CRYPTO

CRYPTO MAGAZINE

N° 1 | 2013

Crypto AG an der Front

Geschätzte Leserin, geschätzter Leser

Ein frischer neuer Wind weht um die Crypto AG. Wir dürfen Ihnen mit Stolz unseren neuen Marktauftritt und unser modernisiertes Firmenlogo präsentieren. Ganz im Zeichen der neuen Ausrichtung Security Solutions und Services – kombiniert mit den bewährten Security Products – zeigt sich die Crypto AG in neuem Gewand. Unter www.crypto.ch können Sie dreidimensional in die Welt der Lösungen, Produkte und Kundengruppen eintauchen.

In der aktuellen Ausgabe haben wir den Fokus auf das neue Erscheinungsbild gelegt und fragen: Haben Sie schon unseren neuen Internetauftritt gesehen?

Ich wünsche Ihnen viel Vergnügen beim Lesen der neusten Ausgabe des CryptoMagazines.

Giuliano Otth

President and
Chief Executive Officer

Focus

Neuer Marktauftritt zur erweiterten Strategie

Seite 3

Impressum

Erscheint 3-mal jährlich | **Auflage** | 6'700 (deutsch, englisch, französisch, spanisch, russisch, arabisch)

Herausgeber | Crypto AG, Postfach 460, 6301 Zug, www.crypto.ch
Redaktionsleitung | Béatrice Heusser, Crypto AG, Tel. +41 41 749 77 22, Fax +41 41 741 22 72, beatrice.heusser@crypto.ch

Konzept/Layout | illugraphic, Sonnhalde 3, 6332 Hagendorn, www.illugraphic.ch

Übersetzung | Apostroph AG, Töpferstrasse 5, Postfach, 6000 Luzern 6, www.apostroph.ch

Druck | Druckerei Ennetsee AG, Bösch 35, 6331 Hünenberg

Bildnachweis | Crypto AG: S. 2, 9, 10, 14, 19, 21, 22, 23
illugraphic: Titelseite, S. 3, 4, 5 | LABOR SPIEZ: S. 11, 13 | MetaDesign: S. 5
Shutterstock: S. 7, 8, 11, 19, 24 | Alan49 / Shutterstock.com: S. 17

Neuer Marktauftritt zur erweiterten Strategie

Informationssicherheit, als Markt verstanden, ist im Begriff, sich tief greifend zu wandeln. Statt Einzelkomponenten und -leistungen rücken immer mehr umfassende Solutions ins Zentrum der Kundenbedürfnisse. Crypto AG trägt dieser Entwicklung mit einer angepassten Marktstrategie Rechnung. Sichtbar wird dies an der neu gestalteten Webseite www.crypto.ch. Alle weiteren Werbemittel werden sukzessive nachziehen.

