvisierten Sprengfallen (RC-IED), die über Funk ausgelöst werden. Ein geringes Gewicht von etwa 1 Kilo, einfache Bedienung und lange Batterielaufzeit von mindestens acht Stunden zeichnen die bereits bei mehreren NATO-Mitgliedsstaaten im Einsatz befindlichen Systeme aus. Die Geräte werden in Großbritannien hergestellt und gehören zur Jammer STORM-H Familie.

Thales ist im Foyer I, Stand F13 zu finden.

Abbildungen © Thales

Zu sehen auf der 32. AFCEA-Fachausstellung

BWI zeigt mobile IT-Lösungen von heute und Anwendungen von morgen

Um den digitalen Anforderungen moderner Streitkräfte gerecht zu werden, ist nicht nur flexible und mobile IT gefragt, diese muss auch hohen Sicherheitsstandards entsprechen. Als verlässlicher IT-Dienstleister der Bundeswehr stellt sich die BWI diesen Anforderungen. Auf der AFCEA-Fachausstellung am 11. und 12. April 2018 zeigt das Unternehmen deshalb Lösungen, die den hohen Ansprüchen der Bundeswehr bereits heute Sorge tragen und gibt gleichzeitig einen Ausblick auf künftige Möglichkeiten.
Ein geräteunabhängiger, mobiler und in Echtzeit erfolgender Zugriff auf Anwendungen und Daten soll bei der Bundeswehr bald genauso selbstverständlich sein wie im Privatleben. Die BWI präsentiert dafür auf der 32. AFCEA-Fachausstellung entsprechende Geräte, die Sichere Mobile Kommunikation (SMK) ermöglichen. Damit erhalten Besucher einen Eindruck von der Technologie, die künftig bei der Bundeswehr zur Verfügung gestellt wird.

BWI-Stand auf der AFCEA-Fachausstellung 2017.
© HHK / StefanVeres

Cloud on Mobile
Auf diesen Geräten können Besucher auf dem BWI-Stand eine Cloud on Mobile und damit einen Ausblick auf eine Virtuelle Desktop-Infrastruktur (VDI) erleben. Bei der AFCEA-Fachausstellung nutzt die BWI hierzu noch einen Demonstrator, die VDI soll für Teile der Bundeswehr allerdings noch 2018 Realität werden.
Der Blick der BWI geht auch noch weiter in die Zukunft: Anhand eines Beispiels aus dem Bundeswehr-Alltag zeigen die BWI-Experten die Möglichkeiten, die „Blockchain" den Streitkräften bieten kann, und macht so Innovation konkret greifbar.
Besuchen Sie die BWI am Stand M16 im Saal Maritim im Maritim Hotel Bonn. Informieren Sie sich im persönlichen Gespräch mit den BWI-Experten und testen Sie die gezeigten IT-Lösungen der Zukunft selbst.

RUAG Defence präsentiert die neueste Entwicklung – RUAG ARANEA Communication Expert

Rettungs- und Sicherheitseinsätze militärischer wie ziviler Organisationen werden immer komplexer und vielschichtiger. Eindimensionale Standardszenarien gehören weitgehend der Vergangenheit an. Um die zahlreichen involvierten Akteure ideal zu befähigen, hat sich RUAG Defence deshalb auf schnelle, sichere und interoperable Kommunikationslösungen spezialisiert – getreu dem Motto: „We guarantee fast communication".

© 2018 RUAG Schweiz AG, RUAG Defence

An der diesjährigen AFCEA in Bonn präsentieren wir unsere neueste Entwicklung – RUAG ARANEA Communication Expert. Diese Kommunikationslösung gewährleistet den Aufbau einer schnellen und sicheren Kommunikationsinfrastruktur in kürzester Zeit bei autarker Stromversorgung. Verschiedenste Endgeräte, Technologien und Features werden dabei nahtlos integriert.
Auf der AFCEA treten wir zusammen mit ND SatCom auf. Mit mehr als 30 Jahren Erfahrung im Bereich Satellitenkommunikation ist ND SatCom der weltweit führende Lieferant von satellitenbasierten Kommunikationssystemen und Bodenstationen. Wir laden Sie herzlich ein, uns im Foyer F1 am Stand F07 zu besuchen. Unsere Experten freuen sich darauf, Sie persönlich zu begrüßen.

