AFCEA 2013

Fraunhofer FKIE

ISBN 978-3-934401-15-0

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

Schutzimpfung für das IT-System

BWI – Strategischer Partner der Bundeswehr für Informations- und Kommunikationstechnik

Dank HERKULES ist die IT-Sicherheit in der Bundeswehr auf hohem Niveau.

Vertraulichkeit, Integrität, Verbindlichkeit und Verfügbarkeit sind die zentralen Ziele der IT-Sicherheit in der Bundeswehr. Die Schutzimpfung für das IT-System der Bundeswehr umfasst unter anderem eine von der BWI eingeführte Verschlüsselung des Weitverkehrsnetzes und einen zentralen Virenschutz. Zudem sorgt die neu eingeführte Netzwerkauthentifizierung dafür, dass sich nur noch in einer zentralen Datenbank erfasste Geräte im HERKULES-Netz anmelden können. Zusätzlich gewährleistet das Schnittstellenmanagement die Sicherheit direkt an den Arbeitsplätzen aller Nutzer. Rund um die Uhr ist so das IT-System der Bundeswehr vor Viren, Schadsoftware und anderen unerwünschten Eindringlingen geschützt.

Weitere Informationen unter: www.bwi-it.de

BWI

Bonn, April 2013

Sehr geehrte Damen und Herren,

vor zwei Jahren habe ich im Jubiläumsjahr von AFCEA Bonn e.V. erstmals die Schirmherrschaft über die Fachausstellung übernehmen dürfen. Es ist mir eine große Freude, die Veranstaltung auch in diesem Jahr als Schirmherr zu begleiten. Die AFCEA-Fachausstellung hat sich seit ihrer Premiere im Jahre 1986 zu einer Erfolgsgeschichte entwickelt, die nun mit der 27. Fachausstellung ihre Fortsetzung findet. Die kontinuierlich gestiegene Zahl ausstellender Firmen und das große Publikumsinteresse verdeutlichen die besondere Bedeutung der AFCEA-Fachausstellungen sowohl für die nationale Informations- und Telekommunikationstechnik (ITK)-Branche als auch für die Bundeswehr. Darüber hinaus gewinnt die Fachausstellung für den internationalen ITK-Bereich zunehmend an Attraktivität. Dies belegt die Zahl der Anmeldungen ausländischer Firmen.

Was erwartet Sie in diesem Jahr in der Stadthalle Bonn-Bad Godesberg? Auf 1.800 Quadratmetern Fläche werden erneut mehr als 100 Firmen vertreten sein und ihre Produktvielfalt präsentieren. Dies reicht vom mittelständischen Kleinbetrieb bis zum Großkonzern, von der IT-Beratungsfirma über den Anbieter von IT-Ausbildung bis hin zum Lieferanten hoch spezieller Softwareanwendungen für Informations- und Materialmanagement und IT-Sicherheit.

Die Vortragsreihe der diesjährigen Fachausstellung steht unter der Überschrift “IT-Services – Enabler in multinationalen Koalitionen”. Unternehmen, Behörden und nicht zuletzt auch die Streitkräfte sind heute wesentlich von moderner, leistungsfähiger und vernetzter ITK abhängig, um ihre jeweiligen Organisationsziele zu erreichen. Die ITK beeinflusst den Erfolg der Organisation durch die Verzahnung mit dem Kerngeschäft und die übergreifende Unterstützung der Geschäftsprozesse. Es kommt also darauf an, die zur Unterstützung der Führungs- und Arbeitsprozesse erforderlichen ITK-Dienstleistungen als IT-Services zuverlässig und in der notwendigen Qualität verfügbar zu machen. Welche Anforderungen sich daraus an die Leistungsfähigkeit von IT-Services und deren Bereitstellung durch Service Provider der ITK-Branche sowie der Bundeswehr und der NATO ergeben, wird Ihnen aus unterschiedlichen Blickwinkeln im Rahmen von Vorträgen kenntnisreicher Redner vorgestellt werden.

Ich bin sicher, dass auch diese 27. Fachausstellung mit ihrem vielfältigen Angebot Ihre Erwartungen erfüllen wird. In diesem Sinne wünsche ich Ihnen, sehr geehrte Damen und Herren, einen informativen Besuch der Fachausstellung, aufschlussreiche Vorträge sowie anregende Gespräche und Diskussionen. Hierzu darf ich Ihnen auch die Lektüre des Begleitheftes “AFCEA 2013” empfehlen, welches mit dem Themenschwerpunkt “Fraunhofer FKIE” einen Überblick über die Aktivitäten des Fraunhofer-Instituts in Wachtberg bietet.

Mit freundlichen Grüßen

Stéphane Beemelmans
Staatssekretär im Bundesministerium der Verteidigung

AFCEA 2013

1. AFCEA Bonn e.V. – Diensteorientierung in der IT

2. Fraunhofer FKIE – Cyber Security

3. Beitrag aus der Industrie

4. AFCEA-Fachausstellung

Impressum: Sonderheft Behörden Spiegel "AFCEA 2013" **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:** Birte Schulz, Behörden Spiegel **Fotos:** Autoren, AFCEA Bonn e.V., Fraunhofer FKIE, Behörden Spiegel Archiv **Druck:** Heider Druck GmbH, Bergisch Gladbach **Heftpreis:** 7,50 Euro
www.behoerdenspiegel.de

AFCEA Bonn e.V. – gemeinnützig im Dienste der IT für Bundeswehr und BOS

Generalmajor Erich Staudacher, Vorsitzender AFCEA Bonn e.V.

Generalmajor Erich Staudacher

Dienen – was für ein altertümliches Wort! Dienstorientierung – welch sperrige Formulierung! Und dennoch besitzen beide Begriffe eine ungebrochene Aktualität und Gültigkeit, gerade in unserer heutigen "Service"-orientierten Gesellschaft. Nicht nur im neuen Markenclaim der Bundeswehr, "Wir.Dienen.Deutschland.", kommt ein gleichermaßen traditionelles wie modernes Selbstverständnis zum Ausdruck. Auch in unserem Verhältnis zur Informationstechnologie rückt derzeit die dienende Funktion wieder stärker in den Mittelpunkt. Doch wer dient hier wem? Nach der bisherigen, langjährigen Schlagwort-Charakterisierung der IT als "enabler", als komplexer Unterstützer im Erreichen (ungeahnter) Möglichkeiten, vor allem auf dem Gefechtsfeld, haben wir jetzt vielleicht wieder verstärkt das Bedürfnis, Herr der fortgeschrittenen Systeme und Anwendungen im Alltag zu werden, den Nutzen der IT nicht mehr nur als Möglichkeit und Versprechen, sondern real und sofort zu erfahren.

Vizeadmiral Rühle, Generalmajor Staudacher und der inzwischen beförderte Generalmajor Dr. Rieks (von links nach rechts) freuen sich über die AFCEA-Fachausstellung 2012.

Dies verlangt zumindest beim durchschnittlichen Nutzer nach dem Gefühl, nicht von der IT als der heimlichen Dominierenden seines Tuns getrieben zu sein, sondern diese als selbstverständliche Dienst- und Unterstützungsleistung zu beherrschen.

Dienstorientierung geht aber weit über diesen Handhabungsaspekt von IT hinaus! Mit dem international etablierten Verständnis der "Service-orientierten Architektur" existiert ein Gestaltungsprinzip für das Design von IT-Anwendungen wie auch für die Organisation von Fähigkeiten und Aktivitäten. In der Verknüpfung beider Aspekte kann so ein flexibler, ressourcensparender Organisations- wie Operationsansatz entstehen, der uns in hohem Grade anpassungsfähig an noch unbekannte Herausforderungen künftiger Einsätze sein lässt. Gerade diese Chance jetzt zu ergreifen, scheint mir das Gebot der Stunde zu sein!

Dabei fällt unser Blick nach allen Erfahrungen aus den jüngsten Einsätzen fast zwangsläufig auf international standardisierte Lösungen. Die überaus positiven Erfahrungen des Afghan Mission Networks, sowohl in der zur Anwendung kommenden Technik als auch – viel bedeutsamer noch – das für seine Nutzung notwendige neue Grundverständnis des "need-to-share", eröffnen neue Horizonte einer interoperablen, effizienten IT-Nutzung im Bündnis wie national. Der begonnene Ausbau eines Future Mission Networks der NATO ist ein Beispiel.

Überhaupt beobachte ich ein gestiegenes Bedürfnis nach Zusammenarbeitsfähigkeit über Nationen- und Organisationsgrenzen hinweg. Vielleicht kommt hierbei ein fortentwickeltes Verständnis der Grundidee des "pooling and sharing" zum Ausdruck, nämlich nicht langfristig eine bessere Einsatzfähigkeit über eine wechselseitige Spezialisierung in den Fähigkeiten (mit all ihren Abhängigkeiten, Begrenzungen oder bewussten Einschränkungen) anzustreben, sondern die bessere Durchhaltefähigkeit und Flexibilität durch eine leichtere Ablösefähigkeit von nationalen Kontingenten in Einsätzen zu erzielen. Letzteres bedingt selbstverständlich ein höheres Maß an technischer Interoperabilität und Verfahrensvereinheitlichung, die aber politisch und finanziell leichter realisierbar sein dürfte als der bisher versuchte, schwierige endgültige Verzicht auf ganze Fähigkeiten.

Beeinflussen Service-orientierte Architektur-Ansätze schon unsere heutigen Organisationsstrukturen, wie dies klar in der prozessorientierten Neuausrichtung der Bundeswehr zum Ausdruck kommt, so erwachsen aus der immer selbstverständlicher werdenden Nutzung der "Social Media" im privaten Bereich noch ganz andere Einflüsse auf unsere gewachsenen Aufbau- und Ablauforganisationen. Klassische Entscheidungs- und Führungsprozesse mit Aufgabenspezialisierung und Informationszuteilung dürften bald zunehmend durch ein anderes IT-Anwenderverhalten, das auf dem Grundgedanken des "need-to-share" beruht, und durch entsprechende Erwartungen der IT-Nutzer herausgefordert sein. Ich bin überzeugt, gerade unsere jüngeren AFCEA-Mitglieder könnten in den auch in Behörden und Streitkräften entstehenden Diskussionsprozess ihre Sichtweisen und Erfahrungen nutzenstiftend einbringen. Es ist das Anliegen von AFCEA Bonn e.V., ihnen hierfür Diskussions- und (Mit-) Gestaltungsmöglichkeiten zu bieten. Bei allem mutigen Beschreiten neuer Wege und Berücksichtigen der modernen Ansprüche wird aber immer wieder auch den Aspekten der IT-Sicherheit der fällige Tribut zu zollen sein.

AFCEA Bonn e.V. möchte unter dem diesjährigen Jahresthema der "Dienstorientierung in der IT – Motor für flexible Anwendungen" in gewohnter Weise dem Informationsaustausch, der Vermittlung von Ideen und Lösungen, dem Artikulieren von Bedürfnissen ohne Eigennutz Raum und Rahmen bieten. Dies verstärkt für ein breiter werdendes Publikum, das aus Anwendern und Entscheidern der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) und der Bundeswehr auf Seiten der Ressourcenbereiche wie der Streitkräfte, in Ministerien wie Kommandobehörden und Truppe besteht. Aus vielen Gesprächen wurde mir deutlich, wieviele Chancen in der gegenseitigen gedanklichen Befruchtung liegen. Allerdings müssen erst noch überkommene Vorbehalte im Dialog abgebaut werden. Noch wird AFCEA zu sehr als "militär"-ausgerichtet angesehen. Schon aber die deutsche Bezeichnung unseres "Anwenderforums...." sollte deutlich machen, dass es uns nicht nur um militärische Nutzanwendungen geht. Insbesondere das diesjährige Jahresthema eröffnet breiten Raum für einen Erfahrungsaustausch aller mit Sicherheitsfragen befassten Organisationen und ermöglicht am Ende hoffentlich eine bessere "Interoperabilität", wo sie notwendig und zulässig ist. Notwendig erscheint sie mir allemal, denn die budgetären Rahmenbedingungen sind auch für die Realisierung von IT-Lösungen bei allen öffentlichen Auftraggebern schwieriger geworden sind.

Nicht nur thematisch, auch in regionaler Hinsicht ist ein größer gewordener Bereich abzudecken. Im Gefolge der

Vorstand AFCEA Bonn e.V. 2013

Geschäftsführender Vorstand

Vorsitzender
Erich Staudacher

Stellvertretender Vorsitzender und Leiter Programmbeirat
Reimar Scherz

Stellvertretender Vorsitzender und Sprecher Industriebeirat
Joachim Mörsdorf

Beauftragter für internationale Angelegenheiten
und Programmbeirat
Hans-Ulrich Schade

Geschäftsführer
Rolf-Dieter Zeckai

Erweiterter Vorstand (Beisitzer)

Leiter AFCEA-Fachausstellung
Friedrich W. Benz

Industriebeirat
Andreas Höher

Industriebeirat
Hartmut Jäschke

Behörden und Organisationen mit Sicherheitsaufgaben (BOS)
Dietrich Läpke

Programmbeirat und Young AFCEANs
Ralph Michel

Presse- und Öffentlichkeitsarbeit,
Repäsentant im Young AFCEANs Advisory Council
Jochen Reinhardt

Programmbeirat
Dr. Ansgar Rieks

Internationale Angelegenheiten und
Regional Vice-President (RVP) Central Europe
Wolfgang Taubert

Schriftführer
Kurt D. Wachsmuth

Nachwuchsförderung
Dr.-Ing. Michael Wunder

Mitwirkende Vorstandsgäste

Programmbeirat
Karin Börsch

Programmbeirat und Young AFCEANs
Katja Frintrop

Programmbeirat
Tobias Schönherr

Programmbeirat
Götz Stuck

Stolze AFCEA-Studienpreisträger 2012

Neuausrichtung der Bundeswehr haben wir von AFCEA Bonn e.V. nun auch in Berlin erfolgreich begonnen, Angehörige der Bundeswehr und der BOS, die eng mit den Organisationen und Einrichtungen der "Rheinschiene" verknüpft sind, dort "abzuholen" und für unsere – nein besser: für Ihre – Themen zu interessieren. Diesen Weg werden wir fortsetzen.

Wir sind zuversichtlich, auch dieses Jahr mit unserem Jahresthema Ihr Interesse wecken und befriedigen zu können und dabei weiterhin die Brücke in IT-Anwenderfragen zwischen Amtsseite, Forschung, Industrie und Lehre bilden zu können. Auch weiterhin steht AFCEA Bonn e.V. mit seinem ehrenamtlichen, gemischten Team des Vorstandes und der bewährten Zusammenarbeit mit ZVEI und BITKOM Ihren Wünschen und Anregungen wie stets offen gegenüber. Ich möchte Sie ermuntern, ganz im Sinne einer breiten Nutzung der Social Media uns noch stärker Ihre Auffassungen und Kommentare zugänglich zu machen.

Lieber Leser, in diesem Sinne wünsche ich Ihnen viel Vergnügen mit der Lektüre dieses Heftes und sehe den Gesprächen mit Ihnen z.B. anlässlich unserer Fachausstellung, unserer Fachtagung oder unserer Fachveranstaltungen in Bonn, Köln, Koblenz oder Berlin mit Freude entgegen.

Wir von AFCEA Bonn e.V. stehen zu Ihren Diensten!

Die Neuausrichtung der Bundeswehrplanung als Dienstleistung und Steuerung für die Bundeswehr

Generalmajor Dr. Ansgar Rieks, Vorstand AFCEA Bonn e.V.

Generalmajor Dr. Ansgar Rieks

Im Zuge der Neuausrichtung der Bundeswehr ist Steuerung eine wesentliche Dienstleistung, die durch die neue Planung in der Bundeswehr erbracht wird. Steuerung bedeutet entscheidungsorientiertes und zukunftsbezogenes Handeln, das dem Erreichen von Zielen dient. Es ist ein Gestaltungsauftrag.

Es sind im Wesentlichen drei Entwicklungen, die eine Neuausrichtung der Bw erforderlich machten: Die Verstetigung der Sicherheitslage in Europa, die in den Einsätzen gemachten Erfahrungen und das Neue Strategische Konzept der NATO. Daneben hat die Lagefeststellung und Analyse im Vorfeld der Neuausrichtung aber auch ergeben, dass Organisation und Prozesse der Bundeswehr für die Auftragserfüllung angepasst werden müssen. Deshalb wurde u.a. der Planungsprozess neu gestaltet.

Bisher waren Bundeswehrplanung, Haushalt und Controlling drei getrennt ablaufende Prozesse mit unterschiedlichen Datenerhebungen. Das Vorgehen in den jeweiligen Prozessen war nicht immer zielgerichtet aufeinander abgestimmt, was meist zu langwierigen Abstimmungsprozessen führte. Im Integrierten Planungsprozess, kurz IPP, wurden nunmehr diese drei Prozesse zusammengeführt. Damit werden die Bereiche strategische Zielsetzung, mittelfristige Planung und Fähigkeitsentwicklung sowie die Aktivitäten zur Aufstellung des Haushaltes eng miteinander verbunden und von Anfang an in Einklang gebracht. “Planung für die Bundeswehr” im Zuge des IPP orientiert sich damit noch stärker am Machbaren. Durch mehrere “Filter” im Sinne schrittweiser eingrenzender Bewertungen erfolgt eine an Zielen und Mitteln ausgerichtete Priorisierung. Bereits sehr früh wird identifiziert, welche Maßnahmen finanziell realisierbar sind und folglich weiter betrachtet werden. Die Neugestaltung des planerischen Prozesses für die gesamte Bundeswehr im IPP führt zudem zu klaren Zuständigkeiten und zu einer Reduzierung von Schnittstellen. Der Abteilungsleiter Planung verantwortet das für die Aufgabenwahrnehmung erforderliche Handlungs- und Leistungsvermögen der Bundeswehr und plant die zu dessen Erreichung erforderlichen Maßnahmen. Die Ressourcenabteilungen sind für die Bereitstellung der benötigten Ressourcen zuständig.

Der Integrierte Planungsprozess ist darauf ausgelegt, die drei Fragen der Planung zu beantworten: Die Zukunftsentwicklung beschreibt das “Was?”, das Fähigkeitsmanagement das “Wie?” und die Planungsumsetzung das “Womit?” Konsequenterweise sind auch die Strukturen der Abteilung Planung und das Planungsamt der Bundeswehr für diese Dienstleistung ausgerichtet.

Die Zukunftsentwicklung gewährleistet eine permanente Anpassung an ein sich schnell änderndes strategisches Sicherheitsumfeld als kontinuierlicher zielgerichteter Prozess zur Gestaltung und Weiterentwicklung der Bundeswehr. Hierbei werden aus unterschiedlichen Perspektiven Maßnahmen zur Weiterentwicklung des Handlungsvermögens der Bundeswehr entwickelt. U.a. werden Initiativen und Impulse zur Weiterentwicklung aus der Truppe und den Einsätzen systematisch aufgegriffen. Hier kann sich auch die Wirtschaft und Industrie mit ihren Erkenntnissen und Vorschlägen einbringen. Dann erfolgen eine ministerielle

AFCEA Fachausstellung 2012 – Vizeadmiral Rühle und Generalmajor Dr. Rieks auf dem Stand der BWI

AFCEA-Schulförderung – Generalmajor Dr. Rieks und Herr Reinhardt (Mitte) mit Lehrern und Schülern des Bornheimer Alexander-von-Humboldt-Gymnasiums

konzeptionelle Bewertung sowie die Prüfung der Aufnahme in die neu eingerichtete Mittelfristplanung. Nach Erfüllung dieser Kriterien werden daraus Projekte für die Planung und Bedarfsdeckung entwickelt. Das gesamte Leistungsprofil der Bundeswehr wird planerisch einbezogen, d.h. die Fähigkeiten der Streitkräfte und die Kapazitäten des zivilen Bereichs.

Die Mittelfristplanung ist das verbindende Element zwischen den konzeptionellen Grundlagen und dem jährlichen Planungszyklus. Sie bildet ein Scharnier zwischen der Zukunftsentwicklung und dem Fähigkeitsmanagement sowie der Finanzbedarfsanalyse, Ressourcenplanung und Haushaltsaufstellung. Für die Steuerung setzt sie konkrete planerische Ziele für das Leistungsspektrum der Bundeswehr, insbesondere auch für die Fähigkeitsentwicklung und die Planungsumsetzung. Das Fähigkeitsmanagement zielt darauf ab, das für die Aufgabenwahrnehmung der Streitkräfte erforderliche Fähigkeitsprofil zu erreichen und dauerhaft zu erhalten.

Die Betrachtungen im Rahmen des Fähigkeitsmanagements erfolgen von Beginn an bundeswehrgemeinsam und ganzheitlich mit Blick auf alle Planungskategorien: Personal, Rüstung, Infrastruktur, Organisation und Betrieb. Die Planungskategorien werden dabei wesentlich stärker als bisher “miteinander” verknüpft.

Für die Streitkräfteplanung legen wir einen umfassenden Fähigkeitsbegriff zu Grunde. Entlang des bekannten Dreiklangs “Ziele – Wege – Mittel” setzen sich Fähigkeiten zusammen aus den Komponenten: Ziele, Funktionalitäten und Ressourcen. Diese Systematik wird klare Aussagen darüber ermöglichen, welche Aufgaben der Bundeswehr mit welchen Fähigkeiten und mit welchen zugeordneten Ressourcen hinterlegt sind – also auch, welcher finanzielle Aufwand betrieben werden muss, um bestimmte Aufgaben wahrnehmen zu können. Gleiches gilt für die Kapazitäten des zivilen Bereichs.

In der Planungsumsetzung greift die Finanzbedarfsanalyse einige Elemente des bisherigen Bundeswehrplans auf und ergänzt diese mit weiteren haushalterischen Aspekten. Die mittel- bis langfristigen Aspekte des ehemaligen Bundeswehrplans werden durch die Mittelfristplanung aufgegriffen. Die Planungsumsetzung führt die erforderlichen Daten frühzeitig in einer gemeinsamen, konsistenten Datenbasis zusammen. Abschließendes Produkt ist der Ressourcenplan. Er wird in Detaillierung und formaler Gestaltung so entwickelt, dass er den technischen Anforderungen einer titelscharfen Gesamtanmeldung zum Haushalt entspricht. Haushalts-, Finanz- und Ressourcenplanung erfolgen aus einer Hand.

Alle für die spätere Aufstellung des Haushalts erforderlichen Informationen liegen somit zentral, umfassend, transparent und nachvollziehbar für die Prozessbeteiligten bereit. Eine gemeinsame, einheitliche Datenbasis für alle Prozessanteile über den gesamten Bearbeitungszeitraum bis zum Haushaltsvoranschlag stellt dies sicher. Der IPP umfasst damit als ganzheitlicher Planungsprozess den Weg von der Idee bis zur Umsetzung im Haushalt und parallel die Begleitung durch das Controlling.

Deutschland benötigt einsatzbereite und bündnisfähige Streitkräfte. Ein wesentliches Gestaltungselement hierfür ist die im IPP neu ausgerichtete Planung für die Bundeswehr. Es geht darum, die Kräfte auf die relevanten Aufgaben zu konzentrieren. Auf weniger Relevantes wird verzichtet. Im Kern kommt es darauf an, die Bundeswehr schlanker, robuster und effizienter zu machen. All dies dient dem gesamtplanerischen Ziel, die Einsatzfähigkeit der Bundeswehr zu verbessern. Wesentliche Leistung der Planung ist es, konkrete Schritte zu diesem gesamtplanerischen Ziel zu entwickeln und dafür die Steuerung vorzugeben. Dabei kommt es darauf an, im vorgegebenen Rahmen gestalterischen Handlungsspielraum zu schaffen und zu nutzen. Im Fokus stehen gleichermaßen die Fähigkeiten der Streitkräfte und die Kapazitäten des zivilen Bereichs, also das gesamte Leistungsspektrum der Bundeswehr. Gleichzeitig wird dadurch ein wesentlicher Beitrag zur langfristigen Sicherheitsvorsorge geleistet. Mit dieser Dienstleistung trägt die Planung wesentlich dazu bei, der Politik in einem wenig vorhersehbaren sicherheitspolitischen Umfeld vielfältige Handlungsoptionen zu bieten, der Rolle und Verantwortung Deutschlands in den Bündnissen gerecht zu werden und für unsere Bündnispartner ein verlässlicher Partner zu bleiben.

Das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) – Ein neuer Gesamtverantwortlicher auch für die IT der Bundeswehr

Hans-Ulrich Schade, Direktor BAAINBw, Vorstand AFCEA Bonn e.V.

Hans-Ulrich Schade

Die im Rahmen der Neuausrichtung der Bundeswehr beauftragte Schaffung eines neuen effizienten und einheitlichen Ausrüstungs- und Nutzungsprozesses mit der Vorgabe, die Beschaffung und die Materialverantwortung für die Einsatzreife in einem zentralen Ausrüstungs- und Nutzungsamt zusammen zu führen, hat zu erheblichen aufbau- und ablauforganisatorischen Veränderungen in den Organisationsbereichen der Bundeswehr geführt.

Auf der Grundlage konzeptioneller Überlegungen zum neuen Ausrüstungs- und Nutzungsprozess wurden die Verfahrensbestimmungen für die Bedarfsermittlung, Bedarfsdeckung und Nutzung in der Bundeswehr – der novellierte CPM (Costumer Product Management) – erarbeitet.

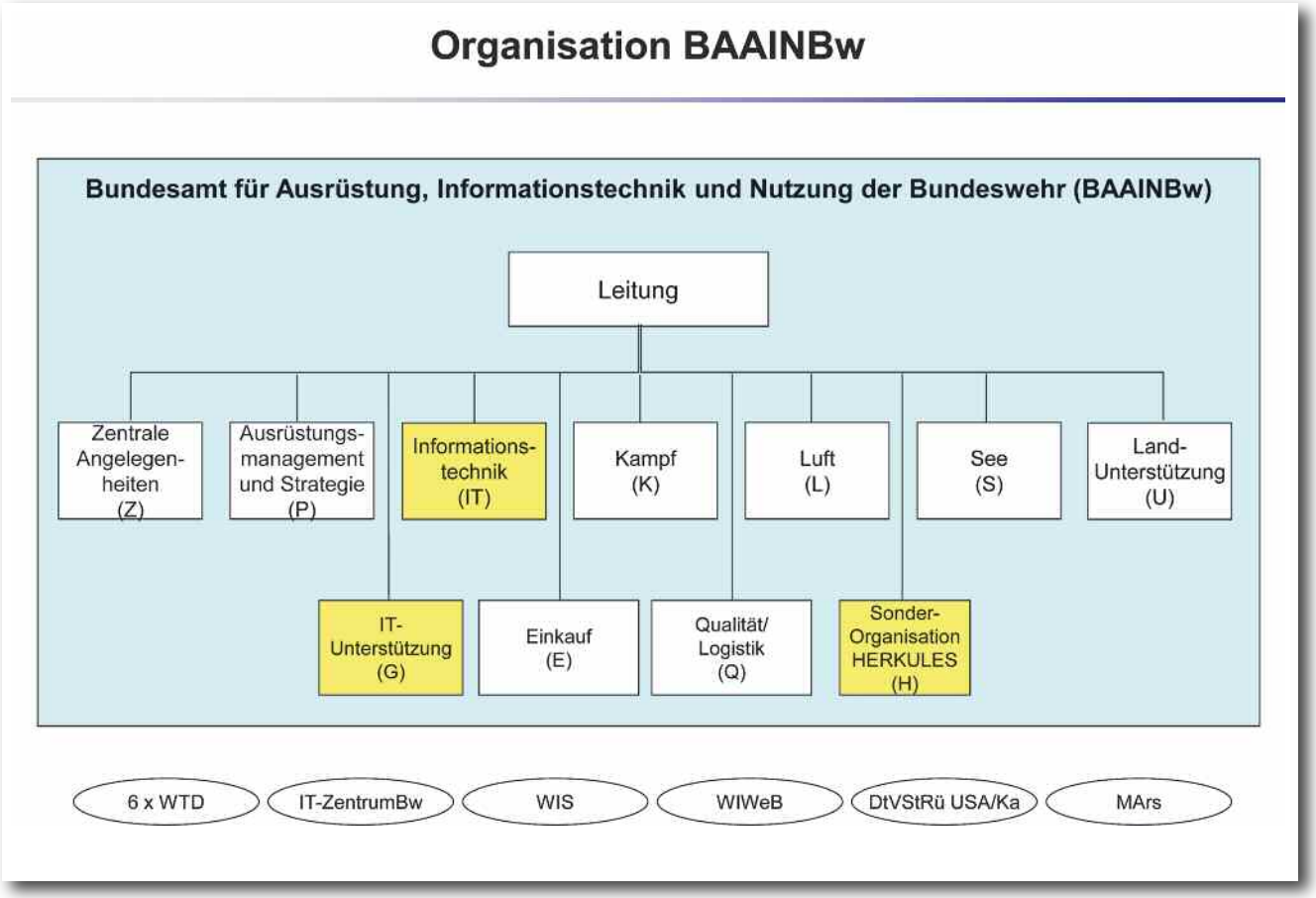
Wesentliche Merkmale des am 1. Januar 2013 in Kraft gesetzten novellierten CPM sind:

- drei statt vier Phasen, nämlich Analysephase, Realisierungsphase und Nutzungsphase,
- Einrichtung von Integrierten Projektteams (IPT) während des gesamten Lebenswegs von Produkten und Dienstleistungen,
- klare Trennung zwischen ministeriellen Steuerungs- und ämterseitigen Durchführungsaufgaben,
- eindeutige Zuordnung von Verantwortlichkeiten und Entscheidungskompetenzen mit einer deutlichen Stärkung der Position des Projektleiters,
- weitgehender Verzicht auf umfängliche Phasendokumente und Mitzeichnungsgänge,
- deutliche Reduzierung der Schnittstellen bei Bedarfsermittlung, Bedarfsdeckung und Nutzung,
- Wegfall des Sonderverfahrens für “Einsatzbedingten Sofortbedarf” durch Integration entsprechender Maßnahmen in den neuen Ausrüstungs- und Nutzungsprozess als “Sofortinitiative für den Einsatz”.

Parallel zur Erarbeitung dieser prozessualen Vorgaben wurden entsprechende aufbauorganisatorische Maßnahmen geplant und umgesetzt. In diesem Zusammenhang sind insbesondere die Gründung des Bundesamtes für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) zum 1. Oktober 2012 sowie die Aufstellung des Planungsamtes der Bundeswehr und der Kommandobehörden der Teilstreitkräfte zu erwähnen.

Vornehmlich das Zusammenspiel zwischen dem Planungsamt, dem im ersten Teil der Analysephase Verantwortung für die organisationsbereichsübergreifende Bedarfsermittlung zugeordnet ist, und dem BAAINBw, das die durchgängige Verantwortung von der Erarbeitung materieller Lösungen (Produkte, Dienstleistungen) über deren zeit- und kostengerechte Realisierung und Nutzungssteuerung – hier die Materialverantwortung für die Einsatzreife – bis hin zur Aussonderung und Verwertung von Wehrmaterial trägt, ist für den Erfolg des neuen Ausrüstungs- und Nutzungsprozesses von besonderer Bedeutung.

Die in meinem Artikel zur AFCEA Fachausstellung 2012 mit Planungsstand Februar 2012 dargestellte Organisation des BAAINBw mit zehn Abteilungen und einer Sonderorganisation wurde so in Kraft gesetzt. Demzufolge findet die IT organisatorisch insbesondere ihren Niederschlag in den Abteilungen Informationstechnik und IT-Unterstützung sowie in der Sonderorganisation HERKULES (siehe Abbildung). Dabei wurden alle Aufgaben der einsatzbezogenen IT-Systeme (Kommunikationssysteme, Führungsinformationssysteme) sowie Fachaufgaben der technologischen Weiterentwicklung, der IT-Sicherheit und Cyber Defence der Abteilung Informationstechnik (I) zugeordnet. Die Zuständigkeit für Aufgaben aus den Bereichen der Fachinformationssysteme –



Das neue BAAINBw und die besondere Rolle der Informations- und Kommunikationstechnik

einschließlich der Realisierung von SASPF – liegt in der Abteilung Informationstechnik-Unterstützung (G). Die IT-Ausstattung im Heimatland ist weiterhin Hauptaufgabe der Sonderorganisation HERKULES (H).

Weitere Aufgaben mit strategischer Ausrichtung im Umfeld der Informationstechnik (z.B. IT-System der Bundeswehr, Architekturen, Netzwerkbasierte Operationsführung, Interoperabilität) sind der Abteilung Ausrüstungsmanagement und Strategie (P) zugeordnet. Die waffensystembezogene Informationstechnik ist jeweils den Abteilungen Kampf, Luft, Land-Unterstützung und See zugeordnet, wobei die Abteilung P im Rahmen ihrer Zuständigkeit für das IT-System der Bundeswehr koordinierende Aufgaben wahrnimmt. Aktuelle Organigramme des Amtes und der Abteilungen sind auf der Homepage des BAAINBw unter www.baain.de zu finden.

Die ministerielle Fachaufsicht für die Aufgaben der Informationstechnologie liegt in der Unterabteilung IV der Abteilung Ausrüstung, Informationstechnik und Nutzung (AIN) im BMVg. Der Unterabteilungsleiter AIN IV ist zugleich IT-Direktor und IT-Sicherheitsbeauftragter der Bundeswehr. In letzterer Funktion wird er durch seinen Stellvertreter im BAAINBw – in Person des militärischen Vizepräsidenten des Amtes – unterstützt.

Die Einsätze der Bundeswehr sowie die rasche technische Fortentwicklung mit ihren immer kürzer werdenden Innovationszyklen machen schnelle und flexible aufbau- und ablauforganisatorische Rahmenbedingungen erforderlich. Der neue Ausrüstungs- und Nutzungsprozess sowie die neue gemischt zivil/militärisch besetzte Beschaffungsorganisation der Bundeswehr richten sich – auch im Bereich der Informationstechnik – konsequent an diesen Anforderungen aus.

Für AFCEA Bonn e.V. ist das BAAINBw mit seiner umfassenden Zuständigkeit – auch im Bereich der Informationstechnik – und seiner zivil/militärisch geprägten Kompetenz einer der wichtigsten Partner, um dem Anspruch als fachliches Forum und “Brückenbauer” zwischen Planern, Anwendern, Industrie und Wissenschaft im Umfeld der Informationstechnik gerecht werden zu können.

Das Fraunhofer-FKIE als Dienstleister für die Forschung und Entwicklung im Bereich ITK

Dr.-Ing. Michael Wunder, Vorstand AFCEA Bonn e.V.

Dr.-Ing. Michael Wunder

Das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie betreibt Forschung für Verteidigung, Sicherheit und Krisenreaktion. Stets geht es dabei um die Analyse, Entwicklung und Verbesserung von Technologien zur Erkennung, Aufklärung und Abwehr von Gefahren. So entstehen innovative Methoden und Verfahren für Informations- und Kommunikationssysteme, die ein gemeinsames Ziel verfolgen: Menschen im Einsatz unterstützen.

Mit über 350 Mitarbeitern arbeitet das FKIE in erster Linie für die Bundeswehr. Darüber hinaus werden Forschungs- und Entwicklungsvorhaben für zivile Sicherheitsbehörden und die Industrie durchgeführt. Die Entwicklung anspruchsvoller Methoden und Algorithmen zum Beherrschen sicherheitskritischer Prozesse steht dabei im Vordergrund.

Der Ursprung des heutigen Instituts liegt im Jahr 1963, als das Forschungsinstitut für Funk und Mathematik (FFM) innerhalb der Forschungsgesellschaft für Angewandte Naturwissenschaften (FGAN) gegründet wurde. Das FFM ging schließlich im Jahr 1999 nach einigen organisatorischen Anpassungen im heutigen FKIE auf. Seit 50 Jahren betreibt das Institut angewandte Forschung, es unterstützt seine Kunden bei Bedarf aber auch mit kurzfristigen Systemlösungen. Das Vorantreiben von Zukunftstechnologien bis zur Anwendungsnähe und die engagierte Mitarbeit in internationalen Gremien sind auch heute noch unverzichtbar für den Erhalt der Urteils- und Beratungsfähigkeit für die Bundeswehr. Im Jahre 2009 wurde das Institut nach einer vorausgegangenen Evaluation durch den Wissenschaftsrat der Bundesregierung in die Fraunhofer Gesellschaft aufgenommen. Damit verbunden ist eine weitere Öffnung der Forschungsleistungen für den zivilen Bereich. Dieser Prozess erfolgt aber so, dass die Identität des Instituts als Dienstleister für den Bereich Verteidigung und Sicherheit beibehalten wird. Dabei wird darauf geachtet, dass die F&T-Arbeiten sogenannte "Brückentechnologien" ermöglichen, also im Sinne eines "Dual-Use" für beide Anwendungsbereiche nutzbar sind.

Die bei der Auflösung der FGAN und Integration des Instituts in die Fraunhofer-Gesellschaft anfänglich herrschende Skepsis der Belegschaft ist schnell verschwunden, da sich die Bundeswehr als sehr starker und verlässlicher Partner zeigt und umfangreich auf die Forschungs- und Beratungsangebote des FKIE zurückgreift.

Das Institut ist in sechs hochspezialisierte Organisationseinheiten gegliedert, die je nach Projektanforderungen interdisziplinär zusammenarbeiten. Wohltuend für alle Beteiligten ist dabei, dass im Institut ein über lange Jahre gepflegtes Klima des gegenseitigen Vertrauens herrscht – eine wesentliche Basis für zielgerichtete und ergebnisorientierte Kooperation zum Wohle des Kunden und nicht zuletzt auch wichtig für die Arbeitszufriedenheit der Belegschaft.

Alleinstellungsmerkmal des Instituts ist, dass es sowohl auf der Systemebene als auch an allen Stellen in der Verarbeitungskette bei Führungs- und Aufklärungssystemen substanzielle Beiträge leistet.

- Dabei wird die Erfassung komplexer Daten im Rahmen der Fernmeldeaufklärung unterstützt,

Forschungsstandort Wachtberg Quelle: Fraunhofer FKIE

Operationszentrale der Zukunft

- es werden Verfahren für deren effiziente und sichere Übertragung entwickelt,
- die Datenkonsistenz bei der Verteilung wird sichergestellt,
- es werden Daten zur Erzeugung von Lagebildern unter Einbeziehung komplexer Datenfusions- und Sprachverarbeitungsverfahren verarbeitet,
- Darstellungsmöglichkeiten, die auch unter schwierigen Einsatzbedingungen effektiv sind, werden untersucht,
- Soldaten werden bei der schnellen und sicheren Lageerfassung und Entscheidungsfindung unterstützt,
- Schutzmechanismen gegen Bedrohungen, die sich aus der digitalen Vernetzung ergeben, werden entwickelt und
- die technischen Grundlagen für den Einsatz von unbemannten Systemen in Situationen, die für Menschen extreme Gefahren bergen, werden geschaffen.

Bei allen Forschungsaktivitäten werden im Sinne eines "Technology Watch" verfügbare und sich entwickelnde Technologien beobachtet, ausprobiert und weiterentwickelt, sowie hinsichtlich der Nutzbarkeit für die Verteidigung und Sicherheit bewertet. Weiterhin werden Empfehlungen für vertiefende Forschungsarbeiten gegeben. Hilfreich dafür ist einerseits die enge Einbindung des Instituts in laufende Projekte bei der Bundeswehr und zivilen Organisationen sowie andererseits die Präsenz bei internationalen F&T-Aktivitäten, wie EU-Projekten, bei der EDA und bei der NATO-Science and Technology Organisation (STO, ehemals RTO). Die intensivsten Verbindungen hat das FKIE dabei mit der NATO STO. Die Institutsmitarbeiter sind als deutsche Vertreter in mehreren Panels, mehrheitlich im Information Systems Technology Panel (IST), als Mitglieder in Arbeitsgruppen oder deren Leiter tätig und so auch in der Lage, im internationalen Kontext eine Standortbestimmung bei der wehrtechnischen F&T vorzunehmen.

Natürlich muss noch erwähnt werden, dass zahlreiche Mitarbeiter des Instituts seit den Anfangszeiten von AFCEA Bonn e.V. aktive Vereinsmitglieder sind und auf vielen AFCEA Veranstaltungen ihre Fachbeiträge geleistet haben. In dem Viererdiskurs (von Nutzer, Bedarfsdecker, Industrie und Wissenschaft) unterstützen sie damit eine der vier Säulen von AFCEA.

Stärken Sie Ihre Stärken.

Ein starker Bündnispartner: HP hält Ihnen den Rücken frei.

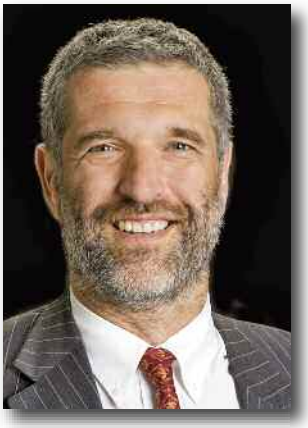
Mit dem Know-how des weltweit größten Technologieanbieters sind Sie bestens für Ihre Anforderungen gerüstet. Modernste Technologien und Services unterstützen Sie dabei, Ihre Einsatzfähigkeit, Mobilität und Verlegefähigkeit zu verbessern. Setzen Sie auf bedarfsgerechte Lösungen nach Maß und die langjährige Erfahrung eines Spezialistenteams, bei dem jeder Handgriff sitzt!

Besuchen Sie uns auf der AFCEA am 24./25. April 2013, Stand K4 (kleiner Saal).

Kontakt:
germandefence@hp.com

Die NATO Communications & Information Agency – einer neuer Ansatz für IT-Dienstleistungen der NATO

Wolfgang Taubert, Vorstand AFCEA Europe und Regional Vice President Central Europe AFCEA International



Wolfgang Taubert

Die NATO Reform schreitet voran. Im Jahre 2010 haben die 28 NATO Nationen und der NATO Generalsekretär die Richtung vorgegeben – kleiner, effektiver und effizienter (und ein wenig sparsamer natürlich) soll es werden. Zwanzig Prozent Einsparung bei einer Steigerung des Servicelevels steht auf dem Wunsch-(besser Vorgabe-)zettel der Nationen. Ein Schwerpunkt ist dabei der Bereich Informationstechnik – deren Entwicklung, Beschaffung und Betrieb.

Deutlich mehr als 50% der NATO Investitionen gehen in den erweiterten Bereich der Informationstechnik – C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance). C4ISR ist der Stoff (besser Klebstoff – "glueware"), der die NATO technisch zusammenhält. Im wesentlichen definiert sich die NATO bekanntlich über die nationalen Beiträge ihrer Mitglieder. C4ISR ist hierbei die große Ausnahme von der Regel.

In der Vergangenheit haben fünf Einrichtungen die IT-Leistungen für die NATO bereitgestellt – die NC3A[1.)], NACMA[2.)], und das BMD[3.)] Programme Office für den Projektbereich und die NCSA[4.)] sowie ICTM[5.)] für den IT-Betrieb. Seit dem 1. Juli sind diese fünf Einrichtungen Geschichte und Teil der neuen NATO Communications & Information Agency (NCI Agency). Aber zuerst zum Stichwort Größe – die fünf Einrichtungen haben etwa 3.800 Dienstposten an 34 Standorten eingebracht. Die Projektarbeit an den zentralen Standorten Brüssel, Den Haag, Mons und Glons wird von zivilen Mitarbeitern, der Betrieb an den dezentralen Standorten von militärischen dominiert.

Eine weitere Herausforderung ist die Kombination von fünf sehr unterschiedlichen Kulturen und Geschäftsprozessen. Zusammenlegung und daraus resultierende Größe ist nun kein Garant für Effektivität und Effizienz. Das Ganze erscheint als wahrlich herkuleanische Aufgabe. Jede Reform dieser Dimension bedarf eines oder besser mehrerer "game changer". Einfach weiter so mit neuen Namen aber vergleichbaren Prozessen, Strukturen und Personal führt lediglich zur Neudekorierung der Schaufenster. "Game changer" im Sinne der Reform der NATO IT sind zwei Dinge – voller Lebenszyklussupport und ein kundenfinanziertes Finanzregime (customer funding).

NCI Agentur Mitarbeiter bei ISAF *Quelle: NCI Agency – Creative Media Centre*

Die IT-Unterstützung der NATO war vor der Reform strikt unterteilt in so etwas wie Bedarfsträger und Bedarfsdecker. Der neue Ansatz einen lebenzyklusübergreifenden Ansatz zu implementieren, ist aus Sicht der Bundeswehr keine überraschende und neue Entwicklung. Die Herausforderungen, bei der NATO dies zu realisieren, liegen sehr stark in den bestehenden Genehmigungs- und Finanzierungsprozeduren. Diese sind traditionell stark auf Einzelprojekte und deren Investitions- und Betriebsmittel orientiert.

Das Prinzip der Kundenfinanzierung

ist für die Bundeswehr terra incognita. Die meisten NATO-Agenturen werden aus dem allgemeinen NATO-Haushalt finanziert (28 Nationen, “common funded”) – das entspricht im wesentlichen den Finanzierungsprinzipien einer deutschen Behörde – jährliche Mittelzuweisung. Zwei[6.)] der alten NATO Agenturen verfügten über ein sogenanntes Kundenfinanzierungsmodell (“customer funded”) – die finanziellen Mittel liegen bei den Kunden (Hauptquartiere, Nationen) und werden bei Projektauftrag bzw. Projektende den Agenturen überwiesen. Diese wiederum begleichen alle ihre Ausgaben (Gehälter, laufender Betrieb, Dienstreisen, …) aus einem Aufschlag auf die Projektkosten. Das erlaubt Flexibilität und führt zu Leistungsdruck. Mangelhafte oder unpünktliche Projektarbeit und folgerichtiges Ausbleiben von “Folgeaufträgen” führt konsequent zu Defiziten im Budget der entsprechenden Agentur. Die Konsequenzen sind (nicht nur theoretisch) die Kürzungen bei Personal und anderen Ausgaben. Die ehemalige NC3A war nach diesem Prinzip finanziert. Die Nationen haben entschieden, dass die neue NATO Communications & Information Agency das als effizient und effektiv bewährte Prinzip des “customer funding” anzuwenden hat.

Die NCI Agentur ist nunmehr im zehnten Monat ihrer Existenz und hat im Januar 2013 ihre Zielstruktur eingenommen. Die Hauptaufgaben liegen im Augenblick in den Bereichen

- ISAF-Unterstützung (Projekte wie AMN – Afghanistan Mission Network und FMN – Future Mission Network)
- Raketenabwehr – das NATO BMD (Ballistic Missile Defence) Programm;
- Cyber Defence
- Joint ISR
- IT Unterstützung für die NATO Kommandostruktur und das NATO Hauptquartier.