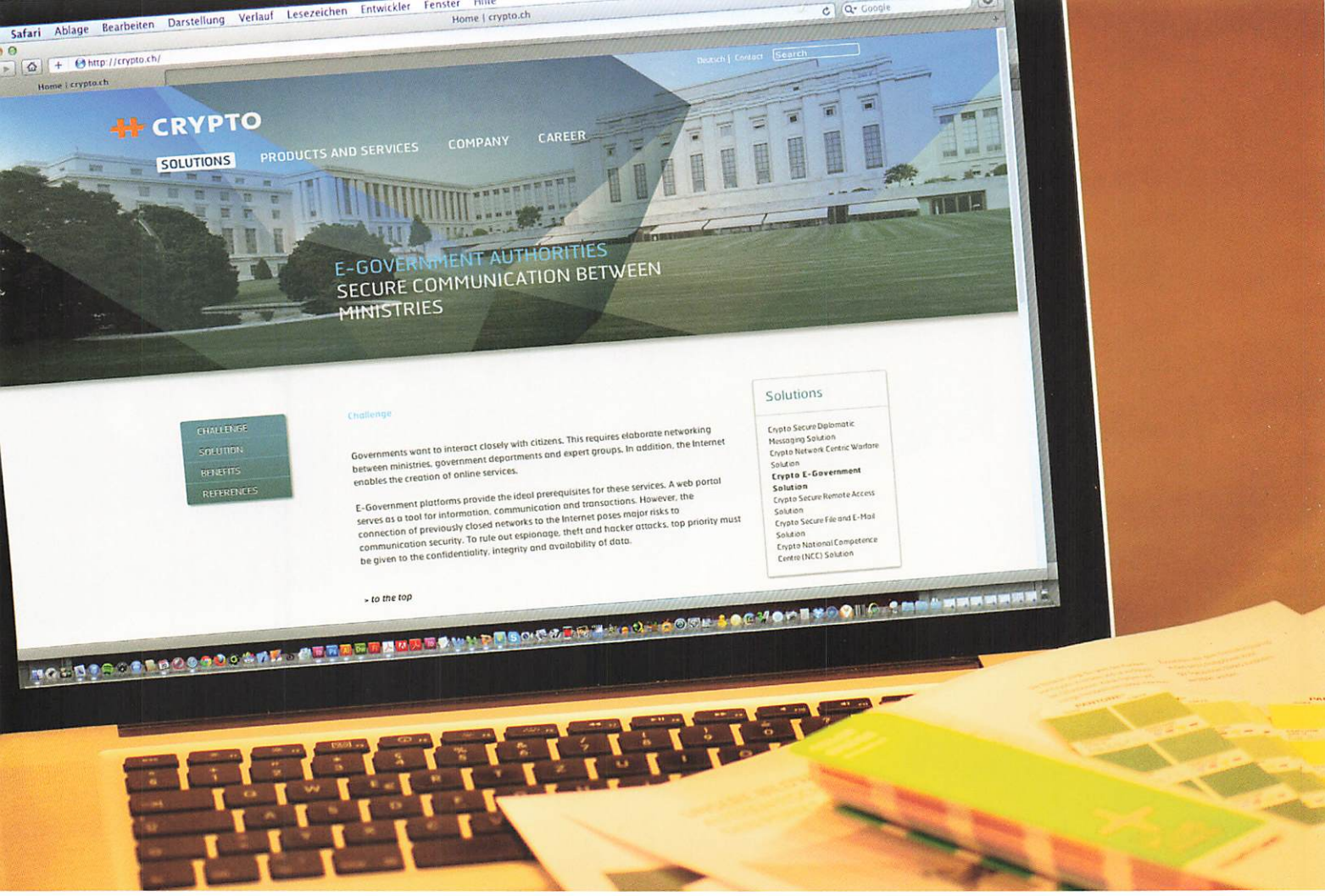
Urs Kürzi | Customer Segment Manager

Mit der Ausdehnung ihres Angebots auf umfassende Solutions für Informationssicherheit kommt Crypto AG differenzierten Forderungen ihrer Kunden nach. Informationssicherheit wird zunehmend zu einem mehrdimensionalen Thema, welches von Beratungsleistungen über Zonierungs- und Klassifikationskonzepte bis hin zu individuellen Supportmodellen reicht.

Hier bestätigt sich wieder einmal, dass das Ganze mehr als die Summe seiner Teile darstellt. Folgerichtig begrüsst der neue Webauftritt die Besucher prominent mit den Referenzmodellen, die auf realen Solutionsprojekten basieren. Selbstverständlich wird der Diskretion betreffend einzelne Länder und Kunden höchster Stellenwert beigemessen.

Ein schickes Logo zur Orientierung

Dem Besucher der Webseite dürften gleich zwei Elemente auffallen: Zum einen besticht die frische Farbigkeit des Designs, zum andern präsentiert sich das neue Logo als moderne Wortmarke. Letzteres vermittelt beschwingte Modernität und trägt gleichwohl die Wiedererkennbarkeit in sich: Das schlanke H im bewährten Orange gehalten, mit in Leserichtung weitergeführtem Firmennamen. Die Ecken wurden gerundet, die Abstände optimiert und die Linien geschärft. Das Crypto-Logo gibt den Kunden Orientierung in der Flut der Botschaften. Die starke Marke Crypto steht wie ein Leuchtturm an der Küste.



Willkommen auf der neuen Webseite. Referenzmodelle realer Solutions stehen im Fokus.

