AFCEA 2017

BWI Informationstechnik

ISBN 978-3-934401-39-6

Behörden Spiegel-Gruppe
in Zusammenarbeit mit AFCEA Bonn e.V.

bechtle.com

KIRCHE & WOHLFAHRT

EUROPÄISCHE INSTITUTIONEN

GESUNDHEITSWESEN

KOMMUNEN & SCHULEN

Wer die besonderen Anforderungen öffentlicher Auftraggeber erfüllen will, muss sie verstehen. Dazu gehört die Fähigkeit, über den eigenen Horizont hinauszublicken. Bechtle handelt vernetzt, mit klarem Fokus auf die Zielgruppe – und ist als anerkannter Partner öffentlicher Auftraggeber etabliert. Europaweit.

Es geht immer ums Ganze.

BUND & LÄNDER

Die IT-Landschaft befindet sich im Wandel. Technologie verändert sich und mit ihr die Ansprüche der Kunden. Um hohe Ziele zu erreichen, brauchen öffentliche Auftraggeber einen Partner, der IT als Erfolgsfaktor versteht. Einen Dienstleister, der herstellerunabhängig moderne, sichere und effiziente Lösungen entwickelt, der zugleich mit traditionellen Werten wie Bodenhaftung, Beharrlichkeit, Zuverlässigkeit und Begeisterungsfähigkeit punktet. Und dabei nie den Blick fürs Ganze verliert. Für die Zukunft der Gemeinschaft.

ENERGIE & VERBÄNDE

FORSCHUNG & LEHRE

Bechtle GmbH & Co. KG
IT-Systemhaus Bonn/Köln
Friedrichsweg 18
53177 Bonn
Telefon +49 228 6088-0
bonn@bechtle.com

Ihr starker IT-Partner.
Heute und morgen.

BECHTLE

Ludwig Leinhos
Generalleutnant

Sehr geehrte Damen und Herren,

wir alle erleben es jeden Tag: Die Informationstechnik nimmt starken Einfluss auf unser Tun und Handeln, unsere Alltagsprozesse sind zunehmend digitalisiert. Ob Smartphone, Tablet oder Laptop – ständig bewegen wir uns in der Digitalen Welt. Wir sind in einer Digitalgesellschaft. Das Schlagwort "Industrie 4.0" fasst dies treffend für die digitalisierten Arbeitsprozesse zusammen, aber auch wir in der Bundeswehr profitieren von dieser Digitalisierung, wir sind Teil der "Inneren und Äußeren Sicherheit 4.0".

Diese bietet großartige Chancen und Annehmlichkeiten, birgt aber auch Risiken für jeden Einzelnen, Staat und Gesellschaft. Vorfälle wie der "Bundestaghack" oder der erst vor kurzem stattgefundene Angriff auf die Telekom haben die Verwundbarkeit im Cyber- und Informationsraum plakativ gezeigt. Die Reihe der Beispiele ließe sich fortsetzen. Klar ist, dass Zahl und Qualität der Cyberangriffe und Maßnahmen im Informationsumfeld in den letzten Jahren mit exponentieller Geschwindigkeit zugenommen haben, eine Kehrtwende dieses Trends ist nicht zu erwarten, im Gegenteil.

Die Bundeswehr nimmt diese Bedrohungen sehr ernst und stellt sich mit der Aufstellung eines eigenen Organisationsbereiches schlagkräftig und modern gegen Gefahren aus dem Cyber- und Informationsraum auf. Wir sind uns aber sehr wohl bewusst, dass erfolgreiche Abwehr von Cyberangriffen eine umfassende, ressortübergreifende enge Zusammenarbeit erfordert. Die Bundeswehr leistet daher auch im Cyber- und Informationsraum einen Beitrag zur gesamtstaatlichen Sicherheitsvorsorge. Auch wir wollen von den Möglichkeiten der Digitalisierung profitieren, gleichzeitig aber die Risiken minimieren. Wir bauen vorhandene Cyber-Fähigkeiten der Bundeswehr aus, schaffen neue Fähigkeiten, strukturieren und konsolidieren diese – immer im gesetzlichen Rahmen.

Deshalb begrüße ich es, dass sich AFCEA Bonn e.V. diesem Jahresschwerpunkt widmet und gemeinsam mit Experten aus Wissenschaft, Wirtschaft, Politik und Militär über "Innere und äußere Sicherheit 4.0 – Schlüssel zur digitalen Souveränität" diskutiert. Mein Team und ich freuen sich auf interessante und gewinnbringende Gespräche mit Ihnen auf den zahlreichen Veranstaltungen.

Ihr Ludwig Leinhos
Inspekteur Cyber- und Informationsraum

Impressum: Sonderheft Behörden Spiegel "AFCEA 2017" **Redaktionelle Leitung:** Reimar Scherz, Behörden Spiegel, Telefon: 0228 / 970 97-83 **Herausgeber** (presserechtlich verantwortlich): R. Uwe Proll, Behörden Spiegel-Gruppe **Verlegt** von der ProPress Verlagsgesellschaft mbH, Berlin/Bonn **Anzeigen:** Beatrix Lotz, Helga Woll **Herstellung:** Spree Service- und Beratungsgesellschaft mbH, Berlin **Satz und Layout:** Cornelia Liesegang, Behörden Spiegel **Fotos:** Autoren, AFCEA Bonn e.V., BWI Informationstechnik GmbH, Behörden Spiegel Archiv **Druck:** KÖLLEN DRUCK & VERLAG GMBH, Bonn **Heftpreis:** 7,50 Euro ©Alle Beiträge (Wort und Bild) in diesem Heft sind urheberrechtlich geschützt. Eine Weitergabe – auch digital – bedarf der Einwilligung des Verlages. www.behoerdenspiegel.de

AFCEA 2017

1. AFCEA Bonn e.V. – ein zuverlässiger Partner

Innere und äußere Sicherheit 4.0 – Schlüssel zur digitalen Souveränität
Generalmajor a.D. Erich Staudacher . . . . . Seite 6

Die Infoseite zu AFCEA-Preisen und Veranstaltungen . . . . . Seite 8

AFCEA Fachausstellung in neuem Ambiente
Friedrich W. Benz. . . . . . Seite 10

Cyber-Sicherheitsarchitektur 4.0 – Schlüssel zur digitalen Souveränität
Andreas Höher . . . . . Seite 13

Cyber- und Informationsraum – Äußere Sicherheit und Verteidigung 4.0?
Oberst i.G. Armin Fleischmann . . . . . Seite 15

Industrie 4.0 aus Industrieperspektive
Cyber-Abwehr in der Industrie 4.0: Der Mensch bleibt im Mittelpunkt
Götz Piwinger . . . . . Seite 17
Perspektiven der Cybersicherheit im Internet der Dinge
Alfred Saal . . . . . Seite 18

Innere Sicherheit 4.0 – Gibt es die?
Tobias Schönherr . . . . . Seite 20

Sichere Luftfahrt der Zukunft: IT als ein wichtiger Schlüssel
Generalmajor Dr. Ansgar Rieks . . . . . Seite 22

2. BWI Informationstechnik

HERKULES: ein starkes Fundament für die Zukunft
Michael Krause, Mitglied der Geschäftsleitung für den Geschäftssbereich Account Management, BWI Informationstechnik GmbH . . . . . Seite 28

Proaktiv, ganzheitlich und stark
Im Gespräch: Ulrich Meister, Vorsitzender der Geschäftsführung der BWI Informationstechnik GmbH . . . . . Seite 31

Die neue BWI – eine Organisation für die Zukunft
Dr. Jürgen Bischoff, Geschäftsführer Corporate Human Resources der BWI Informationstechnik GmbH . . . . . Seite 34

Das Management-Team der BWI . . . . . Seite 38

Innovation als Schlüssel zum Erfolg
Markus Hauff, Leitung Innovation & Portfolio Strategy, BWI Informationstechnik GmbH . . . . . Seite 40

Gut aufgestellt für neue Herausforderungen
Drei Delivery-Bereiche übernehmen die Leistungserbringung der BWI:
User Communication Services, Cloud Infrastructure Services und Business Consulting & Application . . . . . Seite 42

User Communication Services
André Prekop, Mitglied der Geschäftsleitung der BWI Informationstechnik GmbH
für den Geschäftsbereich User Communication Services . . . . . Seite 44

Cloud Infrastructure Services
Robert Knapp, Mitglied der Geschäftsleitung der BWI Informationstechnik GmbH
für den Geschäftsbereich Cloud Infrastructure Services. . . . . . Seite 46

Business Consulting & Application
Christine Serrette, Mitglied der Geschäftsleitung der BWI Informationstechnik GmbH
für den Geschäftsbereich Business Consulting & Application. . . . . . Seite 48

Gute Perspektiven für Soldaten bei der BWI
Im Porträt: Dr. Christian Marwitz, Mitglied der Geschäftsleitung der BWI Informationstechnik GmbH
und ehemaliger Zeitsoldat . . . . . Seite 50

3. Weitere Beiträge

Digitale Schockwellen
Jörn Becker, Leiter Civil & National Security – Business & Platform Solutions, Atos Deutschland
Hubert Geml, Leiter Verteidigung, Innere Sicherheit, Atos Deutschland . . . . . Seite 54

4. AFCEA-Fachausstellung

AFCEA-Symposium . . . . . Seite 57

Ausstellerliste . . . . . Seite 58

Standplan . . . . . Seite 60

Firmenprofile . . . . . Seite 62

Innere und äußere Sicherheit 4.0 – Schlüssel zur digitalen Souveränität

Generalmajor a.D. Erich Staudacher, Vorsitzender AFCEA Bonn e.V.

Erich Staudacher
Generalmajor a.D.
Foto: Privat

Sind wir noch souverän?

Die Beeinflussung des US-Wahlkampfes, Hackerangriffe auf die NATO-Website, Cyberangriffe auf militärische Systeme, oder der Fall Lisa – all diese Ereignisse besitzen Gemeinsamkeiten. Immer zielten die Urheber auf die Handlungsfreiheit des betroffenen Staates.

Unter Zuhilfenahme des Cyber-Raumes sind die Möglichkeiten der schädlichen Einflussnahme auf die Bundesrepublik Deutschland unzweifelhaft gewachsen. Und sie wachsen weiter.

Nach den Cyberaktionen im US-Wahlkampf dürften die Verursacher zu noch mehr fähig sein. Nicht nur Deutschland, sondern viele westliche Staaten, scheinen hier nur bedingt abwehrbereit.

Innere und äußere Sicherheit stehen vor neuen Herausforderungen

Das Austesten der Resilienz unserer Gesellschaft, die Angriffe auf staatliche Organe und die Einsatzfähigkeit der Streitkräfte sind erst der Anfang. Eigentlich positive technologische Entwicklungen wie Big Data in Verbindung mit dem Internet of Things bergen auch neue Anfälligkeiten für Daten-Manipulation und -Störungen.

Deshalb müssen Abwehrschritte sowohl in den Cyber-Abwehrzentren als auch auf politischer Ebene und in Beschaffungsprozessen schneller ablaufen. Neue (Entscheidungs-)Strukturen und verbesserte technische Möglichkeiten sind gefordert. Gleichzeitig ist Prävention noch wichtiger als ein Analysieren stattgefundener Cyber-Attacken. Das verlangt Kenntnisse, die nur aktiv zu erwerben sind. Daher dürfen offensive Operationen im gegebenen rechtlichen Rahmen kein Tabu sein.

Allmählich entwickelt sich auch in Deutschland ein entsprechendes Bewusstsein, ebenso die Erkenntnis, dass innere

AFCEA Vorstand und Aufgaben

Geschäftsführender Vorstand

Vorsitzender
Erich Staudacher

Stv. Vorsitzender, Vorsitzender Programmbeirat
Dr. Ansgar Rieks

Stv. Vorsitzender und Vertreter Industriebeirat
Joachim Mörsdorf

Vertreter Beirat Bundeswehr
Hans-Ulrich Schade

Vertreterin Arbeitskreis Young AFCEANs
Katja Frintrop

Geschäftsführer, Schatzmeister, Veranstaltungsmanagement
Christian Hartrott

Weitere Mitglieder

Vertreter Arbeitsgruppe BOS
Andreas Höher

Vertreter Arbeitskreis Berlin
Armin Fleischmann

Beauftragter Fachausstellung
Friedrich W. Benz

Vertreter Arbeitsgruppe Internationales
Wolfgang Taubert

Vertreter Arbeitskreis Medien, Pressesprecher
Jochen Reinhardt

Vertreter Beirat Wissenschaft
Dr. Michael Wunder

Schriftführer
Götz Stuck

Industriebeirat
Franz Bernd Möllers

Arbeitsgruppe BOS
Tobias Schönherr

AFCEA Bonn e.V. hat seine Vorstandsarbeit um thematische Beiräte ergänzt. Sie stellen jeweils einen Vertreter im Vorstand. Damit will sich die gemeinnützige Informationsplattform besser auf den Austausch mit ihren Mitgliedern konzentrieren und eine bessere Informationsaufbereitung in den Kernthemen erreichen. Zu den Beiräten gehören die Gremien Programmbeirat, Industriebeirat, der Arbeitskreis Young AFCEANs sowie die Jury des AFCEA Studienpreises.

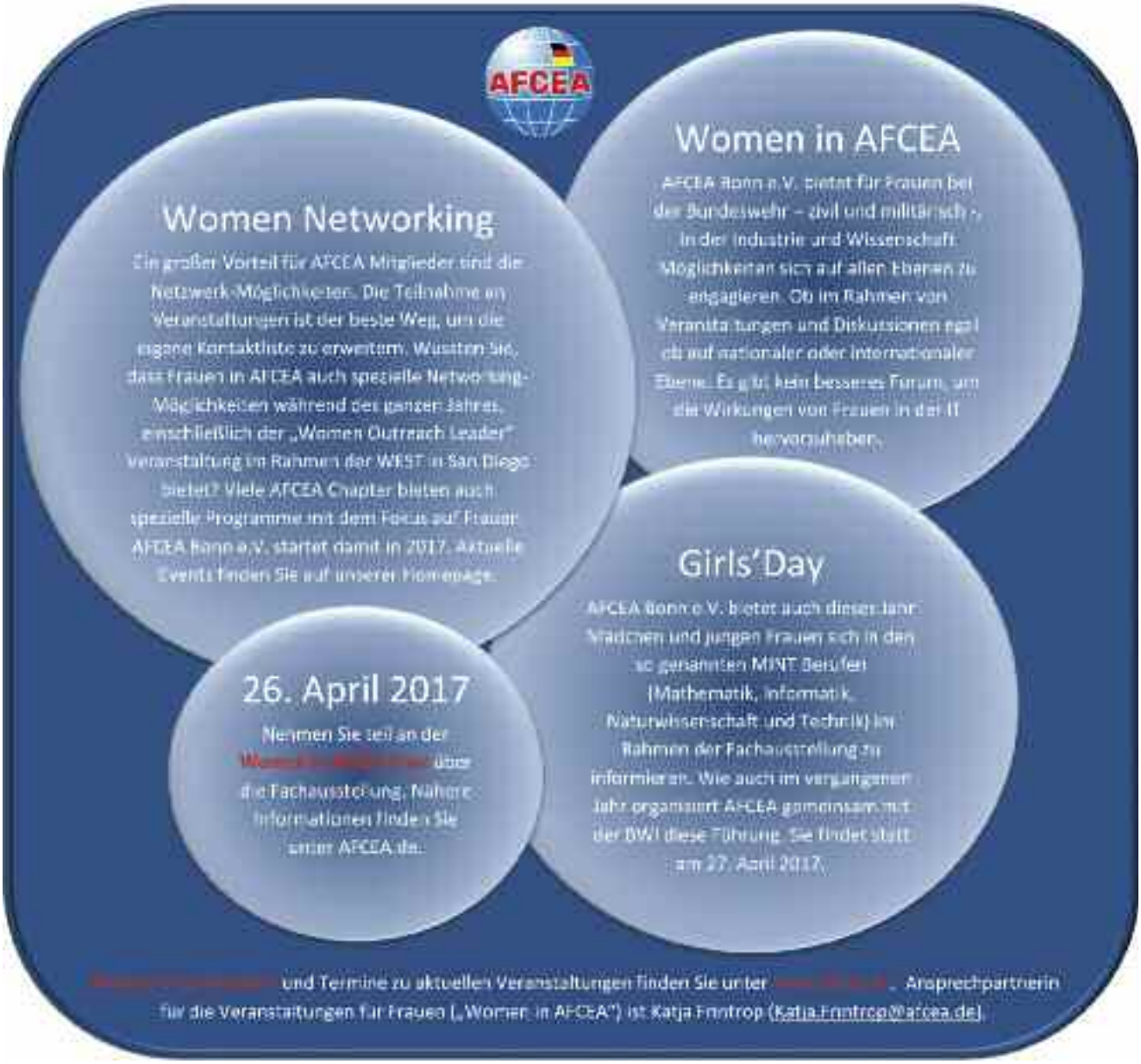
und äußere Sicherheit auf keinem Gebiet so eng verbunden sind wie hier im Cyber-Raum.

Es gibt noch mehr zu tun!

Staatliche und nicht-staatliche Institutionen müssen sich besser vernetzen, um das Bewusstsein um den Cyber-Raum zu verbessern und Talente zu fördern. Cyber-Hygiene muss als ein “whole-of-a-nation”-Ansatz bis hinein in die Schulen getragen werden. Hackathons sind als sportliche Erfahrung in den Dienst der Gemeinschaft zu stellen.
Für die Immunisierung gegen Cyber-Angriffe, sowohl auf gesellschaftlicher wie individueller Ebene, sind viele verknüpfte Wege denkbar: Lernen aus Fehlern, hochentwickelte technische Abwehr, gesetzliche Verhaltensregeln.

Was AFCEA einbringt

Sicher fallen nicht alle Fragen in die Kompetenz von AFCEA Bonn e.V. Doch wir können als gemeinnützige, unparteiische Organisation bei der Bewusstwerdung unterstützen und kritischen Fragen sowie Antworten Raum bieten. In insgesamt 20 hochwertigen Veranstaltungen unseres Jahresprogrammes werden wir kompetente Vertreter von Amtsseite, Industrie und Wissenschaft zu Wort kommen lassen. Markante fachlich-technische und operative Beiträge sowie wechselseitig nutzbare Hochtechnologie-Lösungen für äußere und innere Sicherheit zu erörtern, ist unser AFCEA-Beitrag zum Schutz der Souveränität! Auf die Begegnung dabei mit Ihnen, verehrte Leser, freuen wir uns.



Die Infoseite zu AFCEA-Preisen und Veranstaltungen

“Wissenschaftliche Auslese”

Preise für wissenschaftliche Arbeiten gibt es viele. Aber wenige, die einen Bezug zur Wehrtechnik haben und die dabei auch noch so gut honoriert werden. AFCEA Bonn e.V. beteiligt die Hochschulen im unmittelbaren räumlichen Wirkungskreis des Vereins und natürlich beide Bundeswehruniversitäten, weil sie dem thematischen Fokus des Vereins, nämlich Verteidigung und Sicherheit entsprechen.

Auch weil das Wort Eliten in Deutschland zwiespältig diskutiert wird, will der Verein bewusst eine Auslese wissenschaftlicher Spitzenleute für ihre Leistungen auszeichnen. Unser Land braucht diese wissenschaftliche Elite und muss sie fördern – AFCEA Bonn e.V. leistet dazu seinen Beitrag und vergibt den jährlich mit insgesamt 15.000 Euro dotierten AFCEA Bonn e.V. Studienpreis. Seit 2008 sind damit über 100.000 Euro an 36 Preisträger ausgeschüttet worden.

Young AFCEANs: Ausgezeichnete Angebote

AFCEA bietet für Mitglieder bis 40 Jahre (Young AFCEANs) neben dem Angebot der Fachausstellung, der Koblenzer IT-Tagung und Fachveranstaltungen weitere besondere Aktivitäten: Zum Vernetzen und Austauschen werden den jungen Fach- und Führungskräften sowie Hochschulabsolventen eigene Fach- und Karriereveranstaltungen im Bonner sowie Berliner Raum angeboten.
Aktivitäten mit anderen AFCEA Chaptern – vor allem mit Young AFCEANs aus Kaiserlautern und dem Eifeler Chapter – ergänzen das Angebot. Gemeinsam besuchen sie beispielsweise Forschungslabore verschiedener IT-Firmen, die CeBIT oder die Air Base Ramstein.
Darüber hinaus gibt es seit 2015 die European Young AFCEANs Conference, die die Möglichkeit des fachlichen Austausches auf europäischer Ebene bietet. Nach der Premiere in Berlin ist die zweite Konferenz im Rahmen der TechNet Europe 2017 in Stockholm, Schweden vom 16. bis 18. Oktober 2017 derzeit in Planung. Wer Interesse hat, bei der Organisation der Konferenz zu unterstützen, ist herzlich willkommen (Kontaktdaten siehe unten).
Für den ganz jungen Nachwuchs – Mädchen und Jungen im Alter zwischen 10 und 16 Jahren - bietet AFCEA Bonn e.V. auch in diesem Jahr die Möglichkeit an, in Kooperation mit der BWI im Rahmen des Girls’Day am 27. April 2017 verschiedene Firmen auf der Fachausstellung kennenzulernen.

Weitere Informationen und Termine zu aktuellen Veranstaltungen findet Ihr unter www.afcea.de. Ansprechpartnerin für die Young AFCEANs Veranstaltungen ist:
Katja Frintrop (Katja.Frintrop@afcea.de).

Die verlässliche Referenz für Beobachtung und Ortung – weltweit

Der Name Vectronix steht im Marktsegment elektrooptischer Entfernungsmesser für hochstehende Premiumprodukte. Professionelle Anwender weltweit vertrauen auf die Geräte des in der Ostschweiz ansässigen Herstellers.
Die Firmengeschichte des Schweizer Traditionsunternehmens reicht bis ins Jahr 1921 zurück, als die Firma unter dem Name Wild Heerbrugg gegründet wurde. In den 1990er Jahren erfolgte die Umbenennung in Leica. 2003 wurde Vectronix als selbständige Firma gegründet und noch im gleichen Jahr von der französischen Safran-Gruppe übernommen. Der Firmensitz befindet sich weiterhin im St. Galler Rheintal, wo die Firma über 4.000 m² Produktionsfläche verfügt.
Die Safran Vectronix AG verbessert kontinuierlich die Qualität ihrer Produkte. Sie bringt innovative und technisch hochstehende Neuerungen auf den Markt. Die Effizienz interner Prozesse, sowie die Mitarbeiterzufriedenheit tragen zum Erfolg bei. Es ist nicht die zentrale Frage der Firma, wie Preise gesenkt werden können, sondern wie spezifisch auf die komplexen Bedürfnisse der Kunden eingegangen werden kann. Mit diesem Mehrwert hebt sich Vectronix von den Mitbewerbern ab.

MOSKITO TI

Das Multifunktionsgerät darf als der weltweit modernste Distanzmesser bezeichnet werden. Es sind nicht nur die zehn Kilometer, die das MOSKITO TI (Thermal Imager) mit einem augensichern Laser vermisst. Insgesamt verfügt das intuitiv zu bedienende Beobachtungs- und Aufklärungsgerät über neun Funktionen. Einsatzkräfte können Missionen effizienter und mit weniger Eigengefährdung durchführen. Das MOSKITO TI bringt knapp 1,3 Kilogramm auf die Waage und ist unwesentlich größer als ein herkömmliches Beobachtungsfernglas der Dimension 8x50. Ein maßgeblicher Erfolgsfaktor der Safran Vectronix AG erklärt sich dadurch, dass die Produktentwickler eine enge Vernetzung zu Angehörigen von Kampf-, Aufklärungseinheiten und Spezialkräften pflegen. Vectronix Ingenieure leisten zum Teil selber Milizmilitärdienst und wissen daher aus erster Hand, dass der moderne Infanterist eine leichte Ausrüstung bevorzugt. Die Ausbildungszeit vor dem Einsatz ist eine knappe Ressource. Der Anwender muss das Gerät bereits nach kurzer Einweisung unter erschwerten Bedingungen sicher bedienen können. Trotz einer Vielzahl an Funktionen ist es Vectronix gelungen, die MOSKITO TI Bedienung einfach zu halten. Funktionsknöpfe sind ergonomisch und robust angeordnet. Doppel- oder Dreifachfunktionen wurden vermieden.

Funktionen

Neben der Grundfunktion “Distanzmessen” verfügt das MOSKITO TI über einen ungekühlten Wärmebildsensor mit einem Sehfeld von 213 mil. Der Glaskanal besitzt eine 6-fach Vergrößerung und ein Sehfeld von 111 mil; genauso wie die integrierte Low-Light Kamera mit aktivem Pixelsensor (CMOS). Der digitale Magnetkompass misst Lage und Neigungswinkel auf sieben mil bzw. drei mil genau. Ein augensicherer Infrarot Laser Pointer (840 nm) erlaubt eine optische Zielzuweisung mit Nachtsichtgeräten. Das integrierte Satellitennavigationssystem arbeitet auf Basis von NAVSTAR oder Military GPS, Galileo oder GLONASS. Mit der integrierten digitalen Bild- und Videoverarbeitung können Aufklärungsergebnisse in Echtzeit übertragen werden. Es stehen Standardschnittstellen (RS-232 / USB / Ethernet) sowie eine kabellose Bluetooth-Übertragung zur Verfügung. C4I-Funktionen (Command, Control, Computers, Communications, Information) des Führungsinformationssystems stellen die Vernetzbarkeit sicher.
Durch eine Kombination mit seinen Einzelfunktionen kann das MOSKITO TI exakte Zielkoordinaten vermessen. Die Feuerunterstützung für Bogenschusswaffen wird dadurch erheblich vereinfacht. MOSKITO TI ist weltweit führend unter den Aufklärungsgeräten.

Kompakt und multifunktional – entwickelt für die komplexen Anforderungen moderner Sicherheitskräfte.

AFCEA Fachausstellung in neuem Ambiente

Friedrich W. Benz, Leiter AFCEA Fachausstellung, Vorstand AFCEA Bonn e.V.

Friedrich W. Benz

30 Jahre lang führte AFCEA Bonn ihre Fachausstellung in der Stadthalle Bad Godesberg durch. Mit der Fachausstellung 2016 endete dort die Ära der AFCEA Fachausstellungen, denn selbst unter Ausnutzung der Ausstellungsflächen in allen Räumen und in einem nochmal erweiterten Zelt auf der Terrasse konnte nicht allen interessierten Firmen ein Ausstellungsstand angeboten werden. Deshalb entschied der Vorstand von AFCEA Bonn e.V., die AFCEA Fachausstellung, Treffpunkt der IT-Community der Bundeswehr und der an der Bundeswehr und BOS interessierten Unternehmen, in den nächsten Jahren im Maritim Hotel Bonn durchzuführen.

Anfänge der AFCEA Fachausstellung

1983, nach der Gründung von AFCEA Bonn e.V. als erstes deutsches Chapter der bereits 1946 in den USA von amerikanischen Fernmeldern gegründeten AFCEA (Armed Forces Communication Electronics Association), stellte sich die Frage, wie die Betriebskosten für den Verein künftig bestritten werden sollen. Da die Zielsetzung des Vereins war, den Informationsaustausch zwischen Bedarfsträgern und Bedarfsdeckern, zwischen Anwendern und Herstellern im Bereich der Führungsunterstützung (Funkgeräte und andere Fernmeldemittel, Führungs- und Fachinformationssysteme, Gefechtsstände und Gefechtsstandtechnik, etc.) zu intensivieren, lag nahe, die neuesten Produkte der Hersteller in einer Ausstellung dem interessierten Fachpublikum zu präsentieren.

Mit seiner Anregung “Wir müssen mal etwas Hardware zeigen!” in einer Vorstandssitzung 1985, hatte das damalige Vorstandsmitglied Rainer Ramin, zu diesem Zeitpunkt Referatsleiter im Amt für Datenverarbeitung der Bundeswehr, gleich den Auftrag, eine diesbezügliche Ausstellung zu organisieren und wurde so zum “Erfinder”, Motor und Leiter der AFCEA Fachausstellung. Bei der ersten Ausstellung 1986 in der Stadthalle Bad Godesberg stellten 14 Firmen aus, unter anderem Nixdorf, Wang und einige Softwarehäuser wie GEI und Ploenzke. Diese erste wirkliche Großveranstaltung des Vereins AFCEA Bonn e.V. war ein großer Erfolg. Besonders ein Satz aus der Rede von Staatssekretär Prof. Dr. Manfred Timmermann, der mit einem Vortrag die Ausstellung eröffnete, war Balsam für den Vorstand. Er sagte “Wenn es AFCEA noch nicht gäbe, müsste der Verein erfunden werden”.

Die neue Location der AFCEA Fachausstellung: Das Maritim Hotel Bonn *Foto: Maritim Bonn*

20 Prozent mehr Ausstellungsfläche *Grafik: Benz / AFCEA*

Entwicklung der AFCEA Fachausstellung über 30 Jahre

Was 1986 mit 14 Ausstellern im Großen Saal der Stadthalle begann, entwickelte sich in den folgenden Jahren erfreulich dynamisch weiter. Immer mehr Aussteller suchten die Plattform der AFCEA Fachausstellung, um ihre Produkte und Dienstleistungen dem Kunden Bundeswehr und den BOS zu präsentieren und füllten mit ihren Ständen nach und nach alle Räume der Stadthalle. Im Laufe der Jahre hat sich die AFCEA Fachausstellung zur anerkannten Dialogplattform der IT-Community Bundeswehr/BOS entwickelt, bei der die Aussteller eine Vielzahl von Ansprechpartnern aus einer großen Anzahl von Dienststellen erreichen. Vor allem Konzeptionäre der Bedarfsträger und Projektleiter/-mitarbeiter der Bedarfsdecker schätzen das umfassende Informationsangebot. Aber auch für die Business-to-business (B2B)-Aktivitäten zwischen den Firmen spielt die Fachausstellung eine nicht zu unterschätzende Rolle.

2007 stellten bereits 70 Firmen aus. Trotz Wirtschaftskrise ging auch unter dem neuen Leiter der Fachausstellung, Oberst a.D. Friedrich W. Benz, der Aufwärtstrend unverändert weiter, so dass zur Erweiterung der Ausstellungsflächen sogar ein Zelt auf der Terrasse und das Basement als neue Ausstellungsfläche herangezogen wurden. 2016 stellten, bei erstmals um 150 qm vergrößertem Zelt, insgesamt 114 Aussteller aus, was einen neuen Ausstellerrekord bedeutet. Unter dem Eindruck der Bedrohung in der vernetzten Welt sind in den letzten Jahren mehr und mehr Firmen aus dem Bereich der IT-Sicherheit zu den Ausstellern gestoßen, aber auch Firmen mit Anwendungen zur Nutzung von Geodaten. Ruggedized Laptops und Tablets, abstrahlarme Hardware, SASPF und Ausbildung sind schon lange Jahre Themen, die bei der AFCEA Fachausstellung zuhause sind. Und der An–drang, bei der AFCEA Fachausstellung Aussteller zu werden, hält unvermindert an.

Maritim Hotel Bonn als neue Location

Da die Zeltlösung zur Erweiterung der Ausstellungsflächen der Stadthalle nur ein Notbehelf war, hat sich AFCEA Bonn e.V. schon seit längerem mit Alternativen zum Ausstellungsort beschäftigt. Naheliegend war die Nutzung des neu erbauten World Conference Centers Bonn, mit guten Ausstellungsflächen, dem ehemaligen Bundestag als geschichtsträchtigen Vortragsraum sowie eine für die Fachausstellung rundum ideale Infrastruktur. Im Herbst 2009 waren die Planungen für die Fachausstellung 2010 im World Conference Center Bonn (WCCB) nahezu abgeschlossen, als der Baustopp diese Alternative hinfällig werden ließ. Nach der Fertigstellung 2015 konnte das WCCB wegen der Verpflichtungen gegenüber der Vereinten Nationen zur Durchführung von Klimakonferenzen für die AFCEA Fachausstellung bedauerlicherweise keine Ausstellungstermine in den gewünschten Zeiträumen anbieten.

Somit mussten weitere Alternativen gesucht werden. Diese wurde im Maritim Hotel Bonn als neue Location der AFCEA Fachausstellung gefunden. Obwohl das Hotel, wie zuvor die Stadthalle, keine ideale Ausstellungslocation ist, bietet es großzügige Räume und Foyerflächen, und ein angenehmes Ambiente für die traditionelle Ausstellung.

Mit Ständen im Saal Maritim, im Saal Beethoven und im Saal Schumann sowie auf den verbindenden Foyerflächen konnte im Vergleich zur Stadthalle Bad Godesberg 20 Prozent mehr Ausstellungsfläche angeboten werden. Für die

Vorträge im Rahmen des begleitenden Symposiums wird der Saal Reger genutzt werden. Zudem bietet das Hotel weitere Annehmlichkeiten: Aussteller und Besucher können im gleichen Gebäude übernachten und haben somit einen kurzen Weg zur Ausstellung. Parkplätze stehen im Hotel und um das Hotel zur Verfügung. Zusätzlich ist geplant, vor dem Maritim Hotel Bonn, auf der nahegelegenen Jean-Monnet-Straße und Heinemannstraße, in der Rheinaue und an der Petra-Kelly-Allee weitere Sonderparkflächen für Besucher der AFCEA Fachausstellung einzurichten.

Nach 30 Jahren Stadthalle ist die Fachausstellung im Maritim Hotel Bonn in gewisser Weise ein Neuanfang. Über die letzten Jahre und Jahrzehnte hat sich bei der Fachausstellung ein treuer Stamm von Ausstellern herausgebildet. Mehr als 80 Prozent der Aussteller nahmen jedes Jahr wieder an der Ausstellung teil und dies an dem angestammten Ausstellungsstand. Mit dem Wechsel in das Maritim Hotel Bonn begann für die Aussteller das Rennen um die vermeintlich besten Platzierungen für die Ausstellungstände. In einem etwas längeren Verfahren ist es gelungen, eine einvernehmliche Lösung für die “Startaufstellung” für die erste Fachausstellung in der neuen Location zu finden. Auch wenn sich die Umgebung etwas geändert hat, geht AFCEA Bonn e.V. davon aus, dass die IT-Community Bundeswehr und BOS den neuen Ausstellungsort positiv annehmen wird. Die Steigerung der Ausstellungsfläche um mehr als 20 Prozent ist dafür ein gutes Indiz.

Zudem kommt AFCEA Bonn mit der neuen Location in besonderem Maße auf den Kunden Bundeswehr zu: ganz in der Nähe liegt die neu geschaffene Dienststelle des Kommandos Cyber und Informationsraum, deren ersten Aktivitäten von der Community aufmerksam beobachtet und verfolgt werden und deren Mitarbeiter einen besonders kurzen Weg zur AFCEA Fachausstellung haben.

Cyber-Sicherheitsarchitektur 4.0 – Schlüssel zur digitalen Souveränität

Andreas Höher, msg systems AG, Vorstand AFCEA Bonn

Andreas Höher

Die Digitalisierung ist geprägt durch die Möglichkeit, über das Internet als Dateninfrastruktur alles und jeden miteinander zu vernetzten. Insbesondere die rasante Entwicklung der Anzahl der vernetzungsfähigen Geräte (Internet of Things) wird den Trend in Richtung vernetzter Welten und Industrie 4.0 fortsetzen. Statistische Erhebungen des Dienstleisters Statista prognostizieren für das Jahr 2020 weltweit 50,1 Milliarden vernetzter Geräte. Man spricht hier schon vom "Internet of Everything", das heißt von der Vernetzung von Menschen, Prozessen, Daten, Maschinen, Geräten und Sensoren, die über das Internet miteinander kommunizieren.

Die Digitalisierung verfolgt dabei keinen Selbstzweck, sondern ist das wirksamste Mittel zur Steigerung der Wettbewerbsfähigkeit der Wirtschaft quer durch alle Segmente. Die Digitalisierung legt damit die Grundlagen für den Wohlstand künftiger Generationen, für gesellschaftliche Teilhabe und staatliche Handlungsfähigkeit. Doch neben aller Euphorie über technologische Möglichkeiten und der Notwendigkeit, diese Technologien einzusetzen, lauern auch vielfältige Gefahren.

Gerade Beispiele aus der jüngsten Vergangenheit zeigen, dass unsere digitale Souveränität, also im digitalen Raum als Staat, Unternehmen oder Individuum sicher, frei und selbstbestimmt handeln und entscheiden zu können, bedroht zu sein scheint. So kam es beispielsweise durch Hacker-Angriffe auf eine Vielzahl von Unternehmen, teils auch öffentlichen Einrichtungen und private Nutzer zur Verbreitung von Kryptotrojanern/Schadsoftware, sogenannte Ransomware, welche darauf abzielt, die Daten eines Nutzers so zu verschlüsseln, dass dieser nur nach Zahlung eines Lösegeldes wieder auf seine Daten zugreifen kann.

Auch Attacken durch sogenannte Bot-Netze, das heißt automatisierte Computerprogramme (Bots), die meist Hacker über das Internet auf privaten Geräten wie Computer, Smartphones oder Tablets installieren, zu Netzwerken zusammenschließen und dann unbemerkt vom Nutzer zentral für ihre Angriffe steuern, etwa um durch Massenanfragen (Spam-Phishing-Mails) gezielt Server lahmzulegen oder Bank- und Kreditkartendaten zu stehlen, machten in 2016 von sich reden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ging bereits im 1. Quartal 2015 davon aus, dass es im Zusammenhang mit Bot-Netzen zu mehr als 60.000 Neuinfektionen täglich kommt, Tendenz steigend.

Es ist damit ebenfalls leicht nachvollziehbar, dass Cyber-Angriffe auf sogenannte Kritische Infrastrukturen (Energie, Gesundheit, IT und TK, Transport und Verkehr, Medien und Kultur, Wasser, Finanz- und Versicherungswesen, Ernährung, Staat und Verwaltung) sehr reale kriminelle, extremistische/terroristische, militärische oder nachrichtendienstliche Bedrohungen von weitreichender Tragweite darstellen.

Eine ganz neue "Qualität" haben hingegen die automatisierten Meinungsplatzierungen durch Social Bots und sogenannte Fake News mit dem Ziel der gezielten Einflussnahme, so geschehen im US-Wahlkampf. Social Bots, maschinell gesteuerter Social Media Accounts, stellen dabei auf der technologischen Grundlage der Bot-Netze eine legale Komponente einer Social Media Kampagne dar. Im US-Wahlkampf haben mindestens 33 Prozent der über die Social Media verbreiteten Pro-Trump Tweets ein Computerprogramm als Absender![1] Das BSI hält es ebenfalls für möglich, dass diese Manipulationen ebenfalls in Deutschland bei den in 2017 bevorstehenden Landtags- und insbesondere bei der Bundestagswahl auftreten können und Vorsorge gegen Wahlmanipulationen erforderlich ist.

Wie also bewahren wir uns als Staat, Unternehmen und Bürger unsere digitale Souveränität?

Bereits im Koalitionsvertrag hat sich die Bundesregierung der Wahrung und Rückgewinnung technologischer Souveränität zum Ziel gesetzt. Zu diesem Zwecke wurde die Cyber-Sicherheitsstrategie aus dem Jahre 2011 überarbeitet und im November 2016 als Cyber-Sicherheitsstrategie 2016 vom Bundeskabinett beschlossen. Diese stellt die ressortübergreifenden strategischen Aktivitäten der Bundesregierung zum Thema Cyber-Sicherheit dar.

Einen Schwerpunkt der vier Handlungsfelder umfassenden Cyber-Sicherheitsstrategie bildet der Aufbau einer leistungsfähigen und nachhaltigen gesamtstaatlichen Cyber-Sicher-

Akteure der Cyber-Sicherheitsarchitektur *Grafik: Höher /AFCEA*

heitsarchitektur (Handlungsfeld 3).

Mit dieser wird die gezielte Verzahnung von Organisationen und Einrichtungen mit Cyber-Sicherheitsbezug von Bund, Ländern, Wirtschaft und Wissenschaft mit der Absicht der Prävention, Gefahrenabwehr, Strafverfolgung, Spionage- und Sabotageabwehr, nachrichtendienstlichen Aufklärung und Cyber-Verteidigung im Cyber-Raum verfolgt. Die föderale, ressort- und behörden- sowie grenzübergreifende Zusammenarbeit wird dabei bewusst zur Erschließung von Synergien angestrebt.

Im Nationalen Cyber-Abwehrzentrum werden beispielsweise unter der Federführung des BSI – unter Beachtung der jeweiligen verfassungsrechtlich gebotenen Zuständigkeiten und Cyber-Schwerpunktsetzungen – die Kompetenzen des Bundesamts für Verfassungsschutz, Bundesamts für Bevölkerungsschutz und Katastrophenhilfe, Bundeskriminalamts, Zollkriminalamts, Bundesnachrichtendienstes, der Bundespolizei und der Bundeswehr gebündelt und die Cyber-Sicherheitslage Deutschlands geführt.

Dabei verfügen die einzelnen Organisationen über spezialisierte Teams, wie z.B. das “Mobile Incident Response Teams” (MIRTs) des BSI, das technische Sicherheitsvorfälle analysiert und bereinigt, zum Zwecke der Strafverfolgung die Quick Reaction Force (QRF) des BKA oder die mobilen Cyber-Teams des BfV bei Vorliegen nachrichtendienstlicher oder extremistischer/terroristischer Cyber-Attacken.

Für präventive und reaktive technische Maßnahmen im IT-Sicherheitsbereich und als Ansprechpartner für die Verwaltung, Betreiber Kritischer Infrastrukturen, die Wirtschaft aber auch für die Bürger nimmt das BSI die Rolle des nationalen Computer Emergency Response Teams (CERT) wahr.

Der Bundeswehr obliegt im Rahmen ihres verfassungsmäßigen Auftrags und im Rahmen der IT-Sicherheitsarchitektur die Cyber-Verteidigung. Zum Schutz eigener Informationen, IT sowie Waffen- und Wirksysteme nutzt die Bundeswehr dabei ihre eigenen Fähigkeiten zum Wirken im Cyber-Raum gegen Cyber-Angriffe.

Die enge Verzahnung behördlichen Handelns mit der Wirtschaft und Wissenschaft komplettiert die Cyber-Sicherheitsarchitektur.

Fazit:

Cyber-Sicherheit muss als gesamtstaatliche Aufgabe verstanden werden. Nur durch das Zusammenwirken von Organisationen und Einrichtungen mit Sicherheitsbezug kann den Herausforderungen im Cyber-Raum begegnet werden. Eine wirksame Cyber-Sicherheitsarchitektur, die die Risiken durch Cyber-Angriffe beherrschbar macht, bildet dabei den Schlüssel zur Handlungsfähigkeit und digitalen Souveränität Deutschlands.

[1] Vgl. Bence Kollanyi u.a.: Bots and Automation over Twitter during the First U.S. Presidential Debate, in: COMPROP DATA MEMO 2016.1 / 14 OCT 2016.

Cyber- und Informationsraum – Äußere Sicherheit und Verteidigung 4.0?

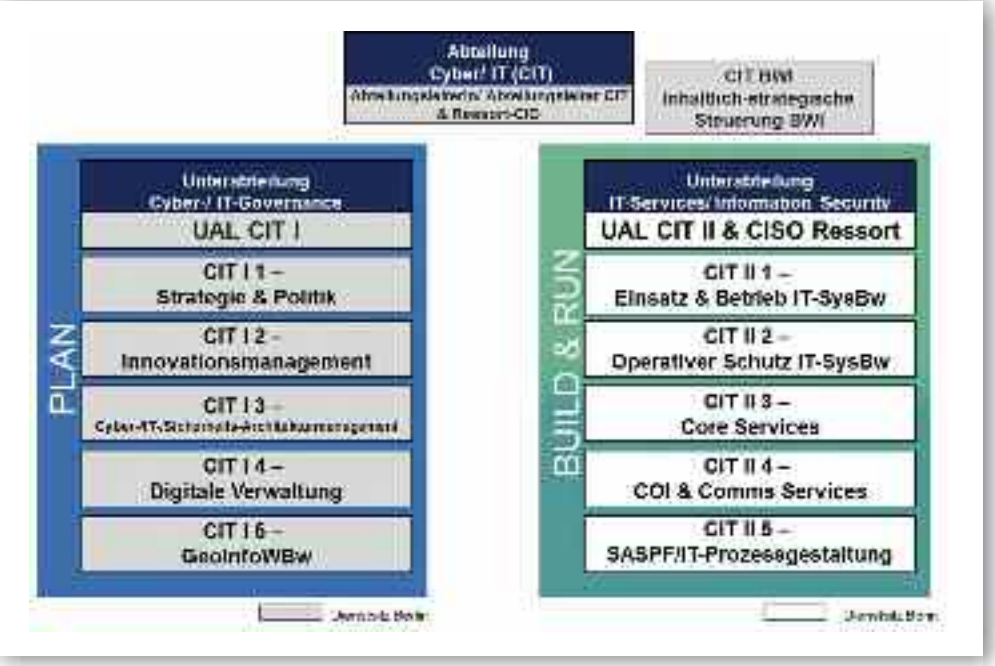
Oberst i.G. Armin Fleischmann, Abteilungsleiter Planung CIR
und Vorstand AFCEA Bonn e.V.