Trusted solutions from a single source.

Von kompakten IT-Sicherheitsprodukten für KMUs bis zu skalierbaren Enterprise-Lösungen, Rohde & Schwarz Cybersecurity sorgt für:

- **Sichere und transparente Netzwerke**
- **Schutz von Webapplikationen**
- **Abhörsichere Kommunikation**
- **Endpoint-Schutz und Trusted Management**

Unsere mehrfach ausgezeichneten Lösungen schützen Unternehmen, Betreiber kritischer Infrastrukturen und Behörden vor Spionage und Cyberangriffen. Sie folgen dem „Security by Design"-Ansatz und verhindern proaktiv selbst komplexe Angriffe.

cybersecurity.rohde-schwarz.com

2018

Security
Services & Solutions
Rising Star Germany

ISG Provider Lens™

ROHDE&SCHWARZ
Cybersecurity

Besuchen Sie uns auf der AFCEA 2018: 11. – 12. April | Maritim Hotel | Bonn | Stand M08

IT-Dienstleister Materna stellt sich vor

Materna ist ein etablierter Partner der öffentlichen Verwaltung und führender deutscher Anbieter für die Digitalisierung im Public Sector.

Materna ist ein führendes IT-Dienstleistungsunternehmen im Premium-Segment mit fast 40 Jahren Erfahrung in der IT-Beratung, -Entwicklung und -Integration in bestehende Systeme. Der IT-Dienstleister mit Hauptsitz in Dortmund ist an zahlreichen Standorten in Deutschland sowie im Ausland vertreten und beschäftigt weltweit mehr als 1.900 Mitarbeiter. Namhafte Kunden wie Finanzministerium NRW, Generalzolldirektion, DHL, Bundesagentur für Arbeit, Lufthansa, Siemens, Telekom, Vodafone und Daimler vertrauen auf die Expertise zertifizierter Experten von Materna.

Mit den Lösungen von Materna kommen täglich Millionen Menschen in Kontakt, oft, ohne es zu wissen, beispielsweise wenn sie am Flughafen am Automaten einchecken, im Internet ein Päckchen bei einem großen Logistiker nachverfolgen oder eine elektronische Zollanmeldung abgeben.

Materna ist ein etablierter Partner der öffentlichen Verwaltung und führender deutscher Anbieter für die Digitalisierung im Public Sector. Der IT-Dienstleister begleitet die digitale Transformation, von der Beratung über die Implementierung standardisierter skalierbarer IT-Lösungen bis zur Entwicklung und Integration ressortspezifischer Fachverfahren zu ganzheitlichen Lösungen, für durchgängig elektronische Verwaltungsdienste. Die Kompetenzfelder im Bereich der digitalen Verwaltung reichen von E-Government über Internet- und Intranet-Portale bis zu Formular-Management, Dokumenten-Management und der elektronischen Aktenführung. Darüber hinaus unterstützt Materna seine Kunden bei vielfältigen Infrastrukturthemen, wie zum Beispiel IT-Service- und Operations Management, Cloud, Security, Managed Services und IT-Consulting.

Zur Materna Gruppe gehören weiterhin mehrere Tochtergesellschaften und Beteiligungen. Dazu zählen unter anderem die cbs Corporate Business Solutions als Prozessberater und SAP-Spezialist, die Infora GmbH als Beratungshaus für die Öffentliche Verwaltung, die IQDoQ mit Lösungen für eine Personal- und Vertragsakte und die Materna TMT GmbH für Softwarelösungen und Dienstleistungen im Aus- und Weiterbildungsbereich.

Frank Grotheer, Sales Director Defense bei Materna GmbH

Materna verknüpft bewährte Vorgehensweisen mit neuen Technologien und integriert Lösungen etablierter Partner und marktführender Software-Hersteller. Mit umfassender Erfahrung in allen marktrelevanten Technologien sowie in aktuellen Technologietrends wie Cloud, Chatbots, Blockchain oder Cognitive Computing steht Materna den Organisationen auf dem Weg zu einer agilen und effizienten IT zur Seite.