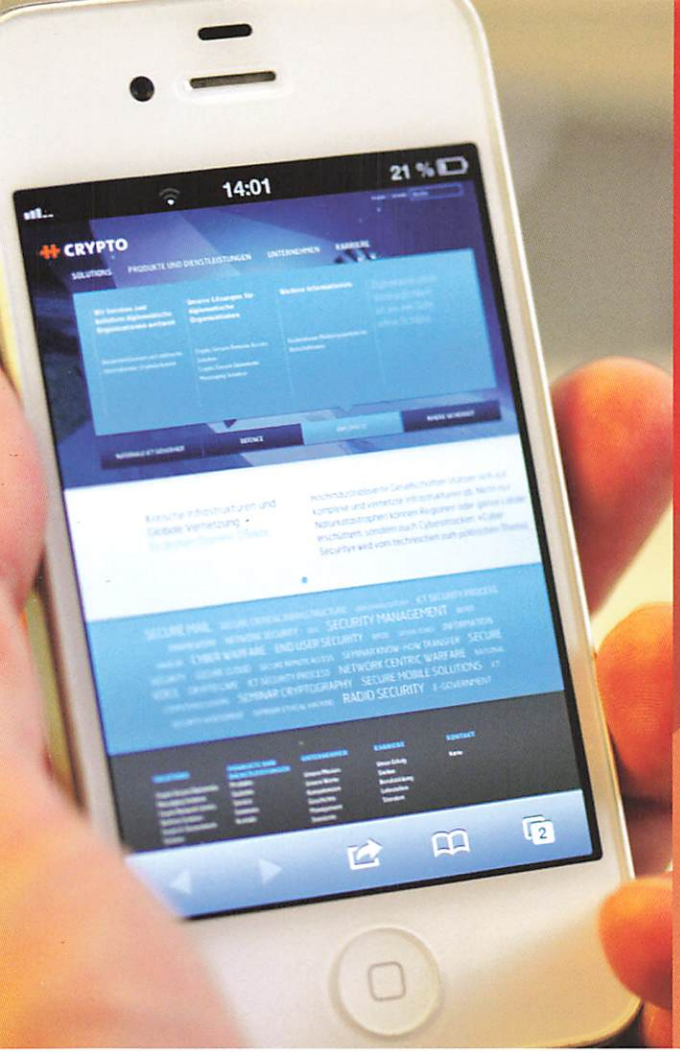
Sicherheitslösungen der Crypto AG schaffen für den Kunden geschützte Kommunikationsräume. Visualisiert wird dieser Aspekt mit unterschiedlichen, über die Bilder gelegten Mustern. Sie bilden damit symbolisch die Kommunikationsräume nach und illustrieren darüber hinaus die strukturierte, mathematische exakte Welt der Kryptografie. Die sechs verschiedenen Akzentfarben der Visuals manifestieren die vielschichtige Angebotspalette und erzeugen dadurch eine eigenständige Differenzierung im Solutionsangebot. Grossformatige Fotos legen den Rahmen des neuen Auftritts fest. Die Bilder zeigen Personen als Akteure in realen und authentischen Situationen. Ausgesprochen motivierte Menschen arbeiten hier mit Leidenschaft, bedienen sich sicherer Informations- und Kommunikationssysteme, diskutieren Sicherheitsthemen oder sind ganz einfach in typischen Regierungsszenarien abgebildet.

Produktplattformen als Basis von Solutions

Ein Meilenstein auf der neuen Webseite ist mit der Kommunikation über Produktplattformen gelungen. Der Kundennutzen ist auf einen Blick ersichtlich, weil die spezifischen «Security Applications» in den Vordergrund rücken. Icons für Applikationen, welche grafisch neben dem Chiffriergerät platziert sind, visualisieren die möglichen Verschlüsselungsfunktionen. Dies bedeutet, dass eine bestimmte «Crypto-Plattform» für einen spezifischen Einsatz konzipiert bzw. konfiguriert wurde und je nach Bedarf mit einzelnen oder mehreren Sicherheitsapplikationen versehen werden kann. Eine solche Chiffrierplattform ist für den Anwender viel vorteilhafter, als für jedes einzelne Kommunikationsmedium ein separates Chiffrierprodukt zu betreiben. Das Plattformkonzept schützt getätigte und zukünftige Investitionen und bildet nicht zuletzt die Basis für sehr individualisierte Sicherheitssolutions.

Die Benutzerfreundlichkeit entscheidet

Webnutzer schätzen es, wenn sie schnell und unkompliziert durch eine Webseite navigieren können – andernfalls sind sie mit einem Klick im Cyberspace verschwunden. Was profan klingt, ist in der Realität schwierig zu erreichen. Eine gute Orientierung beginnt mit geeigneten Strukturierungen, Hierarchien, Abständen und Typografie. Informationen



Die Werkzeugkiste für den Solutionanbieter Crypto AG: Grafische Elemente symbolisieren geschützte Kommunikationsräume, Akzentfarben visualisieren das breite Angebot, und mit den neuen Icons lassen sich selbst komplexe Szenarien einfach darstellen.

sollen möglichst intuitiv gefunden werden können. Nur getreu dem Grundsatz «der Aufbau folgt dem Inhalt» kann eine Homepage zum immer wieder gern genutzten, virtuellen Kundentreffpunkt mutieren. Mit Blick in die Zukunft und auf das Potenzial des digitalen Marketings wurde die Webseite bereits mit einer vertikalen Scrollfunktion auf Tablet-Computer und Smartphones ausgerichtet. Die tadellose Gebrauchsfähigkeit einer Webseite ist die erste Voraussetzung für einen unmittelbaren Kundennutzen.

Die «Schlagwortwolke»

Eine Besonderheit ist die sogenannte Schlagwortwolke (Tag-Cloud). Sie bietet sich an, um gewichtige Themen der Sicherheitsbranche strukturell losgelöst zu kommunizieren. Je nach Häufigkeit, mit der die Nutzer einzelne Wörter aufgerufen haben, wird die Schrift grösser oder kleiner dargestellt. Eine Tag-Cloud ermittelt so die Gewichtung dynamisch und macht sie auf einen Blick erfassbar.

Das Internet ist zum Leitmedium unserer Gesellschaft geworden und erreicht uns in allen Lebenssituationen.