Armin Fleischmann
Oberst i.G.

Die zunehmende Digitalisierung und Vernetzung unseres Alltags bietet nicht nur Chancen, sondern birgt auch Risiken. Staat, Wirtschaft und Gesellschaft sind für Angriffe im Cyber- und Informationsraum (CIR) verwundbarer geworden. Zahl und Qualität der Cyber-Angriffe und Aktivitäten im Informationsumfeld nimmt dabei exponentiell zu. Aktuelle Vorfälle zeigen, dass Angriffe und Technologien hoch entwickelt sind. Deutlich wird auch, dass das Wirken im "virtuellen" Cyber-Raum Effekte in der "realen" Welt hat. Estland und Georgien belegen, dass Cyber-Attacken auf staatliche Institutionen und kritische Infrastruktur bereits heute Realität sind. Die Urheber sind schwer zu identifizieren und die Angriffe kostengünstig. Deshalb sind diese häufig zu einem wirkungsvollen Mittel geworden, um Ziele unterhalb der Schwelle eines militärischen Angriffs durchzusetzen.

Mit der Cyber-Sicherheitsstrategie für Deutschland vom 9. November 2016 hat die Bundesregierung einen ressortübergreifenden, strategischen Rahmen geschaffen. Die Wahrung der Cyber-Sicherheit ist eine gesamtstaatliche Aufgabe. Dazu gehört auch der gemeinsame Schutz der Kritischen Infrastrukturen. Die gesamtstaatliche Cyber-Sicherheitsarchitektur weist den verschiedenen Ressorts unterschiedliche Aufgaben zu. Verteidigungsaspekte werden dem Bundesministerium der Verteidigung und als verfassungsgemäßem Auftrag der Bundeswehr zugewiesen.

Unverändert ist es Aufgabe der Sicherheits- und Verteidigungspolitik, die territoriale Unversehrtheit sowie die Souveränität Deutschlands und seiner Verbündeten zu wahren. Künftig wird die Sicherheit Deutschlands auch im CIR zu verteidigen sein. Es gilt die eigenen Kräfte handlungsfähig zu halten. Nicht nur durch Teilhabe am Informationsaustausch sondern auch mit den Erhalt der Funktionsfähigkeit moderner, IT-gesteuerter Plattformen und Waffensysteme. Somit kommt dem Schutz eigener Systeme eine wesentliche Bedeutung zu. Die Bundeswehr stellt ein Hochwertziel für die Akteure im CIR dar und muss neben den tausenden täglichen Malware- und Spam-Attacken jederzeit mit hochprofessionellen Cyber-Angriffen rechnen. Der Aufbau robuster Cyber-Fähigkeiten mit dem Zusammenwirken konventioneller Kräfte in der Bundeswehr ist daher von besonderer Bedeutung; und dieses von der Rüstung bis hin zum Auslandseinsatz.



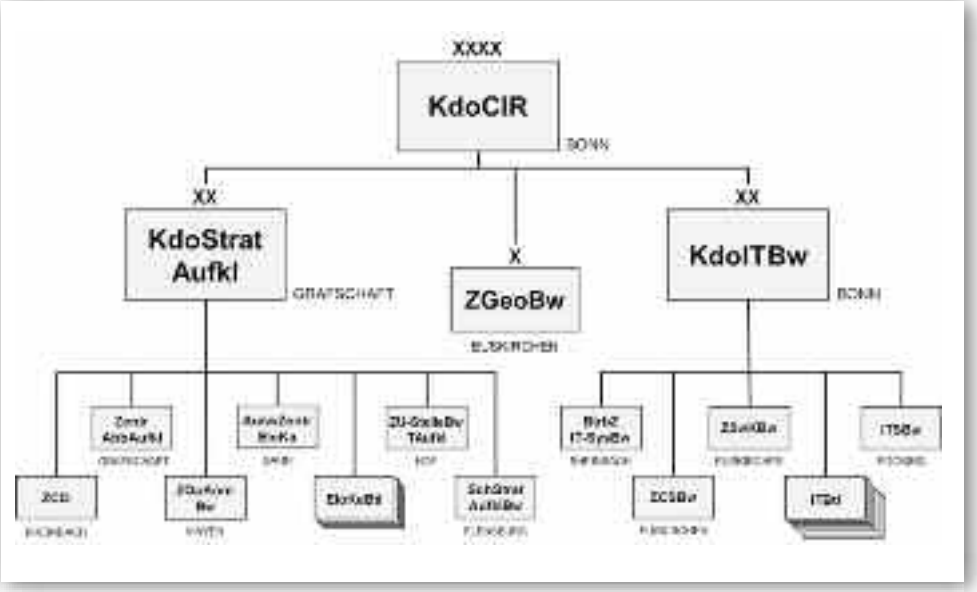
Die neue Abteilung CIT im BMVg

Grafiken: Fleischmann /CIT BMVg

Cyber/IT aus einer Hand – die neue Abteilung CIT im BMVg

Mit der neuen Abteilung CIT im BMVg ist seit Oktober 2016 unter der Führung eines "Ressort Chief Information Officer (CIO)" die Verantwortung für das Thema Cyber und IT gebündelt worden. Klaus Hardy Mühleck ist als CIO verantwortlich für die Digital- und Cyberpolitik, die IT-Strategie und -Architektur, die IT- und Cybersicherheit, die Realisierung und den Betrieb des IT-Systems der Bundeswehr sowie die inhaltliche Steuerung der BWI Informationstechnik GmbH.

Der CIO ist nicht nur für die in der Bundeswehr eingesetzten IT-Systeme, -Projekte und deren Weiterentwicklung verantwortlich. Als Architekt des IT-Systems der Bundeswehr in seiner Gesamtheit schafft er die Grundlagen zur Wirkungsfähigkeit von Plattformen und Waffensystemen und macht dabei auch die Vorgaben für deren "Embedded-IT". Er legt damit die strategische Ausrichtung Cyber/IT der Bundeswehr fest, kann frühzeitig innovative Impulse für den Aufbau militärischer Fähigkeiten im Bereich Cyber/IT aufnehmen und geben und einen wirkungsvollen Beitrag für Waffensysteme und Plattformen leisten.



Der neue militärische Organisationsbereich Cyber- und Informationsraum

KdoCIR – Konzentration und Bündelung

Im neuen militärischen Organisationsbereich CIR werden die Kräfte und Mittel der Bundeswehr in der Dimension CIR gebündelt. Er wird durch das "Kommando Cyber- und Informationsraum" (KdoCIR) geführt. Ähnlich wie die Teilstreitkräfte für ihre Dimensionen Land, Luft und See zuständig sind, werden die Mitarbeiter des neuen Organisationsbereiches für die Dimension Cyber- und Informationsraum verantwortlich sein.

Die Position des Inspekteurs CIR in der Dimension CIR manifestiert sich in seiner Eigenschaft als Taktgeber für die Entwicklung von Karrierepfaden und Gestaltung von Werdegängen für das Fachpersonal ebenso wie durch die zukunftsgerichtete Planung und Weiterentwicklung. Bei der Ausplanung des neuen KdoCIR wurde bei den erforderlichen Dienstposten für die truppendienstliche Führung und die querschnittlichen Aufgaben eines militärischen Organisationsbereiches bewusst ein sehr schlanker Ansatz gewählt. Dies gilt für den Dienstpostenumfang als auch die Dotierung gleichermaßen.

Im KdoCIR werden neben den Führungsaufgaben für den Organisationsbereich auch die fachlichen Aufgaben in der Weiterentwicklung sowie übergreifende Aspekte für die fachspezifische Ausbildung zusammengefasst. Weiterhin wird die Unterstützung des Einsatzführungskommandos der Bundeswehr und des Nationalen Territorialen Befehlshabers durch CIR-Kräfte oder -Fähigkeiten sichergestellt. Im Gemeinsamen Lagezentrum soll das relevante Wissen in der Bundeswehr korreliert und verfügbar gemacht werden.

Die Konzentration der fachlichen Aufgaben im KdoCIR führt dazu, dass die nachgeordneten Stäbe entsprechend schlanker gestaltet werden. Diese Ebene wird sich zukünftig auf die operativen Aufgaben konzentrieren.

Fazit

Mit der Aufstellung eines eigenen ministeriellen Bereiches und dem Aufbau eines neuen militärischen Organisationsbereiches sind die Grundlagen gelegt, um wirksame Cyber-Fähigkeiten der Bundeswehr auszubauen und neu zu schaffen. Es wird ein Balanceakt werden, traditionelles militärisches Verständnis mit den fachlich bedingten Eigenheiten des jungen Organisationsbereiches in Einklang zu bringen. Vieles wird neu gedacht werden müssen und auch Etabliertes muss sich einer kritischen Betrachtung unterziehen. Nur so wird eine moderne Bundeswehr mit der neuen Identität CIR die Verteidigungsaufgaben erfüllen können.

Industrie 4.0 aus Industrieperspektive

AFCEA Bonn e.V. – mit über 900 persönlichen und mehr als 90 Firmenmitgliedern – hat in den vergangenen Jahren ein umfangreiches, inhaltlich sehr fundiertes Jahresprogramm entwickelt. Die inhaltliche Umsetzung und Ausgestaltung erfolgt durch verschiedene Gremien, die sich alle dem Motto "Mehr Wissen teilen" verschrieben haben und die Inhalte aus Bundeswehr, Behörden, Wissenschaft und Industrie beitragen. Der Industriebeirat (IBR) setzt sich aus Vertretern der Mitgliedsfirmen zusammen. Er bringt Themenvorschläge für das Jahresthema und die Veranstaltungen ein. Dieses Gremium hat die folgenden zwei Beiträge zum Jahresthema "Industrie 4.0" aus seinem Kreis ausgewählt, die dieses Thema aus verschiedenen Industrie-Perspektiven beleuchten.

Cyber-Abwehr in der Industrie 4.0: Der Mensch bleibt im Mittelpunkt

Götz Piwinger, Chief Digital Officer (CDO) ML Consulting Service & Support GmbH

Götz Piwinger

Foto: ML Consulting

Fünfzig Prozent der Cyber-Angriffe werden durch den Menschen verursacht oder nicht verhindert. Daher ist es von entscheidender Bedeutung, Methoden und Systeme zum Einsatz zu bringen, um alle Beteiligten permanent und aktuell mit der erforderlichen Cyber-Souveränität auszustatten. Diese Herausforderung ist – unter anderem durch den demografischen Wandel – durch den schneller werdenden Wechsel der eingesetzten Systeme oder dezentrale Einsatzorte sehr vielschichtig. In der Öffentlichkeit werden Attacken auf IT-Systeme in der Regel als technische Probleme dargestellt. Die Angreifer werden "Cyber-Kriminelle" genannt.

Warum gelingen immer größere Angriffe auf deutsche Unternehmen?

Die Ursache liegt häufig in der Schwachstelle Mensch. Hier gilt: Die Summe kleiner Fehler einzelner Menschen kann sich zu einem riesigen Gefahrennetzwerk ausbilden, wenn unterschiedliche Daten zusammengeführt und für Cyber-Attacken genutzt werden.

Wenn wir Cyber-Kriminalität an der Wurzel bekämpfen wollen, brauchen alle Mitarbeiter einer Organisation einen hohen Grad von "Digitaler Souveränität" im Sinne von Umgang mit Daten und persönlichem Verhalten. Nur damit kann das Knowhow deutscher Unternehmen nachhaltig geschützt werden. Aber wie kann man diese Souveränität steuern und messen?

Es ist bekannt, dass regelmäßige Schulungsmaßnahmen die Situation verbessern, nur: Wenn die Zyklen der Angriffe aufgrund den Technologiewandels immer schneller werden, muss die Aufmerksamkeit der Mitarbeiter mindestens ebenso schnell mitwachsen, ohne dabei hektisch oder neurotisch zu werden. Dazu ist es notwendig, den Reifegrad der Mitarbeiter dynamisch zu formulieren und in Echtzeit zu messen. Nichts eignet sich dafür besser als ein kombiniertes, webbasiertes Lern- und Talentmanagementsystem. Solche Systeme gibt es für wenige

Cyberspionage *Foto: Marco Piunti*

Euro pro Mitarbeiter. In Kombination mit einer Kompetenzmodelltransformation vom Modell bis zum selbstbestimmten Lernen schaffen Unternehmen parallel einen Wandel zur modernen Unternehmenskultur (digital leadership).
Das Projekt "Digitale Souveränität" ist im Idealfall zunächst eine unternehmensweite Kampagne, durch welche die Mitarbeiter im späteren Unternehmensalltag durch kleine Lerneinhei-ten – idealerweise als eLearning – spielend auf dem aktuellen Stand gehalten werden.

Dieses Verfahren bringt langfristig Sicherheit ins Unternehmen und nützt im privaten Alltag. Wichtig ist dabei, neben der Auswahl von Methodik/Didaktik und Inhalt der Bildungsmaßnahme, auch die Motivation und die Grundeinstellung der Betroffenen zu maximieren, um die gewünschte Sensibilisierung zu erreichen. Eine Cyber-Sicherheitskampagne will also gut vorbereitet sein. Unternehmen sollten deshalb nicht lange zögern, den Startschuss zu geben. Denn auch hier gilt die alte Weisheit: Im Anfang war die Tat!

Perspektiven der Cybersicherheit im Internet der Dinge

Alfred Saal, Business Development Executive, IBM Deutschland GmbH

Alfred Saal *Foto: Privat*

Industrie 4.0, als Synonym für die vierte industrielle Revolution, steht für eine umfassende Vernetzung von Produktions- und Wertschöpfungsketten. Das Ziel ist die Integration von Prozessen – vertikal von der Fabrikhalle bis zur Führungsetage, horizontal entlang der Wertschöpfungsketten sowie entlang des gesamten Lebenszyklus der Produkte und Systeme.

Ohne Sicherheit wird Industrie 4.0 scheitern

Die Verschmelzung der realen mit der virtuellen Welt in einem Industrial oder Military Internet of Things (IIoT bzw. MilIoT) wird nur dann zu Akzeptanz und Wertschöpfung führen, wenn die meist komplexen, oft geschäftskritischen Lösungen mit der notwendigen Sicherheit untermauert werden.
Während in der klassischen IT die Sicherheit kontinuierlich entwickelt wurde, gestaltet sich die Absicherung industrieller Infrastrukturen meist als sehr viel schwieriger. Hauptursachen dafür sind die hohe Komplexität bei oft großer Fragmentierung, zahlreiche Angriffsflächen und wenig Aktualisierung trotz altbekannter Schwachstellen, sowie mangelnde Sichtbarkeit oder unterschiedliche Bewertung von Risiken. Neue Bedrohungen entstehen insbesondere dann, wenn Maschinen im Zuge von Industrie 4.0 direkt an das Internet angekoppelt werden.
Die Angriffe können neben Datenverlust (Spionage, Erpressung) beispielsweise die Sabotage oder Manipulation von Arbeitsabläufen oder Systemen zur Folge haben, etwa der Ausfall der Fahrzeugschlüssel-Codierung, Manipulation von Lackierrobotern, Störungen oder Fehlfunktionen in Waffensystemen. Moderne Angriffe sind komplex, verschlüsselt, verschachtelt, nutzen "legitime" Kommunikationswege und sind sozusagen minimal invasiv.

Mit Sicherheit Wertschöpfung statt "Internet of Trouble"

Die Herausforderung ist, sowohl durchgängige Sicherheitsstrukturen in den vertikalen Prozessen zu schaffen als auch die Sicherheit entlang der horizontalen Wertschöpfungskette zwischen Herstellern und Kunden, das heißt für die Bundeswehr "from factory to foxhole" zu gewährleisten.
Analoge Ziele verfolgt der deutsche Arbeitskreis "Plattform Industrie 4.0", die insbesondere die Harmonisierung klassischer und industrieller Sicherheitsmaßnahmen berücksichtigt, Fertigungs-Know-How mit IT-Wissen verknüpft und die besonderen Anforderungen von Herstellern und Betreibern beachtet. So erarbeitet IBM mit Firmen wie etwa AT&T, Bosch und CISCO im Industrial Internet Consortium (IIC) ein Industrial Internet Security Framework (IISF) für eine durchgängige, industrielle IT- und Cybersicherheit mit dem Ziel, Vertraulichkeit, Integrität und Ausfallsicherheit zu gewährleisten, so der Arbeitskreis "Plattform Industrie 4.0."

Mit Cyber-Resilienz Angriffen erfolgreich begegnen

Allerdings ist eine 100-prozentige Sicherheit selbst mit sehr hohem Aufwand nicht möglich. Das Ziel muss deshalb sein, über Vorkehrungen hinaus mit intelligenten, integrierten Lö-

Industrieroboter in der IT *Foto: IBM*

sungen Bedrohungen möglichst frühzeitig, also präventiv zu erkennen, und auf Attacken schon reagieren zu können, während sie geschehen (detektiv) und spätestens direkt nachdem sie erfolgt sind (forensisch korrektiv).

Regelmäßige Übungen für Sicherheitsexperten, Anwender und Entscheider und konkrete Pläne helfen, auf Krisensituationen durch Cyber-Angriffe gut vorbereitet zu sein. Ein durchgängiges, integriertes Identitäts- und Asset-Management ist ebenfalls wesentlich.

Permanente Innovation in Detektion und Reaktion sind essentiell im Wettlauf gegen die Angreifer. Hierzu zählt beispielsweise eine moderne Security-Intelligence- und Analyse-Plattform. In den kommenden zwei bis drei Jahren werden kognitive Sicherheitslösungen gerade im komplexen IIoT-Umfeld eine wichtige Unterstützung und Entscheidungshilfe sein. Da Expertise und Erfahrung nur begrenzt verfügbar sind, wird die Zusammenarbeit mit Partnern immer wichtiger. Austauschplattformen wie etwa die IBM X-Force-Exchange, unterstützen die Zusammenarbeit von Industrie, Wirtschaft und Verwaltung sowie Sicherheitsfirmen, Wissenschaft und Forschung.

Fazit: Eine so aufgebaute, dynamische **“Industrial Security”** bietet das Rüstzeug, um Cyber-Gefahren möglichst effektiv abzuwehren. Eine starke Cyber-Resilienz gewährleitstet den bestmöglichen Schutz in der Industrie 4.0 oder einem militärischen IoT.

Innere Sicherheit 4.0 – Gibt es die?

Tobias Schönherr, Leiter Luftfahrerschule der Bundespolizei und Vorstand AFCEA Bonn e.V.

Tobias Schönherr

Foto: Schönherr /AFCEA

Ich gebe zu, diese Fragestellung hat mich selbst überrascht. Natürlich beschäftigt man sich, gerade als Mitglied von AFCEA Bonn e.V. mit vielen Fragen der Informationsverarbeitung, der Elektronik, der IT insgesamt. Industrie 4.0 ist allgegenwärtig, durchdringt unser Leben und unser Wirken. Das gilt nicht nur für jene, die sich dem Kreis der IT-Spezialisten zugehörig fühlen, sondern für alle, die Interesse an dieser technologischen und gesellschaftlichen Entwicklung aus der Industrie heraus haben, aber auch für alle Endnutzer. Nach Mechanisierung, Elektrifizierung und Digitalisierung entsteht nun eine, nicht nur im Namen "Industrie 4.0" durch Deutschland vorangetriebene Vernetzung. Ist ein Übertragen dieser Begrifflichkeit auf die innere Sicherheit, zum Beispiel die Polizei, überhaupt möglich?

Die Mechanisierung der Polizei in den zwanziger Jahren des letzten Jahrhunderts sah so aus, dass Polizeieinsätze nach Munitionsverbrauch abgerechnet wurden. Telefone und Funkgeräte prägten die Einsätze in den beiden deutschen Staaten nach dem zweiten Weltkrieg. Eine in den 90er Jahren eingeführte elektronische Datenverarbeitung zur Vorgangsbearbeitung und Analyse polizeilicher Einsätze revolutionierte vor allem die Büroarbeit der Organisationen der inneren Sicherheit. Die ersten PC, damals schon vernetzt in eigenen geschützten Umgebungen, machten die Polizeiarbeit effizienter. 16 Landespolizeien, das Bundeskriminalamt und die Bundespolizei, in vielen Einsätzen gemeinsam und in gegenseitiger Unterstützung tätig, entwickelten und entwickeln weiterhin Strategien, die sich auch in der Informationsverarbeitungstechnik niederschlagen. Dies geschah auch in Kooperation, meist mit eigenen Mitteln und eigenem Personal. Ein Einsatz-Protokollierungssystem der bayrischen Kollegen wurde unter anderem auch von anderen Polizeien verwendet.

Das erste große gemeinsame Projekt, nicht nur der Polizeien von Bund und Ländern, sondern von allen BOS (Behörden und Organisationen mit Sicherheitsaufgaben; dazu zählen auch die Rettungsdienste und die Feuerwehren), war der Digitalfunk. In den 90er Jahren begonnen, bietet er heute eine flächendeckende Kommunikationsmöglichkeit für alle BOS. Es ist die Digitalisierung, also Polizei 3.0, um im hier betrachteten Sprachgebrauch zu bleiben. Aber die Zeit, die uns, vom Mooreschen Gesetz getrieben rasante Entwicklungen in der IT erleben lässt, hat diesen Digitalfunk dort belassen, wo er herkommt: in den Neunzigern. Das lässt sich gut mit der Entwicklung von Smartphones und Tablets vergleichen, für viele von uns eine Selbstverständlichkeit – hat der durchschnittliche deutsche Bürger doch heute schon 2,7 solcher IT-Endgeräte. Auf die Frage, wann es denn das erste Tablet gab, antworten junge Menschen meist: schon immer. Meine Generation überlegt lange und tippt meist auf den Zeitraum zwischen 2002 bis 2004. Tatsächlich war es im Frühjahr 2010, als Steve Jobs in seiner unnachahmlichen Art etwas vorstellte, das sich zu diesem Zeitpunkt kaum jemand vorstellen konnte.

Entwicklungen für die Innere Sicherheit unterliegen immer einem Weg des öffentlichen Dienstes, da sie höchstmögliche Systemsicherheit einerseits mit den Verwaltungsverfahren und der sich immer schneller bewegenden "zivilen" Technologieweiterentwicklung andererseits verbinden muss. Digitalfunk 3.0 kann so Funktionalitäten von Smartphones und Tablets mit komplexen Vernetzungen von Informationen nicht abbilden.

Wie ist es nun um die Innere Sicherheit 4.0 bestellt? Unter Berücksichtigung der Ausgangsbetrachtungen wird dies auch zu einer philosophischen Frage: Ist eine Vernetzung der polizeilichen Systeme wie Fahndungsdatenbanken, Vorgangsbearbeitung aber auch die Entwicklung prädiktiver Systeme zu gesamtstaatlichen Sicherheitsvorsorge, wie beispielsweise für die Erkennung von Anschlagsgefahren, im Gleichklang zur

"Polizei 3.0": Start in neue Entwicklungen?

Innere Sicherheit 4.0: Es geht um Vernetzung

"zivilen" Entwicklung digitaler Technologien überhaupt möglich? Sollte nicht lieber auf einer "zivilen" Basis der Technologien lediglich eine geschützte, nicht einsehbare BOS-IT-Infrastruktur geschaffen werden? Bewegen wir uns dann auf militärischem Terrain wie für einen Panzergrenadier der Zukunft? Auch folgende Frage darf dann gestellt werden: Ginge es dann schneller und besser?

Polizei in Deutschland braucht Vernetzung und das ähnlich zu der von den Kolleginnen und Kollegen im privaten Umfeld bereits genutzten Technologie. "WhatsApp" sollte niemals die Führungsgrundlage eines Polizeieinsatzes darstellen. Aber die Idee der Messenger-Dienste schon. Die Daten der Polizei gehören immer auch in sichere IT-Umgebungen. Seit Dezember 2016 gibt es einen polizeieigenen Messenger-Dienst.

"Polizisten auf die Straße!" ist das Ziel jeder Polizeireform, in der Büroarbeitsplätze abgebaut werden und die Beamtinnen und Beamten in den "Dienst für den Bürger" gehen sollen. Der IT-Arbeitsplatz muss aber mitgenommen werden können, und zwar mit all seinen Funktionalitäten wie beispielsweise den genannten Fahndungsdatenbanken und Vorgangsbearbeitungen. Und der Kollege in Mainz muss dem Polizisten in Hamburg das Bild eines gewalttätigen "Fußballfans" direkt übermitteln können. Der "Fan" ist schnell in Hamburg, die Polizei muss schneller sein.

Es geht hier um Vernetzung. Auch zwischen den Polizeien. Die Innenministerkonferenz im November 2016 hat dazu eine IT-Strategie veröffentlicht. Alle (18) Polizeien sollen kompatible IT-Systeme betreiben. Erfolgreich. Interoperabel.

Lassen Sie uns über den Begriff "Innere Sicherheit 4.0" wieder reden, wenn er inhaltlich umgesetzt wurde. Es gibt nur eine "Innere Sicherheit" in Deutschland.

Besuchen Sie uns auf der AFCEA im Saal MARITIM: M 19

SDoT Diode

SDoT Diode®
Die Hochgeschwindigkeits-Netzwerkdiode
für gehobene Ansprüche

- Der neuste Zuwachs in der **SDoT®**-Produktfamilie von **Hochsicherheits-Appliances**
- **Highspeed**-Datenübertragung mit bis zu **9 GBit/s** effektiv von LOW nach HIGH
- Zulassung durch das BSI bis GEHEIM beantragt
- Ab sofort erhältlich – **Live-Demo** an unserem Stand

infodas

Rhonestraße 2 • 50765 Köln • Telefon (0221) 70912-0 • Fax (0221) 70912-55
E-Mail vertrieb@infodas.de • Internet www.infodas.de

Sichere Luftfahrt der Zukunft: IT als ein wichtiger Schlüssel

Generalmajor Dr. Ansgar Rieks, Amtschef Luftfahrtamt der Bundeswehr, stv. Vorsitzender AFCEA Bonn e.V. und Leiter Programmbeirat *)

Dr. Ansgar Rieks
Generalmajor
Foto: Luftwaffe / Timm Grommes

"IT als ein wichtiger Schlüssel für die sichere Luftfahrt" ein Satz, der so selbstverständlich klingt wie das "Amen" in der Kirche. Jedoch zeigt der im November 2016 stattgefundene Hackerangriff auf 900.000 mobile Endgeräte der Deutschen Telekom, dass global angelegte Cyberangriffe ernstzunehmende Bedrohungen sind. In diesem Kontext gerät unser für selbstverständlich erachtetes IT-Sicherheitsgefühl gewaltig ins Wanken. Der Telekom-User hat es am eigenen Beispiel vor kurzem erlebt.

Der Stellenwert von IT hat sich in den letzten Jahrzehnten in Organisationen und Unternehmen drastisch verändert. Die IT, früher eine Wissenschaft für sich und nur wenigen Experten vorbehalten, gehört in der heutigen Zeit zum Schul- und Alltagswissen. Zunehmend ist IT eine fest implementierte Größe, die auf vielen Ebenen der Organisations- und Geschäftsprozesse nicht mehr wegzudenken ist. Die Einstiegsbarriere für Angriffe ist dementsprechend gering und kann mit entsprechender Hardware und einem Internetzugang, egal von wo auf der Welt, durchgeführt werden. Der Reiz dabei ist, dass jeder "David" einen "Goliath" in die Knie zwingen kann.

Schauen wir zunächst mit der Brille des Endnutzers in den Bereich der alltäglichen Nutzung von IT. Dem IT-kundigen Leser wird das beschriebene Szenario möglicherweise nicht unbekannt erscheinen, bereits der Zusammenbruch der mobilen Internetverbindung auf unserem Handy führt an mancher Stelle zu einem temporären Chaos. Als gutes Beispiel erscheint dabei die auf dem Handy genutzte Navigationsfunktion, die in den meisten Fällen mit einer Internetverbindung funktioniert. Es ist sicherlich nicht zu verallgemeinern, aber unser Handy ist ohne Internetzugang ein nahezu nutzloser Gegenstand, der uns oftmals nur noch wenig helfen kann.

Weitere Praxisbeispiele für die Nutzung von IT findet beinahe jeder an seinem Arbeitsplatz. In der täglichen Aufgabenerfüllung begleitet uns die IT selbstverständlich bei fast allen Tätigkeiten. Wir telefonieren über Zeitzonen hinweg mit unseren internationalen Partnern. Mal eben eine "WhatsApp"-Nachricht geschrieben, um letzte wichtige Informationen einzuholen, wer kennt das nicht! Die Kommunikationswege sind dadurch schneller geworden, und wir haben die technischen Hilfsmittel in unser Leben integriert. Die dargestellten Szenarien liegen im Kontext der Endnutzung von IT. Wir gehen davon aus, dass jegliche Kommunikationswege sicher sind, und vertrauen den Providern.

Als Luftfahrtamt der Bundeswehr ist die Sicherheit der militärischen Luftfahrt das Hauptanliegen unserer Arbeit. Die Bundeswehr betreibt zahlreiche Luftfahrzeuge. Jedes dieser Waffensysteme, wie beispielsweise der neue Marinehubschrauber "Sea Lion", ist mit modernster IT ausgestattet, welche die unterschiedlichsten Aufgaben erfüllen. Diese reichen von einfachsten Kommunikationswegen innerhalb des Luftfahrzeuges, über IT-gestützte Sensorik zur Überwachung der Systemfunktionen bis hin zur Kommunikation mit der Bodenstation. Viele IT-gestützten Funktionen verbessern die Sicherheit.

Gehen wir nun einen Schritt weiter. Die IT kann und wird in Zukunft die Luftfahrt immer stärker tangieren. Ein viel diskutiertes Beispiel ist die unbemannte Luftfahrt. Wesentlicher Vorteil ist, dass der Operateur von einer Bodenstation aus agiert und sich somit nicht unmittelbar in der Einsatzzone befindet. Die Steuerung des unbemannten Luftfahrzeuges geschieht mit Hilfe einer Datenverbindung. Diese Datenverbindung kann als ein zentrales Element der unbemannten Luftfahrt identifiziert werden. Störungen können durch Spoofing (Vortäuschen falscher Signale), Jamming (Überlagern eines Signals durch ein stärkeres Signal) oder der einfache Verbindungsverlust aufgrund technischer Probleme auftreten. Dies gilt es zu verhindern. Die Bundeswehr tut viel dafür, damit solche Daten- und Linksysteme vor äußeren Störeinflüssen geschützt werden. Dazu zählen Maßnahmen, wie das Verstärken der eigenen Signale, speziell entwickelte Richtantennen oder auch das Verschlüsseln.

Doch wie genau funktioniert das Verschlüsseln eines Datenpaketes? Das bekannteste Kryptiergerät der Neuzeit ist die Enigma-Maschine aus dem Zweiten Weltkrieg. Diese war ähn-

Erstflug und Übergabe der vorläufigen Verkehrszulassung für den Marinehubschrauber "Sea Lion"

lich einer Schreibmaschine aufgebaut, nur dass drei unterschiedliche Walzen den eingegebenen Text mit unterschiedlichen Buchstaben oder Zahlen verschlüsselte." Diese Verschlüsselung war sehr effektiv, bis die Alliierten den Enigma-Code entschlüsselten. Somit war die Verbindung nicht mehr sicher. Heutige Kryptiergeräte sind weitaus komplexer und unterliegen den hohen Geheimhaltungsstufen der Bundeswehr. Sie sind verantwortlich dafür, der Achillesferse "Datenverbindung" einen sicheren Rückhalt zu geben.

Ich möchte es auf den Punkt bringen: Das Luftfahrtamt der Bundeswehr bündelt alle Kompetenzen für die Sicherheit der deutschen militärischen Luftfahrt. IT ist dabei allgegenwärtig. Ferner werden wir in allen Themen der Zulassung, des Flugbetriebs sowie bei Boden- und Radaranlagen Cybersicherheit einbeziehen müssen. Die Cybersicherheit ist eine internationale Herausforderung, der wir uns gemeinsam mit der NATO stellen. Dabei stellt sich nicht die Frage "ob", sondern "wie" wir dieser potentiellen Bedrohung begegnen. Daraus resultiert für das Luftfahrtamt der Bundeswehr die Aufgabe, mit dem in der Bundeswehr neu aufgestellten Organisationsbereich Cyber- und Informationsraum im engen Schulterschluss zusammenzuarbeiten, um mögliche Bedrohungen zu bekämpfen. Es gilt die möglichen Angriffsstellen auf genutzte IT zu identifizieren, Lösungen zu erarbeiten und diese schnellstmöglich zu integrieren. Wir sind für die Sicherheit der Luftfahrt verantwortlich, und IT ist ein wesentlicher Schlüssel dazu.

*) Dieser Beitrag entstand im engen Zusammenwirken mit Hauptmann Stefan Beyer, Leitungsbüro LufABw

AFCEA Veranstaltungskalender 2017
... nach der Fachausstellung

» 26./27. April
31. AFCEA Fachausstellung mit Symposium (Bonn)
Innere und äußere Sicherheit 4.0 – Schlüssel zur digitalen Souveränität

» 27. April
Young AFCEANs bei der Fachausstellung (Bonn)
Girls Day 2017

» 17. Mai
Info-Veranstaltung Young AFCEANs (Bonn)

» 23. Mai
Fachveranstaltung Internationales (Bonn)
Cyber als operationelle Domäne – quo vadis NATO?

» 14. Juni
Gemeinsame Veranstaltung AFCEA – KdoCIR (Bonn)

» 29. Juni
Mitgliederversammlung mit Vorstandswahl AFCEA Bonn e.V.

» 5./06. Juni
D-A-CH Security 2017 (UniBw München)

» 7. September
Koblenzer IT-Tagung 2017
Innere und äußere Sicherheit 4.0 – Schlüssel zur digitalen Souveränität

» 28. September
AFCEA Technologieforum Fraunhofer FKIE (Wachtberg)
“Automatisierte Meinungsbeeinflussung – Manipulation on offenen Medien”

» 10. Oktober
Fachveranstaltung (Bonn)
Internet der Dinge für Systeme der Bundeswehr – Vernetzung und Souveränität

» 18. Oktober
eGovernment und digitale Souveränität
Föderales IT-Sytem – Vernetzte Verwaltung

» 6. November
Info-Veranstaltungen Young AFCEANs (Bonn und Berlin)
Karriere Cyber/IT

» 17. November
AFCEA Mittagsforum mit Computacenter

» 23. November
Fachveranstaltung mit DBwV (Berlin)
Smart Mobility versus Mobile Security – Aktuelle Innovationen

» 5. Dezember
Fachveranstaltung (Wachtberg)
Big Data 4.0 – Analyse und Schutz

» 11. Dezember
YA Programmplanung 2018 (Berlin)

Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr

AFCEA Bonn e.V.

Das neue digitale Gefechtsfeld – Auswirkungen auf Sicherheit und Souveränität

Die Digitalisierung der Gesellschaft schreitet immer weiter voran und verändert fast alle Geschäftsprozesse. Auch auf dem Gefechtsfeld stellt sich dies als eine tiefgreifende und unumkehrbare Entwicklung dar. Eine zielgerichtete Gestaltung dieses Phänomens ist u.a. Grundvoraussetzung für die eigene Informationsüberlegenheit und damit für die Führungs- und letztlich die Wirkungsüberlegenheit. Auch in anderen Aufgabengebieten sowohl der Streitkräfte als auch der Organe der öffentlichen Sicherheit revolutioniert die Digitalisierung Informationsbeziehungen und Handlungsoptionen.

Wie uns Medienberichte regelmäßig vor Augen führen, ist die Informationstechnik nicht nur ein Mittel zur Erlangung der eigenen Überlegenheit, sondern auch Angriffspunkt und mögliche Schwachstelle.
Für den Schutz der eigenen IT-Systeme und der darin verarbeiteten Informationen müssen neue Sicherheitsmaßnahmen und Gegenoptionen gefunden und etabliert werden. Eine eigene Souveränität, zumindest bei ausgewählten Schlüsseltechnologien auf dem "digitalen Gefechtsfeld", ist ein wichtiger Schritt hierzu.

Doch um welche Schlüsseltechnologien handelt es sich? Wie kann eine solche Souveränität erlangt und aufrechterhalten werden? Welche Maßnahmen können im Bereich außerhalb der Schlüsseltechnologien ergriffen werden? Wo sind die Grenzen eigener Souveränität in einer globalisierten Wirtschaft und bei einer multinationalen Zusammenarbeit auf dem Gefechtsfeld?

Wir möchten mit Ihnen bei unserer **Koblenzer IT-Tagung am 07. September 2017** über diese und ähnliche Fragen diskutieren. Hierzu laden wir Sie zu dieser Veranstaltung ein und freuen uns, Ihnen ein interessantes Programm sowie einen unterhaltsamen Abend bieten zu können – einschließlich der Möglichkeit zu zahlreichen Gesprächen.

Ort:	Rhein-Mosel-Halle Julius-Wegeler-Straße 4, 56068 Koblenz		
Datum/Zeit:	Donnerstag, 07.09.2017 mit "Koblenzer Abend"	09:00 – 18:30 Uhr 18:30 – 21:00 Uhr	(Einlass 08:00 Uhr)
Teilnehmer:	Bundesministerium der Verteidigung; Kommandobehörden, Ämter, Dienststellen und Truppenteile der Bundeswehr; Behörden, Organisationen aus dem Bereich der öffentlichen Sicherheit (BOS); Institute, Verbände; Universitäten und Hochschulen; Industrie mit Schwerpunkt Informations- und Kommunikationstechnik; internationale Gäste		
Fachliche Leitung:	Brigadegeneral Jens-Olaf Koltermann, Abteilungsleiter Informationstechnik BAAINBw Generalmajor a.D. Erich Staudacher, AFCEA Bonn e.V.		
Programm:	+ aktuelle Informationen unter www.afcea.de und www.baainbw.de		
Kostenbeitrag:	+ Eintritt: 90,- €, einschließlich "Koblenzer Abend" + Öffentlicher Dienst und AFCEA-Mitglieder: Eintritt 20,- € Tagungspauschale, Teilnahme am Koblenzer Abend: 20,- € zusätzlich		

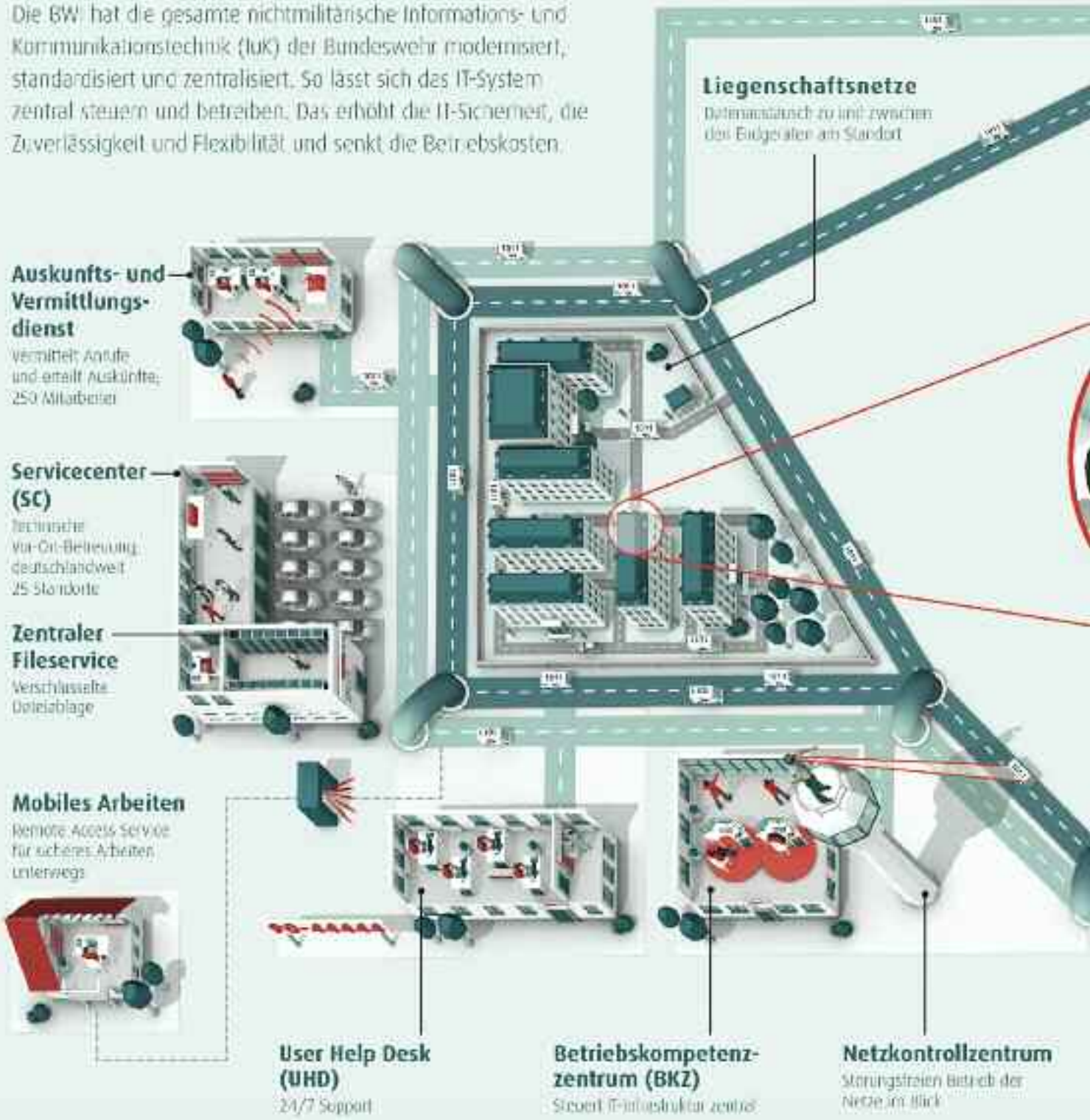
Klaus F. Veit, Generalmajor
Vizepräsident BAAINBw

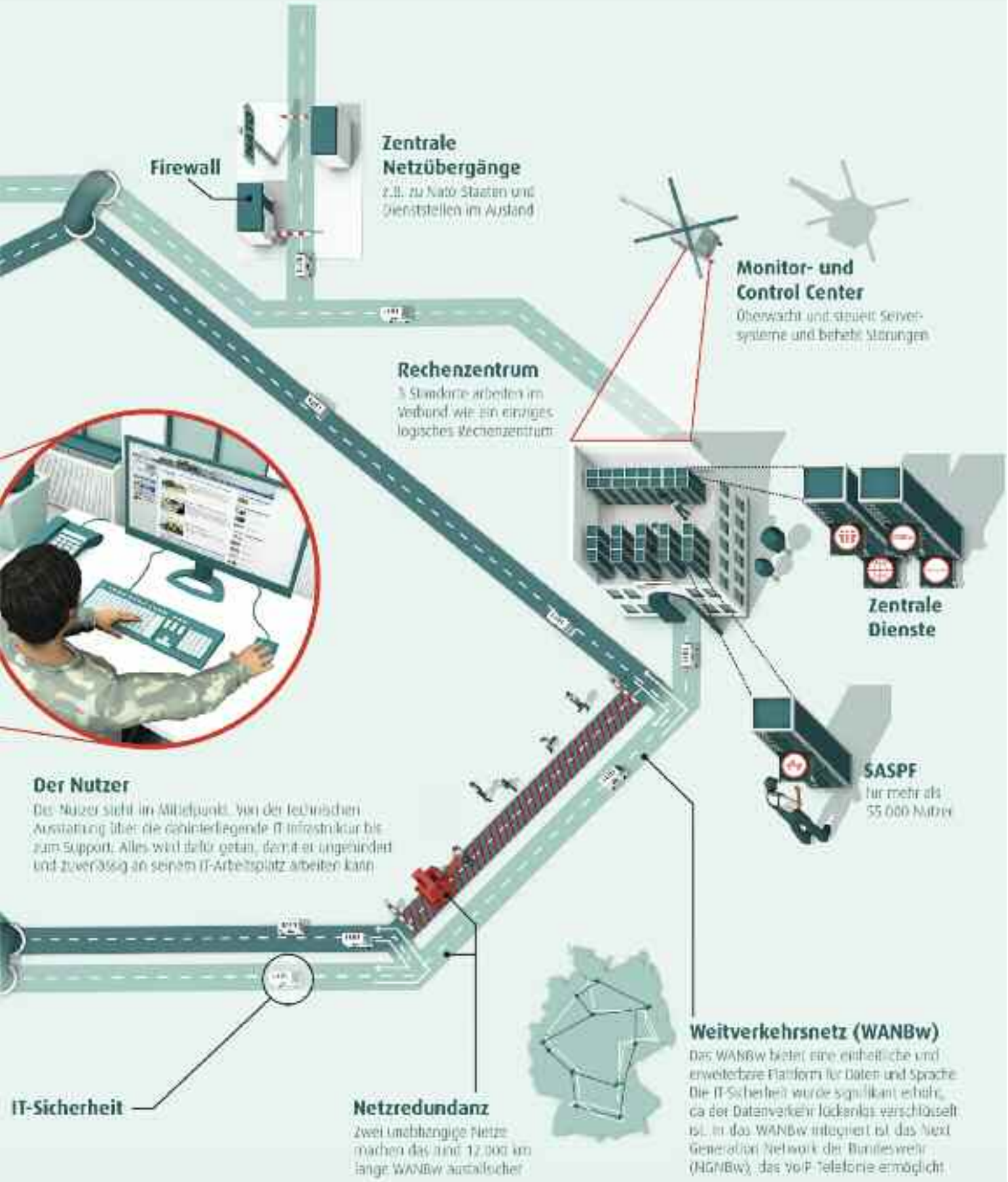
Erich Staudacher, Generalmajor
Vorsitzender AFCEA Bonn e.V.