Bereit für die digitale Transformation in der Bundeswehr

Als langjähriger IT-Dienstleister und Lösungsanbieter für das Informations Technik Zentrum Bund (ITZBund) und andere Bundes- und Landeseinrichtungen berät und unterstützt Materna auch Behörden und Organisationen mit Sicherheitsaufgaben. Für Bereiche der inneren und äußeren Sicherheit kann Materna mit modernen Informationstechnologien, die individuell an die Anforderungen im Sicherheitsumfeld angepasst sind, einen Beitrag leisten. Es bestehen heute bereits bundeswehrspezifische Rahmenverträge für die Realisierung unterschiedlichster Lösungsansätze. Im Zuge der Ausweitung des Geschäftsbereiches Public Sector sind Bundeswehr-Projekte künftig eine weitere Säule im Materna-Portfolio.

Sie möchten mehr erfahren?
Nehmen Sie mit uns Kontakt auf:
Materna GmbH
Telefon: +49 231 5599-00
E-Mail: frank.grotheer@materna.de
www.materna.de

Sichere Kommunikation in Echtzeit

Der Schutz vertraulicher Informationen ist bei militärischen Einsätzen ein Muss. Gleichzeitig ist es notwendig, dass benötigte Informationen weitergegeben werden können. Viele Einsatzszenarien verlangen darüber hinaus eine verzugslose Datenübertragung. All dies ließ sich bisher nicht optimal miteinander verbinden. Die INFODAS GmbH präsentiert auf der AFCEA Fachausstellung in Bonn vom 11. bis 12. April mit der Express-Variante ihres bewährten SDoT Security Gateways erstmals eine sichere Netzübertragung großer Datenmengen in Echtzeit.

In der militärischen Kommunikation kommt neben der Wahrung der Sicherheit ein weiterer entscheidender Aspekt ins Spiel: Geschwindigkeit. Etwa wenn Sensordaten von Radaranlagen oder Steuerbefehle an Lenkflugkörper übertragen werden sollen. Oder wenn sensible personenbezogene Informationen zwischen unterschiedlichen Behörden ausgetauscht werden müssen, um ein vollständiges Gefährdungslagebild zu erstellen. Solche Daten bzw. Befehle werden in schneller Folge in Form von so genannten „Telegrammen" übermittelt. Für eine sichere Übertragung zwischen zwei Domänen ist deren schnelle Prüfung notwendig. Die INFODAS GmbH hat ihre bewährte Lösung für die sichere Netzübertragung SDoT Security Gateway an diese Anforderungen angepasst. „Bei der Übertragung militärischer Daten geht es nicht allein um Sicherheit – sondern auch um Geschwindigkeit", erklärt Thomas Günther, Leiter der Business Unit IT Security Solutions bei der INFODAS GmbH. „Mit unserer Express-Lösung des Security Gateways ist nun beides möglich."

Für die Express-Variante des SDoT Security Gateways wurde die interne Sicherheitsarchitektur des Gateways auf die hochperformante und latenzarme Übertragung der zu prüfenden Telegramme hin optimiert. Damit ist es möglich, hochfrequente Datenpakete mit sehr niedriger Latenz und hohem Datendurchsatz zwischen unterschiedlichen Sicherheitsdomänen auszutauschen. Die bewährten Filtermechanismen für die Prüfung von typisch militärischen bzw. von BOS verwendeten Nachrichtenformaten (z.B. XML, Link 16, ASTERIX, ADatP-3, ADEXP, NMEA, DIS, etc.) können vollumfänglich weiterverwendet werden. Das „SDoT Security Gateway" der INFODAS GmbH ermöglicht eine automatisierte Kommunikation zwischen unterschiedlich eingestuften Netzen. Das SDoT-Security Gateway hat eine Zulassung des BSI bis GEHEIM. Der Zulassungsantrag für das neue Produkt „Express" wurde gestellt. (2.409)

Die INFODAS GmbH gehört zu den führenden und innovativen Beratungsunternehmen für IT-Sicherheit in Deutschland. Das mittelständische Systemhaus verfügt über 40 Jahre Erfahrung in der Entwicklung und Umsetzung von Lösungen für den Schutz der IT-Infrastruktur in Unternehmen, Behörden und militärischen Einrichtungen. Die besondere Expertise der INFODAS liegt in der Implementierung eines Informationssicherheitsmanagementsystems (ISMS) gemäß ISO 27001 auf der Basis von BSI IT-Grundschutz. INFODAS führt auch die entsprechenden Zertifizierungsaudits durch.