Diesen Gegebenheiten hat die Crypto AG Rechnung getragen und mit dem Aufschalten der neuen Webseite einen omnipräsenten Zugang in die Welt der Sicherheitslösungen geschaffen. Wir wünschen Ihnen viel Vergnügen beim Erkunden dieser virtuellen Dimension und stehen Ihnen gerne zur Verfügung, wenn Sie anschliessend bei uns auch die reale kennenlernen möchten.

Sicheres Messaging als Basis für gute Polizeiarbeit

Diese von Crypto AG realisierte sichere Messaging-Lösung für eine grosse, landesweit operierende Polizeiorganisation hat ihre operative Bewährungsprobe soeben glänzend bestanden. Ihre Funktionalität als anwenderspezifisch konzipiertes Gesamtsystem erreicht völlig neue Dimensionen.

Dr. Rudolf Meier | Publizist

Jahrzehntelang diente Fax als bewährtes Kommunikations- und Führungsinstrument bei dezentral operierenden Polizeiorganisationen. Heute werden diese Funktionen mehrheitlich von elektronischen Messaging-Systemen übernommen. Mit ihnen lassen sich sowohl einzelne Personen Meldungen zustellen («Push»-Verfahren) als auch ganzen Dienststellen (definierter Empfängerkreis). Wenn nötig können Meldungen auch direkt an einen Drucker übermittelt und von diesem sofort gedruckt werden. Dass auf der Netzebene modernste Technologien genutzt werden, welche eine flexible Topologie ermöglichen, versteht sich von selbst.

Heute spielen daneben jedoch auch Sicherheitskriterien wie Vertraulichkeit, Integrität und Authentizität der kommunizierten Informationen eine entscheidende Rolle. Bei alledem soll das System auch noch möglichst einfach bedienbar sein und eventuelle Fehler gleich selber verhindern. Daraus ist unschwer abzuleiten, dass derart praxisorientierte Anforderungen nur mit einer universellen, von A bis Z individuell durchkonzipierten Messaging-Lösung erfüllt werden können.

Crypto AG realisiert Messaging-Lösungen oft in ziemlich unterschiedlichen Szenarien. Das kürzlich abgeschlossene Projekt für ein flächendeckendes, landesweites Netz mit mehreren Hundert angeschlossenen Polizeiaussenstellen war jedoch selbst für die erfahrenen Ingenieure, Techniker und Kryptografen von Crypto AG eine interessante Herausforderung.

Netztopologie? So, wie man sie gerade benötigt!
Die Grundstruktur dieses typischen Client-Server-Systems ist recht einfach: Der zentrale Netzserver steht im Hauptquartier (HQ) der Polizeiorganisation. Er ist direkt mit der zentralen Datenbank vernetzt, damit die im Einsatz befindlichen Polizeieinheiten online Datenzugriffe – zum Beispiel betreffend Fahndungsraster – vornehmen können. Weiter «hängt» hier am Server auch das computergestützte, zentralisierte Network und Security Management.

Gleichzeitig ist der Server Ausgangspunkt für die sternförmige, landesweite Vernetzung der geografisch teilweise weit entfernten Polizeistellen. Der Datentransport kann – auf Internet-Protokoll-Basis – über unterschiedliche Wege erfolgen: über Leased-Lines mehrerer Provider, via MPLS (wenn grosse Flexibilität nötig ist) und als direkte Internetanbindung. Aus topografischen Gründen mussten auch einige VHF- und Richtfunkstrecken integriert werden. Später ist ausserdem der Einbezug von Küstenwachschiffen via Sat-Links vorgesehen. Für die Systemfunktionen ist es unerheblich, welcher Kanal (automatisch gewählt) zum Einsatz kommt.

Der gesamte Datenverkehr zwischen dem HQ inklusive Datenbank und den Clients (Aussenstellen) ist mittels IP-VPN-Chiffrierung auf höchstem Niveau geschützt.

Dazu werden je nach Einsatzort und -profil (HQ, Aussenstellen, Fahrzeuge, Schiffe) Geräte der Familien HC-7825 und HC-7835 eingesetzt. Es handelt sich folglich um ein virtuell komplett «geschlossenes System».

Jede Polizeiaussenstelle bildet einen Netzknoten (Client), an dem ein Server (integriert im Chiffriergerät) die intelligente Netzintegration gewährleistet. Als Arbeitsgeräte werden handelsübliche PCs, Laptops und Peripheriegeräte (Drucker, Scanner) eingesetzt.

Was sichere Kommunikation wirklich wert ist, zeigt sich erst in der rauen Praxis.

Die Netztopologie umfasst mehrere Hierarchien, indem bestimmte Netzbereiche mit einem Subserver zu jeweils einem Subnetz zusammengefasst sind. Diese Subnetze lassen sich unabhängig im Onlinemodus vom HQ aus administrieren, was zum Beispiel für Katastropheneinsätze äusserst wichtig sein kann.