AFCEA Bonn e.V., Borsigallee 2, 53125 Bonn, Tel.: 0228 / 925 82 52, Fax: 0228 / 925 82 53
BAAINBw, Ferdinand-Sauerbruch-Str. 1, 56073 Koblenz, Tel.: 0261 / 400-22023, Fax: 0261 / 400-22005

Das IT-System der Bundeswehr

Die BW hat die gesamte nichtmilitärische Informations- und Kommunikationstechnik (IuK) der Bundeswehr modernisiert, standardisiert und zentralisiert. So lässt sich das IT-System zentral steuern und betreiben. Das erhöht die IT-Sicherheit, die Zuverlässigkeit und Flexibilität und senkt die Betriebskosten.




Firewall
Zentrale Netzübergänge
z.B. zu Nato Staaten und Dienststellen im Ausland
Monitor- und Control Center
Überwacht und steuert Serversysteme und behebt Störungen
Rechenzentrum
3 Standorte arbeiten im Verbund wie ein einziges logisches Rechenzentrum
Zentrale Dienste
SASPF
für mehr als 55.000 Nutzer
Der Nutzer
Der Nutzer steht im Mittelpunkt. Von der technischen Ausstattung über die dahinterliegende IT-Infrastruktur bis zum Support. Alles wird dafür getan, damit er ungehindert und zuverlässig an seinem IT-Arbeitsplatz arbeiten kann.
Weitverkehrsnetz (WANBw)
Das WANBw bietet eine einheitliche und erweiterbare Plattform für Daten und Sprache. Die IT-Sicherheit wurde signifikant erhöht, da der Datenverkehr lückenlos verschlüsselt ist. In das WANBw integriert ist das Next Generation Network der Bundeswehr (NGNBw), das VoIP-Telefonie ermöglicht.
IT-Sicherheit
Netzredundanz
Zwei unabhängige Netze machen das rund 12.000 km lange WANBw ausfallsicher.

HERKULES: ein starkes Fundament für die Zukunft

Michael Krause, Mitglied der Geschäftsleitung für den Geschäftsbereich Account Management, BWI Informationstechnik GmbH

Michael Krause

Das Projekt HERKULES, die größte öffentlich-private Partnerschaft (ÖPP) Europas, ging 2006 an den Start. Die Aufgabe: die vollständige Modernisierung der nichtmilitärischen Informations- und Kommunikationstechnik (IuK) sowie deren Betrieb. Für den BWI Leistungsverbund, der für die Umsetzung des Projekts von den Partnern Bundeswehr, Siemens und IBM Deutschland gegründet wurde, standen neben der Modernisierung stets die Standardisierung, Konsolidierung und Zentralisierung der IT-Infrastruktur im Fokus. Die Konzentration auf wenige Standorte und die Vereinheitlichung von Systemen und Anwendungen erhöhen die Leistungsfähigkeit, Verfügbarkeit und Sicherheit eines IT-Systems deutlich und senken zugleich die Kosten für Pflege und Betrieb.

Die Partner sollten ein IT-System aufbauen, das zuverlässig, leistungsstark, flexibel und sicher ist. Dabei geht es nie um ein Entweder-oder. Nur im engen Zusammenspiel all dieser Kriterien bei der Datenübertragung, -verarbeitung und -speicherung, der Arbeitsplatzausstattung, Systempflege und dem Support ist auf ein IT-System Verlass. Ein Blick auf die heutige nichtmilitärische Bundeswehr-IuK verdeutlicht, wie konsequent und erfolgreich die BWI diesen ganzheitlichen Ansatz bei der Modernisierung des IT-Systems verfolgt hat.

Weitverkehrsnetz: ausfallsicher, leistungsstark und flexibel erweiterbar

Betrachten wir zunächst die Datenübertragung. Für die IT von Organisationen wie der Bundeswehr mit ihren vielen verteilten Standorten und Sicherheitsanforderungen bildet ein eigenes, hochverfügbares und leistungsstarkes Weitverkehrsnetz eine unverzichtbare Grundlage. Daher zählte der Aufbau eines solchen Netzes zu den ersten und wichtigsten Vorhaben, die die BWI zu Beginn des Projekts HERKULES in Angriff nahm. Dabei legte die BWI besonderen Wert auf Verfügbarkeit, Sicherheit, Zuverlässigkeit, Leistungsstärke und flexible Erweiterbarkeit des Glaserfaserkabelsystems. Im Ergebnis verfügt die Bundeswehr heute über eines der größten, stabilsten und leistungsfähigsten Weitverkehrsnetze in Deutschland. Seine Leistungsstärke beweist das WANBw auf einem Netzabschnitt zwischen Rheinbach und Köln. Hier können Daten mit bis zu 100 Gigabit pro Sekunde transportiert werden. Doch damit ist das Potenzial des WANBw noch nicht ausgeschöpft. Da die Plattform einheitlich, erweiterbar und skalierbar ist, sind in Zukunft noch weitaus höhere Übertragungsraten denkbar. Somit ist das Netz nicht nur gut aufgestellt für den steigenden Bedarf an Bandbreiten und künftige Anforderungen der Bundeswehr, sondern eröffnet dem Bund die Möglichkeit, es auch für die IT-Konsolidierung in anderen Bereichen zu nutzen.

In das Weitverkehrsnetz integriert ist die Telekommunikation der Bundeswehr. Dafür hat die BWI ein Next Generation Network (NGN) aufgebaut und betreibt dieses. Es basiert auf dem Voice over Internet Protocol (VoIP) und erlaubt die gleichzeitige Übertragung aller Arten von Daten über das Transportnetz – unabhängig davon, um welchen Dienst oder welche Anwendung es sich handelt.

Rechenzentren: hohe Flexibilität und Reaktionsfähigkeit

Das zweite zentrale Element eines IT-Systems neben der Datenübertragung ist die Datenverarbeitung und -speicherung. Bei der Bundeswehr decken drei Rechenzentren den Bedarf an Rechenleistung und zentralem Speichervolumen für die Datenverarbeitung ab. Die Standorte in Köln/Bonn, Wilhelmshaven und Strausberg wurden von der BWI grundlegend modernisiert beziehungsweise komplett neu gebaut. Die Server-

HERKULES hat seine Ziele erreicht.

Foto: erhui1979 / DigitalVision Vectors, Fotolia.com

farmen sind über das WANBw miteinander verbunden. So können sie im Verbund arbeiten und lassen sich wie ein einziges logisches Rechenzentrum führen. Zudem werden wichtige Ressourcen doppelt vorgehalten. Auf diese Weise steigen Flexibilität und Reaktionsfähigkeit nachhaltig und eine hohe Ausfallsicherheit ist gewährleistet.

Betriebskontrolle: hoher Automatisierungsgrad

An die Stelle der betreuungsintensiven dezentralen Standorte ist im Zuge von HERKULES ein zentralisierter Betrieb gerückt, der einen hohen Grad der Automatisierung zulässt. Auch der Wildwuchs bei Hard- und Software ist Geschichte. Für den Betrieb von Lotus Notes wurden früher beispielsweise mehr als 1.600 Server in 1.500 Liegenschaften separat verwaltet. Heute sind dafür weniger als 100 Server notwendig. Zudem sind sämtliche Prozesse an bewährten Industriestandards ausgerichtet. Von besonderer Bedeutung ist hierbei das Monitor- und Control-Center (MCC) in Bonn, das die zentrale Steuerung und Überwachung sämtlicher Server übernimmt. Das MCC setzt einheitliche Verfahren, Prozesse und Werkzeuge ein. Dadurch wurde ein Automatisierungsgrad bei der Betriebskontrolle erreicht, der mindestens auf, wenn nicht sogar in Teilen über Industriestandard liegt. Einen weiteren Beitrag zur Effizienzsteigerung leistet eine umfassende Virtualisierung. Diese ermöglicht es, Hardware-Ressourcen besser auszunutzen, da zahlreiche Betriebssysteme und Anwendungen parallel auf einem Server laufen können. Die Vorteile für die Bundeswehr: höhere Flexibilität sowie bessere Verfügbarkeit und Ausfallsicherheit.

Arbeitsplatzausstattung: umfassende Standardisierung und Konsolidierung

So elementar Weitverkehrsnetz und Rechenzentren auch sind, für die Nutzer selbst sind ihre Leistungen so unsichtbar und dennoch selbstverständlich wie Strom aus der Steckdose. Wesentlich greifbarer für sie sind hingegen die Hard- und Software-Ausstattung ihrer Arbeitsplätze sowie ein befriedigender Support.

Hier hat die BWI zunächst eine umfassende Standardisierung und Konsolidierung vorgenommen. Drei Standard-APC-Typen, die regelmäßig aktualisiert werden, haben eine Vielzahl unterschiedlicher PC-Varianten abgelöst. Vormals mehr als 7.000 verschiedene Software-Produkte in unterschiedlichen Versionen wurden auf rund 300 reduziert. Das senkt die Lizenz- und Betriebskosten deutlich. Zudem wurde dadurch ein zentrales Software-Management möglich, das systematische und weitgehend automatisierte Services wie Updates und Patches sowie Aktualisierungen des Betriebssystems bietet. Das zentrale Software- und Patch-Management sorgt dafür, dass die Software der HERKULES-PCs stets auf dem aktuellen Stand ist, und leistet dadurch einen wichtigen Beitrag zur IT-Sicherheit, der die BWI besondere Beachtung schenkt.

Nutzerbetreuung: engmaschiges IT-Service- und Störungsmanagement

Neben einer modernen Arbeitsplatzausstattung trägt eine umfassende Nutzerbetreuung dazu bei, dass sich die Bundeswehr-Angehörigen auf ihre inhaltliche Arbeit konzentrieren können. Mit dem User Help Desk (UHD), den Betriebskompetenzzentren (BKZ) und den Servicecentern hat die BWI das IT-Service- und Störungsmanagement dreistufig aufgebaut. Den Erstkontakt übernimmt der UHD, der für die Bundeswehr-Angehörigen die zentrale Anlaufstelle ist. Der UHD ist ganzjährig rund um die Uhr besetzt. Die BKZ nehmen alle Veränderungen am System vor, sodass sich die Nutzer nicht mehr selbst um Updates oder Installationen kümmern müssen. Die rund 1.000 Mitarbeiter der 25 Servicecenter leisten den Vor-Ort-Service. Innerhalb von zwei Stunden erreichen sie jeden Bundeswehr-Standort in Deutschland. Die umfassende Nutzerbetreuung wird von den Bundeswehr-Angehörigen hoch geschätzt. In regelmäßigen Befragungen zur Zufriedenheit mit dem IT-System erhalten die Mitarbeiter der BWI-Serviceeinheiten kontinuierlich Bestnoten.

Das Weitverkehrsnetz der BWI: ausfallsicher, leistungsstark und flexibel erweiterbar. Foto: erhui1979 /DigitalVision Vectors, Fotolia.com

HERKULES hat alle Ziele erreicht

Stabile und skalierbare Datennetze, ausfallsichere und leistungsstake Rechenzentren, moderne IT-Arbeitsplätze sowie

eine umfassende Nutzerbetreuung – die Bundeswehr verfügt heute über alles, was eine moderne und zuverlässige IuK ausmacht. Und nicht nur das: Das nichtmilitärische IT-System ist so ausgelegt, dass es mit neuen Herausforderungen wachsen kann. So geht die Bundeswehr gut gerüstet in die Zukunft. Das Projekt hat alle Bedingungen erfüllt, die die Bundeswehr seinerzeit an die Entscheidung für die IT-Modernisierung in Form einer öffentlich-privaten Partnerschaft geknüpft hatte: die möglichst schnelle Umsetzung, eine spürbare Entlastung ihres Personals, das bestimmte Aufgaben nun nicht mehr zwingend selbst übernehmen muss, sowie größtmögliche technische Stabilität und damit wirtschaftliche Verlässlichkeit.

Know-how der BWI auch für andere Bundesbereiche nutzbar

Ende 2016 hat HERKULES nun seinen planmäßigen Abschluss gefunden. Geblieben ist die BWI. Als 100-prozentige Bundesgesellschaft sorgt sie weiterhin für den zuverlässigen und sicheren Betrieb der nichtmilitärischen Bundeswehr-IuK. Das IT-System ist nicht nur aktuell gut aufgestellt, sondern lässt sich kontinuierlich weiterentwickeln, damit es den Anforderungen der Streitkräfte stets gewachsen bleibt.

Mit der BWI hat der Bund ein modernes und leistungsfähiges IT-Haus bekommen, das in den vergangenen zehn Jahren einen großen Erfahrungsschatz angesammelt hat. Und das nicht nur in Aufbau und Betrieb von komplexen IT-Infrastrukturen, sondern auch im erfolgreichen Management von äußerst anspruchsvollen und vielschichtigen Großprojekten. Dieses umfassende Know-how, das den Vergleich mit Industriestandards besteht, ist von unschätzbarem Wert – und es eröffnet dem Bund auch in zahlreichen anderen Bereichen Wege, moderne und verlässliche IT-Infrastrukturen zu etablieren beziehungsweise zu konsolidieren. So wurde mit HERKULES ein Fundament gelegt, das noch wesentlich mehr tragen kann als die IuK der Bundeswehr.

Proaktiv, ganzheitlich und stark

Im Gespräch: Ulrich Meister, Vorsitzender der Geschäftsführung der BWI Informationstechnik GmbH und der BWI Systeme GmbH, über die Perspektiven der BWI als Bundesgesellschaft

Herr Meister, lassen Sie uns zunächst einen kurzen Blick zurückwerfen, bevor wir uns der Zukunft widmen: Sie sind bereits seit Mai 2016 Geschäftsführer in der BWI. Wo sehen Sie die Stärken der BWI und was hat Sie bisher am meisten überrascht?

Ulrich Meister: Positiv überrascht hat mich vieles bei der BWI. Zum einen die hohe Qualität der Leistungserbringung – das war in der Außensicht nicht so deutlich. Ebenfalls von außen nicht sofort erkennbar war die hohe Transformationskompetenz der BWI. Tatsächlich ist diese auf dem Stand großer IT-Unternehmen, wenn nicht sogar besser. Auch der große Anteil an sehr guten Mitarbeitern hat mich beeindruckt. In der BWI gibt es, sagen wir es mal so, viele "Hidden Champions", denen man eine noch größere Sichtbarkeit geben sollte. Zu der Kompetenz, eine komplexe Projektlandschaft zu managen, kommt hinzu, dass die Zuverlässigkeit und das Verantwortungsbewusstsein gegenüber dem Kunden sehr hoch sind. Was ich andererseits nicht erwartet hätte, sind die teils noch vorhandenen kulturellen Unterschiede innerhalb der BWI-Gesellschaften.

Ulrich Meister, CEO der BWI Informationstechnik GmbH, im Gespräch. *Foto: BWI*

Wohin wird sich die BWI als 100-prozentige Gesellschaft des Bundes entwickeln?

Da gibt es unterschiedliche Dimensionen. Die eine ist die Bundeswehr. Hier wird die BWI die Bandbreite ihrer Leistungen erweitern und mehr Aufgaben übernehmen, sei es nun auf der Ebene der IT-Infrastruktur, wie Datennetze und Rechenzentren, oder auf der Anwendungsseite, wie etwa SASPF. Es wird für uns darum gehen, die Tiefe und Breite unserer Wertschöpfung zu erhöhen. Damit uns das gelingt, schärfen wir unsere Kernkompetenzen weiter und bauen neue Fähigkeiten auf und aus. Das gilt sowohl für unsere strategischen Kompetenzen als auch für unser Verhalten. Wichtige Stichworte hierbei sind unter anderem: Service- und Kundenorientierung, Proaktivität und Innovation. Das führt zu einem weiteren wichtigen Aspekt: der Effizienz. Hier wird die BWI große Schritte machen, um Benchmark-fähige Preise zu liefern. Denn indem wir unsere Effizienz verbessern, steigern wir auch unsere Wettbewerbsfähigkeit und damit unsere Wachstumschancen. Wir werden zum einen die Wertschöpfung innerhalb der Bundeswehr erhöhen. Zum anderen werden wir künftig auch anderen Ressorts auf Bundesebene standardisierte Portfolioelemente anbieten. In diesem Bereich wird ein interessantes Spannungsfeld aus Zusammenarbeit und Wettbewerb mit dem ITZBund entstehen, mit dem wir einen Leistungsverbund bei der IT-Konsolidierung des Bundes bilden werden.

Welche Chancen, aber auch Herausforderungen ergeben sich Ihrer Meinung nach für die BWI als Bundesgesellschaft?

Die BWI muss nicht mehr mehreren Herren dienen, wie das zu HERKULES-Zeiten mit Bundeswehr, Siemens und IBM der Fall war. Wir haben jetzt nur noch einen Gesellschafter, dessen Zielvorgaben wir zu erfüllen haben. Ein klarer Vorteil. Unser Augenmerk liegt nach wie vor auf Stabilität, Qualität und Effizienz. Allerdings ist jetzt mit Effizienzsteigerung nicht mehr die Gewinnmaximierung gemeint. Vielmehr heißt Effizienz für den Bund: mehr Leistungen für dasselbe Geld. Zudem wird die BWI als IT-Dienstleistungszentrum des Bundes auch IT-Services für andere Kunden aus dem Bereich der öffentlichen Hand anbieten können. Diese Erweiterung des Aufgabenspektrums, gepaart mit dem unternehmerischen Handlungsspielraum einer GmbH, erhöht auch die Attraktivität der BWI als Arbeitgeber.

Welche strategischen Schwerpunkte setzt die neue Geschäftsführung der BWI?

Wir haben im Grunde drei Dimensionen im Fokus: ein stan-

dardisiertes Serviceportfolio mit hoher Innovationskraft, eine starke Kundenorientierung und einen effizienten und wettbewerbsfähigen Servicekatalog. All das müssen wir schnell entwickeln und realisieren, um das IT-Systemhaus für Bundeswehr und Bund zu werden. Wir wollen als ganzheitlicher, proaktiver und starker Partner unseren Wahlspruch "IT für Deutschland" erfüllen. Sowohl für die Bundeswehr als auch für andere Bundesbehörden.

Inwiefern wird sich die Rolle der BWI im Vergleich zur HERKULES-Zeit verändern?

Bei HERKULES war der vertragliche Rahmen im Prinzip klar abgesteckt. Es gab hier und da Ergänzungen und Anpassungen während der Laufzeit, die vom Kunden an uns herangetragen wurden. Jetzt sind wir gefordert, ein anderes Selbstverständnis zu entwickeln und viel stärker proaktiv zu agieren. Künftig werden wir unsere Lösungskompetenz bereits in frühen Projektphasen einbringen und unsere Kunden beraten. Wir fangen also viel, viel eher an, und das proaktiv und nicht wie in der Vergangenheit oft reaktiv. Wir wandeln uns nun zum IT-Systemhaus für Bundeswehr und Bund. Das heißt: Wir bieten die ganzheitliche, proaktive Beratung und Betreuung des Kunden – von der Problemerkennung über die Lösung bis hin zur Implementierung und zum Betrieb. Die BWI erbringt also nicht nur bestimmte Services, sondern fühlt sich für die Qualität und die Zukunftsfähigkeit der IT grundsätzlich zuständig.

Die BWI soll künftig auch Leistungen bei der militärischen IT für die Bundeswehr erbringen. Was wäre hier denkbar?

Ein Thema, das sich förmlich aufdrängt, ist das Desktop-Management. Die BWI betreibt bereits heute für die Bundeswehr mehr als 140.000 Arbeitsplatzcomputer im nichtmilitärischen Bereich. Allein aus Effizienzgründen bietet es sich an, auch das Asset- und Lizenzmanagement für die PCs im Einsatz an die BWI zu übertragen. Insgesamt wird es darum gehen, auch im Einsatz stärker zu standardisierten IT-Lösungen zu kommen – was so heute noch nicht geschieht. Die BWI hat diese Kompetenz. Die Bundeswehr sollte sie nutzen. Auch bei HaFIS und den Auslandsdienststellen sind Synergien denkbar.

Wie will die BWI den Spagat zwischen IT-Systemhaus der Bundeswehr einerseits und IT-Dienstleistungszentrum des Bundes andererseits bewältigen?

Das ist kein Spagat. Zunächst: Die BWI ist Teil der Bundeswehr. Das bedeutet vor allem auch, dass wir gleich gerichtete Interessen haben und die Bundeswehr als Partner dabei unterstützen werden, die besten Lösungen zu finden. Sie wird sich also weiterhin auf die hohe Qualität unserer Services verlassen können. Auf der anderen Seite können nun auch andere Ressorts von unseren Leistungen und Erfahrungen profitieren. Unsere Services sind skalierbar. Dadurch können Synergieeffekte und somit Kostenvorteile erzielt werden, die am Ende zum Vorteil aller sind. Wir werden uns hierfür BWI-intern anders aufstellen, wenn wir mehr als einen Kunden bedienen. Aber das ist lediglich eine organisatorische Frage. Über allem werden jedoch eine einheitliche Strategie, standardisierte Prozesse und eine zentrale Steuerung der Leistungserbringung liegen. Und davon profitieren alle unsere Kunden.

Proaktiv, ganzheitlich und stark: die BWI verfolgt eine klare Strategie als 100-prozentige Bundesgesellschaft. Foto: erhui1979/DigitalVision Vectors, Fotolia.com

Die BWI begreift sich künftig als Innovationstreiber. Warum ist diese neue Denkweise Ihrer Meinung nach erforderlich?

Insbesondere im IT-Bereich sind Innovationen unerlässlich für alle, die Probleme wirklich erkennen und lösen wollen. Nur so kann man der Digitalisierung begegnen und die immer kürzeren Innovationszyklen sinnvoll gestalten. Die Lösungen im IT-Bereich liegen heute zunehmend in den Prozessen, nicht mehr ausschließlich auf technologischer Ebene. Wer hier Vorreiter sein will – und das will die BWI –, muss selbst innovativer denken, um seine eigene Problemlösungskompetenz zu erhöhen. Dafür schaffen wir in unserem Unternehmen die notwendigen Strukturen und auch Freiräume, die es ermöglichen, innovative Lösungen zu erarbeiten und zu erproben. Außerdem werden wir die Bundeswehr beim Aufbau eines Innovati-

on Hub unterstützen. Insgesamt wird es darum gehen, den proaktiv beratenden Tätigkeiten unseren Kunden gegenüber mehr Gewicht zu geben und schon früh in die Problemlösungsprozesse als Partner mit einzusteigen. Dafür werden wir selbst innovative Lösungen entwickeln, aber auch den Markt genau beobachten und mit Blick auf unsere Kunden entsprechend bewerten.

Wie wird die Zusammenarbeit mit der Abteilung CIT im BMVg aussehen?

Eng, kooperativ, partnerschaftlich. Bereits in den vergangenen Monaten haben wir ein gemeinsames Entscheidungsgremium genutzt, in dem wir die Sicht der verschiedenen Bundeswehr-Bereiche austauschen und uns abstimmen. Teilnehmer sind: Staatssekretärin Dr. Katrin Suder, Generalmajor Ludwig Leinhos, Kommandeur CIR, der Abteilungsleiter des CIT Klaus-Hardy Mühleck, der Vize-Präsident des BAAINBw Generalmajor Klaus Veith und ich. In der noch kurzen Zusammenarbeit konnten wir bereits wertvolle Diskussionen führen und gemeinsame Lösungen finden – wie ich meine, eine sehr gute Grundlage für ein konstruktives Miteinander.

Wo liegen die wichtigsten Aufgaben für die BWI in 2017?

Die entscheidenden Schlagworte für die nächste Zeit sind für mich: Verschmelzung, Wandel, Portfolio und Effizienz. Wir sind jetzt gefordert, uns auf die organisatorische und prozessuale Ausrichtung der BWI auf mehr als einen Kunden zu fokussieren. Das ist die Voraussetzung, um unser gewünschtes Wachstum bei bestehender Servicequalität vollziehen zu können. Dafür werden wir die Services aus dem HERKULES-Leistungsvertrag in ein standardisiertes Portfolio überführen, die Effizienz steigern und uns kundenorientiert aufstellen.

Bitte vervollständigen Sie diesen Satz: In vier bis fünf Jahren wird die BWI …

… das IT-Systemhaus der Bundeswehr und auch anderer Bundesressorts sein. Die BWI wird der verlässliche und innovative Partner sein, der zukunftsfähige IT-Lösungen bietet. Unser Leistungsspektrum wird massiv gewachsen sein. Dabei werden wir sicherlich nicht mehr bei allen Services die Leistungstiefe abbilden, wie das heute der Fall ist. Das wiederum eröffnet externen Dienstleistern die Chance, uns mit ihren Services zu unterstützen.

Die neue BWI – eine Organisation für die Zukunft

Dr. Jürgen Bischoff, Geschäftsführer Corporate Human Resources der BWI Informationstechnik GmbH

Dr. Jürgen Bischoff

Das Jahr 2017 steht für die BWI unter dem Motto "Aus zwei mach eins". Spätestens Anfang 2018 soll aus den derzeit zwei Gesellschaften BWI Systeme und BWI Informationstechnik ein Unternehmen geworden sein. Dazu wird die BWI Systeme auf die BWI Informationstechnik verschmolzen. Damit verbunden ist eine Neustrukturierung der Aufbau- und Ablauforganisation. Dabei soll die neue Aufbauorganisation – zunächst in Form einer Projektorganisation – möglichst früh gelebt werden und damit auch das kulturelle Zusammenwachsen unterstützen.

Die neue Organisation wird sowohl eine stärkere Kundenorientierung als auch eine professionellere Handhabung des erweiterten Leistungsspektrums ermöglichen. Kurz: Die BWI stellt sich als IT-Systemhaus des Bundes auf.

Die Geschäftsführung setzt sich aus dem Chief Executive Officer und Vorsitzenden der Geschäftsführung Ulrich Meister, der Chief Financial Officer Katharina Hollender und dem Chief Human Resources Officer Dr. Jürgen Bischoff zusammen.

Unterstützt wird die Geschäftsführung von der Geschäftsleitung, die sechs Mitglieder zählt: den Leiter Account Management Michael Krause, den Leiter Innovation, Solution & Delivery Management Dr. Christian Marwitz, die drei Leiter der Delivery-Einheiten André Prekop, Robert Knapp und Christine Serrette sowie die Leiterin des Bereichs Corporate Development & Strategy Saskia Ringleff. Damit besteht das Managementteam der neuen BWI aus organisationserfahrenen und neu hinzugekommenen Personen, die ein breites Wissen und vielfältige Erfahrungen aus unterschiedlichen Unternehmen einbringen können.

Gemeinsam ist allen der Wille, die Werte der BWI, "Verlässlichkeit", "Kreativität", "Respekt", "Leistung" und "Offenheit", mit Leben zu füllen. Zudem wollen sie das Ziel, Systemhaus des Bundes zu werden, möglichst rasch erreichen – ohne allerdings den Hauptkunden Bundeswehr aus dem Fokus zu verlieren.

Kundenorientierung und hohe Leistungsfähigkeit stehen an erster Stelle

Mit neuen Kundenanforderungen wird ein noch kundenorientierter aufgestelltes Account Management notwendig. Das neue Account Management sorgt daher mit einer Aufstellung nach Key Accounts für eine noch stärkere Ausrichtung an den spezifischen Erwartungen und Bedürfnissen der einzelnen Kunden. Entlang dieser neuen Aufstellung wird ein effizienter Ende-zu-Ende-Vertriebsprozess aufgebaut und von einem operativ orientierten Sales Reporting begleitet. Die enge Abstimmung mit der Delivery steht hierbei stets im Mittelpunkt. Darüber hinaus öffnet sich die BWI gegenüber strategischen Partnerschaften, um neue Themen zu bedienen. Ein weiteres Ziel ist, ein kompetentes Team aufzubauen, das die Fähigkeiten für Großaufträge bündelt und die langfristige Planung und das Partnermanagement sicherstellt. So wird eine proaktive Vertriebskultur gezielt und aktiv gefördert.

Um auch künftige technologische Entwicklungen beurteilen und ihre Einsatzmöglichkeiten frühzeitig erproben zu können, wird zudem ein zentrales digitales Transformationsmanagement etabliert. Schlüsselelemente hierbei sind das Strategische Portfolio Management der BWI, das Innovationsmanagement und die Steuerung der BWI-eigenen Unternehmens-IT. All diese Aspekte sind im neuen Bereich Innovation, Solution & Delivery Management (ISDM) gebündelt, wo auch das übergreifend agierende Strategische Service Management angesiedelt ist. Daneben wird in der BWI die Funktion des Chief Information Security Officers neu eingerichtet, die sowohl in der BWI als auch für unsere Kunden für ein Höchstmaß an IT-Sicherheit sorgen soll.

Der Übergang bei der Übernahme neuer Kunden und Leistungsfelder findet in Zusammenarbeit mit den drei Delivery-Einheiten statt. Hier schlägt das Herz der BWI, in diesen Bereichen erfolgt die Leistungserbringung. Die Delivery der BWI besteht aus drei Unternehmensbereichen mit unterschiedlichen Schwerpunkten, die sich in dieser Publikation noch einzeln vorstellen. Dies sind Cloud Infrastructure Services (CIS), User Communication Services (UCS) und Business Consulting & Application (BCA).

CIS umfasst unter anderem die Bereitstellung und den Be-

trieb von Server- und Storage-Systemen sowie Anwendungen im Bereich der Altsysteme. UCS verantwortet geschäftsprozessübergreifende Anwendungen, Netze, Endgeräte, Vor-Ort-Services sowie das IT-Projekt-Management und das Lizenz-Management. BCA sorgt für Applikationen aus einer Hand und einen größeren Fokus auf Beratung. Da nur ein vollständig integrierter Delivery-Prozess die Servicequalität der BWI auch zukünftig sicherstellen kann, wird hierauf besonders geachtet.

Neu strukturierte zentrale Einheiten unterstützen Leistungserbringung

Um ihre Leistungen erbringen zu können, benötigt die BWI eine zukunftsfähige und passende Kompetenzstruktur. Den Kompetenzaufbau verwirklicht die BWI mit strategischem Recruiting und gezielter Mitarbeiterentwicklung. Entsprechend ist der Corporate-Human-Resources-Bereich (CHR) aufgestellt. Funktionen wie Learning & Development, Staffing & Resourcing inklusive einer umfangreichen eigenen Ausbildung und Studienförderung sowie die auf die Führungskräfte ausgerichtete HR-Business-Partner-Organisation sichern die künftige Kompetenzstruktur. Ergänzt wird der CHR-Bereich von Funktionen wie Labour Relations, Occupational Safety, Health & Environmental Protection und Fleet Management.

Der kaufmännische Bereich unterstützt das operative Geschäft bestmöglich mit einem Team aus kaufmännischen Leitern und Business-Partnern, effizientem Performance-Management und einem professionellen Einkauf sowie Einheiten, die die Einhaltung gesetzlicher Vorgaben sicherstellen, zum Beispiel Steuern und Recht sowie interne Kontrollsysteme. Mit einem umfassenden Finance- und Accounting-Bereich ist der kaufmännische Bereich professionell aufgestellt.

Neu geschaffen wurde der Zentralbereich Corporate Development & Services, der übergreifende Funktionen von Qualität & Risiko, Compliance, Prozessmanagement, Governance & Performance Services bis zu Strategie und Kommunikation in einem Bereich bündelt. Diese Services heben Synergien, schaffen Transparenz, optimieren die Zusammenarbeit und erbringen notwendige zentrale Dienstleistungen und Governance-Funktionen. Daneben liegt hier die Verbindungsstelle zur unternehmerischen Steuerung der BWI durch die Abteilung CIT des BMVg.

Die Zukunft kann kommen. Die BWI ist hierfür gut aufgestellt.

Die Zielorganisation der BWI. Foto: BWI

Software Defined Storage – ein wesentlicher Schritt zur digitalen Verwaltung

Stetig wachsende Datenmengen und die Nutzung mobiler Endgeräte führen dazu, dass auch der Bedarf an flexiblem Speicher stetig wächst. Dazu kommen neue Technologien wie etwa Body-Cams oder digitale Informationsdienste, die gewaltige Datenmengen erzeugen. Proprietäre Lösungen bieten Behörden zu wenig Flexibilität, denn Systemerweiterungen sind sehr kostspielig und nur mit großem Aufwand auf dem aktuellen Stand der Entwicklung zu halten. Cloud Computing und das softwarebasierte Rechenzentrum bieten hier zukunftsweisende Lösungen und ebnen den Weg in die digitale Verwaltung.

Branchengrößen wie Amazon, Google oder Netflix haben die Nutzung und Bereitstellung von IT grundlegend verändert, indem sie ihre Services aus rein softwarebasierenden Rechenzentren heraus zur Verfügung stellen. Fakt ist, dass Cloud Computing und softwarebasierte Infrastrukturen in allen Behörden und Unternehmen Einzug halten – bei manchen sind sie bereits Teil der strategischen Ausrichtung, doch der Großteil der deutschen Behörden und Unternehmen hat das Thema Software-Defined noch auf der Aufgabenliste.

Zur erfolgreichen Umsetzung dieser Strategie ist es notwendig, alle Elemente der IT-Infrastruktur zu virtualisieren und an einem einzigen Servicepunkt zur Verfügung zu stellen. Software Defined Storage ist die wesentliche Säule im Wandel zu einer softwarebasierten Infrastruktur, da sie die Grundlage für Agilität in der IT bildet. Softwarebasierte Storage-Lösungen setzen hier neue Maßstäbe, in dem sie sich zum Beispiel als Basis für OpenStack-Umgebungen anbieten und durch die gleichzeitige Unterstützung klassischer Storage-Protokolle einen “sanften Übergang” ermöglichen.

Open Source und Hybrid Cloud: Innovation, Agilität und Flexibilität

Die IT-Abteilungen kämpfen schon seit Jahren mit einem enormen Anstieg der Anforderungen an Storage und Rechenleistung. Die stetig steigenden Aufwände für proprietäre Systeme verhindern Innovation. Daher haben bisher gültige Strategien in der digitalen Transformation ausgedient.

Im “Software Defined Datacenter” der Zukunft werden viele Behörden die erforderliche Leistung nicht mehr ausschließlich im eigenen Rechenzentrum erbringen wollen und können. In Leistungsspitzen kann etwa die Public Cloud die interne IT sinnvoll ergänzen. Gemeinsam bilden Private- und Public-Cloud dann eine Hybrid Cloud. Auch die unaufhaltsam wachsenden Speicheranforderungen können über einen hybriden Ansatz effektiv abgebildet werden: indem die individuelle IT-Infrastruktur mit den Cloud-Diensten nahtlos zusammen arbeitet. Hier können Software Defined Storage-Lösungen (SDS) durch die Unterstützung der gängigen Protokolle und einer “Scale Out”-Architektur die richtige Lösung bieten.

SDS fördert Agilität

Die richtige SDS-Lösung sollte offen, selbstreparierend und -verwaltend sein sowie nahezu unbegrenzt skalierbare Speicherkapazitäten bieten. Im Gegensatz zu herkömmlichen Speichersubsystemen sollte jeder zusätzliche Hardwareknoten nicht nur die Kapazität erweitern, sondern auch die Performance. Also ein echtes “Scale Out”-System, welches darüber hinaus auch die Möglichkeit bietet, Speicherplatz über Standorte und Hardware-Systeme beliebig zu verteilen. Damit können Behörden etwa landes- oder bundesweite Ressourcen bereitstellen, deren Konsistenz jederzeit sichergestellt ist. Ohne die Begrenzungen auf ein monolithisches System können Storage-Ressourcen effizienter genutzt und die Verwaltung durch automatisiertes, regelbasiertes Management wesentlich vereinfacht werden. Durch die vollständige Entkopplung von Speicher-Hardware und Speicher-Software entfällt auch die aufwändige und immer riskante Migration von Daten. Software-Updates und der Austausch von Hardware finden so im laufenden Betrieb statt.

Fazit

Die Flexibilität klassischer Speichersysteme ist an einem kritischen Punkt angekommen, denn die IT-Infrastrukturen der Behörden müssen immer schneller auf Veränderungen reagieren. Die Bereitstellung von Software-Produkten ist durch Verfahren wie DevOps im Minutentakt möglich, monatelange Datenmigrationen auf herkömmlichen Speichersysteme sind da kontraproduktiv.

Es lohnt sich also immer, die Vorteile von SDS genauer zu betrachten. Mit der richtigen Lösung, erlangen Behörde die Flexibilität und Agilität, die sie benötigen, um die künftigen Anforderungen der Fachreferate schnell und kostengünstig zu erfüllen. www.suse.com

rsCyInt®

Cyber Intelligence

Intelligente Cyber-Auswertung

Wann steht Ihre Organisation im Fokus?! Eine Vielzahl von IT-Lösungen identifiziert sicherheitsrelevante Ereignisse, Cyberattacken, Hacks, Viren, Trojaner, Schadsoftware – aber wie wird daraus Handlungsfähigkeit? Hinter jeder Attacke stecken Menschen – Einzeltäter oder kriminelle Gruppen. Oft liegen Erkenntnisse aus anderen Ermittlungsbereichen bereits vor. Wie können die Erkenntnisse zusammengeführt werden?

rsCyInt® – das ist Analyse und Verknüpfung strukturierter und unstrukturierter Daten aus IT Security Operation Systemen - und aus realen Ermittlungserkenntnissen.

Damit aus Informationen ein Situationsbild entsteht: Voraussetzung für **Abwehr, Schutz** und **Prävention.**

Funktionalität von rsCyInt®

- Tatbestände, Beziehungen und Muster bei Cyber-Attacken identifizieren
- Cyber-Vorfälle mit Ermittlungs-Erkenntnissen aus der realen Welt verbinden
- Automatischer und manueller Import aus unterschiedlichen Quellen
- Nutzung von Informationen aus der Analyse sozialer Medien
- STIX Schnittstelle und Datenmodell
- Zahlreiche Recherchefunktionen wie Wildcard-, fragmentarische, phonetische, Ähnlichkeits-, Komplex-Suche, GIS- Recherche
- Automatische Entitäts-Extraktion
- Duplikats-Meldewesen
- Automatische Warnung bei neuen Erkenntnissen
- Integration von GIS-Systemen zur Darstellung geographischer Beziehungen
- Generator für die Erstellung von Anfragen, Formularen, Berichten und Statistiken
- Oberfläche und Workflow Management anpassbar
- Skalierbare Zugangskontrolle durch Rechte- und Rollenkonzept
- Wiedervorlage- und Löschfristenkontrolle

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

rola Security Solutions

T · Systems

Das Management-Team der BWI

Die Geschicke der BWI werden von drei Geschäftsführern gelenkt: Ulrich Meister, Dr. Jürgen Bischoff und Katharina Hollender. Hinzu kommt eine Geschäftsleitung, die mit Michael Krause, Dr. Christian Marwitz, André Prekop, Robert Knapp, Christine Serrette und Saskia Ringleff sechs Mitglieder zählt und direkt an den CEO berichtet. Wir stellen die Personen zu diesen Namen vor:

Ulrich Meister ist Vorsitzender der Geschäftsführung der BWI Informationstechnik GmbH sowie der BWI Systeme GmbH. Der 56-Jährige trat im Mai 2016 in die Geschäftsführung der BWI ein und verantwortete in dieser Funktion das Account Management. Im Dezember 2016 wurde er zum Chief Executive Officer (CEO) ernannt. Bevor Ulrich Meister zur BWI kam, fungierte er als Leiter Kontinentaleuropa beim IT-Dienstleister Wipro Technologies. Bis 2013 hatte der Mathematiker und Volkswirtschaftler das Systemintegrationsgeschäft der Telekom-Tochter T-Systems geleitet.

Dr. Jürgen Bischoff ist als Geschäftsführer der Chief Human Resource Officer der BWI Informationstechnik GmbH. Der 51-Jährige kam 2007 zur BWI und übernahm die Aufgaben des Bereichsleiters Personalmanagement, war Sprecher der Betriebsleitungen sowie Leiter der BWI Akademie. Vor seinem Wechsel zur BWI war der promovierte Wirtschafts- und Sozialwissenschaftler in verschiedenen Consulting- und Führungsfunktionen der Siemens AG tätig. Zuletzt leitete er bei Siemens Business Services den Bereich HR M&A / Subsidiaries.

Katharina Hollender ist kaufmännische Geschäftsführerin der BWI Informationstechnik GmbH und der BWI Systeme GmbH. Ende 2016 kam sie als Chief Financial Officer (CFO) zur BWI. Von 1998 bis 2016 war die 50-Jährige bei der Deutschen Telekom AG sowie verschiedenen Tochtergesellschaften des Telekommunikationsunternehmens in führenden Positionen für Controlling und Finanzen tätig. Frühere berufliche Stationen machte die Diplom-Kauffrau bei o.tel.o. communications GmbH & Co., Vebacom GmbH und LION Gesellschaft für Systementwicklung mbH.

Michael Krause ist Mitglied der Geschäftsleitung der BWI Informationstechnik GmbH. In dieser Funktion ist er verantwortlich für das Account Management. Der 48-Jährige ist seit 2007 bei der BWI. In dieser Zeit war er Leiter des Büros der Leitung, Compliance Officer und Leiter Interne Revision. Nach mehreren Jahren in Vertriebs- und Marketingfunktionen im Mittelstand und einem Masterstudium war er seit 1995 in verschiedenen Funktionen bei Siemens tätig, zuletzt als Leiter Strategie bei Fujitsu Siemens Computers IT Product Services.

Dr. Christian Marwitz verantwortet in der Geschäftsleitung der BWI Informationstechnik GmbH das Innovation, Solution & Delivery Management (ISDM). Der 40-Jährige kam 2007 zunächst als beurlaubter Soldat zur BWI. Ab 2008 übernahm er verschiedene Leitungsfunktionen im Bereich der Betriebskompetenzzentren (BKZ), zuletzt war der promovierte Wirtschaftswissenschaftler Segmentleiter Service Delivery Management.

André Prekop ist Mitglied der Geschäftsleitung der BWI Informationstechnik GmbH. In seinen Verantwortungsbereich fällt der Service-Delivery-Bereich User Communication Services (UCS). Der 56-Jährige kam 2007 zur BWI – als Geschäftsführer der BWI Services GmbH, Chief Operations Officer und Mitglied der Geschäftsleitung der BWI Informationstechnik GmbH. 2006 war der Diplom-Ökonom als Planungsbeauftragter der Leistungserbringung im Projekt HERKULES für die Siemens AG tätig, wo er bereits seit 1992 mit verschiedenen Aufgaben betraut gewesen war.

Robert Knapp ist Mitglied der Geschäftsleitung der BWI Informationstechnik GmbH und verantwortet den Service-Delivery-Bereich Cloud Infrastructure Services (CIS). Der 48-Jährige kam 2010 zur BWI Systeme GmbH und war zuletzt Bereichsleiter SD IT (Service-Delivery-Bereich IT-Infrastruktur) sowie Mitglied der Geschäftsleitung der BWI Systeme GmbH. Vor seinem Wechsel zur BWI hatte der Nachrichtentechnik-Ingenieur verschiedene Führungspositionen bei IBM inne.

Christine Serrette zeichnet als Mitglied der Geschäftsleitung der BWI Informationstechnik GmbH für den Service-Delivery-Bereich Business Consulting & Application (BCA) verantwortlich. Die 49-Jährige ist 2009 bei der BWI Systeme GmbH als Abteilungsleiterin Interne IT, Desktop Management und 2nd Level Support eingestiegen. 2010 wurde sie Leiterin der Hauptabteilung “Applikation 1 – Zentrale Dienste”, 2016 wechselte sie als Leiterin in die Hauptabteilung “Applikation 2 – SAP und Applikationen”. Vor ihrem Wechsel zur BWI war die Diplom-Kauffrau u.a. für Logitech und Unilever tätig.