Major General (rtd) Koen Gijsbers, General Manager NCI Agency

Synergieeffekte mit der Bundeswehr liegen auf der Hand – Projektergebnisse der NCI Agentur “gehören” allen 28 NATO Nationen und können von diesen frei genutzt werden. Um diesen Prozess zu vereinfachen und zu beschleunigen, hat

Übergabe Erstbefähigung Raketenabwehr – u.a. MajGen (ret) Sandro Pera (NCI Agentur, Programm Direktor NATO BMD) und Generalleutnant Dieter Naskrent.

Quelle: NCI Agency – Creative Media Centre

das BMVg und die NCI Agentur die Unterzeichnung eines Memorandum of Agreement (Rahmenvertrag) vereinbart.
Zum Abschluss noch einige Zahlen, um die Größenordnung der NCI Agentur zu verdeutlichen:

- aktuelle Anzahl Dienstposten – ca. 3.800; davon militärisch – ca. 2.200 und zivil – ca.1.600;
- aktuelle Mitarbeiterzahl – ca. 3.000; davon militärisch – ca. 1.600 und zivil – ca.1.400;
- aktuelle Anzahl deutsche Mitarbeiter – militärisch ca. 190 (ca. 12%) und zivil ca. 120 (ca. 8%);
- Anzahl Dienstposten in der Zielstruktur der NCI Agentur – ca. 2.500;
- Anzahl der Projekte – ca. 600;
- Jährliches Vergabevolumen – ca. 600 Mio. Euro (Anteil deutscher Auftragnehmer – unter 3%).

Angehörige der NCI Agentur unterstützen ISAF

Dieser kurze Steckbrief zeigt Größenordnung und Bedeutung der NCI Agentur im NATO Kontext. Die deutsche Präsenz bei Personal und insbesondere bei der industriellen Teilhabe liegt deutlich unter dem finanziellen Beitrag Deutschlands zur NATO (ca. 15%). Ein erhebliches Potential für deutschen politischen Einfluss auf Dinge wie Cyber Defence und Raketenabwehr, für die Präsenz von deutschem Personal und zu guter Letzt für die Teilhabe deutscher Industrie liegen auf der Hand. Durch eine verstärkte Kooperation hat die Bundeswehr ein klares Gewinnpotenzial. Die NCI Agentur wird im Rahmen der Umsetzung der NATO Reform effizienter und effektiver werden – das Prinzip der Kundenfinanzierung bietet hierfür klare Anreize jenseits politischer Rhetorik. Für die Bundeswehr wird sich der Trend einer strategischen Partnerschaft verstärken – es geht zunehmend weniger um ausschließlich Geben (Ressourcen) als um ein Geben und Nehmen (Partizipieren an und Übernahme von strategischen Projekten wie AMN, FMN, BMD und ICC).

1.) NATO Consultation, Command and Control Agency

2.) NATO Air Command and Control Management System Agency

3.) Ballistic Missile Defence

4.) NATO Communication and Information Systems Services Agency

5.) NATO HQ Information and Communication Technology Service

6.) NC3A und NAMSA

Wandler zwischen den Welten – Nutzerakzeptanz als Ausgangspunkt für SOA

Hartmut Jäschke, Mitglied der Geschäftsleitung und Vice President Marketing & Sales, Thales Deutschland; Vorstand AFCEA Bonn e.V.

Hartmut Jäschke

Viele IT-Systeme verstehen einander einfach nicht. Und der Nutzer noch weniger. Warum der Ausgangspunkt für serviceorientierte Architektur (SOA) der Nutzer sein muss.

Über die Philosophie des Fortschritts in der Informationstechnik und Vernetzung zu sprechen oder zu schreiben, ist im Grunde überflüssig. Die dem Nutzer nahen Systeme, ob Computer, Smartphones, Tablets oder sogar Haushaltsgeräte, sind omnipräsent. Es ist für Experten wie auch für gewöhnliche Nutzer ein rasanter Prozess, der neue Wege findet und neue Pfade ebnet. Aber alles funktioniert (meist) irgendwie miteinander.

Dieser Fortschritt ist aber nur auf den ersten Blick von der Technologie und der zu Grunde liegenden Architektur getrieben – Hardware, Netzwerken, Protokollen. Denn es ist in Wirklichkeit der Nutzer, der hier kräftig treibt und seinen Informationsraum ständig ausdehnt. Und zwar durch seine Akzeptanz und die Bereitschaft, die vorhandenen Systeme zu nutzen, auszuprobieren und auch neu zusammenzufügen. Die jüngere Geschichte besteht natürlich nicht nur aus solchen Erfolgen, sondern ist auch voll von gescheiterten oder schnell vom Markt verschwundenen Ideen. Aber nicht, weil diese technisch schlecht waren. Sondern, weil sie nicht die volle Nutzerakzeptanz fanden. Informationstechnik kommt nur zur Wirkung, wenn sie Mehrwert bringt und gleichzeitig auch angenommen wird. Sie ist nämlich längst keine Herrschaftswissenschaft mehr, die in abgeschotteten Spezialistenzirkeln mit Schnittstellendogmen praktiziert wird – die Einbindung der (End)anwender in die in der Regel IT-technologielastigen Projektorganisationen tut dringend Not.

Etwas setzt sich durch, wenn es die breite Nutzerschaft wirklich will und mitmacht. Und zwar mit der Bereitschaft, ständige Updates und Produktwechsel zu durchleben – "Never change a running system" kann in Zeiten tausender Apps mit praktisch täglichen inkrementellen Updates und Funktionserweiterungen kein Dogma mehr sein.

Das gilt bislang für die private und in Grenzen auch kommerzielle Nutzung von vernetzter Informationstechnik. Im Bereich von Sicherheit und Verteidigung sowie bei zivilen kritischen Großsystemen und Entscheidungsketten sieht das (noch) ganz anders aus. Das Beharren auf stark spezialisierten, unabhängig eingeführten, intensiv erprobten Systemen und Strukturen hat hier einen guten Grund: alles muss für sich reibungslos und verlässlich jederzeit funktionieren. Denn von jedem dieser einzelnen Systeme hängen wichtige Entscheidungsketten, Güter und sogar Menschenleben ab. Geändert wird hier oft nur, wenn es nicht mehr anders geht. Realistisch betrachtet kann das Auseinanderdriften dieser beschriebenen beiden Welten auf Dauer nicht gut gehen. Nutzerakzeptanz entsteht neben anderen Aspekten vor allem aus der Leichtigkeit von Zugang und Bedienung und natürlich dem Mehrwert der Dienste und Systeme. Es ist nicht nur das "ob", es ist immer mehr auch das "wie". Und hier gibt es eine Menge Nachholbedarf in den Bereichen Sicherheit und Verteidigung. Die rasante Verbreitung von Weboberflächen mit hochauflösenden Multi-Touchscreens hat breitbandig einen Wandel an der Mensch-Maschine-Schnittstelle und einen Zugang zu komplexesten Funktionen gebracht. Weder Kommandozeile noch durchdachteste Menümasken ermöglichten jemals eine so sichere gleichzei-

AFCEA-Fachausstellung 2012 – Wichtiger Besuch auf dem Thales-Stand

Die Koblenzer IT-Tagung – seit vielen Jahren ein Highlight des AFCEA-Programms

tige Information und Bedienung auch in komplexen Situationen.

Nicht nur zur Gewinnung und Überzeugung von Nutzern und Bedienern, sondern auch bei der effizienten Aggregation von Informationen aus bisher inselartigen Systemen spielen diese technischen Verbesserungen eine entscheidende Rolle. Deshalb müssen sie auch in kritische und komplexe Systeme Einzug halten. Und zwar zügig.

Und hier kommt die Serviceorientierte Architektur (SOA) ins Spiel. Stark vereinfacht zieht SOA eine Abstraktionsebene ein, die als Wandler, Vermittler und Steuermann zwischen den Welten wirkt. Nämlich zwischen den existierenden inselartigen, spezialisierten und in ihren kritischen Funktionen hochsicher ausgelegten Systemen sowie der Bedien-, Darstellungs- und Prozessebene. Dafür braucht an den bestehenden Systemen nicht einmal etwas geändert werden. Mehr noch: Sie können später sogar ausgetauscht und aktualisiert werden, ohne das Gesamtsystem oder andere Inseln zu stören. Über die Abstraktionsebene werden sie angebunden an die moderne Bedien- und Darstellungsebene sowie an die komplexen Prozessabläufe – und bleiben dennoch gekapselt. Das bringt vielfachen Mehrwert: Auswahl und Zulassung werden vereinfacht, Kosten reduziert und das Gesamtsystem lässt sich so schrittweise modern halten. Als Nebeneffekt kommt eine Trainings- und Simulationsmöglichkeit mit echten Systemfunktionen im Offlinebetrieb hinzu.

Möglich machen dies neben der SOA-Philosophie zwei Komponenten: der Systemaufsatz (SOA connector), der zwischen der System- und der protokollkonformen SOA-Umgebung wandelt, sowie der Applikationsserver als orchestrierendes Prozesssteuerungselement. Thales Deutschland hat hier mit dem Hypervisor als Plattform für die Formatierung der Informationen und zur Vereinheitlichung von Entscheidungsabläufen anhand existierender Einsatzregeln schon einige Zeit eine solche übergreifende Lösung mit eingebauter Sicherheitsarchitektur entwickelt, die zivil wie militärisch Anwendung findet.

Bei dem SOA Framework und den Services des Hypervisors beginnend, lässt sich eine Parallele zu den Vorhaben “Einsatzunterstützender Systemverbund Aufklärung Führung Wirkung” (EiS-A-F-W) und “Referenzumgebung Dienste” (RuDi) der Bundeswehr ziehen. Ziel von EiS-A-F-W ist es, einen auf den Bedarf der Bundeswehr zugeschnittenen Systemdemonstrator detailliert zu entwerfen, unter Nutzung der “Referenzumgebung Dienste” aufzubauen und dessen Nutzen nachzuweisen. RuDi ähnlich dem Thales Hypervisor, basiert dabei auf dem Open Source SOA-Framework Apache CXF. Der Systemdemonstrator EiS-A-F-W untersucht konkret einen streitkräftegemeinsamen, Führungsebenen übergreifenden Systemverbund unter Betrachtung der gesamten Funktionskette Aufklärung-Führung-Wirkung.

Wie aktuelle Einsatzerfahrungen zeigen, sind Erfassung, Bewertung und Priorisierung sowie die Informationsvermittlung schon in ruhigen Zeiten komplex und brauchen Konzentration. Im Einsatzstress ist diese Kette kaum noch zu bewältigen, so dass hier nicht noch komplizierte (Drehstuhl-) Schnittstellen stören dürfen. SOA kann hier als Bindeglied die Informationsverarbeitung der Einzelsysteme so zusam-

men wirken lassen, dass trotz voller Verlässlichkeit und hohem Meldeaufkommen nichts verloren geht und die wirklich wichtigen Dinge zuerst getan werden.

Mit Hilfe des Hypervisor erhalten komplexe Entscheidungsprozesse, die auf den Informationen unterschiedlicher Führungssysteme und Quellen beruhen, eine einheitliche Benutzeroberfläche. Vorteile sind Akzeptanz, Bedienung, Verständnis und Konzentration auf das Wesentliche. Wie das alles zusammen spielt, merkt der Nutzer nicht. Denn bei konsequenter SOA sieht er immer die ihm vertraute und gut trainierte Oberfläche mit den jeweils relevanten Informationen und Optionen.

Auch auf der taktischen Ebene bleibt das Prinzip wirksam: Hier sind oft viele Geräte in Nutzung, die gar keine IP-Funktionalität, geschweige denn Serviceorientierung, haben, weil sie nur für die Bedienung direkt durch den lokalen Nutzer ausgelegt sind. Beispiel Einsatzfahrzeug: Es trägt verschiedene Sensoren für Nachtfahren, Navigation, Feuerleitung mit jeweils eigenem Benutzerinterface. Funk- und Datenverbindungen bestehen auf Gruppen- und Zugebene mit wenig Bandbreite. Die einzelnen Geräte spielen derzeit wenig oder gar nicht zusammen und erfordern viel Denk- und manuelle Koordinationsarbeit, um die relevanten Lageinformationen allen Beteiligten zugänglich zu machen. TSBI, das Tactical Service Bus Interface von Thales, ermöglicht hier als militärischer “SOA-Connector in a Box” eine Interaktion solcher originär unabhängigen Systeme über eine schlanke Schnittstelle unter Verwendung von Web Services. Mit dem TSBI und der zughörigen Software-Entwicklungsumgebung können Hersteller ihre Geräte ohne Offenlegung der inneren Arbeitsweise und der externen Schnittstellen SOA-fähig machen, ohne sich selbst mit SOA befassen zu müssen. Damit erfahren bestehende und in ihren Teilen einfache, im Zusammenwirken aber sehr komplexe Plattformen eine erhebliche Steigerung der Fähigkeiten im Verbund der Systeme – bei spürbar vereinfachter Nutzung.

Dass das technische Prinzip der Service-Orientierung funktioniert und nutzbringend ist, hat der Einsatz im zivilen Umfeld auch in kritischen Anwendungen längst bewiesen. Und dass die Nutzerakzeptanz heute unabdingbar für den Nutzungserfolg ist, kann nicht mehr länger ignoriert werden. Wie beides aber in der sehr speziellen Welt von Sicherheit & Verteidigung umgesetzt werden kann, dass ist noch nicht geklärt. Bei konsequenter und stärkerer Verwendung des Instrumentes CD&E im Zusammenwirken von Nutzer und Industrie sollte eine erfolgreiche Umsetzung und Einführung aber schneller und einfacher als gedacht eintreten.

AFCEA Veranstaltungskalender 2013

21. Januar
Fachveranstaltung: Diensteorientierung in der IT – ein neuer Hype oder ein sinnvoller Ansatz?

28. Februar
Sonderveranstaltung BOS
Die Strukturen und der Technologiebedarf der deutschen Sicherheitsbehörden

08. März
AFCEA-Forum CeBIT 2013: Diensteorientierung in der IT – ressortübergreifende Nutzung von Services

25. März
Fachveranstaltung:
Diensteorientierung – aber mit Management

24. April
Young AFCEANs: Karrierestarterforum

24./25. April
Fachausstellung:
Symposium: IT-Services – Enabler in multinationalen Koalitionen

14. Mai
Info-Veranstaltung Young AFCEANs:
Bring Your Own Device – Ein unaufhaltsamer Trend?

24. Mai
Mittagsforum: AFCEA-Mitgliedsfirmen stellen sich vor

11. Juni
BOS-Tagung:
IT-Services für Polizeibeamte im Einsatz auf der Straße

27. Juni
Mitgliederversammlung AFCEA Bonn e.V.

04. Juli
Fachveranstaltung AFCEA/ZVEI/Bw: Diensteorientierung in der IT – unter dem Schirm der IT-Sicherheit

29. August
Koblenzer IT-Tagung 2013: IT-Serviceorientierung – wiederbelebter Hype oder Blaupause für die Bundeswehr?

23. September
Info-Veranstaltung Young AFCEANs:
Apps der öffentlichen Verwaltung – Dienste für mobile Anwendungen

11. Oktober
Mittagsforum: AFCEA-Mitgliedsfirmen stellen sich vor

23. Oktober
Zukunfts- und Technologieforum IT

18. November
Fachveranstaltung: MOTS-Store – der einfachere Weg?

III. Quartal
Gespräch im Park
Social Media

Bundesamt für Ausrüstung,
Informationstechnik und Nutzung der Bundeswehr

AFCEA Bonn e.V.
Anwenderforum für Fernmeldetechnik,
Computer, Elektronik und Automatisierung

IT-Serviceorientierung – wiederbelebter Hype oder Blaupause für die Bundeswehr?

Organisationen können nur in dem Maße auf die notwendigen Änderungen reagieren, wie die Informationstechnik (IT) diesen Änderungen folgen kann. Die Flexibilität einer Organisation steht damit in direktem Zusammenhang zur Flexibilität ihrer IT, d.h. zur Fähigkeit, die in der IT implementierten Prozesse und Funktionalitäten ändern zu können.
Daher werden heute auf der Grundlage einer Dienste- bzw. Serviceorientierten Architektur (SOA) vorhandene IT-Komponenten (Infrastruktur und Software) in Dienste aufgeteilt. So müssen im Falle einer notwendigen Änderung eines Geschäftsprozesses lediglich einzelne Glieder dieser Komponentenkette modifiziert oder ausgetauscht werden. Eine ggf. fehlerträchtige und teure Änderung eines gesamten IT-Systems oder einzelner Module wird damit vermieden. In einem Dienst werden die einzelnen IT-Komponenten soweit gekapselt, dass auch Dritte am Markt diesen anbieten oder nutzen können. Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Security as a Service oder Everything as a Service (XaaS) sind entsprechende Ausprägungen dieses Gedankens.
Auch die Bundeswehr setzt bei der Neu- und Weiterentwicklung von IT-Systemen auf die Diensteorientierung. Die IT-Strategie des BMVg macht hierzu klare Vorgaben. IT-Services sollen dabei je nach Einsatzanforderung so zusammengestellt werden, dass der Informationsbedarf flexibel und agil gedeckt werden kann. Die standardisierten Schnittstellen und Prozesse einer SOA sollen Dienste querschnittlich nutzbar machen und so zur gewünschten Flexibilität und Interoperabilität führen.
Wir möchten mit Ihnen bei unserer **Koblenzer IT-Tagung am 29. August 2013** über diese Serviceorientierung diskutieren. Wird dieser Ansatz die Lösung für die Zukunft sein oder erwarten wir zu viel? Wir laden Sie zu dieser Veranstaltung mit internationaler Beteiligung ein und freuen uns auf ein interessantes Programm sowie einen unterhaltsamen Abend mit der Möglichkeit zu vielen Gesprächen.

Ort:	Rhein-Mosel-Halle, Julius-Wegeler-Straße 4, 56078 Koblenz	
Zeit:	Donnerstag, 29.08.2013	09:00 – 18:30 Uhr
	mit “Koblenzer Abend”	18:30 – 21:00 Uhr
Teilnehmer:	Bundesministerium der Verteidigung; Kommandobehörden, Ämter, Dienststellen und Truppenteile der Bundeswehr; Behörden und Organisationen mit Sicherheitsaufgaben (BOS); Institute, Verbände; Universitäten und Fachhochschulen; Industrie mit Schwerpunkt Informations- und Kommunikationstechnik; internationale Gäste	
Fachl. Leitung:	Generalmajor Klaus F. Veit, Vizepräsident BAAINBw Brigadegeneral a.D. Reimar Scherz, Vorstand AFCEA Bonn e.V.	
Programm:	+ aktuelle Informationen unter www.afcea.de und www.baain.de	
Kostenbeitrag:	+ Eintritt: 75,- €	
	+ Öffentlicher Dienst und AFCEA-Mitglieder: Eintritt kostenfrei; es wird jedoch ein Betrag von 15,- € für die Verpflegung erhoben.	

Klaus F. Veit, Generalmajor
Vizepräsident BAAINBw

Erich Staudacher, Generalmajor
Vorsitzender AFCEA Bonn e.V.

AFCEA Bonn e.V., Borsigallee 2, 53125 Bonn, Tel.: 02 28 / 9 25 82 52, Fax: 02 28 / 9 25 82 53
BAAINBw, Ferdinand-Sauerbruch-Str. 1, 56073 Koblenz, Tel.: 02 61 / 4 00-2801, Fax: -41 05

Die IKT der BOS – Dienstleistungen für die Innere Sicherheit

Tobias Schönherr, Diplomingenieur und Polizeioberrat der Bundespolizei, Vorstand AFCEA Bonn e.V.

Tobias Schönherr

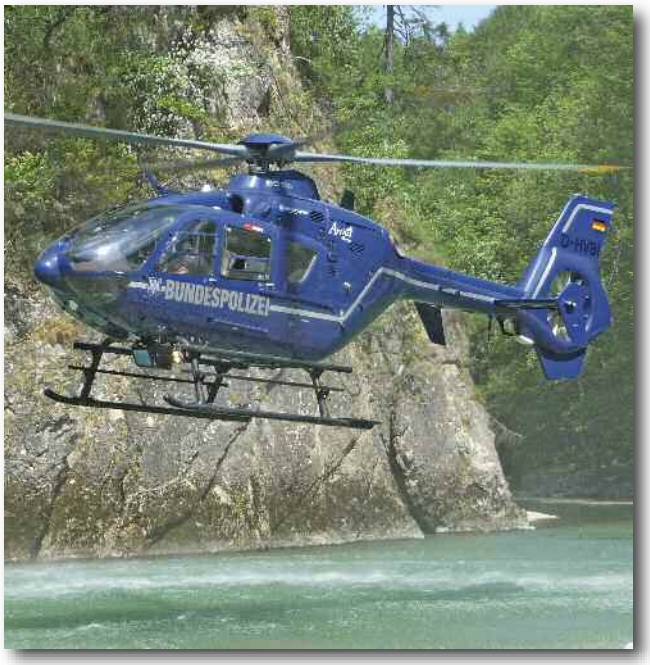
Bereits diese erste gewählte Überschrift ist ein Sinnbild unserer Zeit. Wenige Buchstaben enthalten Informationen, die für die Einen les- und verstehbar, für die Anderen nur ein weiteres Beispiel eines vermuteten Abkürzungswahns gewisser Institutionen sind. Um die hier zu behandelnde deutsche Polizei in den Fokus zu rücken, ist insbesondere das I aus IKT, also die Information, wichtig.

Das Ermittlerteam Thiel/Boerne im virtuellen Münsterland gewinnt seine Informationen medial wirksam zur Tatortzeit, wie auch richtige Streifenpolizisten oder besser Kontroll- und Streifenbeamte, für Eingeweihte: KSB, diese vielschichtigen Fakten sammeln, neu verknüpfen und natürlich, Teamfähigkeit beweisend, austauschen. Hoffentlich, und dies sollte der Polizei immanent sein, tun sie dies in der Majorität der Fälle nicht zur Verfolgung von Straftaten, sondern zur Abwehr dieser und aller anderen Gefahren, die einer Bevölkerung im Laufe der Zeit so begegnen. So ganz nebenbei war dies für alle Nichtpolizisten auch einer kurzer Abriss der Aufgaben der Polizei, Bildung findet ja bekanntlich immer statt.

Bereits in den letzten Jahren auch medial diskutiert, in den meisten osteuropäischen Mitgliedsstaaten der Europäischen Union auch dank Fördermitteln bereits verwirklicht, ist die digitale Kommunikation der Behörden mit Ordnungs- und Sicherheitsaufgaben (hier ist nun endlich Platz, das BOS aus der Überschrift zu erklären) ein wichtiger Schritt in die Zukunft der Kommunikation. Und dies heißt nicht, die Grimme-Preis verdächtigen Äußerungen von Thiel/Boerne audiovisuell zu übertragen, auch wenn dies der geistigen Belebung wie auch Zerstreuung dient, sondern vielschichtige Informationen und deren Ebenen miteinander zu verketten.

An dieser Stelle erreichen wir das T der Überschrift. Technologie wird zum Motor dieser Entwicklungen und damit auch der modernen Polizeiarbeit. Und es geht dabei nicht nur um die Nutzung von Digitalfunk, der in den Augen der meisten Kolleginnen und Kollegen der BOS und wohl auch in der derzeitigen Ausbaustufe, eine schwieriger zu handhabende Mischung aus altem Analogfunkgerät und dem geliebten eigenen Mobiltelefon für dienstliche Belange besteht.

Dazu ein Gedankenspiel: Nach einer Sensormeldung über den Ausfall einer kabelgestützten Signalverbindung an einer Schnellfahrstrecke der Deutschen Bahn begeben sich Polizeikräfte zum Ereignisort. Die hochauflösenden Bilder der in der Luft operierenden Observationsplattform, sei es ein Helikopter, ein Flugzeug oder auch eine unbemannte fliegende Station, werden nicht nur in der Einsatzzentrale, sondern auch in den bodengebundenen Fahrzeugen sowie auf persönlichen Unterarm- oder Hand-Displays der beteiligten Polizeibeamten empfangen. Zugleich wird jede Einsatzkomponente, “getrackt” durch in die persönlichen Kommunikationseinheiten integrierte Satellitenortungssysteme, in Echtzeit mit Bewegungsprognose dargestellt. Der Operator,



EC 135 im Gebirgseinsatz Quelle: Bundespolizei

EC 155 der Bundespolizei im maritimen Einsatz

Quelle: Eurocopter

früher Einsatzleiter, ist nun in der Lage, seine Kräfte per "drag and drop" zu dirigieren, also einfach mit dem Finger auf einem berührungsempfindlichen Display zu verschieben – der "angeklickte" Mann vor Ort erhält seinen Marschbefehl über eine Pfeildarstellung im Monokel, einem optischen Prisma vor seinem Auge, welches in Echtzeit die optisch wahrnehmbare Umgebung mit einer sensorischen Spektralerweiterung verknüpft. Die Ingewahrsamnahme zweier verdächtiger Personen, die es offensichtlich auf das Kupfer der Signalkabel abgesehen haben, ist nun nur noch eine Sache von Minuten. Interessante Bilder der Zukunft…

Auf dem Weg dorthin gibt es eine entscheidende Hürde zu minimieren: Die Polizei hat kaum Zeit, sich mit Technologien der Zukunft zu beschäftigen. Obwohl zahlenmäßig stärker als die sich in einer wichtigen Reform befindlichen deutschen Streitkräfte, ist die Einsatzlastigkeit der Personalstruktur zwar ein wichtiges Zeichen der Funktion im Sinne der Konzentration auf die tatsächliche Aufgabe von Gefahrenabwehr und Strafverfolgung. Dennoch sollte im Sinne der Zukunftsausrichtung strategisch ebenda investiert werden. Dass dies am besten gemeinsam funktioniert, zeigen viele andere Projekte und Einrichtungen, in denen Bund und Länder gemeinsam arbeiten.

Der Anspruch von AFCEA Bonn ist es, mit vielfältigen Veranstaltungen die begrenzten Ressourcen der Behörden mit Ordnungs- und Sicherheitsaufgaben, die innovative Kraft der deutschen Industrie und den Willen des Volkes, vertreten durch die Politik, zu bündeln.

Ein herzliches Willkommen zur AFCEA-Fachausstellung 2013 für alle Mitstreiter im Bereich der Inneren Sicherheit!

Der ZVEI – ein Industrieverband der Hightech-Branche für vernetzte Sicherheit

Oberst a.D. Friedrich W. Benz, Vorstand AFCEA Bonn e.V. und Betreuer der Gremien des Leitmarktes Defence im ZVEI-Fachverband Sicherheit

Friedrich W. Benz

AFCEA Bonn e.V. führt neben den bekannten eigenen Veranstaltungen auch "Sonderveranstaltungen" mit Verbänden, die einen hohen Bezug zu den AFCEA-Kernthemen haben, durch, wie z.B. mit dem ZVEI Zentralverband Elektrotechnik- und Elektronikindustrie e.V. Bei bisherigen Veranstaltungen mit starker Bundeswehrbeteiligung standen dabei "Taktische Kommunikation" (2010) und die "Auswirkungen des Afghanistan Mission Network (AMN) auf die FüInfoSys der Bundeswehr" (2011) im Mittelpunkt. Die nächste Veranstaltung von AFCEA Bonn e.V. mit dem ZVEI-Fachverband Sicherheit wird am 4. Juli 2013 mit dem IT-Zentrum Bundeswehr in Euskirchen unter dem Titel "Dienstorientierung in der IT – unter dem Schirm der IT-Sicherheit", durchgeführt, wobei auch das CERTBw vorgestellt werden wird.

Interessenvertreter der innovativsten Industriebranche Deutschlands

Der ZVEI ist einer der wichtigsten Industrieverbände Deutschlands. Er vertritt die Interessen einer Hightech-Branche mit einem sehr breit gefächerten und äußerst dynamischen Produktportfolio in Deutschland und auf internationaler Ebene.

Starke Mitgliedschaft

Mehr als 1.600 Unternehmen haben sich für die Mitgliedschaft im ZVEI entschieden. Sie beschäftigen rund 90 Prozent der Mitarbeiterinnen und Mitarbeiter der Elektroindustrie in Deutschland. Unter seinen Mitgliedern finden sich Global Player genauso wie Mittelständler und Familienunternehmen. Die Unternehmen der Elektroindustrie sind besonders innovativ. Etwa 40 Prozent ihres Umsatzes entfällt auf neuartige Produkte und Systeme. Grundlage dieser Innovationskraft sind die hohen Aufwendungen für Forschung und Entwicklung, im Jahr 2011 von insgesamt knapp 13 Milliarden Euro. Der ZVEI repräsentiert mit seinen 26 Fachverbänden und korporativen Mitgliedern eine Branche mit 178 Milliarden Euro Umsatz im Jahr 2011 und mehr als 840.000 Beschäftigten. Mit den noch einmal über 630.000 Mitarbeitern außerhalb Deutschlands ist die Wertschöpfung der Elektroindustrie am stärksten von allen Branchen global vernetzt.

Schrittmacher des Fortschritts

Grundlage der Verbandsarbeit ist der Erfahrungs- und Meinungsaustausch zwischen den Mitgliedern über aktuelle technische, wirtschaftliche, rechtliche und gesellschaftspolitische Themen im Umfeld der Elektroindustrie. Hieraus werden gemeinsame Positionen erarbeitet.

Vernetzung ist entscheidend für erfolgreiche Verbandsarbeit. Der ZVEI leistet diese in Frankfurt am Main, Berlin, Brüssel, Peking und in den Landesstellen; letztlich dort, wo der Stimme der deutschen Elektroindustrie Gehör zu verschaffen ist.

Mit Vorschlägen zur Forschungs-, Technologie-, Umweltschutz-, Bildungs- und Wissenschaftspolitik ist der ZVEI Schrittmacher des technischen Fortschritts. Er unterstützt eine marktbezogene internationale Normungs- und Standardisierungsarbeit. Getragen wird dieses Engagement von rund 150 Mitarbeitern im Hauptamt und über 5.000 Angehörigen der Mitgliedsunternehmen im Ehrenamt.

Enger Draht zur Politik: ZVEI-Präsident Friedhelm Loh und Bundeskanzlerin Dr. Angela Merkel

Themenfelder des ZVEI mit Berührung zu Bundeswehr und BOS

Übergeordnete Themen des ZVEI, wie z.B. Energieeffizienz; Embedded Systems und Elektromobilität haben bereits jetzt oder zumindest mittelfristig auch Auswirkungen auf die Bundeswehr und Behörden und Organisationen für Sicherheitsaufgaben (BOS).

In den mobilen Lösungen der Verteidigungs- und Sicherheitsindustrie hat das Thema Energieeffizienz zum Teil einen systembestimmenden Einfluss. Auch nutzen die komplexen Systeme der Verteidigungs- und Sicherheitsindustrie die Schlüsseltechnologie Embedded Systems erfolgreich bereits seit längerer Zeit. Bereits jetzt kristallisieren sich erste konkrete Lösungen der Elektromobilität für mittelfristig zu nutzende Produkte heraus.

Der Fachverband Sicherheit im ZVEI

Sicherheitsmärkte und Sicherheitstechnologien sind in stetigem Wandel. Der ZVEI hat der beschleunigten Entwicklung durch die Zusammenführung alle Aspekte der Sicherheit unter dem Dach des neuen Fachverbandes Sicherheit Rechnung getragen, um in der Gremienarbeit umfassend Synergien zu nutzen. Im Fachverband Sicherheit mit den Leitmärkten Safety, Security und Defence werden aktuelle Herausforderungen der Inneren/Öffentlichen Sicherheit aufgegriffen, wobei im Leitmarkt Security der Fokus des ZVEI auf den Bereichen des Bevölkerungs- und Katastrophenschutzes sowie Krisenmanagement, dem Schutz kritischer Infrastrukturen und öffentlicher Räume, der Überwachung und Kontrolle von Grenzen sowie der maritimen Sicherheit liegt. Im Leitmarkt Defence richtet sich der Blick auf die in Einsätzen festgestellten Fähigkeitslücken und den daraus entstehenden Ausrüstungsbedarf sowie die mögliche Industrieunterstützung im Einsatz im Bereich Logistik und IT. Cyber Security wird künftig als Querschnittsthema mit hoher Priorität bearbeitet.

Dem Begriff “Leitmarkt” liegt die Überzeugung zugrunde, durch Bündelung von Produkt- und Systemkompetenz erfolgreicher auftreten zu können. Dass mit der Überwindung der bisherigen Grenzen – auch zwischen Verbänden – und der gemeinsamen Themenbearbeitung in Leitmärkten der richtige Weg eingeschlagen wurde, zeigt die Wahrnehmung des Fachverbandes Sicherheit bei Amtsseite und Politik.

Sicherheit als Standortfaktor

Sicherheit ist Standortfaktor und – im Falle Deutschlands – Standortvorteil. Die deutsche Elektrotechnik- und Elektronikindustrie ist mit ihren innovativen Lösungskonzepten und ausgereiften Lösungen der leistungsfähige Partner für die Bewältigung der anstehenden Aufgaben. Wie keine andere Branche liefert die Elektrotechnik- und Elektronikindustrie Produkte und Lösungen, die das künftige Zusammenleben der Menschen wesentlich beeinflussen. Für die materielle Ausstattung der Bundeswehr, der Sicherheitsbehörden und zum Schutz (super)kritischer Infrastrukturen ist sie der Lieferant innovativer und robuster Lösungen. Als Schlüsselindustrie entscheidet sie zudem maßgeblich über die Zukunftsfähigkeit Deutschlands.

Events AFCEA Europe 2013

- **5th AFCEA Europe Student Conference:**
  27-29 May 2013, Military University of Technology, Warsaw, Poland
- **TechNet Europe 2013:**
  in cooperation with the European Defence Agency (EDA), the General Staff Polish Armed Forces and the Military University of Technology, Warsaw, 28-29 May 2013, Hilton Warsaw Hotel, Poland
- **TechNet International 2013:**
  organized in partnership with the NATO Communications and Information (NCI) Agency, Lisbon, Portugal, 23-24 Oct 2013
- **AFCEA Global Intelligence Forum:**
  Brussels, Belgium, 19-20 Nov 2013

www.afceaeurope.org

EUROPE'S EVENTS
SECURITY and DEFENCE

SECURITY: DISASTER MANAGEMENT
9th EUROPEAN CONGRESS ON CIVIL PROTECTION
Bonn, 18/19 Sept 2013
www.disaster-management.eu

Main Speakers at the last congress

Dr. Hans-Peter Friedrich, Minister, Federal Ministry of the Interior

Ueli Maurer, Head of the Federal Department of Defence, Civil Protection and Sports

Claus Sørensen, Director General, DG ECHO, Humanitarian Aid and Civil Protection, European Commission

SECURITY AND DEFENCE: BSC
BERLIN SECURITY CONFERENCE 2013 – 12th CONGRESS ON EUROPEAN SECURITY AND DEFENCE
Berlin, 26/27 Nov 2013
www.euro-defence.eu

Main Speakers at the last congress

Andrey Denisov, First Deputy Foreign Minister of the Russian Federation

Dr. Erato Kozakou-Marcoullis, Minister of Foreign Affairs of the Republic of Cyprus

General Patrick de Rousiers, Chairman of the EU Military Committee

SECURITY: POLICE
17th EUROPEAN POLICE CONGRESS
Berlin, 18/19 Feb 2014
www.european-police.eu

Main Speakers at the last congress

Noburo Nakatani, Executive Director IGCI, INTERPOL

Michèle Coninsx, President, Eurojust-Collegium

Troels Oerting, Assistant Director, Head of European Cybercrime Centre (EC3), Europol

Impressum: The European – Security and Defence Union
ProPress Publishing Group Bonn/Berlin

Information and participation contact:
Hartmut Bühl,
Behörden Spiegel Office Brussels
Avenue des Celtes, 30, B 1040 Bruxelles
Tel/Fax: +32 2 732 31 35, GSM: +49 172 32 82 319
E-Mail: hartmut.buehl@orange.fr

Helga Woll
Behörden Spiegel Office Bonn
Friedrich-Ebert-Allee 57, D 53113 Bonn
Tel/Fax: +49 228 97 09 70
E-Mail:helga.woll@behoerdenspiegel.de

www.behoerdenspiegel.de

Young AFCEANs – Die Digital Natives bestimmen die Zukunft!

Jochen Reinhardt, Ralph Michel, Katja Frintrop, Vorstand AFCEA Bonn e.V.

Jochen Reinhardt

Ralph Michel

Katja Frintrop

Geht es heutzutage um IT und deren Nutzung, unterscheidet man bei den Anwendern zwischen den "Digital Natives" und den so genannten "Digital Immigrants". Digital Immigrants ist ein Synonym für diejenigen, die in den letzten Jahren gelernt haben, mit der Informationstechnik und den Begleiterscheinungen, wie Social Media und Mobile Computing, umzugehen. Die Digital Natives sind diejenigen, die bereits damit aufgewachsen sind und die sich ein Leben ohne Smartphone, Tablet und Notebook bzw. PC nicht mehr vorstellen können. Also diejenigen, die sich darüber wundern, dass es Menschen gibt, die ihre Fernsehzeitschrift oder die Tageszeitung auf Papier gedruckt kaufen.

Diese Digital Natives bestimmen die Zukunft. Sie werden die Informationstechnik und den Umgang damit durch ihre Gewohnheiten beeinflussen und damit die Zukunft, bei der die Informationstechnik in der Bedeutung Rang zwei nach der Nahrungsaufnahme einnehmen wird. Diese Gruppe anzusprechen und attraktive Angebote zu machen, ist das Ziel der sogenannten Young AFCEANs – ein Forum für diese IT-affinen jungen und jung gebliebenen Mitglieder und Interessenten bis zum Alter von rund 40 Jahren. AFCEA Bonn e.V. bietet eigene Aktivitäten für Soldaten/innen und zivile Mitarbeiter/innen, die nach dem Studium auf IT- oder IT-nahen Dienstposten eingesetzt sind und für interessierte Studierende aber auch junge Fach- und Führungskräfte aus Bundeswehr, Industrie und BOS (Behörden und Organisationen mit Sicherheitsaufgaben) sowie aus der Wissenschaft.

Eine eigenständige Arbeitsgruppe Young AFCEANs (YA) organisiert seit Anfang 2012 die Veranstaltungen und Aktivitäten unter der Leitung von Jochen Reinhardt. Die Arbeitsgruppe Young AFCEANs steht allen engagierten Young AFCEANs offen, die sich in die Gestaltung von Aktivitäten einbringen wollen.

Das Programm besteht aus zwei Young AFCEANs Informationsveranstaltungen im Jahr mit Vorträgen, Diskussion und Netzwerkmöglichkeiten zu ausgewählten Fachthemen, die sich am Jahresthema von AFCEA Bonn e.V. orientieren und dieses aus dem Blick der Digital Natives betrachten.

Zusätzlich bringt das Young Leadership Forum junge Führungskräfte mit hochrangigen Führungskräften aus Bundeswehr, BOS, Industrie und Wissenschaft zusammen, um Erfahrungen und Tipps für den weiteren Karriereweg auszutauschen. Die Veranstaltung findet jedes zweite Jahr statt. Das Karrierestarter Forum, das im jährlichen Wechsel dazu stattfindet, bietet eine Plattform, auf der sich junge Fach- und Führungskräfte am Beginn ihres Berufslebens über ihre Erfahrungen und Erwartungen austauschen können und Tipps für einen gelungenen Start erhalten.

Unregelmäßig können zusätzlich Sonderveranstaltungen für Young AFCEANs dazu kommen, beispielsweise gemeinsame Aktivitäten mit Young AFCEANs der US-Chapter in Kaiserslautern/Ramstein und Stuttgart oder eine exklusive Führung über die jährliche AFCEA Fachausstellung in Bonn-Bad Godesberg.

Die Young AFCEANs bieten damit ein Netzwerk für junge Menschen, für die Informationstechnik in Beruf und Privatleben nicht mehr wegzudenken ist und die sich gerne über Möglichkeiten informieren und mit Gleichgesinnten austauschen möchten. Dabei wird bewusst "über den Tellerrand" geschaut und diskutiert, wie neue Entwicklungen und Trends in der Industrie z.B. im Bereich Social Media und

Mobile Computing auf den Dienst übertragen werden können bzw. könnten.

Der Anspruch der Young AFCEANs ist es auch, künftig Veranstaltungen zu organisieren, bei denen die "Alten", die in den oberen Ebenen der Hierarchie oft auch abgekoppelt von den Entwicklungen an der Basis sind, von den Digital Natives lernen können. Sei es beim Umgang mit Social Media oder bei der Risikoanalyse bei der Nutzung neuer Trends im täglichen Dienstbetrieb.

Machen Sie sich auf der AFCEA Fachausstellung ein eigenes Bild: Die Young AFCEANs treffen sich auch 2013 wieder zu einer exklusiven Führung.

AFCEA-Fachausstellung 2012 – Young AFCEANs auf dem Stand des Behörden Spiegel

Fraunhofer
FKIE

FRAUNHOFER-INSTITUT FÜR KOMMUNIKATION, INFORMATIONSVERARBEITUNG UND ERGONOMIE FKIE

Forschung für mehr Sicherheit

Cyber Security – Herausforderungen und Lösungsansätze

Prof. Dr. Peter Martini, Fraunhofer FKIE, Institutsleiter
Prof. Dr. Michael Meier, Fraunhofer FKIE, Leiter des Bereichs Cyber Security

Prof. Dr. Peter Martini

Prof. Dr. Michael Meier

Sehr geehrte Leserin, sehr geehrter Leser,

für diese Broschüre haben wir Kollegen von verschiedenen Fraunhofer-Instituten und von Behörden des Bundes und der Länder dazu eingeladen, ihre Arbeiten zum Thema Cyber Security vorzustellen. Mit den hier zusammengestellten Artikeln erhalten Sie einen Einblick in den Forschungsbereich Cyber Security im Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE, im Fraunhofer-Institut für Sichere Informationstechnologie SIT und im Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS. Wir betreiben wehrtechnisch relevante Forschung in der Informations- und Kommunikationstechnologie. Unsere Aufgabe ist, die Sicherheit von Netzwerken, von Daten und Kommunikation zu gewährleisten.

Entsprechend befassen sich die Beiträge in diesem Bericht mit der Prävention, der Erkennung und der Analyse von Angriffen aus dem Netz, sowie mit möglichen Reaktionen darauf. Maßnahmen der Behörden gegen Angriffe und wertvolle Eindrücke aus der Ermittlungsarbeit schildern drei Beiträge des Bundesamts für Sicherheit in der Informationstechnik (BSI), das Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) und des Landeskriminalamts NRW (LKA NRW).

Computer vor Angriffen durch Schadsoftware zu schützen, ist Gegenstand des Artikels zur Immunisierung mit Infektionsmarkern. Bei der Immunisierung gegen Schadsoftware wird eine bereits erfolgte Infektion des Systems vorgetäuscht, so dass dieses für Angreifer schlicht uninteressant wird. Ebenfalls mit Prävention beschäftigt sich der Artikel zu SEAMAN, in dem die Autoren ein neues Sicherheitsprotokoll für die Datenübertragung in mobilen und sich selbst organisierenden Kommunikationsnetzen (MANETs) vorstellen. Wie Daten mit digitalen Wasserzeichen geschützt werden können, ist Thema des Fraunhofer SIT. Was morgen für die Sicherheit von Energieversorgung, Telekommunikation und Internet oder Verkehrssysteme wichtig sein wird, ist Fokus des Beitrags “Neue Sicherheitskonzepte für Kritische Infrastrukturen der Zukunft” des Fraunhofer IAIS.

Gefahren aus dem Netz zu erkennen und zu analysieren, ist unter anderem das Thema des Beitrags von Chapman et al. Die Autoren analysieren den Netzwerkverkehr von infizierten Rechnern und finden dabei Merkmale, mit denen sich Botnetze identifizieren lassen. Ein weiterer Beitrag zur Erkennung und Analyse stellt ein kooperatives Monitoring-Modell zum Schutz kritischer Infrastruktur vor: Das Projekt MonIKA soll es Partnern ermöglichen, ihre Maßnahmen zur Sicherung von Infrastrukturen zu koordinieren. Weitere Beiträge zum Thema beleuchten die Disziplin der Sensordaten- und Informationsfusion im Kontext von Cyber Defense und die automatisierte Informationsauswertung aus offenen Textquellen; Benutzeraspekte und die Integration von Mensch und Technik stehen im Mittelpunkt eines Beitrags zur Human Systems Integration in Cyber Defense.

Kooperationen und Gegenmaßnahmen durch Bund und Länder sind Schwerpunkte der folgenden Beiträge: Was die Simulation einer bundesweiten Krise in LÜKEX 2011 für die praktische IT-Sicherheitsvorsorge bedeutet, erörtert Werner Baach vom BBK. Dr. Harald Niggemann (BSI) stellt die vom BSI und dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM e.V.) initiierte “Allianz für Cyber-Sicherheit” vor. Sie bietet eine Plattform für den Informations- und Erfahrungsaustausch zur Cyber-Sicherheit.

Einen wertvollen Einblick in die behördliche Ermittlungsarbeit gibt der Beitrag zur Prävention und Verfolgung der Cyberkriminalität im LKA NRW. Die Anzahl der Straftaten, die Cyberkriminalität zugeordnet werden, steigt weiter, während die Aufklärungsquote sinkt. Was können Behörden und Unternehmen tun, um die Aufklärung zu verbessern? Mit diesem Beitrag eröffnen wir unsere Reihe von Aufsätzen zum Thema Cyber-Sicherheit und wünschen Ihnen eine interessante Lektüre!

Prävention und Verfolgung der Cyberkriminalität im Landeskriminalamt (LKA) Nordrhein-Westfalen

Leitender Kriminaldirektor Markus Röhrl, Leiter Abteilung 4 im LKA NRW

Markus Röhrl

"Die Bedrohung für Unternehmen, etwa durch Hackerangriffe, ist weitaus größer als in der Öffentlichkeit wahrgenommen wird", sagte der Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Michael Hange, der FTD[1.)], die an diesem Tage mit der Schlagzeile aufmachte: "Deutschland steht kurz vor dem Internet-GAU". Und die meisten der in den vergangenen Monaten gezielt befragten deutschen Manager fürchten, dass das Problem für die deutsche Wirtschaft größer wird. Symantec sieht Deutschland gar bereits als "Cybercrime-Europameister"[2.)].

Die Innenministerkonferenz hat in ihrem Beschluss zur "Strategie zur Bekämpfung der IuK[3.)]-Kriminalität" am 27./28.05.2010 festgestellt, "dass die von der IuK-Kriminalität ausgehende Bedrohung derzeit eine der wesentlichen Herausforderungen im Bereich der Verbrechensbekämpfung und Prävention darstellt".

Die polizeiliche Kriminalstatistik (PKS) des Jahres 2011 für NRW bestätigt, dass der schon seit Jahren festgestellte Aufwärtstrend bei den angezeigten bzw. ermittelten Straftaten der Computerkriminalität im engeren Sinne anhält. Zu diesen Straftaten zählen vor allem der Computerbetrug (§ 263a StGB), die Datenveränderung in Datenspeichern (§ 303a StGB), die Computersabotage (§ 303b StGB) und das Ausspähen und Abfangen von Daten (§ 202a - c StGB). Auch Straftaten, die die Polizei unter der Überschrift "Tatmittel Internet" erfasst, nehmen zu, was in Anbetracht der fortschreitenden Digitalisierung aller gesellschaftlichen Lebensbereiche nicht weiter verwundert.