Gezielt unterstützte Führungsfunktionen

Jeder im System authentifizierte Client kann auf praktisch jedem Kommunikationskanal online und sicher auf die voll integrierte Datenbank zugreifen und Daten dorthin übermitteln (Push- und Pull-Modus). Für Datenabfragen und standardisierte Botschaften wurden organisationsspezifische Formulare kreiert. Ebenso ist die Such- und Speicherlogik so organisiert, dass sie den spezifischen Polizeibedürfnissen genau entspricht. Für den Messaging-Verkehr zwischen HQ und Aussenstellen können den Messages (Mails) Attachements jeder gebräuchlichen Art angehängt werden. Alle diese Datentransfers erfolgen selbstverständlich nur chiffriert. Fehler werden so praktisch ausgeschlossen.

Das System liefert online Empfangs- und Lesebestätigungen an den Sender zurück (und Bestätigungen, wenn eine Meldung ausgedruckt wurde), was für dieses Arbeitsszenario unverzichtbar ist. Nachdrücklich gefordert wurde in der Projektphase vonseiten des Auftraggebers auch die Möglichkeit, Meldungen «an alle» (Broadcast-Mode) zu übermitteln – was nun praktisch innert Sekundenschnelle möglich ist. Wie bei den meisten staatsnahen Arbeitsszenarien ist die automatische Aufzeichnung des gesamten Datenverkehrs auch hier eine Selbstverständlichkeit. Den Anforderungen an den Datenschutz wurden unter anderem mit der starken Benutzerauthentifizierung mittels Passwort und Fingerprint bei jedem Client Rechnung getragen.

An den Clients (Laptops oder PCs) lässt sich komfortabel mit gewohnten Office-Oberflächen arbeiten. Daten können lokal (und chiffriert) gespeichert werden. Ausserdem hat jeder Client einen Dokumenten-Scanner zur Verfügung, damit Originaldokumente (z. B. Pässe) an die Datenbank übermittelt werden können. Das Anwählen der einzelnen Teilnehmer im Netz erfolgt bequem mit einem elektronischen Adressbuch, was wiederum Fehler ausschliesst.

Bereits praxisbewährt

Bereits in den ersten Phasen des «scharfen» Systembetriebs hat sich gezeigt, dass die Automatisierung aller wichtigen Sicherheitsfunktionen das Vertrauen in die Sicherheit und Effizienz der Führungsfunktionen sehr erhöht. Fehler, wie man sie früher gerade bei Faxlösungen im manuellen Betrieb kannte – beispielsweise irrtümliche Klartextsendungen oder falsche Adressierungen –, werden durch dieses geschlossene System bereits konzeptionell verhindert. Da sich die Topologie dieser Dienststellenorganisation ständig «in Bewegung» befindet, wird auch das komfortable Security Management mit dem zentralen, computergestützten Security Management Centre im HQ sehr geschätzt.

Wenig bemerkt, jedoch letztlich sehr nützlich, sind die automatischen Back-ups, welche das System täglich vornimmt. Ein ausgefallener Knoten beispielsweise wäre relativ einfach zu restituieren.

Damit ist der Aufbau der Lösung zwar abgeschlossen. Crypto AG wird jedoch während der gesamten Lebensdauer des Systems (in der Vergangenheit waren dies oft Jahrzehnte) die Wartung und Ersatzteillieferung gewährleisten.

Die Crypto AG an der IDEX

Dass sich alles, was Rang und Namen hat unter den Anbietern von Rüstungsgütern, alle zwei Jahre in Abu Dhabi trifft, liegt sicher auch an der mit viel Showeffekten geladenen Atmosphäre. Praktisch lückenlos sind alle wichtigen Technologiebereiche vertreten.

Markus Baumeler | Head of Bid Management

Auch die Crypto AG ist jeweils im Swiss Pavillon präsent. Bei kaum einer anderen Gelegenheit lassen sich so viele nachhaltige Kontakte knüpfen und pflegen wie hier – und dies nicht nur mit internationaler Kundschaft, sondern auch mit Schweizer Militärexperten und Behördenvertretern.

Realität oder Fiktion? Auf Grossleinwänden meldet der Sprecher einer nachgestellten Nachrichtensendung einen fiktiven Angriff auf eine Hafenstadt. Begleitet von ohrenbetäubendem Gefechtsspektakel rollen Panzer über Rampen, Kampfjets donnern über das Gelände, Explosionen simulieren die Einschläge von Bomben. Zwischen den Panzern flitzen Sandbuggys hin und her, an deren Antennen schwarze Flaggen flattern. Motocross-Fahrer schiessen über Rampen Richtung Himmel und vollführen akrobatische Einlagen, während um sie herum eine Schlacht tobt[1]. Unverkennbar: Die IDEX weiss sich einmal mehr ihre typische, eindrückliche Atmosphäre zu schaffen.