Saskia Ringleff ist als Mitglied der Geschäftsleitung der BWI Informationstechnik GmbH für den Bereich Corporate Development & Services verantwortlich. Die 30-Jährige kam 2016 zur BWI. Zuvor war die Wirtschaftssinologin bei Wipro Technologies als Head of Strategy and Business Functions Europe tätig. Frühere berufliche Stationen machte Saskia Ringleff bei T-Systems und Sennheiser.

Innovation als Schlüssel zum Erfolg

Markus Hauff, Leitung Innovationsmanagement,
BWI Informationstechnik GmbH

Markus Hauff

Innovation bedeutet Erneuerung. Im Bereich der IT entsteht sie unter anderem, indem neue oder bekannte Technologien, Produkte oder Prozesse kombiniert werden. So entstehen neue oder weiterentwickelte Lösungen. Dabei ist stets eine zusätzliche Wertschöpfung das Ziel. Dieser Vorgang ist besonders erfolgreich, wenn er in enger Interaktion mit Anwendern, im interdisziplinären Austausch und unter kreativitätsfördernden Bedingungen stattfindet.

Innovationen erfordern Anstrengung und Kreativität von Menschen mit Ideen, Mut und Leidenschaft für Veränderungen. Innovationen brauchen eine klare Vision sowie die bereitwillige und engagierte Unterstützung des Managements bis hinein in die Geschäftsführung. Dabei sind Innovation und Management zunächst gegensätzliche Mechanismen. Ein Zuviel an Innovation und ein Zuwenig an Management ist ebenso wenig Erfolg versprechend wie andersherum. Daher ist eine ausgewogene Vorgehensweise erforderlich, die bestehende Strukturen im Unternehmen mit neuen Elementen kombiniert. Hier greift das Innovationsmanagement (IM). Darunter versteht man die systematische Planung und Steuerung von zielgerichteten Veränderungen, also die Generierung, Kanalisierung und Priorisierung von Ideen sowie deren Umwandlung in konkrete Wertschöpfung. Dabei ist das Management von Innovationen als Teil der Unternehmensstrategie zu verstehen und umzusetzen. Damit bezieht sich IM auf das gesamte Leistungsspektrum des Unternehmens.

Bislang lag der Fokus auf klar definierten Vorgehensweisen

So weit, so gut. Doch wie ist es in Sachen Innovation bei der BWI bestellt? Und wie möchte das Unternehmen künftig damit umgehen? In der HERKULES-Zeit, also den Jahren 2006 bis 2016, war die BWI der IT-Dienstleister der Bundeswehr. Als klassische Delivery-Organisation hatte sie Innovation im eigentlichen Sinn nicht in ihrem unmittelbaren Fokus. Es war in dieser Form auch nicht von ihr gefragt, denn der HERKULES-Vertrag gab klar vor, welche Leistungen wie zu erbringen waren. Daraus resultierte eine geschlossene und strukturierte Funktionsweise nach klar definierten Prozessen und Absprachen mit dem Kunden, wie beispielsweise Service-Level-Agreements (SLA).

Und die BWI funktionierte gut. Der Betrieb war äußerst stabil und die Services sehr ausfallsicher angelegt. Ein guter Zustand. Doch Innovationen sind hier schwer einzubringen, denn jede Neuerung bedeutet Veränderung. Und jede Veränderung hätte sich gegebenenfalls auf die SLA ausgewirkt und damit auf die Kosten. Das Budget erlaubte jedoch nur, dass die SLA genau so erfüllt wurden wie vereinbart. Eine Pattsituation – und nicht der beste Nährboden für die Entwicklung neuer Ideen und deren erfolgreiche Umsetzung.

Zwar hat die BWI bereits in der Vergangenheit die Kreativität ihrer Mitarbeiter gefördert, Freiräume und Anreize für Innovation geschaffen sowie die kontinuierliche Verbesserung in den Unternehmensrichtlinien verankert. Doch ein definiertes und etabliertes Innovationsmanagement gab es bislang nicht. Das ändert sich nun.

Auch BMVg arbeitet an Innovationsmanagement

Die BWI hat den HERKULES-Vertrag sehr gut erfüllt. Jetzt beginnt ein neues Kapitel – nicht nur als 100-prozentige Gesell-

BWI wird ein nachhaltiges Innovationsmanagement etablieren.

Foto: erhui1979/DigitalVision Vectors, Fotolia.com

schaft des Bundes. Das Unternehmen wandelt sich von einer Delivery-Organisation hin zu dem IT-Systemhaus der Bundeswehr. Ausdrücklich gewünscht und gefordert von ihrem neuen Eigentümer wird die BWI künftig auch neue Formen von IT-Dienstleistungen erbringen, wie zum Beispiel Cloud Computing und Services im Bereich der einsatzrelevanten IT der Bundeswehr. Darüber hinaus soll sie auch andere Ressorts oder Bundesbehörden mit IT-Services bedienen. Dies kann jedoch nur mit einer hohen Innovationsfähigkeit gelingen – seitens der BWI und auf Seite der Bundeswehr. Daher arbeiten sowohl BMVg als auch BWI daran, in ihren Organisationen ein nachhaltiges Innovationsmanagement zu etablieren und diese miteinander zu verknüpfen.

Anforderungen an Mobilität und Flexibilität bestimmen die Richtung für künftige Entwicklungen in der IT. *Foto: erhui1979/DigitalVision Vectors, Fotolia.com*

Die BWI ist nun gefordert, als Treiber von Innovation das IT-System der Bundeswehr voranzubringen und einen umfassenden Gestaltungsauftrag zu übernehmen. Nicht nur der Geschäftsauftrag und die Kundenanforderungen, sprich in allererster Linie die Bedürfnisse der Bundeswehr, fordern dies. Hinzu kommt das technologische Umfeld, in dem sich die BWI bewegt. Der Markt wird zunehmend der wesentliche Impulsgeber für Innovationen. Nehmen wir nur die Schlagworte Cloud Computing, Big Data und Internet of Things: In den vergangenen Jahren hat die Anzahl potenziell disruptiver Technologien, sprich Innovationen, die eine bestehende Lösung möglicherweise vollständig verdrängen, rasant zugenommen. Der strukturierte Umgang mit diesen Entwicklungen und eine zielgerichtete Prüfung, ob sie für das eigene IT-System adaptiert werden sollten, sind unerlässlich geworden. Auch gesellschaftliche Veränderungen wirken auf die Überlegungen ein. Nicht nur die Bundeswehr, sondern auch die BWI muss sich als attraktiver Arbeitgeber positionieren. Die sogenannten Millennials, die in den kommenden Jahren auf den Arbeitsmarkt drängen, setzen die Verfügbarkeit mobiler Anwendungen und benutzerfreundlicher Schnittstellen schlicht voraus.

Geschäftsstrategie gibt Richtung für Innovationen vor

Die vielfältigen Herausforderungen, die aus Geschäftsauftrag, Kundenanforderungen, technologischem Umfeld und gesellschaftlichen Entwicklungen erwachsen, verdeutlichen, warum die BWI den Ausbau ihrer Innovationsfähigkeit als einen zentralen Punkt ihrer Unternehmensstrategie begreift. Ein IM schafft eine wesentliche Grundlage, um als strategischer Partner zeitgemäße und zukunftsfähige Leistungen erbringen zu können. Dabei geschieht Innovation nicht um der Innovation willen. Vielmehr ist die Geschäftsstrategie der maßgebliche Korridor, in dem sich Innovation bewegt. IM dient der BWI zur kontinuierlichen Weiterentwicklung ihres Portfolios.

Apropos Portfolio: Wer sich als IT-Systemhaus versteht, muss auch Lösungen anbieten, die er heute noch nicht im Portfolio hat. Es gilt, die Kunden- und Geschäftsanforderungen kontinuierlich zu analysieren, den Markt auf passende Lösungen hin genau zu prüfen und dann Vorschläge hinsichtlich einer Serviceentwicklung und zeitgerechten sowie wirtschaftlichen Implementierung zu unterbreiten. Und sollte es die entsprechenden Lösungen noch nicht auf dem Markt geben, wird man gefordert sein, selbst in Zusammenarbeit mit geeigneten Partnern in der Entwicklung aktiv zu werden. Es wird also für die BWI unerlässlich sein, ein starkes Engagement im Bereich des strategischen Portfoliomanagements zu entwickeln. Die Stoßrichtung ist dabei klar: Das Portfolio der BWI muss bedarfsorientiert, flexibel, anpassbar, leistungsstark, hochmodern, effizient und zukunftsgerichtet sein – und hat bei alldem selbstredend den hohen Sicherheitsanforderungen der Bundeswehr und anderer Ressorts beziehungsweise Behörden gerecht zu werden. Um hier die notwendige Durchschlagskraft zu erzielen, ist es sinnvoll, das strategische Portfoliomanagement, das IM und die Interne IT der BWI eng miteinander zu verzahnen. Von dem Zusammenführen der drei Bereiche im Innovation, Solution & Delivery Management (ISDM) erhofft sich die BWI verschiedene positive Effekte. Zunächst lassen sich Innovationen schneller ins eigene Unternehmen bringen. Hier kann dann das Potenzial der Lösung ordentlich bewertet und im Folgenden eine entsprechend zügige Transferleistung in eine Serviceentwicklung für den Kunden erzielt werden.

Gute Perspektiven für Kunden und Mitarbeiter der BWI

Der Weg der BWI zu einem innovationsstarken Unternehmen erfordert ein Umdenken auf vielen Ebenen. Die Grundlage bildet die Anpassung der Prozesse, der Organisation und der Unternehmenskultur. IM ist eine unternehmensweite Aufgabe, die es zielgerichtet über definierte Verfahren, Schnittstellen und Ansprechpartner auszugestalten gilt. Eine Schlüsselrolle hat hierbei die Unternehmenskultur, denn kreatives und visionäres Verhalten setzt ein förderliches Umfeld mit flexiblen Strukturen und entsprechender Fehlertoleranz voraus. Hier kann die BWI vielfältige Rahmenbedingungen schaffen. Dazu zählen zum Beispiel die Verankerung von Innovation im betrieblichen Anreizsystem, die Schaffung von Freiräumen für kreatives Denken im operativen Tagesbetrieb, entsprechend flache Hierarchien in der Unternehmensstruktur sowie die Vernetzung von Mitarbeitern und die Zusammenstellung interdisziplinärer Teams.

Abseits struktureller Grundlagen und Prozesse ist der Wandel zu einem innovativen Unternehmen ein kontinuierlicher Veränderungsprozess. Bis die neue Herangehensweise als Chance verstanden, gelernt und schließlich gelebt wird, wird die BWI sicherlich mehrere Jahre benötigen. Doch das Engagement wird sich lohnen: Die BWI kann dem innovativen Denken ihrer Mitarbeiter einen festen Rahmen geben und deren Ideen in die Tat umsetzen. So lässt sich das große Potenzial, das bereits heute vorhanden ist, voll zur Entfaltung bringen und in echten Kundennutzen verwandeln. 2006 hat sich die BWI schon einmal selbst erfunden. Jetzt ist sie gefordert, sich erneut neu zu finden und zu erfinden. Mit dem Aufbau eines soliden Innovationsmanagements schafft sie dafür wichtige Grundlagen und stellt die Weichen für ihre erfolgreiche Zukunft.

Gut aufgestellt für neue Herausforderungen

Drei Delivery-Bereiche übernehmen die Leistungserbringung der BWI: User Communication Services, Cloud Infrastructure Services und Business Consulting & Application

Bundeswehr und BWI haben ein neues Kapitel aufgeschlagen: Am 28. Dezember 2016 schlossen die beiden Partner einen neuen Vertrag, der ihre Zusammenarbeit für die kommenden sieben Jahre regelt. Wie bereits während der HERKULES-Zeit organisiert die BWI ihre Leistungserbringung in ihrer Service Delivery. Die zahlreichen Aufgaben wurden in drei Bereiche unterteilt:

- User Communication Services (UCS)
- Cloud Infrastructure Services (CIS)
- Business Consulting & Application (BCA)

Der Zuschnitt der Delivery hat sich in der Vergangenheit bewährt. Daher wird an der Aufgabenverteilung im Wesentlichen auch in Zukunft festgehalten. Dort, wo sinnvoll, wurden Leistungen stärker bei einem Bereich gebündelt, um die Kundenbedürfnisse künftig noch besser aus einer Hand bedienen zu können. Auch bei der personellen Besetzung setzt die BWI auf Kontinuität. Mit André Prekop (UCS), Robert Knapp (CIS) und Christine Serrette (BCA) werden die Bereiche von drei erfahrenen Managern geführt, die sich bereits seit vielen Jahren in der Delivery der BWI engagieren und bestens vertraut mit den Anforderungen der Bundeswehr sind.

Die drei Leitungen der Service-Delivery-Bereiche sind Teil der neuen BWI-Geschäftsleitung und damit dem Chief Executive Officer der BWI direkt unterstellt. Dadurch rücken die Service-Delivery-Leiter auch organisatorisch enger zusammen, um die Leistungserbringung ihrer Bereiche eng miteinander abzustimmen und zu verzahnen. Im Folgenden stellen die drei verantwortlichen Mitglieder der Geschäftsleitung die Aufgaben und Leistungen ihrer Delivery-Bereiche vor. Zudem geben sie einen Ausblick, wie sich ihr jeweiliges Portfolio in Zukunft bei Bedarf noch erweitern ließe, damit die BWI als IT-Systemhaus für die Bundeswehr und als IT-Dienstleistungszentrum des Bundes für andere Ressorts und Behörden überzeugen kann.

Die Leistungen der BWI-Delivery-Bereiche sind aufeinander abgestimmt.

Foto: erhui1979, DigitalVision Vectors, Fotolia.com

Digitalisierung als Zukunftsprojekt

Ralf Oehlmann und Mario Riesmeier

Die Digitalisierung ist auch für den Öffentlichen Sektor eine Herausforderung. Es geht jedoch nicht allein darum, die IT zu modernisieren, sondern ein ganzheitliches Konzept für den Aufbau einer zukunftsfähigen IT-Infrastruktur zu etablieren.
Mittlerweile stellt sich der Öffentliche Sektor der Herausforderung der Digitalen Transformation, aber sehr oft fehlt dafür ein konsistentes, ganzheitliches digitales IT-Konzept. Häufig gibt es keine strategische Zielarchitektur und die damit verbundenen auditierten Standards. Vielfach werden nur einzelne Prozesse herausgelöst, analysiert und auf die eine oder andere Weise digitalisiert.
Im Allgemeinen orientieren sich Behörden bezüglich Technologie immer noch am Bestehenden und nicht an Innovationen. Digitale Transformation erfordert aber einen gänzlich neuen Denkansatz, der das bisherige Zusammenwirken von Menschen und Technik, von IT und Kommunikation neu organisiert.

Flexibilität und Agilität steigern

Die Einführung einer E-Akte ist für die Behörden ein erster wichtiger Schritt in die Digitalisierung. Durch die Unterstützung erfahrener Partner können alte Zöpfe abgeschnitten und neue technologische Wege einschlagen werden. Mit einer strukturierten Bedarfsanalyse kann er zügig ermitteln, wo konkrete Ansatzpunkte für eine IT- und Prozessoptimierung innerhalb der gesetzlichen Vorgaben bestehen, welche bedarfsgerechten Ressourcen bereitgestellt werden sollten und wo Aufwände eingespart werden können.
Zu den interessanten neuen Technologien mit großem Einsparungspotenzial zählt auch für den Öffentlichen Sektor Cloud Computing. Cloud-Modelle ermöglichen es, Infrastrukturen und Dienste, wo immer es sinnvoll ist, zu automatisieren und/oder auszulagern und durch On-Demand-Konzepte Kosten zu reduzieren. Auch die Bereitstellung von Fachanwendungen als Software-as-a-Service mindert die Wartungskosten der IT ganz erheblich.
Cloud Computing bietet viele Vorteile, zum Beispiel flexible Servicemodelle, mit denen kurzfristige Spitzenbeanspruchungen, wie in einem Krisenfall, abgefangen werden können. Somit können zusätzliche Ressourcen bei Bedarf einfach abgerufen werden. Auch E-Government-Lösungen können in der Cloud betrieben werden. Lösungen, wie das einsatzfertige und OKeVA-konforme (Organisationskonzept elektronische Verwaltungsarbeit) CGI E-Government Framework, werden bereits heute von 20.000 Anwendern in Deutschland genutzt.
Vor dem Hintergrund der Anforderungen des E-Government dürfen sich Verwaltungen nicht damit zufriedengeben, nur einzelne Prozesse zu automatisieren. Sie müssen insgesamt ihre Verfahren so strukturieren, dass sie automatisierbar sind. Die sich abzeichnende immer weitergehende Verlagerung der internen Verfahren nach außen, zum Beispiel zu Bürger-Self-Service-Portalen, ist anders gar nicht darstellbar. Man denke in diesem Zusammenhang zum Beispiel auch an die Übergabe von Akten an Gerichte sowie Anfragen nach dem Informationsfreiheitsgesetz.
Die Bürger leben bereits in der digitalen Welt und erwarten, dass sich auch ihre Behörde in diese Welt einpasst. Das gilt auch für den Nachwuchs im Öffentlichen Sektor, der mit Internet, Laptop und Smartphone aufgewachsen ist. Die Mitarbeiter von heute erwarten einen modernen Arbeitsplatz. Laut der CGI Umfrage Global 1000 haben 42% der Leiter von Behörden die Herausforderung erkannt, Mitarbeiter mit neuem digitalen Know-how zu finden und zu binden. Wenn die Behörden den Kontakt zu den besten Köpfen nicht verlieren wollen, müssen sie die Arbeitsplätze und die damit verbundenen Prozesse an den Anforderungen der Digitalen Welt ausrichten.
An diesem Punkt zeigt sich, weshalb Digitalisierung und Modernisierung langfristige Projekte sind. Es geht darum, eine zukunftssichere Infrastruktur aufzusetzen, auf deren Grundlage eine digitalisierte Öffentliche Verwaltung auch in den nächsten zehn oder fünfzehn Jahren noch effiziente Arbeit leisten kann. Die IT bildet den zentralen Hebel, den “Driver”, für eine nachhaltige und agile IT-Umgebung.

**Ralf Oehlmann ist Sales Director Federal and Healthcare bei CGI in Köln; Mario Riesmeier ist Senior Consultant Workplace and Cloud bei CGI in Köln*

User Communication Services

André Prekop, Mitglied der Geschäftsleitung der BWI Informationstechnik GmbH für den Geschäftsbereich User Communication Services

André Prekop

Die Aufgaben

Der Delivery-Bereich User Communication Services (UCS) ist zuständig für geschäftsprozessübergreifende Anwendungen. Dazu zählen zum Beispiel Groupware Domain Services, File Service, Zentraler Verzeichnisdienst, Identity- und Access-Management, Telefonie, Zugangsdienste, Kollaboration, Dokumentenmanagement und spezifische Betriebsverfahren. Darüber hinaus verantwortet UCS die Endnutzer-Services und Communication Services. Hierunter fallen die Arbeitsplatzcomputer (APC) inklusive Client-Software und Asset- und Configuration-Management sowie Mobility-, Print- und Video-Dienste, Liegenschaftsnetze (LAN) und das Weitverkehrsnetz der Bundeswehr (WANBw). Ebenfalls in die Zuständigkeit dieses Delivery-Bereiches fällt der Vor-Ort-Service, der in mehr als 750 Bundeswehr-Liegenschaften in Deutschland geleistet wird. Wichtige Bestandteile von UCS sind zudem das IT-Projektmanagement zum Beispiel für große Rollout-Vorhaben, die Cloud Computing Services sowie das Lizenz- und Asset-Management. Auch die Leitung und Steuerung von zentralen Betrieben wie den Betriebskompetenzzentren fallen in den Aufgabenbereich von UCS.

Die Neuerungen

Veränderungen ergeben sich vorrangig BWI-intern, da die Delivery-Bereiche untereinander den Aufgabenzuschnitt etwas verändert haben. So hat zum Beispiel UCS die Verantwortung für die Groupware Services übernommen, jedoch den operativen Betrieb des Service Desks (User Help Desk sowie Auskunfts- und Vermittlungsdienst) und den Server-Basisbetrieb an CIS abgegeben.

Denkbar ist, dass Leistungen, die UCS bereits heute für die nichtmilitärische IT erbringt, auch für die einsatzrelevante IT erbracht werden können. Angedacht ist unter anderem die Ausdehnung der bei der BWI vorhandenen Services, zum Beispiel Endgeräte. Zudem ist auch das Erbringen von zentralen Managementleistungen beabsichtigt, beispielsweise ein zentrales Lizenzmanagement, das dazugehörige Asset- und Configuration-Management sowie das Carrier-Management.

Die vereinbarten Leistungen

Erst einmal soll die Leistungserbringung in einem Umfang fortgeführt werden, wie es bereits zu HERKULES-Zeiten der Fall war. Hier liegt der Fokus von UCS klar darauf, die hohe Qualität der Services, den sehr stabilen Betrieb und die hohe Nutzerzufriedenheit auch weiterhin zu gewährleisten. Darüber hinaus wird darüber diskutiert, welche Leistungen die BWI künftig im Bereich der einsatzrelevanten IT erbringen könnte. Eine mögliche neue Aufgabe könnte die Unterstützung der Bundeswehr mit speziell für Auslandsdienststellen und Dienststellen im Einsatz geeigneter und angepasster IT-Ausstattung sein, sofern dies von der Bundeswehr gewünscht wird.

Darüber hinaus ist zu erwarten, dass neue Services verstärkt im mobilen Umfeld entstehen werden, um die Attraktivität des Arbeitsplatzes bei der Bundeswehr zu erhöhen. Hier werden unter anderem Managed Mobile Devices wie Smartphones und Tablets er-

Neue Services werden vermehrt im mobilen Umfeld entstehen.

Foto: erhui1979 / DigitalVision Vectors, Fotolia.com

wartet oder auch Cloud-Technologien im Bereich der Kollaboration und der IT-Sicherheit.

Was die Bundeswehr erwarten kann

In erster Linie wird sich die Bundeswehr auch weiterhin auf einen stabilen und sicheren Betrieb sowie eine hohe Servicequalität verlassen können. Zudem wird sie eine auf ihre Bedürfnisse zugeschnittene Weiterentwicklung der vorhandenen Services und Leistungen von der BWI erwarten können sowie Innovationen, etwa in den Themenfeldern mobiles Arbeiten mit Smartphones und Tablets, Kollaboration und Cloud-Architekturen wie der VDI.

Die Herausforderungen

Herausforderungen werden sich im Bereich der Personalrekrutierung sowie der Integration ergeben und hinsichtlich der neu zu etablierenden Geschäftsmodelle für andere Ressorts.
Um ihre Rolle als IT-Systemhaus zu erfüllen, ist eine engere Zusammenarbeit mit der Bundeswehr unabdingbar. Nur wenn sich die BWI bereits früh in den Prozess der Lösungsentwicklung beratend einbringen kann, werden sich in der Folge optimal auf den Kunden zugeschnittene Leistungen und Services entwickeln lassen.
Damit die BWI auch weitere Kunden im Behördenumfeld bedienen kann, wird für sie eine Erstbefähigung zu einer Mandantenfähigkeit und einer möglichen Mandantentrennung ein notwendiger Schritt werden. Dies ist verbunden mit einer nicht unerheblichen Investition in den Umbau der BWI-eigenen Verfahren und Tools, also der vorhandenen Systemmanagement-Infrastruktur des IT-Dienstleisters.

Die Chancen

Die BWI hat umfassendes Know-how und langjährige Erfahrung in der Migration, Transformation und im Betrieb komplexer IT-Landschaften. Bereits heute verfügt sie über ein sehr breit aufgestelltes Serviceportfolio, verbunden mit einer hohen Prozessreife und einem hohen Grad der Standardisierung und Automatisierung. Dies ist eine gute Ausgangsbasis, um Services schnell und effizient auch anderen Kunden im Behördenumfeld zugänglich zu machen und sie zuverlässig und hochwertig zu betreuen. Hohen Kundenbedarf sieht UCS unter anderem in den Bereichen Mobilfunk-Services, flächendeckender Vor-Ort-Support und Weitverkehrsnetz-Leistungen. Mit der BWI als 100-prozentiger Bundesgesellschaft eröffnen sich für die Bundeswehr neue Möglichkeiten, IT-Dienstleistungen und Services, die heute in großen Teilen noch von eigenem Fachpersonal geleistet werden, künftig von ihrem zentralen IT-Dienstleister erbringen zu lassen. Hierdurch können Skaleneffekte genutzt werden, von denen beide Partner schlussendlich profitieren – und zudem wird zusätzlich das Bundeswehr-Personal von IT-Aufgaben entlastet und kann sich auf seine Kernaufgaben konzentrieren.

Cloud Infrastructure Services

Robert Knapp, Mitglied der Geschäftsleitung der BWI Informationstechnik GmbH für den Geschäftsbereich Cloud Infrastructure Services

Robert Knapp

Die Aufgaben

Der Service-Delivery-Bereich Cloud Infrastructure Services (CIS) ist für den Betrieb der Bundeswehr-Rechenzentren (RZ) verantwortlich. Neben diesen zentralen Systemkomponenten wird CIS künftig auch für den Server- sowie Storage-Betrieb zuständig sein, der heute noch an einigen wenigen Standorten in der Fläche verteilt ist. So bietet die BWI der Bundeswehr Managed-Server, Managed-Storage und Managed-Datenbank aus einer Hand und stellt die Basis für die Private Cloud der Bundeswehr (pCloudBw) bereit.

Die Neuerungen

Neben dem sogenannten Tier-1-Betrieb, also den Rechenzentren, übernimmt der Delivery-Bereich CIS auch die Betriebsleistung an den Tier-2-Standorten der BWI. Dies sind Serverlokationen, die beispielsweise die Fileserver für die Bundeswehr betreuen und die zumeist in größeren Bundeswehr-Liegenschaften in Deutschland untergebracht sind. Das war bislang bei der BWI bedingt durch den HERKULES-Vertrag anders organisiert. Neu aufgeteilt wird zudem der Applikationsbetrieb, der künftig von den Delivery-Bereichen BCA und UCS betreut wird. Die neue Organisation der Bereiche sieht vor, dass der Betrieb aller übergreifenden Betriebsverfahren und Tools von CIS geleistet wird. Dazu zählen beispielsweise zentrale Virenscanner und das Service-Request-Tool des Kunden. Zudem ist geplant, ein zentrales Change- und Test-Office aufzubauen. Auch dieses betreibt dann CIS.

Der Aufbau einer pCloudBw ist eines der Ziele, die die Bundeswehr in ihrer IT-Strategie formuliert hat. Hier wird die BWI eine der tragenden Säulen sein und hat dafür bereits wichtige Grundlagen geschaffen. Nun wird CIS die Lösung weiter konsequent vorantreiben, um eine hochautomatisierte, schnelle Bereitstellung von Ressourcen zu erreichen. In diesem Zusammenhang ist von einem erhöhten Bedarf an RZ-Kapazitäten auszugehen, der mittelfristig nicht mehr mit den bestehenden Anlagen gedeckt werden kann. Daher prüfen Bundeswehr und BWI aktuell, ob zwei zusätzliche Rechenzentren errichtet oder bestehende ausgebaut werden sollen.

Zudem fordert die Bundeswehr, die Hochverfügbarkeit der RZ noch weiter zu steigern. Hier geht es vor allem darum, die Wartungsfenster zu reduzieren, damit einsatzrelevante IT-Komponenten unterbrechungsfrei rund um die Uhr verfügbar sind. Eine Optimierung ist auch beim IT-Service-Management vorgesehen. Momentan arbeiten Bundeswehr und BWI noch mit zwei voneinander getrennten Systemen. Nun ist geplant, diese Plattformen zu harmonisieren oder zumindest ihre Interoperabilität herzustellen, um Störungen künftig genau lokalisieren und ein übergreifendes IT-Lagebild für die sogenannte “grüne” und “weiße” IT darstellen zu können.

Eine weitere Neuerung ist die Zentralisierung des Service Desks. Der UHD und der Auskunfts- und Vermittlungsdienst werden bei CIS zusammengeführt.

Die vereinbarten Leistungen

In den kommenden sieben Jahren wird die BWI die Bundeswehr-Rechenzentren weiter zuverlässig und sicher betreiben. In diesen Verantwortungsbereich fallen auch die Webauftritte der Bundeswehr, NuKomBw (Nutzerorientierte Kommunikation in der Bundeswehr), die sogenannte demilitarisierte Zone (DMZ), die Public Key Infrastructure der Bundeswehr (PKIBw), die Systeme in Nutzung der Bundeswehr (SinN), die Zugangsdienste für SASPF (Standard-Anwendungs-Software-Produkt-Familien) sowie die Druckerei in Strausberg. Im Einzelnen bedeutet dies: Der Delivery-Bereich CIS wird auch künftig die Infrastruktur für die Internet- und Intranetauftritte der Bundeswehr bereitstellen und diese betreiben. Diese werden zurzeit gemeinsam mit dem BMVg sowie BCA aktualisiert und es wird eine neue, moderne CMS-Technologie auf einer bereits etablierten Cloud-Infrastruktur eingeführt. Auch über die Modernisierung von NuKomBw, deren zentrale Komponenten in den BWI-Rechenzentren betrieben werden, diskutieren Bundeswehr und BWI bereits.

Ebenfalls zum Aufgabenbereich von CIS zählt der Betrieb der DMZ, die den sicheren Übergang vom WANBw zum Internet, aber auch zu Partnern und Auslandsdienststellen bildet. Vor Kurzem wurde hier die Kapazität erhöht, sodass nun an jedem der beiden Standorte Übertragungsraten von 9 Gigabit pro Sekunde zur Verfügung stehen. Die PKIBw versorgt den elektronischen Dienst- und Truppenausweis und bildet unter anderem

die Basis für bestimme Zugriffe, wie zum Beispiel auf den verschlüsselten File Service. Hierfür betreut und betreibt die BWI eine PKI-Umgebung für mehr als 120.000 Karten und ist zudem für den Betrieb der mehr als 200 Fachverfahren aus dem Bereich der zentralen SinN der Bundeswehr zuständig.
Der überwiegende Teil der SASPF-Nutzer in der Bundeswehr greift über eine Webschnittstelle auf die SAP-Lösung zu. Grundlage dieses Portals ist eine Virtualisierungstechnik für Applikationen. Auch diese Zugangsdienste für SASPF werden in den Rechenzentren betrieben. Hinzu kommt die Unterstützung von weiteren CPM-Projekten.

Was die Bundeswehr erwarten kann

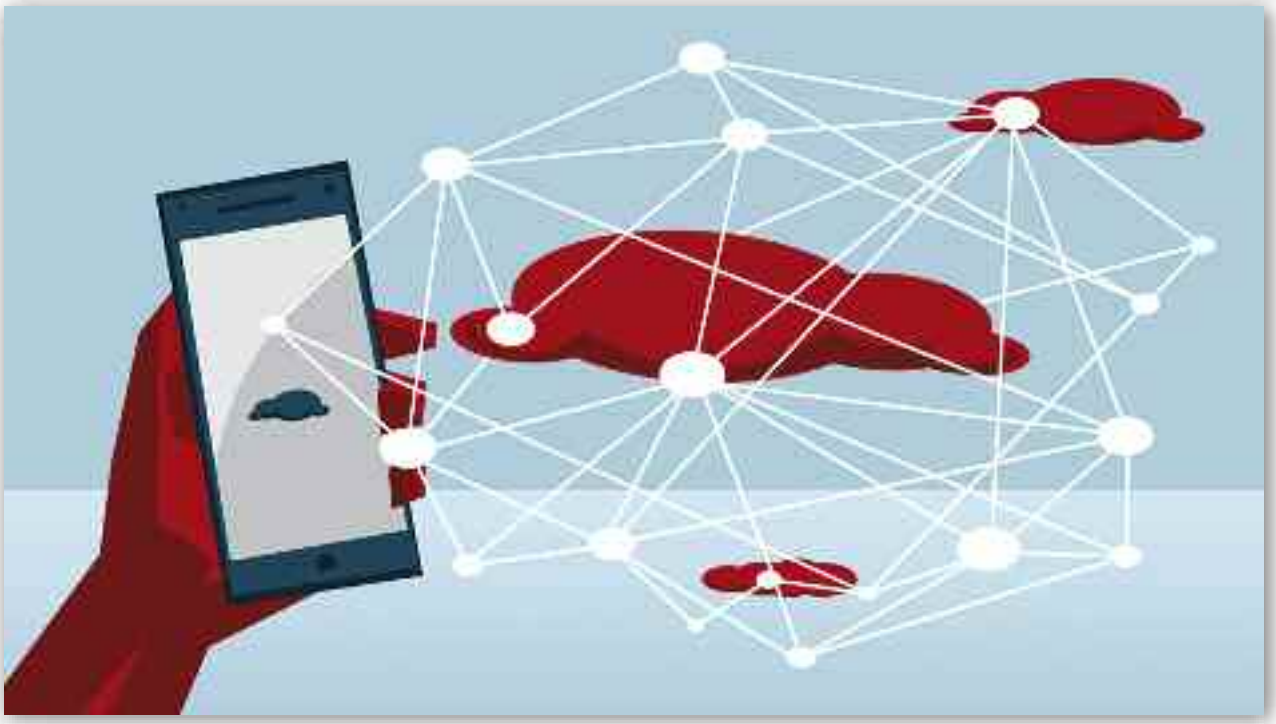
Eines der großen Ziele der BWI ist es, der Bundeswehr eine solide Basis für ihre Private Cloud zur Verfügung zu stellen und weiter auszubauen. Diese Infrastruktur wird hochautomatisiert und dynamisch skalierbar sein und mit den Anforderungen der Bundeswehr mitwachsen können. Das wird nicht nur die Geschwindigkeit und die Zuverlässigkeit der Services steigern, sondern auch zur verbesserten Einsatzunterstützung beitragen und die Kostentransparenz und -flexibilität erhöhen.

Die Herausforderungen

Mit der Bundeswehr-Cloud wird die BWI bereits 2017 einen großen Schritt vorankommen. Doch die dafür notwendige Infrastruktur benötigt RZ-Kapazitäten. Es erfordert nicht nur Zeit, diese aufzubauen, sondern auch die korrespondierenden Finanzmittel. Davon wird die Realisierung maßgeblich abhängen.

Die Chancen

Die Bundeswehr wächst, und das ist auch für die BWI die Möglichkeit mitzuwachsen. Dabei kann der IT-Dienstleister, falls von der Bundeswehr gewünscht, weitere Leistungen im Bereich der grünen IT übernehmen. Ein Beispiel hierfür wäre HaFIS (Harmonisierung der Führungsinformationssysteme); hierfür könnte die BWI bestimmte Anteile im Inland bis zu einer gewissen Systemebene übernehmen und die Bundeswehr dadurch entlasten.
Auch die IT-Konsolidierung des Bundes bietet zahlreiche Möglichkeiten, den Verantwortungsbereich der BWI auszuweiten. Für die Rolle als IT-Dienstleistungszentrum des Bundes ist die BWI aktuell schon gut aufgestellt. Es gibt einige Themen, beispielsweise bei der Optimierung von IT, Betrieb und Diensten, die die BWI zügig übernehmen könnte – die erforderlichen RZ-Kapazitäten immer vorausgesetzt. Ein Beispiel ist das RZ-Housing, also die Bereitstellung der RZ-Infrastruktur für Server Dritter. Diesen Betrieb von Serverkomponenten könnte die BWI auch gut anderen Ressorts anbieten. Auch Dienstleistungen wie die PKI ließen sich schnell anderen Organisationen der öffentlichen Hand zur Verfügung stellen.



Ziel der BWI: Bereitstellung einer soliden Basis für eine Private Cloud Bundeswehr. Foto: erhui1979 / DigitalVision Vectors, Fotolia.com

Business Consulting & Application

Christine Serrette, Mitglied der Geschäftsleitung der BWI Informationstechnik GmbH für den Geschäftsbereich Business Consulting & Application

Christine Serrette

Die Aufgaben

Der Service-Delivery-Bereich Business Consulting & Application (BCA) ist für das Management und die Entwicklung von Anwendungen zuständig. Hauptthema ist und bleibt SASPF (Standard-Anwendungs-Software-Produkt-Familien) sowie deren Komplementärprodukte, also bundeswehrspezifische Anwendungen, die teils von den Streitkräften selbst entwickelt wurden, ergänzt um alle Formen von Webanwendungen, wie das InternetBw und das IntranetBw, Social Media und Content-Management-Systeme.

Die zweite Säule dieses Delivery-Zweiges bildet die Beratung in den verschiedensten IT-Bereichen. Das hat die BWI teilweise schon in der Vergangenheit gemacht, unter anderem zu allen Fragestellungen rund um SAP. Auch Aspekte der IT-Sicherheit deckt der IT-Dienstleister bereits ab, zum Beispiel bezogen auf die Public Key Infrastructure der Bundeswehr (PKIBw), die Handhabe von Rollen und Berechtigungen in verschiedenen Anwendungen und das Wissensmanagement.

Die Neuerungen

Ein wesentlicher Unterschied zur HERKULES-Zeit besteht in der neuen Organisation von SASPF. Neu ist, dass nun der gesamte Betrieb der SAP-Landschaft in die Zuständigkeit von BCA fällt. Hier bündelt die BWI die notwendigen Kompetenzen, sodass SASPF künftig aus einer Hand kommt. Neben dieser organisatorischen Neuerung ist zudem geplant, dass die BWI mehr Leistungen im Bereich SASPF erbringt als bisher. Insbesondere soll in den IT-Infrastructure-Library-Prozessen (ITIL) mehr Verantwortung übernommen werden, um die Bundeswehr hier zu entlasten.

Die BCA soll zu einer echten IT-Beratung ausgebaut werden. In der HERKULES-Zeit war es häufig so, dass die BWI relativ spät in die Überlegungen, zum Beispiel zu neuen Tools zur Unterstützung von Geschäftsprozessen, einbezogen wurde. Da waren die Entscheidungen bei der Bundeswehr meist schon gefallen. Der Gestaltungsspielraum war dementsprechend begrenzt. Eines der großen Ziele ist es, in Zukunft bereits bei der Gestaltung neuer Prozesse und somit auch bei der Auswahl entsprechender Tools zu beraten. Das heißt, die BWI wird früher an der Diskussion beteiligt sein und kann Empfehlungen für die Entscheidungsfindung einbringen. Das Kopfzerbrechen darüber, mit welchem Tool ein Problem optimal gelöst werden kann, wird der Bundeswehr so abgenommen werden. Um diesen Ansatz der ganzheitlichen Beratung mit Leben zu füllen, stellt sich die BWI auch intern neu auf und bündelt ihr Know-how, um effizienter und ganzheitlicher arbeiten zu können. Eine Voraussetzung hierfür: die Bündelung von Kompetenzen an einer zentralen Stelle. So schafft sich die BWI ein umfassendes Bild von den Kundenbedürfnissen und kann diese koordiniert bedienen.

Die vereinbarten Leistungen

Von der Beratung und der Entwicklung über den Rollout und Betrieb bis hin zu Support und Nutzerausbildung übernimmt BCA das gesamte Leistungsspektrum für SASPF und die Online-Medien. Es gibt zahlreiche Projekte, die weiterlaufen, neu starten oder in Planung sind. Dazu zählen, um nur ein paar Beispiele zu nennen: das autarke SASPF-System für die Fregatte 125, SASPF on mobile, SAP HANA, ITU-Zentrallogistik und der Relaunch der Internetpräsenz des BMVg sowie der Bundeswehr. Und nach wie vor sind die Altsysteme ein Thema. Aktuell gibt es immer noch um die 70 SinN, von denen nur knappe 40 als Komplementärprodukt übrig bleiben sollen. Das heißt, die BWI wird auch weiterhin mit der Migration oder Ablösung beschäftigt sein. Hinzu kommen zahlreiche CMP-Projekte, bei der BCA die Bundeswehr unterstützen wird.

Was die Bundeswehr erwarten kann

In den kommenden sieben Jahren kann die Bundeswehr sehr viel Unterstützung bei der Modernisierung ihrer IuK, in der Beratung und in der Übernahme von Aufgaben erwarten. Die BWI wird der Bundeswehr ein verlässlicher und mitdenkender Partner sein, der ihr einen echten Mehrwert bietet. Ein Ziel dabei ist es, genau hinzuschauen und aktiv mitzudenken, um neue Wege aufzeigen zu können. Die BWI wird der zuverläs-

Aufgabenfeld der BCA: Von der IT-Beratung bis zum Management und der Entwicklung von Anwendungen. *Foto: erhui1979 / DigitalVision Vectors, Fotolia.com*

sige Dienstleister sein, dem die Bundeswehr getrost Aufgaben übertragen kann, die dann vom Unternehmen komplett umgesetzt werden – und das nicht nur stabil, sondern vor allem auch sicher. Auf diese Weise kann sich die Bundeswehr voll auf ihre eigene neue Organisation und auf ihre Kernaufgaben konzentrieren.

Die Herausforderungen

Naturgemäß sind nie alle von einer Lösung restlos überzeugt. Daher wird die BWI gefordert sein, auch Kritiker der HERKULES-Folgelösung von der BWI und ihrer Leistungsfähigkeit zu überzeugen. Um künftigen Anforderungen gerecht zu werden, braucht die BWI vor allem eines: gutes Personal. Es wird eine sehr schlagkräftige Mannschaft benötigt werden, um alle Herausforderungen meistern zu können. Wichtig wird es daher sein, qualifizierte und engagierte Mitarbeiter zu finden, diese für die BWI zu begeistern und den Bedürfnissen der Kunden entsprechend auszubilden. Hier konkurriert die BWI mit den Großen der Industrie um die klügsten Köpfe.

Die Chancen

Als IT-Systemhaus kann die BWI ihre Rolle als verlässlicher Partner künftig besser erfüllen, da sie früher in Gespräche miteingebunden werden kann, als das verständlicherweise in der Vergangenheit der Fall war, als sie noch ein externes Unternehmen war. Die BWI kann also mehr Verantwortung übernehmen und Aufgaben selbstständig und eigenverantwortlich realisieren. Für die Bundeswehr ist das eine Entlastung, da sie Leistungen bekommt, ohne dafür eigenes Personal bereitzustellen.

Die Weiterentwicklung der Services verspricht der Bundeswehr viele Vorteile. Es wird ein ganzheitlicher Ansatz verfolgt, der alle Aspekte abdeckt, also von der Beratung bis hin zur Umsetzung und zum Betrieb. Das ist von großem Kundennutzen. Die BWI ist künftig der zentrale IT-Dienstleister der Bundeswehr und hat bereits heute den Überblick über die nichtmilitärische IT. Dieses umfassende Wissen wird der Bundeswehr jetzt noch besser zugänglich und nutzbar gemacht werden. Wer, wenn nicht die BWI, sollte hier ganzheitlicher beraten können?

Gute Perspektiven für Soldaten bei der BWI

Im Porträt: Dr. Christian Marwitz, Mitglied der Geschäftsleitung der BWI Informationstechnik GmbH und ehemaliger Zeitsoldat

Die Bundeswehr und die BWI – das ist von Beginn an eine besondere Verbindung, die über das klassische Verhältnis von Kunde und Dienstleister hinausreicht. Dafür sorgt allein schon das Personalmodell. In dem eigens für die Umsetzung des Projekts HERKULES gegründeten BWI Leistungsverbund finden sich binnen drei Monaten nach Vertragsunterzeichnung circa 2.800 Mitarbeiter ein. 2.400 kommen von der Bundeswehr, die anderen aus der Industrie, vorrangig von Siemens und IBM Deutschland. Im Laufe der Zeit nutzen viele Bundeswehr-Angehörige die Möglichkeit, den Arbeitsvertrag zu wechseln, und finden so dauerhaft ihre berufliche Heimat bei der BWI.

Christian Marwitz: Vor zehn Jahren bei der BWI eingestiegen und schnell Karriere gemacht. Foto: BWI

Auch Soldaten verstärken das BWI-Team. Sie engagieren sich zum Beispiel im Rahmen des Kooperationsmodells oder des Steuerungs- und Kontrollelements (SKE). Auch beurlaubte oder pensionierte Soldaten und ehemalige Zeitsoldaten arbeiten bei der BWI. Einer von ihnen ist Dr. Christian Marwitz. Hätte man ihm allerdings vor zehn Jahren prophezeit, dass er einmal in einem IT-Unternehmen arbeiten würde, hätte er vermutlich ungläubig den Kopf geschüttelt. Heute kann sich der frühere Soldat keinen Arbeitsplatz vorstellen, an dem er lieber wäre.