Mit der Produktfamilie SDoT (Secure Domain Transition) bietet INFODAS ein umfassendes Portfolio an Produkten für den Hochsicherheitsbereich bei Streitkräften, öffentlichen Auftraggebern und Unternehmen der Privatwirtschaft. Durch eine intensive Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) haben diese Lösungen mehrfach Zulassungen für eine Nutzung bis GEHEIM erhalten. INFODAS wurde im Jahr 1974 gegründet. Neben dem Hauptsitz in Köln gibt es weitere Standorte in Berlin und München.

www.infodas.de

systerra computer GmbH auf der AFCEA 2018

Auf der AFCEA 2018 zeigt die systerra computer GmbH einen Ausschnitt ihres Produktportfolios im Rugged-Server-Umfeld

Neu! Rugged "Server-to-Go"
Der besonders kompakte mobile Server im Aktenkoffer-Format (10,2 cm x 34,3 cm x 27,8 cm klein und 6,8 Kg leicht) mit einer bis zu 20-Kern Xeon-CPU, 8 x 15mm 2,5" Laufwerken, 2 PCIe Erweiterungs-Slots und Hochgeschwindigkeits- I/O bietet viel Rechen- und Speicherleistung auf kleinstem Raum. Er erfüllt MIL-STD-810G, MIL-STD-901D, und MIL-STD-167-1.

Abbildung 1: Der mobile Mini-Server im Aktenkofferformat.

Neu! Höchste Leistung, Zuverlässigkeit und Widerstandsfestigkeit für den Einsatz in anspruchsvoller Umgebung
In nur 2U und 17,5" Einbautiefe bietet der Rugged Industrieserver SRS (Abb. 2, rechts) mit den neuesten Intel Xeon™ Scalable CPUs bis zu 44 (2x22) Prozessorkerne, 1TB DDR4 Hauptspeicher und bis zu 18 hot-swap 2,5" SAS-3/SATA-III Laufwerke: 2xBoot, 16xDaten-Storage (Raid o,1,5,6,10) mit einer Aufzeichnungsschreibrate >10 GByte/sec.
Die integrierten redundanten Netzteile erlauben, je nach Variante, AC oder DC (24V) Versorgung.
Das flexible Design ermöglicht diverse Erweiterungen sowie Ergänzungen durch die vorhandenen PCIe Steckplätze. Der SRS ist für missionskritische Anwendungen in anspruchsvoller Umgebung sowohl im stationären als auch im mobilen Betrieb ausgelegt.

Lüfterlos in rauer Umgebung
Der lüfterlose Xeon-D™ embedded Server MXCS (Abb. 2, Mitte) von systerras Schweizer Partner MPL widersteht auch ohne aktive Kühlung extremen und harschen Umgebungsbedingungen.
Der MIL-STD-810, -461, -704, -1275 zertifizierte Rechner ist als Open Frame erhältlich oder in speziell entwickelten Aluminium- oder MIL-IP67-Gehäusen verbaut und kann von -20 bis +60°C betrieben werden. Er verfügt über 8 x 2,5" SSD Slots und ist mit vier PCI/104-Express sowie vier PCI-Express Mini Card Schnittstellen bedarfsgerecht ausbaubar. Die MPL AG entwickelt und fertigt alle Produkte in der Schweiz und garantiert eine Verfügbarkeit und Wartbarkeit für 10+ Jahre.