Ungebrochenes Wachstum

Auf 124'000 Quadratmetern präsentierten über 1'000 Hersteller aus 59 Ländern ihre jüngsten Rüstungsentwicklungen zu Wasser, zu Land und in der Luft an der weltgrössten Fachmesse in Abu Dhabi – welche vom 17. bis 21. Februar stattfand. Allein 140 lokale Unternehmen waren vor Ort, daneben 900 internationale Anbieter. Dieses Jahr standen nicht weniger als 33 Länderpavillons auf dem riesigen Gelände, wobei die grössten Aussteller aus der UAE, den USA, aus Frankreich, der Türkei, China, Deutschland, Russland und Italien stammten. Schirmherr der Messe war Scheich Khalifa Bin Zayed Al Nahyan, Präsident der Vereinigten Arabischen Emirate und Oberbefehlshaber der Truppen des Landes.

Ermöglicht wurde die alle zwei Jahre stattfindende IDEX auch aufgrund der Unterstützung von Seiner Hoheit General Sheikh Mohammed Bin Zayed Al Nahyan, dem Kronprinzen von Abu Dhabi und Stellvertretenden Oberbefehlshaber der Streitkräfte. An der Liveshow sozusagen «in eigener Sache» wurde natürlich auch die neuste Errungenschaft der UAE Armed Forces präsentiert: Der Airbus A330 MRTT Tanker/Transporter. Die Übergabe an die Streitkräfte war am 6. Februar erfolgt.

Unbemannte Fahrzeuge strategisch immer wichtiger

Bei der von 600'000 Besuchern frequentierten Mammutausstellung gab es wieder diverse konzeptionelle Erweiterungen: Ins Auge stach etwa die First-Time Exhibitor Zone (FTEZ) mit 65 Firmen, welche zum ersten Mal an der IDEX präsent war.

Auf reges Interesse stiess auch der neue Helikopter-Pavillon – eine Aussenausstellung mit verschiedenen Exemplaren von Helikoptern der Typen Bell UH-1Y (US Navy), Panther (UAE), Super Puma (UAE) und Black Hack (UAE). Und die auf Kriegsschiffe ausgerichtete NAVDEX wuchs im Vergleich

Kompakte Eleganz: Der Crypto-Stand im Swiss Pavillon.

um enorme 50 %. Auf 6'000 Quadratmetern tummelten sich 80 Firmen, und sechs Kriegsschiffe aus Amerika, Italien, Frankreich, UK und Pakistan standen zur Besichtigung bereit.

Ganz besonders ins Zentrum gerückt wurden die unbemannten Flugsysteme: Mit einem eigenen Bereich, der «Unmanned System Area», inklusive einer riesigen Ausstellungshalle, Aussenstellplätzen und zahlreicher Livedemonstrationen. Zudem wurde am 19. Februar ein technischer Workshop zu den unbemannten Fahrzeugen angeboten, da diese neuen Systeme einen wichtigen Platz in jeder modernen Armee einnehmen. Dies bestätigen auch die GCC Countries, welche vor einer 360-Millionen-Dollar-Investition in Unmanned Aerial Vehicles (UAV) in den nächsten 10 Jahren stehen.

Crypto AG präsentiert neues Network-Modell

Die Schweiz war auch dieses Jahr wieder mit mehr als 30 Unternehmen an der IDEX vertreten, darunter auch die Crypto AG. Dabei stellte wie gewohnt der Swiss Pavillon eine attraktive Plattform für die meisten dieser Schweizer Firmen dar. Diese grosse Präsenz aus unserem Land zeigt die ausgezeichnete Zusammenarbeit der Golfstaaten mit der neutralen Schweiz und ihren unabhängigen Firmen auf. Sie basiert ganz offensichtlich auf langjährigem Vertrauen und gegenseitiger Wertschätzung.

Dass Informationssicherheit in Verteidigungsministerien und Regierungsorganisationen dieser Region von existenzieller Bedeutung ist, zeigten die vielen Besucher am Stand der Crypto AG. Die Besucher nutzten die Gelegenheit, unter Experten über verschiedene Lösungen zu diskutieren und

[1] Siehe auch «Der Spiegel», 18.2.2013, und «DIE ZEIT», 19.2.2013

Oben: In der Aussenausstellung NAVDEX konnte man Drohnen, Helikopter sowie Schiffe bestaunen und begehen.

Links: Ranghohe Persönlichkeiten durften wir begrüssen (v.l.n.r.): Markus Baumeler, Daniel Bucher, der Chef der Schweizer Armee Korpskommandant André Blattmann, Brigadier Rolf Siegenthaler, Heinrich Düringer.

anhand von Livedemonstrationen den praktischen Einsatz hautnah mitzuerleben. Der Stand-Setup wurde rege benutzt, vor allem die Radio-Kommunikation mit dem neuen MultiCom Radio-Encryption HC-2605-Terminal und dessen Interoperabilität mit dem HC-2650 MultiCom sowie das Messaging mit dem MultiCom Messenger. Auf grosses Interesse stiess weiter im Bereich Enduser/Office-Lösungen die Demonstration der Kompatibilität von Secure GSM HC-9100 und Desktop Station HC-9300.