Beurlaubung als Einstieg in die BWI

Doch der Reihe nach: 1996 verpflichtet sich Christian Marwitz für zwölf Jahre als Soldat auf Zeit bei der Bundeswehr. Drei Jahre später beginnt der Offiziersanwärter ein Studium der Wirtschafts- und Organisationswissenschaften an der Universität der Bundeswehr in München. Als Diplom-Kaufmann verlässt er die Uni 2002. So zumindest der Plan. Doch eine Bundeswehr-Reform hat die Truppenstärke zwischenzeitlich deutlich verringert. Seine vorgesehene Verwendung gibt es schlichtweg nicht mehr. Daher bleibt der Schwabe als wissenschaftlicher Mitarbeiter am Institut für Allgemeine Betriebswirtschaftslehre und promoviert.

Mittlerweile schreiben wir Januar 2007 und das Projekt HERKULES ist gerade einmal ein paar Tage alt. Nun gibt die BWI eine Studie bei der Bundeswehr-Universität in Auftrag. Das junge Unternehmen will wissen, wie es die Dienststellen am besten über die bevorstehenden HERKULES-Services informieren kann. Christian Marwitz beteiligt sich an der Untersuchung und stellt die Ergebnisse wenig später den Verantwortlichen in der BWI vor. Die Präsentation überzeugt und er erhält das Angebot, selbst das Projekt “Rolloutkommunikation” bei der BWI aufzubauen. Gesagt, getan. Im Sommer 2007 beginnt die einjährige Beurlaubung des Soldaten. Was folgt, ist eine sehr spannende, abwechslungsreiche und auch äußerst arbeitsreiche Zeit. “Schließlich wurde mit der BWI ein Unternehmen aus dem Nichts aufgebaut. Hier mitgestalten zu können, war ein besonderer Reiz für mich, und ich war der festen Überzeugung, dass Engagement honoriert wird. Und so war es ja dann auch”, erinnert sich Christian Marwitz.

Offenes und vertrauensvolles Miteinander

Dass er sich – obwohl Wirtschaftswissenschaftler und kein IT-Experte – schnell in seinem neuen Arbeitsumfeld einfindet, liegt seiner Meinung nach vor allem am BWI-Team. “Die Zusammenarbeit mit meinen Kollegen bei der BWI habe ich von Anfang an als fruchtbares Geben und Nehmen empfunden. Von meinen IT-Kollegen lernte ich in den vergangenen Jahren sehr viel technisches Know-how. Ich wiederum konnte mein Wissen über die Bundeswehr beisteuern – das ist hilfreich im Umgang mit dem Kunden. Wir ergänzen uns also bestens.” An seinem ersten Berufsleben als Soldat hat er insbesondere die Kameradschaft geschätzt. Auch in der zweiten Karriere fühlt er sich gut aufgehoben, denn “bei der BWI pflegen wir ein herzliches, vertrauensvolles und offenes Miteinander”.

Als 2008 die Beurlaubung endet, folgt das Angebot, fest bei der BWI einzusteigen. Die Offerte kommt für Christian Marwitz genau zur rechten Zeit, sprich pünktlich zum Ende seines zwölfjährigen Dienstes als Zeitsoldat. Die Entscheidung für den Wechsel fällt ihm mehr als leicht. “Mir war

Gute Perspektiven in der BWI für ehemalige Zeitsoldaten. *Foto: erhui1979 / DigitalVision Vectors, Fotolia.com*

klar, dass ich nicht als Berufssoldat weitermachen wollte. Die BWI bot mir jedoch die Möglichkeit, mit der Bundeswehr Kontakt zu halten. Ich musste also keinen harten Schnitt zu meiner Vergangenheit machen, sondern habe immer noch einen Bezug zu dieser."

Karrierepfad geht schnell steil bergauf

Nach dem Einstieg bei der BWI geht es Schlag auf Schlag für den Major der Reserve. Zunächst übernimmt er die Leitung einer Fachabteilung, die unter anderem für das Servicemanagement zuständig ist. 2010 bekommt er die Projektleitung für die Einführung des Bestellportals IT-SPS in die Bundeswehr übertragen, im April 2011 steigt er zum Leiter eines Betriebskompetenzzentrums (BKZ) auf. Dort befasst er sich zunächst mit den sogenannten Backoffice Services, zu denen unter anderem der File Service, der Virenschutz, die Drucker sowie die zentralen und dezentralen Server zählen. Im Sommer 2012 übernimmt er die BKZ-Leitung auch für die Client und Application Services, womit auch die Arbeitsplatzcomputer, Softwareprodukte und Peripheriegeräte in seinen Zuständigkeitsbereich fallen. Mitte 2016 folgt der nächste Karriereschritt: Christian Marwitz wird Segmentleiter Service Delivery Management. 2017 schließlich kommt der Ruf in die Geschäftsleitung der BWI Informationstechnik GmbH, wo er den Bereich Innovation, Solution & Delivery Management (ISDM) verantwortet. Vieles ist passiert seit seinem ersten Tag bei der BWI vor zehn Jahren. Geblieben sind stets die Freude an seiner Tätigkeit und die Begeisterung für das Projekt. "Ich bin davon überzeugt, dass ich mit meiner Arbeit einen kleinen Beitrag zu etwas Größerem leisten kann. Für mich ist das mehr als "nur" IT." Blickt der 40-Jährige heute auf seine berufliche Laufbahn zurück, stellt er zufrieden fest: "Ich würde es immer wieder so machen. Bislang habe ich keinen Tag bedauert – weder bei der Bundeswehr noch bei der BWI." Auch der Zukunft schaut er voller Optimismus entgegen. "Ich bin sehr guter Dinge. Auf die BWI warten viele spannende Aufgaben als IT-Systemhaus der Bundeswehr. Aber auch die IT-Konsolidierung des Bundes verspricht viel Neues. Auf uns warten große Herausforderungen, aber daran werden wir erfolgreich wachsen, und es wird der BWI guttun, ein breiteres und tieferes Themenspektrum zu bearbeiten", sagt Christian Marwitz und betont: "Die BWI kann das. Davon bin ich fest überzeugt. Und das macht die BWI auch als Arbeitgeber weiterhin sehr interessant."

Der Einstieg bei der BWI

Neue berufliche Perspektiven: Im Anschluss an die Dienstzeit können ausscheidende Berufs- und Zeitsoldaten direkt bei der BWI einsteigen oder eine Maßnahme zur beruflichen Orientierung beziehungsweise Berufsförderung absolvieren. Die BWI arbeitet mit dem Berufsförderungsdienst (BFD) der Bundeswehr zusammen und bietet Soldaten zudem die Möglichkeit, im Rahmen einer Zivilberuflichen Aus- und Weiterbildung (ZAW-Maßnahme) ein Praktikum zu absolvieren.

>> **Weitere Informationen unter www.bwi-karriere.de**

Kreative und wirtschaftliche Konzepte für die Raumfahrt

Seit 35 Jahren überzeugt die OHB System AG am Markt. Die Expertise erstreckt sich über alle relevanten Raumfahrtbereiche mit klarem Fokus auf konkreten Kundennutzen. Im Mittelpunkt steht die Entwicklung und Bereitstellung von Satellitensystemen.

Mit der Bundeswehr verbindet OHB eine erfolgreiche Partnerschaft: SAR-Lupe, das radargestützte Aufklärungssystem der Bundeswehr, liefert bereits im elften Jahr zuverlässig Daten. Auch das Nachfolgesystem SARah inklusive aller Bodenanlagen wird von OHB bereitgestellt werden. Für die militärische Satellitenkommunikation im UHF-Bereich (P-Band) entwickelt das Unternehmen ein Managementsystem (UHF-Dama).

Der erste SmallGEO Telekommunikationssatellit, H36W-1, während der Testkampagne.

Foto: OHB System AG

Das Marktsegment Telekommunikation wird mit einer Neuentwicklung und bereits vier Missionen in der Realisierung bedient: Die modulare und an Kundenbedürfnisse anpassbare SmallGEO-Produktlinie ist für den geostationären Einsatz konzipiert. Der erste SmallGEO-Satellit H36W-1 wurde erfolgreich gestartet, der zweite Satellit EDRS-C wird momentan integriert. Die geplante Mission Heinrich Hertz wird neben technologischen Experimenten auch eine militärische Nutzlast mitführen. Die vollelektrische SmallGEO-Konfiguration ELECTRA, die OHB gemeinsam mit dem Satellitenbetreiber SES entwickelt, wird eine neue Dimension bei Effizienz und Kundennutzen eröffnen.

In der Erdbeobachtung verantwortet OHB unter anderem die nationale Mission EnMAP mit ihrem Hyperspektralinstrument, und ist maßgeblich an der Weiterentwicklung der europäischen Wettersatelliten beteiligt. OHB ist außerdem Hauptauftragnehmer für 22 Galileo FOC-Satelliten, von denen 14 bereits gestartet wurden.

Traditionellen IT-Sicherheitssystemen fehlt die Schwarmintelligenz

SOPHOS
Security made simple.

Jahrelang galt in puncto IT-Sicherheit die Maxime "Netzwerk ein Anbieter und Endpoint ein Anbieter – das sorgt für optimalen Schutz". Doch dieses Mantra gilt heutzutage nicht mehr. Der Grund dafür ist die ständige Weiterentwickelung von Technologien. Das gilt sowohl für Hersteller von IT-Security-Lösungen als auch für die Hackerszene. Tradition ist gut und notwendig. Das gilt auch für IT-Sicherheitslösungen. Ohne die Erfahrungen der letzten Jahrzehnte wären Infrastrukturen bei weitem nicht so gut geschützt, wie sie es heute sind. Allerdings ist das alleinige Vertrauen auf Tradition eine Sackgasse. Es müssen neue Wege gefunden werden, modernen Hackerangriffen einen Riegel vorzuschieben und sich für die Herausforderungen durch immer weiter auflösende Peripherien sowohl in der Geschäfts- als auch Alltagswelt zu wappnen. Es ist heutzutage einfach nicht mehr ausreichend, zwei Produkte mit einer guten Erkennungsrate zu verbinden, um für ausreichend Schutz zu sorgen. Die Netzwerkgrenzen werden immer durchlässiger und die Verantwortlichen für IT-Sicherheit müssen neue Werkzeuge an die Hand bekommen, um auf die zunehmende Mobilität der Arbeitswelt reagieren zu können.

Die immer häufigeren Schlagzeilen über gehackte Konzerne machen deutlich: Wir stehen an einem Scheideweg in Sachen IT-Sicherheit. Egal ob Sony oder Bundestag, selbst Systeme, bei denen man getrost davon ausgehen darf, dass State-of-the-Art-Lösungen im Einsatz sind, lassen zu viele Lücken zu. Erkennungsraten top, die Firewall perfekt eingerichtet, Technologien wie Advanced Threat Protection installiert – und dennoch Einbrüche über den Onlinekanal? "Wie kann das sein?", werden sich viele fragen. Die Antwort ist recht einfach. Während bislang mit den traditionellen Herangehensweisen Hacker meist ausreichend in die Schranken gewiesen werden konnten, hat sich auch der Cyberkriminalismus weiterentwickelt, ist sehr viel versatiler geworden. Und eben diese Flexibilität macht den traditionellen Sicherheitssystemen zu schaffen, da Ihnen die Schwarmintelligenz fehlt. Sämtliche Funktionen für sich gesehen funktionieren einwandfrei, aber entscheidend ist heute, dass alle diese Systeme intelligent miteinander verknüpft sind, miteinander kommunizieren. Nur so lassen sich die Lücken zwischen den Lösungen schließen und die immer ausgeklügelteren Attacken erfolgreich abblocken. Denn was nutzen die besten Erkennungsraten des Antivirus-Systems, wenn der Schädling über andere Wege ins System eindringt und unerkannt sein Werk vollbringen kann?

Miteinander vernetzte Intelligenz kann Großes bewältigen. Das gilt auch für IT-Sicherheit. Foto: Richard Carey, Fotolia.com

Ein gutes Beispiel für ein Next-Generation-Feature auf Endpoint-Ebene ist Malicious Traffic Detection. Diese Funktion enttarnt kompromittierte Computer während diese mit den "Command-and-Control"-Servern der Angreifer kommunizieren. Eine ähnliche Technologie in Next Generation Firewalls kann Administratoren über die Präsenz eines kompromittierten Systems im Netzwerk informieren. Indem das Feature in den Endpoint integriert wird, können Kompromittierungen nicht nur innerhalb, sondern auch außerhalb des Netzwerks erkannt, die spezifische Schaddatei identifiziert und die Infektion beseitigt werden. Anwender profitieren so von besseren Erkennungsraten und verbringen weniger Zeit mit Nachforschungen und manuellen Bereinigungen kompromittierter Systeme.

Was in Sachen Unternehmensschutz außerdem nicht unter den Tisch gekehrt werden darf, ist das Thema Verschlüsselung, das aufgrund seines schlechten Rufs in Bezug auf die Produktivität des Mitarbeiters und der Systeme in der Vergangenheit oftmals gemieden wurde. Doch auch hier gilt es mit Vorurteilen aufzuräumen. Moderne Verschlüsselungslösungen beeinträchtigen aktuelle Arbeitssysteme kaum noch und sind ebenfalls für die Nutzung in einer mobilen Welt ausgelegt. Und letztendlich ist die Verschlüsselung der Daten der perfekte Schutz, um Hackern den Wind aus den Segeln zu nehmen, selbst wenn Sie es bis ins System geschafft haben sollten. Ungewollter Datenabfluss ist nie ganz einzudämmen, dafür sorgt alleine der Faktor "Mensch". Deshalb drehen Next-Gen-Lösungen den Verschlüsselungsspieß in der Zukunft um. Es wird nicht mehr festgelegt, was verschlüsselt wird, sondern was nicht. Diese automatische Codierung aller Daten sorgt für ein enormes Sicherheitsplus und ist technologisch heutzutage gut umsetzbar.

www.sophos.de

Digitale Schockwellen

Jörn Becker, Leiter Civil & National Security – Business & Platform Solutions, Atos Deutschland
Hubert Geml, Leiter Verteidigung, Innere Sicherheit, Atos Deutschland

Jörn Becker

Hubert Geml

Die aktuelle Bedrohungslage bei zunehmender Digitalisierung stellt die Bundeswehr vor neue Herausforderungen. Die Beherrschung des Cyber- und Informationsraums bleibt kritischer Erfolgsfaktor – hier muss das IT-System der Bundeswehr Schritt halten. Die Auswirkungen der "digitalen Schockwellen" werden die Auftragserfüllung der Bundeswehr jedoch erheblich beeinflussen.
Bislang entwickelten sich die Aufbau- und Ablauforganisationen der Bundeswehr und ihre IT-Landschaft noch streng formal und hierarchisch. Die meisten Systemarchitekturen sind etwa noch isoliert ausgebracht und geprägt von Altanwendungen für dedizierte Benutzergruppen. Eine weitgehende Serviceintegration und -orientierung, wie sie in der Industrie im digitalen Zeitalter bereits üblich ist, fehlt noch. Dies führt zu erheblichen Zeitverlusten und Lücken in der Informationsversorgung. Das Ziel ist aber, dass Services grundsätzlich endgeräte- und ortsunabhängig in möglichst kurzer Zeit allen berechtigten Akteuren und Systemen im nationalen sowie im Bündnis-Kontext zur Verfügung stehen.

Streitkräfte sind "digitalen Schockwellen" ausgesetzt

Im Zeitalter der Digitalisierung wirken mehrere "digitale Schockwellen" aufeinander, die erhebliche und teilweise unerwartete Auswirkungen auf Industrie und Alltag eines jeden haben. Den Ursprung der Schockwellen erkennt Atos in vier Bereichen, die im Folgenden skizziert werden:

Disruptive Technologies
50 Milliarden Objekte werden schätzungsweise in naher Zukunft miteinander vernetzt sein und die zunehmende Entwicklung des Internets der Dinge wird erhebliche Veränderungen herbeiführen. Das Cloud Kontinuum verschiebt sich von zentralisierten Rechenzentren hin zu vielen dislozierten Endgeräten mit enormer Rechenpower. Die Selbstorganisation und -konfiguration der IT-Systeme wird zunehmen. Auch industrielle Fertigungsprozesse verändern sich und können bspw. durch Additive Manufacturing (beispielsweise 3D-Druck) nutzerorientiert angepasst und dezentralisiert werden. Virtuelle Roboter mit künstlicher Intelligenz werden manuelle Arbeit zunehmend substituieren.

Ways of Working
Der Arbeitsplatz der Zukunft ist virtuell, kollaborativ vernetzt und flexibel. Ermöglicht wird dies zum Beispiel durch den Einsatz von tragbaren Endgeräten wie Smart Glasses in Verbindung mit "Augmented Interactive Reality". Fehlende individuelle Fähigkeiten werden somit ortsunabhängig durch die Einspielung von zusätzlichen kontextbasierten Echtzeitinformationen in die Endgeräte eingeblendet. So können etwa Wartungsarbeiten trotz fehlender Qualifikationen verrichtet werden.

Business Models
Konventionelle interne und externe Unternehmensgrenzen werden zukünftig eine geringere Rolle spielen und neue Entwicklungen weniger einschränken. In naher Zukunft wird jeder Prozess, jedes Produkt und jeder Service digitalisiert und vernetzt sein. "Common Industrial Data Platforms" und "Innovation Value Labs" ermöglichen den schnellen Aufbau von Geschäftsbeziehungen sowie den sicheren Datenaustausch mit den relevanten Stakeholdern. Für Organisationen bedeutet das unter anderem, dass Routine-Arbeit automatisiert und von Robotern erledigt werden kann. Die Arbeitsmodelle der Zukunft konzentrieren sich auf typisch menschliche Fähigkeiten, wie etwa Kreativität.

Evolving Challenges

Neue Technologien bringen neue Herausforderungen mit sich. Schneller Datenaustausch erfordert neue Werkzeuge für die Analyse und Verarbeitung. Aber auch Aspekte wie Ethik, Sicherheit, Schutz von Identität und Privatsphäre müssen adressiert werden, da ihre Bedeutung im Zuge der Digitalisierung signifikant zunimmt.

Die 4 Quellen digitaler Schockwellen *Quelle: Atos, Ascent Journey 2020*

Die vier skizzierten Bereiche digitaler Schockwellen verändern sich permanent. Neue Impulse führen meist zu Interaktionen mit anderen Quellen und unvorhersehbaren komplexen Veränderungen. Auch die Streitkräfte müssen sich für diese Situation wappnen, damit sie ihrem Auftrag zukünftig gerecht werden.

Mit Cloud Services ins digitale Zeitalter

Mit dem Programm “HaFIS” (Harmonisierung und Migration der Führungs-informationssysteme) begann für die Streitkräfte unter Begleitung von Atos und weiteren Partnern der Industrie der Weg ins digitale Zeitalter. Die Führungsfähigkeit der Bundeswehr wird seitdem mittels moderner Informationstechnologien erheblich verbessert. Die Cloud-Service-Integration geht unter strengen Vorgaben der IT-Sicherheit schrittweise voran. Ein zentrales Element wird ein militärischer “Enterprise App Store” für Grundbetrieb und Einsatz sein, der modernen digitalen Industriestandards entspricht.

Die wachsende Bedrohungslage im Cyberraum fordert die bestehenden Systeme jedoch heraus. Die Angreifer sind schwer identifizierbar, eine Attacke ist relativ einfach umzusetzen und kann Staat und Wirtschaft erheblichen Schaden zufügen. Im Gegenzug beeinträchtigt aber hoher technischer Schutz die Nutzbarkeit der Systeme. Daher wird für zukünftige Einsätze der Bundeswehr ein Trade-off zwischen technischem Schutz und operativer Nutzbarkeit im Rahmen einer Missionsdomäne erwogen. Atos unterstützt die Streitkräfte, eine Funktionale IT-Sicherheitsarchitektur (FITSA) für Einsätze der Bundeswehr zu entwickeln. Hierbei gilt es auf Basis einer risikobasierten Betrachtung, Gefährdungsprofile für Missionen festzulegen und den Schutzbedarf sowie adäquate IT-Sicherheitsmaßnahmen abzuleiten.

Einsatz-IT digital betrachtet

Während eines Einsatzes der Bundeswehr gibt es nur selten vor Ort ausreichend Spezialisten, die mit allen Aspekten des IT-Betriebs vertraut sind. Dokumente wie Betriebshandbücher sind bei einer Störung nicht sofort zur Hand, Expertenwissen ist isoliert und steht nicht allen gleichermaßen zur Verfügung. Im Bereich Betriebsunterstützung für Einsatz-IT haben sich die von Atos entwickelten “Digital Field Services” bewährt.

Atos hat im Industrieeinsatz erprobte, für Satellitenkommunikation ausgelegte Remote Support Services entwickelt. Damit werden Mitarbeiter im Ausland in Echtzeit durch Expertenteams in der Heimat unterstützt, wenn Services oder Systeme vor Ort ausfallen oder gewartet werden müssen. Die für die Industrie entwickelten “Real Time Collaboration Solutions” und “Observation Services” ermöglichen bandbreitenoptimierte, latenzarme Audio- und Videokommunikation. Genutzt werden dafür Tablets, Headsets und Bodycams. Head Mounted Displays werden zukünftig die bereits genutzten mobilen Endgeräte wie Tablets und Smartphones entscheidend ergänzen. Sie transportieren “Augmented and Mixed Reality” direkt in das Sichtfeld des Nutzers.

Damit ist eine digitale Brücke zwischen der physikalischen und digitalen Welt geschlagen, die zudem Benutzerfreundlichkeit und Einfachheit steigert. Eine Integration dieser Lösung in das IT-System der Bundeswehr liegt nahe. Im Idealfall kann die Instandsetzung oder Wartung eines Geräts vor Ort von Personal ohne Spezialkenntnisse durchgeführt werden. Auch logistische Anforderungen und Verfahren in Produktionsprozessen werden sich sukzessive ändern. Sollten Ersatzteile vor Ort fehlen, kann man sich aus den Möglichkeiten des Additive Manufacturing bedienen: Mittels professionellen Life Cycle Managements und geeigneter 3D-Drucker wird die Produktion an den Einsatzort verlagert. Dringend erforderliche Ersatzteile können somit ad hoc repliziert und eingesetzt werden. “Remote Diagnostic”- und “Predictive

Maintenance”-Verfahren runden das Bild ab: Wartungsintervalle müssen nicht mehr turnusmäßig durchgeführt werden, einzelne Systemkomponenten geben auf Basis von hoch entwickelten mathematischen Algorithmen von sich aus Austauschzeiten vor und informieren frühzeitig das Betriebspersonal. Fazit: Das digitale Zeitalter ermöglicht die Reduktion von Betriebspersonal im Einsatzland und eine Steigerung der Effektivität.

Neue Herausforderungen annehmen und antizipieren

Das digitale Zeitalter ist bestimmt von der Fähigkeit, Informationen zielgerichtet auszuwerten und einzusetzen sowie von innovativen Technologien, die umfassende Rechenoperationen extrem schnell durchführen. Die Entwicklungen in der Unternehmenswelt und neuer Technologien sollten für militärische Zwecke geprüft, wo möglich antizipiert und schnell umgesetzt werden. Atos setzt sich mit vollem Engagement dafür ein, die Bundeswehr bei der Entwicklung der IT-Systeme und -Services optimal zu unterstützen sowie bei der Digitalisierung zu beraten, damit diese ihren Auftrag bestmöglich erfüllen kann und für die Zukunft gewappnet ist.

1) Ausführliche Informationen finden Sie in der Atos Trend-Analyse: Ascent Journey 2020 – Digital Shockwaves in Business, https://ascent.atos.net/journey-2020/

AFCEA Bonn e.V.

Anwenderforum für Fernmeldetechnik, Computer, Elektronik und Automatisierung

31. AFCEA-Fachausstellung

Informations- und Kommunikationstechnik

Innere und Äußere Sicherheit 4.0 – Schlüssel zur digitalen Souveränität

26./27. April 2017 • Maritim Hotel Bonn

	26. April 2017
09:00 – 18:00 Uhr	**Ausstellung · Vorträge im Saal REGER** *Moderation:* Oberst i.G. Armin Fleischmann, AFCEA Bonn e.V.
10:00 Uhr	**Begrüßung/Eröffnung der 31. AFCEA-Fachausstellung** Oberst a.D. Friedrich W. Benz, Vorstand AFCEA Bonn e.V. und Leiter AFCEA-Fachausstellung
10:15 Uhr	**Grußwort "IT-Standort Bonn"** Reinhard Limbach, Bürgermeister der Bundesstadt Bonn
10:30 Uhr	**"Cyber-Sicherheit und -Verteidigung als Schlüssel für Informations-, Führungs- und Wirkungsüberlegenheit bei Landoperationen"** Generalleutnant Jörg Vollmer, Inspekteur des Heeres, Kommando Heer, Bundeswehr
14:00 Uhr	**"Cyber-Cluster@UniBwM: ein Ökosystem für Forschung, Entwicklung und Innovation"** Prof. Dr. Gabi Dreo-Rodosek, Lehrstuhl Kommunikationssysteme und Internet-Dienste an der Universität der Bundeswehr, München
18:00 – 21:00 Uhr	**Get-together AFCEA Fachausstellung** *AFCEA Bonn e.V. lädt Besucher und Aussteller* der AFCEA Fachausstellung 2017 ein zu *Kölsch mit Snacks im Ausstellungsbereich Fachausstellung, Foyer I/II*
	27. April 2017
09:00 – 17:00 Uhr	**Ausstellung · Vorträge im Saal REGER** *Moderation:* Generalmajor Dr. Angar Rieks, Stv. Vorsitzender AFCEA Bonn e.V.
10:00 Uhr	**"Der neue Organisationsbereich Cyber- und Informationsraum - ein Eckpfeiler der gesamtstaatlichen Sicherheitsarchitektur"** Generalleutnant Ludwig Leinhos, Inspekteur Cyber/Informationsraum, Kommando CIR, Bundeswehr
14:00 Uhr	**Vortragsthema tbd** Mr. Yair Reuven Attar, Head of "IR and Hunting Section" Israel Ministery of Defense
Abschluss	Generalmajor Dr. Angar Rieks, Stv. Vorsitzender AFCEA Bonn e.V.

Ausstellerliste AFCEA-Fachausstellung 2017

	Ausstellende Firma/Organisation	Stand
1	A.WEIDELT Systemtechnik GmbH & Co. KG	F 30
2	ACT Gruppe	B 14
3	AD2V Industries GmbH	S 02
4	Adobe Systems GmbH	S 04
5	Airbus Defence and Space	M 01
6	Airbus Defence and Space / PMR	ME 06
7	Amphenol Military & Aerospace	B 05
8	AOC Red Baron Roost	F 46
9	apra-norm Elektromechanik	F 44
10	Aruba	S 03
11	Aschenbrenner Elektronik GmbH	S 02
12	ATM ComputerSysteme GmbH	M 06
13	Atos IT Solutions and Services GmbH	M 03
14	Avitech GmbH	S 11
15	Bechtle GmbH & Co. KG	M 07
16	Behörden Spiegel / ProPress Verlagsgesellschaft mbH	F 20
17	beltronic-IPC AG	F 47
18	blackned gmbh	M 31
19	BRUGG KABEL AG	B 02
20	BWI	M 10
22	CANCOM on line GmbH	ME 01
23	Carl-Cranz-Gesellschaft e.V.	B 15
24	Carmenta AB	F 21
25	CeoTronics AG	M 33
26	CGI Deutschland Ltd. & Co. KG	F 07
27	Cisco Systems GmbH	B 07
28	Citrix Systems GmbH	M 30
29	COMPAREX AG	F 14
30	Computacenter	M 22
31	Comrod Communications AS	F 42
32	Comsoft Solutions GmbH	B 09
33	Condok GmbH	S 06
34	CONET	M 13
35	conpal Information Security Systems GmbH	S 10
36	consistec Engineering & Consulting GmbH	ME 04
37	Cordsen Engineering GmbH	F 09
38	cpm communication presse marketing GmbH	F 58
39	crisis prevention	F 59
40	CSC Deutschland GmbH	M 04
41	dainox GmbH	M 24
42	DATAGROUP	M 23
43	Deutsche Gesellschaft für Wehrtechnik e.V. (DWT)	F 54
44	DeviceLock Europe GmbH	F 22
45	Die Plusbringer GmbH	F 52
46	DIGITTRADE GmbH	F 49
47	DSI Datensicherheit GmbH	B 01
48	ECOS Technology GmbH	F 29
49	EGL Elektronik Vertrieb GmbH	M 32
50	ELNO GmbH	B 02
51	ESET Deutschland GmbH	B 14
52	ESG Elektroniksystem- und Logistik-GmbH	M 05
53	Esri Deutschland GmbH	M 17
54	FFG FLENSBURGER FAHRZEUGBAU GmbH	S 02
55	Fraunhofer FKIE	M 27
56	Fraunhofer IOSB	B 12 + S 02
57	FREQUENTIS Deutschland GmbH	B 09
58	GBS TEMPEST & Service GmbH	S 05
59	Gebr. Friedrich Industrie- und Elektrotechnik GmbH	S 06
60	genua gmbH	M 15
61	griffity defense GmbH	S 02
62	Haivision Network Video	F 28
63	Hardthöhenkurier	F 55
64	Harris	B 04
65	HENSOLDT	S 08
66	Hexagon Safety & Infrastructure – c/o Intergraph SG&I Deutschland GmbH	F 15
67	Hitachi Data Systems GmbH	M 14
68	IABG mbH	M 28
69	IBM Deutschland GmbH	M 09
70	IHS Markit	S 07
71	INDRA SISTEMAS S.A.	S 11
72	INFODAS GmbH	M 19
73	IT-Standort Bonn	F 04
74	itWatch GmbH	F 26 + F 05
75	JK Defence & Security Products GmbH	F 41
76	Kongsberg Defence & Aerospace	F 48
77	Lachen helfen	B 16
78	Luciad	S 07
79	Matrox Electronic Systems GmbH	F 51
80	Media Broadcast Satellite GmbH	F 27
81	Microsoft Deutschland GmbH	F 08
82	Mittler-Report-Verlag	F 56
83	ML Gruppe	B 13
84	MÖNCH Verlagsges. mbH	F 57
85	Motorola Solutions	F 23
86	MSAB	S 12
87	ND SatCom GmbH	F 06
88	NYNEX satellite OHG	F 27
89	OHB System AG	F 01
90	ORACLE Deutschland B.V. & Co. KG	F 11
91	Panasonic Computer Product Solutions	F 02
92	Peli Hardigg	S 01
93	PlaceWorkers GmbH	F 52
94	promegis GmbH	B 08
95	PWA Electronic Service- und Vertriebs-GmbH	F 02
96	Rafael Advanced Defense Systems Ltd.	F 45
97	Rheinmetall Defence	M 02
98	Rheinmetall Technical Publication GmbH	S 09
99	Rockwell Collins Deutschland	B 03
100	roda computer GmbH	F 03
101	Rohde & Schwarz	M 16
102	rola Security Solutions GmbH	B 11
103	RUAG Schweiz AG – RUAG Defence	F 06
104	Saab International Deutschland GmbH	B 06 + S 02

Ausstellerliste AFCEA-Fachausstellung 2017

	Ausstellende Firma/Organisation	Stand
105	Saab Medav Technologies GmbH	S 02
106	SAF Tehnika JSC	ME 05
107	Safran Vectronix AG	F 53
108	SAP Deutschland SE & Co. KG	M 11
109	Schönhofer Sales and Engineering GmbH	F 24
110	SciEngines GmbH	F 10
111	Scopeland Technology GmbH	F 52
112	secunet Security Networks AG	M 20
113	Secusmart GmbH	M 12
114	Selex ES GmbH	M 21
115	Sennheiser Vertrieb und Service GmbH & Co. KG	F 32
116	SFC Energy AG	S 02
117	SINUS Electronic GmbH	F 31
118	Software AG	M 18
119	Solidtec GmbH	F 43
120	Sophos	S 10
121	Sopra Steria Consulting	F 12
122	SQS Software Quality Systems AG	F 50
123	steep GmbH	M 08
124	SUSE Linux GmbH	F 25
125	SVA System Vertrieb Alexander GmbH	M 14
126	Symantec	F 14
127	Systematic GmbH	M 26
128	systerra computer GmbH	ME 02
129	TAS – Telefonbau Arthur Schwabe GmbH & Co. KG	ME 03
130	TELEFUNKEN Radio Communication Systems GmbH & Co. KG	M 25
131	Textron Systems	B 08
132	Thales Deutschland	F 13
133	T-Systems International GmbH	B 10
134	Utimaco	S 10
135	Veritas	F 14
136	VITES GmbH	S 02
137	ZARGES GmbH	M 29

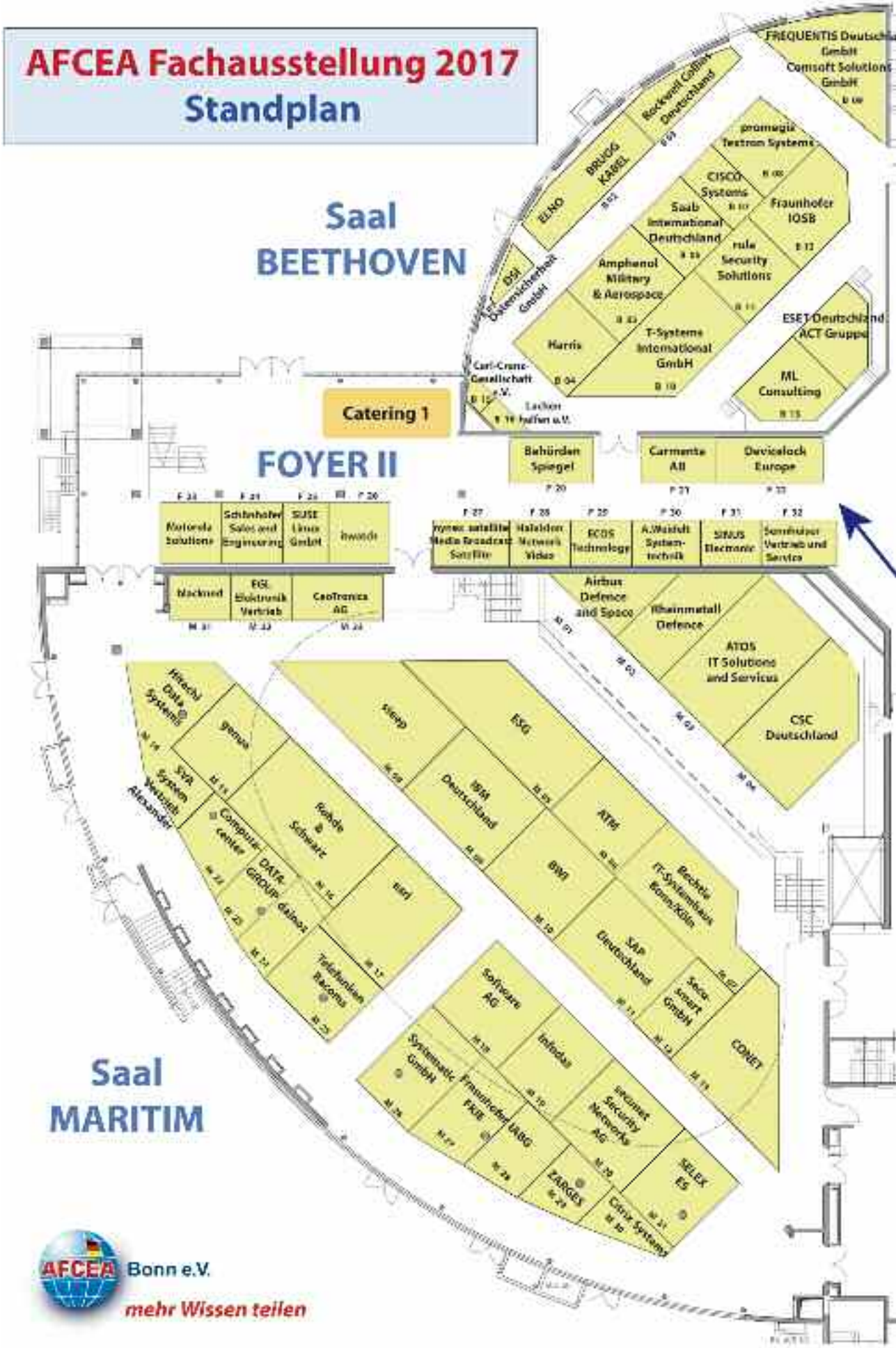
WLAN Fachausstellung 2017

gesponsort von

aruba

a Hewlett Packard
Enterprise company

AFCEA Fachausstellung 2017
Standplan



griffity defense GmbH
Aruba
Adobe Systems
GBS TEM PEST & Service
Austeller Gemeinschaftsstand griffity defense
Saal SCHUMANN
Condok
Lucind
Gebr. Friedrich
HENSOLDT
IHS Markit
Utimaco Sophos Conpal
Avitech Indra Sistemas S.A.
Saal REGER (Vorträge)
ORACLE Deutschland
Sopra Steria Consulting
Thales
COMPAREX Symantec Veritas
Hexagon Safety & Infrastructure
„IT-Standort Bonn"
Microsoft
CGI
RUAG Defence ND Saccom
Rwatch
roda computer
PWA
Panasonic
OHB

FOYER I < Eingang zur Fachausstellung

Catering 2
AFCEA Ausstellungs-büro

FOYER III
(Obergeschoss - über FOYER II)
Luftraum Foyer II
IK Defence & Security Products GmbH
Conrad AS
Solidtec GmbH
Rafael Advanced Defense Systems Ltd.
AOC Red Baron Rosat

Saal MARITIM - Empore
(Obergeschoss - Eingang über FOYER III)
CANCOM on line GmbH
systema GmbH
TAS
consistec
SAF Tehnika JSC
Airbus Defence and Space PMR

Stände:

Saal BEETHOVEN	B 01 - B 14
Saal MARITIM	M 01 - M 33
Saal MARITIM - Empore	ME 01 - ME 06
Saal SCHUMANN	S 01 - S 12
FOYER I	F 01 - F 15
FOYER II	F 20 - F 32
FOYER III	F 41 - F 59

Aussteller AFCEA-Fachmesse 2017

**Die folgenden Angaben wurden von den jeweiligen Anbietern geliefert.
Sie tragen für diese Eigenangaben und deren Wahrheitsgehalt die Verantwortung.**

A.WEIDELT Systemtechnik GmbH & Co. KG F 30

Die A. Weidelt Systemtechnik ist ein seit Jahrzehnten führender Systemintegrator und unverzichtbarer zuverlässiger Partner der Bundeswehr und ziviler Kunden. Durch langjährige Erfahrung in der Realisierung mobiler und stationärer Systeme, sowie

- ein hohes Maß an Kompetenz und Erfahrung spezialisierter Mitarbeiter,
- fachkompetente Projektleitung, Konstruktion und Integration,
- Systemschulung und Dokumentation,
- ständige Weiterentwicklung von Systemen und Neukonzipierungen,
- einen bundesweiten Vor-Ort-Service,
- umfangreiche Erfahrungen in der Durchführung von militärischen Beschaffungsvorhaben und Projekten,

liefern wir Lösungen zugeschnitten auf die individuellen Problemstellungen des Kunden.

ACT Gruppe B 14

Die ACT ist eine mittelständische Unternehmensgruppe mit 170 qualifizierten Mitarbeitern. Seit 1982 als IT-Dienstleister am Markt, unterstützen wir Unternehmen und Organisationen bei der Optimierung ihrer IT-Landschaften und sorgen für einen reibungslosen IT-Betrieb. Zu unseren Tätigkeiten gehören die Planung, Einrichtung und Überwachung hoch verfügbarer IT-Infrastrukturen, die Entwicklung und Integration individueller Customer Communication Management-Lösungen, die Analyse von Geschäftsprozessen sowie die Unterstützung von Betriebsorganisationen durch qualifizierte Dienstleistungen.
Im Bereich der IT-Security ist die ACT Experte für die Initiierung und Aufrechterhaltung von IT-Prozessen mit hohen Sicherheitsanforderungen. Wir unterstützen Unternehmen bei der Einrichtung von Informationssicherheitsstrategien, etablieren Risiko- und Notfallmanagements und trainieren Kundenmitarbeiter im Umgang mit unvorhersehbaren Risiken sowie bei der Erfüllung von Compliance-Anforderungen.
Kontakt: ACT IT-Consulting & Services AG, Rudolf-Diesel-Straße 18, 53859 Niederkassel,
Internet: www.actgruppe.de

AD2V Industries GmbH S 02

Die AD2V Industries GmbH ist ein hoch innovatives österreichisches Unternehmen, welches weltweit im Fachbereich von lichtempfindlichen optronischen Sensoren und Systemen für professionelle und behördliche sowie militärische Anwendungsgebiete tätig ist. Das Kerngeschäft des Unternehmens ist die Entwicklung, die Produktion und der Vertrieb von patentierten digitalen optoelektronischen Geräten und Systemen, insbesondere von digitalen Nachtsichtsystemen.Die Produktpalette reicht von Tag- und Nachtsichtsystemen über externes Zubehör bis hin zu individualisiertem Project Engineering, um spezielle Kundenbedürfnisse erfüllen zu können bzw. die Produkte optimal in die bestehende Infrastruktur integrieren zu können.

Adobe Systems GmbH S 04

Adobe ist der weltweit führende Anbieter von Software und Online-Services für Digitale Medien und Digitales Marketing. Drei leistungsstarke Cloud-Lösungen ermöglichen Kunden innovative digitale Inhalte zu kreieren, zielgenau auf allen relevanten Kanälen zu veröffentlichen, den Erfolg zu messen und kontinuierlich zu optimieren. Adobe beschäftigt weltweit über 14.000 Menschen bei einem Jahresumsatz von 5,85 Milliarden US-Dollar (im Finanzjahr 2016). Die Adobe Systems GmbH in München steuert Vertrieb, Marketing und Kundenbetreuung in Deutschland, Österreich und der Schweiz. Weitere Informationen erhalten Sie auch im Internet unter www.adobe.de.

Airbus Defence and Space M 01

AIRBUS ist ein weltweit führendes Unternehmen im Bereich Luft- und Raumfahrt sowie den dazugehörigen Dienstleistungen. Der Umsatz betrug im Jahr 2015 ~ Euro 64,5 Mrd., die Anzahl der Mitarbeiter rund 136.600. Das Unternehmen ist die europäische Nummer 1 und weltweit die Nummer 2 im Raumfahrtgeschäft. Airbus Defence and Space ist eine der Divisionen von AIRBUS und europäischer Marktführer im Verteidigungs- und Raumfahrtgeschäfts. Die Lösungen von Airbus Defence and Space garantieren außen- und verteidigungspolitische Souveränität. Zudem sichert das Unternehmensportfolio innovative End-to-End sichere Kommunikationsdienste & Lösungen, Mobilität und die Erweiterung von Know-how. Pioneering the future together www.airbusdefenceandspace.com

Airbus Defence and Space / Secure Land Communications ME 06

Das Tochterunternehmen Secure Land Communications (SLC) von Airbus entwickelt, installiert und wartet professionelle Mobilfunknetzwerke (PMR/LMR). Diese basieren auf Tetra-, Tetrapol- und P25-Technologien und bieten Kunden weltweit eine umfassende Palette an Lösungen für die Funkkommunikation. Darüber hinaus umfasst das Portfolio Notrufzentralen (911/112) und einsatzkritische Breitbandlösungen basierend auf 3GPP Standards. Mit rund 280 Funknetzen in mehr als 74 Ländern ist SLC weltweit einer der führenden PMR-Anbieter. Mit der Notrufbearbeitungslösung VESTA 911 bedient SLC mehr als 60 % des US-Markts für 911-Notrufzentralen. SLC beschäftigt knapp 1.700 Mitarbeiter in 20 Ländern.
www.securelandcommunications.com

Amphenol Military & Aerospace B 05

Amphenol ist weltweit einer der führenden Steckverbinder-Hersteller in den Bereichen Luftfahrt, Militär und Industrie. Unser Lieferspektrum umfasst auch viele Produkte für High-Speed / Ethernet / Datenübertragung. Unsere Steckverbinder und Leitungen eignen sich für hohe Übertragungsraten bis zu 10 Gigabit bei Kupfer- und › 10 GBit bei Glasfaser-Systemen. Viele dieser Amphenol-Produkte verfügen über eine VG-Zulassung und sind damit als bevorzugte Lösung für Militärapplikationen in Deutschland und Europa anzusehen, wie z.B. RJ45 Ethernet-Steckverbinder für Datenübertragung nach VG96983 plus passendes CAT7-Kabel nach VG95218 T 31 B 001.
Kontakt: Amphenol-AirLB GmbH, Am Kleinbahnhof 4, D-66740 Saarlouis,
Tel. +49/68 319 810-0, info@amphenol-airlb.de, www.amphenol-airlb.de

AOC Red Baron Roost F 46

Der AOC Red Baron Roost ist das deutsche Chapter der internationalen Fachinteressengemeinschaft für den Elektronischen Kampf, der in den 1960'ziger Jahren gegründeten Association of Old Crows. Wir bieten unseren Mitgliedern aus den Streitkräften, den wehrwissenschaftlichen und wehrtechnischen Instituten und der Rüstungsindustrie ein anerkanntes Forum zum fachlichen Erfahrungs- und Interessenaustausch. Neben dem für unsere Mitglieder kostenfreien monatlich erscheinenden Fachmagazin "Journal of Electronic Defence (JED)" bieten wir regelmäßige Informationsveranstaltungen und Themenabende zu aktuellen Themen rund um die Bereiche EW, IO, EMSO und CEMA an. Sie finden weitere Informationen unter www.aoc-redbaronroost.de und www.crows.org

apra-norm Elektromechanik F 44

apra-norm ist der Spezialist für EMV-geschützte 19"-Schränke und Gehäuse für kritische und sicherheitsrelevante EDV und IT-Anwendungen. Seit 1969 entwickelt und fertigt apra-norm High-Tech Elektronik-Gehäuse und Schränke für Anwendungen in der Daten- und Netzwerktechnik, der Elektronikindustrie, der Mess- und Regeltechnik sowie der Sicherheits- und Informationstechnik. Zusätzlich zum reinen Gehäuse werden auf Wunsch Bauelemente wie Kabel, Stecker, Lüfter oder Stromversorgungen vorkonfektioniert und die Baugruppen auf Herz und Nieren geprüft und getestet. Eine besondere Stärke der apra-Gruppe ist die Fertigung kundenspezifischer Gehäuse in Klein-, Mittel und Großserien aus Stahlblech, Edelstahl, Aluminium und Kunststoff – auch ohne Werkzeugkosten.
Kontakt: apra-norm Elektromechanik GmbH, Ihr Kontakt: Jörg Stölben, Tel.: 06592 / 204-160, J.Stölben@apra.de, Gewerbegebiet • D-54552 Mehren / Vulkaneifel, Tel.: 06592 / 204-0 Fax: 06592 / 204-100 • vertrieb@apra.de, www.apra.de

Aruba S 03

Aruba, a Hewlett Packard Enterprise company, ist ein führender Anbieter von Next-Generation-Netzwerklösungen für Unternehmen jeder Größe weltweit. Das Unternehmen liefert IT-Lösungen, mit denen Organisationen die neueste Generation von technikversierten Nutzern, die sich sowohl bei der Arbeit als auch im Privatleben voll und ganz auf Cloud-basierte Geschäftsanwendungen verlassen, unterstützen.Weitere Informationen und aktuelle Nachrichten zu Aruba erhalten Sie auf http://www.arubanetworks.com, Twitter und Facebook. Um mehr über die neusten technischen Diskussionen zu Mobility und Produkten von Aruba zu erfahren, besuchen sie Airheads Social unter http://community.arubanetworks.com.