Die Aufklärungsquote der Computerkriminalität im engeren Sinne dagegen sinkt. Sie betrug in 2012 in Nordrhein-Westfalen nur noch gut 24% der angezeigten oder anderweitig durch die Strafverfolgungsbehörden erfassten Delikte. Aber die PKS beantwortet nicht alle Fragen im Hinblick auf die Entwicklung der IuK-Kriminalität bzw. der Cybercrime[4.)].

Auch wenn ergänzend auf alle zur Verfügung stehenden Daten in den speziellen polizeilichen Programmen zurückgegriffen würde, bliebe das Bild ungenau. Wie in anderen Kriminalitätsfeldern existiert auch bei der Cybercrime eine Diskrepanz der erfassten Straftaten zu der tatsächlichen Kriminalitätsbelastung.

Dieses sogenannte Dunkelfeld aufzuhellen, insbesondere die Melde- bzw. Anzeigebereitschaft von Wirtschaftsunternehmen und Behörden zu steigern, ist Ziel vieler Kampagnen im Lande. Das LKA NRW unterstützt zum Beispiel innerhalb der "Sicherheitspartnerschaft NRW"[5.)] das BSI[6.)] bei seiner "Allianz für Cybersicherheit" mit einer Veranstaltungsreihe zugunsten nordrhein-westfälischer Unternehmen.

Das LKA NRW, i. e. S. das dort unter meiner Leitung eingerichtete Cybercrime-Kompetenzzentrum mit aktuell 100 Mitarbeiterinnen und Mitarbeitern, hat erfolgreich eine 24/7-Hotline eingerichtet (0211/939-4040). Unternehmen und Behörden können bei diesem Single Point of Contact (SPOC) fachlich kompetente Unterstützung "im ersten Angriff", wie dies im Polizeideutsch heißt, erhalten. Die erste Beratung übernimmt ein Kriminalist, der spezielle Fachkenntnisse zur Bekämpfung und der Prävention von Cybercrime hat. Er schlägt Maßnahmen vor, z.B. um den Status quo eines DDoS-Angriffs zu erheben, den Angriff abzuwehren oder die forensischen Spuren einer Datenveränderung im Netzwerk zu sichern. Er leitet ggfls. ein Strafverfahren ein und vermittelt den Anzeigenerstatter an die für ihn im Weiteren zuständige Polizeibehörde, indem er selbst mit der übernehmenden Behörde oder der zuständigen Staatsanwaltschaft den ersten Kontakt aufnimmt.

Trotz des Strafverfolgungszwangs der Polizei (Legalitätsprinzip) allgemein und auch des LKA NRW bei Bekanntwerden einer Straftat verfolgt das Cybercrime-Kompetenzzentrum in Absprache mit der Staatsanwaltschaft und zusammen mit dem anzeigenden Unternehmen das Ziel, einen Imageschaden für das Unternehmen möglichst zu verhindern. Presseverlautbarungen – sofern sinnvoll oder notwendig – werden mit dem Betroffenen abgesprochen. Die Ermittlungen werden – in der Regel im notwendigen Zusammenwirken mit der (IT-)Sicherheitsstelle der Unternehmen – möglichst so angelegt, dass die Betriebsabläufe wenig gestört werden.

Das Cybercrime-Kompetenzzentrum beim LKA NRW besteht nicht nur aus dem SPOC, sondern bündelt seit Ende 2011 die Kompetenzen des LKA NRW im Phänomenbereich Cybercrime, Internetkriminalität, IT-Überwachung, IT-Forensik, Prävention, "Streife gehen im Netz" und Bekämpfung der Kinderpornografie. Die Einsetzung dieses Kompetenzzentrums im LKA ist eine ressourcenintensive Maßnahme, die das Ministerium für Inneres und Kommunales des Landes NRW im Rahmen seiner strategischen Schwerpunktsetzung "Bekämpfung der IuK-Kriminalität" unterstützt bzw. angeordnet hat.

Neben dem Cybercrime-Kompetenzzentrum wurden weitere Maßnahmen umgesetzt. Im Wesentlichen haben alle Polizeibehörden des Landes den personellen und organisatorischen Ausbau der Fachdienststellen vorangetrieben, wobei die flächendeckende Qualifizierung der Ermittlungskräfte einerseits und die Einstellung von IT-Fachingenieuren zur Unterstützung der Kriminalisten andererseits wesentliche Bausteine sind.

Eine andere wesentliche, bereits unmittelbar wirkende, aber vor allem in die Zukunft weisende Kooperation ist das Cybercrime-Kompetenzzentrum mit dem Hightech-Verband BITKOM e.V. 2011 eingegangen. Unterzeichnet wurde eine "Kooperationsvereinbarung zur Förderung der Sicherheit bei der Nutzung von Informations- und Kommunikationstechnologie sowie zur präventiven und repressiven Bekämpfung der Computerkriminalität". Die Zusammenarbeit zielt auf den gegenseitigen Informationsaustausch, Wissenstransfer über technologische Entwicklungen, Hospitationen, gemeinsam organisierte Fachkongresse, gemeinsam entwickelte Präventionsansätze und allgemein die gegenseitige Information zu Kriminalitätsphänomenen in der Netzwelt ab. Die Kooperation ist bislang einmalig und steht weiteren Partnern offen. Im Rahmen dieser Kooperation haben Spezialisten des LKA zusammen mit Entwicklern eines weltweit bedeutenden IT-Hauses in einem zweiwöchigen Workshop die Fähigkeiten und Grenzen der semantischen Analyse unstrukturierter Massendaten anhand eines bedeutsamen, grenzübergreifenden Phishing-Falles untersucht.

Das Cybercrime-Kompetenzzentrum unterstützt auch die Präventionsinitiative des Landespräventionsrates NRW. Für u.a. den Deutschen Präventionstag und die Präventionsarbeit der Polizeibehörden vor Ort wurden sechs professionelle Kurzfilme erstellt, die im Umgang mit Daten, Spam-Mails, unbekannten Datenträgern und Smartphones zur Vorsicht sensibilisieren sollen.

Auf die Cybercrime-Ermittler des LKA NRW und der Spezialdienststellen der örtlichen Polizeibehörden warten aktuell und in naher Zukunft trotz der neuen, guten Rahmenbedingungen vielfältige Problembereiche. Als Stichworte dienen – exemplarisch – IPv6, Cloud-Computing, unstrukturierte Massendaten, Verschlüsselungssysteme, fehlende Mindestdatenspeicherfrist, umständliche und zeitraubende Rechtshilfe im Ausland, Cyberaktivisten, schnelllebige Technik und extrem anpassungsfähige, neue Modi operandi, neue Tätertypologien etc.

Kooperationen und Koalitionen – entsprechend dem Motto der diesjährigen Fachtagung von AFCEA in Bonn – sind für die Polizeiarbeit im Themenfeld Cybercrime von zukunftsweisender Bedeutung. Damit Deutschland den wenig attraktiven Titel des Cybercrime-Europameisters möglichst schnell abgeben kann, wollen wir – das LKA und die Polizei NRW – substantielle und strukturelle Partnerschaften zwischen Strafverfolgungsbehörden, der Wirtschaft und dem Forschungssektor weiter ausbauen. Die Fachmesse AFCEA bietet auch hierfür ein gutes Parkett.

1.) Financial Times Deutschland, Ausgabe 13. November 2012

2.) Symantec Pressemitteilung vom 2. Mai 2012 zu 17. Symantec Internet Security Threat Report

3.) IuK steht für Informations- und Kommunikationstechnik

4.) Seit Herbst 2012 nutzt die Polizei nun auch offiziell diesen global assoziativ verstandenen Begriff für das Phänomen der Computerkriminalität bzw. der Kriminalität mittels moderner IT

5.) "Vereinbarung über die Sicherheitspartnerschaft gegen die Wirtschaftsspionage und Wirtschaftskriminalität" zwischen dem VSW e.V., der IHK NRW, dem Innenministerium sowie dem Wirtschaftsministerium NRW

6.) Bundesamt für Sicherheit in der Informationstechnik

Verwendung von Infektionsmarkern zur Immunisierung gegen Schadsoftware

André Wichmann und Dr. Elmar Gerhards-Padilla, Forschungsgruppe Cyber Defense, Fraunhofer FKIE

André Wichmann

Dr. Elmar Gerhards-Padilla

Entwickler von Schadsoftware und Betreiber von Botnetzen, also Netzverbünden von mit Schadsoftware infizierten Computern, verdienen im Untergrund sehr viel Geld durch Überlastangriffe auf Server im Internet, Diebstahl von Informationen, Versand von Spam-Emails, Manipulation von Transaktionen beim Online-Banking und ähnlichen kriminellen Aktivitäten. Aus diesem Grund betreiben sie einen großen Aufwand, um die Analyse ihrer Schadprogramme so schwierig wie möglich zu machen. Je länger die Entwicklung von Erkennungs- und Gegenmaßnahmen dauert, desto mehr Zeit hat eine neu entwickelte Schadsoftware, sich auszubreiten und desto wertvoller ist sie für Ihre Entwickler. Ein extremes Beispiel in dieser Hinsicht ist der berüchtigte Stuxnet-Wurm, bei dem erst mehrere Monate nach seiner Entdeckung sämtliche Verbreitungswege und Angriffsarten erforscht waren.

In der Forschungsgruppe Cyber Defense des Fraunhofer-Instituts FKIE wurde nun ein neuartiger Ansatz entwickelt, mit dem im Kampf gegen eine neu entdeckte Schadsoftware wertvolle Zeit gewonnen und während der Analysephase deren weitere Ausbreitung eingedämmt werden kann. Hierbei wird sich zunutze gemacht, dass viele Schadprogramme bei der Infektion eines Computersystems dieses durch einen sogenannten Infektionsmarker als befallen markieren.

Infektionsmarker...

Aus Sicht eines Entwicklers von Schadsoftware ist die mehrfache Infektion desselben Computers nicht wünschenswert. Da sich die Schadprogramme die Ressourcen eines Rechners wie den Prozessor oder die Netzanbindung teilen müssen, ergibt sich kein Vorteil aus einer zweiten Installation. Es kann sogar im Gegenteil die Stabilität des Rechners beeinträchtigt werden, da sich Schadsoftware häufig tief im befallenen Betriebssystem einnistet und dort Änderungen vornimmt, welche bei mehrfacher Durchführung zu ungeplanten Konsequenzen führen können.

Um dies zu verhindern, setzen Schadprogramme häufig nach einem erfolgreichen Angriff auf einen Rechner dort einen Infektionsmarker, indem z.B. ein bestimmter Schlüssel in der Registry oder ein sog. Mutex-Objekt im Speicher erstellt wird. Greift nun eine zweite Instanz der Schadsoftware diesen Computer an, erkennt sie am Vorhandensein dieses Markers, dass der Rechner bereits befallen ist, und bricht den Angriff ab (siehe Abbildung 1).

Eine wichtige Beobachtung hierbei ist, dass ein Infektionsmarker für alle Varianten einer Schadsoftware gleich aussehen muss, damit jede Variante zuverlässig eine bereits vorhandene Infektion erkennen kann. Typischerweise ändert Schadsoftware mit hoher Frequenz ihre Gestalt, um einer Erkennung durch Antiviren-Software zu entgehen. Für den Infektionsmarker ist ihr dies jedoch prinzipbedingt nicht möglich.

...als Impfstoff verwenden

Die Idee ist nun, diesen Infektionsmarker auf noch nicht befallenen Rechnern zu setzen und somit eine Infektion vorzutäuschen. Greift die Schadsoftware an, entdeckt sie den Marker und beendet den Angriff, ohne sich auf dem System zu installieren – der Computer ist gegen diese Schadsoftware immunisiert.

Das Fraunhofer FKIE hat ein Klassifizierungssystem für Infektionsmarker und ein Verfahren entwickelt, mit dem vollständig automatisiert und ohne Expertenwissen der Marker eines Schadprogramms extrahiert und klassifiziert werden kann. Das Ergebnis ist ein kleines Programm, welches auf anderen Rechnern installiert werden kann und diese immunisiert. Hierbei wird ausgenutzt, dass für Infektionsmarker

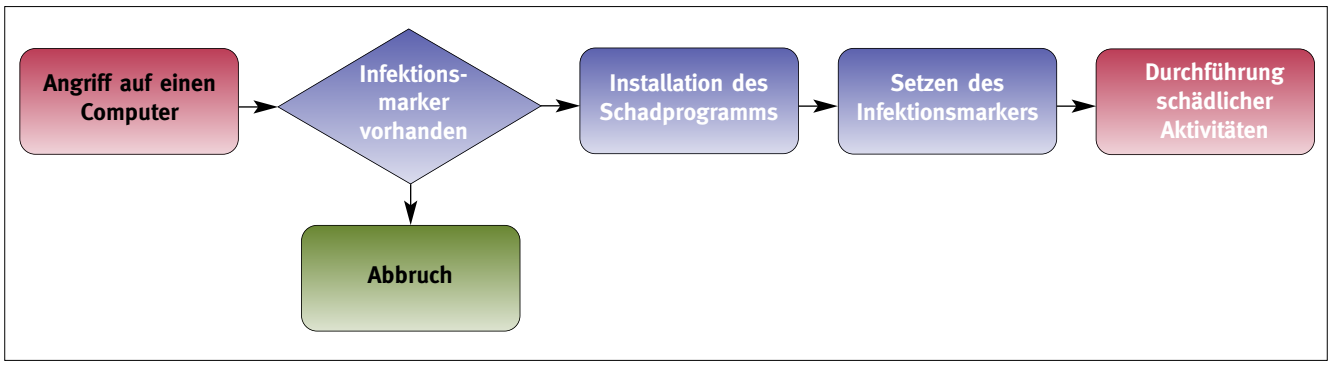


Abbildung 1: Typischer Ablauf einer Infektion mit Schadsoftware

Strukturen des Betriebssystems eingesetzt werden, auf die die Schadsoftware über eine wohldefinierte und begrenzte Schnittstelle zugreift. Dies ermöglicht eine vollständige Automatisierung des Verfahrens, während für die tiefergehende Analyse von Schadprogrammen normalerweise das Wissen und die Arbeitszeit menschlicher Experten nötig sind. Wenn eine neuartige Schadsoftware entdeckt wird, können so sehr schnell bedrohte Rechner immunisiert und die Ausbreitung der Schadsoftware eingedämmt werden, während tiefergehende Analysen durchgeführt werden.

Wirksamkeit des Verfahrens

In einer groß angelegten Untersuchung mit einem umfassenden Korpus von über tausend Schadprogrammen unterschiedlichster Art und Herkunft wurde die Wirksamkeit des Verfahrens überprüft. Es stellte sich heraus, dass die überwältigende Mehrheit (über 95%) aller untersuchten Schadprogramme, welche Infektionsmarker verwenden, anfällig für eine Immunisierung ist. In fast allen dieser Fälle (99,4%) konnte automatisch ein Impfprogramm erstellt werden, welches nicht befallene Rechner zuverlässig vor einer Infektion schützte. Nur in 0,6% der Fälle konnte zwar der Typ des Markers identifiziert, dieser aber nicht extrahiert werden.

Neben dem Testkorpus wurden noch zwei detaillierte Fallstudien durchgeführt, bei denen die zwei laut dem Symantec Intelligence Report 2012 am weitesten verbreiteten Schadprogramme, Conficker und Sality, betrachtet wurden. Wie sich herausstellte, konnte in beiden Fällen der Infektionsmarker korrekt erkannt und klassifiziert werden. Für Sality wurde automatisch ein Programm zur Immunisierung erstellt. Für Conficker war dies auf Grund des verwendeten, sehr seltenen Markertyps nicht automatisiert möglich, allerdings konnten mit Hilfe des Verfahrens hinreichend genaue Informationen bereit gestellt werden, mit deren Hilfe eine manuelle Erstellung eines entsprechenden Programms in kürzester Zeit möglich war.

Ausblick

Wie sich gezeigt hat, lassen sich Infektionsmarker von Schadprogrammen hervorragend zur Immunisierung von noch nicht infizierten Rechnern einsetzen. Die typische Struktur dieser Marker erlaubt es, den Prozess zur Erstellung von Impfprogrammen in den meisten Fällen vollständig zu automatisieren. Auch zukünftige Schadsoftware wird ein Interesse daran haben, ein Computersystem nicht mehrfach zu infizieren und daher eine Form von Infektionsmarkern verwenden. Aus diesem Grund arbeitet das Fraunhofer FKIE aktiv daran, das Verfahren zur Extraktion zu verfeinern und zu generalisieren, um möglichen Gegenmaßnahmen seitens der kriminellen Entwickler von Schadsoftware zuvorzukommen und zukünftige Infektionsmarker möglichst unabhängig von ihrer Struktur auch weiterhin finden zu können.

SEAMAN – Sicherheit in MANETs für zukünftige Funkübertragungsverfahren

Dr.-Ing. Marc Adrat, Thomas Bosch, Harald Bongartz, Fraunhofer FKIE

Dr.-Ing. Marc Adrat

Thomas Bosch

Harald Bongartz

MANET steht als Abkürzung für »Mobile Ad Hoc Network« und bezeichnet ein bewegliches und sich selbst organisierendes Kommunikationsnetz. Alle Teilnehmer des Netzes kooperieren miteinander und passen ihre Konfiguration automatisch den aktuellen Gegebenheiten an. Ein MANET erlaubt es, sehr dynamisch auf Veränderungen zu reagieren (neue Teilnehmer kommen hinzu oder geraten außer Reichweite), und weist eine hohe Robustheit auf (wenn Teilnehmer ausfallen, übernehmen andere Knoten die Weiterleitung).

Durch die MANET-Fähigkeit ergeben sich viele Vorteile in der spontanen Vernetzung, jedoch müssen auch einige Herausforderungen gelöst werden, bevor die Technologie einen praktischen Mehrwert in zukünftigen Funkübertragungsverfahren liefert. Ein wichtiger Aspekt ist die Sicherheit der Datenübertragung. Das bedeutet, die Schutzziele der Informationssicherheit müssen garantiert werden. Dabei betrachten wir hier hauptsächlich die folgenden drei Ziele:

- Vertraulichkeit – ein Unbekannter darf keine Nachrichten abhören können,
- Verbindlichkeit – der angegebene Absender ist der wirkliche Absender der Nachricht – und
- Integrität – die Nachricht kann während der Übertragung nicht manipuliert werden.

Und hier kommt SEAMAN ins Spiel: Die Abteilung Kommunikationssysteme des Fraunhofer FKIE hat ein Konzept entwickelt, welches den Aufbau und den Betrieb eines MANETs absichert. Es ist das Sicherheitsprotokoll-Konzept “Security-Enabled Anonymous MANET”. Das Protokoll berücksichtigt die speziellen militärischen Anforderungen, wie z. B. die Unterstützung von effizienter Gruppenkommunikation, und sichert ein MANET hinsichtlich der zuvor genannten Schutzziele ab. Darüber hinaus bietet es noch weitere Sicherheitsfunktionalitäten, wie z.B. einen anonymen Verbindungsaufbau, der keine Rückschlüsse auf die Identität eines Funkteilnehmers zulässt.

Funktionsweise von SEAMAN

In einem durch SEAMAN geschützten taktischen MANET wird ein gemeinsamer “MANET-Key” verwendet, den ein zuständiger “Key-Manager” dynamisch verwaltet. Die Knoten in einem MANET können dadurch ihre Routing- und Nutzdaten im Sinne der Informationssicherheit schützen.

Zwei unterschiedliche MANETs können aufgrund verschiedener Schlüssel nicht miteinander kommunizieren. Damit dennoch eine Kommunikation möglich wird, wird zwischen zwei unterschiedlichen MANETs zunächst eine “Bridge” aufgebaut. Die Bridge wird durch zwei Knoten zwischen den beiden Netzen aufgebaut, sobald Daten von einem unbekannten Netz empfangen werden (Nachbarschaftserkennung). Bei der Bridge handelt es sich um eine speziell gesicherte Verbindung mit einem separaten “Bridge-Key”.

Über die Bridge können die beiden zuständigen Key-Manager eine MANET-Zusammenführung aushandeln. Dabei wird einer der beiden Key-Manager das Management übernehmen und einen neuen gemeinsamen MANET-Key erzeugen und verteilen. Nachdem jeder Knoten den neuen MANET-Key erhalten hat, wird die Bridge abgebaut. Diese wird nicht mehr benötigt, da nun eine sichere direkte Kommunikation durch den gemeinsamen MANET-Key möglich ist.

SEAMAN im OSI-Referenzmodell

Im OSI-Referenzmodell befindet sich SEAMAN auf dem Link-Layer, um dem Protokoll einen Zugriff auf die Frames zu gewährleisten. Alle Daten inklusive dem Protokoll-Header von OSI Layer 3 und höher werden auf dem Link-Layer mit dem MANET- bzw. Bridge-Key verschlüsselt. Zusätzlich wird die Integrität jedes Frames durch Hinzufügen eines "Keyed-Hashing Message Authentication Code" (HMAC) gesichert. SEAMAN schützt somit neben den eigenen Daten auch die Daten der höheren OSI-Schichten.

Paralleles Aufbauen und Absichern eines MANETs mittels SEAMAN

Im Frame-Header wird von SEAMAN ein zusätzliches, unverschlüsseltes Feld benötigt, welches spezifiziert, ob ein Frame mit einem MANET- oder Bridge-Key verschlüsselt wurde. Bei der Entschlüsselung können im Unterschied zur Verschlüsselung vorübergehend mehrere MANET-Keys gleichzeitig zum Einsatz kommen. Der Grund dafür liegt im gewählten "Re-Keying" Verfahren. Dieses Verfahren trägt der Tatsache Rechnung, dass in einem MANET mit Multihop-Verbindungen keine zeitlich synchronisierte

Schlüsselverteilung möglich ist. Des Weiteren sendet der Link-Layer alle Daten per Broadcast, deshalb wird die Quell- und Ziel-Adresse im Frame entweder auf eine vorher festgelegte oder die allgemeine Link-Layer-Broadcast-Adresse gesetzt.
Die immer gleichen Quell- und Ziel-Adressen sowie das Bridge-Flag sind die einzigen unverschlüsselten Informationen im MAC Link-Layer, die jedoch für einen Angreifer keine verwertbare Information enthält. Auch die Anonymität der Kommunikationspartner bleibt dadurch erhalten.

Unterstützte Netzoperationen

Im Folgenden wird eine kurze Übersicht über die von SEAMAN unterstützten Netzoperationen gegeben:

- "Node Join": Bei der Node Join-Operation tritt ein einzelner Knoten einem MANET bei. Für die Operation ist mindestens ein Bridge-Aufbau mit anschließendem Re-Keying nötig.
- "Network Merge": Bei der Network Merge-Operation verschmelzen zwei MANETs zu einem MANET. Für die Operation ist mindestens ein Bridge-Aufbau mit anschließendem Re-Keying erforderlich.
- "Node Leave": Bei der Node Leave-Operation verlässt ein einzelner Knoten das MANET. Die Operation kann nur durch ein Re-Keying durchgeführt werden, da ansonsten der selbe MANET-Schlüssel weiter verwendet wird. Das Re-Keying wird in SEAMAN aus diesem Grund regelmäßig durchgeführt, z.B. jede Stunde.
- "Network Partition": Durch die Network Partition-Operation wird ein MANET in zwei MANETs aufgeteilt. Analog zur Node Leave Operation muss ein Re-Keying erfolgen.
- "Node Eject": Diese Operation wird benötigt, um z.B. einen kompromittierten Knoten vom Netzwerk zu isolieren. Der Ausschluss des Knotens wird zunächst im Netzwerk propagiert. Anschließend wird ein Re-Keying durchgeführt, bei dem der kompromittierte Knoten keinen neuen MANET-Schlüssel erhält. Zusätzlich wird sichergestellt, dass der Knoten zukünftig auch keine Bridge mehr aufbauen kann.

Evaluation der Anwendbarkeit von SEAMAN

Im Rahmen einer Studie wurde die grundsätzliche Anwendbarkeit des SEAMAN-Konzepts überprüft. Da eine analytische Überprüfung aufgrund der komplexen Interaktionen mit anderen Komponenten wie z.B. Routingprotokoll, Key-Management, Signalausbreitung, eine nur geringe praktische Aussagekraft hätte, wurde SEAMAN mit Hilfe eines Netzwerksimulators evaluiert. Für die Bewertung der Anwendbarkeit wurden jeweils ein statisches und ein mobiles Szenario mit 30 Knoten betrachtet. Beim statischen Szenar sollten sich 30 Einzelknoten zu einem durch SEAMAN abgesicherten MANET zusammenschließen und im mobilen Szenar zwei Teilnetze mit je 15 Knoten. Untersucht wurden die Konvergenzzeit und die Anzahl der MANET-Zusammenführungen sowie der Overhead.
Die ersten Ergebnisse zeigten z.B., dass zwei zuvor einander unbekannte MANETs im mobilen Szenar durchschnittlich innerhalb von 75 Sekunden und im statischen Szenar nach ca. 50 Sekunden zu einem durch SEAMAN abgesicherten MANET zusammengefügt wurden. Diese auf den ersten Blick langen Zeiten liegen u.a. darin begründet, dass die Schlüsselaushandlung aufgrund von Paketkollisionen unzuverlässig abläuft und sich MANETs zeitweise wieder partitionieren. Die Zeiten lassen sich z.B. durch Anwenden von randomisierten Protokollen im Bridge-Aufbau erheblich senken, jedoch auf Kosten einer höheren Netzlast. Erste Verbesserungsmaßnahmen führten bereits zu einer Reduktion der Konvergenzzeit um ca. 30%.

Einfluss von Jamming

Neben den Analysen im freundlichen Umfeld wurde SEAMAN auch zusätzlich hinsichtlich der Beeinflussung durch Jamming untersucht. Es zeigte sich, dass, wenn überhaupt, das SEAMAN-Protokoll während des Zusammenwachsens von MANETs gefährdet ist. Wenn ein MANET bereits vollständig abgesichert ist, d.h. wenn alle Knoten über einen gemeinsamen MANET-Key verfügen, verursacht der Jammer nur zusätzliche Netzwerklast. Der Jammer ist nicht in der Lage, das Netzwerk zu partitionieren, sofern in Anbetracht der zusätzlichen Netzlast ein Mindestmaß an Durchsatz für die Kommunikation übrig bleibt.

Fazit

Das Sicherheitsprotokoll-Konzept SEAMAN ermöglicht einen anonymen Verbindungsaufbau und eine authentifizierte und vollständig verschlüsselte Übertragung in einem MANET und kann in Verbindung mit jedem proaktivem Routingprotokoll eingesetzt werden. Das SEAMAN-Konzept wurde bereits im Rahmen einer Studie in einem Netzwerksimulator evaluiert, um den Nachweis der grundsätzlichen Anwendbarkeit von SEAMAN erbringen zu können. Es hat sich gezeigt, dass das parallele Aufbauen und Absichern eines MANETs in vertretbarer Zeit und robust möglich ist.

Schutz kritischer Daten – Lösungen für den Ernstfall

Dr. Carsten Rudolph, Dr.-Ing. Martin Steinebach, Fraunhofer SIT

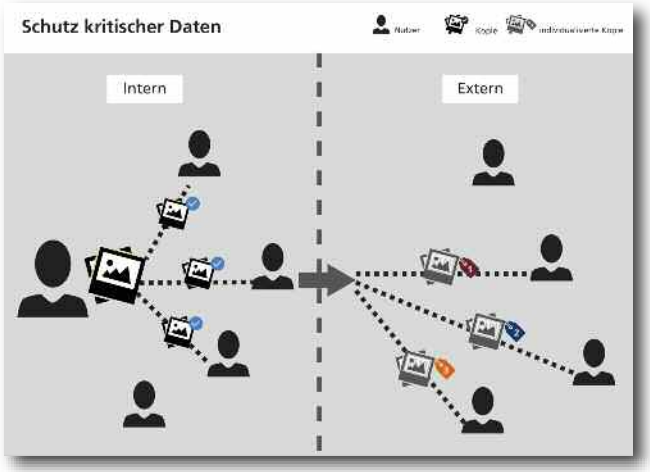
Dr. Carsten Rudolph

Dr.-ing. Martin Steinebach

Einleitung

In vielen IT Netzen werden Daten mit unterschiedlichen Vertraulichkeitsstufen erzeugt, bearbeitet, gespeichert und weitergegeben. Die Kontrolle über diese Daten wird dabei grundsätzlich über eine Kombination von Sicherheitsmechanismen realisiert. Starker Zugriffsschutz, Segmentierung von Netzen oder die Verwendung starker Verschlüsselungsmechanismen können in geeigneter Kombination einen ausreichenden Schutz liefern. Dies gilt jedoch meist nur solange Daten innerhalb einer klar begrenzten und kontrollierten Umgebung gehalten werden. Aktuelle Lösungen weisen jedoch meist gravierende Schwachpunkte auf. Erstens hängt die Vertraulichkeit von kritischen Daten sehr stark vom Verhalten der Personen ab, die auf die Daten zugreifen dürfen. Meistens liegt es im Ermessen dieser Personen, an wen und an welche anderen technischen Geräte Informationen weitergegeben werden. Zweitens besteht oft kein Schutz mehr, sobald Daten außerhalb eines vordefinierten Bereiches an eine größere Anzahl Personen weitergegeben werden müssen. Ergänzt man den klassischen Sicherheitsmix durch neue praxiserprobte Technologien wie hardware-basierte Sicherheitsbausteine oder digitale Wasserzeichen, so lassen sich diese typischen Sicherheitslücken schließen – kostengünstig und ohne Nachteile für die handelnden Personen. Teilweise unterstützen diese Techniken auch die Nutzung mobiler Geräte.

Die folgenden Abschnitte skizzieren Lösungen, die durch die Kombination existierender Sicherheitsmechanismen eine grundlegende Verbesserung in beiden genannten Bereichen bietet. In geschützten Umgebungen wird die Weitergabe von Daten technisch, hardware-gesichert auf vorher festgelegte (oder von einer autorisierten Person kontrollierte) Geräte eingeschränkt. Müssen die Daten außerhalb dieses stark abgesicherten Bereiches weitergegeben werden, liefert die Lösung ein Mindestmaß an Sicherheit, das zwar nicht die Geheimhaltung garantieren kann, aber zumindest die Verteilungswege der Daten durch personalisierte Kopien nachvollziehbar macht.



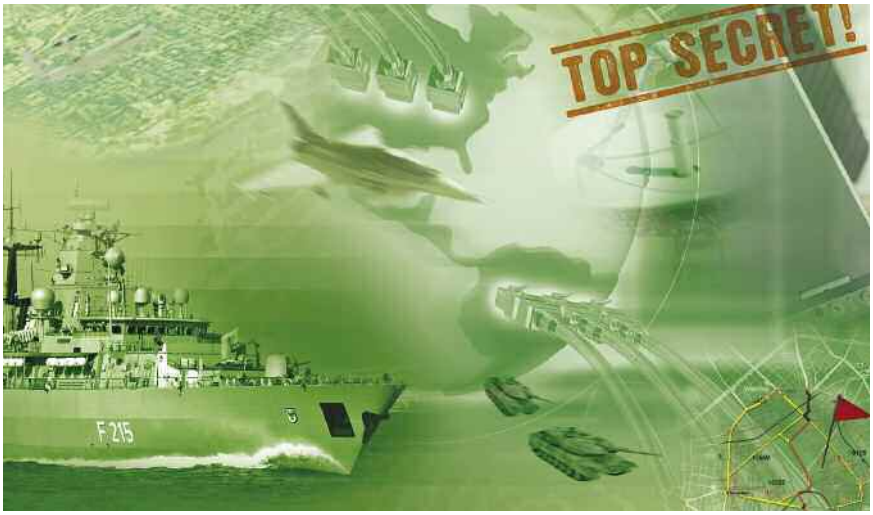
Hardwarebasierte Sicherheitsmechanismen schützen Dokumente in internen Netzen. Digitale Wasserzeichen machen digitale Kopien nachverfolgbar. Quelle: Fraunhofer SIT

In sicheren Netzen

Innerhalb von über Firewalls und andere Mechanismen abgeschotteten Netzen wird oft auf die Perimetersicherheit vertraut und Vertraulichkeit von Daten lediglich über Zugriffskontrollmechanismen abgesichert. Unterschiedliche Angriffe, zum Beispiel Stuxnet, Flame oder die aktuellere sogenannte “Operation Roter Oktober”, haben aber gezeigt, dass Perimetersicherheit zwar wichtig ist, um Angriffe abzuhalten und zu erkennen, aber nicht ausreicht, um Rechner in internen Netzen vor Angriffen zu schützen. Abtrennungen zwischen Netzsegmenten sind nicht undurchlässig oder unumgehbar. Sogar Computer ohne Netzzugang können z.B. über USB Laufwerke oder andere Schnittstellen verwundbar sein. Das heißt, Angriffe z.B. durch Schadsoftware oder Social Engineering können auch innerhalb geschützter Netze auftreten.

Hardware-basierte Sicherheit kann zusätzlichen Schutz bieten. Ein Beispiel dafür ist das Trusted Platform Module TPM, das bereits in vielen PCs, Laptops und Servern integriert ist und auch als MTM für Mobiltelefone spezifiziert ist. Damit kann

rs IntCent® – das Lagebild vor Ort



Schutz internationaler Einsätze

Bei ihren Einsätzen in internationalen Krisenregionen übernimmt die Bundeswehr komplexe Aufgaben. Die deutschen Soldaten leisten Aufbauhilfe oder schützen vor Piraten, während die Gefahr von Übergriffen droht. Unerlässlich für Aufgabenerfüllung und Schutz der Truppe ist eine hochmoderne, verlässliche Ausstattung.

Marineeinheiten, Spezialkräfte, das Einsatzführungskommando sowie das Kommando Strategische Aufklärung arbeiten mit **rs*IntCent***®. Die IT-Lösung von rola Security Solutions (Oberhausen) unterstützt die strukturierte Informationserschließung in der Kommunikationsaufklärung.

Dynamische Auswertung

Für Einsätze in Kriegs- und Krisengebieten ist es von vitaler Bedeutung, dass alle verfügbaren Informationen vorliegen, um die Lage der operierenden Einheiten einzuschätzen und absichern zu können. Einzelerkenntnisse müssen verarbeitet und in einen Zusammenhang gestellt werden, um die Analyse von Netzwerken – z. B. terrorverdächtiger Personen – durchführen zu können. Dies gilt im Vorfeld eines Einsatzes, um eine möglichst verlässlich Planungsgrundlage zu erhalten. Aber auch während des Einsatzes müssen weiter aktuelle Erkenntnisse gesammelt und effizient analysiert werden. Das heißt, der Prozess der Informationsgewinnung und -auswertung muss dynamisch gestaltet werden können.

Lagebild

Durch das **rs*IntCent***® System von rola werden Einzelerkenntnisse aus unterschiedlichsten Quellen – Humint, Sigint, MilNw – in einer Datenbank gesammelt.

Durch zahlreiche Auswerte- und Analysemechanismen entsteht aus Einzelinformationen ein Informationsraum, der Beziehungen, etwa zwischen Personen, zwischen Personen und Orten oder Personen und Ereignissen (IED-Anschläge, Treffen) usw. sichtbar macht und in Diagrammen und Schaubildern verständlich darstellt – ein wesentlicher Beitrag zum Lagebild! Und damit die Grundlage für die Beurteilung der Lage und für die Entscheidungsfindung.

Mobilität

Mit der Verwendung mobiler Einsatzkomponenten (Mobile Computing) können diese Informationen im Reachbackverfahren zwischen den beteiligten Dienststellen ausgetauscht und repliziert werden. Abstimmungsprozesse werden spürbar beschleunigt. Zudem wird ein wesentlicher Beitrag zur Force Protection geleistet. Aufgrund seiner Mehrsprachigkeit ist **rs*IntCent***® auch im multinationalen Umfeld einsetzbar.

Sicherheit

rola Security Solutions konnte die IT-Lösung **rs*IntCent***® jeweils fristgerecht innerhalb kürzester Zeit einsatzbereit im vollen geforderten Funktionsumfang und budgetgerecht zur Verfügung stellen – inklusive der Erstellung projektbezogener Konzepte (z.B. IT-Sicherheitskonzept) und unter Beachtung aller datenschutzrechtlichen Vorgaben.

Weitere Informationen unter
www.rola.com.

Mit Trusted Computing lässt sich der Zustand eines Geräts prüfen Quelle: Fraunhofer SIT

durch die Verschlüsselung von Daten und das Binden des Schlüssels an einen bestimmten Rechner und an einen bestimmten Zustand des Rechners erreicht werden, dass eine Entschlüsselung nach einer Manipulation nicht mehr möglich ist.

Eine besondere Funktion des TPM ist die kontrollierte Migration von kryptographischen Schlüsseln. Ein TPM kann selbst asymmetrische Schlüssel erzeugen, bei denen der private Teil des Schlüssels nie im Klartext außerhalb des TPMs vorliegt. Mit einem solchen Schlüssel können verschlüsselte Daten nur von genau demselben TPM entschlüsselt werden. Bei der Migration von Schlüsseln kann nun der Schlüssel sicher an ein weiteres TPM weitergegeben werden, so dass Daten auf einem anderen Rechner entschlüsselt werden können. Das Besondere dabei ist, dass sich Bedingungen für den Zustand des Zielgerätes festlegen lassen und so die Einhaltung gewisser Sicherheitsvorkehrungen auf dem Gerät sichergestellt werden kann. Das heißt, die Daten können nie auf einem Gerät mit unbekanntem Zustand entschlüsselt werden. Damit kann zwar die Infektion mit Schadsoftware nicht verhindert werden, aber Daten sind auf dem infizierten Gerät nicht mehr im Klartext verfügbar.

Für die Migration gibt es im Prinzip zwei Möglichkeiten der Kontrolle. Erstens können für einen migrierbaren Schlüssel die Zielgeräte für die Migration fest vorgegeben werden und untrennbar mit dem Schlüssel verbunden werden. Eine flexiblere Lösung bieten so genannte Migration Authorities, bei denen ein weiterer Rechner mit TPM als Kontrollinstanz fungiert, die jeweils Freigaben erteilt, wenn ein Schlüssel zu einem bestimmten anderen Rechner migriert.

So kann eine Einsatzleitung etwa die Weitergabe von Daten auf vordefinierte Teams beschränken, oder eine Kontrollinstanz festlegen, die genehmigt, an wen kritische Daten weitergegeben werden können. Für die Realisierung ist keine aufwändige neue Public Key Infrastruktur notwendig, da TPMs bereits mit einer eigenen Public Key Infrastruktur (PKI) ausgestattet sind. Zertifizierte TPMs liefern dabei ein Sicherheitslevel, das mit der Sicherheit von SmartCard Chips vergleichbar ist. Schlüsselmanagement ist allerdings nötig, da TPM Schlüssel den jeweiligen Rechnern zugeordnet werden müssen (z.B. durch die Migration Authority). Außerdem müssen für die Daten die jeweiligen Zugriffsrechte explizit definiert werden. Der gerätebasierte Zugriff über TPMs kann auch mit benutzerspezifischen Zertifikaten (z.B. über eine bereits existierende PKI) kombiniert werden.

Falls die Software der verwendeten Geräte eine Kontrolle der Verwendung von Daten ermöglicht, kann zusätzlich noch erzwungen werden, dass eine Weitergabe der Daten außerhalb des durch Schlüsselmigration definierten Bereiches immer nur unter der Verwendung zusätzlicher Sicherheitsmechanismen erfolgen kann. Naheliegend ist eine gezielte Verschlüsselung. Damit ist aber nur der erste Schritt der Weitergabe geschützt. Für einen weitergehenden Schutz müssen die Daten mit Merkmalen versehen werden, die sich nicht leicht entfernen lassen und bei der Bearbeitung der Daten stabil bleiben. Das folgende Kapitel zeigt eine am Fraunhofer SIT entwickelte praktikable Lösung, um einen solchen weitergehenden Schutz zu erreichen.

Jenseits sicherer Infrastrukturen

Hardwaregebundene Lösungen wie die gerade beschriebene bieten einen zuverlässigen Schutz in Umgebungen, die sich gezielt auf die Verbreitung kritischer Informationen vorbereiten lassen. In der Praxis ist es jedoch immer wieder erforderlich, Informationen in unsicheren oder teilweise unsicheren Kontexten auszutauschen. Im Folgenden wird deshalb diskutiert, wie ein Schutz von Informationen auch jenseits sicherer Infrastrukturen erreicht werden kann. Leitlinie dabei ist nicht das Verhindern einer Weitergabe von Informationen – diese erfolgt ja in solchen Situationen meist ganz bewusst –, sondern die kontrollierte Weitergabe von Informationen mit Hilfe von vorbeugender Wasserzeichentechnik, die eine Rückverfolgung unerlaubt weitergegebener Informationen zu ihrer Quelle erlaubt. Zwar wäre ein stärkerer Schutz wie der innerhalb von sicheren Infrastrukturen auch hier wünschenswert, kann aber aufgrund von Aspekten wie der notwendigen Verteilung von Schlüsseln oder

Mit Hilfe von digitalen Wasserzeichen lassen sich Informationen im Bildrauschen einbetten. Dadurch kann man individuelle Kopien erzeugen, mit denen Informationsquellen eindeutig zu identifizieren sind. Quelle: Fraunhofer SIT

Hardware sowie dem Aufbau von Vertrauensmodellen in der Praxis nicht immer ad hoc erreicht werden.

Denn in einer Krisensituation kann es notwendig sein, digitale Informationen schnell und unbürokratisch verschiedenen Parteien zur Verfügung zu stellen. Dies können Bilder, Videoaufzeichnungen, Kartenmaterial oder auch Textdokumente sein. Beispiel Naturkatastrophe: Ein Aufklärungsfoto aus dem Krisengebiet soll umgehend verschiedenen lokalen Einsatzkräften zur Verfügung gestellt werden, um sie über die Lage zu informieren. Die ortskundigen Einsatzkräfte verwenden Endgeräte, die nicht in die sichere Infrastruktur eingebunden sind. Nun gilt es, eine Entscheidung zu treffen, ob das Foto die sichere Umgebung verlassen darf oder nicht.

Da die Einsatzleitung die Inhalte bewusst weitergibt, liegt das unkalkulierbare Risiko in solchen Situationen darin, dass das Foto nach dem Verlassen der sicheren Umgebung ungeschützt ist und beliebig weitergegeben werden kann, ohne dass die Quelle dieser unerlaubten Verbreitung Konsequenzen zu erwarten hat. Denn bei Nutzung herkömmlicher Lösungen können Einsatzkräfte im Nachhinein nicht feststellen, aus welcher Quelle das Foto stammt, also welche der verschiedenen lokalen Einsatzkräfte es unerlaubt weitergegeben haben.

Abhilfe schafft ein Sicherheitsmechanismus, der sich im Bereich des Schutzes gegen Urheberrechtsverletzungen beim Verkauf von Mediendateien bereits etabliert und bewährt hat: Digitale Wasserzeichen ermöglichen eine individuelle Markierung aller Kopien, die an die Endbenutzer ausgegeben werden. Es kann immer wieder die Beziehung zwischen Medium und Empfänger hergestellt werden, so dass dieser von einer unberechtigten Weitergabe abgeschreckt wird. Wird trotzdem eine unberechtigte Kopie gefunden, kann deren Quelle identifiziert werden.

Zur Nutzung von Wasserzeichentechnik lassen sich bestehende Infrastrukturen erweitern. Dateien können innerhalb der geschützten Umgebung wie oben beschrieben sicher verwendet werden. Zusätzlich erlaubt die Erweiterung jedoch den Export in unsichere Umgebungen jenseits der kontrollierten Infrastruktur. Bei diesem bewussten Verlassen der geschützten Umgebung wird die Datei mit einer individuellen Kennung markiert, sodass bei mehreren Kopien jede eindeutig zu unterscheiden ist. Diese Kennung wird in der eigenen Infrastruktur in einer Datenbank gespeichert; dabei werden auch Empfänger und Exportierender hinterlegt. Die Datei ist nun ungeschützt, aber individuell identifizierbar.

Soll eine Einsatzkraft von einem Anwender der sicheren Infrastruktur beispielsweise ein Aufklärungsfoto auf ihr privates Smartphone geschickt bekommen, da eine andere Lösung nicht zur Verfügung steht, dann würde dieses Foto vorher markiert und beispielsweise als MMS oder Email-Anhang versendet werden. Die Einsatzkraft würde darauf hingewiesen, dass es sich um vertrauliche Informationen handelt und eine Weitergabe untersagt ist. Weiterhin wird ihr mitgeteilt, dass die Datei durch eine Individualisierung geschützt ist und Zuwiderhandlung verfolgt werden kann. In der Datenbank der Infrastruktur sind nach diesem Vorgang die Kennungen der Einsatzkraft, des Anwenders und die individuelle Kennung, die als Wasserzeichen eingebettet wurde, gespeichert, gegebenenfalls mit weiteren vorhanden Daten wie Zeitpunkt oder Einsatzkennung.

Der derzeitige Stand der Technik erlaubt entsprechende Vorgehensweisen, in der Praxis werden auf analogem Weg beispielsweise Bemusterungskopien von Kinofilmen oder Musikalben an Rezensenten ausgeliefert. Wasserzeichenverfahren müssen für unterschiedliche Medientypen individuell erstellt werden. In der Praxis sind heute Lösungen für Fotos, Zeichnungen, Videos, Audio sowie formatierte Dokumente im Einsatz. Algorithmen für beispielsweise Vektorgrafiken, Text, 3D-Modelle sind ebenfalls bereits entwickelt worden. Diese Verfahren weisen bereits einen hohen Reifegrad auf. Audiowasserzeichen überstehen

selbst starke verlustbehaftete Kompressionen und können selbst aus analogen Überspielungen ausgelesen werden. Wasserzeichen in Fotos überstehen Größenänderungen und selbst das Ausdrucken und wieder Einlesen der Fotos.

Die Einbindung in ein übergeordnetes System ist ebenfalls unkompliziert. Abstrakt kann ein Wasserzeichen als PlugIn betrachtet werden, welches ausgehendes Medienmaterial leicht verändert, ohne dabei für den Menschen wahrnehmbar zu sein. Ein entsprechendes PlugIn kann beispielsweise in die Exportfunktion eines Content Management Systems eingebunden werden.