Auch die neusten Modelle aus dem Network-Portfolio waren stark gefragt, standen doch eine robuste und stark widerstandsfähige (Rugged) Version sowie eine in Transport- und Überwachungsflugzeugen, Helikoptern und Drohnen einsetzbare spezielle (Airborne) Variante der Rugged Ethernet/IP Network Encryption Platform HC-8224 zur Verfügung.

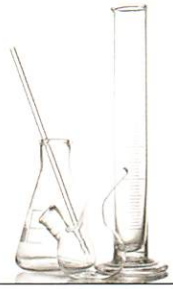
Reger Austausch mit VIPs und Militärbehörden

Der erste Ausstellungstag war den offiziellen VIPs und hochrangigen nationalen und internationalen Delegationen vorbehalten. Diese durchschritten im Anschluss an die offizielle Eröffnung die Ausstellung und statteten einigen namhaften Unternehmen einen Kurzbesuch ab. Auch dieses Jahr durfte die Crypto AG wieder den Chef der Schweizer Armee, Korpskommandant André Blattmann, und weitere hochrangige Offiziere sowie die Schweizer Botschafterin Andrea Reichlin an ihrem Stand begrüssen. Bei einem Kaffee konnten Experten der Crypto AG die neusten Lösungen und Trends der Informationssicherheit präsentieren und mit den Interessenten ausgiebig diskutieren.

Im Namen des gesamten Teams und der Crypto AG bedanke ich mich herzlich bei allen Kunden, Partnern und Interessenten, die uns mit ihrem Besuch an der IDEX beehrt haben.

Bis zur nächsten IDEX, die vom 22. bis 26. Februar 2015 stattfinden wird.

Generell werden externe Risiken überbewertet und interne zu wenig ernst genommen



Das LABOR SPIEZ im Schweizer Kanton Bern erarbeitet das Grundlagenwissen für den ABC-Schutz. Es erbringt Dienstleistungen für internationale Organisationen, für die Behörden und für die Bevölkerung in den Bereichen Rüstungskontrolle, Schutzmassnahmen und Ereignisbewältigung. Damit leistet das zivile Labor einen wissenschaftlichen Beitrag zur Sicherheit von Mensch und Umwelt.

Das Interview führte Casha Frigo Schmidiger

Herr Dr. Bucher, das LABOR SPIEZ ist weltweit hoch anerkannt in Fragen des Schutzes vor ABC-Waffen. Ist nun Ihre Arbeit eher politisch oder eher wissenschaftlich einzuordnen?
Wir sind klar wissenschaftlich orientiert, jedoch unser Motto, sprich unsere Vision, ist eine Welt ohne Massenvernichtungswaffen. Dementsprechend liegt der Fokus unserer Arbeit heute auf Fragen der Rüstungskontrolle. Seit 25 Jahren kümmern wir uns unter anderem auch im Auftrag der UNO um diesen Themenbereich. In diesem Sinne machen wir zumindest indirekt Politik, indem wir der Schweizer Diplomatie Unterstützung anbieten. Wir halten zu diversen Themen der Rüstungskontrolle Konferenzen ab und verfassen Dokumentationen, welche die Schweizer Delegationen in internationale Verhandlungen einbringen können. Ein Beispiel eines solchen Themas sind neuartige chemische Stoffe, die kampfunfähig machen, die «Incapacitating Chemical Agents», welche wir wissenschaftlich aufarbeiten.

Woher kommen diese Stoffe? Wer hat diese Agents auf der Agenda?
Das sind verschiedene Länder. Incapacitating Chemical Agents sind toxische Stoffe mit speziellen Wirkungen – Stoffe wie beispielsweise das Fentanylderivat, das bei der Befreiung der Geiseln aus dem Moskauer Theater eingesetzt wurde. Zwar wurden da die Geiselnehmer unschädlich gemacht, viele Geiseln sind jedoch auch umgekommen. Das Problem ist, dass das internationale Chemiewaffenübereinkommen den Einsatz toxischer Stoffe für Polizeiaufgaben erlaubt, jedoch offenlässt, welche Einsätze genau darunterfallen.

Von welchen Waffen gehen die meisten Gefahren aus, von A-, B- oder C-Waffen?
Das sind ganz unterschiedliche Bedrohungen. Jede dieser Klasse hat eine gewisse Geschichte. Begonnen hat es im Ersten Weltkrieg mit Gasangriffen. Im Kalten Krieg lag der Fokus eher auf der atomaren Bedrohung – diese hält bis heute an. Die B-Waffen sind die «jüngste Klasse». Hier ist es für uns schlussendlich irrelevant, ob ein Erreger von einem Terroristen verbreitet wird, oder ob es sich um einen sich natürlich verbreitenden Virus (Pandemie) handelt. Unsere Aufgabe ist es, die Art des Erregers zu identifizieren, wofür wir speziell ausgerüstet sind.