Aschenbrenner Elektronik GmbH S 02

Aschenbrenner Elektronik was founded in 1948. Since then we have become a leading company in developing, manufacturing and testing rugged vision- and camera- systems, mobile X86 computer platforms and hardened power supplies as well as special analog to digital visual interface adaptions for military CRT-Monitor replacements. Many years of experience in combination with in-house capabilities for manufacturing, environmental and EMI testing leads us to be a strong OEM/ODM partner for our customers. Our custom specific solutions are used in wheel/chain- driven vehicles as well as in aviation, navy and railway.
Products:

- Dual Sensor Thermal
- HD Camera Systems
- other Customized Systems

ATM ComputerSysteme GmbH M 06

Die ATM ComputerSysteme GmbH ist ein international aktives Systemhaus für gehärtete IT-Hardware und Software. Als langjähriger Partner der Bundeswehr ist die ATM seit mehr als drei Jahrzehnten erfolgreich. Fokus der Entwicklungen sind Computer- und Displaysysteme, Panel-PCs,

mobile wie stationäre Kommunikationsanwendungen sowie die Erstellung leistungsfähiger und passgenauer Software. Die IT-Systeme trotzen härtesten Umweltbedingungen, wie sie zu Land, zu Luft und zu Wasser herrschen. Wer im internationalen Markt bestehen will, muss maßgeschneiderte Produkte präsentieren. Die ATM verwirklicht dies mit ihren innovativen Lösungen. Dienstleistungen und Beratung rund um das Produkt charakterisieren die Unternehmens- und Produktphilosophie.
Kontakt: ATM ComputerSysteme GmbH, Max-Stromeyer-Str. 116, 78467 Konstanz,
Tel. +49/75 31 808 44 62, info@atm-computer.de, www.atm-computer.de

Atos IT Solutions and Services GmbH — M 03

Atos SE (Societas Europaea) ist ein führender Anbieter von digitalen Services mit einem Pro-forma-Jahresumsatz von rund 12 Milliarden Euro und circa 100.000 Mitarbeitern in 72 Ländern. Atos unterstützt Unternehmen weltweit mit Beratungsleistungen und Systemintegration, Managed Services & Business Process Outsourcing (BPO) sowie Cloud-, Big-Data- und Sicherheitslösungen. Hinzu kommen Services von der Tochtergesellschaft Worldline.Atos präsentiert auf der AFCEA seine Lösungskompetenz bei der Entwicklung und Betriebsunterstützung von einsatzfähigen IT-Plattformen (insbesondere Führungsinformationssystemen) und bietet Informationen zu Technologietrends.
Kontakt: Atos IT Solutions and Services GmbH; Franz-Geuer-Str. 10; D-50823 Köln;
Hubert Geml (Leiter Defense); Tel: +49 (0)173 / 979 38 04; hubert.geml@atos.net

Avitech GmbH — S 11

Avitech GmbH, eine Tochtergesellschaft der Indra Sistemas S.A., ist seit über 20 Jahren kompetenter und verlässlicher Systempartner der Bundeswehr für das FSInfoSysBw und InfoDADBw. Unsere Kompetenzen liegen im Bereich der Aeronautischen und Hindernis Datenbank, Luftfahrtkarten, sowie Flugplan- und Pilotenbriefingssysteme inklusive Schnittstelle zur zivilen Flugsicherung und zu Euro-control. Darüber hinaus sind Meldungsvermittlungs- und Kommunikations-systeme sowie SWIM Lösungen bei der Bw im Einsatz. Avitech Produkte werden bundeswehrweit und von den in Deutschland stationierten Bündnispartnern an ca. 100 Standorten genutzt. Auf der AFCEA 2017 ist Interoperabilität, Datenversorgung für Missionsplanung und Datenvisualisierung unser Schwerpunkt.
Kontakt: Thomas Mattick, Programm Manager Bundeswehr, Bahnhofplatz 1,
88045 Friedrichshafen, Telefon: +49 (0)7541 / 282-0, www.avitech.aero

Bechtle GmbH & Co. KG — M 07

Das Bechtle IT-Systemhaus Bonn/Köln gehört zur Bechtle AG, die mit rund 70 Standorten, 40 Bechtle Competence Centern sowie einem Umsatz in 2015 von rund 2,8 Mrd. Euro zu einem der führenden Systemintegratoren in Deutschland zählt. Seinen mehr als 75.000 Kunden aus Industrie, öffentlichen Auftraggebern und Finanzmarkt bietet Bechtle herstellerneutral ein lückenloses Angebot rund um die IT-Infrastruktur. Unsere zentralen Lösungsthemen: Client Management, Server & Storage, Networking Solutions, Virtualisierung, IT-Security und Software.
Bechtle ist seit Jahren mit einem spezialisierten Geschäftsbereich Öffentliche Auftraggeber erfolgreich und bietet seinen Kunden in diesem Segment unter anderem den Einkauf ihrer IT über die maßgeschneiderte Online-Beschaffungsplattform **bios®government.** Weiterführende Informationen – auch zu unseren Bundeswehr Rahmenverträgen 2./3. Rechnerebene und Notebook Standard – erhalten Sie an unserem Stand M07 im Saal Maritim. Mehr zu Bechtle unter www.bechtle.com

Behörden Spiegel / ProPress Verlagsgesellschaft mbH — F 20

Der Behörden Spiegel ist mit einer Druckauflage von 112.000 Exemplaren monatlich die auflagenstärkste unabhängige Zeitung für den Öffentlichen Dienst in Deutschland. 108.385 Zeitungen (4. Quartal 2016 IVW) werden nachweislich verbreitet.
Neben der Bundeshauptstadt Berlin sind 16 Landeshauptstädte, der Standort Bonn und letztlich jede Kommune und jeder Landkreis Ziele des Vertriebs. Zudem ist die Gesellschaft Ausrichter mehrerer großer Kongresse, so u.a. der Berliner Sicherheitskonferenz, des Europäischen Polizeikongresses und des Europäischen Katastrophenschutzkongresses.

beltronic-IPC AG — F 47

Wir entwickeln und fertigen wir Embedded-PCs, Portable-PC's und Displays für industrielle und militärische Anwendungen. Basierend auf hochzuverlässigen embedded COTS Komponenten konzentrieren wir uns auf die Entwicklung und Produktion von extrem robusten, zuverlässigen und kosteneffizienten Systemlösungen gemäss den jeweiligen Kunden Projektspezifikationen. Wir verfügen über eine Jahrzehnte lange Erfahrung bezüglich robuster PC'S, Portables und Displays. Unsere Unternehmensstruktur ist sehr flexibel, damit sind wir in der Lage kundenspezifische Lösungen auch in sehr kleinen Losgrössen zu fertigen.
In Deutschland verfügen wir über einen eigenen ISO-9001 zertifizierten Fertigungs-Betrieb (ALR rugged solutions GmbH)
Kontakt: beltronic-IPC AG, CH 8455 Rüdlingen, Benno Ledergerber, benno.ledergerber@beltronic-ipc.com, Tel. +41 / 448 672 489,
www.beltronic-ipc.com, www.beltronic.fr

blackned gmbh — M 31

blackned ist Hersteller moderner Kommunikations- und Netzwerklösungen mit Sitz in Süddeutschland. Mit ihrem Portfolio bietet blackned Kommando-, Kontroll- und Kommunikationslösungen für unterschiedliche Branchen und Anwendungen. Im militärischen Bereich ist blackned führender Kompetenzpartner in Konzeption und Betrieb verlegefähiger Netzwerke. Für den zivilen Bereich stellt blackned Lösungen für hochmobile zellulare Daten- und Kommunikationsnetzwerke bereit. So ermöglicht z.B. die modulare Software Plattform RIDUX eine einfache Bedienung von hoch komplexen Kommunikations- und Datenübertragungssystemen: von der Bereitsstellung des Übertragungsmediums bis hin zur MANET-fähigen Dienste- und Servicearchitektur.blackned – critical command and control solutions. anywhere. blackned gmbh · +49(0)8331/9959 – 600 · info@blackned.de · www.blackned.de

BRUGG KABEL AG — B 02

Brugg Cables ist für Signal- und Energiekabel weltweit bekannt. In der **Wehrtechnik** besticht Brugg Cables durch **besonders robuste taktische fiberoptische Feldkabel,** konfektioniert mit verschiedensten **Militärsteckertypen.** Diese Stecker sind zu tausenden seit über 10 Jahren im harten Feldeinsatz. Die breite Zubehörpalette, **zur Feldverlegung,** die **Test-, Unterhalts-** und **Reparaturkits** werden von anspruchsvollen Militärkunden gefordert. Die angebotenen **Lösungen** sind in der **Schweizer Armee,** der **Bundeswehr,** bei weiteren **NATO-Mitgliedern** und **Streitkräften weltweit** beliebt. Der große **Erfahrungsschatz** in **Design** und **Systemintegration** fließt in die **Lösungspalette,** sowie in **Kundenschulungen** ein. **Am Stand B02 im Saal Beethoven präsentieren wir als Hauptthema unsere patentierten Blitzschutzlösungen für den Ausseneinsatz.**
Kontakt: Brugg Kabel AG, Klosterzelgstrasse 28, CH-5201 Brugg, Vertrieb Deutschland, Edi Lützenkirchen Tel. +49(0)170 / 188 20 71

BWI — M 10

Die BWI gehört zu den Top 10 der IT-Service-Unternehmen in Deutschland. Gegründet wurde sie Ende 2006 als öffentlich-private Partnerschaft zwischen Bundeswehr, Siemens und IBM, um das IT-Projekt HERKULES für die Bundeswehr zu realisieren. Wie vorgesehen endete das Projekt im Dezember 2016. Bis dahin hatte die BWI das nichtmilitärische IT-System der Bundeswehr konsolidiert, zentralisiert und modernisiert. Seit dem 28. Dezember 2016 ist die BWI eine 100-prozentige Bundesbeteiligung, die als GmbH rechtlich selbstständig bleibt. Sie ist weiterhin der zentrale IT-Dienstleister der Bundeswehr und erbringt hierbei vielfältige Leistungen (u.a. Rechenzentren, Netze, IT-Arbeitsplatzausstattung, SASPF). Neben der kontinuierlichen Verbesserung und Weiterentwicklung der IT-Services soll die BWI künftig weitere Aufgaben übernehmen und sich zum IT-Systemhaus der Bundeswehr entwickeln. Die BWI informiert bei der AFCEA-Fachausstellung 2017 über ihren Weg zum IT-Systemhaus und über IT-Entwicklungen bei der Bundeswehr.

CANCOM on line GmbH — ME 01

Die CANCOM on line GmbH ist aufgrund seiner mehrjährigen Erfahrung im Public-Sektor optimal darauf eingestellt, die dedizierten Anforderungen von Bund, Ländern und Kommunen zu erfüllen. Darüber hinaus unterstützen wir seit Jahren Sicherheitsbehörden sowie die Bundeswehr. Unser bundesweit agierendes Team erfasst Ihre speziellen Ansprüche und bietet maßgeschneiderte Lösungen und Dienstleistungen für diesen Bereich an.Mit CANCOM Public Solutions betreuen wir Sie umfassend in verschiedenen Bereichen des Öffentlichen Sektors:Gewährleistung einer sicheren und störungsfreien IT Infrastrukturumfassender Schutz personenbezogener DatenIndividuelle Beratung und Konzeptionierung einer IT Architektur für Ihre BedürfnisseBranchenspezifische Lösungen und umfassendes Know How im Public Bereich, seit 25 JahrenAlle Anforderungen bezüglich Spezialisierung und Zertifizierung

Carl-Cranz-Gesellschaft e.V. — B 15

Gesellschaft für technisch-wissenschaftliche Weiterbildung.Technisch-wissenschaftliche Weiterbildung für Ingenieure und Naturwissenschaftler auf höchstem Niveau – Dieser Aufgabe widmet sich die Carl-Cranz-Gesellschaft e.V. (CCG) als gemeinnützige Einrichtung seit mehr als 50 Jahren. Gemeinsam mit führenden Experten aus Forschung & Entwicklung sowie Industrie erarbeiten wir das Potenzial zukunftsträchtiger Technologien und stellen bedarfsgerechte, praxisorientierte Fort- und Weiterbildungen in unserem Seminarzentrum in Oberpfaffenhofen, an weiteren Standorten in Deutschland, Frankreich, Österreich, der Schweiz sowie bei Bedarf auch Inhouse zur Verfügung. Kleine Lerngruppen und renommierte Dozenten aus Hochschule, Forschung und Industrie garantieren den Lernerfolg. Zu unseren Kernkompetenzen zählen die Fachgebiete Informations- und Kommunikationstechnologie, Führungs- und Aufklärungssystemsysteme, Mobilität / Transport- und Verkehrssysteme, Sensorik, Verteidigung- und Sicherheitstechnik, Werkstoffkunde und Werkstofftechnologie sowie fachgebietsübergreifende Querschnittsthemen.
Kontakt: Petra Walter, Marketing, Argelsrieder Feld 11, 82234 Weßling/Obb.,
Tel. +49 (0)8153 / 881 198 13, Fax +49 (0)8153 / 881 198 19, petra.walter@ccg-ev.de, www.ccg-ev.de

Carmenta AB — F 21

Carmenta AB ist ein schwedisches Unternehmen mit nun 30 Jahren Erfahrung im high-performance GIS Geospatial Technology Software Bereich für Systeme in der Verteidigung und in Public Safety Anwendungen. Als aktives Mitglied des Open Geospatial Consortiums (OGC) unterstützen wir die möglichst weitreichende Nutzung von Standards.
Verteidigung
Unsere Technologien und Lösungen für den Verteidigungssektor werden von mehreren Armeen genutzt. Unsere GIS Entwicklungswerkzeuge wurden zusammen mit den Kunden optimiert. Durch die partnershaftliche Zusammenarbeit mit unseren Anwendern sichern wir auch die Unterstützung für zukünftige Aufgaben. Unsere Lösungen finden Anwendung in allen drei Bereichen Luft, Land und See.
Public Safety Systeme

Carmentas Public Safety Lösungen basieren auf unseren GIS – Technologien, ergänzt um Kommunikations-Lösungen für Notrufzentralen.
Kontakt: Carmenta AB, www.carmenta.com , Gordian Massing, Röhlenend 96, D-41751 Viersen, Tel: 02162 / 949311, Gordian.Massing@carmenta.com

CeoTronics AG — M 33

CeoTronics AG – Innovative Produkte "Made in Germany"
Seit über 30 Jahren vertrauen die Spezialkräfte von Polizei und Militär auf die Zuverlässigkeit der Kommunikationssysteme von CeoTronics. Die kundenindividuellen Lösungen werden in enger Zusammenarbeit mit den Anwendern entwickelt. Hierbei schätzen unsere Kunden den kurzen Weg zum Ingenieurs-Know-how. Der Konzern umfasst derzeit drei Tochterunternehmen in drei Ländern, Vertriebsmitarbeiter im In- und Ausland sowie Vertriebspartner, die die in Deutschland entwickelten und produzierten Produkte in über 40 Ländern der Erde verkaufen. Zahlreiche Premium-Hersteller von Schutzhelmen, Funkgeräten, Spezialfahrzeugen und Flugzeugen vertrauen auf die Produkte der CeoTronics AG und ihrer Tochterunternehmen.
CeoTronics AG, Audio • Video • Data Communication, Adam-Opel-Str. 6, 63322 Rödermark (Germany), Tel. +49 (0)6074 / 8751-0, Fax +49 (0)6074 / 8751-265, verkauf@ceotronics.com, www.ceotronics.com

CGI Deutschland Ltd. & Co. KG — F 07

CGI, gegründet 1976, ist ein globaler Dienstleister für IT und Geschäftsprozesse, der mit 68.000 Mitarbeitern Business- und IT-Beratung, Systemintegration und Outsourcing Services auf Top-Niveau anbietet. Unsere langjährige Erfahrung in der Zusammenarbeit mit Auftraggebern aus Militär und BOS ist der Garant für höchste Qualität, Innovation und Einsatzorientierung unseres Portfolios an marktverfügbaren Produkten und Dienstleistungen. Wir präsentieren Lösungen für den stationären, verlegefähigen und mobilen Einsatz (HaFIS verlegefähig und mobil) sowie für die aktuellen und kommenden Herausforderungen im Bereich der Cyber-Sicherheit. Mit DokMBw demonstrieren wir die Zukunft für die Stabs- und Verwaltungsarbeit der Bundeswehr.
Kontakt: CGI Deutschland Ltd. & Co. KG, Andreas Pankratz, T. +49 (0)2203 / 6993-0, andreas.pankratz@cgi.com, de.cgi.com

Cisco Systems GmbH — B 07

Netzwerke sind heute wichtiger Teil der Infrastruktur im Bereich der Verteidigung. Die von Cisco entwickelten Produkte auf Basis des Internet-Protokolls sind Grundlage dieser Netzwerke und machen Cisco zum weltweit führenden Anbieter.Für Institutionen im Bereich der Verteidigung eröffnet die Vernetzung über die Domänen Heimatland, verlegefähige Systeme, mobile Infrastrukturen und abgesessene Einheiten sowie mit Koalitionspartnern zahlreiche Möglichkeiten: Durch intelligentes Zusammenspiel von Personen, Prozessen, Daten und Dingen können Prozesse optimiert, Ressourcen effizienter und sicher genutzt und Vorteile in allen Domänen für Aufklärung, Gefecht, Logistik und Sanitätswesen realisiert werden.Im Geschäftsjahr 2016 erzielte Cisco einen Umsatz von 49,2 Milliarden $ mit weltweit ca. 71.500 Mitarbeitern.

Citrix Systems GmbH — M 29

Citrix (NASDAQ:CTXS) entwickelt Lösungen für eine Welt, in der Menschen, Organisationen und Dinge sicher miteinander vernetzt sind, um das Außergewöhnliche zu erreichen. Die Citrix-Technologien machen Apps und Daten weltweit sicher und einfach abrufbar, damit Menschen zu jeder Zeit und von überall aus arbeiten können. Citrix bietet ein integriertes Lösungsportfolio für Workspace-as-a-Service, Anwendungsbereitstellung, Virtualisierung, Mobility, Networking und Filesharing. Mehr als 400,000 Organisationen und 100 Millionen Anwender setzen auf Technologien von Citrix. Im Jahr 2016 erwirtschaftete das Unternehmen einen Umsatz von 3,42 Milliarden US-Dollar.
Kontakt: Citrix Systems GmbH, Guido Maßfeller, Erika-Mann-Straße 67-69, 80636 München, Mobil: +49 (0)151 / 140 587 30, E-Mail: guido.massfeller@citrix.com, Internet: www.citrix.de

COMPAREX AG — F 14

COMPAREX ist ein weltweit agierendes IT-Unternehmen, das auf Lizenzmanagement, Software-Beschaffung, technische Produktberatung sowie Cloud-basierte Services spezialisiert ist. Mit seiner mehr als 30-jährigen Markterfahrung adressiert COMPAREX Öffentliche Verwaltungen und Mittelstand ebenso wie Industrieunternehmen und international agierende Konzerne. Das Angebotsportfolio umfasst Software-Lizenzen von mehr als 3.000 Herstellern sowie Beratungs- und Service-Leistungen. COMPAREX ist ausgewiesener Cloud-Experte für maßgeschneiderte sichere Cloud Computing-Lösungen und Security-Konzepte.
COMPAREX ist Microsoft Global Partner Nr. 1 in Deutschland und führend in Europa. Das IT-Dienstleistungsunternehmen mit 3.300 Zertifizierungen von 60 Herstellern, ist für seine Kunden an mehr als 80 Standorten in 35 Ländern präsent.
Kontakt: Mathias Matzner, COMPAREX Sales Executive Region West,
Telefon: +49 (0)2219 / 938 586 18, Mobil: +49 (0)163 / 729 54 38, Mathias.Matzner@comparex.de

Computacenter — M 22

Computacenter ist Europas führender herstellerübergreifender Dienstleister für Informationstechnologie. Kundennähe bedeutet für uns, Geschäftsanforderungen zu verstehen und präzise darauf einzugehen. Auf dieser Basis entwickeln, implementieren und betreiben wir für unsere Kunden maßgeschneiderte IT-Lösungen.
Darüberhinaus hält Computacenter diverse Rahmenverträge mit Landesministerien und Dienstleistungszentren verschiedener Länder und Kommunen.
Weitere Informationen erhalten Sie gerne an unserem Stand oder über Dr. Carsten Jürgens /Direktor Geschäftsfeldentwicklung (carsten.juergens@computacenter.com).

Comrod Communications AS — F 43

Comrod Communications AS have their corporate headquarters in Stavanger, Norway with manufacturing facilities in Norway, France, Hungary and the USA. Comrod designs and manufactures manpack, vehicle, remote and shipboard antennas in the HF/VHF/UHF/SHF frequency bands. Sophisticated multiband versions are available to overcome co-site or space constraints. Support masts are available to elevate top loads at heights ranging from 5 to 34 metres (16 to 110 ft). Aluminium telescopic, composite telescopic, sectional tripod and manpack sectional models are available. Comrod ComPact series power supplies and battery chargers provide the best power to size density available on the market today.

Comsoft Solutions GmbH — B 09

Die Comsoft Solutions GmbH ist ein mittelständisches Technologieunternehmen mit Sitz in Karlsruhe. Als Anbieter individueller Systeme und Dienstleistungen beliefern wir zivile und militärische Flugsicherungsbehörden weltweit. Unsere Lösungen sind in Flugkontrollzentren und Flughäfen in mehr als 80 Ländern im Einsatz und leisten dort einen wichtigen Beitrag zur internationalen Flugsicherheit.
Im Bereich der Message Handling Systeme ist Comsoft Solutions seit Jahren Weltmarktführer, und auch bei anderen hochkomplexen Technologien sind wir einer der Top-Anbieter. Seit 2016 ist Comsoft Solutions Teil der Frequentis Firmengruppe, einem global sehr erfolgreich agierenden Konzern mit Hauptsitz in Wien und zahlreichen Niederlassungen weltweit.

Condok GmbH — S 06

Die CONDOK GmbH ist ein Systemhaus für technische Dienstleistungen, System-Entwicklung und Realisierung. Neben der Spezialisierung auf die Erstellung von IETD nach S1000D/ S2000M werden vielfältige und umfangreiche Technische Dokumentationen, Bebilderte Teilekataloge, Technische Übersetzungen und Computer Based Trainings erstellt. Als Systemhaus entwickelt und realisiert CONDOK Einrüstungs- und Umrüstungsmaßnahmen in Kabinen und Fahrzeugen und führt Instandsetzungsleistungen durch. Das Portfolio wird durch die Bereiche der Produkt- und Betriebssicherheit sowie Themen des Integrated-Logistic-Support abgerundet. Mit mehr als 110 Mitarbeitern in Kiel, Hamburg und Koblenz unterstützt die CONDOK mit umfangreichen technischen und logistischen Dienstleistungen die Bundeswehr sowie eine große Anzahl von Unternehmen der Wehrtechnik und der zivilen Industrie.
Kontakt: www.condok.de

CONET — M 13

"Erfolg. Unsere Leidenschaft." CONET ist das kompetente IT-System- und Beratungshaus für SAP, Infrastructure, Communications, Software und Experts. CONET begleitet die Bundeswehr seit mehr als 25 Jahren als zuverlässiger Berater und Realisierer in allen Fragen der Informationstechnologie. Durch partnerschaftliche Zusammenarbeit, Innovationsfähigkeit und hohe Dienstleistungsqualität entstanden und entstehen erfolgreiche gemeinsame Implementierungen für Fach- und Führungsinformationssysteme, SAP, Kommunikationsarchitekturen und IT-Infrastrukturen. An seiner Plan-Bar (Stand M 13) präsentiert CONET aktuelle Lösungen etwa für IT-Sicherheit und Cyber Defense, Modellierung im Architekturmanagement, die eRecruiting-Plattform der Bundeswehr und Entwicklungsansätze für schnellere und gleichzeitig einfachere Prozesse mit SAP HANA.
Kontakt: www.conet.de | info@conet.de

conpal Information Security Systems GmbH — S 10

conpal Information Security Systems GmbH ist ein Anbieter von Lösungen im Bereich IT-Sicherheit mit Fokus auf den Themen Endgeräte-Sicherheit, Authentisierung sowie Identity und Access Management. Grundlage des Angebotes sind eigenentwickelte Standard-Software-Lösungen und Technologien sorgfältig ausgewählter Partnerunternehmen. Durch kontinuierliche Analyse von Markt- und Technologieentwicklungen erreichen wir in unserem Portfolio einen optimalen Mix zukunftssicherer Technologien in Verbindung mit praxisorientierter Umsetzung. Die Lösungen von conpal sind konsequent an den Bedürfnissen der Kundenumgebungen ausgerichtet, einfach einzuführen und verhalten sich robust im Betrieb.

consistec Engineering & Consulting GmbH — ME 04

consistec Engineering & Consulting ist ein innovatives mittelständisches Unternehmen mit langjähriger Erfahrung im ITK- und Industriebereich. Mit den Geschäftsbereichen "Tracing & Monitoring – Made in Germany" und "Softwareentwicklung für technische Systeme" unterstützt consistec u.a. die Deutsche Telekom als Preferred Supplier.
caplon©-Systeme von consistec überwachen Qualität, Verfügbarkeit, Integrität sowie Performance und Normverhalten von IT-Systemen und IP-basierten Diensten (Services) und berücksichtigen die Umsetzung deutscher/europäischer Datenschutzaspekte (EU-DSGVO, BDSG, TKG, ...) – ohne Backdoors.
Segmente:
- **Tracing:** Compliance-Monitoring, Fehleranalyse in Hochgeschwindigkeitsnetzen
- **Service-Monitoring:** Performance-, Prozess-Monitoring, User-Experience-Monitoring
- **VoIP-Monitoring:** Call- und Qualitätsanalyse, Fraud-Detection
- **Security-Monitoring:** Risikominimierung, Event-Detection

Produktinnovation: caplon© Privacy-Protection – Pseudonymisierung personenbezogener Daten
- Informationen schützen, technische Probleme trotzdem erkennen
- Hohe Hürden gegen Datenmissbrauch

Cordsen Engineering GmbH F 09

CORDSEN Engineering GmbH entwickelt und fertigt eine breite Palette an militärisch gehärteten (Ruggedized) Workstations und Peripheriegeräten nach MIL-STD-810F / MIL-STD-461E für mobilen und stationären Einsatz, sowie abstrahlsichere (TEMPEST) Produkte nach SDIP 27 Level A / COMSEC Zone 0, wie Workstations, Server, TFT-Displays bis 65", FO-Hubs, Drucker und Scanner.
Mit der Fa. Aqeri/Schweden, einem der führenden Hersteller von rugged Equipment, wurde ein Kooperationsvertrag abgeschlossen.
Wir verfügen über zwei TEMPEST/EMV-Labore: Für Zulassungsmessungen nach SDIP 27 Level A/B/C, sowie für Zulassungsmessungen und KMVs nach dem Zonenmodell. Als Dienstleistungen bieten wir u. a. Platform-Testing an.
Kontakt: Cordsen Engineering GmbH, Am Klinggraben 1A, D-63500 Seligenstadt
Tel. 06182 / 9294-0, Fax 06182-9294-45, Internet: www.cordsen.com

cpm communication presse marketing GmbH F 58

cpm communication presse marketing GmbH wurde 1989 als Dienstleistungsgesellschaft für Publikationen, Tagungen und Studien in ausgewählten Marktsegmenten gegründet. In enger Zusammenarbeit mit vornehmlich militärischen Stellen und der Wirtschaft veranstaltet cpm nationale und internationale Fachtagungen (z.T. mit begleitender Ausstellung).
Zu unseren Veröffentlichungen gehören:
- **cpm forum – Das Magazin für Wehrtechnik und Logistik** als themenorientierte wehrtechnische Dokumentationen mit jährlich 6 Publikationen
- Taschenbuch "Deutsche Bundeswehr – Folge 5 (2015)" als aktuelles Nachschlagewerk über die deutschen Streitkräfte
- Taschenbuch "Die Ausrüstung der Bundeswehr" – Folge 2 (2013).
- Die Internetplattform **"German Defence Industry"**

info@cpm-st-augustin.de / www.german-defence-industry.com

crisis prevention F 59

CRISIS PREVENTION, das Fachmagazin für Innere Sicherheit, Bevölkerungsschutz und Katastrophenhilfe, bietet ein Forum zum fachlichen Austausch zur Prävention von Großschadensereignissen und zu Konzepten zur Krisenbewältigung. In der Vernetzung der verantwortlichen Akteure untereinander möchte CRISIS PREVENTION einen Beitrag als Plattform zur Kommunikation leisten, um Synergien aufzudecken und deren Nutzung effizienter zu gestalten. Thematisch deckt CRISIS PREVENTION die Arbeitsbereiche der vielfältigen Leserschaft ab: Von BOS bis zur Bundeswehr, vom Brand- und Katastrophenschutz bis zur Informations- und Kommunikationstechnologie und Geoinformationssystemen.
Kontakt: CRISIS PREVENTION/Beta Verlag GmbH – Celsiusstr. 43 – 53125 Bonn – André Birr
Tel.: 0228 / 919 37-68 – E-Mail: andre.birr@beta-publishing.com

CSC Deutschland GmbH M 04

CSC begleitet Kunden auf ihrem Weg in die digitale Transformation. Das Unternehmen bietet innovative Next-Generation-IT-Dienstleistungen und -Lösungen sowie umfassende Branchenexpertise, globale Reichweite, Technologie-Unabhängigkeit und ein weitreichendes Partner-Netzwerk. Mithilfe von modernen Technologielösungen unterstützt CSC führende Organisationen aus der Privatwirtschaft sowie dem internationalen öffentlichen Sektor auf der ganzen Welt bei der Modernisierung ihrer Geschäftsprozesse, Applikationen und Infrastrukturen.
Kontakt: CSC, Abraham-Lincoln-Park 1, 65189 Wiesbaden, E-Mail: deutschland@csc.com, Internet: www.csc.com/de

dainox GmbH M 24

dainox ist ein Hersteller verlegefähiger Kommunikationslösungen der Bundeswehr und etablierter Dienstleistungsanbieter in den Themengebieten Internetworking, Computing und Virtualisierung. **dainox** unterstützt bei der Planung, Implementierung, Dokumentation und dem Betrieb von IT Infrastrukturen. Mit Hilfe der **dainox** Strategie- und IT Architekturberatung werden nachhaltige und langlebige IT Lösungen geschaffen.
In unseren Projekten wird über eine enge Zusammenarbeit mit dem Kunden ein effizienter Ablauf mit einem optimalen Know-how Transfer garantiert und so eine hohe Wertschöpfung ermöglicht.
Gebündeltes Fachwissen auf den Punkt gebracht – dainox ®.
Technologie – Ausbildung – Konzeption – Umsetzung – Betrieb – Optimierung
dainox GmbH, info@dainox.net, www.dainox.net

DATAGROUP M 23

DATAGROUP ist einer der führenden deutschen IT-Dienstleister und betreut für mittelständische und große Unternehmen sowie öffentliche Auftraggeber über 550.000 IT-Arbeitsplätze weltweit. Über 1.700 Mitarbeiter in ganz Deutschland konzipieren, implementieren und betreiben Business Applikationen und IT-Infrastrukturen.
Mit über 30 Jahren Erfahrungen in Defense & Security haben wir Expertenwissen zu Prozessen, IT-Systemen und –Architekturen der Bundeswehr, NATO und wehrtechnischen Industrie.
Unser Leistungsportfolio:
- DATAGROUP ILS Softwareprodukte
- Software-Entwicklung
- Betrieb von komplexen IT-Infrastrukturen
- Cybersicherheit
- Integrated Logistic Support und Analysis
- ASD-/ATA-Realisierungen
- Stammdaten-Management
- Prozessberatung
- Unterstützung von SAP ERP/ SASPF
- Business Intelligence und Big Data

www.datagroup.de

DEUTSCHE GESELLSCHAFT FÜR WEHRTECHNIK e.V. (DWT) F 54

Die DEUTSCHE GESELLSCHAFT FÜR WEHRTECHNIK e.V. wirkt als neutrale Dialog- und Informationsplattform für Fragen der Sicherheits- und Verteidigungspolitik, der Wehr- und Sicherheitstechnik sowie der Verteidigungswirtschaft.
Die DWT und ihre Tochtergesellschaft, die Studiengesellschaft der DWT mbH (SGW) führen Entscheidungsträger aus Politik, Wirtschaft, Industrie und Dienstleistungssektor, Bundeswehr / Bundeswehrverwaltung, anderen Behörden / Organisationen mit Sicherheitsaufgaben (BOS) sowie Wissenschaft, Forschung und Öffentlichkeit zusammen, um Ausrüstungs- und Ausstattungsfragen der Bundeswehr unter Berücksichtigung nationaler und internationaler Interessen und Rahmenbedingungen zu erörtern.
In der Fläche wird die DWT in zahlreichen regional wirkenden Sektionen und in Wehrtechnischen Arbeitskreisen tätig.

DeviceLock Europe GmbH F 22

DeviceLock ist seit über 20 Jahren internationaler Lösungsanbieter für Data Leak Prevention und unerlässlicher Bestandteil der IT-Sicherheit und -Compliance. Mit weltweiten Niederlassungen und über 1.000 Businesspartnern, bietet DeviceLock eine kundenorientierte und globale Vertriebs- und Supportstruktur. Als technologischer Spitzenreiter in der DLP schützt DeviceLock in über 80.000 Organisationen mehr als 7 Millionen Clients aus der Bank- & Finanzindustrie, der Pharma-Industrie, Regierungen, dem Militär sowie Industrie- und Handelskonzernen. DeviceLock ist ein Garant für eine innovative, vollumfängliche und gehärtete DLP-Solution, mit kürzesten Implementationszeiten bei geringen Anschaffungs- & Wartungskosten.
Kontakt: www.devicelock.de, +49 (0)2102 / 131840

Die Plusbringer GmbH F 52

Die Plusbringer GmbH hat sich, mit Ihren Partnerunternehmen, auf die Umsetzung von benutzerfreundliche Individual-Lösungen fokussiert. Unser besonderer Fokus liegt auf einem durchgängigen User Interface Design und anwenderorientierten USABILITY-Konzept. Wir entwickeln u.a. Anwendungen im Umfeld der Virtual- und Augmented-Reality, die wir auf der Messe auch live zeigen werden. Für eine effiziente Umsetzung verwenden wir moderne Technologien und Architekturen, die auf eine möglichst gute Wiederverwendbarkeit und Datenbankanbindung ausgerichtet sind. Gerne unterstützen wir Sie beim Erkunden neuer Wege.
Kontakt: Die Plusbringer GmbH, Kiefernweg 15, D-72581 Dettingen, Telefon: 07123 / 37410-50, Mail: info@dieplusbringer.de, www.dieplusbringer.de

DIGITTRADE GmbH F 49

Seit 2005 entwickelt und produziert die DIGITTRADE GmbH externe Festplatten und USB-Sticks mit Hardwareverschlüsselung, die Geschäfts- und Privatdaten sicher vor unbefugten Zugriffen schützen. Dazu zählt unter anderem die **externe High Security Festplatte HS256S,** welche durch ULD-Zertifizierung zur Speicherung personenbezogener Daten zugelassen ist. Die Festplatte HS256S3 befindet sich zudem in der Abschlussphase der BSI-Zertifizierung.
Die Kommunikations-Plattform Chiffry ist die neueste Entwicklung des Unternehmens mit dem Qualitätszeichen "IT Sicherheit made in Germany", die eine sichere und umfangreiche Kommunikation für Behörden und Unternehmen ermöglicht. Mit Chiffry können Anwender abhörsicher telefonieren und ihre Bilder, Videos, Kontakte sowie Sprach- und Textnachrichten vertraulich versenden.
Kontakt: www.digittrade.de, www.chiffry.de

DSI Datensicherheit GmbH B 01

"Data Security for Harsh Environments" ist der Maßstab unseres Handelns.
Unsere Kompetenz für Krypto- und Kommunikationslösungen stellen wir seit Jahren im Bereich Aerospace unter Beweis.
Die Erfahrungen aus der Satelliten- und Drohnentechnologie fließen in unsere Krypto- und Kommunikationslösungen ein, auch außerhalb des Aerospace Bereichs.
Krypto und TEMPEST gehören in vielen Projekten zusammen. Da DSI Datensicherheit GmbH beide Kernkompetenzen in einem Unternehmen vereint, realisieren wir Projekte von der Studie bis zur komplexen Hard- und Softwareentwicklung, inklusive Tempest Design und Tempest Tests.
Zu unseren Kunden gehören nationale und internationale Behörden und Unternehmen, die wir in Projekten wie z.B. Eurohawk, SARah und Galileo unterstützen.
Weitere Informationen unter: www.dsi-ds.de

ECOS Technology GmbH F 29

Die ECOS Technology GmbH hat sich auf die Entwicklung und den Vertrieb von IT-Lösungen für den sicheren Fernzugriff auf zentrale Daten und Anwendungen zur Gewährleistung eines erhöhten Schutz vor Spionage und Cyberangriffen bei gleichzeitiger Senkung der Kosten und einer Vereinfachung der Administration, spezialisiert.
Die Lösungen **ECOS SECURE BOOT STICK** und **ECOS SECURE BOOT MODUL** ermöglichen einen hochsicheren Fernzugriff auf Citrix, VMware Horizon oder Webanwendungen der Bundeswehr, von jedem beliebigen PC oder Mac aus.
Unsere Themenschwerpunkte auf der AFCEA 2017:
- Hochsicherer Remote-Zugriff (z.B. auf VS-NFD-Daten)

- Stärkung der Bundeswehr als attraktiver Arbeitgeber
- Remote Access in Weiterbildung und Schulung
- Einbindung von Reservisten in die IT-Infrastruktur
- Ortsunabhängiger Zugriff auf SASPF oder LoNo

EGL Elektronik Vertrieb GmbH — M 32

Ihr Partner für Abstrahlsicherheit.
Vielen Nutzern ist es nicht bekannt, dass bei einer Daten-Verarbeitung unweigerlich kompromittierende Abstrahlung direkt an der aktuell genutzten Hardware auftritt.
Diese Abstrahlung kann zur Wiederherstellung der Daten genutzt werden und somit zum Verlust der Vertraulichkeit der zu schützenden geheimen Information führen.
Mit geeigneten Abschirmmaßnahmen kann diese kompromittierende Abstrahlung auf ein nicht auswertbares Maß reduziert werden.
Auf diese Schirmung und Entstörung hat sich die Firma EGL Elektronik Vertrieb GmbH spezialisiert. Gerne stehen wir Ihnen für Fragen zur Verfügung.
Kontakt: Tel.: 06051 / 71838, E-Mail: info@eglgmbh.de

ELNO GmbH — B 02

Die ELNO GmbH ist Mitglied der internationalen Unternehmensgruppe ELNO bestehend aus mittelständischen Firmen in Frankreich, Italien und Deutschland.
Firmensitz ist Grünstadt in der Pfalz. Wehrtechnischer Umsatzanteil 90%.
ELNO ist Hersteller elektronischer Kommunikationsgeräte und -systeme und verfügt über:
- eine Entwicklungsabteilung mit moderner CAD/CAE Ausstattung
- langjährige Erfahrung in der Herstellung professioneller Elektronikprodukte
- langjährige Erfahrung als Lieferant für den öffentlichen Auftraggeber
- eigene Abteilung für Kundenschulungen
- ein Qualitäts-Management System ISO 9001:2000

Produkte
- Funktechnik: Handfunksprechgeräte, tragbare Funkgeräte, Fahrzeugfunkanlagen, professionelle und militärische Antennen
- Kommunikationstechnik: Neu: IP-basierende Intercom-Systeme für Ketten und Radfahrzeuge IP-basierende Feldtelefone auch für weite Entfernungen
- Audiotechnik: Handapparate, Kopfsprechsätze, Audiohelme für Piloten- und Fahrzeugbesatzungen

Kontakt: Kirchheimer Str. 49, D-67269 Grünstadt, Tel. +49 (0)6359 / 9463 643,
Fax +49 (0)6359 / 9439 817, s.eulenhofer@elno.fr, www.elno.fr

ESET Deutschland GmbH — B 14

ESET ist ein europäisches Unternehmen mit Hauptsitz in Bratislava (Slowakei). Seit 1987 entwickelt ESET preisgekrönte Sicherheits-Software, die bereits über 100 Millionen Benutzern hilft, sichere Technologien zu genießen. Das breite Portfolio an Sicherheitsprodukten deckt alle gängigen Plattformen ab und bietet Unternehmen und Verbrauchern weltweit die perfekte Balance zwischen Leistung und proaktivem Schutz. Das Unternehmen verfügt über ein globales Vertriebsnetz in über 180 Ländern und Niederlassungen in Jena, San Diego, Singapur und Buenos Aires. Für weitere Informationen besuchen Sie www.eset.de oder folgen uns auf LinkedIn, Facebook und Twitter.