Fazit

Typische Schwachstellen bestehender Lösungen beim Schutz kritischer Daten lassen sich durch Nutzung neuer Technologien beheben, die sich bereits in der Praxis bewährt haben. Um eine Anwendung in hochsicheren Umgebungen zu ermöglichen, sind zwar noch Anpassungen notwendig, die aber auch in kommerziellen zivilen Kontexten bisher immer problemlos erfolgten. Ob eine Lösung für den individuellen Einsatzfall realisierbar ist, hängt weniger von den individuellen Infrastrukturen ab als vielmehr von den genutzten Geräten und den zu schützenden Inhalten. TPM-basierte Verfahren lassen sich auf alle möglichen digitalen Inhalte anwenden. Sichere Wasserzeichen müssen auf die jeweiligen zu schützenden Inhalte angepasst werden. Während für Bild- und Ton-Dateien ausgereifte Algorithmen existieren, die bereits auf Kartenmaterial oder Videos angewandt wurden, bedürfen die Wasserzeichen-Algorithmen für offene Textdateien oder 3D-Modelle noch der Erprobung. Die aktuellen Forschungsaktivitäten inner- und außerhalb der EU lassen aber einen raschen Fortschritt erwarten.

Wer sich heute also für eine Schutz von Audio, Video und Bild interessiert, der auch außerhalb sicherer Infrastrukturen Bestand hat, kann Lösungen für Betriebssysteme wie Windows oder Linux lizensieren, die an anderer Stelle bereits täglich im Einsatz sind. Lediglich die Integration in die eigene Infrastruktur, beispielsweise in ein Content Management System oder einen Email-Server muss dann individuell erfolgen, was aber bei offenen Systemen nur einen geringen Aufwand mit sich bringt.

Neue Sicherheitskonzepte für Kritische Infrastrukturen der Zukunft

Dr. Rüdiger Klein, Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS

Dr. Rüdiger Klein

Kritische Infrastrukturen wie Energienetze, terrestrische und mobile Telekommunikation sowie das Internet, oder Verkehrs- und Logistiksysteme sind heute schon sehr komplex. Diese Komplexität wird in den nächsten Jahren rasch weiter zunehmen. Die zahlreichen Veränderungen, etwa im Energiebereich – in Deutschland häufig als "Energiewende" apostrophiert – führen dazu, dass diese Systeme schon in wenigen Jahren völlig anders aussehen werden als vor zehn oder zwanzig Jahren. Sie werden technisch heterogener sein, sie werden stärker verteilt sein, und sie werden vor allem viel mehr Intelligenz durch Informations- und Kommunikationssysteme beinhalten, um unter jeglichen Bedingungen optimal gesteuert werden zu können. Erneuerbare Energiequellen erfordern viel flexiblere Steuerungsverfahren als die Energieproduktion in Großkraftwerken, und eine flexible Steuerung auf der Verbraucherseite ermöglicht eine stärkere Anpassung des Energiekonsums an die aktuell verfügbare Energieproduktion. Die resultierenden "Smart Grids" bieten durch intelligente Steuerung und neuartige Geschäftsmodelle zahlreiche neue Möglichkeiten einer effizienten, kostenoptimierten und nachhaltigen Energiewirtschaft.

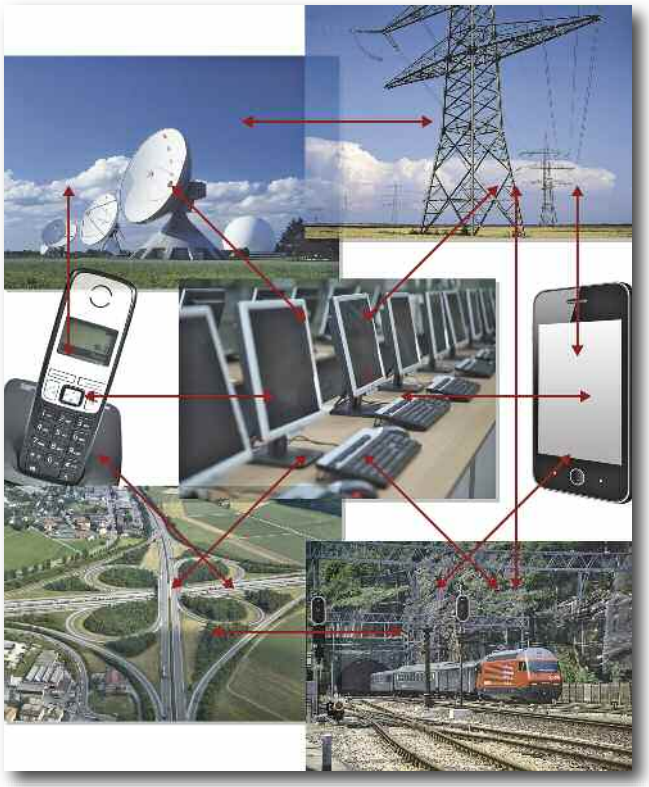


Abb 1: Wechselseitige Abhängigkeiten moderner Kritischer Infrastrukturen *Quelle: Fotolia/MEV*

Ähnliche Trends beobachten wir auch in anderen Bereichen. Die Vision der "Smart Cities" zum Beispiel zielt auf die immer engere Verflechtung verschiedener Bereiche in urbanen Räumen: unterschiedlicher Verkehrssysteme, mobiler Kommunikation, elektronischer Medien, Großveranstaltungen, Notfall- und Rettungssysteme etc. Auch hier spielen Informations- und Kommunikationssysteme eine zentrale Rolle: sie wirken, hier wie in anderen Kritischen Infrastrukturen, als "Nervensysteme", ohne die eine ordnungsgemäße Funktion dieser komplexen Gebilde nicht mehr möglich ist.

Chancen und Risiken

Mit den neuen Chancen entstehen auch neue Risiken. Wir erwarten wie selbstverständlich, dass uns Kritische Infrastrukturen ihre Services bereitstellen – rund um die Uhr, überall und unter allen Bedingungen. Gleichzeitig wachsen die wechselseitigen Abhängigkeiten dieser Systeme voneinander: eine Störung in einer Starkstromleitung in Norddeutschland kann sich auf die Energiesituation in anderen Teilen des Landes auswirken, und Probleme im mobilen Kommunikationsnetz in einer Region können die Steuerung des Smart Grids oder der Verkehrssysteme empfindlich beeinträchtigen. Dabei können solche Störungen vielfältige Ursachen haben: von Umwelteinflüssen wie Stürmen und Hochwasser über das Versagen technischer Komponenten bis zu Fehlern oder gezielten Angriffen in den IKT-Systemen oder menschlichem Versagen.

Unter diesen Bedingungen erweisen sich bisherige Sicherheitskonzepte als nicht mehr ausreichend. Wir benötigen neue Konzepte, die den zukünftigen Kritischen Infrastrukturen mit ihren

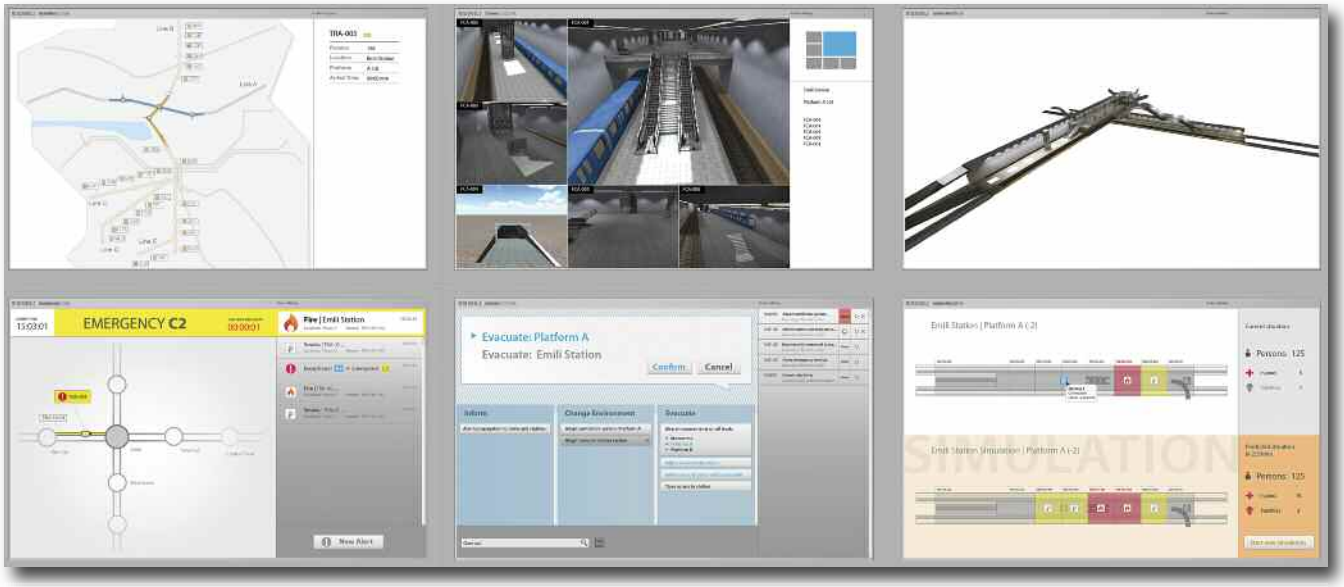


Abb 2: Entscheidungsunterstützung durch integrierte Information und Simulation *Quelle: SKYTEC AG*

verteilten, heterogenen, wechselseitig beeinflussten und hochgradig von IKT abhängigen Systemen Rechnung tragen. Der verteilte Charakter Kritischer Infrastrukturen bewirkt, dass sie durch unterschiedliche Organisationen und Systeme gesteuert werden. Durch die wechselseitigen Abhängigkeiten erfolgen diese Steuerungen jedoch nicht unabhängig voneinander. Folglich müssen Informationen zwischen den Steuerungszentralen der einzelnen Infrastrukturen ausgetauscht werden – rechtzeitig, in erforderlichem Umfang und in einer menschen- und computerverständlichen Form. Wer die Komplexität heutiger SCADA- und Steuerungssysteme kennt, ahnt, wie weitreichend eine solche Anforderung ist. Die Heterogenität der Systeme wirft ähnliche Fragen auf: Systeme, die unabhängig voneinander entstanden sind, müssen nun zuverlässig zusammenarbeiten – unter allen Bedingungen, also nicht nur im Normalbetrieb, sondern gerade auch im Störungs- oder Katastrophenfall. Insbesondere für die IKT- und Steuerungssysteme ist das eine große Herausforderung, denn häufig verfügen diese über ganz unterschiedliche Datenstrukturen, Informationsmodelle und Problemverarbeitungsalgorithmen, deren Interoperabilität alles andere als trivial ist.

Cyber-Physical Systems: Methodik, Modellierung, Simulation

Am Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS befassen sich Wissenschaftlerinnen und Wissenschaftler seit Jahren mit diesen Herausforderungen und entwickeln im Kontext europäischer und nationaler Forschungsprojekte (IRRIIS, DIESIS, EMILI, VASA, SECRET, HiPow)[1.)] einen einheitlichen methodischen Rahmen und leistungsfähige Softwaresysteme dafür. Die Methodik basiert auf dem Konzept der Cyber-Physical Systems (CPS) – Systemen also, die sowohl durch ihre physikalische Verhaltensweise als auch durch ihre Steuerung charakterisiert sind. Physikalische Modelle und Steuerungsverfahren müssen eng aufeinander abgestimmt werden – und das nicht nur für ein System, sondern für verteilte, heterogene "Systems of Systems", und nicht nur für den Normalbetrieb, sondern insbesondere auch für alle erdenklichen Arten von Störungen und Ausnahmesituationen. Dies wirft eine Reihe interessanter neuer Fragen auf, deren Beantwortung die Verbindung ganz unterschiedlicher Ansätze erfordert.

Im Kern geht es darum, eine neuartige ganzheitliche Sicht auf komplexe technische Systeme und ihre Umgebung zu entwickeln. Für zahlreiche einzelne "Sichten" existieren bereits erprobte Verfahren. Für den Lastfluss in Energienetzen oder den Verkehrsfluss in Ballungsräumen zum Beispiel gibt es bewährte Methoden. Die aktuellen Herausforderungen bestehen in der Vielfalt und dem Zusammenspiel unterschiedlicher Aspekte – insbesondere für Normal- und Ausnahmesituationen. Eine einfache Integration verschiedener Sichten scheitert häufig an den zugrundeliegenden unterschiedlichen Beschreibungs- und Modellierungsformen. Die Problemstellungen wie auch die verwendeten Datenmodelle und Problemlösungsverfahren sind zu verschieden, als dass eine einfache Verbindung mit vertretbarem Aufwand möglich ist. Mit konventioneller Softwaretechnologie ist das aufgrund der Komplexität häufig sehr aufwendig und kompliziert. Wir brauchen neue Methoden und neue Softwaretechnologien.

Neue semantische Softwaretechnologien

Die Methodik der Cyber-Physical Systems und semantische Softwaretechnologien bieten den erforderlichen leistungs-

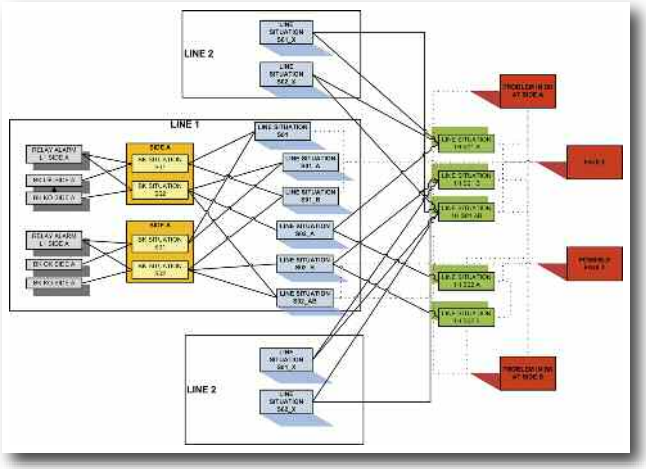


Abb 3: Komplexes Event Processing in einem Energienetz zur Klärung einer Fehlersituation Quelle: Groupo AIA

fähigen Rahmen. Mithilfe semantischer Verfahren lassen sich vielschichtige ganzheitliche Modelle komplexer Systeme entwickeln. Sie bieten die Basis für die erforderliche konsistente und transparente Integration unterschiedlicher Sichten – der Struktursicht, der Service- und Prozesssicht, der Steuerungs- und Kommunikationssicht etc. Dynamische semantische Simulationen unter Einschluss komplexer Ereignis- und Situationsmodelle ("Complex Event Processing") und entsprechender Reaktionsmöglichkeiten ("reactive rules") gestatten die Analyse des Systemverhaltens unter allen erdenklichen Bedingungen. Insbesondere können verschiedenste Störungs- und Ausnahmesituationen detailliert modelliert, simuliert und analysiert werden.

Dies spielt auch für die IT-Sicherheit in Kritischen Infrastrukturen eine zentrale Rolle. Zum einen wird niemand erwarten, dass in Kritischen Infrastrukturen gelingt, was in anderen Computer-Netzwerken nicht gelang: einen einhundertprozentigen Schutz gegen "cyber attacks". Cyber attacks der verschiedensten Art – vom "hacker kid" bis zu hochprofessionellen Kriminellen oder Terroristen – sind in der Realität zukünftiger Kritischer Infrastrukturen nicht auszuschließen. Es wird darum gehen, Angreifern das Handwerk so schwer wie möglich zu machen und die Schäden so weit wie möglich zu begrenzen. Dazu werden alle etablierten Mittel der Computersicherheit wie Antivirus-Programme und Firewalls in einer für Kritische Infrastrukturen adäquaten Weise zum Einsatz kommen. Dabei ist zu berücksichtigen, dass Kritische Infrastrukturen in mehrfacher Hinsicht von klassischen Computernetzen zu unterscheiden sind: sie sind zwangsläufig über physikalische Sensoren und Aktuatoren offene Systeme, sie sind oftmals sehr heterogen und verteilt und Menschen spielen in ihnen in verschiedenen Funktionen (Operator, Konsument, Teilnehmer) eine wichtige Rolle.

IT-Sicherheit für Kritische Infrastrukturen

Die Methodik der Cyber-Physical Systems sowie die darauf basierenden semantischen Modelle und dynamischen Simulationen bieten gerade auch für die Fragen der Cyber Security in Kritischen Infrastrukturen eine leistungsfähige Plattform. Die große Vielfalt technischer Komponenten und Systeme, ihr physikalisches Verhalten und ihre Wechselwirkungen, die Kommunikation der verschiedenen Steuerungssysteme, Sensoren und Aktuatoren einschließlich der Software und IT-Sicherheitskomponenten lassen sich in diesem einheitlichen Rahmen in all ihrer Diversität und Dynamik adäquat modellieren und simulieren. Verschiedene Szenarien können modelliert, simuliert und analysiert werden und es können geeignete Gegenmaßnahmen bewertet werden.

Entscheidungsunterstützung

Zur Beherrschung der Komplexität moderner Kritischer Infrastrukturen bedarf der Mensch der Unterstützung durch leistungsfähige Informationssysteme. Entscheidungsrelevante Informationen müssen in Echtzeit in geeigneter Weise bereitgestellt werden. Gleichzeitig müssen die Auswirkungen möglicher Entscheidungen analysiert werden können. Das kann angesichts der Komplexität der Systeme nur in seltenen Fällen "durch scharfes Hinschauen" geschehen. Oftmals sind genauere Berechnungen und Simulationen zukünftiger Systementwicklungen als Folge zu treffender Entscheidungen erforderlich. Entscheidungsunterstützungssysteme für Kritische Infrastrukturen benötigen umfangreiche Informationen sowie adäquate Modelle und Simulationen, um dem Operator die erforderlichen Hilfestellungen bieten zu können. Als Ergebnis unserer Forschungen entstehen Methoden und Systeme, die für ein großes Spektrum moderner Kritischer Infrastrukturen den Aufbau leistungsfähiger Entscheidungsunterstützungssysteme ermöglichen.

Verweise

[1] EMILI project, Deliverable D3.3: Use case modelling for implementation in SITE (www.emili-project.eu)

[2] R. Klein, Information Modelling and Simulation in Large Dependent Critical Infrastructures – An Overview on the European Integrated Project IRRIIS, in: R. Setola and S. Geretshuber (Eds.): CRITIS 2008, Critical Information Infrastructure Security. Springer Lecture Notes in Computer Science, 2009, Volume 5508, pp.131-143, DOI: 10.1007/978-3-642-03552-4_12

[3] R. Klein, St. Rilling, A. Usov, J.Q. Xie: Using complex event processing for modeling and simulation of cyber-physical systems, in: International Journal on Critical Infrastructures (IJCIS), Inderscience Publ., Vol.9 No. 1/2, 2013, pp.148-172.

1.) Siehe auch www.irriis.org, www.diesis-project.eu, und www.emili-project.eu

Die Botnetze von morgen schon heute erkennen

Jonathan P. Chapman, Dr. Felix Govaers und Dr. Elmar Gerhards-Padilla, Fraunhofer FKIE

Jonathan P. Chapman

Dr. Felix Govaers

Dr. Elmar Gerhards-Padilla

Sie stehlen Kontodaten, versenden Spam-Emails und manipulieren die Steuerung von Fabrikanlagen. Moderne Viren infizieren einen Rechner nicht nur, sondern bauen auch eine Verbindung zu ihren Autoren auf, über die der Rechner ferngesteuert werden kann. Ohne das Wissen ihrer Besitzer schließen sich die Rechner zu einem Botnetz zusammen, das von einem "Botherder" für seine Zwecke missbraucht werden kann. Botnetze werden nicht nur für gut sichtbare Angriffe wie Distributed Denial of Service (DDoS) genutzt, sondern auch für ungleich schwerer zu entdeckende Spionage und Sabotage, nicht zuletzt gegen Hochtechnologie-Unternehmen oder Behörden und Organisationen mit Sicherheitsaufgaben.

Die meisten Computer-Benutzer schützen sich mit einem Virenscanner, einer Firewall und regelmäßigen Betriebssystem-Updates gegen diese Angriffe. Wird ein Rechner dennoch infiziert, kann der Virus diese Schutzmaßnahmen aber deaktivieren und ist damit nicht mehr zu entdecken. Betreiber größerer Netzwerke sichern sich zusätzlich mit einem Intrusion Detection System (IDS), das – wie ein Virenscanner – den Netzwerkverkehr nach Mustern bekannter Angriffe absucht. Allerdings leiden sowohl lokale Virenscanner als auch IDS unter dem "Henne-Ei-Problem"; eine Infektion kann nur erkannt werden, wenn sie bekannte Muster aufweist; damit eine entsprechende Signatur erstellt werden kann, muss der Angriff jedoch erst einmal erkannt werden.

Als weitere Herausforderung für klassische IDS zeichnen sich zudem robuste Verschlüsselungsmechanismen ab. Im Alltag schützen sie unsere Passwörter und Kontodaten vor neugierigen Blicken und Missbrauch, sie können aber auch von Botherdern verwendet werden, um netzwerkbasierten Systemen den Blick in ihre Netzwerkpakete zu verwehren. Der Netzwerkverkehr enthält dann keine Muster mehr, die ein IDS erkennen könnte.

Dass dies keine rein theoretische Überlegung ist, beweist nicht zuletzt das im Dezember 2012 entdeckte SkyNET-Botnetz. Es nutzt den Anonymisierungsdienst "Tor", der zum einen die Kommunikationsinhalte verschlüsselt, zum anderen aber auch die Adressen der Kommunikationsteilnehmer verschleiert. Besonders perfide: Der SkyNET Command & Control-Server wird als "Tor Hidden Service" betrieben, die infizierten Rechner können so mit ihm kommunizieren, ohne dass dabei die Adresse des Servers bekannt wird. Traditionelle IDS haben daher keine Chance, von SkyNET infizierte Rechner zu erkennen.

Um diese und weitere komplexe Bedrohungen erkennen zu können, muss also ein völlig neuer Ansatz entwickelt werden. Die Forschungsgruppe Cyber Defense und die Abteilung für Sensordaten- und Informationsfusion des Fraunhofer FKIE arbeiten daher gemeinsam an einem System, das nicht die ausgetauschten Daten, sondern das Verhalten der Anwendungen, die diese Daten austauschen, analysiert. Anwendungen, die direkt von einem Benutzer bedient werden, werden hier als stochastischer Prozess mit großer Unsicherheit modelliert, während das fest einkodierte Verhalten der Schadsoftware wiederkehrende Muster aufweist.

Erste mit anderer Zielrichtung entwickelte Ansätze anderer Einrichtungen stellten sich bei genauerer Analyse als nicht übertragbar heraus. Die Forschungsgruppe Cyber Defense hat daher eine neue Methodik entwickelt, die wesentliche Merkmale des Anwendungsverhaltens aus der Messung von Netzwerkpaketen einer Verbindung extrahiert. Anders

als bei vergleichbaren Ansätzen werden die extrahierten Daten nun allerdings nicht isoliert, sondern jeweils die Gesamtheit der auf einen Rechner bezogenen Messungen betrachtet. Ein infizierter Rechner wird hier Konzentrationen im Messraum aufweisen, die das fest einprogrammierte Verhalten des Virus widerspiegeln.

Bei den oben genannten Messungen wird der Dateninhalt der erfassten Pakete, d.h. die Inhalte der Kommunikation, nicht berücksichtigt, das Verfahren also durch eine eventuell vorhandene Verschlüsselung nicht behindert. Dies kommt auch potentiellen Bedenken der Netzwerkbenutzer entgegen; das System erlangt zu keinem Zeitpunkt Kenntnis über die Inhalte ihrer Kommunikation. Auch die Endpunkte können durch eine Pseudonymisierung verschleiert werden, diese kann dann erst, z. B. durch einen Administrator, aufgehoben werden, wenn konkrete Hinweise für eine Infektion vorliegen. Die Verschleierung, wie sie das oben erwähnte SkyNET mit Hilfe von Tor durchführt, ist hingegen unwirksam, da sie die erfassten Kommunikationsmuster nicht hinreichend beeinträchtigt.

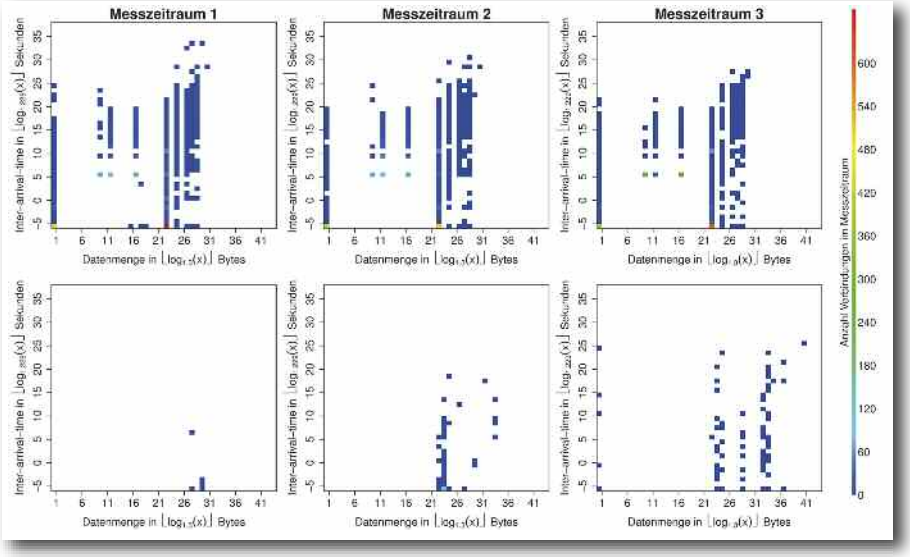


Abb 1: Datenmenge und zeitlicher Abstand zur letzten vorangegangenen Netzwerkverbindung mit ähnlicher Datenmenge in Messzeiträumen von jeweils 20 Minuten Länge. Die Grafiken in der oberen Reihe zeigen Messungen für eine Schadsoftware, die untere Reihe bildet Messungen für einen nicht infizierten Rechner ab.

In einem Testaufbau wurde echte Schadsoftware in einer gesicherten Umgebung, ohne Zugang zum Internet, ausgeführt und ihr Netzwerkverkehr aufgezeichnet. Zum Vergleich dienen Messungen für einen nicht infizierten Rechner, die am Internet-Zugang einer neuseeländischen Universität durchgeführt wurden. Die Messwerte der beiden Systeme unterscheiden sich in der erwarteten Weise.

Abbildung 1 zeigt einen Ausschnitt der oben angesprochenen Messungen. Betrachtet wird, wie häufig bestimmte Kombinationen der in einer Verbindung übertragenen Datenmenge mit dem zeitlichen Abstand zur letzten vorangegangenen Verbindung, in der eine ähnliche Datenmenge übertragen wurde, der "Inter-Arrival-Time", vorkommen. Da Letztere in einem kontinuierlichen Raum gemessen wird, wurden die Werte hier diskretisiert und zu Intervallen zusammengefasst. Messungen der Inter-Arrival-Time wurden in Abschnitte zusammengefasst, wenn ihr abgerundeter Logarithmus zur Basis 1,229 auf denselben Wert fiel. Analog wurde die Datenmenge in Abschnitte diskretisiert, hier wird allerdings der Logarithmus zur Basis 1,3 abgerundet. Die Basen der Logarithmen wurden so gewählt, dass sich die Messungen für eine große Anzahl Netzwerkverbindungen möglichst gleichmäßig auf die entstandenen Abschnitte verteilen.

Die obere Zeile von Abbildung 1 zeigt Messungen für die oben angesprochene Schadsoftware in drei aufeinanderfolgenden Messzeiträumen von jeweils 20 Minuten Länge, die Zeile darunter zeigt die entsprechenden Messungen für das nicht infizierte System. Auffällig ist nicht nur die große Anzahl der Verbindungen, die die Schadsoftware erzeugt, sondern vor allem deren Regelmäßigkeit. So zeugt z.B. in der linken unteren Ecke der Grafiken jeweils ein grüner Kasten von den knapp unter bzw. über 400 Verbindungen, die die Schadsoftware mit dieser Messwert-Kombination erzeugt hat. Die Messungen für den nicht infizierten Rechner zeigen zwar eine Tendenz zum Bereich 400-1500 Bytes, in dem üblicherweise die Anfragen eines Web-Browsers liegen, lassen aber kein wiederkehrendes Muster erkennen.

Im Fokus der Arbeit steht nun die automatisierte Verdichtung der Messungen zu einem präzisen und zuverlässigen Lagebild, so dass Netzwerkbetreiber rechtzeitig alarmiert oder sogar automatisiert Gegenmaßnahmen eingeleitet werden können. Das Fraunhofer FKIE trägt damit dazu bei, den Schutz unserer Unternehmen, Behörden und Organisationen vor neuartigen und hochentwickelten Bedrohungen wesentlich zu verbessern.

Kooperatives Monitoring zum Schutz kritischer Infrastrukturen

Till Elsner, Arnold Sykosch & Matthias Wübbeling, Fraunhofer FKIE

Till Elsner

Arnold Sykosch

Matthias Wübbeling

In einer zunehmend vernetzten Welt gewinnen elektronische Kommunikationsinfrastrukturen immer mehr an Bedeutung. Durch die Definition als kritische Infrastruktur (KRITIS) wird für Infrastrukturen mit besonderer Bedeutung für die Gesellschaft ein besonderer Schutzbedarf formuliert. Die "Nationale Strategie zum Schutz Kritischer Infrastrukturen" (KRITIS-Strategie) spricht von einem "zentralen Thema der Sicherheitspolitik unseres Landes".

Das Internet ist integrativer Bestandteil unserer heutigen Gesellschaft. Es ist in vielen Staaten die zentrale Ressource zur Informationsweitergabe für weitere kritische Infrastrukturen und trägt damit essenziell zur Funktionsfähigkeit von Staat und Wirtschaft bei. Als weltumspannendes Kommunikationsmedium ist es jedoch auch Nährboden für Bedrohungen globalen Ausmaßes. Angreifer können problemlos über Landes- und Verbundgrenzen hinweg agieren. Angriffe lassen sich mit minimalem Aufwand in globalem Maßstab koordinieren und durchführen.

Dies stellt den Schutz kritischer, vom Internet abhängiger Infrastrukturen vor eine besondere Herausforderung. Öffentliche und private Akteure müssen Bestandteile dieser Infrastruktur, die unter ihrer Verantwortung stehen, gegen die Bemühungen weltweit verteilt operierender Angreifer verteidigen. Den Sicherheitsverantwortlichen steht dabei meist nur eine sehr eingeschränkte Sicht auf potentiell bedrohliche Vorgänge zur Verfügung. Damit existiert ein verheerendes Informationsungleichgewicht zwischen den Sicherheitsverantwortlichen und den Angreifern, die sich lange in den Tiefen des globalen Netzes verbergen können.

Der Schutz vernetzter Informationssysteme erfordert zu jeder Zeit einen umfassenden Kenntnisstand über die aktuelle Lage und eventuelle Vorkommnisse in den betreffenden Netzen, die sich zu einer Gefahr für die zu schützenden Systeme entwickeln könnten. Das weltumspannende Ausmaß des Internets und die Unterteilung verschiedener administrativer Domänen macht die Gewinnung von Informationen über sich entwickelnde Bedrohungen für einzelne Organisationen besonders schwierig. Für den optimalen Schutz kritischer Informationssysteme ist jedoch ein umfassendes Bild der globalen Bedrohungslage erforderlich.

Im Projekt "MonIKA – Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung" nehmen wir uns dieser Herausforderung, durch Nutzung verteilter und kooperativer Ansätze zum Monitoring vernetzter Systeme, an. Die hier erarbeiteten Verfahren und Methoden sollen es in Sicherheitsfragen kooperierenden Partnern ermöglichen, gemeinsame Anstrengungen zur Sicherung von Infrastrukturen zu koordinieren und somit Sicherheitsressourcen effizienter nutzen zu können. Auf diese Weise können lokale Sicherungs- und Abwehrstrategien zur großflächigen Verbesserung der Sicherheitslage globaler Netze und damit auch der auf diesen Netzen basierenden, kritischen Infrastrukturen beitragen. Der Komplexität der Problemstellung mit Herausforderungen auch außerhalb der Informationstechnologie wird im Projekt "MonIKA" dabei durch ein Konsortium mit Experten auf allen, zur ganzheitlichen Betrachtung der Aufgabe notwendigen, Gebieten Rechnung getragen – neben dem Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE), der EADS Deutschland GmbH (Cassidian) arbeiten auch die Zivilrechtliche Abteilung des Instituts für Informations-, Telekommunikations- und

Medienrecht der Universität Münster (ITM) sowie das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) zusammen.

Ziel des Projekts ist die Schaffung eines Frameworks (vgl. Abbildung 1), das administrativen und operativen Sicherheitsverantwortlichen in Unternehmen, Behörden und anderen Institutionen Werkzeuge und Prozesse für eine intensive und gewinnbringende Kooperation bei der Sicherung von IT-Infrastrukturen an die Hand gibt. Zu diesem Zweck werden technische Verfahren entwickelt, die lokales Monitoring zu gemeinsamen verteilten Ansätzen bündeln. Zu diesem Zweck werden lokal erzeugte Datensätze zunächst pseudonymisiert, anschließend mit den Daten aller Teilnehmer fusioniert und für die Klassifikation der Ereignisse analysiert. Um die Praxistauglichkeit dieser Verfahren zu gewährleisten, werden diese während der gesamten Entwurfs- und Entwicklungsphase kontinuierlich auf ihre Konformität zu gesetzlichen Vorgaben und Datenschutzrichtlinien geprüft. Darüber hinaus wird mit der Orientierung an in der IT-Sicherheit etablierten Standards der Grundstein für eine reibungslose Integration in existierende Prozesse gelegt.

Beispielhaft für allgegenwärtige Gefahren für kritische Infrastrukturen werden im Rahmen des Projekts “MonIKA” Botnetze und Anomalien im globalen Internet-Routing als Bedrohungsszenarien aufgegriffen. Auf diese Weise lässt sich besonders gut der Nutzen und die Wirkungsweise der erarbeiteten Lösungen an Beispielen mit großem Gefahrenpotential aufzeigen.

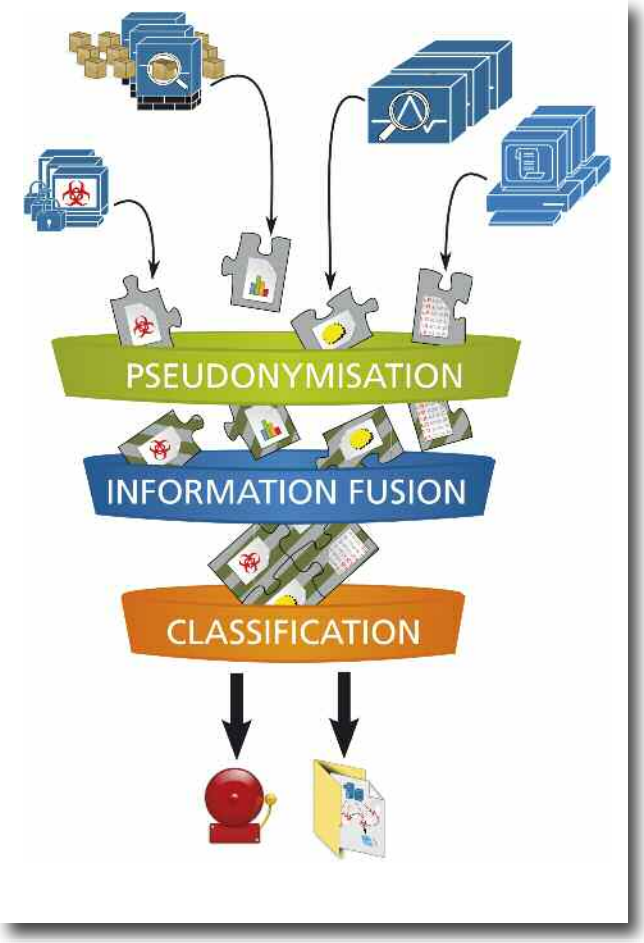


Abb 1: MonIKA-Prozess

Botnetzerkennung

Bei einem Botnetz handelt es sich um ein Netz von Computersystemen, die über einen gemeinsamen Kontrollkanal ferngesteuert werden können. Dabei handelt es sich bei diesen Computersystemen meist selbst um “Opfer”, die der Betreiber des Botnetzes durch Ausnutzung einer Sicherheitslücke unter seine Kontrolle gebracht hat. Das große Gefahrenpotential eines Botnetzes liegt darin, dass der Betreiber durch die Möglichkeit der Fernsteuerung einer immens großen Anzahl von Netzteilnehmern über extreme Ressourcen verfügt. Botnetzattacken, die häufig von mehreren tausend Rechnern gleichzeitig ausgehen, halten oft auch aufwändige Sicherheitsvorkehrungen nicht stand. Der sicherste Schutz vor Botnetzattacken ist die effektive Bekämpfung von Botnetzen selbst.

Um Botnetze effektiv bekämpfen zu können, sind genaue Kenntnisse über Aufbau, Kommandostruktur und Beschaffenheit des Botnetzes nötig. Je früher in seiner Entstehung ein Botnetz entdeckt wird, desto schneller lässt es sich unschädlich machen und kann so weniger Schaden anrichten. Hier profitiert der Kampf gegen Botnetze von verteiltem, kooperativem Monitoring. Einzelne, im lokalen Monitoring auffällig werdende Sicherheitsverstöße können so miteinander korreliert werden, um diese als Aktivität eines Botnetzes anstatt als isoliertes Ereignis identifizieren zu können.

Im Projekt “MonIKA” wird dafür, statt speziell auf die Detektion von Botnetzen ausgelegte Sensorik, auf bereits vorhandene Monitoring- und Sicherheitsinfrastruktur gesetzt. Da es sich bei Bots im Grunde um “normale” Schadsoftware handelt, können einzelne Aktionen dieser Bots mit Einrichtungen wie Malware-Scannern, Intrusion-Detection-Systemen oder Firewalls, die Bestandteile üblicher IT-Sicherheitsinfrastruturen sind, erkannt und analysiert werden. Besonderes Merkmal des Botnetzes ist die Kombination bestimmter Fähigkeiten sowie das koordinierte Verhalten von Bots. Hier bietet das MonIKA-Projekt ein Framework, mit dessen Hilfe diese Ereignisse in globalem Kontext analysiert und so die Erkennung und Analyse von Botnetzen unterstützt werden können. Durch Schnittstellen zu existierender Sensorik und die Entwicklung von Verfahren zur rechtskonformen

verteilten Erhebung, Zusammenführung, Fusion und Analyse von IT-Sicherheitsinformationen, schafft das MonIKA-Framework die Basis für eine erfolgreiche Kooperation von IT-Sicherheitsverantwortlichen, um durch den Austausch von Wissen und die Klassifikation von Vorfällen auf einer gemeinsamen Informationsbasis besser gegen Gefahren von globalem Maßstab, wie Botnetze, gewappnet zu sein.

Erkennung von Anomalien im globalen Internet-Routing

Das globale Internet-Routing ist trotz intensiver Forschung noch immer eine der bedeutendsten Schwachstellen des Internets. Da dieses lediglich ein Zusammenschluß voneinander (administrativ und operativ) unabhängiger Netze ist, ist auch die Kontrolle der tatsächlichen Kommunikationswege nicht ohne Weiteres möglich. Sobald ein IP-Paket auf dem Weg zum Ziel die eigene Domäne verlassen hat, gibt es weder die Möglichkeit, auf die gewählte Route Einfluß zu nehmen, noch sie überhaupt zuverlässig zu bestimmen. Selbst die übliche SSL-Verschlüsselung von Verbindungen bietet nach der Kompromittierung verschiedener Zertifizierungsstellen dann keinen realistischen Schutz mehr. Mögliche Angriffe gehen weit über das Abhören von Kommunikationsinhalten hinaus. Es ist möglich, Inhalte zu verändern und sogar den Kommunikationspartner komplett zu ersetzen, bzw. vom restlichen Internet abzuschotten. In regelmäßigen Abständen lässt sich beobachten, dass Routingänderungen zu weltweiten Verbindungsproblemen führen. Diese global sichtbaren Anomalien führen in den meisten Fällen zu einem systemweiten Ausfall betroffener Dienste. Deutlich unauffälliger und gefährlicher sind lokale Routing-Veränderungen. Da diese nur einen kleinen Teil des Internets betreffen, sind die Folgen in vielen Fällen nicht global sichtbar und sind aus diesem Grund in vielen Fällen auch für betroffene Internetnutzer nicht erkennbar.

Die Überwachung globaler Routing-Information ist derzeit auf einer sehr hohen Ebene bei Tier-1- und Tier-2-Providern möglich, dafür gibt es Daten vom RIS-Projekt des RIPE und vom RouteViews-Projekt der Universität Oregon. Lokale Anomalien können durch diese in der Regel nicht zuverlässig erkannt werden. Das “MonIKA”-Projekt adressiert diese Problematik durch die Nutzung unterschiedlicher Routing-Informationen von assoziierten Partnern. Diese sollen spezielle Monitoring-Software als Ergänzung zu bestehenden Systemen betreiben und liefern so wertvolle Informationen zu tatsächlicher Routennutzung.

An zentraler Stelle werden die unterschiedlichen Daten der jeweiligen Teilnehmer ausgewertet und ein aktuelles Bild der Routinglage erzeugt. Sollten Anomalien im globalen Internetrouting erkennbar sein, sollen betroffene Netze und alle MonIKA-Teilnehmer darüber informiert werden.

Es wurde bisher an verschiedenen Gegenmaßnahmen geforscht, allerdings gab es trotz vieler Konzepte noch kein tatsächlich wirksames Mittel, um Routing-Anomalien zu verhindern. Da Internet-Routing grundlegend für alle Dienste des modernen Internet ist, sind alle über das Internet abgewickelten Dienste von Anomalien im Routing betroffen. Diese Erkennung wird durch das Teilvorhaben “Erkennung von Anomalien” (EvA) innerhalb des MonIKA-Projekts abgedeckt.

Cockpit für die Cybersicherheit

Cyberkriminalität stellt eine ernste Bedrohung für Unternehmen und staatliche Institutionen dar. Doch wie kann man sich schützen? HP hat mit dem Private Security Operations Centre (PSOC) einen umfassenden Ansatz für ein internes und situationsbezogenes Cybersicherheitsmanagement entwickelt.

Kaum ein Tag vergeht ohne Meldung, dass Cyberkriminelle in das Netzwerk eines Unternehmens oder einer Behörde eingedrungen sind. Nach dem HP 2012 Cyber Security Risk Report ist die Zahl der aufgedeckten Sicherheitslücken 2012 um 19 Prozent auf 8.137 gestiegen. Gleichzeitig investieren die Organisationen immer mehr in die IT-Sicherheit sowie in Governance, Risikomanagement und Compliance (GRC) – doch offensichtlich ohne den gewünschten Erfolg. Die Gründe dafür: Das traditionelle IT-Sicherheitsmodell greift zu kurz; es werden oft punktuelle Problemlösungen implementiert; und meist handelt es sich um reaktive Maßnahmen.

Insofern ist es nach Meinung von HP Zeit für einen Paradigmenwechsel in der IT-Security: Eine effektive Cyber-Abwehr bedarf eines proaktiven Ansatzes, der auf einer ganzheitlichen Sicht beruht. HP unterstützt Bedarfsträger in den Ämtern und Ministerien sowie in Forschung und Industrie mit einer effektiven Architektur für internes und situationsbezogenes Cybersicherheitsmanagement, genannt HP PSOC. Es handelt sich um eine Komplettlösung, die sowohl Technologien als auch Mitarbeiter, Richtlinien und Prozesse sowie Informationen abdeckt. Sie kann schnell bereitgestellt und vollständig in die vorhandene Umgebung integriert werden.

Das HP PSOC lässt sich dabei auf die spezifischen Anforderungen einer Organisation abstimmen und führt durch die folgenden Aufgaben:

Cyber Readiness Assessment: Der erste Schritt besteht aus einer Bewertung der aktuellen Umgebung. Das Ergebnis ist ein Architekturkonzept und -modul mit Sicherheitskontrollen auf mehreren Ebenen.

Security Event Management: Sicherheitswarnmeldungen und -vorfälle, die im Netzwerk einer Organisation auftreten, werden überwacht und diese Vorfälle in Beziehung zueinander gesetzt sowie analysiert.

Integrated Threat Intelligence: Das System sammelt Informationen zu potenziellen Bedrohungen und Schwachstellen der Informations-Assets. So können Informationen analysiert und deren Glaubwürdigkeit und Zuverlässigkeit bewertet werden. Auch Bedrohungen und Schwachstellen werden so bewertet.

Security Operations Workflow: Das Framework bietet einen standardisierten Workflow für das Management und die Metriken der Sicherheitsverfahren.

Dashboard Reporting: Die Dashboards für Betriebsabläufe und Verwaltung bieten in Echtzeit Transparenz über den aktuellen Status des Sicherheitsrisikomanagements in der Organisation einschließlich ihrer spezifischen Business-Relevanz.

HP Enterprise Services bieten passend dazu umfassende Services zum Thema Unternehmenssicherheit und unterstützt Organisationen bei der Pflege und Verwaltung des PSOC sowie bei der Schulung der Mitarbeiter.

/go/defense

Warum HP?

HP verfügt über

- Technologieführerschaft: HP verfügt über langjährige Erfahrung und ein einzigartiges Portfolio an Servern, Storage und Networking, das für jede Kundenanforderung die passende Lösung bereitstellt
- mehr als 3.000 Sicherheits- und Datenschutzexperten und rund 17.000 zertifizierte ITIL-Experten
- mehr als 600 Sicherheitspatente und 5 Global Security Operations Center
- führende Forschungsgruppen und Initiativen im Security-Umfeld wie HP DVLabs, HP Fortify Software Security Research, HP Security Research und Zero Day Initiative
- eine Vielzahl von Security-Produkten, die Analysten wie Gartner immer als die führenden am Markt einstufen. Dazu gehören HP Enterprise Security Products, HP ArcSight, HP TippingPoint und HP Fortify. Daneben stehen Produkte aus dem Partner-Netzwerk zur Verfügung – einschließlich McAfee, Symantec und Checkpoint
- eine Vielzahl von Kunden im Verteidigungssektor. Dazu gehören das britische Verteidigungsministerium und die US-Marine

Transferpotential der Fusionstechnologie für Cyber Defense

Priv.-Doz. Dr. Wolfgang Koch, Sabine Schreiber-Ehle, Fraunhofer FKIE

Dr. Wolfgang Koch

Sabine Schreiber-Ehle

Realistische Chancen, die vielschichten Herausforderungen beim Schutz sicherheitskritischer Informationssysteme vor Cyber-Angriffen zu meistern, können sich in akzeptabel kurzen Zeitspannen nur dann ergeben, wenn alle bereits verfügbaren IT-Technologien auf ihre Relevanz geprüft und gegebenenfalls für die besonderen Bedürfnisse angepasst oder weiterentwickelt werden. Von wachsender Bedeutung ist in diesem Kontext die Daten- und Informationsfusion, deren Methoden zu verbessertem Cyber-Situationsbewusstsein beitragen können, der Voraussetzung für lageadäquate Bedrohungsabwehr.