Zuverlässige Performance für die „großen Jobs" in höchster Packungsdichte
Die Enterprise Server von Themis (Abb. 2, links) bieten höchste Rechnerleistung mit Single oder Dual Xeon E5-2600v4 Prozessoren, je 4…20 Cores und bis zu 2 TB ECC RAM. Die Server verfügen über Wechselrahmen für acht oder sechzehn SATA/SAS3 Laufwerke und HW-RAID Support. Sie arbeiten auch in anspruchsvoller Umgebung, wo Größe, Gewicht, Umweltbedingungen und Stromverbrauch relevant sind, stabil und zuverlässig.
Der Betriebstemperaturbereich beträgt 0…+50°C bei voller Rechenleistung.
Die Server sind mit 1 oder 3HE Bauhöhe und Einbautiefen von ca. 35,6 bis 53,3 cm erhältlich.
Die modulare, hochkompakte high-density Variante der Server bietet Platz für bis zu sechs Computer-Module mit jeweils Single/Dual XEON CPU und dual 10/40Gbit/s Ethernet-Ports in 20 Zoll tiefen 2HE oder 3HE Chassis.

systerra computer GmbH – was wir für Sie tun
Mit der Erfahrung und Expertise aus zahlreichen Projekten erstellt systerra in enger Zusammenarbeit mit Kunden und Herstellern applikationsspezifische Hardwarelösungen, unterstützt bei der Projektierung, Zertifizierung und Implementierung der Produkte.
Die systerra computer GmbH ist seit 15 Jahren Anbieter von MIL-konformen Rechner-, Speicher- und Netzwerkplattformen für den erweiterten Betriebstemperaturbereich.
Der Schwerpunkt liegt dabei auf Spitzentechnologie mit hoher Verfügbarkeit, Zuverlässigkeit und Tauglichkeit in anspruchsvoller Umgebung wie zum Beispiel dem mobilen und stationären Einsatz am Boden, in der Luft und auf See.
systerra setzt auf anerkannte und bewährte Hard- und Software-Standards.

Partner sind u.a.: MPL AG, Themis Computer, Moxa, RTD und Acromag

Kontakt: systerra computer GmbH,
Kreuzberger Ring 22, 65205 Wiesbaden,
Tel. 0611/44889-400,
E-Mail: info@systerra.de,
Internet: www.systerra.de

Abbildung 2: High-Density Server (links), lüfterloser Xeon-Server (Mitte) und Rugged Industrieserver SRS (rechts).

Abbildungen © systerra computer GmbH

Computacenter – Wir digitalisieren die Verwaltung

Bereits seit vielen Jahren ist Computacenter als Dienstleister für Bund, Länder und Kommunen tätig, in steigendem Umfang auch für die Bundeswehr. Die rasante Entwicklung im Bereich der Informationstechnik, von der e-Akte über Cloudtechnologien bis hin zu den Herausforderungen des Cyber- und Informationsraumes hat das Unternehmen stets aufgegriffen, sich intern entsprechend aufgestellt und ausreichend Kapazitäten entwickelt.

Computacenter ist daher in der Lage, in nahezu allen Bereichen der öffentlichen Hand Unterstützung zu leisten, von der Gestaltung moderner Arbeitsplätze bis hin zu Beratungsleistungen für die Abwehr von Bedrohungen aus dem Cyber- und Informationsraum unter dem Leitspruch: „Wir digitalisieren die Verwaltung".
Die Neugestaltung der IT des Bundes mit den nun breit aufgestellten Dienstleistern BWI-IT und ITZBund bietet die einmalige Gelegenheit, Erfahrungen mit der IT im öffentlichen Bereich des Bundes und speziell der Verteidigung zusammenzuführen, eine moderne aufgabengerechte IT zu entwickeln und einen effektiven IT–Betrieb einzurichten. Computacenter hat neben Lieferung, Installation und Betrieb von IT-Systemen bis hin zu Rechenzentren umfangreiche Kenntnisse und Erfahrungen beim Aufbau von privaten und öffentlichen Clouds, sowie bei der Gestaltung von Arbeitsplätzen der Zukunft. Wenn es um die Verarbeitung von VS-NfD Daten geht, bietet Computacenter Lösungen an, die vom BSI zugelassen sind. Beratungsleistungen gerade auch im Hinblick auf die neuen Herausforderungen aus dem Cyberraum sind ein weiterer Schwerpunkt. Mit einem der umfangreichsten Security-Portfolios im deutschen Markt, kann Computacenter der Bundeswehr nicht nur Beratung und Lösungen in den klassischen Bereichen Infrastructure Security und Endpoint Security anbieten, sondern auch zu den Themen Cyber Defense, Identity & Access Management und Information Security Management.
Auf der AFCEA-Fachausstellung konzentriert sich Computacenter auf die Themen