ESG Elektroniksystem- und Logistik-GmbH — M 05

Die ESG ist eines der führenden System- und Softwarehäuser Deutschlands in den Bereichen Sicherheit und Verteidigung. Unsere langjährige Partnerschaft mit unseren Kunden aus Streitkräften, Behörden und Industrie zeichnet sich durch eine besondere Leidenschaft für Technik, Innovationskraft und -fähigkeit aus.
Wir präsentieren maßgeschneiderte verlegefähige und mobile Lösungen im Bereich Führungs- und Gefechtsstandsysteme, zur Verbesserung der Fähigkeiten der Bundeswehr in aktuellen und zukünftigen Einsätzen. Darüber hinaus können Sie sich bei uns einen Einblick über die nächste Generation von Führungsinformationssystemen verschaffen.
Als Highlight präsentieren wir Ihnen neben unserem Cyber/IT-Serviceportfolio das erste Cyber Simulation Center Deutschlands für Cyber Defence Training und Testing.
Kontakt: ESG Elektroniksystem- und Logistik-GmbH, Livry-Gargan-Str. 6, 82256 Fürstenfeldbruck, Tel. 089 / 9216-0, E-Mail: defenceandsecurity@esg.de, www.esg.de

Esri Deutschland GmbH — M 17

Esri ist Anbieter der ArcGISPlattform für alle Sicherheitsorgane. ArcGIS strukturiert Informationen über Raumbezug und visualisiert Ergebnisse und Zusammenhänge in 2D, 3D und 4D. Damit vernetzt die Technologie alle Beteiligten – vom Analysten bis zum Entscheider – mit einem einheitlichen, räumlichen Verständnis zur Operationsführung.
Kontakt: Esri Deutschland GmbH, Niederlassung Bonn, Rheinallee 24, 53173 Bonn,
Tel.: +49 (0)89 / 207 005 1720, E-Mail: info@bonn.esri.de, www.esri.de

FFG FLENSBURGER FAHRZEUGBAU GmbH — S 02

FFG – das junge Systemhaus
Durch die über fünfzigjährige Erfahrung als Instandsetzer für die Bundeswehr und Armeen befreundeter Nationen hat sich die FFG zum Upgrade-Spezialisten weiter entwickelt. Diese Aktivitäten führten u.a. zu umfangreichen Produktweiterentwicklungen, wie z.B. den NDV 1 und 2 für die deutschen M113 oder zu einer FFG-eigenen elektro-hydraulischen Steuerung für Leopard 1 Familienfahrzeuge. Innerhalb der letzten zehn Jahre investierte die FFG in Eigenentwicklungen und ist seitdem mit eigenen Fahrzeugsystemen am Markt vertreten. Sowohl der Protected Mission Module Carrier (PMMC) G5 als auch der WiSENT 2 sind hochgeschützte Fahrzeugplattformen, die dem Kunden durch ihre Modularität eine Vielzahl von Einsatzmöglichkeiten ermöglichen. FFG hat sich vom Instandsetzer über den Upgrade-Spezialisten konsequent zum Systemanbieter weiterentwickelt und ist dabei, sich als Systemhaus auf dem Weltmarkt zu etablieren.

Fraunhofer FKIE — M 27

Das Fraunhofer FKIE entwickelt Sicherheitslösungen in der Informations- und Kommunikationstechnologie. Bei der Forschungsarbeit für die Bundeswehr geht es um die Themen Führung, Aufklärung, Unterstützung und Schutz. Die "Analyse- und Testumgebung" ermöglicht die Simulation von FülInfoSys- und KomSys-übergreifenden Wirkketten in Echtzeit. Zentrale Elemente des taktischen Bereichs werden in Form virtueller Ressourcen bereitgestellt und im Verbund untersucht. Im Projekt "Testumgebung taktischer Router mit emulierten Anteilen" wurde auf Basis von OLSRv2 mit MTR-Erweiterungen ein Verbund unterschiedlicher Wellenformen in ein gemeinsames, durchgängiges ad-hoc-fähiges Netz integriert. Embedded Devices, wie Drucker oder IP-Kameras, bedeuten ein hohes Risiko für Unternehmensnetze. Das Exponat zeigt, wie leicht ein Drucker manipulierbar ist und stellt ein Framework zur automatisieren Firmware-Analyse vor.
Kontakt: www.fkie.fraunhofer.de

Fraunhofer IOSB — B 12

Das Geschäftsfeld Verteidigung ist das größte Geschäftsfeld des Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB). Es steht unter dem Leitthema **"Beratung und Technologie für die Verteidigung"** und entwickelt aus wehrtechnischer Grundlagenforschung Machbarkeitsstudien und Verfahren. Es bewertet Trends und Technologien, prüft und entwickelt Demonstratoren, unterstützt die Industrie und stellt innovative Ausrüstung her.
Kernkompetenzen sind die Erzeugung von Bildern und verwandten Sensorsignalen, die dazugehörige Signalverarbeitung und die Nutzung von Bildern in Systemen. Dabei konzentrieren wir uns auf die Bereiche Aufklärung, Navigation, Simulation, Satellitentechnik, land-, luft- und seegestützte Plattformen, Zielannäherung, Wirkung und Schutz, die Ausrüstung des Soldaten sowie Informationstechnologie.
www.iosb.fraunhofer.de/verteidigung

Auf dem griffity Gemeinschaftsstand — S 02

DigLT – Digitaler Lagetisch in der virtuellen Realität
Fraunhofer IOSB zeigt mehrere Beiträge zur Visualisierung von geodatenbasierter Lageinformation. Im Rahmen einer Ausstattung eines Einsatzfahrzeugs der Zukunft werden auf Stand **S02** Arbeitsplätze für den S3 "Operationsführung" und den S4 "Logistik" gezeigt. Ergänzt werden die Arbeitsplätze um einen Blickgesteuerten 360°-View aus dem inneren des Fahrzeugs für die sichere Umweltüberwachung.
Auf dem Stand **B12** zeigen wir zum Thema Lagevisualisierung eine Umsetzung derselben Software in VR.

FREQUENTIS Deutschland GmbH — B 09

Die Lösungen von Frequentis Defence greifen auf mehr als 60 Jahre Erfahrung im Bereich von ATM Lösungen zurück. 50 Jahre davon widmen sich direkt der militärischen Flugsicherung. Diese industrieübergreifende Erfahrung ermöglicht es, Lösungen zu entwickeln, die sich auf den Bereich Luft und See spezialisieren. Der Geschäftsbereich Defence baut auf diesem Wissen auf und entwickelt Lösungen für Kontrollzentralen in den Bereichen Land, See und Luft, um verbesserte Funktionalitäten zur Verfügung zu stellen, die missionskritische Kommunikation der Zukunft ermöglichen. Im Laufe der Zeit bietet die Ergänzung von verschlüsselten mobilen Übertragungen für Sprache und Daten ebenso wie situational awareness, eine missionskritische Unterstützung für die Anforderungen im Bereich der Luftverteidigung.
Kontakt: FREQUENTIS Deutschland GmbH,Team Bundeswehr, Graurheindorferstr. 159, 53117 Bonn, +49 (0)6103 / 300 86 54, team-bw@frequentis.com

GBS TEMPEST & Service GmbH — S 05

Die GBS GmbH, mit Sitz in Diepholz, betreibt ein vom BSI anerkanntes Abstrahlprüflabor. Für das Geschäftsfeld TEMPEST, verfügt die GBS GmbH über zwei firmeneigene TEMPEST-Labore.
Neben der Berechtigung zur Durchführung von Zonenkurzmessungen ist die GBS GmbH auch ein vom BSI anerkanntes Abstrahlprüflabor für Zulassungsmessungen nach SDIP 27 Level A, Level B und Level C (International) und dem Zonenmodell (National).
Kontakt: GBS TEMPEST & Service GmbH, von-Braun-Straße 6, D-49356 Diepholz,
Tel: +49 (0)5441 / 9758-100, Fax: +49 (0)5441 / 9758-129,
Homepage: http://www.gbs-tempest.de, E-Mail: info@gbs-tempest.de

Gebr. Friedrich Industrie- und Elektrotechnik GmbH — S 06

Die Gebr. Friedrich Industrie- und Elektrotechnik GmbH (GFE) ist seit vielen Jahren Rahmenvertragspartner des BAAINBw. Ganz egal ob es sich um die Einrüstung von Kabinen und geschützten Fahrzeugen oder um Instandsetzungsmaßnahmen handelt. In den Bereichen Kommunikationstechnik, IT oder Maschinenbau kämpft das Team der Gebr. Friedrich Industrie- und Elektrotechnik GmbH (GFE) an vorderster Front. GFE stellt sich den Forderungen der Bundeswehr und liefert einsatzfertige Systeme. Selbstverständlich werden dabei die strengen Maßstäbe der VG-Normen erfüllt. Auch ein weltweiter Einsatz ist für GFE selbstverständlich: Überall, wo Einheiten technische Hilfe benötigen, ist GFE vor Ort: auf Zypern genauso wie am Horn von Afrika.
Weitere Informationen: www.gfelektro.de

genua gmbH — M 15

Umfassende Lösung für VS-Datenkommunikation
Das deutsche IT-Sicherheitsunternehmen genua bietet eine umfassende

Komplettlösung für die VS-Datenkommunikation. Mobile Anwender, Home Offices und verteilte Standorte lassen sich über die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für VS-NfD zugelassene Kommunikationslösung einfach und sicher anbinden. Der Datenaustausch erfolgt über ein Virtual Private Network (VPN) via Internet oder WAN, die Identifizierung der Anwender komfortabel per Smartcard oder elektronischem Dienstausweis. Im Backend sorgen VPN- und Firewall-Systeme für hochwertige Sicherheit. Die Lösung kann einfach auf bestehende Infrastrukturen aufgesetzt werden.
Darüber hinaus bieten wir IT-Sicherheitslösungen für diese Aufgaben:
• Absicherung und Kontrolle hochsensibler Netzwerk-Schnittstellen
• Fernwartungs-Zugriffe in VS-NfD-Netze
Kontakt: genua gmbh, Domagkstraße 7, 85551 Kirchheim bei München
tel +49 (0)89 / 991950-0, www.genua.de

griffity defense GmbH S 02

griffity defense berät Unternehmen und öffentliche Auftraggeber bei der Lösung komplexer Herausforderungen in den Bereichen Verteidigung und Innerer Sicherheit. Zu unserem umfassenden Leistungsspektrum gehört zudem die Unterstützung bei der Geschäftsentwicklung und alle Services der Marketing-Kommunikation. Unser Fokus liegt auf der Erarbeitung von klaren, umfassenden, zukunftssicheren Strategien und Konzepten und deren abgeleiteten technischen Lösungen für unterschiedlichste Einsatzszenarien.

Leistungsangebot:
Analyse und Entwicklung von Szenaren um optimale technische Unterstützung eines Einsatzes oder einer Krisensituation zu erreichen und Defizite zu eliminieren Beratungsleistungen an der Schnittstelle zwischen Technologie und Anwendung mit dem Ziel, innovative und bezahlbare Lösungen für den täglichen Einsatz verfügbar zu machen Erarbeitung realisierungsfähiger Konzepte mittels industrieller Partner

Haivision Network Video GmbH F 28

Haivision bietet End-to-End Lösungen für die schnelle und sichere Übertragung von Video zusammen mit zeitkritischen Metadaten (KLV oder Sensorik-Daten) über verschiedene IP-Netzwerke oder Satellitenverbindungen.
Haivision Video Encoder/Decoder Produkte erfüllen NATO und MISB Standards (STANAG 4609) und werden bereits weltweit im Bereich C4ISR Ultra Low Latency Videoübertragung auf unterschiedlichsten Plattformen und Programmen erfolgreich eingesetzt.
Haivision ist ein globales Unternehmen mit Hauptsitz in Montreal / Kanada und in Chicago, sowie weiteren regionalen Niederlassungen Europa/Deutschland und in Asien. Haivision Produkte sind ITAR free und werden weltweit über zertifizierte Distributoren, Reseller und Systemintegratoren vertrieben.
Weitere Informationen finden Sie unter: www.haivision.eu / www.haivision.com

Hardhöhenkurier F 57

Der **Hardthöhenkurier** ist ein periodisch erscheinendes Magazin, das sich seit 33 Jahren mit aktueller Berichterstattung an Soldaten der Bundeswehr wendet und sich als Bindeglied zwischen der Bundeswehr, der wehrtechnischen Industrie und der Wirtschaft versteht. Der Hardthöhenkurier informiert über sicherheitspolitische Rahmenbedingungen, Einsätze der Bundeswehr, aktuelle Vorhaben der Streitkräfte sowie Neuerungen in der Wehrtechnik und der Rüstungsindustrie. Das Fachmagazin ist eine in Deutschland und in den europäischen Nachbarländern anerkannte Informationsquelle für Streitkräfte und Wehrtechnik.
Verlagsdirektion Bonn • Postanschrift: Borsigallee 12, 53125 Bonn,
Telefon: +49 (0)228 / 25900-344 • Telefax: +49 (0)228 / 25900-342,
E-Mail: redaktion@hardthoehenkurier.de • Internet: www.hardthoehenkurier.de

Harris B 04

Der Harris-Konzern liefert integrierte Lösungen für Verteidigung und Sicherheit weltweit und besteht aus den vier Geschäftsbereichen
Space and Intelligence Systems
Payload und Sensoren für Satelliten und Luftfahrzeuge, militärisches GPS, Erd- und Wetterbeobachtung, Prozessierung und Analyse von Fernerkundungs- und Geodaten,
Communication Systems
Netzwerke, Funk- und Satellitensysteme für Sprachkommunikation sowie Nachtsichtsysteme,
Electronic Systems
Elektronische Systeme, Radar- und Sonarsysteme, Flugsicherung, Kompositstrukturen für Luftfahrzeuge,
Critical Networks
Dienste für Flugverkehrsmanagement, Energie und maritime Kommunikation sowie Betrieb und Aufrechterhaltung von kritischen und ausfallsicheren IT-Systemen.
Informieren Sie sich auf unserem diesjährigen Stand auch speziell über
ENVI & SARscape
Lösungen für die Bildaufbereitung und -analyse (z. B. RGB, IR, SAR, LiDAR),
Jagwire
Vernetzte Systeme für Fernerkundungsdaten aller Sensoren (v. a. Video, WAMI),
Geiger-mode LiDAR
Sensorik, Datenprozessierung und Analytik für die großflächige und hochgenaue 3D-Topografieerfassung (Höhemodelle, Klassifikation, Objektextraktion).

HENSOLDT S 08

Premium-Sensoren für Verteidigung und Sicherheit
HENSOLDT ist ein weltweit führender Anbieter von Premium-Sensoren für Sicherungs-, und Überwachungsmissionen. Das Unternehmen ist Weltmarktführer u.a. bei Flugkörperwarnsystemen und U-Boot-Periskopen. Außerdem ist HENSOLDT stark auf dem Markt für Radare, Optronik und elektronische Schutzsysteme vertreten.
Das Unternehmen wurde gebildet aus den Verteidigungselektronik-Aktivitäten von Airbus, die 2016 aus dem Airbus-Konzern ausgegliedert wurden und jetzt zusammen mit der früheren Airbus DS Optronics unter dem Markennamen HENSOLDT als neues Sensorhaus an den Markt gehen.
Das Unternehmen fußt auf renommierten Vorgängerfirmen wie Telefunken, Dornier, Siemens Sicherungstechnik und Carl Zeiss Optronics. HENSOLDT erzielt derzeit mit etwa 4.000 Mitarbeitern einen Jahresumsatz von rund 1 Mrd. Euro.
Kontakt: Hensoldt, Willy- Messerschmitt Str. 1, 82024 Taufkirchen, Germany
E-Mail electronics_bordersecurity@airbus.com, Website www.detectandprotect.org

Hexagon Safety & Infrastructure – c/o Intergraph SG&I Deutschland GmbH F 15

Als internationaler Innovator in Sachen GIS- und Geo-Lösungen konzentriert sich Hexagon Safety & Infrastructure (eine Division von Intergraph) auf die Branchen Verteidigung und Nachrichtenwesen sowie Sicherheit, Rettung und Katastrophenschutz. Unsere Lösungen bereiten umfangreiche, komplexe Datenmengen in aussagekräftigen, graphischen Darstellungen auf. So sind zeit- und situationsgerechte Entscheidungen zum Schutz von Menschen und Infrastrukturen gewährleisten. Die komplette digitale Datenverarbeitung ist abgedeckt: Missionsplanung, Datenmanagement, Datenspeicherung, Datenprozessierung, Informationsverteilung und -auswertung.
Kontakt: Hexagon Safety & Infrastructure – c/o Intergraph SG&I Deutschland GmbH, Niederlassung Bonn, Koblenzer Str. 112, 53177 Bonn, Tel. +49 (0)228 / 3915-0, www.hexagonsafetyinfrastructure.com

Hitachi Data Systems GmbH M 14

Die Digitale Transformation erhöht durch besseres Datenmanagement die Kosteneffizienz, sorgt für schnellere Produkteinführungen und verbessert die Kundenerfahrung eines jeden Unternehmens. Niemand kennt sich besser mit Daten aus als Hitachi Data Systems. Wir helfen den weltweit größten Organisationen bei einer Sache – Daten. Unsere integrierte Strategie und unser Portfolio helfen Unternehmen ihre Daten zu verwalten, zu steuern, zu mobilisieren und zu analysieren, um Erkenntnisse darin zu finden, die zu besseren Resultaten führen. Hitachi Data Systems ist Ihr Partner für die Digitale Transformation – heute und in Zukunft.
Kontakt: Roger Rogacki, Enterprise Account Manager, Hitachi Data Systems GmbH

IABG mbH M 28

Die IABG arbeitet an Lösungen für eine sichere und zuverlässige Kommunikation und Lageführung in multinationalen Einsätzen. Hierbei beraten wir zu sicherer Kommunikation mit digitalen Endgeräten, dem Einsatz von Satellitenkommunikation und -navigation, den Herausforderungen bei der Kommunikation auf der letzten Meile sowie dem sicheren Zugriff auf Dienste.
Unter Verwendung innovativer Technologien rückt für uns das Thema Cyber Security zunehmend in den Mittelpunkt. Wir beschäftigen uns u.a. mit Ausbildungs- und Trainingskonzepten, Cyber-Härtung von Waffensystemen mittels Vulnerability Tests, Risikoanalysen sowie Detection & Response Mechanismen für Cyberangriffe. Darüber hinaus unterstützen wir bei der Erstellung und Weiterentwicklung von IT-Sicherheitskonzepten auf Basis der neuen zentralen Dienstvorschrift A-960/1.

IBM Deutschland GmbH M 09

IBM ist einer der weltweit größten Anbieter von Informationstechnologie. Das Lösungsportfolio reicht vom Supercomputer über Software und Beratungsleistungen bis hin zur Erarbeitung komplexer Anwendungslösungen sowie Outsourcing.
Mit hohen Investitionen in Forschung und Entwicklung adressiert IBM die Wachstumsinitiativen Business Analytics, Cloud Computing, Mobile Enterprise, Social Computing und Security.
Der kognitiven Erschließung komplexer und großer Datenmengen trägt IBM Rechnung durch den neuen **Geschäftsbereichs Watson IoT, der gemeinsam mit dem ersten europäische Watson Innovation Center in München seine Zentrale hat.**
Kontakt: IBM Deutschland GmbH, Godesberger Allee 127, D-53175 Bonn
Klaus Lilge, klaus_lilge@de.ibm.com, Mobile: +49 (0)175 / 581 38 42

IHS Markit (Jane's) S 07

With a legacy of over 100 years, Jane's delivers the world's leading defence and security insight to help you make critical decisions. Our renowned open-source intelligence and powerful analytical tools encompass data on equipment, technology, parts, standards and logistics, as well as objective analysis of markets, programmes and budgets, risk and capabilities assessments, training and consulting services. Government, military and defense organizations gain insight into, plan for and act upon critical threats in the current global national-security environment. Businesses leverage tools and resources for more cost-effective defense-system design, delivery and support.
Over 3000 thought leaders provide you with actionable intelligence for expedited and improved decision making. Customers, prospects and the media outlets alike rely upon Jane's thought leaders for analysis, forecasts, and perspectives on topics, events, and issues that impact the global business landscape.

Indra Sistemas S.A. S 11

Indra Sistemas S.A. ist der führende Spanische Elektronik Konzern, der sich in den letzten 30 Jahren zu einer multinationalen welt-weit operierenden Verteidigungs- und Sicherheitstechnologie-Firma entwickelt hat. Im Sicherheits- und Verteidigungsbe-

reich unterstütz Indra u.a. Anwendungen in den Bereichen Grenzschutz, Schutz kritischer Infrastrukturen, Krisenmanagement, Interoperabilität verschiedener Einsatzkräfte auf allen Ebenen. Die wichtigsten Technologien in diesem Bereich sind Simulationsumgebungen, Radarsysteme, Wissensmanagement und Flex IT/Cloud Lösungen.
Kontakt: Thomas Mattick, Programm Manager Bundeswehr, Bahnhofplatz 1, 88045 Friedrichshafen, Telefon: +49 (0)7541 / 282-0, www.avitech.aero

INFODAS GmbH — M 19

Die **INFODAS** ist seit 1974 als unabhängiges und herstellerneutrales Software- und Beratungsunternehmen ein verlässlicher Partner der Bundeswehr.
Kernkompetenzen sind:

- SDoT Security Gateway, bidirektionale Netzkopplung unterschiedlicher Informationsräume/Sicherheitsdomänen
- SDoT Diode, hochsichere High-Speed-Datenübertragung von LOW- auf HIGH-Netzwerke
- SDoT Labelling Service, Kennzeichnung und Auswertung von Security Labeln
- SDoT SIS & SD, elektronische VS-Registratur zur vorschriftenkonformen Bearbeitung und Verwaltung von digitalen Verschlusssachen
- SAVe, IT-Sicherheitsdatenbank mit integrierten Sicherheitsvorgaben ZDv A-960/1
- PATCH.works, Patch-Managementsystem für geschlossene IT-Systeme der Bw
- Informationssicherheitsberatung und Erstellung von IT-Sicherheitskonzepten
- Projekt-, Anforderungs-, Nutzungs-, Konfigurations-, Qualitätsmanagement sowie weitere Beratungsleistungen und Analysen für den öAG

www.infodas.de – vertrieb@infodas.de

"IT-Standort Bonn" — F 04

Bonn gehört zu den wichtigsten IT-Standorten in Europa. Die Europäische Kommission hat in einer europaweiten Studie die wichtigsten Zentren der IT-Wirtschaft analysieren lassen (European Poeles of ICT Excellence EIPE). Bonn liegt im europäischen Standortwettbewerb auf Rang 12 von 1300 Regionen in Europa. Besondere Stärken sind hier die lokale Wissenschaft und die bestehenden Wirtschaftsunternehmen am Standort Bonn. Die Schwerpunktsetzung liegt in den Bereichen Geoinformatik, IT für Gesundheit und Ernährung, sowie im Bereich der Cybersicherheit
Kontakt: Thomas Poggenpohl
Amt für Wirtschaftförderung, Liegenschaften und Tourismus
Besucher: Loggia am Stadthaus, Thomas-Mann-Straße 4, 53111 Bonn
Postanschrift: Bundesstadt Bonn, 53103 Bonn
Tel.: +49 (0)228 / 77 57 88, Fax: +49 (0)228 / 77 20 34 ,
email: thomas.poggenphl@bonn.de

itWatch GmbH — F 26 + F 05

itWatch steht für innovative IT-Sicherheit "made in Germany" mit Fokus auf Endgeräte-Sicherheit, Data Loss Prevention, Verschlüsselung und Kostenreduktion des IT-Betriebs. Im Public Sector und der Inneren Sicherheit bieten die patentierten **itWatch**-Lösungen durch ihre weltweiten Alleinstellungsmerkmale viele Vorteile. Die hohen Anforderungen von Nachrichtendienst, Militär (Einsatz bis GEHEIM und NATO-restricted) und Polizei werden ebenso erfüllt, wie solche von Spezialinstallationen. Einzelinstallationen mit weit über 140.000 Lizenzen beweisen die Stabilität und Effizienz. Alle Produkte werden ohne Zukauf im Haus der itWatch in Deutschland frei von Hintertüren hergestellt.
Als Innovationen präsentiert itWatch die Produkte "itWash" – Datenschleuse mit Datenwäsche – und "Private Data Room" – sicherer Datenraum als vollständige daten- und nutzerzentrierte Vertrauenskette für den gesamten Lebenszyklus sensibler Daten und Services. Ein Schwerpunkt liegt auf dem seit einigen Jahren angebotenen sicheren mobilen Arbeitsplatz, z.B. als kosteneffizienter Heimarbeitsplatz.
Kontakt: itWatch GmbH, Aschauer Straße 30, 81549 München,
Tel.: 089 / 620 301 00, Fax: 089 / 620 301 069, info@itwatch.de, www.itwatch.de

JK Defence & Security Products GmbH — F 41

Die JK DEFENCE & SECURITY PRODUCTS GMBH steht seit über 20 Jahren für Qualität und Zuverlässigkeit im Bundeswehrgeschäft. Lag in der ersten Dekade der Schwerpunkt in der Beschaffung ausländischer Luftfahrzeugteile für die deutsche Luftwaffe, beschäftigen wir uns heute auch mit der Beschaffung und Integration von militärischen Funksystemen.
Als Deutschland-Vertretung von **Harris RF,** dem größten Hersteller von militärischen Funkgeräten, bieten wir die komplette Bandbreite von portablen und stationären Funk- und Aufklärungsgeräten an. Ob als Hand-Held oder Man-Pack, modular oder fest eingebaut in gepanzerten Fahrzeugen, Booten oder Schiffen: Wir haben immer eine hauseigene Lösung für Kommunikation und Aufklärung.
Zum Beispiel das Software Defined Radio PRC-117/G, welches bestehende und zukünftige Wellenformen in einem Frequenzbereich von 30MHz bis 2GHz abdecken kann.
Kontakt: JK Defence & Security Products GmbH / Industriering Ost 74 / 47906 Kempen / www.jkdefence.de / info@jkdefence.de

Kongsberg Defence & Aerospace — F 51

KONGSBERG is an international technology corporation based in Norway that supplies reliable, advanced technological solutions that improve the reliability, safety and efficiency of complex operations and under extreme conditions. KONGSBERG delivers defense systems for Air Defence, remote weapon systems, missiles, surveillance and communications.
KONGSBERG is the supplier of K-TaCS. K-TaCS comprises of tactical radio relays (Richtfunk), routers and VHF/UHF radios for Army and Air Defence networks. High data capacities are combined with advanced ECCM capabilities and embedded encryption.
The radio relays operates in NATO band 3 and 4 and are known for ease of use. The VHF radio family has superior range and coverage capabilities, especially in difficult terrain with severe multi-paths. The high capacity UHF radio family supports up to 2.5 Mbps data on the move combined with transfer of voice. These radios are optimized for use in advanced sensor systems.
The KONGSBERG equipment is Ruggedized by Design. www.ktacs.com

Lachen helfen — B 16

Im ehemaligen Jugoslawien beschlossen Bundeswehrsoldaten Mitte der 90er Jahre, sich neben ihren dienstlichen Aufgaben auch privat für humanitäre Projekte zugunsten von Kindern zu engagieren. Um den traumatisierten, verwundeten oder elternlosen Kindern dauerhaft, schnell und unbürokratisch zu helfen, gründeten sie 1998 einen gemeinnützigen Verein. Die gute Zusammenarbeit mit der Polizei führte 2009 zu dem Entschluss, sie in den Verein zu integrieren. Seitdem ist Lachen Helfen e.V. die **"Initiative deutscher Soldaten und Polizisten für Kinder in Kriegs- und Krisengebieten".** Seit dem Jahre 2001 sind wir nach wie vor in Afghanistan und auf dem Balkan tätig. Momentan werden jedoch insbesondere im **Irak,** in **Mali,** im **Südsudan,** in **Somalia,** in der **Ukraine** und seit kurzem auch in **Syrien** Hilfsprojekte erkundet.

Luciad — S 07

Luciad ist Anbieter von Softwarelösungen zur räumlichen Lagebilddarstellung von Geoinformationen für Anwendungen in missionskritischen Systemen. Luciad Softwarekomponenten bieten eine effiziente und visuelle Datenanalyse, die es ermöglicht, Echtzeit-Lagebilder zu erstellen und damit die Grundlage für Geoinformationssysteme der nächsten Generation zu schaffen.
Von militärisch genutzten Command and Control Systemen bis hin zur Schaffung von digitaler Infrastruktur für Smart Cities helfen Luciad Softwarekomponenten eine intuitive Lagebilddarstellung zu generieren. Weltweit verlassen sich Kunden auf leistungsstarke Visualisierungslösungen aus dem Hause Luciad.
Unser Motto lautet: "Connect, visualize, analyze, act".

Matrox Electronic Systems GmbH — F 51

Matrox Graphics ist ein globaler Hersteller zuverlässiger und hochwertiger ASICs, Boards, Appliances und Software. Unterstützt durch die firmeneigene Design-Expertise und einen dedizierten technischen Support liefern Produkte von Matrox unvergleichliche Leistung bei Quellen-Erfassung, KVM-Extension, der Distribution von Videodaten und bei Multi-Display-Anordnungen aller Art. Matrox entwickelt seit 1976 hoch-qualitative Produkte, deren Technologie von Experten und Partnern auf der ganzen Welt vertraut wird.
Durch jahrzehntelange Erfahrung bei der Entwicklung und Bereitstellung zuverlässiger und hochwertiger AV- und IT-Produkte besitzt Matrox alles für ihre effiziente IT- und AV-Infrastruktur im missionskritischen Umfeld. Matrox ist ein privat geführtes Unternehmen mit Sitz im kanadischen Montreal.
Kontakt: Joerg.Langeheine@matrox.com – +49 (0)89 / 621 70-446

Media Broadcast Satellite GmbH — F 27

MB Satellite realisiert über seine Erdfunkstelle in Usingen satellitenbasierte, weltweite Zuführungs- und Verteilnetze. Für Unternehmen im privaten und behördlichen Sektor realisieren wir Lösungen zur IT-Vernetzung, Sprachkommunikation sowie Transport breitbandiger Video/Mediensignale in Echtzeit via Satellit. Die Übermittlung von Informationen aller Art über Satellit ist immer dann vorteilhaft wenn entlegene Standorte mit einer unzureichenden terrestrischen Netzinfrastruktur erreicht werden müssen. Für solche Anforderungen bieten wir zuverlässige und gesicherte Ein- und Zwei-Wege-Kommunikationslösungen, die für alle Branchen und Institutionen individuell konfiguriert werden können. Durch die zentrale Lage des Teleports können Daten jeglicher Art von und nach Europa, Asien und weiteren Kontinenten empfangen und verteilt werden.
Weitere Informationen finden Sie unter www.media-broadcast.com/satellite oder kontaktieren Sie gerne auch Herrn Manfred Rupp per Email: manfred.rupp@media-broadcast.com

Microsoft Deutschland GmbH — F 08

Die Leistungsfähigkeit moderner Streitkräfte hängt von erfolgreicher Interoperabilität ab. Auf technischer Seite steht dabei die nahtlose Zusammenarbeit von IT-Systemen und Geräten, wie Hololens oder Surface, im Fokus. Insbesondere wenn verschiedene Einheiten oder internationale Koalitionen Informationen austauschen müssen, ohne die Informationssicherheit zu gefährden. Microsoft unterstützt Sie mit einer hochintegrativen Plattform bei diesen Herausforderungen. Mit SharePoint für Zusammenarbeit und Skype for Business für die vereinheitlichte Echtzeitkommunikation wird eine flexible, zeitgemäße Zusammenarbeit ermöglicht. Mit der Microsoft Cloud für Deutschland bietet Microsoft diese Dienste auch aus Rechenzentren in Deutschland an – mit T-Systems als Datentreuhänder für Ihre Daten.

Mittler Report Verlag GmbH — F 56

Der Mittler Report Verlag gilt als führender Fachverlag für Sicherheitspolitik, Streitkräfte, Wehrtechnik, Rüstung, IT und Logistik im deutschsprachigen Raum. Das Portfolio umfasst Zeitschriften, Broschüren, Informationsdienste und Fachtagungen. Dazu zählen die in vertraglich geregelter Zusammenarbeit mit dem Bundesministerium der Verteidigung herausgegebene Monatszeitschrift "Europäische Sicherheit & Technik", die neunmal jährlich erscheinende internationale Fachzeitschrift "European Security and Defence", die Fachzeitschrift "MarineForum", die Broschürenreihen "Wehrtechnischer Report" und "Sicherheitstechnischer Report" sowie die Online-Newsletter "ESD Spotlight" und "Wehrwirtschaft". Da-

neben gelten die jährlich stattfindende Sicherheitspolitische und Wehrtechnische Tagung in Bonn sowie die NATO LCM Conference in Brüssel als etablierte Foren für den Informationsaustausch unter Experten und Entscheidungsträgern.
www.mittler-report.de

ML Gruppe B 13

Die ML Gruppe ist ein führender Fullservice-Dienstleister für individuelle Trainingsprojekte und gezieltes Consulting. Als Spezialisten für moderne, kompetente Wissensvermittlung unterstützen wir unsere Kunden zukunftssicher insbesondere im Bereich Digitalisierung. Die ML ist seit Jahren in großen Bundeswehrprojekten aktiv, wie

- im Rahmenvertrag IT-Ausbildung der Bw,
- an der Führungsunterstützungsschule
- im Projekt SASPF im Integrierten Fach- und Ausbilderzentrum
- bei der Informationssicherheits-Sensibilisierungskampagne "PIA"

und unterstützt dabei auch mit Modernen Ausbildungstechnologien/E-Learnings. Mit der Studie "Kompetenzorientierte Aus-, Fort- und Weiterbildung in der Bundeswehr" hat ML ihre Expertise als Berater und Dienstleister für Transformationsprozesse zur Kompetenzorientierung auch bei der Bw eingebracht.
Kontakt: ML Gruppe, Peter Brandt, Max-Planck-Str. 39, D-50858 Köln,
Tel.: 02234 / 9203-112, www.mlgruppe.de, info@mlgruppe.de

MÖNCH Verlagsges. mbH F 55

Die MÖNCH Gruppe ist einer der weltweit führenden Zeitschriftenverlage in den Bereichen Verteidigung und Sicherheit. Die Zeitschriften erscheinen auf deutsch, englisch, arabisch, spanisch und auf italienisch.
Dazu gehören:

- Wehrtechnik (Deutsch): Erscheinungsweise zweimonatlich für Leser in Deutschland, Österreich und in der Schweiz.
- Military Technology (Englisch): erscheint monatlich
- Naval Forces (Englisch): Erscheinungsweise zweimonatlich
- Safety & Security International (Englisch): Erscheinungsweise zweimonatlich.
- Handbuch der Bundeswehr (Deutsch)

Darüber hinaus werden ca. 250 Buchtitel im Segment Verteidigung, Technologie, Politik und Geschichte seit vielen Jahren durch Bernard & Grafe verlegt
Kontakt: Herr Christian Lauterer, MÖNCH Verlagsges.mbH, Christine-Demmer-Str. 7,
53474 Bad Neuenahr-Ahrweiler, Tel.: 02641 / 3703-0,
e-mail: info@moench-group.com, www.monch.com

Motorola Solutions F 23

Motorola Solutions bietet innovative sicherheitskritische Kommunikationslösungen und -services für Streitkräfte, Behörden und Organisationen mit Sicherheitsaufgaben sowie Unternehmen. Die zukunftsweisenden und hochverfügbaren Lösungen ermöglichen Anwendern eine zuverlässige Kommunikation. Das Angebot reicht von Endgeräten und Infrastruktur bis hin zu Software und Services für Militär, Polizei, Feuerwehr, Rettungsdienste, Bundesbehörden sowie Energie- und Versorgungsunternehmen, Fertigung, Transport und Logistik, Gastgewerbe, Einzelhandel und Bildungsinstitute.
Der Hauptsitz der Motorola Solutions, Inc. befindet sich in Chicago, USA. In Deutschland ist die Motorola Solutions durch die Motorola Solutions Germany GmbH mit Sitz in Idstein präsent. Weitere Niederlassungen sind in Alsdorf und Berlin, wo sich das weltweite Motorola Solutions Kompetenzzentrum für den TETRA-Digitalfunk befindet. Weitere Informationen unter www.motorolasolutions.de sowie auf Twitter unter @MotSolsDE oder in der Motorola Solutions LinkedIn-Community.

MSAB S 12

MSAB ist globaler Marktführer in forensischer Technologie für die Untersuchung von Mobilgeräten. Mit den Mobilgeräteforensik-Tools – XRY Office, Field Version, Kiosk, Tablet, XRY PinPoint und XAMN – können Benutzer Daten aus unterschiedlichsten Mobilgeräten extrahieren, vergleichen, analysieren und protokollieren. MSAB-Schulungen optimieren Ihr Wissen in Theorie und Praxis von der Datenextraktion bis zum Beweisvortrag vor Gericht. Hervorragender technischer Support vervollständigt das Lösungspaket.
Zu den Kunden von MSAB zählen Strafverfolgungsbehörden, Militär und Nachrichtendienste. Neben seinem Hauptsitz in Stockholm, Schweden, unterhält MSAB Tochtergesellschaften in Großbritannien, Kanada, USA, Australien und China. MSAB beschäftigt Vertriebsmitarbeiter und ein Distributoren-Netzwerk rund um den Globus.
Weitere Informationen erhalten Sie unter www.msab.com

ND SatCom GmbH F 06

Mit mehr als 30 Jahren Erfahrung im Bereich Satellitenkommunikation ist ND SatCom der weltweit führende Lieferant von satellitenbasierten Kommunikationssystemen und Bodenstationen, um Kunden mit kritischen Operationen überall auf der Welt zu unterstützen.
Kunden in mehr als 130 Ländern haben sich für ND SatCom als eine zuverlässige Quelle für qualitativ hochwertige und sichere Lösungen, die schlüsselfertige und maßgeschneiderte Systeme beinhalten, entschieden. Die innovativen Technologien des Unternehmens werden weltweit von Regierungen, dem Militär sowie in den Bereichen Fernseh- und Rundfunkübertragung, der Telekommunikation und von Unternehmen eingesetzt.
Das Kernprodukt SKYWAN ermöglicht Tausenden von Nutzern täglich, eine sichere, zuverlässige und schnelle Kommunikation.
Kontakt: ND SatCom GmbH, Graf-von-Soden-Strasse, D-88090 Immenstaad,
Tel: +49 (0)7545 / 939 0, Fax: +49 (0)7545 / 939 8702, Email: info@ndsatcom.com.
Kontaktperson: Frau Arzu Evlek, Specialist Marketing & Communications,
Tel.: +49 (0)7545 / 939 8751, Mobil: +49 (0)170 / 563 8349, Arzu.Evlek@ndsatcom.com

NYNEX satellite OHG F 27

Die NYNEX satellite OHG ist einer der führenden Integratoren von satellitenbasierenden Datenverbindungen für die Regionen EMEA. Die NYNEX satellite OHG verfügt über eigene HUB-Infrastruktur sowie Satellitensegment – somit ist ein unabhängiger und techniknaher Support, ein individuelles Consulting sowie professionelle Integration bezüglich der Themengebiete RF und IP möglich.
Die NYNEX satellite OHG betreibt Satellitennetzwerke zur Datenkommunikation seit 2000 von Darmstadt aus und verfügt über ein weltweites Partner- und Installateurnetzwerk. In den vergangenen 17 Jahren haben wir umfangreiche Erfahrungen bei der Implementierung von internationalen Sattelitennetzwerken im Bereich Ministerien, Behörden und Institutionen gesammelt.
Weitere Informationen: www.nynex.de.
Professional Satellite Services made in Germany!

OHB System AG F 01

Die OHB System AG ist eines der drei führenden Raumfahrtunternehmen Europas. Der Systemanbieter gehört zum börsennotierten Hochtechnologiekonzern OHB SE, in dem rund 2.200 Fachkräfte und System-Ingenieure an zentralen europäischen Raumfahrtprogrammen arbeiten. Mit zwei starken Standorten in Bremen und Oberpfaffenhofen bei München und 35 Jahren Erfahrung ist die OHB System AG spezialisiert auf High-Tech-Lösungen für die Raumfahrt. Dazu zählen erdnahe und geostationäre Satelliten für Erdbeobachtung, Navigation, Telekommunikation, Wissenschaft und Exploration des Weltraums ebenso wie Systeme für die Astronautische Raumfahrt, Luftaufklärung und Prozessleittechnik.
Mehr über das Unternehmen und aktuelle Projekte erfahren Sie unter www.ohb-system.de

ORACLE Deutschland B.V. & Co. KG F 11

Für mehr als 400.000 Kunden – darunter alle Fortune 100 Unternehmen – und in allen vertikalen Märkten in mehr als 145 Ländern bietet Oracle ein umfassendes und komplett integriertes Set an Cloud-Anwendungen, Plattform Services und Engineered Systems. Da alle Oracle Produkte für den traditionellen On-Premise Einsatz und für Private, Public oder Oracle Cloud@Customer identisch sind, wird es den Kunden ermöglicht, das jeweils geeignete Cloud Modell zu wählen. Bei der Bundeswehr haben sich Oracle Produkte seit vielen Jahren als robuste und zuverlässige Grundlage für Datenmanagement bei einsatzkritischen Systemen bewährt.
Mehr Informationen hier: https://www.oracle.com/de/corporate/features/oeffentlicher-sektor/index.html

Panasonic Computer Product Solutions F 02

Panasonic Computer Product Solutions (CPS) bietet Unternehmen und Behörden besonders robuste, energieeffiziente und extrem zuverlässige mobile Computing-Lösungen für IT-feindliche Bedingungen. Von robusten Outdoor-Notebooks und TOUGHBOOK Business Laptops bis hin zu TOUGHPAD-Tablets sowie zahlreiche Serviceleistungen und Zubehör für optimale Bedienung. Mit 30 Jahren Erfahrung auf diesem Gebiet und dem diesjährigen 20-jährigen Jubiläum der Marke TOUGHBOOK ist Panasonic Marktführer am europäischen Markt für robuste Notebooks (VDC Research, März 2016).

- "Full-Ruggedized" Schutz gemäß aller notwendigen Standards unter anderem IP65- und teils IP68-Zertifizierung sowie Militär-Standards (MIL-STD 810G, MIL-STD 461F) ,
- ergonomische Formfaktoren und geringes Gewicht,
- leuchtstarke Outdoor-Displays für ideale Ablesbarkeit auch unter Sonnenlicht sowie
- äußerst lange Akklaufzeiten und Hot-Swap Funktionen für unterbrechungsfreien 24-Stunden-Einsatz

Kontakt: www.toughbook.de/kontakt oder Tel. +49 611 1252

Peli Hardigg S 01

Peli-Hardigg is World's largest manufacturer of Military, Aerospace and Security approved reusable plastic containers. During AFCEA, Peli-Hardigg™ will present its rotomoulded protection solutions, (Mobile Armoury, Mobile IT, Mobile Medical), XL shipping containers and 19" rack-mount Cases.
Since 1976, Peli-Hardigg engineers have proudly developed custom solutions for the transport and packaging needs for the military market. Our innovative products enable sensitive equipment to travel through hostile environments and arrive operational. By developing custom solutions and continuously improving designs, we have been able to build a robust line of products that proudly live up to the harsh demands of the military.
Kontakt: www.peli.com / info@peli.com

PlaceWorkers GmbH F 52

Wir helfen Ihnen auf dem Weg in die Mobile Zukunft. Wir entwickeln sowohl Applikationen in FIORI als auch für die Plattformen iOS, ANDROID oder WINDOWS. Die mobilen Anwendungen unterstützen Online- und Offlinefähigkeit sowie die Integration in bestehende operative Anwendungen bzw. die SAP- Kundenumgebung. Gerne entwickeln wir auf der SAP-Entwicklungsumgebung Ihre mobilen Softwarelösungen. Wir haben über 15 Jahre Erfahrung und unsere Expertise umfasst gleichfalls Konzepte der Testgetriebenen Entwicklung sowie Methoden der effizienten Erweiterbarkeit mobiler Anwendungen.
Kontakt: PlaceWorkers GmbH, Moritz-Hensoldt-Strasse 32, D-35576 Wetzlar contact@placeworkers.com, Tel: 06441 / 44 50 03-0, www.placeworkers.com

promegis GmbH B 08

Als Spezialist für Geoinformatik, Geoinformationssysteme, Bildverarbeitung, Bildauswertung, Softwareentwicklung und IT-Servicedienstleistungen entwickelt unser Unternehmen Anwendungen und fachspezifische Systemlösungen für die Bereiche der öffentlichen Verwaltung, der Behörden und Organisationen mit Sicherheitsaufgaben (BOS), des militärischen Nachrichtenwesens (MilNW) und der militärischen Aufklärung sowie der Energie- und Versorgungswirtschaft. Darüber hinaus unterstützen wir unsere Kunden bei der Umsetzung umfangreicher IT-Projekte.
Die promegis setzt auf innovative und gleichzeitig zukunftssichere Lösungen und steht Ihnen mit langjähriger Erfahrung bei der Realisierung komplexer, integrationsfähiger Systemlösungen zur Seite. Als deutscher Vertriebs- und Entwicklungspartner der Firma Textron Systems bieten wir Ihnen die volle Bandbreite der High-End GIS und Image Analysis Lösungen.
Weitere Informationen finden Sie unter www.promegis.de.
Kontakt: Klaus Scholle, Tel. +49 (0)5422 / 9629-0, E-Mail: klaus.scholle@promegis.de

PWA Electronic Service- und Vertriebs- GmbH F 02

PWA – Ihr Spezialist für Beratung, Vertrieb, Service und Support von gehärteten Notebooks, Komponenten und Peripherie für mobile Anwendungen. Inzwischen blicken wir gemeinsam mit Panasonic Computer Product Solutions auf eine Erfahrung von mehr als 20 Jahren zurück. Wir bieten für die Panasonic Toughbooks und Toughpads das komplette Sortiment an Unterstützung an: Neugeräte, Zubehör, Restposten, Ersatzteile, Service und Support. Seit September 2007 sind wir außerdem exklusiver Panasonic Service-Partner für Deutschland und Österreich.
Zusammen mit unserem Partner Panasonic Computer Product Solutions (CPS) zeigen wir auf der diesjährigen AFCEA die aktuellsten Mobile Computing Geräte von Panasonic Toughbook und Toughpad live vor Ort.
Weitere Informationen finden Sie auf unserer Homepage: www.pwa-electronic.de

Rafael Advanced Defense Systems Ltd. F 45

Rafael Advanced Defense Systems Ltd. konstruiert, entwickelt, produziert und liefert eine breite Palette von Hightech-Abwehrsystemen für Luft-, Land-, See-, Weltraum- und Cyber-Anwendungen für Kunden auf der ganzen Welt. Das Unternehmen bietet seinen Kunden innovative Lösungen auf dem neuesten Stand der Technik. Diese Systeme basieren auf umfangreicher Erfahrung, technologischem Know-how und einem gründlichen Verständnis der spezifischen Anforderungen.
Rafaels Bodenkommunikationslösungen für die mobile taktische Kommunikation sind auf dem neuesten Stand der Technik und umfassen VHF/UHF-Software-Defined-Radios, Satcom-on-the-move-Terminals, taktische Funksysteme, taktische Router für mobile Kommunikationsknoten und C2-Anwendungen.
Kontakt: c4isr_mkt@rafael.co.il or Intr-mkt@rafael.co.il, Internet: www.rafael.co.il

Rheinmetall Defence M 02

Die börsennotierte Rheinmetall AG ist ein weltweit agierender Hochtechnologiekonzern, der sich den Zukunftsthemen Sicherheit und Mobilität verschrieben hat. Das Unternehmen gliedert sich in zwei operative Unternehmensbereiche: Rheinmetall Defence und Rheinmetall Automotive. Mit rund 23.000 Mitarbeitern erwirtschaftet der Konzern einen Jahresumsatz von rund 5,6 MrdEUR.
Der Unternehmensbereich Defence deckt mit seinen drei Divisions Weapon and Munition, Vehicle Systems sowie Electronic Solutions als einer der führenden Anbieter weltweit das gesamte Fähigkeitsspektrum von Streit- und Sicherheitskräften ab: Mobilität, Aufklärung, Führung, Wirkung und Schutz. Eine der Stärken Rheinmetalls ist es, als Generalunternehmer System- und umfassende System-of-systems-Lösungen anzubieten. Dabei kooperiert das Unternehmen eng mit industriellen Partnern im In- und Ausland.
Rheinmetall sieht es als seine Verpflichtung, den Streit- und Sicherheitskräften sowohl in Deutschland wie auch in den internationalen Partnerländern zur Seite zu stehen und ihnen die bestmögliche Ausrüstung zur Verfügung zu stellen.