"Kognitive Tools" für Lagebewusstsein

Aus wehrtechnischen Anwendungen erwachsen, möchte diese vergleichsweise junge Disziplin der Informatik die von Menschen geleistete Verknüpfung von Einzelinformationen verstehen, durch leistungsfähige Algorithmen nachbilden und verbessern, automatisieren sowie neuartige, von Menschen nicht unmittelbar auswertbare Daten einbeziehen. Betrachtet werden dabei unterschiedlichste Datenquellen, zum Beispiel Sensoren, die dem militärischen Nutzer neue Wahrnehmungsdimensionen erschließen, vor allem aber auch weiträumig verteilte Netze solcher Quellen. Wichtig sind ferner Datenbankensysteme, die verfügbares Hintergrundwissen zugreifbar machen, und nicht zuletzt die intelligente Interaktion mit den militärischen Akteuren, durch die individuelles Wissen und Erfahrungen in den Fusionsprozess einbezogen werden können.

Im Kontext von Intrusion-Detektion-Systemen (IDS), der Botnetz-Erkennung und Spionageabwehr sind wie in den meisten Anwendungen der Fusionstechnologie die zu fusionierenden Einzelinformationen in der Regel ungenau, unvollständig, falsch oder verfälscht, teilweise veraltet, schwer zu formalisieren oder manchmal sogar in Einzelaspekten widersprüchlich. Die technologisch-wissenschaftliche Herausforderung besteht darin, mit intelligenten Algorithmen auch aus Informationsbruchstücken hochwertige Information zur Lagebeurteilung zu extrahieren und dabei das zu nutzende Informationsaufkommen adäquat zu nutzen (Resource Management). Fusionssysteme bieten daher dem Nutzer "kognitive Tools", gewissermaßen eine "Servolenkung fürs Hirn", die seine Wahrnehmungs- und damit Entscheidungsfähigkeit ebenso steigern können wie konventionelle Werkzeuge seine physischen Kräfte.

Cyber-JDL-Modelle der Datenfusion

Entstanden ist die Sensordaten- und Informationsfusion für militärische Einzelanwendungen, in denen ein besonderer Unterstützungsbedarf besteht, etwa in zeitkritischen Situationen mit hohem Entscheidungsrisiko und zur Auswertung massenhaft einströmender Daten. Heute durchziehen Fusionstechnologien praktisch alle innovativen Bereiche der Wehrtechnik. Vor allem im Kontext der "Vernetzten Operationsführung" besitzt die Fusionstechnologie eine Schlüsselposition, um Sensorik, Vernetzung und Datenverfügbarkeit optimal zu nutzen. Abbildung 1 zeigt das sogenannte "JDL-Modell" der Sensordaten- und Informationsfusion, das die verschiedenen Fusionsebenen veranschaulicht. Dieses Modell gibt eine integrierte Zusammenschau der vollständigen funktionalen Kette von sensoriellen verteilten Datenquellen, Datenbanksystemen sowie menschlichen Beobachtermeldungen und ihren Handlungsoptionen zusammen mit Rückkopplungsschleifen auf unterschiedlichen Ebenen wieder. Es wurde von den "Joint Directors of Laboratories" (JDL) entwickelt, einem Beratungsgremium des US-Verteidigungsministeriums.

All diese Aspekte haben eine natürliche Entsprechung zu den Problemen, die bei der Gewinnung von Cyber-Situationsbewusstsein zunächst begrifflich geklärt, angemessen formalisiert und durch die Entwicklung algorithmischer

Tools gelöst werden müssen. Wie die stetig anwachsende Fachliteratur zu dieser Problematik zeigt, wird dieser Weg bereits in zahlreichen Forschungsgruppen beschritten.

Generell lässt sich bei der Übertragung der Begriffsbildungen aus der "Fusionswelt" festhalten, dass unterschiedliche Auffassungen über Granularität der Input-Daten herrschen sowie Vorstellungen darüber, wie die Prozessketten zur Gewinnung lagerelevanter Informationen in geeignete funktional abgeschlossene Teilschritte gegliedert werden soll. Daraus ergibt sich die Notwendigkeit, das klassische JDL-Modell der Informationsfusion für die Lagebilderzeugung bei Cyber Defence abzuwandeln.

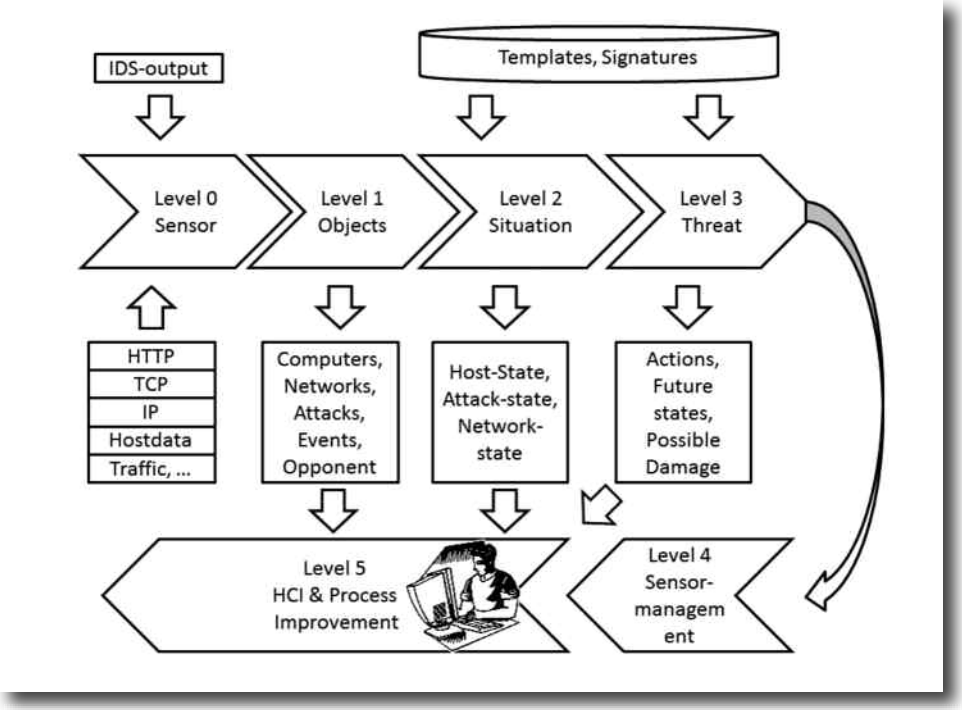


Abbildung 1: Das JDL-Modell, angepasst auf Cyber Situational Awareness, beschreibt die funktionale Fusionskette, von verteilten heterogenen Datenquellen über Datenbanken und Meldungen bis hin zu den Entscheidern einschließlich verschiedener Feed-back-Loops.

Quelle: © Fraunhofer

Als besonders relevant zur Gewinnung von Cyber-Situationsbewusstsein erweisen sich vor allem die Ebenen 2 und 3 des JDL-Modells (Level 2 processing – situation refinement – dynamically develops a description of current relationships among entities and events in the context of their environment; level 3 processing – significance estimation – projects the current situation into the future to draw inferences about threats, vulnerabilities, and opportunities for operation).

Ausgewählte Forschungsansätze

Aber auch Level-o-Verarbeitung (combining signal level data to obtain initial information about an observed phenomenon) besitzt unmittelbare praktische Relevanz. Sie erweist sich als wichtiger Ansatz zur Verdichtung des Outputs von (netzwerkbasierten) IDS, die ihre Input-Daten auf der Grundlage von Domänenwissen interpretieren. Zahlreiche publizierte Ansätze nutzen in diesem Sinne den Output von IDS für die algorithmische Weiterverarbeitung und Verdichtung von Information. Auf den sich daran anschließenden höheren Fusionsebenen werden in der Forschungsliteratur vor allem Fragen des Matchings im Hinblick auf Templates und Signaturen auf der Basis von Datenbanken untersucht, in denen Erfahrungen aus bekannten Cyber-Angriffen als Domänenwissen abgelegt werden.

Ein wesentlicher Vorteil bei der Nutzung von Fusionstechnologie scheint die Reduktion der Falschalarme zu sein, in denen normale Arbeitsaktivitäten als feindliche Aktion interpretiert werden. Neben dem wirtschaftlichen Schaden können etwa im Falle kritischer Infrastrukturen die Auswirkungen gravierender sein.

Darüber hinaus wird in der Literatur berichtet, dass die Erkennung auf andere Weise nicht detektiertbarer Angriffe gesteigert werden kann. Grundsätzlich gibt es zwei Vorgehensweisen: Systeme, die IDS-Output als Sensordaten verwenden und solche, die herkömmliche ID-Systeme ersetzen. Die offene Literatur beschreibt ferner auf fusionsbasierte Methoden zur Prädiktion künftiger Systemzustände und Angreifer-Aktivitäten. Die Bedrohungslage kann auf dieser Basis besser beurteilt und Gegenmaßnahmen effektiver und zeitnah geplant werden. Auch zur Erschließung von Zusammenhängen aus Massendaten mit unsicherem und geringem Informationsgehalt sind Fusionsmethoden anwendbar.

Aufbauend auf der langjährigen Expertise auf dem Gebiet der Sensordaten- und Informationsfusion im Fraunhofer FKIE, wird das Transferpotential der Fusionstechnologie auf Aspekte im Kontext von Cyber Defence ausgelotet.

Informationsauswertung aus offenen Textquellen

Prof. Dr. Ulrich Schade, Fraunhofer FKIE

Prof. Dr. Ulrich Schade

Informationen von allgemeinem und besonderem Interesse sind häufig offen zugänglich. Die Aufgabe, diese Informationen automatisiert aus den offenen Quellen zu gewinnen, ist jedoch nicht einfach, insbesondere dann, wenn die Quelle eine Textquelle ist. Im Folgenden sollen daher computerlinguistische Verfahren vorgestellt werden, mit denen eine Aufbereitung der fraglichen Texte erfolgen kann, so dass diese dann einer automatisierten Auswertung zugänglich sind.

Das Verfahren, mit welchem Texte für die Auswertung aufbereitet werden, beginnt mit der in der Computerlinguistik so genannten "Informationsextraktion". Dabei durchläuft der fragliche Text eine Kette von Prozessen auf der Grundlage von GATE, einer durch die Universität Sheffield entwickelten Software (http://gate.ac.uk/), die de facto den Standard für die Informationsextraktion vorgibt. Die Module für die Einzelprozesse der Prozesskette sind dann in Bezug auf die Sprache, in der der Text vorliegt, und in Bezug auf das Ziel der Textaufbereitung anzupassen bzw. durch eigene Entwicklungen zu ersetzen. Typischerweise werden Module für die folgenden Aufgaben verwendet. Zunächst werden ein "Tokenizer" und ein "Sentence Splitter" eingesetzt, um Wort- und Satzgrenzen zu bestimmen.

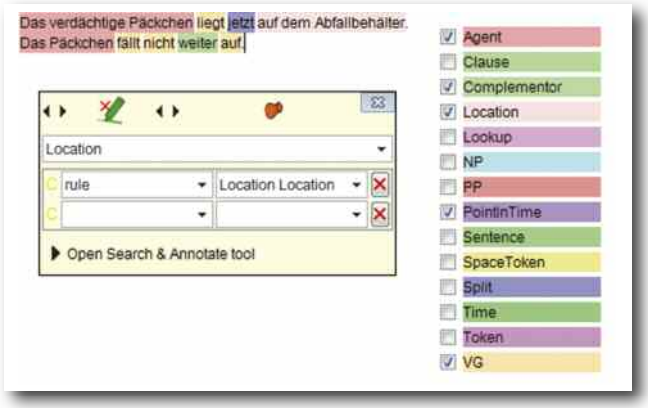


Abb 1: Annotation der semantischen Rollen. Für den ersten Satz wird "jetzt" die Rolle "Point in Time" zugewiesen. Die Konstituente "auf dem Abfallbehälter" wird als "Location" markiert.

Danach ordnet ein "Part-of-Speech Tagger" den erkannten Wörtern deren syntaktische Kategorie zu. Diese Aufgabe ist weniger einfach, als sie zunächst erscheint. So sollte das "auf" in "Das verdächtige Päckchen liegt jetzt auf dem Abfallbehälter." als Präposition klassifiziert werden, wohingegen es in "Das Päckchen fällt nicht weiter auf." als Teil des Verbs ("auffallen") erkannt werden sollte. Nachdem ihre Wortart erkannt wurde, kann man Wörtern mit einem "Morphological Analyzer" auch deren weitere morpho-syntaktischen Eigenschaften zugewiesen, etwa den Numerus bei Nomen ("Päckchen" und "Abfallbehälter" stehen im Singular). Eigennamen und deren Zusammensetzungen werden dann durch einen "Named-Entity-Recognizer" erkannt und in Bezug auf ihren Typ klassifiziert. Die Wortfolge "Frau Dr. Angela Merkel" wird dabei etwa als Bezeichnung für eine Person annotiert. Schließlich erfolgen über Parser- bzw. Chunker-Module, die auf den bis dahin erzielten Ergebnissen aufsetzen, syntaktische Analysen der Sätze, was wiederum als Grundlage des so genannten "Semantic Role Labeling" dient. In diesem Prozess werden den Satzteilen deren semantische Funktionen zugewiesen. So wird etwa die Präpositionalphrase "auf dem Abfallbehälter" in dem erwähnten Beispielsatz als Ortsbezeichnung annotiert. Abbildung 1 zeigt am Beispiel eines englischen Satzes, wie das Ergebnis von Informationsextraktion mit anschließendem "Semantic Role Labeling" aussieht.

Die hier skizzierte Prozesskette von Informationsextraktion und "Semantic Role Labeling" bezieht sich auf die Module, die notwendigerweise eingesetzt werden. Weitere Module sind etwa a) ein "Language Recognizer", der zu Beginn des Prozesses die im Text genutzte Sprache bestimmt bzw. Sprachwechsel annotiert, b) ein Modul zur Rechtschreibkorrektur, welches mögliche Rechtschreibfehler im Text bestimmt und gegebenenfalls korrigiert, oder c) ein Modul zur Auflösung von Anaphern, welches insbesondere für Personalpronomen vorhergehende Konstituenten bestimmt, auf welche sich die Pronomen beziehen.

Das Ergebnis der Textaufbereitung auf der Grundlage von Informationsextraktion und "Semantic Role Labeling" wird in ein XML-Format transformiert, wobei die semantischen Rollen, die das "Semantic Role Labeling" zuordnet als XML-Tags dienen. In dieser Form ist der Text dann automatisch auswertbar. Die Art der Auswertung ist dabei durch die gewünschte Anwendung vorgegeben. Aus den Anwendungen, die Fraunhofer FKIE

untersucht hat bzw. derzeit nutzt, seien hier zwei Beispiele genannt, AUGE und EnArgus.

In dem durch die Bundeswehr geförderten Projekt AUGE (AUtomatisierte GEfahrenerkennung) mit dem Hauptauftragnehmer IABG (Kontakt: ZieglerJ@iabg.de) wurden vorliegende Texte, insbesondere Meldungen, aufbereitet, um dann mit speziell entwickelten Indikatoren abgeglichen zu werden. Werden dabei Indikatoren getroffen, so ergibt sich daraus eine Aktivierung innerhalb eines Bayes'schen Netzwerks, welches die IABG automatisch aus Gefährdungsmodellen berechnet. Kombinationen von Aktivierungen in diesem Modell können dann dazu führen, dass das System von einer Gefährdungsmöglichkeit ausgeht und den Operateur auf die Untermenge der Meldung hinweist, aus der die Gefährdungsmöglichkeit errechnet wurde.

EnArgus® (https://enargus.de/) ist ein aufgrund eines Beschlusses des Bundestages vom Bundesministerium für Wirtschaft und Technologie gefördertes Verbundvorhaben. Wissenschaftler aus den Bereichen Energietechnik und Informatik arbeiten hierbei an der Konzeption, Entwicklung und Erprobung eines zentralen Informationssystems für Energieforschungsvorhaben. Die semantische Suche innerhalb dieses Systems (Abbildung 2 zeigt die entsprechende Ausgangsmaske) nutzt eine Ontologie, welche teilweise mit den genannten Verfahren automatisiert erstellt wurde. Beide Beispiele untermauern die Nutzbarkeit der skizzierten Verfahren und motivieren damit die Entwicklung von Ansätzen, diese Verfahren auch für die Informationsauswertung aus offenen Textquellen nutzbar zu machen.

Abb 2: Maske für die semantische Suche in EnArgus® public

Balanced HSI (Human Systems Integration) und kooperative Automation für eine nutzerorientierte, ausbalancierte Integration von Mensch und Technik in Cyber Defense

Prof. Dr.-Ing. Frank Flemisch, Susan Träber, Dr. Carsten Winkelholz,
Fraunhofer FKIE

Prof. Dr.-Ing. Frank Flemisch

Susan Träber

Dr. Carsten Winkelholz

Cyber Crime und Cyber Defense wurden zwar durch technische Entwicklungen wie Computer und Internet erst möglich, werden aber letztlich immer von Menschen im Zusammenspiel mit Technik ausgeführt. Das Zusammenspiel von Mensch und Technik wird am Forschungsstandort Wachtberg bereits seit einem halben Jahrhundert systematisch unter dem Blickwinkel der Anthropotechnik und Ergonomie erforscht. Die Verbindung von Ergonomie mit den Systemwissenschaften zur Systemergonomie wurde dort erstmals in den 1970ern systematisch ausgearbeitet (z.B. von Bernotat, Döring, Gärtner), hat sich von dort in Europa und die USA verbreitet, wurde in den USA unter Einbeziehung der Human Factors zur Human Systems Integration erweitert und z.B. von NASA und dem US-Verteidigungsministerium als wesentliche Querschnittsdisziplin für sicherheitskritische Projekte eingesetzt. Der Begriff Human Systems Integration findet zunehmend auch in Europa und Deutschland Verwendung, wird dort systematisch in Richtung einer Balanced HSI weiterentwickelt und an klassischen Herausforderungen wie z.B. automatisierten Verteidigungssystemen in Schiffen, Fahrzeugen und Flugzeugen, sowie an historisch neuen Herausforderungen wie Cyber Defense geschärft.

Systemergonomische Analyse: (Wett-)Kampf der Mensch-Maschine Systeme, Kreativität und Komplexität

Wesentlich für Human Systems Integration ist der Gedanke, dass nicht nur Einzelsysteme isoliert betrachtet werden, sondern auch in ihrem Zusammenwirken als Gesamtsystem (System of Systems) innerhalb der relevanten Systemumgebung. Startpunkt von HSI ist oft die Systemanalyse. Für den Anwendungsbereich Cyber Defense konnte folgendes Systemmodell (Abb.1) aus der Analyse abgeleitet werden. Aus der Abbildung 1 wird ersichtlich, dass Cyber Security bzw. Informationssicherheit (Vertraulichkeit, Verfügbarkeit, Integrität) nicht nur als Systemeigenschaft, sondern vor allem als kontinuierlicher Prozess des Cyber Defense Systems verstanden werden sollte. Ziel dieses Prozesses ist es, die zu verteidigenden Systeme gegen Cyber Threats im Sinne eines dynamischen Gleichgewichtes stabil zu halten. Die Herausforderungen, die sich hierbei stellen, ergeben sich aus der sich zunehmend erhöhenden Dynamik, Kreativität der Angreifer und folglich einer nicht-deterministischen Komponente der Cyber-Bedrohungen. Um diesen Herausforderungen angemessen begegnen zu können, ist der Einsatz von rein technischen Lösungen nicht ausreichend. Das “Law of Requisite Variety” (Ashby, 1956) deutet darauf hin, dass es für eine Vielfalt und Kreativität auf der Angriffsseite auch eine ausreichende Vielfalt und Kreativität auf der Verteidigungsseite geben muss, damit Verteidigung langfristig überhaupt eine Chance hat.
Es bedarf also früher oder später der aktiven Einbeziehung des Menschen in die Protektions-, Detektions- und Abwehrprozesse, um der Kreativität der Angreifer entgegenwirken zu können bzw. um die Komplexität der Abwehrmaßnahmen entsprechend der Angriffe zu erhöhen. Nur wenn dies gelingt, kann das Cyber Defense System eine inhärente Anpassungsfähigkeit entwickeln, welche die Adaption an eine sich än-

dernde Umwelt ermöglicht. Durch unterschiedliche Maßnahmen auf den verschiedenen Ebenen des soziotechnischen Systems kann diese Entwicklung systematisch unterstützt werden. Eine stärkere kognitive Einbindung des Menschen kann beispielsweise auf Ebene der Primäraufgaben durch die Anwendung neuer Mensch-Computer-Interaktions-Konzepte (z. B. Kooperative Automation) erzielt werden. Auf organisatorischer Ebene hingegen kann mit Konzepten, welche die Selbstorganisation sowie team/organisational learning fördern, sowie dem dafür dienlichen Einsatz von Kommunikations-, Koordination- sowie Kollaborationsplattformen, unterstützend eingewirkt werden. Weiterhin ist die Komplexität eine wesentliche Systemeigenschaft: Einfache und für den Verteidiger transparente Systeme sind normalerweise einfacher zu verstehen, und damit einfacher zu verteidigen.

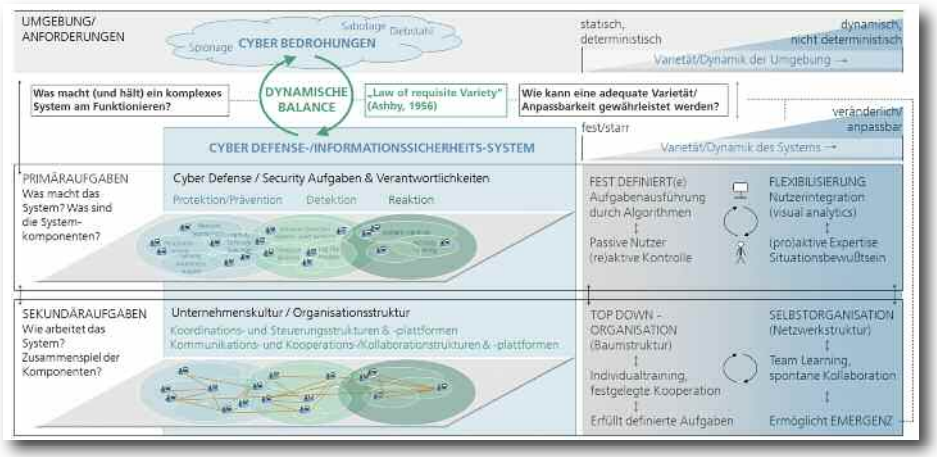


Abb 1: Cyber Defense Systemmodell mit Balance aus Stabilität und Variabilität

Lösungsansatz zur ganzheitlichen Entwicklung von Cyber Defense Systemen: Nutzerorientierte, ausbalancierte HSI und Kooperative Automation

Neben dem Spannungsfeld zwischen Variabilität und Stabilität in Cyber Defense Systemen gibt es eine Reihe weiterer Spannungsfelder wie z.B. die Hauptqualitäten Systemperformanz, Sicherheit, Gebrauchstauglichkeit, Joy of Use und Kosten. Dabei ist es nicht möglich, alle Qualitäten gleichermaßen zu maximieren bzw. minimieren, sondern es ist oft eine Abwägung bzw. ein Ausbalancieren verschiedener Faktoren nötig. Zur Überbrückung dieser Spannungsfelder wird am FKIE und anderen Forschungseinrichtungen die Systemergonomie / HSI unter Einbeziehung des Nutzerzentrierten Gestaltens (User Centered System Design) systematisch zur einem nutzerorientieren, ausbalancierten HSI weiterentwickelt und im Bereich Cyber Defense eingesetzt. Der Grundgedanke der Balance kann auch die Frage nach der richtigen Aufgabenverteilung zwischen Mensch und Automatisierung im System unterstützen: Ziel der vom FKIE und Partnern verfolgten Forschung an kooperativer Automation ist eine synergetische Verbindung zwischen Mensch und Automation, bei der Nutzer und die Automation kompatible Ziel- und Vorgehensmodelle haben und in einer dynamisch ausgehandelten Funktionsverteilung gemeinsam abarbeiten. Die berechtigte Hoffnung ist, dass eine kooperative Automation und eine gut ausbalancierte Vorgehensweise bei der Integration dieser technischen Systeme mit dem Menschen die Verteidigungsfähigkeit gegen Cyberangriffe deutlich erhöhen wird.

Ashby, W.R.: An Introduction to Cybernetics. Wiley, New York, 1956

Strategische Krisenmanagement-Übung "LÜKEX 11" – Weiterentwicklung der Sicherheit in der Informationstechnik

Oberst a.D. Werner Baach, Projektgruppe LÜKEX (Bund) des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe

Oberst a.D. Werner Baach

In einer zunehmend vernetzten Welt sind Staat und Gesellschaft, Wirtschaft und Unternehmen zunehmend vom Funktionieren der Informationsstrukturen abhängig: Ihr Ausfall könnte schwerwiegende Folgen für das öffentliche Leben haben. Je größer die Abhängigkeit der Menschen von der Informationstechnik (IT) wird, desto dringender stellt sich die Frage nach ihrem Schutz. Das stellt auch das Krisenmanagement im Bevölkerungsschutz Deutschlands vor neue Herausforderungen. Es muss, auf der taktisch-operativen Ebene ebenso wie auf der obersten politisch-administrativen (strategischen), auf Bedrohungen des IT-Sektors schnell und wirksam reagieren können. Um den Schutz der IT-Systeme, insbesondere im Bereich Kritischer Infrastrukturen (KRITIS), zu gewährleisten und die Gesellschaft für die Thematik zu sensibilisieren, beschloss die Bundesregierung im Februar 2011 die "Cyber-Sicherheitsstrategie für Deutschland"[1.]. Die Krisenmanagement-Übung "LÜKEX 11"[2.] befasste sich im Sinne dieser Strategie unter der Themenstellung "Sicherheit in der Informationstechnik" mit der Weiterentwicklung sowohl des allgemeinen Krisenmanagements als auch der speziellen Strategien zum Schutz der IT-Infrastrukturen in Deutschland.

LÜKEX steht für Länderübergreifende Krisenmanagement-Übung / Exercise Quelle: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

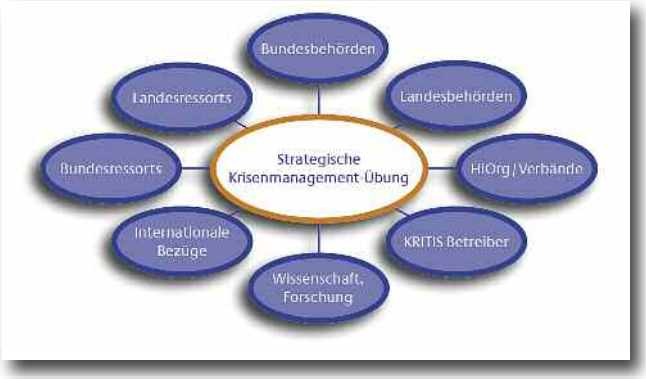
"LÜKEX 11" wurde am 30. November und 1. Dezember 2011 bundesweit durchgeführt. Teilnehmer waren schwerpunktmäßig die für das bereichsübergreifende strategische Krisenmanagement sowie die für das IT-Sicherheitsmanagement verantwortlichen Stellen des Bundes und der Länder, ferner KRITIS-Unternehmen, Hilfsorganisationen und Verbände. Der Übungsdurchführung vorangegangen waren über 18 Monate intensiver Planung und Vorbereitung. Die Federführung für die Übung hatte das Bundesministerium des Innern (BMI) in enger Abstimmung mit den beteiligten Ländern. Planung, Vorbereitung, Durchführung und Auswertung lagen beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK). Die IT-Fachexpertise brachte das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein. Seine Fachkunde war eine wesentliche Voraussetzung für die Entwicklung eines realitätsnahen Krisenszenarios.

Hauptübungsstäbe waren die Krisen-/Verwaltungsstäbe des Bundes und der Länder. Die Länder Hamburg, Hessen, Niedersachsen, Sachsen und Thüringen waren als "Intensiv-Übungsländer" in besonderer Übungstiefe beteiligt. Insgesamt wirkten 10 Bundesressorts, 20 Bundesbehörden, 12 Bundesländer mit nachgeordneten Landesbehörden, 45 KRITIS-Unternehmen, Hilfsorganisationen und Verbände sowie zwei internationale Organisationen (Europäische Zentralbank und EUROCONTROL) mit. In der Phase der Übungsdurchführung, dem Höhepunkt von "LÜKEX 11", waren bundesweit fast 3.000 Personen beteiligt. Durch die breite

Übungsbeteiligung und die lange vertrauensvolle Zusammenarbeit bei Vorbereitung und Durchführung der Übung sind wichtige Kooperationsnetzwerke entstanden, die im Falle einer realen IT-Krise die Abwehr von Bedrohungen wesentlich erleichtern dürften.

Bundesweite Krise durch Cyber-Attacken

Die ministerielle Vorgabe für das Übungskonzept und die Übungsziele forderte "das Beüben der ressortübergreifenden Krisen-/Verwaltungsstäbe des Bundes und der Länder sowie der länderübergreifenden Koordinierungsgremien beim Übergang vom IT-Krisenmanagement zum bereichsübergreifenden Krisenmanagement". Zum Erreichen dieser Zielvorgabe waren die Eckpunkte des Übungsszenarios wie folgt festgelegt worden: "Das Übungsszenario geht von IT-Störungen durch zielgerichtete Angriffe aus … In der Folge können erhebliche Beeinträchtigungen im Bereich Kritischer Infrastrukturen und Versorgungsengpässe im gesellschaftlichen Umfeld eintreten." Die Cyber-Angriffe, so das Übungsdrehbuch, sollten im Übungsverlauf zu einer bundesweiten Krise führen. Von den Störungen und Angriffen besonders betroffen wurden die IT-Strukturen und -anwendungen in vier ausgewählten KRITIS-Sektoren: Staat und Verwaltung; Informationstechnik und Telekommunikation; Transport und Verkehr; Finanz- und Versicherungswesen. Gegen Verwal-



Kooperationsnetzwerke unterstützen reales Krisenmanagement Quelle: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

Sitzung des Krisenstabes BMI

Quelle: Bundesministerium des Innern

tungen des Bundes und der Länder wurde eine multifunktionale Schadsoftware eingesetzt, die in den betroffenen KRITIS-Sektoren erhebliche Störungen verursachte. Auswirkungen auf wichtige Bereiche des öffentlichen Lebens waren die Folge, u.a. im Zahlungsverkehr, im Bereich der Telekommunikation und im Luftverkehr. Das Management der Krisenstäbe richtete in der Übung den Schwerpunkt darauf, durch ressort- und bereichsübergreifendes Zusammenwirken das Funktionieren der Informationsinfrastrukturen so weit wie möglich zu erhalten bzw. wieder herzustellen und die allgemeinen gesellschaftlichen Auswirkungen der Krise so gering wie möglich zu halten.

Gesamtkrisenmanagement weiter verbessert

Ein Hauptziel von "LÜKEX 11", das "Einüben und Erproben des konzertierten Handelns der Krisen- und Verwaltungsstäbe des Bundes und der Länder auf der politisch-administrativen (strategischen) Entscheidungsebene unter Einbeziehung von privaten Betreibern Kritischer Infrastrukturen" wurde durchweg erreicht. Die Stabsstrukturen und -Verfahren konnten gefestigt werden, die Arbeit der Stäbe spielte sich im Verlauf der Übung immer besser ein. Gleiches gilt für das Zusammenspiel von Bund, Ländern und KRITIS-Unternehmen. Es zeigte sich, dass das Konzept der LÜKEX-Übungen die Entwicklung von Stabsstrukturen und -Verfahren, die Weiterbildung des Stabspersonals sowie die Förderung des übergreifenden Zusammenwirkens der Stäbe wesentlich unterstützt. Die Übung zeigte aber auch, dass die Netzwerkbildung, insbesondere zwischen öffentlicher Verwaltung und privaten KRITIS-Betreibern, intensiviert werden sollte.

Ein weiterer Übungsschwerpunkt von "LÜKEX 11" war die externe und interne Krisenkommunikation. Sie ist ein Schlüsselelement im strategischen Krisenmanagement und kann Ausprägung und Verlauf von Krisen entscheidend beeinflussen. Entsprechend dieser Bedeutung wurde von den Krisen- und Verwaltungsstäben eine "breit angelegte, abgestimmte, aktive Öffentlichkeitsarbeit zur situationsgerechten Information der Bevölkerung und Einsatzkräfte im Rahmen eines vorausschauenden, ressortübergreifenden Krisenmanagements" verlangt. Erstmals wurden die Übenden dabei auch mit der Funktionsweise und den Nutzungsmustern der "Neuen Medien" (social media) konfrontiert. Insgesamt haben Leitungen wie Stäbe die Bedeutung der Krisenkommunikation erkannt und in ihre Maßnahmenplanungen angemessen einbezogen. Es zeigte sich dabei aber auch, dass gerade auf dem Gebiet der externen Kommunikation die Verfügbarkeit zahlenmäßig ausreichenden, gut ausgebildeten Personals den Erfolg der Kommunikation wesentlich mitbestimmt.

IT-Krisenmanagement in das Gesamtkrisenmanagement einbinden

Erstmals auf der strategischen Ebene wurden die Strategien zum Schutz der nationalen Informationsinfrastrukturen von Bund, Ländern und KRITIS-Unternehmen in einer gemeinsamen Übung überprüft. Dabei hat sich die existenzielle Bedeutung der Sicherheit einzelner IT- und Kommunikationsstrukturen und -prozesse gezeigt, ebenso die Notwendigkeit, diese Strukturen klar zu identifizieren, um sie wirksam schützen zu können. Insbesondere aber wurde deutlich, dass die Bewältigung einer IT-Krisenlage von Anfang an die Einbindung des IT-Krisenmanagements in das Gesamtkrisenmanagement verlangt. Dazu erforderliche Integrationsprozesse wurden durch die Übung angestoßen. Erstmalig wurde in "LÜKEX 11" auch die Umsetzung des Beschlusses des IT-Rates[3)] für die "Strukturen und Prozesse zur IT-Krisenreaktion der Bundesverwaltung" überprüft. Der Beschluss ist eine wesentliche Grundlage für das Zusammenwirken der Bundesressorts im Fall einer Krise. Die vorbereiteten Strukturen und Prozesse haben sich nach allen vorliegenden Übungserkenntnissen grundsätzlich bewährt. Das BSI konnte als Kompetenzzentrum und Koordinierungsinstanz wichtige Impulse zur Behebung der in die Übung eingespielten IT-Probleme geben und wesentlich zu den Problemlösungen beitragen. Das Amt versorgte die Bedarfsträger verlässlich mit einem aktuellen IT-Lagebild, den notwendigen Warn- und Alarmierungsmeldungen sowie mit Handlungsempfehlungen im Schadens-/Störungsfall.

Im Rahmen der KRITIS-Zusammenarbeit wurde auch der "Umsetzungsplan Kritische Infrastrukturen des Nationalen Plans zum Schutz der Informationsinfrastrukturen" (UP KRITIS) überprüft. Mit diesem Plan verpflichten sich Unternehmen, ein Mindestniveau der IT-Sicherheit einzuhalten und sich mit dem Bund zu Fragen der IT-Sicherheit und der Umsetzung von Schutz- und Abwehrmaßnahmen auszutauschen. Die Zusammenarbeit an den Schnittstellen des Pla-

Virtuelle Medien bei "LÜKEX 11"

Quelle: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

nes konnte in der Übung jederzeit reibungslos sichergestellt werden.

Erstmals war das 2011 als Bestandteil der "Cyber-Sicherheitsstrategie für Deutschland" eingerichtete "Nationale Cyber-Abwehrzentrum" in eine strategische Übung eingebunden. Das Zentrum, als gemeinsame Plattform zum schnellen Informationsaustausch und zur besseren Koordinierung von Schutz- und Abwehrmaßnahmen gegen IT-Sicherheitsvorfälle eingerichtet, konnte in der Übung als "Informationsdrehscheibe" zum Austausch von Lagebeiträgen zwischen den beteiligten Behörden und zur Optimierung der operativen Zusammenarbeit aller für die IT-Sicherheit relevanten staatlichen Stellen beitragen.

Ein wesentliches Ziel von "LÜKEX 11" war schließlich die Einrichtung eines geregelten Informationsaustausches zwischen den Ländern und dem Bund. Dabei lag die besondere Herausforderung darin, dass die länderübergreifenden Meldestrukturen im IT-Bereich noch im Aufbau und das Zusammenwirken zwischen den Strukturen des allgemeinen Krisenmanagements und des speziellen IT-Krisenmanagements noch weitgehend unerprobt waren. Die Übung zeigte, dass auf diesem Gebiet Optimierungsbedarf besteht. So sollten z.B. in den Ländern, soweit noch nicht erfolgt, feste Informations- und Meldeverfahren für den IT-Bereich sowie IT-Sicherheitsstrukturen eingerichtet werden, zum Beispiel Landes-CERTs[4.]. Die Einrichtung eines übergreifenden Verwaltungs-CERT-Verbundes wurde durch die Übung angestoßen mit dem Ziel, die IT-Zusammenarbeit von Bund, Ländern und KRITIS-Betreibern durch einen institutionalisierten Informationsaustausch zu verbessern.

"Treiber" der Weiterentwicklung im strategischen Krisenmanagement

"LÜKEX 11" war mit Blick auf die vorgegebenen Übungsziele und das Ziel, für die Bedeutung der IT-Sicherheit zu sensibilisieren, erfolgreich. Das Hauptziel jeder strategischen Übung, das Zusammenwirken aller Akteure in Krisen über administrative und föderale Grenzen hinweg zu üben, wurde erreicht. Notwendige Integrationsprozesse, z.B. zur Zusammenführung von IT-Krisenmanagement und bereichsübergreifendem Krisenmanagement, wurden angestoßen. Für die Entwicklung des Krisenmanagements auf dem noch relativ jungen Gebiet der IT-Sicherheit konnte "LÜKEX 11" – gleichsam als "Treiber" im Entwicklungsprozess – wichtige Impulse geben.

Nach den Erfahrungen von nunmehr fünf Übungen gilt LÜKEX als bewährtes Modell für die Anlage strategischer Übungen. Dabei hat sich die besondere Eignung der Übungsserie gezeigt, zur Weiterentwicklung des strategischen Krisenmanagements und bestehender Krisenplanungen und -strukturen wesentlich beizutragen. Die Übungsserie hat aber auch wichtige Impulse für andere Felder des strategischen Krisenmanagements gegeben, unter anderem für die Optimierung ressortübergreifender Managementstrukturen, die Verbesserung der Risiko- und Krisenkommunikation sowie die Lehre in allgemeinen Fragen strategischer Krisenbewältigung. So steht LÜKEX heute für einen offenen, zukunftsorientierten Prozess, der wichtige Entwicklungen im Bevölkerungsschutz Deutschlands angestoßen hat und diese stetig vorantreibt.

1.) Cyber-Sicherheitsstrategie für Deutschland, BMI (Hrsg.), Berlin, Februar 2011.

2.) Der Begriff "LÜKEX" steht für "Länder übergreifende Krisenmanagement-Übung / Exercise". LÜKEX ist eine von Bund und Ländern seit 2004 gemeinsam durchgeführte Übungsserie im Bereich des strategischen Krisenmanagements Deutschlands.

3.) Beschluss IT-Rat zum IT-Krisenmanagement bei IT-Krisen mit Auswirkungen auf die Bundesverwaltung vom 31.03.2011

4.) CERT: Computer Emergency Response Team

Allianz für Cyber-Sicherheit – Plattform für den Informations- und Erfahrungsaustausch

Dr. Harald Niggemann, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Dr. Harald Niggemann

Durch die globale Vernetzung der Informationstechnik entstehen ständig neue Bedrohungen durch unterschiedlichste Interessengruppen, die unter Verschleierung ihrer Identität weltweit Ziele angreifen. Der Absicherung vor Gefahren aus dem Cyber-Raum muss daher besondere Aufmerksamkeit entgegengebracht werden. Als Plattform für den Informations- und Erfahrungsaustausch auf diesem Gebiet haben das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM e.V.) die Allianz für Cyber-Sicherheit gegründet.

Die Ursachen für die Gefahr durch Cyber-Angriffe sind vielfältig. Einerseits können viele Angriffsziele relativ einfach angegriffen und die Angriffswege effektiv verschleiert werden. Andererseits ist heutige Informationstechnik aufgrund ihrer Komplexität angreifbar. Täter nutzen nicht nur neue und bislang unbekannte Schwachstellen aus (“Zero Days”), sondern schlagen auch Kapital daraus, dass Updates und Patches in der Praxis häufig verspätet eingespielt werden.

Das Spektrum der Cyber-Angriffe reicht von Denial-of-Service-Attacken durch Aktivisten über die Manipulation von Internet-Banking-Vorgängen durch Kriminelle bis hin zu Spionage und Sabotage in Behörden und Unternehmen durch fremde staatliche Stellen. Nicht selten arbeiten mehrere Tätergruppen bei der Vorbereitung oder Durchführung von Cyber-Angriffen arbeitsteilig zusammen. Über bekannt gewordene Cyber-Angriffe auf private und öffentliche Einrichtungen wird inzwischen nicht nur in Fachkreisen, sondern auch in breiteren Medien berichtet. Aufgrund der vielfältigen Szenarien und Formen von Angriffen im Cyber-Raum ist eine Schätzung der Schäden, die dadurch in Deutschland entstehen, schwierig.

Unbestritten ist jedoch, dass nicht nur die Überlebensfähigkeit einzelner Institutionen bedroht ist, denn auch IT-Systeme der Kritischen Infrastrukturen, die für unsere Gesellschaft von besonderer Bedeutung sind und zu denen beispielsweise die Energie- und Lebensmittelversorgung gehören, sind Teil des Cyber-Raums.

In diesem Zusammenhang stellt sich die Frage, ob angesichts der Gefährdungslage ein wirksamer Schutz vor Cyber-Angriffen überhaupt erreichbar ist. Grundsätzlich gilt auch in der Cyber-Sicherheit, dass es – wie in vielen Disziplinen – keinen absoluten präventiven Schutz gibt. Allerdings zeigen die Erfahrungen der Labors und auch des BSI, dass das technische Niveau der Angriffe sehr unterschiedlich ist und dass sich die meisten Angriffe durch praktikable Schutzmaßnahmen abwehren lassen. Je besser die Schutzvorkehrungen sind, desto geringer ist die Wahrscheinlichkeit eines erfolgreichen Cyber-Angriffes in der eigenen Institution. Auch bei zielgerichteten Angriffen gilt, dass sich die Täter unter Umständen ein leichteres Ziel aussuchen, wenn sie auf wirksame Schutzmaßnahmen treffen.

Für einen angemessenen Schutz insgesamt sind punktuelle Maßnahmen jedoch nicht ausreichend. Die komplexen Strukturen des Cyber-Raums bieten den Tätern heute vielfältige Wege und Werkzeuge, um IT-Systeme zu manipulieren, außer Funktion zu setzen oder um vertrauliche Informationen abfließen zu lassen. Isolierte Einzelmaßnahmen werden von den Angreifern meist nach einer gewissen Zeit umgangen und durch angepasste Angriffsmethoden schließlich unwirksam gemacht. Nachhaltige Cyber-Sicherheit lässt sich daher nur durch

- ein kooperatives Vorgehen aller Akteure in Wirtschaft, Wissenschaft und Staat und
- eine kontinuierliche Anpassung aller Maßnahmen zur Prävention, Erkennung und Reaktion an die Gefährdungslage und die Methoden der Angreifer erreichen.

Als Plattform für den hierfür erforderlichen Informations- und Erfahrungsaustausch haben das BSI und der BITKOM e.V. die Allianz für Cyber-Sicherheit gegründet. Kernziele dieser Initiative sind,

- die Risiken des Cyber-Raums für Deutschland zu bewerten, angemessene Sicherheitsmaßnahmen zu konzipieren und zu realisieren,
- die nationalen Fähigkeiten zum Schutz im Cyber-Raum,

zur Abwehr von Cyber-Angriffen und zur Bewältigung von Cyber-Krisen zu stärken,
- im internationalen Vergleich eine führende Rolle im Bereich Cyber-Sicherheit einzunehmen.

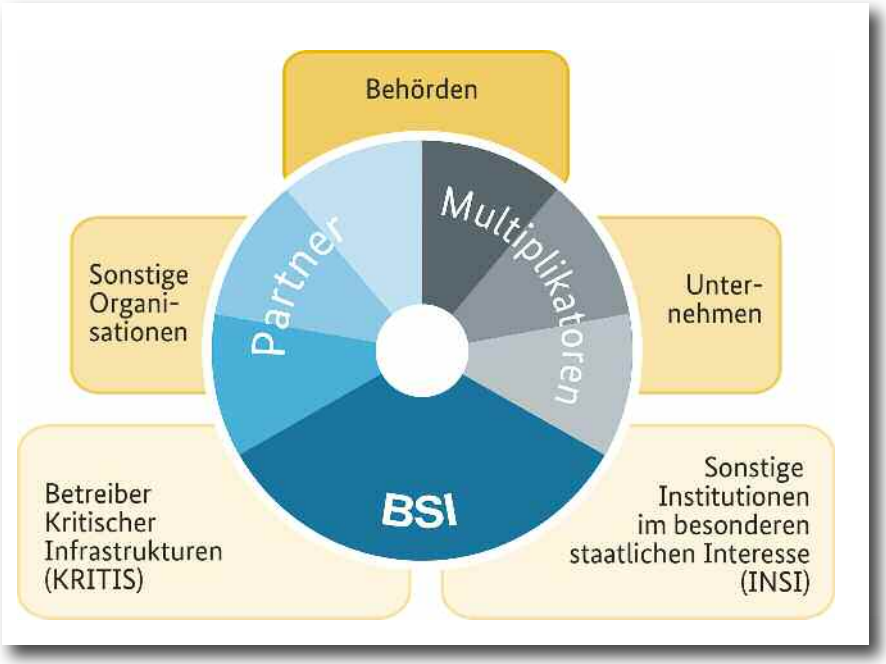
Zur Erreichung dieser Ziele setzt die Allianz für Cyber-Sicherheit auf die Elemente Lageermittlung, Lösungshinweise, Gestaltung und Erfahrungsaustausch.

Das IT-Sicherheitsniveau kann nur weiterentwickelt und verbessert werden, wenn der aktuelle Status bekannt ist und die Beseitigung vorhandener Defizite offen angegangen wird. Im Rahmen der Allianz für Cyber-Sicherheit stellt das BSI daher aktuelle Lageinformationen zur Verfügung, damit Institutionen ihre Aktivitäten daran ausrichten können. Zur Ermittlung der Lage nutzt das BSI nicht nur seine eigenen Erkenntnisse, sondern es fließen auch Beiträge von Partnern der Allianz für Cyber-Sicherheit ein. Um die Vollständigkeit der Lageinformationen weiter zu verbessern, besteht auch die Möglichkeit, Ereignisse im Zusammenhang mit Cyber-Angriffen anonym an das BSI zu melden.