Computacenter auf der Bonner AFCEA-Fachausaustellung.
© HHK / Archiv

Arbeitsplatz der Zukunft, Interoperables Cloud Computing und sichere IT, mit Schwerpunkt Mobilität. Computacenter ist daher mit seinen langjährigen breit gefächerten Erfahrungen in allen Bereichen der öffentlichen Hand einschließlich der Verteidigung sowie als Halter wichtiger Rahmenverträge ein idealer Partner für die Weiterentwicklung der IT der Bundeswehr. Besuchen Sie uns auf dem Stand M23 im Saal MARITIM.

Deutschland digital fit machen

Rohde & Schwarz Cybersecurity bietet IT-Compliance nach europäischer Datenschutz-Grundverordnung an

Ab dem 25. Mai 2018 müssen Unternehmen den Anforderungen der europäischen Datenschutz-Grundverordnung (EU-DSGVO) nachkommen. Der IT-Sicherheitsexperte Rohde & Schwarz Cybersecurity bietet mit seinen Informationssicherheitsberatern des Solutions & Services-Teams Lösungen für die organisatorischen und technischen Herausforderungen der EU-DSGVO und unterstützt Unternehmen bei Vorbereitung, Analyse und Umsetzung der neuen Verordnung.

Die europäische Datenschutzgrundverordnung (EU-DSGVO) führt zu einem Paradigmenwechsel im Datenschutz und birgt große Chancen: Die Verordnung ist eine Modernisierung für wirksamen und konkreten Schutz personenbezogener Daten in Europa. Unternehmen haben die Chance mit Einhaltung der Richtlinien ihr Vertrauensverhältnis gegenüber Kunden, Partnern und Mitarbeitern zu untermauern. Im Zeitalter rasanter Digitalisierung und daten-getriebener Wirtschaft ist ein gewissenhafter und integrer Umgang mit Informationen unabdingbar – Geschäfte und Prozesse im Einklang mit der EU-DSGVO garantieren einen solchen Umgang.

„Wir bieten aktive Unterstützung bei der Umsetzung der EU-DSGVO für Unternehmen: Von der Beratung über die Vorbereitung zur Zertifizierung und Umsetzung bis zur EU-DSGVO-konformen Gestaltung von geeigneten Lösungen“, erklärt Helko Kögel, Director Consulting von Rohde & Schwarz Cybersecurity. Hierzu kooperiert das Team rund um Kögel mit erfahrenen Rechtsexperten. Bei Bedarf kann gleichzeitig das Datenschutzmanagement (Art. 42 DSGVO) und Informationssicherheitsmanagementsystem (ISMS) implementiert werden. Für die konkrete Umsetzung wird das Verarbeitungsverzeichnis (Art. 30 DS-GVO), die erforderlichen Erklärungen sowie eine Risikoeinstufung, die Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) und Maßnahmen zur Risikoeindämmung bei gleichzeitiger Verbesserung der IT- und Datensicherheit angeboten. „Mit dem 25. Mai 2018 ist es noch nicht getan“, unterstreicht Alexander Schellong, Vice President Solution & Services von Rohde & Schwarz Cybersecurity. „Wir wollen Unternehmen über die EU-DSGVO hinaus bei der Implementierung ihrer langfristigen Sicherheits- und Digitalisierungsstrategie und Compliance unterstützen.“

Rohde & Schwarz Cybersecurity schützt Unternehmen und öffentliche Institutionen vor Cyberangriffen

Das breite Lösungsportfolio des IT-Sicherheitsexperten Rohde & Schwarz Cybersecurity stellt darüber hinaus die erforderlichen Produkte und Lösungen mit Funktionen und durchgängigen Konfigurationsmöglichkeit für die Grundwerte des Datenschutzes und der Informationssicherheit bereit. Mehr Informationen erhalten Sie in der Webinar-Aufzeichnung „Die EU-DSGVO konkret umsetzen“: https://cybersecurity.rohde-schwarz.com/de/webinar-eu-dsgvo.