Rheinmetall Technical Publications GmbH S 09

Als zertifiziertes luftfahrttechnisches Unternehmen für Entwicklung, Herstellung und Instandhaltung ist die Rheinmetall Technical Publications GmbH Ihr kompetenter Partner.
Das dürfen Sie von uns erwarten:

- Unterstützung im Lebenszyklus Ihres Produktes, von der Definition über die Entwicklung, Herstellung hin zur Nutzung bis zur Aussonderung,
- Instandhaltung von Luftfahrtgeräten,
- Nutzungsbetreuung vollständiger Systeme,
- Erstellung von Interaktiven Elektronischen Technischen Dokumentationen (IETD),
- Obsoleszenz-Management,
- Logistische Analysen und Berechnungen,
- Ausbildungskonzepte und deren Durchführung.

Unsere Leistungen sind individuell auf Ihre Bedürfnisse ausgerichtet und erfüllen alle gängigen nationalen und internationalen Standards.
Alles aus einer Hand

Rockwell Collins Deutschland B 03

Rockwell Collins Deutschland, mit Firmensitz in Heidelberg, beschäftigt ca. 400 Mitarbeiter. Unsere Kernkompetenzen, aufbauend auf einer 50-jährigen Erfahrung, liegen in Entwicklung, Herstellung, Systemintegration, Vertrieb, Wartung und Instandhaltung von Kommunikations- und Navigationsgeräten, sowie Flugregel- und Wetterradarsystemen, Missionsrechnern und Ausrüstung für militärische und zivile Anwendungen.
Unsere Aktivitäten umfassen unter anderem:

- Avionik-Subsystem Integration
- Geräte und Systemlösungen für UAS/UAV
- Taktische Datenlink-Übertragungssysteme
- Funkgeräte für Luft- und Bodenanwendungen u. a. mit modernster SDR-Technologie
- Militärische Navigationssysteme für Schiffe und Fahrzeuge
- Modulare Rechnersysteme für militärische Anwendungen
- Entwicklung und Herstellung der TELDIX® Space Wheels (Präzisions-Schwungräder) für Satelliten

roda computer GmbH F 03

...ist und bleibt auch im 30. Jahr seines Bestehens ein führender Anbieter von robuster, mobiler und kundenspezifischer IT-Lösungen für den Einsatz in rauen Umgebungen.
2016 wurde zum 4. Mal in Folge der Rahmenvertrag "gehärtete Notebooks" mit der Bundeswehr gewonnen, über den auch Toughbook® und Toughpad® der Panasonic System Communication Company EU bezogen werden können.
rodas aktuelle Produktinnovation ist das "Mobile Server Mission System" für den hochmobilen Einsatz, bestehend aus einem full-rugged Server-Laptop Lizard RW11, verschiedenen Missionsmodulen (Switche, USV, Kabeltrommeln und Clients).
Kontakt: roda computer GmbH, Landstr. 6, 77839 Lichtenau/Baden,
Tel.: +49 (0)7227 / 9579-0, mail@roda-computer.com

Rohde & Schwarz M 16

Rohde & Schwarz steht seit mehr als 80 Jahren für Qualität, Präzision und Innovation auf allen Feldern der drahtlosen Kommunikationstechnologie. Strategisch ist der Elektronikkonzern auf die fünf Standbeine Messtechnik, Rundfunk- und Medientechnik, Cyber-Sicherheit, Sichere Kommunikation sowie Funküberwachungs- und Funkortungstechnik ausgerichtet.
Rohde & Schwarz liefert interoperable Funkkommunikationssysteme für den Einsatz am Boden, zu Wasser und in der Luft. Für die Bundeswehr liefert der Konzern die streitkräftegemeinsame, verbundfähige Funkgeräteausstattung (SVFuA). Mit seinen Empfängern, Peilern, Signalanalysatoren, Antennen und maßgeschneiderten Systemen ist der Konzern seit vielen Jahrzehnten in der inneren und äußeren Sicherheit tätig.
Rohde & Schwarz Cybersecurity bietet eine breite Palette an technisch führenden Lösungen für Informations- und Netzwerksicherheit. Hochsichere Verschlüsselungslösungen, Next-Generation-Firewalls sowie Software für Netzwerkanalyse- und Endpoint-Security schützen Unternehmen und öffentliche Institutionen weltweit vor Spionage und Cyber-Angriffen.

rola Security Solutions GmbH B 11

rola Security Solutions GmbH mit Sitz in Oberhausen zählt seit über 30 Jahren zu den bedeutendsten Anbietern von IT-Lösungen im Bereich der Inneren und Äußeren Sicherheit sowie der nachrichtendienstlichen Aufklärung. Im Fokus stehen Lösungen für Informationsmanagement, Auswertung und Analyse sowie Verbundsysteme.
In der Variante rsIntCent® wird die Software im militärischen Umfeld für Auswertung und Lagefeststellung genutzt. Schwerpunkte bilden Informationszusammenführung und quellenübergreifende Informationserschließung inklusive der Auswertung von unstrukturierten Massendaten sowie die Erzeugung dynamischer Lagebilder und die ebenengerechte Präsentation.
Lösungen für die Analyse Sozialer Medien und für Cyber Auswertung runden das Spektrum ab.
rola ist ein Unternehmen der Deutschen Telekom/T-Systems GmbH – Security made in Germany.
Kontakt: www.rola.com

RUAG Schweiz AG – RUAG Defence F 06

Das Unternehmen RUAG Defence steht für Technologiekompetenz auf allerhöchstem Niveau. Zum Kerngeschäft gehören Produkte und Dienstleistungen für Ketten- und Radfahrzeuge, die realistische Soldatenausbildung sowie zuverlässige Informations- und Kommunikationsinfrastrukturen. Hinzu kommen ballistische und elektromagnetische Schutzlösungen. Betreiber kritischer ICT-Infrastrukturen unterstützt das Unternehmen mit hochmodernen Cyber-Security-Lösungen.
Zu den Kunden von RUAG Defence gehören die Schweizer Armee und internationale Streitkräfte sowie Rettungs- und Sicherheitsorganisationen, Behörden und zivile Organisationen auf der ganzen Welt. An der AFCEA tritt RUAG Defence 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.

Saab International Deutschland GmbH B 06 + S 02

Saab Digital Air Traffic Solutions bietet ein allumfassendes Konzept fürb "Remote Control" von Flugverkehr durch Digitalisierung und Integration aller Aufgabenbereiche von Flughäfen und Flughafenbetreibern. Hierbei spielt es keine Rolle, ob dieser Flughafen eine internationale Drehscheibe, ein kleiner Regionalflughafen oder ein neu zu gestaltender Flughafen ist, SDATS bietet effektive und effiziente Lösungen, welche sowohl die Betriebs- als auch die Flugsicherheit erhöhen. Dieses Remote Tower System von Saab ist für den Betrieb zugelassen und ist weltweit die erste und z. Z. noch einzige zertifizierte Einrichtung dieser Art. Basierend auf diesem allumfassenden Ansatz wird durch die Schaffung und Bildung neuer Umsatzströme für unsere Kunden die ATM-Branche erneuert und auf die Zukunft hin ausgerichtet.

Auf dem griffity Gemeinschaftsstand S 02

TactiCall steht für die umfassende Kontrolle und einen schnellen Zugang im Bereich interner Kommunikationssysteme zu Lande, zu Wasser und in der Luft. Ob im Rahmen von Telefonnetzen, öffentlichen Informations- und Alarmsystemen, Unterhaltungssystemen oder öffentlichen Sendeanstalten – mit TactiCall sind Sie mittendrin!
TactiCall ist hochflexibel und skalierbar und kann daher problemlos in Ihre Arbeitsumgebung integriert werden. Darüber hinaus ist es plattformunabhängig und lässt sich an eine Softwarearchitektur Ihrer Wahl anpassen.

Saab Medav Technologies GmbH S 02

Saab Medav Technologies ist seit mehr als 30 Jahren erfolgreich auf dem Markt der Sicherheitstechnik, der Nachrichtentechnik sowie bei Anwendungen für die Fusion von Informationen. Mit unseren Produkten zur Erfassung, Peilung und Ortung von Funksignalen stellen wir komplette Lösungen für strategische (COMINT) und taktische Anwendungen (C-ESM) zur Verfügung. Eine Anwendung ist die Erstellung eines Lagebilds, das alle Funkemitter und dazugehörige Informationen darstellt und zeitnahe Reaktionen ermöglicht. Saab Medav Technologies wurde 1982 als MEDAV GmbH gegründet. Seit 2012 gehört Saab Medav Technologies mit rund 100 Mitarbeitern zur Saab AB.
Internet: www.medav.de und www.saab.com/saabmedavtechnologies
E-Mail: marketing-smt@saabgroup.com

SAF Tehnika JSC F 41

Wir, bei SAF Tehnika, sind einer der weltweit führenden Produzenten von Richtfunkequipment mit einer globalen Präsenz in über 130 Ländern und bieten maßgeschneiderte Lösungen für verschiedenste Industrien an. Eine unserer neuesten Entwicklungen ist unser handheld Spektrumanalysator "Spectrum Compact" im Bereich 2-40GHz, sowie "Spectrum Compact E-Band" im Bereich 70-87GHz. Das batteriebetriebene Gerät ist bei der Installation, Fehlerbehebung und Planung von Richtfunkstrecken alternativlos. Unsere Punkt-zu-Punkt-Richtfunksysteme bieten die bestmögliche Alternative zur Glasfaser und ermöglichen eine Übertragungsrate von bis zu 10Gbps bei einer niedrigeren Latenz und hoher Effizienz. Richtfunksysteme von SAF Tehnika können dabei Distanzen von bis zu 150km überbrücken.

Safran Vectronix AG F 53

Unsere Mission ist Ihre Zufriedenheit
Safran Vectronix ist ein globaler Marktführer auf dem Gebiet hochmoderner optronischer Geräte, Systeme und Sensoren für militärische und zivile Anwendungen. In unseren Produkten stecken über 90 Jahre Schweizer Herstellertradition und Erfahrung im Bereich Optik und Präzisionstechnik – ob es um handgehaltene Laser-Entfernungsmesser, Nachtsichtgeräte, stativmontierte Orientierungs- und Positionssysteme oder Sensormodule für unsere OEM-Partner geht. Unsere Kunden profitieren von der weltbekannten Präzision, Verlässlichkeit und Qualität unserer Produkte bei niedrigsten Ausfallraten. Wir stellen uns auf spezifische Kundenbedürfnisse ein, liefern maßgeschneiderte Lösungen und bieten Support auf höchstem Niveau über die gesamte Produktlebensdauer hinweg.
Kontakt: Safran Vectronix AG, Max-Schmidheiny-Strasse 202, 9435 Heerbrugg, Schweiz, www.safran-vectronix.com

SAP Deutschland SE & Co. KG M 11

SAP bietet in fast allen Bereichen Lösungen für die Bundeswehr an. Die vielseitigen Anwendungen der Branchenlösung SAP® for Defense & Security unterstützen dabei die Prozessorientierung, reduzieren Kosten und erhöhen die Transparenz. Darüber hinaus bietet die SAP HANA® Plattform mit der zukunftsweisenden In-Memory-Technologie die ideale Grundlage nicht nur zur Digitalisierung sämtlicher Geschäftsprozesse der Bundeswehr, sondern auch zur Umsetzung spannender Innovationsthemen, beispielsweise Echtzeit-Analyse, Prognose und Simulation, sowie "Machine Learning". Dieses Jahr stellen wir u.a. ‚Digitale Assistenzsysteme' zur Analyse und Visualisierung von großen Datenmengen vor, auf denen sich Entscheidungen und Handlungen im Rahmen der Planungsprozesse und Organisationsführung auf allen Ebenen begründen.
Wir freuen uns auf Ihren Besuch am Stand M11.
Weitere Informationen finden Sie auf unserer Homepage unter www.sap.com/defense.

Schönhofer Sales and Engineering GmbH F 24

Die Schönhofer Sales and Engineering GmbH ist ein führender unabhängiger Anbieter von hochentwickelten Analytics-Lösungen und IT-Systemen für öffentliche Auftraggeber, Banken, Versicherungen und Unternehmenskunden. Wir bieten die Integration von Sensordaten, Datenmanagement und Big Data Analytics an, um Risiken besser zu managen und Entscheidungen zu optimieren. Basis vieler Lösungen ist die Schönhofer TARAN Suite®. Sie bietet für jeden möglichen Auswerteschritt und Analysebedarf das richtige Werkzeug: Netzwerk- und Geoanalysen, umfangreiche Text- und Medienanalyse, statistische und lernende Verfahren sowie flexible Berichts- und Ausgabewerkzeuge. Schönhofer ist bevorzugter IBM Partner für Lösungen auf Basis des gesamten Spektrums der IBM i2 Analysesoftware. IBM i2 bietet eine Suite von Analyse- und Datenhaltungsprodukten, die dafür entwickelt wurden, Transparenz in komplexe Zusammenhänge im Kontext von Ermittlung, Analyse und Auswertung zu bringen.
Kontakt: Telefon: +49 (0)2241 / 30990, www.schoenhofer.de

SciEngines GmbH F 10

Die **SciEngines GmbH** bietet spezialisierte Hochleistungsrechner sowie weltweit einzigartige Kryptanalyse Lösungen. "The SciEngines GmbH RIVYERA S6-LX150 system is the only system that can reasonably be expected to meet the Government's requirements relative to performance, space, and power consumption." Diese Aussage einer NATO Streitmacht wird durch die Vorteile der verwendeten FPGA Technologie ermöglicht. Im Vergleich zu herkömmlichen Computern ist das Preis-Leistungsverhältnis für spezialisierte Anwendungen 10x verbessert. Platz- und Energieeffizienz 20x.
Naheliegende Anwendungen für solch massive Rechenleistung:
- **Cyber** (reaktive defense, -warfare, CNO)
- **Aufklärung** (SIGINT/COMINT) und **"ethical hacking"**
- Überprüfung eigener **IT-Sicherheit / Penetrationstests**

Weitere Informationen: www.SciEngines.com oder info@sciengines.com bzw. 0431 / 908 620 00.

Scopeland Technology GmbH F 52

Die SCOPELAND Technologie und die SCOPELAND Methode steht für eine moderne Herangehensweise zur Entwicklung anspruchsvoller IT-basierter Anwendungen Unser Motto: Individuallösungen ja, Individualprogrammierung nein!
Konfigurieren statt Programmieren – 100% Codegenerierung – das ist die Antwort auf die vielen Probleme, die umfangreiche Programmiervorhaben immer wieder aufwerfen. Wir helfen Ihnen durch unsere erprobte SCOPELAND-Technologie und unsere Experten, dass Sie deutlich effizienter, schneller und kostengünstiger neue IT-gestützte Verfahren, als maßgeschneiderte Datenbankanwendungen, entwickelt bekommen. Wir können auf über 20 Jahre Erfahrungen verweisen und sind ein anerkannter Partner im der öffentlichen Verwaltung.

secunet Security Networks AG M 20

secunet ist einer der führenden Spezialisten im Bereich IP-basierter Kryptosysteme in Europa. Die ca. 40 Komponenten der SINA Kryptoarchitektur – Clients, IPsec- und One Way Gateways, Leitungsverschlüsseler sowie Systemlösungen für sichere Nachweisführung und Collaboration – verfügen über alle nationalen sowie wesentliche internationale Zulassungen. Das Produktspektrum SINA bietet Lösungen für unterschiedlichste VS-Zulassungs-Level und innovative VS-IT-Architekturen.
Ausstellungsschwerpunkte:
Ausstattung multinationaler Kommandos und Missionsnetze
- HaFIS s/v Client: SINA Workstation H Client III
- auf gehärteten Notebooks basierende SINA Workstation H R RW11 und Workstation E R RV11
- AMN-Client-Nachfolger: SINA Workstation E Client IV

Weitere SINA Produktinnovationen
- erster GEHEIM zugelassener Ethernet-Verschlüsseler: SINA L2 Box H
- (ultra-)mobile SINA Client S Varianten
- Secure Information Exchange Gateway (Rot/Schwarz)

Secusmart GmbH M 12

Secusmart GmbH (www.secusmart.com), eine Tochtergesellschaft von BlackBerry®, ist weltweit führender Experte bei der Entwicklung und Implementierung von mobilen Abhörschutzlösungen in Unternehmen und Behörden.
Mit der SecuSUITE for Government können Regierungen und Behörden vertraulich über handelsübliche Smartphones verschlüsselt telefonieren.
Zum komfortablen mobilen Arbeiten mit Daten und Apps bietet Secusmart das SecuTABLET, ein vollständig verschlüsseltes Samsung Galaxy Tab S2 mit Android-Betriebssyste. Gemeinsam mit der Bundesregierung nutzen mittlerweile weltweit mehr als 20 Länder die SecuSUITE for Government. Die deutschen Bundesbehörden nutzen seit Jahren die vom BSI zugelassene Lösung SecuSUITE for BlackBerry 10. Secusmart: Saal Maritim, Stand M 12.

Selex ES GmbH M 21

Selex ES GmbH ist Systemlieferant für zuverlässige Kommunikations-Sensorlösungen für die Industrie, Sicherheitsbehörden und Militär. Durch Verwendung modernster Informations- und Kommunikationstechnologien für stationäre oder mobile Systeme bieten die Lösungen von Selex ES dem Nutzer neue Anwendungsmöglichkeiten, die im Rahmen einer modernen militärischen Operationsführung notwendig sind.
Selex ES verfügt über langjährige Erfahrung in der Integration komplexer heterogener Sensornetzwerke.
Alle Sensoren und Systeme von Selex ES können in übergreifende netzwerkzentrische Kampfführungssysteme integriert werden.
Kontakt: www.de.selex-es.com, www.selex-es.de, Tel.: +49 (0)7191 / 378-0, Tel.: +49 (0)2137 / 782-0

Sennheiser Vertrieb und Service GmbH & Co. KG F 32

Professionelle Headset-Lösungen für ATC und Contact Center & Office
Sennheiser ist einer der weltweit führenden Hersteller von Kopfhörern, Mikrofonen, kabellosen Übertragungssystemen, Premium-Headsets und Konferenzlösungen. Die Headsets überzeugen durch HD Sound, erstklassiges Design, robuste Verarbeitung und benutzerfreundliche Handhabung. Sie eignen sich besonders für ATC, Contact Center, Offices, Unified Communications-Umgebungen und mobiles Business. Die perfekte Ergonomie der Sennheiser Produkte garantiert den notwendigen Tragekomfort für langes, ermüdungsfreies Arbeiten. Der Einsatz hochwertigster Materialien lässt Sie selbst und Ihren Gesprächspartner von glasklarer Sprachqualität profitieren. Besuchen Sie uns auf: www.sennheiser.de/cco

SFC Energy AG S 02

Die Brennstoffzellen von SFC sind die ideale Energielösung für netzferne und mobile Anwendungen bei Sicherheitsbehörden und militärischen Organisationen. Die leise, hoch effiziente und intelligente Technologie ermöglicht und unterstützt Einsätze, die mit konventionellen Stromerzeugern oder Batterien nur schwer durchführbar sind und verlängert die Energieautonomie im Einsatz signifikant.
Die Produkte von SFC werden im Bereich der Spezialkräfte eingesetzt und haben ihre Leistungsfähigkeit bewiesen. Auf dieser Grundlage bieten sich auch Anwendungen in anderen Bereichen wie dem Heer, dem Sanitätsdienst bis hin zur Absicherung von Liegenschaften.
SFC Energy AG | Eugen-Sänger-Ring 7 | 85649 Brunnthal
Tel.: +49 (0)89 / 673 592 | email: info@sfc.com | www.sfc-defense.com

SINUS Electronic GmbH F 31

Smarte Feldlagervernetzung im digitalen Zeitalter
Seit mehr als 28 Jahren entwickelt, integriert und liefert die **SINUS Electronic** innovative Produkte an das deutsche Militär.
Mit unseren kundenorientierten Verbindungsschnittstellen für Kommandofahrzeuge und -Shelter sorgen wir für schnellen und sicheren Datenaustausch, Anwendungssicherheit und hohe Verfügbarkeit. Unsere Produkte entsprechen den strengen Anforderungen der Bundeswehr, NATO und MIL-STD.
Mit unserer **SINUS Power-Line-Solution** und **SINUS Hybrid-Solution** bieten wir komplette Infrastrukturen für mobile Gefechtsstände:

- **Strom, Daten und Telefonie – alles in einem Kabel**
- **One-of-a-kind Lösung ermöglicht eine schnelle Bereitstellung im Feld**
- **Das System kann an die bestehende Infrastruktur angepasst werden**
- **Das SINUS-Induktiv-Mobil-Telefon bietet eine bis jetzt ungeahnte Flexibilität**

info@sinus-electronic.de

Software AG M 18

Innovativ. Leistungsstark, Partner der Bundeswehr
Die Software AG hilft Unternehmen, Behörden und Streitkräften ihre Prozesse zu digitalisieren. Mit Lösungen für Big Data, Integration, Prozessmanagement und IT-Portfolio-Management steigern Streitkräfte die Effizienz und optimieren ihre Prozesse, um qualifizierte Entscheidungen in Echtzeit zu treffen.
Als Innovationspartner unterstützt die Software AG die Bundeswehr, ihre Prozesse agil an neue Herausforderungen anzupassen und die IT-Landschaft dynamisch zu skalieren.
www.SoftwareAG.com
Kontakt: Software AG, Uhlandstr. 9, 64297 Darmstadt, Christoph Reich, Director Defense Business, +49 (0)6151 / 924 111, +49 (0)170 / 454 95 37, christoph.reich@softwareag.com

Solidtec GmbH F 45

Solidtec GmbH ist auf die Produktion von Kunststoffprototypen aus Originalmaterialien, Vor- und Kleinserien spezialisiert.
Ausgehend von 3D-Eingangsdaten konstruieren wir die Werkzeugeinsätze passend für unser spezielles Stammwerkzeugsystem und stellen sie mittels HSC-Fräsen aus hochfestem Aluminium her.
Nach dem Aufbau der Werkzeuge mustern wir auf eigenen Spritzgussmaschinen ab.
Unsere Projektleiter begleiten den Kunden durch alle Arbeitsschritte der Prozesskette und stehen ihm bereits vor Auftragsvergabe bei der Entwicklung und Konstruktion seiner Bauteile beratend zur Seite. Durch die lückenlose Prozesskette im Haus erreichen wir höchste Qualität und sehr kurze Durchlaufzeiten vom Auftragseingang bis zum fertigen Produkt.

Sophos S 10

Sophos – Security made simple
30 Jahre Erfahrung und jede Menge Entwicklungsinnovationen fließen bei Sophos in die Entstehung neuer IT-Sicherheitslösungen. Und oft können schon kleine Veränderungen Großes bewirken. So zum Beispiel der Sophos Security Heartbeat, der durch eine innovative Verbindung zwischen Endpoints und Firewall den Austausch wichtiger Detailinformationen ermöglicht und IT-Sicherheit auf diese Weise komplett neu definiert. Sophos realisiert mit diese "Synchronized Security" ein völlig neues Konzept, das verschiedene Endpoint- und Netzwerk-Sicherheitslösungen integriert und automatisiert. Das bedeutet für Kunden nicht nur eine erhöhte Next-Generation-IT-Sicherheit, sondern auch wirtschaftliche Vorteile. Heute sichern Sophos-Produkte Netzwerke, die von 100 Mio. Menschen in 150 Ländern und 100.000 Unternehmen genutzt werden.

Sopra Steria Consulting F 12

Sopra Steria Consulting zählt zu den Top Business Transformation Partnern in Deutschland. Als ein führender europäischer Anbieter für digitale Transformation bietet Sopra Steria eines der umfassendsten Angebotsportfolios für End-to-End-Services am Markt: Beratung, Systemintegration, Softwareentwicklung, Infrastrukturmanagement und Business Process Services. Unternehmen und Behörden vertrauen auf die Expertise von Sopra Steria, komplexe Transformationsvorhaben, die geschäftskritische Herausforderungen adressieren, erfolgreich umzusetzen. Im Zusammenspiel von Qualität, Leistung, Mehrwert und Innovation befähigt Sopra Steria seine Kunden, Informationstechnologien optimal zu nutzen.
Unsere Themenschwerpunkte 2017:

- Nutzung der Rahmenverträge des Bundes für die Bundeswehr
- IT-Service-Management nach ITILv3
- Technische Dokumentation: IETD, ASD SPEC, B007
- SASPF-Einführung
- Betriebsunterstützung
- Cyber Defence und IT-Sicherheit
- Operationelle Architekturen
- Collaboration Management

SQS Software Quality Systems AG F 50

SQS ist der weltweit führende Spezialist für Software-Qualität. Wir bieten durchgehende Qualitätssicherung für Geschäftsprozesse bei softwarebasierten Systemen. Die Experten von SQS identifizieren und mindern Geschäftsrisiken technologischer Transformationsprozesse, wobei standardisierte Methoden, Automatisierungslösungen, Bereitstellungsmodelle sowie tiefgreifendes Fachwissen zum Einsatz kommen. Dank unserer Spezialisierung bieten wir Objektivität und Sicherheit rund um Software-Qualität.
Die Position als Marktführer basiert auf mehr als 30 Jahren erfolgreicher Beratungstätigkeit. Mit über 10.000 abgeschlossenen Projekten besitzt SQS eine starke Kundenbasis, zu der die Hälfte der DAX-30-Unternehmen, nahezu ein Drittel der STOXX-50-Unternehmen und 20 Prozent der FTSE-100-Unternehmen gehören. Das Unternehmen hat seinen Hauptsitz in Köln und beschäftigt rund 4.600 Mitarbeiter.
Kontakt: www.sqs.com

steep GmbH M 08

Die steep GmbH ist ein international erfolgreicher technischer Dienstleister mit mehr als 30 Standorten und rund 700 Mitarbeitern in Deutschland und Europa. Neben den Kernfähigkeiten in den Bereichen Radar-Service, IT-Services, Systemintegration, Training und Mobile Netze zeichnet sich steep durch ein weiteres großes Kompetenzspektrum aus: In Kombination mit den Geschäftsbereichen Logistik und Technische Dokumentation, Material Management, EMV-Service, Managed Services in Partnership und Facility Management profitieren unsere Kunden von der einzigartigen Möglichkeit, alle aufeinander abgestimmten Einzelleistungen in einer gesamtheitlichen Lösung aus einer Hand zu erhalten. In Anlehnung an das diesjährige Thema der AFCEA-Fachausstellung zeigen wir Ihnen unsere neuesten Lösungen für die Bereiche Compliance, mobile taktischen Kommunikation und Einsatzführung.
www.steep.de

SUSE Linux GmbH F 25

Zuverlässige und kostengünstige Bereitstellung geschäftskritischer Services
SUSE, ein Pionier im Bereich Open Source-Software, entwickelt zuverlässige interoperable Linux-, Cloud-Infrastruktur-und Storage-Lösungen, die Unternehmen, Behörden und Streitkräften mehr Kontrolle und Flexibilität ermöglichen. Mehr als 20 Jahre Erfahrung und hervorragende Leistung in den Bereichen Entwicklung und Services machen die SUSE Produkte und den Support leistungsstark und helfen Komplexität zu verringern, Kosten zu reduzieren und verlässlich erfolgskritische Services anzubieten. Weitere Informationen unter: www.suse.com
Wir freuen uns auf Ihren Besuch am Stand F 25 im Foyer II !
Weitere Informationen finden Sie auf unserer Homepage unter www.suse.com
Kontakt: SUSE Linux GmbH, Maxfeldstr. 5, 90409 Nürnberg, kontakt-de@suse.de, +49 (0)911 / 740 537 79
Ihr Ansprechpartner: Harald Zangenberg

SVA System Vertrieb Alexander GmbH M 14

Die SVA System Vertrieb Alexander GmbH ist einer der führenden deutschen System-Integratoren im Bereich Datacenter-Infrastruktur und beschäftigt mehr als 610 Mitarbeiter an 16 Standorten in Deutschland. Das unternehmerische Ziel der SVA ist es, hochwertige IT-Produkte der jeweiligen Hersteller mit dem Projekt-Know-how und der Flexibilität von SVA zu verknüpfen, um so optimale Lösungen für die Kunden zu erzielen.
Kernthemen des Unternehmens sind Hochverfügbarkeit, hoch skalierbare SAN-Architekturen, Security-Lösungen und Disaster Recovery sowie Virtualisierungstechnologien. Darüber hinaus bietet SVA Consulting und Operational Services.
Das zertifizierte Solution Center der SVA in Wiesbaden bietet SVA-Experten und Kunden umfassende Demonstrations-, Entwicklungs- und Schulungsszenarien mit aktuellsten Hardware- und Software-Lösungen.

Symantec F14

Symantec Corporation (NASDAQ: SYMC) ist ein Experte für den Schutz von Informationen, der Privatpersonen, Unternehmen und Regierungen dabei unterstützt, die vielfältigen Möglichkeiten neuer Technologien jederzeit und überall zu nutzen.
Symantec, ein Fortune 500-Unternehmen, wurde im April 1982 gegründet. Das Unternehmen betreibt eines der größten globalen Dateninformationsnetzwerke und stellt führende Sicherheits-, Backup- und Verfügbarkeitslösungen überall dort zur Verfügung, wo wichtige Informationen gespeichert, abgerufen und ausgetauscht werden.
Die mehr als 19.000 Mitarbeiter des Unternehmens sind in über 50 Ländern beschäftigt. Neunundneunzig Prozent der Fortune 500-Unternehmen sind Symantec-Kunden.
Im Geschäftsjahr 2015 verzeichnete Symantec Umsätze von 6,5 Milliarden US-Dollar. Weitere Informationen finden Sie auf www.symantec.de. Oder treffen Sie Symantec in den sozialen Medien unter: http://www.symantec.de/social/.

Systematic GmbH M 26

Systematic bietet interoperable Führungsinformationssysteme für alle Führungsebenen. Die Military-off-the-Shelf Produkte haben sich weltweit in multinationalen und

streitkräftegemeinsamen Einsätzen bewährt und werden unter Einbeziehung der Einsatzerfahrungen permanent weiterentwickelt. Die SitaWare-Suite setzt damit neue Maßstäbe für die Interoperabilität mit nationalen-, internationalen- und NATO-Systemen. Aufgrund serviceorientierter Architekturen und offener Schnittstellen sind die einzelnen Produkte modular, skalierbar und integrierbar in das IT-System der Bundeswehr. SitaWare ist bereits in die Bundeswehr eingeführt und konnte in zahlreichen Vorhaben den sofortigen operationellen Mehrwert unter Beweis stellen. Mit aktuell 24 Nutzerstaaten ist SitaWare eines der meist genutzten Führungsinformationssysteme weltweit und erreicht dadurch eine einzigartige Kosteneffizienz.
Kontakt: Systematic GmbH, Im Zollhafen 24, 50678 Köln, www.systematic.com, contact_de@systematic.com

systerra computer GmbH — ME 02

systerra computer GmbH ist Anbieter von Langzeitverfügbaren, schock-/vibrationsfesten und MIL-konformen Rechner-, Speicher- und Netzwerkplattformen für den erweiterten Betriebstemperaturbereich, zum mobilen und stationären Einsatz am Boden, in der Luft und auf See.
Das Spektrum gehärteter COTS-Rechner von renommierten Herstellern, u.a. Themis Computer, Moxa, MPL, RTD und Acromag, basiert auf anerkannten Standards wie VME, VPX, VITA 74, PC/104, CompactPCI und 19"-Technologie sowie Windows®-, Linux®-, Echtzeit-Betriebssystemen und ist vielfach qualifiziert für die Virtualisierungs-SW (VMWare® etc). systerra computer bietet in enger Zusammenarbeit mit den Kunden auch applikationsspezifische Sonderversionen.
Kontakt: systerra computer GmbH, Kreuzberger Ring 22, 65205 Wiesbaden,
Tel. +49 (0)611 / 448 89-400, E-Mail: info@systerra.de, Internet: www.systerra.de

TAS – Telefonbau Arthur Schwabe GmbH & Co. KG — ME 03

TAS mit Hauptsitz in Mönchengladbach besteht seit 1924 und beschäftigt mehr als 200 Mitarbeiter an 15 Standorten in Deutschland. Das Unternehmen ist auf Lösungen der Sicherheits- und Kommunikationstechnik spezialisiert.
Langjährige Partnerschaften mit diversen Einsatz- und Rettungskräften verdeutlichen die Kompetenz und Zuverlässigkeit des Unternehmens.
TAS bietet hochverfügbare Lösungen mit individuellem Zuschnitt aus eigener Entwicklung und Fertigung.

- Gefährder identifizieren dank Videotechnik
- Automatisierte Protokollierung der Wach- und Streifengänge verbunden mit Alarmierung im Störfall
- Schulungssysteme auf IP-Basis für die Simulation von taktischer Kommunikation innerhalb der Bundeswehr
- Standortalarmierung mit Hilfe des Alarmierungsservers ARUTEL
- Standortabsicherung durch das Alarm- und Störmeldesystem ARUDAN Secure (BSI-zertifiziert)

Kontakt: Telefonbau Arthur Schwabe GmbH & Co. KG, Telefon: 02166/858-0, www.tas.de

TELEFUNKEN Radio Communication Systems GmbH & Co. KG — M 25

TELEFUNKEN RACOMS entwickelt und vertreibt Funkkommunikationssysteme für moderne, sicherheitsrelevante und hochtechnologische Anwendungen. Für die militärische Nutzung steht ein breit gefächertes Angebot an taktischen und strategischen HF-Funksystemen sowie taktischen VHF- und UHF-Funksystemen zur Verfügung. Diese Systeme sind zu Lande, zu Wasser und in der Luft im Einsatz. Die Kompetenz von TELEFUNKEN RACOMS umfasst alle Bereiche der Produktentstehung – vom Systemdesign, der Entwicklung hochperformanter Produkte und der Produktion bis zur Komplettintegration von Funkübertragungssystemen.
Neben dem Kerngeschäft der Funkkommunikation erweitert TELEFUNKEN RACOMS kontinuierlich seine Geschäftstätigkeiten speziell auf den Gebieten Elektrooptische Systeme (z.B. Nachtsichtgeräte, Laserwarnsysteme) und Sensorik und reagiert somit auf den wachsenden Bedarf der Bundeswehr an zuverlässigen und leistungsstarken Systemen zur Unterstützung der Auftragserfüllung in den Einsatzgebieten.
Kontakt: TELEFUNKEN Radio Communication Systems GmbH & Co. KG,
Eberhard-Finckh-Str. 55, 89075 Ulm, info@tfk-racoms.com, www.tfk-racoms.com

Textron Systems — B 08

Textron Systems Geospatial Solutions flagship software products, ELT®, GIV® and RemoteView™, deliver an extensive set of GEOINT collection tools to enhance the intelligence gathering and analysis process. From imgery analysis and radar exploitation, to terrain feature extraction and advanced 3D visualization, Textron offers a proven solution for situational understanding and interoperability. Textron Systems Geospatial Solutions are used across a broad spectrum of industries: military and defense, border security, disaster relief, environmental engineering, ecosystems monitoring, urban planning, insurance, oil and gas exploration, utility companies and more to provide unmatched fidelity and accuracy in mission planning, actionable intelligence and rapid decision making. See www.textronsystems.com for more information.
Kontakt: Kevin Opitz, E-Mail: geosalesteam@overwatch.textron.com

Thales Deutschland — F 13

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 MoTaKo-Programms mit Beratung, Entwicklung, Design, Inbetriebnahme und Service zur Seite.
Thales verfügt über ein Produktportfolio, das modular an den einsatzbedingten Kommunikationsbedarf angepasst werden kann. Eine moderne Systemarchitektur ermöglicht eine nahtlose, medienbruchfreie Kommunikation und bildet einen wichtigen Beitrag zum Missionserfolg.
Einsatzerprobte C2-Kommunikationssysteme sowie die Entwicklung der Breitbandwellenform ESSOR bilden die Säulen einer dienste-orientierten Kommunikation.
Moderne Funksysteme wie die neue Software-Defined-Radio-Produktfamilie SYNAPS, leistungsfähige Kryptologie- und Schlüsselmanagementlösungen und moderne SOTM-Systeme stellen die notwendigen Kommunikationsplattformen zur Sicherstellung eines "Quality of Services" sicher.
Kontakt: www.thalesgroup.com/germany

T-Systems International GmbH — B 10

Flexible Informations- und Kommunikationstechnik für die Bundeswehr.
Mit einer weltumspannenden Infrastruktur aus Rechenzentren und Netzen betreibt T-Systems die Informations- und Kommunikationstechnik (ICT) für multinationale Konzerne und öffentliche Institutionen.
Kompetenter Partner der Bundeswehr.
T-Systems unterstützt die Bundeswehr als erfahrener Partner für sichere und zuverlässige Lösungen rund um die Kernaufgaben Organisation, Aufklärung, Führung, Logistik und Kommunikation. Dabei liegt die besondere Kompetenz von T-Systems darin, handelsübliche Hard- und Softwarekomponenten so anzupassen, dass sie alle Anforderungen der Bundeswehr hinsichtlich Sicherheit, Echtzeitbetrieb und anderer Einsatzbedingungen erfüllen.
Kontakt: T-Systems International GmbH, Friedrich-Ebert-Allee 140, 53113 Bonn,
Tel.: 0228 / 181-38210, Mail: markus.lehmann@t-systems.com, Internet: www.t-systems.de

Utimaco — S 10

Utimaco gehört zu den führenden Herstellern für Hardware-Sicherheitsmodule (HSM), die den Vertrauensanker für das Internet der Dinge liefern. Wir sichern Ihre kryptografischen Schlüssel und digitalen Identitäten, damit kritische digitale Daten und Infrastrukturen geschützt werden.

- Unsere HSM bieten eine einfache, rollenbasierte Verwaltung, Skalierbarkeit, niedrige Gesamtbetriebskosten und beinhalten Zugang zu einem umfangreichen Angebot an Services und Training.
- Zur Einhaltung von Compliance-Anforderungen bieten wir FIPS-zertifizierte und nach Common Criteria evaluierte Produkte an.
- Das Utimaco Software Development Kit (SDK) bietet eine schnelle Umsetzung von Endkunden-Projekten sowie Produktinnovation für Systemintegratoren.
- Durch Professional Services Dienstleistungen unterstützen wir unsere Partner bei der Umsetzung ihrer Lösungen.

Veritas — F 14

Das explosionsartige Datenwachstum und die Ressourcen, die für das Management dieser Daten eingesetzt werden müssen, ist eines der drängendsten Probleme, mit denen Unternehmen heutzutage fertig werden müssen.
Dabei geht es nicht nur um die Menge der Daten, sondern auch darum, wo sie gespeichert sind und wie sie zwischen Private Clouds, Public Clouds und zurück in Systeme vor Ort übertragen werden.
Jede einzelne unserer Lösungen für Informationsmanagement – von Business Continuity über Backup und Wiederherstellung und Software-Defined Storage bis hin zu Information Governance – wurde nach dem Grundsatz konzipiert, dass Informationen wichtiger sind als Infrastruktur.
Weitere Informationen unter: www.veritas.com

VITES GmbH — S 02

Die VITES GmbH ("VITES") ist ein junges, dynamisches, stark wachsendes Unternehmen, das sich auf Produkte der Funktechnik für professionelle Einsatzgebiete spezialisiert hat.
Fokusgebiet des Unternehmens ist eine innovative Funktechnologie für vollelektronische Strahlformung und –nachführung, die kompakte Phased-Array-Antennensysteme mit Modems in Software-Defined-Radio Technologie integriert. Darauf basierend werden breitbandige Datenlinks und SATCOM-on-the-Move-Lösungen, insbesondere für den Security Markt entwickelt.
Ein weiterer Schwerpunkt ist "HiMoNN", die marktführende Produktlösung für breitbandige Funk-Konnektivität im Bereich der Sicherheits- und Katastropheneinsätze. HiMoNN ist eine zuverlässige, robuste, ausgereifte und kosteneffiziente Lösung für Ad-Hoc-Netzwerke in diesem Bereich und seit Jahren sehr bekannt und erfolgreich.
Standort des Unternehmens ist Ottobrunn bei München.
Pressekontakt: VITES GmbH, Einsteinstraße 32, 85521 Ottobrunn, www.vites.de Ansprechpartner: Martin Gassner, Geschäftsführer, Tel. 089 / 6088-4600

ZARGES GmbH — M 30

In den ZARGES Produkten vereinen sich seit über 80 Jahren die vielfältigen Vorteile des Leichtmetall-Werkstoffs Aluminium wie hohe Stabilität bei gleichzeitig geringem Gewicht, Korrosionsfestigkeit sowie Flexibilität im Einsatz. So hat ZARGES für jeden das geeignete Produkt und kann auch individuelle Lösungen anbieten. Ob es ums Konfektionieren, Lagern, Transportieren, Organisieren, Schützen oder Steigen geht: bei ZARGES finden Sie immer eine optimale Lösung auch im Bereich Speziallösungen. ZARGES fertigt nach aktuellen gesetzlichen Normen und Standards für Industrie und Militär. Individuelle Lösungen werden für unsere Kunden maßgeschneidert und können mit offiziellen Zulassungen z.B. nach BAM ausgeliefert werden.
Kontakt: ZARGES GmbH, Tel.: +49 (0)881 / 687-0, Fax: +49 (0)881 / 687-500
Internet: www.zarges.de E-Mail: zarges@zarges.de

BSC Berlin Security Conference

16th Congress on European Security and Defence

Impressions BSC 2016

For further photos and information please see

www.euro-defence.eu

BSC Berlin Security Conference

16th Congress on European Security and Defence

Berlin Security Conference 2017

Europe under pressure – security and defence in unpredictable times

28–29 November 2017, andel's Hotel & Convention Center Berlin

Visit us on Europe's leading event for European Security and Defence

Photos: Dombrowsky

BSC 2016, High-Level Debate

The Berlin Security Conference

- One of the largest yearly events on European Security and Defence
- Meeting place for up to 1 000 participants from more than 50 countries
- International forum for members of parliament, politicians and representatives of the armed forces, security organisations and industry
- Partner in 2017: Sweden
- Former Partners: Russia, United Kingdom, Turkey, USA, France
- Exhibitions with companies from Europe and abroad
- Organised by the Behörden Spiegel – Germany's leading independent Newspaper for the Civil and Military Services

Further Information:

www.euro-defence.eu

Vorankündigung:

32. AFCEA-Fachausstellung

11./12. April 2018

www.afcea.de