Ein weiteres wichtiges Element der Allianz für Cyber-Sicherheit sind Hinweise zu Lösungen. Hierzu gehören unter anderem Empfehlungen zum Einsatz bestimmter Sicherheitsmaßnahmen, zur Konfiguration von Produkten oder zu Sofortmaßnahmen für den Fall, dass eine Institution Opfer eines Cyber-Angriffs geworden ist. Dabei werden nicht nur Lösungshinweise des BSI, sondern auch von Partnern der Allianz für Cyber-Sicherheit zur Verfügung gestellt. Nutzer dieser Informationen haben jederzeit die Möglichkeit, Inhalte zu kommentieren und durch eigene Erfahrungen aus dem Arbeitsalltag zu bereichern. Die Allianz für Cyber-Sicherheit dient somit auch zum schnellen Informationsaustausch, um zeitnah aktuelle Empfehlungen zum Schutz vor und zur professionellen Reaktion auf Cyber-Angriffe bereitzustellen, indem betroffene Institutionen oder Hersteller über praktikable Workarounds berichten.

Das Informationsangebot ist in die folgenden Rubriken unterteilt:
- Sensibilisierung: In die Thematik “Cyber-Sicherheit” einführende Inhalte für Einsteiger,
- Sofortmaßnahmen: Konkrete Handlungsempfehlungen bei Cyber-Sicherheits-Vorfällen,
- Cyber-Sicherheitslage: Aktuelle Warnmeldungen und Lageberichte zur Cyber-Sicherheitslage,
- Angriffsmethoden: Informationen zu bekannten Bedrohungen aus dem Cyber-Raum,
- Werkzeuge: Empfohlene Tools und Signaturen zur Absicherung der eigenen Systeme,
- Kooperationsangebote: Services von BSI und ausgewählten Partnern für Teilnehmer der Allianz,
- Analysen: Auswertungen aus Statistiken des BSI zu Themen der Cyber-Sicherheit,
- Empfehlungen: Konkrete Maßnahmen zu Konfiguration und Aufbau von IT-Systemen,
- Business Continuity Management (BCM): z. B. Unterlagen zur Durchführung von IT-Übungen.

Sowohl bei der Sensibilisierung als auch bei der Konzeption von Maßnahmen kann der Erfahrungsaustausch mit anderen Institutionen einen wesentlichen Mehrwert liefern. Aufgrund der sensitiven Natur des Themas setzt dies jedoch ein besonderes Maß an Vertrauen voraus. Neben der zentralen Informationsverteilung setzt die Allianz für Cyber-Sicherheit daher auch auf den direkten Austausch in kleineren Gruppen, beispielsweise in regionalen und branchenbezogenen Foren, Arbeitskreisen oder Stammtischen. Die Leitung oder Betreuung solcher Gruppen ist eine Möglichkeit für Multiplikatoren zur Mitwirkung in der Allianz für Cyber-Sicherheit.



Akteure der Allianz für Cyber-Sicherheit Quelle: BSI

Freiwillige Registrierung

Es gibt verschiedene Möglichkeiten, die Leistungen der Allianz für Cyber-Sicherheit zu nutzen. Die meisten Publikationen der Allianz für Cyber-Sicherheit

werden ohne Zugriffsbeschränkung auf dem Web-Angebot unter der Adresse https://www.allianz-fuer-cybersicherheit.de zur Verfügung gestellt, damit sie von möglichst vielen Anwendern für die Verbesserung der Cyber-Sicherheit genutzt werden können. Bestimmte Angebote der Allianz für Cyber-Sicherheit richten sich jedoch nur an registrierte Teilnehmer. Die freiwillige Registrierung steht deutschen Institutionen (Unternehmen, Behörden, Forschungseinrichtungen etc.) offen und setzt die Benennung eines Ansprechpartners, der innerhalb der Institution die Verantwortung für Cyber-Sicherheit trägt, und die Unterzeichnung einer Vertraulichkeitsvereinbarung voraus. Typische Ansprechpartner sind CIOs und CISOs, in kleineren Institutionen auch Administratoren. Die Vertraulichkeitsvereinbarung ist notwendig, damit auch nicht-öffentliche Informationen ausgetauscht werden können.

Institutionen im besonderen staatlichen Interesse

Ein erweitertes Informationsangebot besteht für Institutionen im besonderen staatlichen Interesse (INSI). Dazu gehören beispielsweise deutsche Unternehmen in der Geheimschutzbetreuung oder deutsche Betreiber Kritischer Infrastrukturen. Durch die Registrierung können solche Institutionen Zugriff auf einen gesonderten Bereich mit vertraulichen Informationen erhalten.

Partner

Die aktive Mitarbeit von Unternehmen und Behörden trägt wesentlich zum Erfolg der Allianz für Cyber-Sicherheit bei. Partner der Allianz für Cyber-Sicherheit sind deutsche Institutionen, die einen konkreten Mehrwert für die Allianz erzeugen, indem sie beispielsweise exklusive Informationen beisteuern oder kostenlose Dienstleistungen für Teilnehmer anbieten. Typischerweise verfügen Partner daher über hohe IT-Kompetenz und sind beispielsweise CERTs, Hersteller/Dienstleister, die zur Cyber-Sicherheit beitragen, Internet-Infrastrukturbetreiber oder Forschungseinrichtungen mit einem Forschungsschwerpunkt “Cyber-Sicherheit”.
Generell gilt, dass die Beiträge der Partner zur Allianz kostenlos sind.

Multiplikatoren

Cyber-Sicherheit betrifft alle Anwender von Informationstechnik. Die Allianz für Cyber-Sicherheit ist deshalb keine Initiative mit ausgewählten Mitgliedern, sondern richtet sich an alle deutsche Institutionen aus dem privaten und öffentlichen Sektor. Der Beitrag der Multiplikatoren der Allianz für Cyber-Sicherheit ist es, die Reichweite der Allianz zu erhöhen, indem sie beispielsweise

- aktuelle Informationen über die Allianz für Cyber-Sicherheit an ihre Mitglieder oder an andere Adressatenkreise vermitteln,
- Artikel oder Vorträge über die Allianz für Cyber-Sicherheit oder über Themen der Cyber-Sicherheit in ihren Medien oder Organen platzieren oder
- durch Gremien-, Medien- oder Öffentlichkeitsarbeit für die Anliegen der Cyber-Sicherheit sensibilisieren.

Als Multiplikatoren können etwa bundesweit oder regional agierende Wirtschaftsverbände, Industrie- und Handelskammern, Gremien, Vereine, Medien und ähnliche Einrichtungen die Allianz unterstützen.

Fazit

Die zunehmende Professionalisierung von Angriffen im Cyber-Raum stellt eine große Herausforderung für unsere Gesellschaft dar. Die Allianz für Cyber-Sicherheit bietet Unternehmen und Behörden die Möglichkeit, sich mit den notwendigen Informationen zu versorgen, um angemessene Schutzmaßnahmen zu treffen und professionell auf Cyber-Angriffe zu reagieren. Durch die Teilnahme am Erfahrungsaustausch oder auch als Partner/Multiplikator können Institutionen daran mitwirken, die Cyber-Sicherheit in Deutschland weiter zu verbessern und aktiv zu gestalten. Alle deutschen Institutionen sind aufgerufen, sich an diesem Prozess zu beteiligen. Weiterführende Informationen und Formulare zur Interessensbekundung finden sich auf dem Web-Angebot unter der Adresse https://www.allianz-fuer-cybersicherheit.de. Anfragen können per E-Mail an die Adresse info@cyber-allianz.de gerichtet werden.

Harmonisierung der Führungsinformationssysteme

Kritischer Erfolgsfaktor bei der Informationsversorgung im Einsatz

Dipl.-Inform. Jörn Becker, Leiter Civil & National Security, Atos
Dipl.-Ing. Dipl.-Wirtsch.-Ing. Hubert Geml, Leiter Verteidigung, Innere Sicherheit, Atos Deutschland

Jörn Becker

Hubert Geml

Der Einsatz wirkungsvoller Führungsinformationssysteme ist ein kritischer Erfolgsfaktor für die Führungsunterstützung der Bundeswehr und Voraussetzung für die Umsetzung der "Vernetzten Operationsführung".

Die derzeit eingeführten Systeme sind jedoch nur eingeschränkt zum interoperablen, teilstreitkraftübergreifenden Datenaustausch befähigt und können damit nicht den durchgängigen Informationsbedarf im erforderlichen Maße decken.

Im Rahmen der Harmonisierung der Führungsinformationssysteme der Bundeswehr werden die bestehenden Systeme ausgerichtet an den Kriterien Einsatzorientierung, Multinationalität, moderne Technologien und effiziente Ressourcennutzung. Sie werden schrittweise in ein Gesamtsystem migriert, um so die Vorbereitung, Führung und Auswertung von (multi-) nationalen Einsätzen organisationsbereichsübergreifend auf allen Führungsebenen bestmöglich zu unterstützen.[1.)]

Die Forderung nach einer Harmonisierung der Führungsinformationssysteme der Bundeswehr ist nicht neu. Neu ist aber, dass mittlerweile ausgereifte Technologien und Lösungen zur Verfügung stehen, die es ermöglichen, aktuelle und zukünftige funktionale und nichtfunktionale Anforderungen, abgestimmt auf den Auftrag, zeitnah und effizient bedienen zu können.

Atos wurde im Dezember 2012 beauftragt, gemeinsam mit seinen Partnern Logica, Microsoft, Infodas, Geosecure, Frequentis, SAP und Systematic den ersten Teil der Harmonisierung und Migration der Führungsinformationssyteme (HaFIS) durchzuführen.

Service Gedanke ist Basis für einsatzorientierte Führungsunterstützung

Einsatzorientierung im multinationalen Umfeld hat höchste Priorität bei der Harmonisierung der Führungsinformationssysteme. Verfügbare moderne Technologien sowie die Forderung nach einer effizienten Ressourcennutzung führen unweigerlich zum "Ein-System-Gedanken".

Harmonisierung ist dabei nicht gleichzusetzen mit Neuentwicklung, denn Bewährtes bleibt erhalten. Ausgereifte Produkte und Technologien werden identifiziert und evolutionär zu einem Gesamtsystem zusammengeführt, so dass den Nutzern sowohl gewohnte nicht wegzudenkende, als auch neue Fähigkeiten der Systeme in Form von "Services" zur Verfügung gestellt werden.

Aufgrund des immer höher werdenden Kostendrucks lagern mehr und mehr Organisationen ihre Prozesse in die sogenannte "Cloud" aus, da die IT-Kosten auf diese Weise erheblich gesenkt werden können. Im Zuge von HaFIS werden keine Informationen in eine öffentliche Cloud ausgelagert, allerdings werden moderne Cloud-Technologien genutzt unter Berücksichtigung gleichzeitiger Kontrolle der verwendeten Daten, der implementierten Prozesse sowie der anfallenden Kosten.

Diverse erfolgreich realisierte Projekte im Rahmen der Deutschen Teilhabe am AMN (Afghanistan Mission Network) haben bereits wesentliche Grundsteine für eine einheitliche Plattform gelegt. Fragen der Machbarkeit stellen sich somit nicht mehr. Als Blaupause für die Harmonisierung dient hierbei die einsatzerprobte modulare und flexible Architektur der von Atos entwickelten "Building Block Technologie". Dabei werden die Architekturprinzipien des Cloud Computing, insbesondere die Aufteilung in die Ebenen Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS) zu Grunde gelegt.

Virtualisierungstechnologien machen eine konsequente Trennung der angesprochenen Ebenen möglich. Vereinfacht

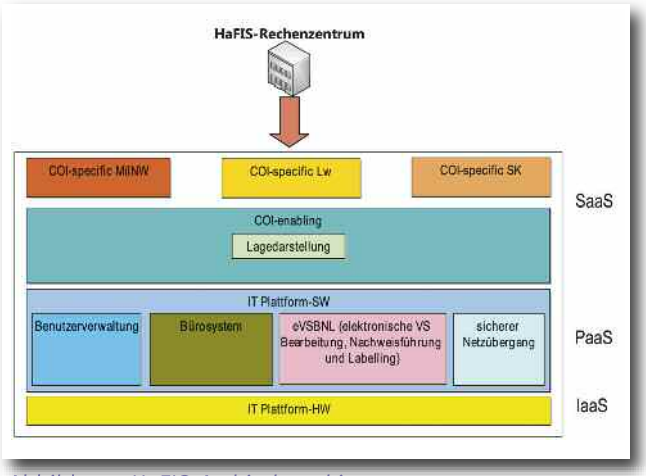


Abbildung: HaFIS Architekturskizze Quelle: Atos

gesagt: Hardware und Software für die Anwendungen sind entkoppelt. Das ermöglicht Flexibilität und Skalierbarkeit bei der Ausgestaltung der Systeme und ist damit ein Garant sowohl für den wirtschaftlichen Einsatz von Ressourcen, für die zielgerichtete Bereitstellung der Funktionalität als auch für die Aufwuchsfähigkeit des Systems. Das einheitliche Architekturprinzip gilt sowohl für die stationären Rechenzentren mit hohen Nutzerzahlen als auch für kleinere spezialisierte Einheiten mit dedizierten Nutzergruppen wie verlegefähige, mobile oder seegängige Systeme.

Einsatzorientierte Konfigurationen aus dem HaFIS-Warenkorb

Spezifische Anwendungen bereits in der Bundeswehr eingeführter Systeme sowie Anwendungen aus dem NATO-Umfeld werden auf der Software as a Service Ebene (SaaS) zusammengeführt und entweder als sogenannte "COI[2.)] specific services" oder als "COI enabling services" den Nutzern über die Plattform HaFIS zur Verfügung gestellt. Dabei versteht man unter "COI specific services" spezifische Dienste der Teilstreitkräfte. Das sind u.a. Funktionalitäten, die ursprünglich in den Systemen FüInfoSysLw[3.)], FüInfoSysSK[4.)] oder JASMIN[5.)] bereitgestellt wurden. COI enabling services sind gemeinsame Nutzerservices wie die Lagebearbeitung.

Abgestimmt auf die Aufgabe werden einsatzorientierte Konfigurationen definiert und die benötigten Funktionalitäten für den Nutzer wie Bausteine aus dem HaFIS "Katalog bzw. Warenkorb" selektiert und angeboten.

Die Platform as a Service Ebene (PaaS) Ebene umfasst querschnittliche Dienste wie Nutzerverwaltung, VS Bearbeitung und Nachweisführung, das Bürosystem inkl. Document Handling System. Die IT Plattform Hardware auf der Infrastructure[6.)] as a Service Ebene (IaaS) stellt Hardware und alle Systemdienste bereit, die zum Betreiben der Hardware notwendig sind. Durch das von der PaaS entkoppelte und zielgerichtete Design der IT Plattform Hardware ist es möglich, Investitionen auf das erforderliche Mindestmaß zurückzuschrauben. Hardware ist restriktionsfrei skalierbar. Redundanzen werden vermieden, sofern sie nicht aus Hochverfügbarkeitszwecken ausdrücklich gewollt sind.

Der Nutzer steht im Mittelpunkt – Kosten werden minimiert

Durch die gewählte Vorgehensweise können im Rahmen der Migration sukzessive alte Instanzen abgeschaltet oder auch Hardware ausgetauscht bzw. modernisiert werden, ohne dass sich eine Beeinträchtigung der Funktionalitäten ergibt. Das offene diensteorientierte Architekturprinzip lässt sich darüber hinaus bis zur letzten Meile anwenden.

Es entsteht ein System, dass sich der heutigen IT-Nutzung unserer Gesellschaft stark anpasst. Nutzerakzeptanz und Bezahlbarkeit sind schließlich entscheidend für den Erfolg der Harmonisierung und im Interesse aller Beteiligten. Das harmonisierte Führungsinformationssystem wird das IT-System Bundeswehr und damit die NetOpFü-Fähigkeit nachhaltig stärken.

Ausblick

HaFIS wird schrittweise in mehreren Migrationsabschnitten realisiert und nach derzeitiger Planung bis 2019 vollständig umgesetzt sein.

Der Projektplan des ersten Migrationsabschnitts sieht vor, bis Mitte dieses Jahres eine harmonisierte Zielarchitektur von HaFIS mit Schwerpunkt auf den stationären Systemanteilen zu spezifizieren. Der Nachweis der Funktionsfähigkeit von specific COIs wird mit Diensten aus dem Bereich Karte/Lage sowie dem Militärischen Nachrichtenwesen (MilNW) geführt. Im Bereich MilNW wird diese Architektur als erstes zum Einsatz kommen und ihre Einsatztauglichkeit einem großen Nutzerkreis unter Beweis stellen. Das Ziel von Atos ist es, in diesem Zuge Wege aufzuzeigen, den Bedarf der Streitkräfte schnell, wirkungsvoll und effizient zu decken.

1.) Quelle Bundeswehr

2.) Community of Interest

3.) Führungsinformationssystem der Luftwaffe

4.) Streitkräftegemeinsames Führungsinformationssystem

5.) Militärisches Nachrichtenwesen

6.) Der Begriff Infrastruktur wird bei der Bundeswehr derzeit unterschiedlich definiert.

AFCEA Bonn e.V.

27. AFCEA Fachausstellung

Informations- und Kommunikationstechnik

unter der Schirmherrschaft des Staatssekretärs im BMVg,
Herrn Stéphane Beemelmans

mit Vorträgen zum Thema

IT-Services – Enabler in multinationalen Koalitionen

24./25. April 2013
Stadthalle Bad Godesberg

Ausstellerliste AFCEA Fachausstellung 2013

	Ausstellende Firma/Organisation	Stand-Nr.
1	A.WEIDELT Systemtechnik GmbH & Co. KG	ZA 2
2	ACME Portable Computer GmbH	F 6
3	ATM ComputerSysteme GmbH	G 2
4	Atos IT Solutions and Services GmbH	Brunnensaal
5	Avitech GmbH	G 14
6	BAKO Systemintegration GmbH & Co. KG	Z 12
7	Bechtle GmbH & Co.KG, IT-Systemhaus Bonn	F 5
8	Behörden Spiegel / ProPress Verlagsgesellschaft mbH	F 12
9	Berner & Mattner Systemtechnik GmbH	P 10
10	BWI Leistungsverbund	G 13
11	CASSIDIAN	Z 6
12	CeoTronics AG	F 1
13	Citrix Systems GmbH	P 7
14	COMPAREX AG	B 4
15	CONDOK GmbH	P 11
16	CONET Business Consultants GmbH	F 10
17	CONET Solutions GmbH	F 10
18	Cordsen Engineering GmbH	F 6
19	CPM Communication Presse Marketing GmbH	FR 2
20	Cross Match Technologies	F 11
21	DATAGROUP BGS GmbH	G 10
22	DATAGROUP Business Solutions GmbH	ZA 1
23	Deutsche Gesellschaft für Wehrtechnik e.V. (DWT)	F 7
24	DeviceLock Europe GmbH	P 2
25	EGL Elektronik Vertrieb GmbH	T 3
26	ELNO GmbH	Z 3
27	Empolis Information Management GmbH	G 6 – G 8
28	ESET Deutschland GmbH	K 7
29	ESG Elektroniksystem- und Logistik-GmbH	G 1
30	Esri Deutschland GmbH	G 6 – G 8
31	ETG – Elektronik + TEMPEST GmbH	FR 5
32	Fraunhofer FKIE	F 8
33	Fraunhofer IOSB	T 1 u. ZA 3
34	FREQUENTIS Nachrichtentechnik GmbH	K 2
35	gabo Systemtechnik GmbH	B 2
36	Galleon Embedded Computing GmbH	P 9
37	GBS TEMPEST & Service GmbH	P 12
38	Gebrüder Friedrich Industrie- und Elektrotechnik GmbH	P 11
39	genua mbH	G 21
40	Geosecure Informatik GmbH	G 6 – G 8
41	GEOSYSTEMS GmbH	G 3
42	GPP Service GmbH & Co KG	K 5
43	Green Data Systems GmbH & Co. KG	ZA 4
44	Hardthöhenkurier	FR 3
45	Hewlett-Packard GmbH	K 4
46	Hexagon GeoSpatial Solutions	G 3
47	Hitachi Data Systems GmbH	T 2
48	IABG mbH	G 17
49	IBM Deutschland GmbH	G 20
50	ICOS Gesellschaft für Industrielle Communicationssysteme mbH	G 22
51	Indra S.A.	G 14
52	INFODAS GmbH	G 9
53	Integer Solutions GmbH	K 8
54	Intergraph SG&I Deutschland GmbH	G 3
55	ITT Exelis	Z 1a
56	itWatch	G 19 u. E 1
57	JHL Communication Technology GmbH	B 3
58	JK DEFENCE & SECURITY PRODUCTS GMBH	P 6
59	Lachen helfen	E 2
60	LANCOM Systems	B 2b
61	Liske Informationsmanagementsysteme	FR 4
62	LOG GmbH	K 6
63	Logic Instrument GmbH	Z 13
64	Logica Deutschland GmbH und Co. KG	K 1
65	Luciad	K 3
66	Maibach Industrie-Plastic GmbH	Z 8
67	Martin Yale International GmbH	P 3
68	MATERNA GmbH	T 2
69	Microsoft Deutschland GmbH	F 9
70	Mittler Report Verlag	P 4
71	ML Consulting Schulung, Service + Support GmbH	F 13
72	Mönch Verlagsgesellschaft mbH	FR 1
73	Motorola Solutions GmbH	K 8
74	ND SatCom Defence GmbH	Z 6
75	Office für Technische Dokumentationen GmbH	F 11
76	ORACLE Deutschland B.V. & Co. KG	T 5
77	Overwatch Systems Ltd.	P 5
78	Panasonic Deutschland GmbH	Z 4
79	Peli Products	B 1
80	PROCITEC GmbH	P 9
81	promegis GmbH	P 5
82	PWA Electronic Service- und Vertriebs- GmbH	Z 4
83	RES Software	B 4
84	RIEDEL Communications GmbH	P 1
85	Rockwell Collins	Z 2
86	roda MilDef GmbH	Z 7
87	Rohde & Schwarz Vertriebs-GmbH	G 18
88	rola Security Solutions GmbH	G 16
89	Romold GmbH	B 2
90	Saab International Deutschland GmbH	Z 1b
91	Samsung Electronics GmbH	F 9
92	SAP Deutschland AG & Co. KG	G 12
93	Schnoor Industrieelektronik GmbH & Co. KG	G 5
94	secunet Security Networks AG	G 15
95	Securiton AG, Alarm and Security Systems	T 6
96	Secusmart	Z 9
97	SELEX Communications GmbH	G 4
98	SIEMENS AG – Industry	G 15
99	SRH SAP Competence Center	T 4
100	steep GmbH	G 11
101	Steria Mummert Consulting AG	F 11
102	SYSTEMATIC GmbH	Z 10
103	systerra computer GmbH	Z 11
104	TASys GmbH	T 4
105	TELEFUNKEN Radio Communication Systems GmbH & Co. KG	F 2
106	Thales Deutschland	Z 5
107	Trend Micro Incorporated	B 4
108	T-Systems International GmbH	F 4
109	UWS Business Solutions GmbH	P 8
110	VEGA Deutschland GmbH	F 3
111	ZVEI – Fachverband Sicherheit	E 3

AFCEA Bonn e.V.

27. Fachausstellung

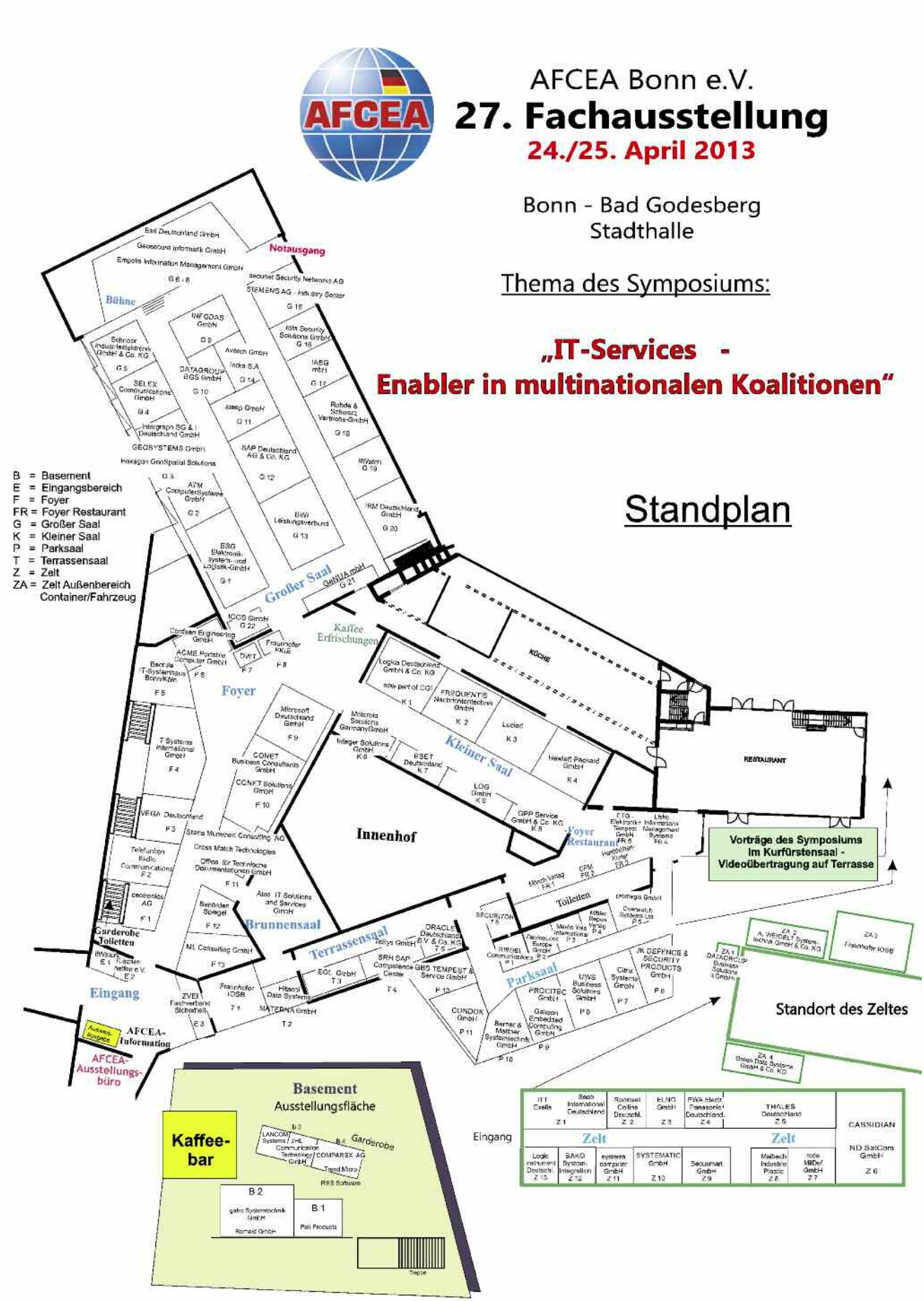
24./25. April 2013

Bonn - Bad Godesberg
Stadthalle

Thema des Symposiums:

„IT-Services - Enabler in multinationalen Koalitionen"

Standplan



27. AFCEA Fachausstellung

Informations– und Kommunikationstechnik

unter der Schirmherrschaft von Staatssekretär Stéphane Beemelmans, BMVg

mit Vorträgen zum Thema

IT-Services —
Enabler in multinationalen Koalitionen

24. April 2013	09.00 Uhr – 18:00 Uhr Ausstellung * Vorträge im Kurfürstensaal ab 18:00 Uhr Kölsch mit Musik	
10:00 Uhr	GenMaj Dipl.-Ing. Dipl.-Oek. Erich Staudacher Vorsitzender AFCEA Bonn e.V.	Begrüßung/ Eröffnung der 27. AFCEA Fachausstellung
10:15 Uhr	MinDirig Dr. Dietmar Theis , IT-Dir BMVg	Grußwort
10:30 Uhr	BrigGen Christian Badia, UAL Planung I, BMVg	Die Abbildung der IT in der Planung der Bundeswehr
14:00 Uhr	FltlAdm Dr. Thomas Daum AbtLtr I im Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr	Die Integration der ITK in das neue BAAINBw - ein gelungener Anfang
16:00 Uhr – 18:00 Uhr	Gesprächsleitung: Katja Frintrop, Vorstand AFCEA Bonn e.V.	Young AFCEANs Karrierestarterforum Informationsveranstaltung für junge Fach-/ Führungskräfte und Studenten
25. April 2013	09.00 Uhr – 18:00 Uhr Ausstellung * Vorträge im Kurfürstensaal	
10:00 Uhr	GenMaj Dipl.-Ing. Heinrich-Wilhelm Steiner Kommandeur Führungsunterstützungs- kommando der Bundeswehr	Führungsunterstützung in der Bundeswehr und in multinationalen Einsätzen unter Nutzung von IT-Services
14:00 Uhr	MajGen (ret.) Koen Gijsbers General Manager NCI Agency	NCI Agency's Journey from Asset Based to Services Based IT Capabilities for NATO

24./25. April 2013 - Stadthalle Bad Godesberg

AFCEA-Fachausstellung 2013

**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 — Stand: ZA 2

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.

ACME Portable Computer GmbH — Stand: F 6

ACME ist Hersteller mobiler Computersysteme für die unterschiedlichsten Anwendungsfelder. Das Spektrum umfasst mobile Beweissicherungslösungen; Systeme für Messtechnik, Video & Broadcasting; Entwicklungen für Luft- und Raumfahrt, Simulationstraining sowie C4ISR und UAV. Alle Produkte werden nach detaillierten Spezifikationen hergestellt und können genau auf die Kundenwünsche ausgerichtet werden.
ACME investiert vergleichsweise viele Ressourcen in die Forschung und Entwicklung seiner Systeme und produziert im eigenen Werk in Taiwan. Auch über zahlreiche OEM/ODM-Partnerschaften hat sich ACME am Markt für portable Computersysteme fest etabliert. Die ACME Portable Computer GmbH ist die Tochterfirma der US-amerikanischen ACME Portable Machines Inc., die in 1994 in Azusa/L.A. gegründet wurde.
Kontakt: Min-Ling Schifferdecker, General Manager, ACME Portable Computer GmbH, Benzstraße 15, 76185 Karlsruhe, Germany, Tel.: +49(0)721 570453-0, info@acmeportable.de

ATM ComputerSysteme GmbH — Stand: G 2

ATM ComputerSysteme aus Konstanz am Bodensee ist ein international aktives Systemhaus für gehärtete IT-Hardware und Software. ATM ist seit mehr als drei Jahrzehnten erfolgreich und langjähriger Partner der Bundeswehr. ATM gehört seit 2001 der Krauss-Maffei Wegmann Gruppe an.
Fokus der Entwicklungsleistungen sind Computer- und Displaysysteme, Panel-PCs und mobile wie stationäre Kommunikationsanwendungen sowie die Programmierung leistungsfähiger und passgenauer Software. Die IT-Systeme trotzen härtesten Umweltbedingungen, wie sie zu Land, Luft und Wasser herrschen. Mit Nachdruck legt ATM deshalb sein Augenmerk auf hohe Qualität. Wer im internationalen Markt bestehen will, muss maßgeschneiderte Produkte präsentieren. ATM verwirklicht dies mit seinen innovativen Speziallösungen. Dienstleistungen und Beratung rund um das Produkt charakterisieren die Unternehmens- und Produktphilosophie.
Kontakt:
ATM ComputerSysteme GmbH, Jörg Sczesny, Max-Stromeyer-Str. 116, 78467 Konstanz, joerg.sczesny@atm-computer.de, Telefon: 07531 808 4208, Fax: 07531 808 4363, Mobil: 01713357778, www.atm-computer.de

Atos — Stand: Brunnensaal

Atos ist ein internationaler Anbieter von IT-Dienstleistungen mit einem pro forma Jahresumsatz für 2011 von 8,5 Milliarden Euro und 74.000 Mitarbeitern in 48 Ländern. Das umfangreiche Portfolio umfasst transaktionsbasierte Hightech-Services, Beratung und Technologie-Services, Systemintegration sowie Outsourcing-Dienstleistungen.
Das Verteidigungsgeschäft ist ein wichtiger Markt für Atos. Der seit langer Zeit bestehende enge und partnerschaftliche Dialog mit der Bundeswehr soll ausgebaut werden.
Atos präsentiert auf der AFCEA seine Lösungskompetenz bei der Entwicklung und Betriebsunterstützung von einsatzfähigen IT-Plattformen (insbesondere Führungsinformationssystemen) und bietet Informationen zu Technologietrends.

Avitech GmbH — Stand: G 14

Avitech GmbH ist seit über 15 Jahren kompetenter und verlässlicher Systempartner der Bundeswehr für das FSInfosysBw und InfoDADBw. Unsere Kompetenz liegt vor allem im Bereich der Aeronautischen und Hindernis Datenbanken, Luftfahrtkarten, sowie Flugplan-und Pilotenbriefingsysteme.
Darüber hinaus bieten wir Meldungsvermittlungs- und Kommunikationssysteme. Die Avitech Produkte werden bundeswehrweit und von den in Deutschland stationierten Bündnispartnern an mehr als 100 Standorten genutzt. Dies beinhaltet auch die Schnittstelle zur zivilen Flugsicherung und zur Agentur Eurocontrol. Auf der diesjährigen AFCEA zeigen wir Produkte, die im FSInfoSysBw und InfoDADBw eingesetzt werden und die flächendeckende Datenversorgung mit Aeronautischen und Hindernis Daten sicher stellen wird.

BAKO Systemintegration GmbH & Co. KG — Stand: Z 12

Konkrete Anwendungen fordern innovative und einsatzgerechte Lösungen.
BAKO Produkte und Dienste bereiten Ihre Anwendung basierend auf Ihrer gewohnten EDV- bzw. Funktionsumgebung auf die härtesten Bedingungen und Umwelteinflüsse weltweit vor und das an Land auf See oder in der Luft. Unsere Erfahrung im Bereich mobiler und verlegbarer Systemlogistik unterstützt Sie, Ihren Einsatz bestmöglich durchzuführen.
Unsere Kundenbasis hat zwei Dinge gemein. Sie benötigen hochempfindliches Equipment in extremen Bedingungen. Und Sie haben entdeckt, dass BAKO die Antwort auf die Anforderungen, die diese Bedingungen darstellen, technologisch lösen kann.

Bechtle IT-Systemhaus Bonn/Köln — Stand: F 5

Das Bechtle IT-Systemhaus Bonn/Köln gehört zur Bechtle AG, die mit rund 65 Standorten, 13 Lösungs- und Competence Centern sowie einem Umsatz von rund 2 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 Business Applications.
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 7 Bund Rahmenverträgen u.a. beim BeschA des BMI, die ein umfassendes Sortiment an Produkten/ Dienstleistungen enthalten (z. B. Virtualisierung, EMC Storage Produkte, Notebooks und Zubehör, HP Netzwerk Produkte) – erhalten Sie an unserem Stand F5.
Mehr zu Bechtle unter www.bechtle.com

Behörden Spiegel – die Zeitung für den Öffentlichen Dienst — Stand: F 12

Der Behörden Spiegel begleitet die öffentliche Verwaltung sowie den Modernisierungsprozess bei der Bundesverwaltung, den Ländern und Kommunen und den Sicherheitskräften. Deutschlands größte und älteste Zeitschrift für den Staat, seine Beschäftigten, seinen Einkauf und seine Modernisierungsfähigkeit zeigt Monat für Monat in journalistisch kritischer und unabhängiger Berichterstattung Wege zu mehr Effizienz in der staatlichen Verwaltung auf.
Der Behörden Spiegel ist ein meinungsbildendes Medium und veranstaltet Kongresse, zu denen Sie weitere Informationen unter folgenden Quellen finden: www.effizienter-staat.de; www.e-nrw.info; www.european-police.eu; www.euro-defence.eu; www.civil-protection.com; www.best-age-conference.com.
Neue Initiative: Cyber Akademie (CAk), www.cyber-akademie.de
Abonnenten des Behörden Spiegel können zudem das digitale Angebot Behörden Spiegel Online kostenlos beziehen (E-Government Newsletter, Newsletter Netzwerk Sicherheit, Newsletter Defence, Newsletter Verwaltung kompakt und Newsletter geodata kompakt).
www.behoerdenspiegel.de

Berner & Mattner Systemtechnik GmbH — Stand: P 10

Sicherheits- und missionskritische Software effizient entwickeln
Berner und Mattner ist als strategischer Entwicklungspartner spezialisiert auf Spezifikation, Entwicklung und Test von missions- und sicherheitskritischen elektronischen Steuersystemen und deren Software.
Entwicklung kompletter Softwarepakete zum Festpreis

- Embedded Systems, PC
- Komplexe HMIs

Systeme für Wissenschaft und Raumfahrt

- ECSS-Standards

Normenkonforme Entwicklungsprozesse

- DO-178B, IEC 61508
- MIL STD 882

Technologie- und Prozessberatung

- DOORS, SysML, UML
- SCADE, MATLAB/Simulink
- V-Modell-XT, CMMI CD&E

Kontakt: Nicole Machula, Berner & Mattner Systemtechnik GmbH, Erwin-von-Kreibig-Str. 3, 80807 München, Tel.: +49 (o)89 608090-0, Fax: +49 (o)89 6098182, info@berner-mattner.com, www.berner-mattner.com

BWI Leistungsverbund — Stand: G 13

Die BWI ist der strategische Partner für die Informations- und Kommunikationstechnik der Bundeswehr. Als Leistungsverbund aus BWI Informationstechnik GmbH, BWI Systeme GmbH und BWI Services GmbH betreibt die BWI die nichtmilitärische Informations- und Kommunikationstechnik der Bundeswehr. Dazu gehört die gesamte Infrastruktur von den Rechenzentren über WAN und LAN bis hin zur IT-Plattform und der Telekommunikation. Die BWI entwickelt und betreibt die Zentralen Dienste der Bundeswehr und ist für die Pflege und Änderungen der Systeme in Nutzung (SinN) zuständig. Mit zentralen Serviceleistungen und einem bundesweiten Vor-Ort-Service bietet die BWI der Bundeswehr einen flächendeckenden Service aus einer Hand. Zusätzlich unterstützt sie die Bundeswehr bei der Neuausrichtung und der Realisierung von SASPF. Die Prozessberatung rundet das Leistungsspektrum der BWI ab. Bei der AFCEA-Fachausstellung 2013 informiert die BWI über Modernisierungsprojekte und ihre Unterstützungsleistung bei der Neuausrichtung der Bundeswehr.

CASSIDIAN — Stand: Zelt Z 6

Kommunikation auf AFCEA-Homepage und Messebroschüre:
Im Rahmen der 27. AFCEA – Fachausstellung "IT-Services – Enabler in multinationalen Koalitionen" am 24. und 25. April, freut sich Cassidian, Sie auf dem Messestand Z 6 begrüßen zu dürfen.
Auf der AFCEA 2013 zeigt Cassidian einen Auszug aus dem komplexen System- und Komponentenportfolio für die militärische Operationsführung am Beispiel von bodengestützten und fliegenden Kräften.
Die kontinuierliche Erweiterung des Einsatzspektrums der Bundeswehr, die Konsolidierung der Fähigkeiten der Teilstreitkräfte und die verteidigungspolitischen Rahmenbedingungen führen auch in der bisherigen Systemlandschaft zu grundlegenden Veränderungen.
Die Fähigkeitsforderungen zur vernetzten Operationsführung in "Joint" wie auch "Combined Operations" bewegen sich dabei weg von geschlossenen Informationssystemen hin zu serviceorientierten Systemen.
Wir freuen uns auf Ihren Besuch. Cassidian – Defending World Security.

CeoTronics AG — Stand: F 1

Mehr als nur Headsets
CeoTronics hat sich als führender Systemanbieter von mobilen digitalen Funk-Netzen und -Endgeräten für lokale Anwendungen sowie von hochwertigen Kommunikations-Headsets und Systemen für die professionelle Nutzung etabliert. Mehr als 97.000 Hör-/Sprechsysteme zum Anschluss an die digitalen Tetra-/Tetrapol-Funkgeräte wurden bereits verkauft. Nutzen Sie dieses Know-how in der Kommunikationszubehör-Anpassung für die Umstellung vom Analog- zum Digitalfunk.
Leistungsführerschaft im Premiumsegment
CeoTronics hat sich seit 1985 in der Spitze der Qualitäts- und Leistungs-Pyramide positioniert und ist zuverlässiger Lieferant von Polizei, Bundespolizei, Militär, Nachrichtendiensten und der Industrie.
CeoTronics AG, Audio • Video • Data Communication, Adam-Opel-Str. 6, 63322 Rödermark Germany, Tel.: +49 6074 8751-0, Fax: +49 6074 8751-676
verkauf@ceotronics.com
www.ceotronics.com

Citrix Systems GmbH — Stand: P 7

Über Citrix
Citrix (NASDAQ:CTXS) ist ein Anbieter von Cloud-Computing-Lösungen, der mobile Arbeitsmodelle unterstützt und Menschen in die Lage versetzt, von überall aus zusammenzuarbeiten und auf Apps oder Daten zuzugreifen – mit jedem beliebigen Endgerät. Und das genauso einfach und sicher wie im eigenen Büro. Die Cloud-Computing-Lösungen von Citrix machen es IT-Abteilungen und Service-Providern möglich, sowohl Private als auch Public Clouds aufzubauen. Dabei kommen Virtualisierungs- und Netzwerktechnologien zum Einsatz, um leistungsstarke, flexible und kostengünstige Dienstleistungen für mobiles Arbeiten zu bieten. Mehr als 260.000 Unternehmen und über 100 Millionen Anwender setzen weltweit auf Produkte von Citrix.
Weitere Informationen unter www.citrix.de

COMPAREX AG — Stand: B 4

COMPAREX ist ein weltweit agierender IT-Dienstleister, der auf Software-Beschaffung, Lizenzmanagement sowie technische Produktberatung spezialisiert ist. Mit seiner 30jährigen Markterfahrung adressiert COMPAREX öffentliche Verwaltung 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. Ein besonderer Fokus von COMPAREX Deutschland liegt auf der Entwicklung innovativer und maßgeschneiderter Cloud Computing-Lösungen. Weltweit beschäftigt die COMPAREX Gruppe rund 1.800 Mitarbeiter an mehr als 75 Standorten in 29 Ländern in Europa, Asien, Afrika und Amerika. Der Umsatz im Geschäftsjahr 2011/12 betrug 1,066 Milliarden Euro. Weitere Informationen erhalten Sie unter www.comparex.de.

CONDOK GmbH — Stand: Parksaal P 11

Die CONDOK GmbH ist ein Systemhaus für Logistik und bietet ihren Kunden ein breites Leistungsspektrum. Neben der Spezialisierung auf die Erstellung von IETD nach S1000D und 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 85 Mitarbeitern in Kiel, Hamburg und Koblenz unterstützt die CONDOK mit umfangreichen logistischen Dienstleistungen die Bundeswehr sowie eine große Anzahl von Unternehmen der Wehrtechnik und der zivilen Industrie.
www.condok.de

CONET Solutions GmbH & CONET Business Consultants GmbH — Stand: F 10

CONET ist seit mehr als 20 Jahren mit partnerschaftlicher Zusammenarbeit, hoher Dienstleistungsqualität und zielgerichteter IT-Unterstützung ein zuverlässiger Wegbegleiter der Bundeswehr.
Während die CONET Solutions GmbH zahlreiche SinN-Verfahren, Fach- und Führungsinformationssysteme, Kommunikationsarchitekturen und IT-Infrastrukturen betreut und weiterentwickelt, bündelt die CONET Business Consultants GmbH breites Beratungs- und Prozesswissen rund um die SAP-Implementierungen der Bundeswehr.
CONET präsentiert auf der AFCEA-Fachausstellung 2013 an seiner **Integrier-Bar (Stand: F 10)** aktuelle Lösungsansätze, die eine Serviceorientierung der Bundeswehr unterstützen: Leistungsfähige Kommunikationsinfrastrukturen, agile Software-Systeme, moderne Fachapplikationen und verlässliche IT-Architekturen sichern die Einsatzfähigkeit und vereinfachen eine reibungslose internationale Zusammenarbeit.
www.conet.de

Cordsen Engineering GmbH — Stand: F 6

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 ab 19", FO-Hubs, Drucker und Scanner.
Eine Reihe von Standardprodukten sind auf der NRPL gelistet, teilweise auch vom DCSSI für den nationalen (französischen) Einsatz zertifiziert.
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.
Vorgestellt werden: TEMPEST und Rugged Produkte.
Cordsen Engineering GmbH, Am Klinggraben 1A, D-63500 Seligenstadt, Tel.: 06182-9294-0, Fax: 06182-9294-45, www.cordsen.com

cpm communication presse marketing GmbH — Stand: FR 2

Die 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 und Kongresse (zum Teil mit begleitender Ausstellung).
Zu unseren Publikationen gehören:
cpm forum – Das Magazin für Wehrtechnik und Logistik als themenorientierte wehrtechnische Dokumentationen mit jährlich 6 Publikationen
Taschenbuch "Deutsche Bundeswehr – Folge 4 (2012)" als aktuelles Nachschlagewerk über die deutschen Streitkräfte
Taschenbuch "Die Ausrüstung der Bundeswehr" – Folge 2 (2013).
Bundeswehr-Standortposter (DIN A1): Heer, Luftwaffe, Marine und Streitkräftebasis.
info@cpm-st-augustin.de

DATAGROUP BGS GmbH — Stand: G 10

DATAGROUP ist ein deutschlandweit flächendeckender Anbieter von IT-Services, IT-Solutions und IT-Consulting. Mit 1.400 Mitarbeitern und 17 Standorten in Deutschland gehört DATAGROUP zu den Top 10 Unternehmen ihres Branchensegments.
Die nach Branchen und Themenschwerpunkten spezialisierten Mitarbeiter beraten den Kunden und entwickeln maßgeschneiderte Lösungen. DATAGROUP BGS GmbH als verlässlicher Partner bietet Unterstützung für die Bundeswehr und die Defense-Industrie.
Im Fokus: Beratungsdienstleistungen, logistische Analysen und Konzepte, Prozessberatung, Expertenwissen über IT-Systeme und -Architekturen der Bundeswehr und Ämter bis zu den Waffensystemen.
Themen: Interaktive Elektronische Technische Dokumentation (IETD), Wartung/Instandhaltung nach internationalen Standards, z.B. der ASD S1000D/S2000M, Stammdatenmanagement, Informationsbereitstellung Logistik, SASPF.

Diese Kompetenzen können Sie sich auf unserem AFCEA Stand G 10 vorstellen lassen.
Standorte: Mainz, Köln/Bonn, Wilhelmshaven
www.datagroup.de

DATAGROUP Business Solutions GmbH Stand: ZA 1

DATAGROUP Business Solutions GmbH (bis 01.04.2013 Consinto GmbH) bietet als Full Service Dienstleister mit mehr als 30 Jahren IT- und Branchenexpertise für den Defence-Bereich den ganzheitlichen Ansatz:

- Beratungs-, Prozess- und Technologie-Expertise im Bereich Integrated Logistic Support (ILS)
- ILS-Software-Suite: Unterstützung der ILS-Disziplinen "Logistic Support Analysis (LSA)" nach MIL-STD-1388-2B bzw. ASD S3000L/S4000M, für "Materiel Management" nach ASD S2000M/ATA S2000 inklusive Ersatzteilmengenoptimierung mit der "Materiel Optimization Engine" (MOE) und Tools zur Erstellung von Technischen Publikationen nach ASD S1000D bzw. ATA iSpec2200.