Mit Browser in the Box wird das Internet zum sichersten Ort der Welt

70% aller Cyberangriffe – wie Zero-Day-Exploits, Ransomware, Viren und Trojaner – erfolgen heute über einen Browser bzw. die besuchte Webseite. Heutige Schadcodes funktionieren immer über eine Verbindung zum Internet – so laden Makroviren Schadcode nach.

Ein vollvirtualisierter Browser schafft Abhilfe

Vollvirtualisierte Browser, wie der gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) für den Behördeneinsatz entwickelte Browser in the Box, verfolgen ein „proaktives“ Modell. Netzwerke werden konsequent getrennt und der Aufbau einer unbekannten und möglicherweise gefährlichen Internetverbindung zur „Nachladung“ von Schadcode wird verhindert. Durch eine Isolation des Intranets kann Schadcode selbst im Falle eines Angriffes, beispielsweise bei unabsichtlichem Download von Malware, nicht in das interne Netz vordringen. Gleichzeitig kann die Schadsoftware wie zum Beispiel Ransomware oder Makroviren keine Verbindung zum Internet herstellen, um die eigentliche Schadsoftware herunterzuladen. Statt eines separaten PCs für den Webzugriff wird ein virtueller PC auf dem Arbeitsplatz-PC erzeugt. Betriebssystem und Browser haben keinen direkten Zugriff

auf die Hardware, sondern lediglich auf die virtuelle Hardware, die wie eine zusätzliche Schutzmauer agiert.
Eindringende Viren, Trojaner und anderer Schadcode bleiben in dieser Umgebung eingeschlossen und können sich nicht auf dem Rechner und im lokalen Netzwerk verbreiten. Ein Neustart des Browsers erfolgt mit einem virenfreien Zustand.

Unabhängigkeit von Windows-Betriebssystemen schafft zusätzliche Sicherheit
Fast 88,6% aller Angriffe sind Windows-basierend. Die Gefahr, sich mit Schadcode zu infizieren, ist groß: Browser in the Box setzt auf Diversität und arbeitet unabhängig vom Windows-Betriebssystem.
Im Gegensatz zu mikrovirtualisierten Browsern verfügen vollvirtualisierte Browser über ein eigenes Betriebssystem und sind nicht mit dem Microsoft-Betriebssystem verzahnt. Bei Fremdkomponenten baut Rohde & Schwarz Cybersecurity mit seinem Browser in the Box ausschließlich auf Open Source. So kann der vertrauenswürdige und unabhängige Hersteller aus Deutschland auch auf Code-Level Analysen durchführen und die eingebauten Komponenten und Module laufenden Kontrollen und Prüfungen unterziehen.

Das IT-Sicherheitsunternehmen Rohde & Schwarz Cybersecurity schützt Unternehmen und öffentliche Institutionen weltweit vor Cyberangriffen. Mit hochsicheren Verschlüsselungslösungen, Next-Generation-Firewalls sowie Software für Netzwerkanalyse und Endpoint-Security entwickelt und produziert das Unternehmen technisch führende Lösungen für die Informations- und Netzwerksicherheit. Das Angebot der mehrfach ausgezeichneten und zertifizierten IT-Sicherheitslösungen reicht von kompakten All-in-one-Produkten bis zu individuellen Lösungen für kritische Infrastrukturen. Es umfasst außerdem Firewalls und Schwachstellenscanner für geschäftskritische Webanwendungen. Im Zentrum der Entwicklung von vertrauenswürdigen IT-Lösungen steht der Ansatz „Security by Design“, durch den Cyberangriffe proaktiv statt reaktiv verhindert werden. Über 500 Mitarbeiter sind an den Standorten in Deutschland, Frankreich und Dänemark tätig.

© https://cybersecurity.rohde-schwarz.com/de

rola.
SECURITY SOLUTIONS

AFCEA Fachausstellung 2018
Stand B11

Zusammenarbeit stärken, Sicherheit schaffen.