DATAGROUP Business Solutions GmbH ist einzigartiger ILS-Komplettanbieter in Deutschland und bietet mit eigenem Rechenzentrum die Möglichkeit, die logistischen Lösungen und Softwareprodukte an Standardprodukte wie z.B. SAP anzubinden.

DEUTSCHE GESELLSCHAFT FÜR WEHRTECHNIK e.V. (DWT) Stand: F 7

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 Stand: P 2

DeviceLock ist seit 16 Jahren als internationaler DLP-Lösungsanbieter technologischer Spitzenreiter in der Datenflusskontrolle und unerlässlich in der IT-Sicherheit&-Compliance. Mit der Vertriebszentrale in Kalifornien und Niederlassungen in Deutschland, Italien, UK sowie Businesspartnern in über 40 Ländern, bietet DeviceLock eine globale Vertriebs-&Supportstruktur. Internationale Entwicklungslabore sind der Garant für eine innovative, vollumfängliche und gehärtete DLP-Solution mit Funktionsbereichen für die Kontextkontrolle aller lokalen Schnittstellen und der Web-&Netzwerkkommunikation sowie einer vollständigen Inhaltsfilterung mit kurzen Implementationszeiten und geringen Anschaffungs-&Wartungskosten. Weltweit wird DeviceLock bei Militär&Polizei, im Finance-&Public-Sektor und globalen Industrie-&Handelskonzernen in über 66.000 Organisationen auf mehr als 4 Millionen abgesicherten Clients erfolgreich eingesetzt.
www.devicelock.de, Tel.: +49 2102 89211-0.

EGL GmbH Stand: T 3

Die Firma **EGL Elektronik Vertrieb GmbH** ist seit über 25 Jahren spezialisiert auf die Umrüstung von handelsüblichen Geräten gemäß dem Zonenmodel der BSI.
Als Prüfgruppe F8 ist sie für die Zertifizierung von Zonengeräten vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen.
Eine Erweiterung um ein zweites BSI zugelassenes Labor wurde 2007 durchgeführt.
Somit ist die Firma EGL in der Lage, die Entwicklungszeiten und die Produktion kundenorientiert zu optimieren.
Für namhafte Firmen, Behörden, Bund und NATO ist die Firma **EGL Elektronik Vertrieb GmbH** der Partner für die Planung und Durchführung von Projekten im IT-Sicherheitsbereich.

Elektronik + Tempest GmbH Stand: FR 5

Elektronik + Tempest GmbH nutzt zwei vom BSI zugelassene Labore, um sich des Problems "Tempest" – also "kompromittierender Abstrahlung" anzunehmen. Hier ist es die Aufgabe der ETG, IT -Equipment entsprechend der Vorgaben des BSI, nämlich eine Abstrahlung zu vermeiden, umzubauen und per Vermessung den Nachweis zu führen, dass diese Maschinen den Schutzrichtlinien des BSI entsprechen. Die hohe Qualifikation unserer Ingenieure und Maschinen ermöglicht es der ETG, beste Ergebnisse dabei zu erzielen und dem Kunden durch qualifizierte Beratung sowohl Kosten zu sparen, als auch "funktionierende" Lösungen für den Schutz von vertraulichen Daten anbieten zu können. Dieses Problem betrifft die Öffentliche Hand ebenso wie die Wirtschaft.
Kontakt: Elektronik+Tempest GmbH, Henleinstraße 16, 28816 Stuhr, www.etgmbh.net, E-Mail: Info@etgmbh.net, Tel.: 0421-8400 790 0, Ansprechpartner: Gerhard Friedrichs

E L N O GmbH Stand: Z 3

Zur AFCEA Ausstellung 2013 stellt die Fa. ELNO GmbH ein neues IP-fähiges Kfz-Intercom System, Funkgeräte, IP-Feldtelefon und Audiozubehör für den militärischen Einsatz vor.

- **Intercom System ELIPS**
  Digitales Intercom System für militärische Fahrzeuge
  Plug & Play IP
  Ethernet Netzwerk
  Modular und programmierbar
- IP- Feldtelefone
- Funkgeräte
- Sprechsätze

Kontakt: Elno GmbH, IBC Ismaning-Business-Center, Gutenbergstr. 1, D-85737 Ismaning, Tel.: 089 329489-0, Fax 089 329489-70
Die Deutsche Webseite ist derzeit im Aufbau. Siehe auch www.Elno.fr

Empolis Information Management GmbH Stand: G 6 – G 8

Empolis ist der Anbieter von Smart Information Management Software zur ganzheitlichen Erstellung, Verwaltung, Analyse, intelligenten Verarbeitung und Bereitstellung aller relevanten Informationen. Die Lösung Empolis Decision Intelligence unterstützt die menschliche Urteilskraft durch die automatisierte Auswertung, Vernetzung, Recherche, Homogenisierung, Normalisierung und Verteilung von strukturierten und unstrukturierten Informationen.
Sie optimiert die Auswertung von Rohdaten sowie den Zugriff auf unterschiedliche Informationsquellen und steuert den Fluss von Informationen sowie Erkenntnissen durch den Einsatz wissensbasierter Verfahren. Sie ermöglicht eine übergreifende Recherchestruktur über alle internen und externen Informationsquellen hinweg unter Berücksichtigung von Daten- und Geheimschutz.

ESET Deutschland Stand: K 7

Der slowakische Antivirenhersteller ESET schützt seit 1992 mit zukunftsweisenden Softwarelösungen Unternehmen und Privatanwender vor Malware aller Art. Der Sicherheitsspezialist gilt als Vorreiter bei der proaktiven Bekämpfung selbst unbekannter Schädlinge.
Die hohe Malwareerkennung und Geschwindigkeit sowie eine minimale Systembelastung zeichnen alle ESET-Antivirenprogramme aus. Zu den bekanntesten Produkten zählen ESET NOD32 Antivirus und ESET Smart Security. Das Produktportfolio umfasst Programme zum Schutz von Windows-, Mac- und Linux-Rechnern sowie von Mail- und Fileservern und Netzwerk-Gateways. ESET Mobile Security bietet Smartphones Sicherheit vor Malware und Datenmissbrauch.
ESET beschäftigt in seiner Unternehmenszentrale in Bratislava (Slowakei) und in der Niederlassung in San Diego (USA) mehr als 700 Mitarbeiter. ESET-Produkte sind über ein weltweites Partnernetzwerk in mehr als 180 Ländern erhältlich. Exklusiver Distributor in Deutschland ist DATSEC Data Security aus Jena.
Kontakt: Maik Wetzel, ESET Deutschland, Talstraße 84, 07743 Jena

ESG Elektroniksystem- und Logistik-GmbH Stand: G 1

Die ESG blickt, ausgehend von der Gründung der FEG Flug-Elektronik-Gesellschaft im Jahr 1963, auf eine nunmehr 50-jährige stabile und gelebte, verlässliche Partnerschaft mit ihren Kunden aus den Bereichen Sicherheit und Verteidigung, Behörden und Industrie zurück. Von Beginn an zeichnet sich diese Partnerschaft durch eine besondere Leidenschaft für Technik, Innovationskraft und -fähigkeit aus.
Mit unseren tragfähigen und nutzerorientierten IT- und Logistik-Lösungen unterstützen wir die Verbesserung der Fähigkeiten der Bundeswehr im Einsatz und Grundbetrieb. Beispiele dafür präsentieren wir auf der diesjährigen AFCEA: Mobile Führungssysteme und einsatzrelevante Systemintegrationsprojekte.
ESG – Dedicated to solutions.
Kontakt: ESG Elektroniksystem- und Logistik-GmbH, Livry-Gargan-Str. 6, 82256 Fürstenfeldbruck, E-Mail: itk@esg.de, Tel.: 089/9216-0, www.esg.de

Esri Deutschland GmbH Stand: G 6 – G 8

Die Esri Deutschland GmbH mit Sitz in Kranzberg bei München ist eine Firma der Esri Deutschland Group GmbH und vertreibt als Distributor und Systemhaus die Produkte von Esri Inc. exklusiv über elf Standorte in Deutschland und der Schweiz. Esri unterstützt die Anwender mit einem breit gefächerten Schulungs-, Support- und Consultingangebot und dem gesamten Erfahrungsreichtum von mehr als 450 Mitarbeitern der Esri Unternehmensgruppe.
Für das Marktsegment BOS hat Esri Deutschland GmbH eine eigene Niederlassung in Bonn aufgebaut, die den BOS Bereich in Deutschland und der Schweiz betreut.
In der Esri Unternehmensgruppe ergänzt seit Januar 2012 die Geosecure Informatik GmbH am Standort Bonn das Leistungsgspektrum durch die Fokussierung einer Professional Services Abteilung speziell für den BOS Bereich mit eigenen Lösungsbausteinen.

Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) — Stand: F 8

Das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) entwickelt Systeme für Verteidigung und Sicherheit, mit denen Informationen gewonnen, übertragen, analysiert und zu ergonomisch adäquat präsentierten Lagebildern fusioniert werden. Dies ist grundlegend für effiziente Entscheidungsprozesse. Das Vorgehen in den Einzelprojekten geschieht nach der Devise "Denken vom Einsatz her". Beispiele sind multinationale Projekte für See-, Küsten- und Bodenüberwachung, in denen aus Datenströmen heterogener Sensorquellen und in Datenbanken abgelegten Hintergrundwissen durch leistungsfähige Algorithmen für Datenfusion und effizientes Ressourcen-Management zeitkritische, entscheidungsrelevante Informationen gewonnen werden. In diesem Sinne sind Fusions- und Management-Algorithmen Beispiele für IT-Services, die bemannte und unbemannte Aufklärungsmissionen in multinationalen Koalitionen ermöglichen.

Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB — Stand: T 1 u. ZA 3

Das Fraunhofer IOSB mit seinen Hauptstandorten in Karlsruhe und Ettlingen verfügt über ein einzigartiges, durchgängiges Kompetenzspektrum von der Objekt- und Atmosphärenphysik über die Optik, die Sensorphysik, die Bild- und Signalauswertung bis hin zur Informations- und Wissensverarbeitung sowie der Mensch-Maschine-Systemtechnik. Ein Schwerpunkt für wehrtechnische Anwendungen liegt in der Echtzeitauswertung und Fusion der Daten vernetzter, abbildender Sensoren, z. B. "Full-Motion-Video", Infrarotkameras, abbildende Laser- sowie Radar-Systeme. Als Elemente einer vernetzten Operationsführung sind die luft- und raumgestützte Aufklärung und Überwachung, die präzise Wirkung durch Zielerkennung und Zielübergabe, der Schutz durch Warnsensorik sowie die Modellgenerierung und Simulatorföderation für Ausbildung und Training wichtige Anwendungsgebiete für das Geschäftsfeld Verteidigung des IOSB.
Ansprechpartner: Dr. Jürgen Geisler, Fraunhoferstraße 1, 76131 Karlsruhe, Telefon +49 (0) 721 6091 262, verteidigung@iosb.fraunhofer.de, www.iosb.fraunhofer.de/verteidigung

FREQUENTIS Nachrichtentechnik GmbH — Stand: K 2

Frequentis Defence bietet individuelle Lösungen für die vernetzte Operationsführung in den Marktsegmenten militärische Flugsicherung, Einsatz- und Operationsführung, taktische Netzwerke, nationale Sicherheit und Grenzschutz sowie Überwachung und Aufklärung. Eine hohe Zuverlässigkeit, innovative Benutzeroberflächen und bewährte Technologien garantieren Kundenzufriedenheit. Als anerkannter Anbieter von integrierten Gefechtsständen versprechen wir maßgeschneiderte Lösungen, eine flexible Skalierbarkeit sowie ein Maximum an Kosteneffizienz. Hervorragende Leistung, Fokus auf Kundenorientierung und Einhaltung internationaler Standards sind hierbei ein Muss! Über 250 Kunden in mehr als 110 Ländern vertrauen auf das Know-how und die Erfahrung von Frequentis. Mit Tochtergesellschaften, Niederlassungen und Repräsentanzen ist das Unternehmen in über 50 Ländern aktiv.

gabo Systemtechnik GmbH — Stand: B 2

Vor mehr als 40 Jahren hat sich gabocom auf Rohrsysteme für die Nachrichten- und Energietechnik spezialisiert. Heute ist das niederbayerische Unternehmen in ganz Europa Inbegriff für höchste Qualität und besten Service. Die innovative Produktpalette umfasst drei multikompatible Systemlösungen – speed•pipe® System, Halbrohr System und allgemeine Formteile. Mit dem speed•pipe® System hat gabocom ein marktführendes Mikrorohrsystem entwickelt, das genau auf den Bedarf moderner Telekommunikations-Gesellschaften und Netzbetreiber zugeschnitten ist. Namhafte Anbieter aus ganz Europa realisieren mit den innovativen Mikrorohren, Formteilen und Abdichtelementen leistungsfähige Fibre-to-the-X Lösungen: in neuen oder bestehenden Rohranlagen, bei Rohr-in-Rohr oder direkter Erdverlegung, von großen Längen bis hin zur letzten Meile.

Galleon Embedded Computing GmbH — Stand: P 9

Galleon Embedded Computing liefert integrierte High Performance Datenrecorder und Mission Computer für den Einsatz in Drohnen, Flugzeugen, Schiffen oder militärischen Fahrzeugen. Der Rugged Recorder XSR ist nur 15 x 17 x 10 cm groß, kann als Gigabit Ethernet, als serial FPDP Recorder oder als Rugged Server konfiguriert werden. Die Kapazität der SSD Wechselspeichereinheit kann bis zu 4 TB betragen. Außerdem liefern wir COTS basierende Board- und Systemlösungen wie z.B.

- Recorder Systeme mit analogem bzw. HF Frontend
- 3rd generation Intel® Core™ i7 basiernde Single Bord Computer
- High Performance Rugged Grafik und Video Boards
- Xilinx Virtex 6 und 7 basierende I/O Boards mit Sampling bis zu 3.6 GHz und DDC

Darüberhinaus zeigen wir das taktische Mikrofonarraysystem "CAPsure" für die akustische Überwachung und Aufzeichnung.

GBS TEMPEST & Service GmbH — Stand: P 12

Die GBS GmbH, mit Sitz in Diepholz, ist ein offiziell anerkanntes und vom Bundesamt für Sicherheit in der Informationstechnik zertifiziertes Unternehmen. Für das Geschäftsfeld TEMPEST, verfügt die GBS GmbH über zwei firmeneigene, BSI geprüfte Tempestlabore.
Neben der Berechtigung zur Durchführung von Zonenkurzmessungen ist die GBS GmbH auch offiziell eine vom BSI anerkannte Prüfstelle für Zulassungsmessungen nach SDIP 27 Level A, Level B und Level C (International) und dem Zonenmodell (National).
Adresse: von-Braun-Straße 6, D-49356 Diepholz, Tel.: +49 5441 9758-100, Fax: +49 5441 9758-129, Homepage: http://www.gbs-tempest.de, E-Mail: info@gbs-tempest.de

Gebrüder Friedrich Industrie- und Elektrotechnik GmbH — Stand: P 11

Die Gebr. Friedrich Industrie- und Elektrotechnik GmbH (GFE) ist seit vielen Jahren Rahmenvertragspartner des BWB/BAAINBw. Ganz egal ob es sich um planmäßige Vorhaben wie z.B. die Einrüstung von Kabinen oder um Maßnahmen im Rahmen der Soft.-Inst. handelt. In den Bereichen Schaltanlagenbau, Elektrotechnik, Elektromaschinenbau, Pumpentechnik oder Kälte-/Klimatechnik 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 mbh — Stand: G 21

genua sorgt für sichere VS-Datenkommunikation
Für die Datenkommunikation bis zur Stufe VS-NfD bietet genua zwei hochsichere Lösungen: die Firewall & VPN-Appliance genuscreen und das Mobile Security Device genucard – beide mit VS-NfD-Zulassung vom Bundesamt für Sicherheit in der Informationstechnik (BSI). genuscreen ist für den stationären Einsatz ausgelegt und umfasst ein VPN-Gateway zur zuverlässigen Verschlüsselung sensibler Daten sowie eine Firewall zur Kontrolle von Netzwerk-Schnittstellen. Die genucard dient dagegen zum Aufbau sicherer Remote-Access-Lösungen. Das kompakte Device wird mit Notebook oder Desktop verbunden und ermöglicht mobilen Anwendern oder Mitarbeitern im Home Office den verschlüsselten Austausch von VS-NfD-Daten.
genua mbh, Domagkstraße 7, 85551 Kirchheim bei München, Tel.: +49 89 991950-0, www.genua.de

Geosecure Informatik GmbH — Stand: G6 – G8

In der Esri Unternehmensgruppe ergänzt seit Januar 2012 die **Geosecure Informatik GmbH** am Standort Bonn das Leistungsspektrum durch die Fokussierung einer Professional Services Abteilung speziell für den BOS Bereich mit eigenen Lösungsbausteinen. Geosecure bietet kompetente und branchenspezifische Unterstützung bei Problemstellungen mit Daten mit Raumbezug und verfügt über spezielle Lösungen, die sich insbesondere auf das militärische GIS, C2 und Intel-Umfeld sowie die damit verbundenen Aufgaben im Bereich der militärischen IT-Sicherheit beziehen.
Kontaktdaten: Esri Deutschland GmbH, Marko Prisky, Niederlassung Bonn, Rheinallee 24, 53173 Bonn, Telefon: 089-20 7005 1720, E-Mail info@bonn.esri.de, Homepage www.esri.de

GEOSYSTEMS GmbH — Stand: G 3

GEOSYSTEMS ist Lösungsanbieter und Softwarevertriebsunternehmen mit herausragender Kompetenz im Geoinformations-Workflow für sicherheitsrelevante Aufgaben. Als Partner von Intergraph® bietet GEOSYSTEMS die Geospatial Produktlinie und maßgeschneiderte Systeme. Produkte von Intergraph Geospatial werden weltweit im Defence-Bereich erfolgreich für die Auswertung hochauflösender Luft- und Satellitenbilddaten, wie auch UAV-Daten eingesetzt. Objekterkennung, Veränderungsnachweise, Höhenmodellgenerierung, Gebäude-Erkennung, Kartenerstellung: Diese Aufgaben werden mit Intergraph Geospatial Kosten sparend gelöst. Geoprocessing im Web eröffnet neue Möglichkeiten für eine rasche, flexible Datenverarbeitung. Unsere kompletten Geodatenmanagementsysteme berücksichtigen alle spezifischen Sicherheits- und Vertraulichkeitsrichtlinien. Die Datenverteilung erfolgt über den derzeit schnellsten Bilddatenserver.
Weitere Informationen finden Sie unter: www.geosystems.de

GPP Service GmbH & Co. KG — Stand: K 5

Projekte gemeinsam zum Erfolg führen
Sie wollen Ihr Projekt zum Erfolg führen. Wir unterstützen Sie dabei, dieses Ziel zu erreichen

- schnell, sicher und ohne Umwege. Seit über 30 Jahren sind wir als kompetente und engagierte Spezialisten für IT-Dienstleistungen im militärischen Bereich etabliert.

Gerne unterstützen wir Sie in den Bereichen

- Systemtechnische Begleitung,
- Projektbezogene IT-Sicherheitskonzepte sowie
- Prozess-Optimierung.

Für die Projektkommunikation ohne Wenn und Aber in allen militärischen Projekten sorgen unsere Projekt-Portale **milport®**.
Darüber hinaus sind wir Experten für die Validierung und Verifikation von Projektergebnissen (IV&V), das V-Modell® XT und IT-Sicherheit (zDV 54/100, ISO 27000).

Besuchen Sie uns im Internet unter **www.gpp-service.de** oder treffen Sie uns persönlich auf der AFCEA Fachausstellung – wir freuen uns auf Sie!

Green Data Systems — Stand: ZA 4

Green Data Systems (GDS) ist spezialisiert auf Hitachi Converged Computing und Container-Rechenzentren.
Ein Schwerpunkt beim Converged Computing ist die Virtualisierung von SAP-Umgebungen. Neben den Komplettlösungen bietet GDS die Möglichkeit, die SAP-Infrastruktur inklusive Services zu kaufen oder pro SAP-User pro Monat abzurechnen.
Die Container-Rechenzentren sind Komplettlösungen, die bis zur schlüsselfertigen Inbetriebnahme inklusive TÜV-Abnahme eine effektive, flexible RZ-Alternative darstellen. Sie verfügen über die relevanten RZ-Standards und Sicherheitsanforderungen und sind ausgestattet mit Kühlung, Zugangskontrolle, Feuerlöscheinrichtungen, USV, Notstromaggregaten sowie Standard 19-Zoll Racks. Auch für die Container-Lösungen bietet GDS vom klassischen Kauf bis hin zu Nutzungsmodellen mit monatlicher Abrechnung flexible und attraktive Kauf-Alternativen an. **www.greendatasystems.de**

Hardthöhenkurier — Stand: FR 3

Der Hardthöhenkurier ist ein periodisch erscheinendes Magazin, das sich seit 29 Jahren mit aktueller Berichterstattung an Soldaten der Bundeswehr wendet und sich als Bindeglied zwischen der Bundeswehr und der wehrtechnischen Industrie und Wirtschaft versteht. Mit seinem neuen Auftritt hat sich das Fachmagazin zu einer in Deutschland und in den europäischen Nachbarländern anerkannten Informationsquelle für Streitkräfte und Wehrtechnik weiter entwickelt. Im Rahmen der Krisen- und Konfliktprävention werden sicherheitspolitische Aspekte der inländischen Sicherheit sowie Auswirkungen internationaler Krisen und Konflikte auf Deutschland betrachtet. Der Hardthöhenkurier informiert über sicherheitspolitische Rahmenbedingungen, Einsätze der Bundeswehr, aktuelle Vorhaben der Streitkräfte sowie Neuerungen in der Wehrtechnik und Rüstungsindustrie. Der Hardthöhenkurier erscheint 6 x jährlich und ergänzt mit aktuellen Sonderausgaben seine Kompetenz auf militär-politischen und wehrtechnischen Gebieten. Mit dem neuen ONLINE Auftritt bieten wir unseren Lesern und Partnern in Ergänzung zu den bisherigen Angeboten im PRINT-Bereich eine tagesaktuelle Berichterstattung und erweiterte Möglichkeiten zur Information über wichtige Ereignisse und Produkte als eine innovative Zusatzleistung mit nahezu unbegrenzten Möglichkeiten, beispielsweise durch Schaltung von Bannern und Video-Clips.
www.hardthoehenkurier.de

Hewlett-Packard GmbH — Stand: K 4

Als weltweit größtes Technologie-Unternehmen bietet HP ein umfassendes Portfolio, das Kunden dabei unterstützt, ihre Geschäftsziele zu erreichen – dazu gehören Lösungen in den Bereichen Software, Services, IT Infrastruktur sowie Drucken und Personal Computing,
HP schafft neue Möglichkeiten für den sinnvollen Einsatz von Technologie und Services für Sicherheitsbehörden, um aktuelle Herausforderungen zu bewältigen:

- Kommando und Kontrolle für die Verteidigung: operationale Informationslösungen ermöglichen bessere und termingerechte Entscheidungen
- Cyber Security für die Verteidigung: Weiterentwickeltes Spektrum an Cyber Security Lösungen auf dafür ausgelegter IT-Infrastruktur
- Verbesserung der Effizienz und Effektivität der Verteidigungslogistik
- Verbesserung der Personaldienstleistungen für die Verteidigung
- HP Lösungen für nationale Sicherheit und Notfallmaßnahmen

Mehr Informationen: www.hp.com/go/defense

Hexagon GeoSpatial Solutions — Stand: G 3

Im Jahr 2010 übernahm der schwedische Hexagon-Konzern die Firma Intergraph. Diese Übernahme machte es möglich, die beiden weltweit führenden Anbieter auf dem Gebiet der Photogrammetrie-Sensorik – den Bereich Airborne Sensors der Firma Leica Geosystems in Heerbrugg/Schweiz und den bis dahin in der Firma Intergraph integrierten Geschäftsbereich Z/I Imaging in Aalen/Deutschland – zum neuen Bereich Hexagon Geospatial Solutions unter dem Dach von Hexagon Geosystems zusammenzuschließen. Damit hat der Markt erstmals die Möglichkeit, von einem Anbieter alle gebräuchlichen Sensoren als Komplettlösung zu beziehen – sowohl Großformat-Kameras als auch Mittelformat-Kameras und LIDAR-Systeme verschiedenster Leistungsklassen.
Weitere Details finden Sie unter http://digital-imaging.leica-geosystems.com/en/index.htm bzw. www.ziimaging.com

Hitachi Data Systems — Stand: T 2

Hitachi Data Systems bietet branchenweit führende Informationstechnologien, Services und Lösungen für einen überzeugenden Return on Invest (ROI) sowie Return on Assets (ROA) und verschafft Unternehmen somit einen nachweisbaren wirtschaftlichen Mehrwert. Der Vision einer virtualisierten, automatisierten, cloud-fähigen und nachhaltigen IT folgend, senken die Lösungen von Hitachi Data Systems die IT-Kosten und erhöhen gleichzeitig die Agilität. Mehr als 5.300 Mitarbeiter weltweit in über 100 Ländern helfen dabei, diese Vision Wirklichkeit werden zu lassen. Die größten Unternehmen der Welt, darunter mehr als 70 Prozent der Fortune-100-Unternehmen sowie über 80 Prozent der Fortune-Global-100-Unternehmen, vertrauen auf die Produkte, Services und Lösungen von Hitachi Data Systems. Daten bewegen unsere Welt – Informationen sind die neue Währung. Für weitere Informationen besuchen Sie www.hds.com/de.

IABG mbH — Stand: G 17

Als ein führendes europäisches Technologieunternehmen mit den Branchen Automotive • InfoKom • Mobilität, Energie & Umwelt • Luftfahrt • Raumfahrt • Verteidigung & Sicherheit konzipieren und entwickeln wir sichere, moderne und innovative Netz- und Systemarchitekturen, realisieren Prototypen und begleiten die Einführung bis zur Abnahme.
In multinationalen Einsätzen sorgen wir mit unseren Open-Source basierten IT-Services für eine sichere und zuverlässige Kommunikation und Lageführung mit Partnern auch auf der schmalbandigen "letzten Meile". Diese Dienste lassen sich in die neue dienstorientierte Architektur des IT-SysBw einbinden.
Auf dem Gebiet hochmobiler, sicherer Netze gestattet unsere HiMoNN-Lösung auch breitbandige Anwendungen (Sprache, Daten, Video) sowie die Anbindung an eine vorhandene Netzinfrastruktur, z.B. über unseren Teleport (SatCom-Services).
Wir unterstützen ein effektives Risiko- und Sicherheitsmanagement hinsichtlich IT-Sicherheit.
IABG mbH, Einsteinstrasse 20, 85521 Ottobrunn, Tel.: +49 89 6088-2030, Fax: +49 89 6088-4000 info@iabg.de www.iabg.de

IBM Deutschland GmbH — Stand: G 20

IBM ist einer der weltweit größten Anbieter von Informationstechnologie und B2B-Lösungen. IBM und Partner bieten den Kunden eine komplette Produktpalette innovativer Informationstechnologie an: von Hardware und Software über Dienstleistungen, inklusive Beratungsleistungen, und komplexe Anwendungslösungen bis hin zu Outsourcingprojekten und Weiterbildungsangeboten sowie Finanzierungskonzepten. Mit hohen Investitionen in die Forschung will IBM auch weiterhin Schrittmacher in der Entwicklung neuer Technologien und Lösungen bleiben.
Mit der diesjährigen Kernbotschaft "Smarter Defense – Integrierte Services in einem heterogenen Umfeld" adressiert IBM die besonderen Anforderungen mit verfügbaren Lösungen für das Informationsmanagement, die Informationsversorgung und die IT-Sicherheit in stationären, verlegefähigen und mobilen Anwendungsfällen. Dies schließt die Sammlung, Auswertung und Aufbereitung von Informationen sowie die bedarfsgerechte Bereitstellung und den sicheren Betrieb der erforderlichen IT Umgebungen mit ein.
www.ibm.com/de

ICOS GmbH — Stand: G 22

Als konzernunabhängiger Hersteller von maßgeschneiderten Systemlösungen für industrielle und wehrtechnische Anwendungen beliefert ICOS seit 1992 die wehrtechnischen Systemhäuser mit gehärteten Kommunikations-Rechnern, Servern, Laptops, hochauflösende Displays (HEL) und IT-Komponenten sowie Software-Lösungen, speziell Visualisierungs- und Kommunikationsanwendungen. Unter Einsatz handelsüblicher IT-Produkte (COTS-Produkte) ergänzt mit spezifischen mechanischen und elektronischen Eigenentwicklungen in Form von Mikrokontroller-basierenden intelligenten Überwachungs- und Steuereinheiten ist ICOS in der Lage, eine den projektspezifischen Anforderungen entsprechende Systemlösung auch für Comsec-Zone 1 Anwendungen zu realisieren.
Die Systeme werden zum Beispiel in der kettengetriebenen Panzerhaubitze PzH2000, im TPZ Fuchs ABC, in U-Booten und LKW-Sheltern erfolgreich eingesetzt, ganz aktuell bei FülnfoSys-Heer und FülInfoSys-Heer-HEL.

Indra S.A. — Stand: G 14

Indra S.A. ist der führende Spanische Elektronik Konzern, der sich in den letzten 30 Jahren zu einer multinationalen weltweit operierenden **Verteidigungs- und Sicherheitstechnologiefirma** entwickelt hat. In Deutschland wird Indra durch seine Tochterfirma **Avitech GmbH,** Friedrichshafen, vertreten.
Indra nutzt ihre eigene Forschung und Entwicklung, um weltweit eine führende Rolle im Markt der hochentwickelten elektronischen Systeme aufzubauen. Die Grundlagen dafür bilden 42,000 hochqualifizierte Mitarbeiter in über 110 Ländern.
Die Indra Verteidigungs- und Sicherheitslösungen werden u.a. in Deutschland, Frankreich, Finnland, Portugal, den USA, Neuseeland, Indien und Brasilien verwendet.
Die **Angebotspalette** erstreckt sich dabei von **Radaren, über elektronische Kampfführung und Aufklärung, Selbstschutz, Kommunikation, Führungssystem, Überwachung, Simulation bis zum Weltraumsegment. Die neueste Entwicklung ist das advanced maritime reconnaissance intelligence (MRI) System auf der Basis des Tecnam P2006T Leichtflugzeuges.**
Kontaktdaten: Avitech GmbH, Peter Rudolph, VP Business Development, Bahnhofplatz 1, 88045 Friedrichshafen, Telefon: +49 (0) 7541-282-0, Fax: +49 (0) 7541-282-199

INFODAS GmbH — Stand: G 9

INFODAS ist seit 1974 als unabhängiges und herstellerneutrales Software- und Beratungsunternehmen ein verlässlicher Partner der Bw. Dieses Wissen ist in unsere langjährige **Beratungs- und Lösungskompetenz** in den Bereichen **IT-Sicherheit** sowie **Informations- und Kommunikationssysteme** eingeflossen. Kernkompetenzen sind:

- SDoT®/RSGate®, sicherer, kontrollierter Informationstransfer an Rot-/Schwarz-Übergängen
- SDoT® Labelling Service, zulassungsfähige Kennzeichnung und Auswertung von Security Labeln
- Offline Systemprüfung, die Prüfsoftware zur Erkennung fehlerhafter Baugruppen in komplexen Umgebungen wie FülnfoSys, Fahrzeugen usw.
- SAVe®, die IT-Sicherheitsdatenbank mit integrierten Sicherheitsvorgaben ZDv 54/100
- Informationssicherheitsberatung und Erstellung von Sicherheitskonzepten

- Planung/Realisierung komplexer Informationssysteme, Netzwerke und IT-Plattformen
- Projekt-, Anforderungs-, Nutzungs-, Konfigurations-, Qualitätsmanagement sowie weitere Beratungsleistungen und Analysen für den öAG
- Hardware/Software-Integration in Kabinen, Fahrzeugen und TULBs.

www.infodas.de – vertrieb@infodas.de

Integer Solutions GmbH — Stand: K 8

Die Integer Solutions GmbH ist Anbieter von IT-Produkten und Lösungen rund um das Thema Identifikation und Automatisierung. Dies beinhaltet Beratung, Programmierung, Integration und Service aus einer Hand.
Das Produktportfolio umfasst u.a.

- Mobile Datenerfassung lokal oder im Außendienst
- Lagerverwaltungssysteme
- SAP Anbindungen
- Individuell angepasste Softwarelösungen
- Kennzeichnungs- und Barcodelösungen
- Datenerfassungstechnologien
- RFID Technologien
- Service und Support

Integer Solutions unterstützt dabei alle gängigen Softwareumgebungen wie SAP, AS/400, Brain, Baan, Unix und Windows in den unterschiedlichsten Branchen.
Das breit gefächerte Partnernetzwerk und die langjährige Erfahrung bilden eine solide Basis für die Lösungen und Dienstleistungen.
Anschrift: Integer Solutions GmbH, Küchlerstrasse 1, 61231 Bad Nauheim, www.integer-solutions.com **Ansprechpartner:** Herr Christoph Rack, Tel.: +49 6032 34956-0, Fax: +49 6032 34956-77, c.rack@integer-solutions.com

Intergraph SG&I Deutschland GmbH — Stand: G 3

Intergraph ist einer der führenden internationalen Anbieter raumbezogener Lösungen für Verteidigung und Nachrichtenwesen, für die öffentliche Verwaltung, Behörden und Organisationen mit Sicherheitsaufgaben (BOS), Transport/Verkehr, Photogrammetrie und Fernerkundung, Versorgungs- und Entsorgungswirtschaft sowie Telekommunikation. Unsere Kunden vertrauen auf Intergraphs Lösungen zur Aufbereitung umfangreicher, komplexer Datenmengen in Form aussagekräftiger, graphischer Darstellungen. Damit lassen sich zeit- und situationsgerecht wichtige Entscheidungen treffen, von denen tagtäglich das Wohlbefinden und die Sicherheit von Millionen von Menschen rund um den Globus abhängig sind. Intergraph bietet Systemlösungen für jeden einzelnen Schritt im Arbeitsablauf der digitalen Datengewinnung: Missionsplanung, Datenmanagement und -speicherung, Datenprozessierung, Verteilung und Auswertung.
Weitere Informationen finden Sie unter: www.intergraph.de

ITT Exelis — Stand: Z 1a

ITT Exelis ist ein neues Unternehmen, das 2011 aus der Teilung des ITT Konzern in drei unabhängige börsennotierte Unternehmen hervorging und mit mehr als 20.000 Beschäftigten im Jahr 2011 einen Umsatz von 5,8 Mrd. USD erwirtschaftet hat. ITT Exelis liefert integrierte Lösungen für Bereiche der militärischen und inneren Sicherheit weltweit.
Das Unternehmen hat sechs Bereiche mit den Schwerpunkten:
Aerostructures: Composite Strukturen für Flugzeuge, Helikopter und UAV's
Electronic Systems: Radar und Sonarsysteme, Elektronischer Kampf, Flugsicherungssysteme, Antennen und IED Jammer
Night Vision and Tactical Communications Systems: Taktische Netzwerke, Funk-und Satellitensysteme für sichere Daten und Sprachkommunikation, Nachtsichtsysteme
Geospatial Systems: Payload für Satelliten, Sensoren für UAV und Helikopter, militärisches GPS
Information Systems: Cyber Warfare, Lösungen zur militärischen und zivilen Nutzung des Weltraums
Mission Systems: Komplettes Dienstleistungsangebot für den Betrieb, Wartung und Vorortunterstützung militärischer Anlagen im Einsatzland und Heimatland

itWatch — Stände: G 19 und E 1

itWatch steht für innovative IT-Sicherheit "made in Germany". Endgeräte Sicherheit, Data-Loss-Prevention, Verschlüsselung und Kostenreduktion des IT-Betriebes stehen im Fokus.
Im Public Sector bieten die patentierten, **itWatch** Sicherheitslösungen durch ihre weltweiten Alleinstellungsmerkmale viele Vorteile – gerade in der Inneren Sicherheit. Hohe Anforderungen von Nachrichtendienst, Militär (Einsatz bis GEHEIM und NATO-restricted) und Polizei werden ebenso erfüllt wie solche von Standard-Büro-Arbeitsplätzen und Spezialprojekten. Mit großen Installationen, weit über 140.000 Lizenzen, stellen die **itWatch**-Lösungen ihre Stabilität und Effizienz täglich unter Beweis.
Alle **itWatch**-Produkte werden, frei von Hintertüren und ohne Zukauf von Teil- oder Gesamtlösungen, im Hause **itWatch**, in Deutschland, entwickelt, getestet und weltweit über Partner vertrieben.
Kontakt: itWatch GmbH, Kristina Ferdowsi, Aschauer Straße 30, 81549 München, Telefon: 089 6203010 - 0, Fax: 089 6203010 - 69, office.muenchen(at)itwatch.de, www.itwatch.de

JHL Communication Technology GmbH — Stand: B 3

JHL Communication Technology GmbH (JHLCT) ist ein internationaler Anbieter von Kommunikations- und Informationstechnologie mit einer vollständigen Produktpalette für das Marktsegment C4I.
Die Mission von JHLCT ist der Entwurf, optimale Integration von maßgeschneiderten C4I-Systemen die den Erwartungen seiner Kunden erfüllen, wenn nicht übertreffen, bei der Verwendung von den neuesten Technologien. JHLCT seine größte Bereicherung sind die engagierten und qualifizierten Mitarbeiter, sie blicken zurück auf eine lange Tradition im Bereich der globalen militärische Kommunikation von Morse bis zur heutigen anspruchsvollen digitalen Kommunikation. Sie haben Kommunikations- und Informationssysteme für Kunden in der ganzen Welt entworfen und geliefert, diese Systeme sind basiert auf das breite Wissen in dem C4I Segment, Hightech-Produkte, technische Fähigkeiten und Systemkompetenzen.
Der Mehrwert bringt JHLCT durch seine kreativen Lösungen für spezifische Kundenanforderungen, auch für kleine Mengen. JHLCT ist der Spezialist bei der Anpassung von Standard COTS Produkten für die harten militärischen Betriebsbedingungen.

JK DEFENCE & SECURITY PRODUCTS GMBH — Stand: P 6

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 des größten Herstellers von militärischen Funkgeräten **Harris-RF** 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.

Lachen Helfen e.V. — Stand: E 2

Eine Initiative deutscher Soldaten und Polizisten für Kinder in Kriegs- und Krisengebieten.
"Lachen Helfen e.V." wurde 1996 durch Soldaten im Einsatz in Kroatien gegründet und ist seit 1998 ein eingetragener, als gemeinnützig anerkannter Verein, mit dem Ziel, Kinder in Kriegs- und Krisengebieten zu unterstützen. Dies geschieht u. a. durch den Wiederaufbau bzw. Bau von Kindergärten, Schulen und Gesundheitszentren. Der Bedarf wird in den Einsatzländern (EUFOR, KFOR und ISAF) durch Soldaten vor Ort erkundet, die Ausführung wird begleitet und überwacht, so wird verhindert, dass Gelder in falsche Hände geraten. Größere Projekte werden vorab mit dem Einsatzführungskommando in Potsdam abgestimmt.
Im Verein sind Mitglieder, sowie ehemalige und aktive Soldaten und Polizisten ehrenamtlich tätig. Das Spendenaufkommen fließt zu 90% in die Projekte ein.
Seit Frühjahr 2009 ist die Polizei in den Verein integriert, eine sehr sinnvolle Kooperation aufgrund der Tatsache, dass sie mit der Bundeswehr häufig im selben Einsatzland Dienst leistet. Der Bundesminister der Verteidigung, der Generalinspekteur, der Wehrbeauftragte sowie viele andere unterstützen "Lachen Helfen e.V." bereits aktiv. Ein Großteil des Sponsorings bestreiten Wirtschaft und Industrie. Ein wertvoller Teil der Vereinsarbeit liegt aber auch in den Händen unserer Standortrepäsentanten.
Mehr unter www.lachen-helfen.de.

Liske Informationsmanagementsysteme — Stand: FR 4

Liske Informationsmanagementsysteme ist Produzent von Informations- und Wissensmanagementsystemen. Mit **MIRAKEL®** steht dafür eine eigene Entwicklungsplattform und Produktpalette zur Verfügung. **MIRAKEL®** verarbeitet und ermöglicht den Zugriff auf Informationen aus Papier, elektronischen Dateien, Mailsystemen wie Outlook oder LOTUS, Internetseiten und Datenbanken. Der direkte Zugriff auf die Informationen in den Originaldateien erfolgt über ein sehr leistungsfähiges, fehlertolerantes Textretrival. Einsatz in konventionellen Netzwerken, im Intranet und Internet.
Zu den auf der Entwicklungsplattform **MIRAKEL®** angebotenen Leistungen gehören die

- Beratung, Installation, Schulung und Wartung zum Einsatz der Standardprodukte
- Analyse und das Reengineering von Informationsprozessen
- Konzipierung, Entwicklung, Anpassung und Implementierung von Informations- und Wissensmanagementsystemen

LOG GmbH — Stand: K 6

Seit über 25 Jahren berät und unterstützt die LOG als enger Partner die Bundeswehr und befreundete Streitkräfte an der Schnittstelle von Technologie und Logistik, auch im Einsatz.
Wir sind der Spezialist für sichere, individuelle logistische **Lösungen.** Mit den Geschäftsfeldern Logistics Consulting, Concepts & Coaching, Life Support, Product Lifecycle Management, Engineering Support und Data Management bieten wir dabei ein breites Spektrum an ganzheitlichen Lösungen an.
An Stand K 6 präsentieren wir einen Ausschnitt unserer SOLUTIONS FOR YOUR SUCCESS und freuen uns auf Ihren Besuch und anregende Gespräche.
Ansprechpartner: LOG GmbH, Volker Reiser, Bereichsleiter Marketing & Vertrieb, Adenauerallee 131a, 53113 Bonn, Tel.: +49 228 4107-142, Fax: +49 228 4107-121, Mobil: +49 171 41 20 688, Mail: Volker.Reiser@LOGmbh.de, http://www.LOGmbh.de

Logic Instrument GmbH — Stand: Z 13

Logic Instrument bietet individuelle hochrobuste Hardwarelösungen im Bereich robuster Tablet PCs und Notebooks für anspruchsvolle Anwendungen im Militär- und Industriebereich.
Mit mehr als 25 Jahren Entwicklungs- und Markterfahrungen, Standorten in Frankreich, den Vereinigten Arabischen Emiraten, den USA und Deutschland, sowie einem engen, weltweiten Partnernetzwerk ist die Logic Instrument Gruppe ein solider und kompetenter Partner für Projekte mit oder ohne zusätzlichen Sonderlösungen. Nennenswert ist hier die Auslieferung von 7000 full-rugged Notebooks an Lockheed Martin, Zulieferer des US-Militärs.
Mehr Informationen finden Sie auf unserer Homepage: www.logic-instrument.com

Logica Deutschland GmbH & Co. KG — Stand: K 1

Ein Unternehmen der CGI-Gruppe
Logica, jetzt Teil von CGI, ist ein globaler Dienstleister für IT und Geschäftsprozesse, der mit 71.000 Mitarbeitern Business Consulting, Systemintegration und Outsourcing Services auf höchstem Niveau anbietet.
Logica unterhält enge Beziehungen zu großen nationalen und europäischen Unternehmen und Institutionen, darunter zu mehreren Verteidigungsministerien, zur NATO und der EU. Unsere Mitarbeiter sind auch in NATO Missionen, z.B. ISAF, vor Ort.
In Deutschland gehört Logica zu den Top-Ten der IT-Beratungs- und Systemintegrationsunternehmen. Bundeswehr und NATO zählen seit vielen Jahren zu unseren zufriedenen Kunden.
Auf der AFCEA präsentieren wir u.a. unsere Lösungen zu den nationalen und internationalen Führungsinformationssystemen und den Document Handling Systemen (DHS).

Luciad — Stand: K 3

Luciad ist der bevorzugte Zulieferer von COTS/MOTS Produkten für Lagedarstellung in missionskritischen C4ISR- und ATC/ATM-Systemen führender nationaler und internationaler Systemintegratoren.
Zu Luciads internationalem Kundenportfolio zählen AENA, Avitech, Belgocontrol, Boeing, Cassidian, DFS, EADS, ENAV, EUROCONTROL, FAA, Frequentis, IABG, Lockheed Martin, LVNL, NATO, NATS, NavCanada, NLR, Saab, SAIC, Sagem, STNA, Thales und Thales Raytheon Systems.
Luciad-Produkte ermöglichen die Entwicklung von hochleistungsfähigen, genauen und nachhaltigen Anwendungen. Außerdem zeichnen sich Luciad-Produkte durch die geringsten Gesamtkosten über die gesamte Nutzungsdauer hinweg und den garantiert längsten Anwendungslebenszyklus aus.
Für mehr Informationen besuchen Sie bitte www.luciad.com oder kontaktieren Sie uns unter Info@luciad.com

MAIBACH Industrie-Plastic GmbH — Stand: Z 8

Verpackungskonzepte für die Streitkräfte
Hochempfindliche Geräte und Baugruppen, Instrumente und Elektronikteile fordern tragbare Lösungen zum Schutz während des Einsatzes, der Lagerung und des Transports.
Die Firma MAIBACH Industrie-Plastic GmbH entwickelt, fertigt und vertreibt seit über 30 Jahren hochwertige wiederverwendbare Transport- und Lagerbehälter aus glasfaserverstärktem Kunststoff.
Mit individuell angepassten Polster- und Haltesystemen können die Behälter sowohl als Dichtbehälter mit 50 bis 100 mbar oder als Leichtbau-Container in modularer Sandwichbauweise geliefert werden. 19“ Transport- und Betriebsbehälter mit und ohne Klimatisierung für die Einrüstung von Truppengeräten runden das Lieferprogramm ab.
Die Behälter entsprechen den Festigungsanforderungen der Bundeswehr Norm VG 95613 und anderen militärischen Normen und bieten außergewöhnlichen Schutz vor Umwelteinflüssen (Schutzklasse IP 67).
Die Gütesicherung während des gesamten Fertigungsprozesses sowie Testdurchläufe und sorgfältige Endkontrollen entsprechen den Anforderungen nach AQAP.
www.maibach-ipg.de

Martin Yale International GmbH — Stand: P 3

Ein Pionier der Informationssicherung – intimus® CRYPTO
Was die Löschung vertraulicher Daten auf Endpoint-Medien angeht, verlassen sich unsere Kunden auf unsere weitreichende Erfahrung. Was vor mehr als 50 Jahren mit dem Reiswolf begonnen hat, ist heute eine Produktpalette für alle Belange der Informationssicherung. Der Name intimus®, lateinisch für den engsten Vertrauten, ist dabei Programm. Dank langjähriger Beziehungen zu Regierungen und Weltkonzernen sind wir mit unseren Forschungen und Entwicklungen den gesetzlichen Vorgaben und technischen Veränderungen immer einen Schritt voraus. Die jüngste Generation von Hochsicherheits-Aktenvernichtern ist seit Juli 2011 NSA-zugelassen (NSA/CSS-Spezifikation 02-01).
Leistungsspektrum:
- Aktenvernichter in allen gängigen Sicherheitsstufen
- Großanlagen für die Vernichtung von digitalen Datenträgern und Dokumenten
- Disintegratoren
- Degausser
- Data Grinder
- Secure Erase

MATERNA GmbH — Stand: T 2

Seit 1989 betreut Materna die IT-Strukturen zahlreicher Behörden und Organisationen mit Sicherheitsaufgaben. Ab 1995 kamen auch Projekte im Bereich der Äußeren Sicherheit hinzu. Zu unseren Schwerpunkten zählen Portal- und Content-Management-Lösungen, die Implementierung von ITIL®-basierten IT-Service-Management-Lösungen sowie User-Helpdesks, individuelle Fachverfahren, Integration von Produkten und die Implementierung von Microsoft Standardprodukten. Mit dem Kommunikationssystem EPOST 810 hat Materna ein IT-Verfahren entwickelt, das Nachrichten revisionssicher zwischen den Einrichtungen der Polizeien in den Bundesländern überträgt. Darüber hinaus realisiert Materna die Anbindung der Netze an den Mobilfunk.
Besonders hohe Sicherheitsstandards, langjährige Erfahrung sowie ein großer Mitarbeiterstamm sorgen dafür, dass die IT- und Telekommunikationslösungen auch sicherheitskritischen Anforderungen genügen. Durch die Mitarbeit am Führungsinformationssystem JASMIN wurde Materna in die Geheimschutzbetreuung aufgenommen und ist auch für NATO-Infrastrukturvorhaben zugelassen.

Microsoft Deutschland GmbH — Stand: F 9

Flexible Produktivität auf Basis der Microsoft-Plattform
Der Einsatz moderner Geräte und Software, Smartphones und Tablets auf Basis einer sicheren, zuverlässigen Plattform kann Motivation und Produktivität der Mitarbeiter steigern. Microsoft setzt mit der neuesten Software- und Gerätegeneration Maßstäbe für die Vereinbarkeit von Flexibilität und Sicherheit: von Windows Server 2012 über Windows 8 und neue Hardware wie Surface und Windows Phone 8 bis zum neuen Office. Außerdem demonstrieren wir spezielle Szenarios, wie auf dieser Basis die Zusammenarbeit National (z.B. bei HaFIS) und in multinationalen Koalitionen optimiert werden kann.
Wir freuen uns darauf, Ihnen die neuen Technologien auf der AFCEA persönlich zu demonstrieren!

Mittler Report Verlag GmbH — Stand: P 4

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 unabhängige Monatszeitschrift “Europäische Sicherheit & Technik”, die internationale Schwesterzeitschrift “European Security and Defence”, die Fachzeitschrift “MarineForum”, die Broschürenreihen “Wehrtechnischer Report” und “Sicherheitstechnischer Report” sowie die Informationsdienste “Mittler-Brief” und “Wehrwirtschaft”. Daneben gelten die jährlich stattfindende Sicherheitspolitische und Wehrtechnische Tagung in Bonn sowie die NATO LCM Conference in Brüssel als etablierte Foren für den qualifizierten Informationsaustausch unter Experten und Entscheidungsträgern.
www.mittler-report.de

ML Consulting Schulung, Service & Support GmbH — Stand: F 13

ML Consulting – Ihr Bildungsdienstleister Nr. 1!
Die ML Consulting ist seit beinahe 25 Jahren einer der führenden Bildungsanbieter. In großen Bildungsprojekten sind wir leistungsstarker Partner öffentlicher Auftraggeber und Unternehmern aller Branchen. Wir bieten unseren Kunden maßgeschneiderte Lösungen mit individueller, kontinuierlicher Betreuung.
Im Rahmen zahlreicher Ausbildungsprojekte wie den Kompetenzzentren IT (KIT), dem Projekt SASPF und bei der Realisierung von Fernausbildung sind wir langjähriger Partner der Bundeswehr.
Mit mehr als 350 festen und freien Mitarbeitern verfügen wir als mittelständisches Unternehmen über hervorragendes Know-how in den Bereichen ERP-Projekte, Informationssicherheit, Servicequalifizierung sowie IT- und Soft Skills-Training.
Kontakt: ML Consulting Schulung, Service & Support GmbH, Peter Brandt, Max-Planck-Str. 39, D-50858 Köln, Tel.: 02234-9203-112, Fax: 02234-9203-231, Homepage: www.mlconsulting.de, E-Mail: info@mlconsulting.de

Mönch Verlagsgesellschaft mbH — Stand: FR 1

Die Mönch Verlagsgruppe ist einer der weltweit führenden Verlage im Bereich der Verteidigungspublikationen. Zur Gruppe gehören mehrere Tochtergesellschaften im In- und Ausland z.B. in der Türkei und Italien. Darüber hinaus werden ca. 250 Buchtitel im Segment Verteidigung, Technologie, Politik und Geschichte seit vielen Jahren durch Bernard & Graefe vermarktet.
Unsere Zeitschriften sind:
- WEHRTECHNIK (DEUTSCH) Erscheinungsweise zweimonatlich
- MILITARY TECHNOLOGY (ENGLISCH) Erscheinungsweise monatlich
- NAVAL FORCES (ENGLISCH) Erscheinungsweise zweimonatlich
- TECNOLOGIA MILITAR (SPANISCH) Erscheinungsweise vierteljährlich
- RIVISTA ITALIANA DIFESA (ITALIENISCH) Erscheinungsweise monatlich
- SAVUNMA VE HAVACILIK (TÜRKISCH) Erscheinungsweise zweimonatlich
- AL DEFAIYA (ARABISCH) Erscheinungsweise zweimonatlich

Unsere Bücher:
- HANDBUCH DER BUNDESWEHR UND DER VERTEIDIGUNGSINDUSTRIE
- WEYERS FLOTTENTASCHENBUCH

und weitere
www.mpgbonn.de

Motorola Solutions — Stand: K 8

Motorola Solutions ist ein führender Anbieter von geschäfts- und sicherheitskritischen Kommunikationslösungen und -services für Unternehmen und Behörden. Durch wegweisende Innovationen in der Kommunikationstechnologie und sein umfassendes Portfolio nimmt Motorola Solutions weltweit eine Vorreiterrolle ein und versetzt Kunden in die Lage, in entscheidenden Momenten ihr Bestes zu geben.
Das Portfolio umfasst:
- Mobile Datenerfassung in Echtzeit
- Barcodescanner
- Tablets
- RFID (Radio Frequency Identification)
- Lizenzpflichtiger und kommerzieller Funk
- WLAN Infrastruktur für In- und Outdoor
- Professional Services: Netzwerksicherheit, Systemintegration sowie Remote Management von Netzen und Geräten

ND SatCom — Stand: Z 6

ND SatCom, ein Tochterunternehmen der Astrium, ist ein führender globaler Anbieter von satellitenbasierten Breitband-VSAT-Systemen, Netzwerklösungen für Fernseh- und Rundfunkübertragung, Regierungs- und Militärkommunikation und von Bodenstationen. Die innovativen Technologien werden weltweit von Regierungen, dem Militär sowie in den Bereichen Fernseh- und Rundfunkübertragung, der Telekommunikation und von Unternehmen eingesetzt. Mit mehr als 30 Jahren Erfahrung im Bereich Satellitenkommunikation ist das deutsche Unternehmen eine zuverlässige Quelle für umfassende und sichere Lösungen, die schlüsselfertige und maßgeschneiderte Systeme beinhalten. ND SatCom ist weltweit durch regionale Vertriebs- und Servicebüros vertreten.

ORACLE Deutschland — Stand: T 5

Oracle entwickelt Hardware und Software, die für den Einsatz in der Cloud, in mobilen Lösungen und im Rechenzentrum optimal aufeinander abgestimmt sind. 380.000 Kunden jeder Größe und Branche setzen in 145 Ländern der Welt Produkte und Lösungen von Oracle ein. Im Fiskaljahr 2012, das zum 31. Mai 2012 endete, erzielte Oracle weltweit einen Umsatz von 37,1 Milliarden US-Dollar. Oracle beschäftigt weltweit 108.000 Mitarbeiter, darunter 32.000 Entwickler, 18.000 Support-Mitarbeiter und 17.000 Consulting-Experten.
Die ORACLE Deutschland B.V. & Co. KG hat ihren Hauptsitz in München. Mehr Informationen unter www.oracle.com
Mehr als 100 Kunden im Verteidigungssektor nutzen heute schon commercial off-the-shelf (COTS) Lösungen von Oracle.

Overwatch Systems Ltd. — Stand: P 5

Overwatch®, a strategic business of Textron Systems Advanced Systems, an operating unit of Textron Systems, is an industry leader in imagery analysis and geospatial intelligence solutions. Our flagship software products, ELT®, GIV® and RemoteView™, provide high-powered image exploitation and mapping for tactical users. Defense and intelligence communities around the world trust Overwatch's software for its positioning accuracy and efficient workflows.
Overwatch understands automatic feature extraction, with proven results through our Feature Analyst™ and LIDAR Analyst® software extensions for ArcGIS®. These products rapidly and accurately collect vector feature data from high-resolution satellite imagery and airborne LIDAR data.
See www.overwatch.com for more information.

Panasonic Computer Product Solutions — Stand: Z 4

In enger Zusammenarbeit mit seinen Kunden entwickelt Panasonic Computer Product Solutions energieeffiziente, widerstandsfähige Mobile Computing Lösungen. Das Produktspektrum der Marken TOUGHBOOK und TOUGHPAD reicht von robusten Outdoor-Notebooks und Convertibles über Business-Laptops bis hin zu Tablet-PCs. Diverse Dienstleistungen und Zubehörartikel wie KFZ-Halterungen, Trage-, Halte- und Body-Mounting-Lösungen ergänzen das Portfolio.
Höchsten Ansprüchen an Mobilität, Rechenleistung und Widerstandsfähigkeit werden die Geräte durch lange Akkulaufzeiten, geringes Gewicht, leistungsstarke und energieeffiziente Komponenten sowie besondere Schutzkonstruktionen gerecht.
Wir zeigen Ihnen dieses Jahr auf der Messe die aktuellsten Mobile Computing Geräte von Panasonic Toughbook und Toughpad live vor Ort.
Darunter die kürzlich gelaunchten Modelle der neuen Toughpad Familie:
- Toughpad FZ-G1 - 10,1" Windows 8 Tablet
- Toughpad FZ-A1 - 10,1" Android Tablet
- Toughpad JT-B1 - 7" Android Tablet

Weitere Informationen finden Sie unter: www.toughbook.de

Peli Products — Stand: B 1

Peli Products is the Europe, Middle East and Africa Headquarters of Pelican Products, Inc., the global leader in design and manufacture of both high-performance case solutions and advanced portable lighting systems. Our products are used by professionals in the most demanding markets including firefighters, police, defense / military, aerospace, entertainment, industrial and consumer. Peli products are designed and built to last a lifetime. The company´s global footprint consists of 22 offices and 6 manufacturing facilities across the globe. For more information visit www.peli.com
Germany: Peli Products Germany GmbH, Graf-Adolf-Platz 15, 40213 Düsseldorf, Germany, T. +49 21188242401, F. +49 21188242200
EMEA headquarters: Peli Products, S.L.U., C/ Provença, 388 Planta 7, 08025 Barcelona, Spain, T. +34 93 467 49 99, F. +34 93 487 73 93

PROCITEC GmbH — Stand: P 9

Die PROCITEC GmbH ist ein weltweit agierendes hoch spezialisiertes Software-Unternehmen im Bereich Nachrichtentechnik und Informationstechnologie.
Wir konzipieren, entwickeln und implementieren Softwareprodukte und Systemlösungen zur Erfassung und Aufklärung von:
- HF/VHF/UHF-Funk
- Satellitenkommunikation
- Laserkommunikation
- Richtfunk

Unsere Lösungen sind offene, skalierbare und erweiterbare Softwaresysteme. Von der manuellen Analyse bis zur vollautomatischen Inhaltsgewinnung decken wir die wichtigsten Schritte der Signalverarbeitung ab:
- Signaldetektion und -klassifikation
- Demodulation und Dekodierung
- Signalaufzeichnung
- Signalanalyse
- Sprachverarbeitung

Wir sind langjähriger Partner der deutschen Sicherheitsbehörden: von der Idee über die Definition bis hin zum erfolgreichen Roll-Out komplexer Systeme.
Kontakt: PROCITEC GmbH, Rastatter Str. 41, 75179 Pforzheim, Tel.: +49 7231/15561-0, E-Mail: o.themann@procitec.de, www.procitec.de

promegis — Stand: P 5

Als Spezialist für Geoinformatik, digitale Bildverarbeitung und IT-Servicedienstleistungen entwickelt unser Unternehmen Anwendungen für Geoinformationssysteme, Image Analysis Produkte sowie fachspezifische Systemlösungen für die Bereiche öffentliche Verwaltung, Behörden und Organisationen mit Sicherheitsaufgaben (BOS), Verteidigung, Wirtschaft und Industrie. 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 Overwatch Systems bieten wir Ihnen die volle Bandbreite der High-End GIS und Image Analysis Lösungen.
Kontakt: promegis Gesellschaft für Geoinformationssysteme mbH, Breslauer Straße 31, D-49324 Melle, Tel. +49 (0) 5422 9629 0, Fax: +49 (0) 5422 9629 20, info@promegis.de, www.promegis.de

PWA Electronic Service- und Vertriebs- GmbH — Stand: Z 4

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 Products Europe auf eine Erfahrung von 17 Jahren zurück. Wir bieten für die Panasonic Toughbooks 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.
Auf der diesjährigen AFCEA zeigen wir Ihnen die aktuellsten Mobile Computing Geräte von Panasonic Toughbook und Toughpad live vor Ort.
Darunter auch die kürzlich gelaunchten Modelle der neuen Toughpad Familie:
- Toughpad FZ-G1 - 10,1" Windows 8 Tablet
- Toughpad FZ-A1 - 10,1" Android Tablet
- Toughpad JT-B1 - 7" Android Tablet.

Weitere Informationen finden Sie auf unserer Homepage www.pwa-electronic.de.

RES Software — Stand: B 4

RES Software eröffnet Unternehmen völlig neue Möglichkeiten, ihre immer komplexer und hybrider werdenden Desktop-Infrastrukturen zu verwalten, zu automatisieren und abzusichern – und dabei Aufwand und Kosten zu sparen. Mit den Lösungen von RES Software können IT-Experten aktuelle Herausforderungen wie die zunehmende Mobilität und Flexibilität der Anwender,

Konsumerisierung der IT, Bring-Your-Own-Device oder Cloud-Technologien einfach meistern. Die patentierten Technologien von RES Software befinden sich weltweit im Einsatz und schließen erstklassigen Kundensupport mit ein.
Weitere Informationen auf www.ressoftware.com.

Riedel Communications GmbH & Co. KG Stand: P 1

Die Riedel Communications GmbH & Co. KG entwickelt, fertigt und vertreibt zukunftsweisende Echtzeitnetzwerke für Video, Audio, Daten und Kommunikation in einsatzkritischen Anwendungen im Militär-, Sicherheits-, Industrie-, Event- und Rundfunkbereich. Das Portfolio umfasst analoge und digitale (TETRA) Funksysteme, digitale drahtlose und drahtgebundene Intercom-Systeme sowie glasfaserbasierte Mediennetzwerke für den Aufbau integrierter Signalinfrastrukturen. Zudem betreibt Riedel ein globales MPLS-Datennetz für hochsichere Datenverbindungen. Die Riedel-Gruppe hat ihren Hauptsitz in Wuppertal und beschäftigt an elf Standorten in Europa, Australien, Asien und Amerika über 350 Mitarbeiter.

Rockwell Collins Deutschland GmbH Stand: Z 2

Rockwell Collins Deutschland, mit Firmensitz in Heidelberg, beschäftigt über 500 Mitarbeiter. Unsere Kernkompetenzen, aufbauend auf eine 50-jährige 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 MilDef GmbH Stand: Z 7

roda MilDef GmbH ist spezialisiert auf Entwicklung, Herstellung und Vertrieb mobiler robuster Rechner. roda hält mehrere Rahmenvertrage mit der Bundeswehr. (z.B. R6645 und R6659)
Die mobilen Rechner zeichnen sich aus durch:

- extreme Robustheit
- geringe EMV-Abstrahlung
- variable Schnittstellen
- modularem Aufbau
- Integrationsvielfalt
- optimale Konfigurierbarkeit
- Umfänglichen MIL-STD – Zertifikaten
- Umfangreicher Dokumentation

NEU bei roda MilDef GmbH:

- Das voll gehärtete Notebook Rocky RS11 mit 14“ Display und geringem Gewicht von nur 2.2 Kg und vollem IP65 Schutz
- Die Notebookserie Rocky und Tablet PC-Serie Panther mit neusten Prozessoren und vollem IP65 Schutz

Kontakt: roda MilDef GmbH, Landstr. 6, 77839 Lichtenau, Tel.: +49 (0 72 27) / 95 79 - 0, Fax: +49 (0 72 27) / 95 79 - 20, E-Mail: mail@roda-mildef.com, Internet: www.roda-mildef.com

Rohde & Schwarz Stand: G 18

Die Rohde & Schwarz GmbH & Co. KG steht seit fast 80 Jahren für Qualität und Präzision in den Bereichen Messtechnik, Rundfunk, sichere Kommunikation sowie Überwachungs- und Ortungstechnik.
Das Unternehmen unterstützt Hersteller in Entwicklung und Produktion elektronischer Geräte mit **Messtechnik** überall dort, wo es gilt, Signale zu generieren, zu analysieren, zu vermessen oder das Spektrum zu analysieren. Im Bereich Aerospace & Defense bündelt der Konzern seine Kompetenz mit Messtechnik-Lösungen für Richtfunkstrecken, Radarsysteme und Satellitenkommunikation.
Rohde & Schwarz liefert interoperable und leistungsfähige **Kommunikationssysteme,** die im Einsatz- oder Krisenfall die zeitnahe Koordination ziviler, behördlicher und militärischer Einsatzkräfte gewährleistet. Durch moderne Verschlüsselungsverfahren erfüllen die Lösungen des Unternehmens höchste Sicherheitsstandards. Für Unternehmen, Regierungsstellen, Bundeswehr und NATO entwickelt und produziert die Rohde & Schwarz SIT GmbH zudem **Kryptoprodukte** und -systeme.
Darüber hinaus entwickelt und produziert Rohde & Schwarz stationäre sowie mobile Systeme zur **Erfassung, Ortung** und **Analyse** von **Funkkommunikationssignalen.**

rola Security Solutions Gmbh Stand: G 16

rola Security Solutions GmbH mit Sitz in Oberhausen zählt seit fast 30 Jahren zu den bedeutendsten Anbietern von IT-Lösungen im Bereich der Inneren und Äußeren Sicherheit sowie der nachrichtendienstlichen Aufklärung. Mit dem Software-Framework **rs*Frame*®** hat sich rola auf Lösungen für Informationsmanagement, vernetzte Fallbearbeitung sowie Auswertung und Analyse spezialisiert.
In der Variante **rs*IntCent*®** wird die Software im militärischen Umfeld für Auswertung und Lagefeststellung genutzt. Schwerpunkte bilden Informationszusammenführung und Informationserschließung sowie die Erzeugung dynamischer Lagebilder und die ebenengerechte Präsentation.
www.rola.com

Romold GmbH Stand: B 2

ROMOLD – IHR PARTNER IM INNOVATIVEN SCHACHTBAU
NUTZEN SIE DAS KNOW-HOW DES MARKTFÜHRERS.
ROMOLD – Wenn`s um Schächte geht: Die ROMOLD GmbH ist europäischer Marktführer im Bereich Kunststoffschächte. Zwanzig Jahre Erfahrung sowie die Spezialisierung auf industriell gefertigte PE/PP-Schächte spiegeln sich in Qualität und Vielfalt des Produktsortiments.
ROMOLD ist Ihr Spezialist für die Herstellung markt- und bedarfsgerechter Kunststoffschächte. Als europäischer Pionier für industriell gefertigte Kunststoffschächte (über 1 Mio. verkaufte Schachtbauteile), lässt ROMOLD das Know-How aus 20 Jahren in die Entwicklung seiner Produkte einfließen.
Das Programm:
Umfangreichstes Kunststoffschacht-Programm für

- Ver- und Entsorgung, Drainage
- Druckentwässerung
- Elektro- und Telekommunikation

und patentierte ***Activ*-Kohlefilter**

- zur H2S-Eliminierung

Das Unternehmen:

- Mit der Erfahrung des Marktführers
- Mit hohem Qualitätsanspruch als ständige Herausforderung
- Mit laufenden Innovationen und Weiterentwicklungen
- Mit qualifizierten, erfahrenen und engagierten Mitarbeitern
- Mit ausgeprägtem Serviceverständnis zum Vorteil der Kunden

Ihre Vorteile:

- Ökonomische Systeme durch effiziente, technisch ausgereifte Lösungen
- Nachhaltige Kostenreduktion durch korrosionsfreie, wartungsarme Anlagen
- Optimierter Zeitaufwand durch flexible Standard- und Sonderlösungen
- Verfügbare, qualifizierte Beratung von der Planung bis zur Ausführung

Saab International Deutschland GmbH Stand: Z 1b

Saab beliefert den Weltmarkt mit weltweit führenden Produkten, Dienstleistungen und Lösungen, von militärischer Verteidigung bis zur zivilen Sicherheit. Ihr Verlangen nach Sicherheit ist die ultimativ treibende Kraft für unser Geschäft. Mit Blick über den Horizont hinaus geben wir unser Bestmöglichstes, um auf das Unerwartete und sogar Unbekannte vorzubereiten. Wir bemühen uns das Morgen vorherzusehen – “DIE ZUKUNFT SCHON HEUTE”.
Saab verfügt über umfangreiche Erfahrungen im Bereich von Verteidigungssystemen, Schutz der Streitkräfte und ziviler Sicherheitstechnologie.
Kontakt: Saab International Deutschland GmbH, Hochkreuzallee 1, 53175 Bonn. Telefon: 0228 3675 60, Telefax: 0228 3675 620, saab.deutschland@saabgroup.com, www.saabgroup.com

SAP Deutschland AG & Co. KG Stand: G 12

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.
Auf der diesjährigen AFCEA zeigen wir neben den streitkräftespezifischen Lösungen auf Basis der SAP Business Suite auch unser mobiles Lösungsportfolio, das wir ständig erweitern: Mit SAP Afaria® bieten wir unseren Kunden eine mobile Lösungsplattform, die die sichere Verwaltung von Endgeräten ermöglicht. Unsere mobilen Applikationen für Instandhaltung liefern Technikern stets aktuelle Informationen vor Ort – auf jedem Endgerät.
Analytische Anwendungen stehen mit SAP HANA® sehr performant zur Verfügung. Der nächste, logische Schritt ist die Bereitstellung der SAP Business Suite auf der In-Memory-Technologie, um so die Geschäftsprozesse ganzheitlich zu beschleunigen.
Wir freuen uns auf Ihren Besuch am Stand G 12!
Weitere Informationen finden Sie auf unserer Homepage unter www.sap.de/defense.

Schnoor Industrieelektronik GmbH & Co. KG Stand: G 5

Schnoor Industrieelektronik ist ein führendes Unternehmen auf dem Gebiet der Funktechnik in Deutschland. Seit 1990 werden individuelle Funk- und Kommunikationslösungen für nationale und internationale Kunden aus namhaften Behörden und Unternehmen entwickelt.
Schwerpunkte sind: Öffentliche Sicherheit (Polizei, Feuerwehr, Bergwacht), Öffentlicher Verkehr (Zugfunk, Verkehrsleitung), Gebäudesicherheit (Industrie, Behörden), Maritime Sicherheit (Seefunk – SEACOM, SARCOM, NIF, NAVTEX).
Von der Planung und Projektierung über die Entwicklung kundenspezifischer Hard- und Software bis hin zu Fertigung, Inbetriebnahme und Support wird alles aus einer Hand geliefert.
Unsere Kompetenzbereiche:

- VoiP-Leitstellentechnik (Seenotrettung, Bergwacht, Küstenfunk)
- Funksysteme analog und digital (TETRA)
- Fahrzeug-Funkanlagen
- Universelle Bediengeräte (seewasserfest, handschuhbedienbar)

Weitere Informationen: www.Schnoor-INS.com

secunet Security Networks AG — Stand: G 15

secunet ist einer der führenden deutschen Anbieter für anspruchsvolle IT-Sicherheit. Mehr als 280 Experten konzentrieren sich auf Themen wie Kryptographie, E-Government, Business Security und Automotive Security und entwickeln dafür innovative Produkte sowie hochsichere und vertrauenswürdige Lösungen. Zu den mehr als 500 nationalen und internationalen Kunden gehören viele DAX-Unternehmen sowie zahlreiche Behörden und Organisationen. Seit 2004 ist secunet IT-Sicherheitspartner der Bundesrepublik Deutschland.
Unsere Ausstellungsschwerpunkte:

- Desktop basierte SINA Workstation H Zone 1
- Gehärtete Notebook basierte SINA Workstation H R RK9
- SINA L3 Box H 200M
- Gehärtete SINA L3 Box H R 200M 27A
- SINA Workflow

Ergänzende Informationen: www.secunet.com

Securiton AG — Stand: T 6

Die Securiton AG steht seit ihrer Gründung 1948 ganz im Dienst der technischen Sicherheit. Mit ihrem Pioniergeist und Weitblick hat sie sich in den letzten 50 Jahren zu einem bekannten Spezialisten für anspruchsvolle Sicherheit entwickelt. Die langjährigen Partnerschaften mit Kunden, Beratern, Instanzen und Auflagebehörden sind ein Vertrauensbeweis für umfassendes Know-how und Qualität. Heute plant, errichtet und wartet die Securiton Anlagen für Hochsicherheitsbereiche (Militär, Polizei und Justiz), Verwaltungen. Handels- und Industriebetriebe:

- Mobiler und permanenter Objektschutz
- Sensor- und Videoüberwachung
- Zutrittskontrolle und Zeiterfassung
- Einbruch-/Überfallmeldung
- Brandmeldung
- Personenschutz
- Gesamtsysteme

Securiton AG, Alarm and Security Systems, Alpenstrasse 20, CH-3052 Zollikofen/Bern, Phone: +41 31 910 11 22, Fax: +41 31 910 16 16, www.securiton.ch
Securiton GmbH, Alarm and Security Systems, Von-Drais-Strasse 33, D-77855 Achern, Phone: +49 7841 6223 0, Fax: +49 7841 6223 10, www.securiton.de

Secusmart — Stand: Z 9

Auf der diesjährigen AFCEA Fachausstellung präsentiert Secusmart die mobile Hochsicherheitslösung "SecuSUITE for BlackBerry 10" im Außenzelt, Stand Z9. Die hardware-basierte Krypto-Lösung SecuSUITE kombiniert den wirkungsvollen Abhörschutz durch die Secusmart Security Card mit dem kompromisslosen Smartphone-Komfort des BlackBerry 10: Die BlackBerry Balance Technologie trennt sensible Informationen zuverlässig von privaten Inhalten. Die Secusmart Security Card gewährleistet auf dem handelsüblichen BlackBerry im Geschäftsbereich erstmals die sichere Verschlüsselung der gespeicherten Informationen, der Sprache, der Textnachrichten, und ermöglicht Secure Browsing, den sicheren Zugriff auf das Intranet sowie auf das Internet über einen definierten, sicheren Zugangspunkt. Damit erfüllt die Lösung die hohen Sicherheitsanforderungen deutscher Behörden, ohne Abstriche beim Nutzererlebnis zu machen.

SELEX Communications GmbH — Stand: G 4

Die SELEX Communications entwickelt, fertigt und integriert zuverlässige Kommunikationslösungen für Industrie, Sicherheitsbehörden und Militär. Durch die Einbindung modernster Informations- und Kommunikationstechnologien eröffnen die Lösungen von SELEX Communications dem Nutzer neue Anwendungsmöglichkeiten, die im Rahmen einer modernen militärischen Operationsführung notwendig sind. Hierbei folgen diese Lösungen den netzwerkübergreifenden, interoperationellen Forderungen nach Mobilität und Verfügbarkeit, basierend auf sicheren IP-Verbindungen.
Neben eingeführten Systemen wie Richtfunk, PRR, Glasfasertechnik und HF/VHF/UHF-Funk bietet die SELEX Communications auch neue Gerätefamilien, wie Breitband IP Radios, SDR-Systeme, Multiservice-Anwendungen für Netzwerke sowie mobile Arbeitsplatzsysteme (verlegefähige Accessnetze) an.
Weitere Informationen finden Sie unter www.selexcom.de
Kontakt: SELEX Communications GmbH, 71522 Backnang, Homepage: www.selexcom.de, Bernd Broghammer, Email: bernd.broghammer@selex-es.com, Tel.: +49 (0) 7191 378-0, Fax: +49 (0) 7191 378-500

Siemens Industry Sector — Stand: G 15

Als Hersteller abhörsicherer PCs ist Siemens seit vielen Jahren erfolgreich im Tempest-Markt unter dem Markennamen SITEMP tätig.
SITEMP-Geräte werden in Deutschland entwickelt, gefertigt und zertifiziert. Siemens verfügt als eines von wenigen Unternehmen weltweit über eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) autorisierte Prüfstelle für die uneingeschränkte Durchführung von Zulassungs- und Serienvermessungen nach NATO-Norm SDIP.
Für unsere Kunden entwickeln wir kundenspezifische Tempest-Lösungen nach SDIP 27 Class A und Zone 1 / SDIP 27 Class B, wie z.B. für unseren langjährigen Partner secunet.
Ergänzende Informationen: www.siemens.com/sitemp

SRH SAP Competence Center — Stand: T 4

Als Bildungs- und Schulungspartner der SAP AG qualifizieren wir seit über 18 Jahren erfolgreich SAP-Berater, Anwender und Entwickler. In mobilen Studios schulen wir national und international auf original SAP®ERP Online-Trainingssystemen mit den SAP®ERP Trainingsunterlagen. Bei unseren SAP®ERP Seminaren kommen nur SAP-zertifizierte Trainer zum Einsatz. Für Firmenkunden entwickeln wir kundenindividuelle Schulungskonzepte.
Als Partner der Bundeswehr schulen wir Soldaten/Innen vom SAP Key User bis zum zertifizierten SAP Berater und Entwickler.
Profitieren Sie von unserer Erfahrung – erhöhen sie Ihre beruflichen Chancen durch qualifizierte Weiterbildung mit modernster Technik.
Kontaktdaten: SRH SAP Competence Center, Herr Detlev Drechsler, R/3, 4-5, 68161 Mannheim, 06221-88-3740

steep GmbH — Stand: G 11

Die steep GmbH ist ein mittelständisches Dienstleistungsunternehmen mit Hauptsitz in Bonn und mehr als 30 weiteren Standorten in Deutschland. Das Dienstleistungsspektrum setzt sich aus den einzelnen Bereichen von "steep" zusammen: **S**ervice, **T**raining, **E**ngineering, **E**nergy und **P**roducts.
Die Kompetenzen der Bereiche, die von prozessoptimierender Beratung und IT-Unterstützung über Einzelleistungen wie Systemintegration, Schulung und Dokumentation bis hin zur Gestaltung kompletter Dienstleistungsfelder reichen, bilden gemeinsam ein einzigartiges Fundament für die Entwicklung maßgeschneiderter, kundenspezifischer Lösungsmodelle.
In den letzten Jahren fand ergänzend eine Entwicklung im Produktgeschäft statt. Entlang unserer Kernkompetenzen werden nach Bedarf hochwertige und innovative Produkte in die kundenorientierten Dienstleistungslösungen integriert.
Wir sehen uns als Partner der Bundeswehr und richten unsere Kompetenzen an den Anforderungen und einsatzbezogenen Bedürfnissen der Bundeswehr aus.

Steria Mummert Consulting AG — Stand: F11

Mit mehr als 35 Jahren Erfahrung in der Bereitstellung von Lösungen zählt Steria Mummert Consulting zu den zehn führenden Business Transformation Partnern im deutschen Markt. Wir verfügen über umfassende Fachexpertise und haben viele ehemalige und erfahrene Soldaten sowie zivile Mitarbeiter in unserem Team, die sicherstellen, dass wir die Anliegen unserer Kunden aus dem Verteidigungs- und Sicherheitssektor bestens verstehen.
In diesem Jahr lautet das Thema IT-Services – Enabler in multinationalen Koalitionen.
Unsere aktuellen Themenschwerpunkte lauten:

- Erstellung Technischer Dokumentation (IETD)
- Einsatz von biometrischen Verfahren für die Zugangskontrolle
- IT-Servicemanagement (ITSM) auf Grundlage der Information Technology Infrastructure Library (ITIL)
- Risikomanagement und IT-Sicherheit

Auf der diesjährigen AFCEA wird Steria Mummert Consulting von Office für Technische Dokumentationen GmbH (www.otd-online.de), spezialisiert auf die Erstellung technischer Dokumentationen und von Cross Match Technologies (www.crossmatch.com), qualifiziert für den Einsatz von biometrischen Verfahren, begleitet.
Steria Mummert Consulting AG, Hans-Henny-Jahnn-Weg 29, D-22085 Hamburg, Homepage: www.steria-mummert.de, Ansprechpartner: Holger Grube, Senior Manager Public Services, Tel.: +49 40 22703-0, Fax: +49 40 22703-3567, E-Mail: public-services@steria-mummert.de

Systematic — Stand: Z 10

Systematic is an independent software company that provides scalable software products, services and projects for defence forces, security organizations and systems integrators, specialising in interoperable command and control (C2) solutions. We are redefining the C2 arena from bespoke systems to COTS products with our unique C2 software, **SitaWare** – a fully integrated product suite from Joint HQ to the commander on the move. It provides a core C2 capability, based on international standards, that can be extended through its open architecture. It can be tailored to meet national requirements whilst maintaining the ability to be interoperable with joint/coalition partners.

systerra computer GmbH — Stand: Z 11

systerra computer GmbH ist Anbieter von Langzeit-verfügbaren, schock-/vibrationsfesten und MIL-konformen Rechner-, Speicher- und Netzwerkplattformen für den erweiterten Betriebstemperaturbereich.
Board- und Komplettsystem-Lösungen von systerra bewähren sich in zahlreichen mobilen und stationären Verteidigungs-Anwendungen am Boden, in der Luft und auf See.
Das Spektrum gehärteter COTS-Rechner basiert auf anerkannten Standards wie VME, VXI, VPX, NanoATR, PC/104, CompactPCI, ATCA, MicroTCA und 19"-Technologie sowie Windows-, Linux und Echtzeit-Betriebssystemen.
Unsere robusten Ethernet Switches, Router und Marine Panel PCs sind u.a. nach DNV und GL zertifiziert.
Neben Standard-Produkten namhafter Hersteller wie Themis Computer und Moxa bietet systerra computer applikationsspezifische Sonderentwicklungen/Systemlösungen, in enger Zusammenarbeit mit Kunden und Partnern entwickelt.
Weitere Informationen: www.systerra.de

TASys GmbH

Stand: T 4

Die TASys GmbH ist Ihr Dienstleister für SAP Beratung, SAP Training und arbeitsplatzspezifische Aus- und Weiterbildung. Wir erstellen Lerninhalte, Simulationen, Dokumentationen, Handbücher und E-Learning Einheiten.

SAP IS-DFPS, SAP A&D, SASPF

Unsere Mitarbeiter begleiten im Projekt SASPF die Einführung industrieller Standardsoftware bei der Bundeswehr.

Wir setzen dabei auf das Know-how ehemaliger Zeitsoldaten und die langjährige Fachexpertise unserer Trainer und Berater.

Unsere umfangreichen Kenntnisse in allen SAP-Modulen und Erfahrung mit den entsprechenden Strukturen, Prozessen und Aufgaben in Streitkräften und Industrie garantieren eine nachhaltige Ausbildung.

Kontakt: TASys GmbH, Harald Müller-Rauch, Höhscheider Weg 21, 42799 Leichlingen, Telefon: 02174 - 89 22 09, harald.mueller-rauch@tasys-it.de, www.TASys-it.de

TELEFUNKEN RACOMS

Stand: F 2

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 liegt nicht nur bei der Herstellung von hochperformanter Hardware, sondern auch im Bereich der Softwareentwicklung zur Integration verschiedenartigster Funkübertragungsprotokolle.

Neben dem Kerngeschäft der Funkkommunikation baut TELEFUNKEN RACOMS seine Geschäftstätigkeiten im Verteidigungsbereich (C4, Aufklärung, Schutz, Wirkung) spürbar aus 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

Thales Deutschland

Stand: Z 5

Thales Deutschland verfügt über eine hohe Produkt-, System- und Lösungskompetenz und ein umfangreiches Portfolio. Die Produkt-, System- und Lösungshighlights reichen von der Sensorik, insbesondere land- und seegestützten Überwachungsradaren, der Optronik sowie kombinierten Sensorsystemen über abhörsichere Multi-band-Truppenfunksysteme bis hin zu komplexen Führungsinformations- und Aufklärungssystemen. Zum Angebot gehören auch taktische Funk- und Führungssysteme für den hochmobilen Einsatz, Software-defined Radio, Kommunikations- und Leitzentralen sowie Feldlagerschutz. Den Schwerpunkt der Marineaktivitäten in Deutschland bilden Über- und Unterwassertechnologien. Bei Führungs- und Waffeneinsatzsystemen für Seestreitkräfte entwickelt Thales sowohl Netzinfrastrukturen als auch Software. Kommunikations- und Ausbildungssysteme, taktische Datenlinks sowie Systeme zur taktischen Aufklärung und Datenauswertung gehören ebenfalls zum Leistungsspektrum. www.thalesgroup.com/germany

Trend Micro Incorporated

Stand: B 4

Trend Micro Incorporated, ein weltweit führender Anbieter von Cloud-Sicherheitslösungen, schafft mit Internet Content Security und Bedrohungsbewältigung eine sichere Welt zum Austausch digitaler Daten für Unternehmen und Privatanwender. Als Pionier im Bereich Server-Sicherheitslösungen mit über 20 Jahren Erfahrung bieten wir Client-, Server- und Cloud-basierte Sicherheitslösungen der Spitzenklasse, die die Anforderungen unserer Kunden und Partner erfüllen. Unsere Lösungen wehren Bedrohungen schneller ab und schützen Daten in physischen, virtualisierten und webbasierten Umgebungen. Unterstützt durch das Trend Micro™ Smart Protection Network™ – unsere branchenführende, webbasierte Sicherheitstechnologie – und über 1.000 Experten weltweit stoppen unsere Produkte und Services Bedrohungen dort, wo sie entstehen: im Internet. Weitere Informationen finden Sie unter www.trendmicro.com.

T-Systems International GmbH

Stand: F 4

Flexible Informations- und Kommunikationstechnik für die Bundeswehr.

Mit einer weltumspannenden Infrastruktur aus Rechenzentren und Netzen betreibt T-Systems die Informations- und Kommunikationstechnik (engl. kurz 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.

T-Systems International GmbH, Am Propsthof 51, 53121 Bonn, Tel.: 0228/181-38 201, Mail: verteidigung@t-systems.com, Internet: www.t-systems.de

UWS Business Solutions GmbH

Stand: P 8

Die UWS Business Solutions GmbH (bis 2011 als Schneider System GmbH) ist ein unabhängiges, inhabergeführtes, mittelständisches Beratungs- und Dienstleistungsunternehmen und unterstützt die Bundeswehr partnerschaftlich seit über 20 Jahren. Wesentliche Kompetenzen liegen in den Feldern Organisationsberatung, IT-Lösungen und Qualifizierung.

Schlagworte zu UWS-Dienstleistungen sind:

- Standards wie ISO 9001, ITIL, IT-Service Management, PRINCE2
- Methoden wie eEPK, BPMN, NAV, IT-Architekturen, Projektmanagement
- Verfahren wie Lean Management, CPM, logistische DV-Verfahren
- Techniken und ganzheitliche Ansätze wie ECM, Webportale, BPM Tools
- Innovative Lösungen mit Wiki, Blogs, Social Networking, semantische Netze
- Technologien wie Nautilus, PHP, App-, MS- und Notes-Entwicklungen
- Bw-Projekte im Bereich Organisation, Lern- und Wissensmanagement

www.uw-s.com

VEGA Deutschland GmbH

Stand: F 3

VEGA Deutschland ist ein führendes Technologie- und IT-Services Unternehmen. Mit über 200 Mitarbeitern und über 30 Jahren Erfahrung in der Realisierung komplexer IT-Projekte unterstützt VEGA ihre Kunden im Verteidigungsbereich bei der Gestaltung und Durchführung von Service-Prozessen in den Bereichen Personalwesen und Infrastruktur.

In diesem Jahr liegt unser Fokus für die AFCEA auf dem Service **Bewerberakten mit SAP Records / Folders Management.**

Umfangreiches Expertenwissen, Prozess-Know-how und hohe Umsetzungskompetenz versetzen uns in die Lage, mit innovativen Lösungen nachhaltig die Leistungsfähigkeit und Zielerreichung unserer Kunden zu optimieren.

Kontakt: VEGA Deutschland GmbH, Industriestr. 161, 50999 Köln, Tel: +49 (0)2236 748-0, E-Mail: info@vega-deutschland.de, www.vega-deutschland.de

ZVEI-Fachverband Sicherheit

Stand: E 3

Vernetzte Sicherheit ist ohne den Einsatz vorhandener und neuer Sicherheitstechnologien nicht denkbar. Hier liegt die innovative Kraft, die erforderlich ist, um innere und äußere Sicherheit ständig zu optimieren und den Bedrohungen von außen sowie den asymmetrischen Bedrohungen durch Terroristen und sonstigen Gefahren für die innere öffentliche Sicherheit mit intelligenter und innovativer Wehr-, Einsatz- und Sicherheitstechnik zu begegnen.

Der **Fachverband Sicherheit** im ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e.V. – bündelt die vielseitigen Kompetenzen der Branche mit den drei Leitmärkte SAFETY (Schutz von Menschenleben, technische Sicherheit von Anlagen und Gebäuden), SECURITY (Schutz von Infrastruktur wie Flughäfen und Energieversorgung, Informationstechnik und Kommunikation sowie Bevölkerungs- und Katastrophenschutz) und DEFENCE (äußere Sicherheit) unter einem Dach.

Nur mit einer Strategie der Vernetzten Sicherheit, bei der politische Institutionen, Konzepte, Strategien und Instrumente der Sicherheitspolitik und des nationalstaatlichen und auch multinationalen Handelns ressortübergreifend abgestimmt, kohärent und koordiniert umgesetzt, wirkungsorientiert und nach Möglichkeit auch präventiv angelegt sind, kann Sicherheit und der Schutz der Gesellschaft in einer zunehmend vernetzten, globalisierten Welt verbessert werden. Sicherheit entwickelt sich vor diesem Hintergrund zu einem maßgeblichen wirtschaftlichen Standortfaktor.

Kontakt: ZVEI-Fachverband Sicherheit, Peter Krapp, Lyoner Str. 9, 60528 Frankfurt/M, Tel.: 069 6302-272, E-Mail: krapp@zvei.org

BSC·Berlin Security Conference

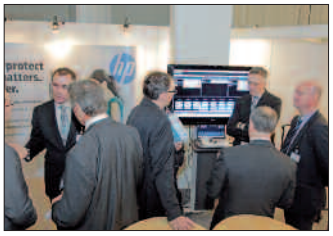
12th Congress on European Security and Defence

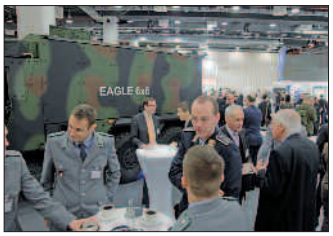
Impressionen 2012



















Weitere Fotos und Informationen zum letzten Kongress finden Sie unter

www.euro-defence.eu

BSC · Berlin Security Conference

12th Congress on European Security and Defence

Post-Afghanistan – neue Anforderungen – neue Chancen für Politik, Militär und Industrie

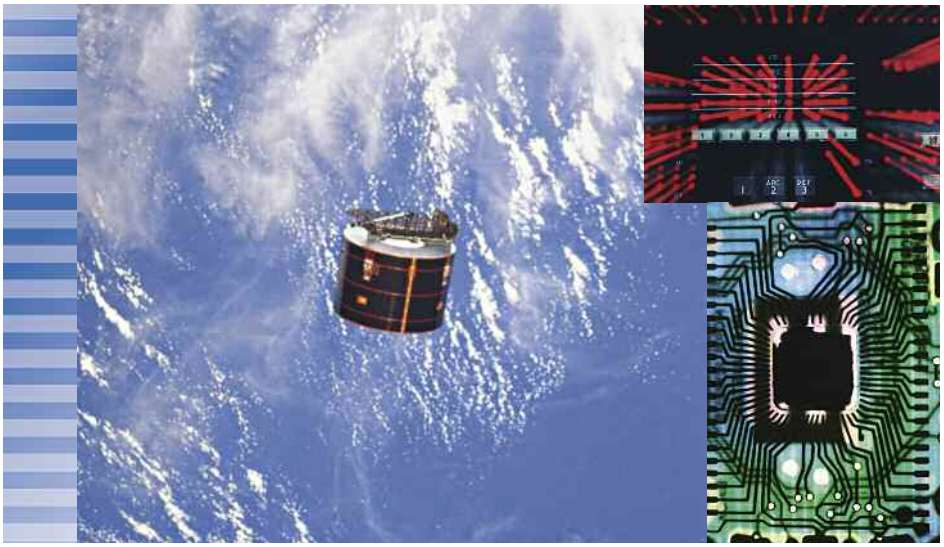
26. – 27. November 2013

andel's Hotel & Convention Center Berlin

- Eine der größten Veranstaltungen zur Europäischen Sicherheit und Verteidigung
- Jedes Jahr bis zu 1.000 Besucher aus einer Vielzahl von Nationen
- Ca. 100 Mitwirkende im Programm, u.a. Parlamentarier, hochrangige Politiker, Militärs, Vertreter der Industrie
- Partner in diesem Jahr: Großbritannien

Anmeldung und weitere Informationen:
www.euro-defence.eu

Foto: Bordignon V. Eurocorps



Vorankündigung:

28. AFCEA-Fachausstellung

07./08. Mai 2014

www.afcea.de