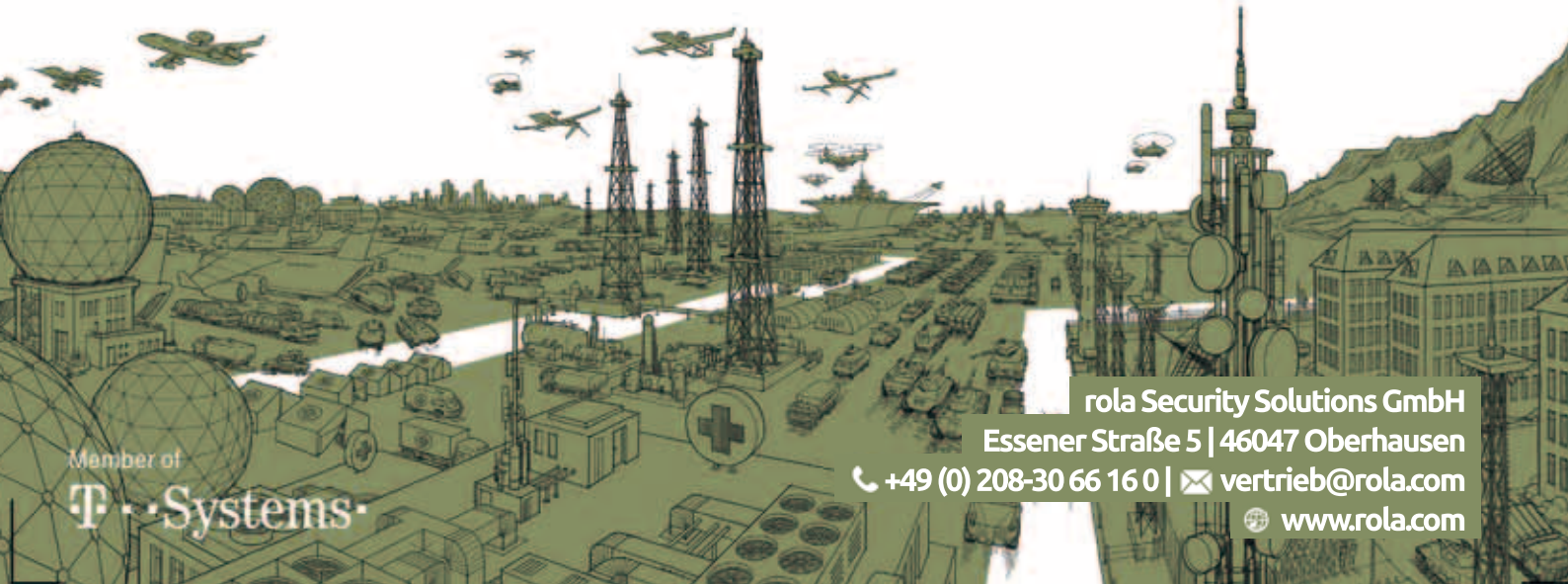
Jederzeit von jedem Ort auf die relevanten Informationen zugreifen zu können: Was vor wenigen Jahren noch als Wunschtraum in der Kriminalitätsbekämpfung galt, wird durch rola Securtiy Solutions zur Realität.

Im Rahmen komplexer Ermittlungen, Gefährdungsanalysen oder der Auswertung von Angriffen, kommt es darauf an, relevante Informationen zeitnah zu erkennen, zusammenzuführen und zu analysieren. Ohne diese Möglichkeiten trägt die reine Information im Zeitalter des Datenüberflusses kaum noch zur Problemlösung bei.

rola entwickelt, vertreibt und integriert seit 1983 IT-Verbundlösungen für die Innere und Äußere Sicherheit. Nationale und internationale Sicherheits- und Ermittlungsbehörden vertrauen unserer Kompetenz. Wir versorgen unsere Kunden mit intelligenten IT-Systemen, die auf den einzelnen Anwender zugeschnitten sind.

- Militärische Lagebilderstellung
- Analyse von Massendaten
- Auswertung Sozialer Medien
- Cyber Threat Intelligence

rsIntCent
rsExTract
rsNetMAn
rsCyInt



Member of T · · Systems ·

rola Security Solutions GmbH
Essener Straße 5 | 46047 Oberhausen
+49 (0) 208-30 66 16 0 | vertrieb@rola.com
www.rola.com