Die Erreger müssen möglichst rasch und zuverlässig identifiziert werden.

Ist es nicht so, dass Sie in Spiez ganz spezielle Erreger wie beispielsweise Ebola züchten?
Unsere Aufgabe ist, die Erreger möglichst rasch zuverlässig identifizieren zu können. Dazu haben wir ein neues biologisches Sicherheitslabor (B-Labor) gebaut, welches wir 2013 in Betrieb nehmen konnten.

Pandemien nehmen tendenziell zu. Welche Rolle spielt hier das LABOR SPIEZ?
Bei Verdacht auf einen bisher unbekannten Erreger, der nicht auf Antibiotika und antivirale Medikamente anspricht und dessen Gefährlichkeit man nicht einschätzen kann, kommen unsere Fachpersonen zum Einsatz. Wir unterstützen das nationale Referenzzentrum für Virenerkrankungen.

Inwiefern kann eine Forschung mit der Herstellung von eigenen chemischen Kampfstoffen und der Arbeit mit hoch ansteckenden Erregern wie Ebola und Anthrax für Ihre unmittelbare Umgebung verantwortet werden? Stossen oder stiessen Sie mit Ihrer Arbeit auf Widerstand bei der Bevölkerung im Kanton Bern?
Das Verhältnis mit der Bevölkerung war immer gut. Das LABOR SPIEZ existiert schon seit über 80 Jahren. Wir haben immer mit gefährlichen Stoffen gearbeitet und bis jetzt gab es keine Zwischenfälle.

Immer wichtig war für uns eine transparente Informationspolitik im Zusammenhang mit dem Bau des neuen B-Labors. Wir informieren die Bevölkerung und die lokalen Behörden über unsere Arbeit, zum Beispiel auch im Rahmen von Tagen der offenen Tür. Dieses Vorgehen zahlt sich im Hinblick auf das gegenseitige Verständnis aus.

Was die Gefahren für die umliegende Bevölkerung betraf, so mussten wir unsere Aufsichtsbehörden darüber orientieren, wie hoch der Ansteckungsradius ist, falls durch ein (in höchstem Masse unwahrscheinliches) Ereignis pathogene Viren nach aussen gelangen könnten. Wir konnten nachweisen, dass die Ansteckungsgefahr ausserhalb eines Radius von 40 Metern aufhört. Falls also ein derartiger Unfall trotz aller Sicherheitsmassnahmen eintreten würde, hätten wir nur auf unserem Gelände ein Problem.

Gehen wir richtig in der Annahme, dass Sie beispielsweise bei Fällen wie dem Briefverteilzentrum Mülligen, wo ein Grossteil der Schweizer Post sortiert wird, zum Einsatz kamen? Es bestand ja ein Verdacht auf einen Anthraxanschlag, und die Angestellten mussten evakuiert werden. Welches ist in einem solchen Fall Ihre Aufgabe?
Für den Nachweis von Erregern wie Anthrax wurde ein spezielles Regionallabornetz eingerichtet. In diesem Verdachtsfall kamen wir nicht zum Zuge. Für den Standort Mülligen ist ein anderes Labor zuständig.

In der ganzen Schweiz sind wir hingegen das einzige Labor zur Analyse von Erregern der höchsten Risikostufe 4. Es gibt vier Risikostufen: Stufe 1 ist zum Beispiel Backhefe, was absolut unschädlich ist. Stufe 2 sind Erreger wie Salmonellen oder Influenza. Stufe 3 sind zum Beispiel Anthraxerreger, welche bereits tödliche Krankheiten auslösen können, jedoch existieren noch Therapiemöglichkeiten. Stufe 4 sind spezielle virale Erkrankungen, etwa das hämorrhagische Fieber wie Marburg oder Ebola. Dort kann man nur noch auf das eigene Immunsystem hoffen, welches jedoch oft versagt. Zur Identifikation dieser Arten von Viren braucht es ganz spezielle Laboreinrichtungen sowie entsprechend ausgebildete Virologen.

Das LABOR SPIEZ leistet mit seiner Forschung einen wichtigen Beitrag zur Prävention und Schadensbegrenzung hinsichtlich des Einsatzes biologischer und chemischer Kampfstoffe. Das wissenschaftliche Renommee ist gross – auch international. Welches sind die wichtigsten Gremien und Partnerorganisationen, mit denen Sie sich in Ihrer täglichen Arbeit austauschen?
Wir arbeiten rund um die Welt mit Partnerlabors zusammen. Wie bereits erwähnt, sind wir für die UNO tätig, dort primär im Bereich Rüstungskontrolle. Hierfür waren wir unter anderem mehrmals im Irak. Zudem sind wir für die UNEP tätig, das Umweltprogramm der Vereinten Nationen. Da geht es vor allem darum, in Nachkriegszeiten potenzielle Umweltbelastungen abzuklären. Wir untersuchen etwa, ob nach einem bewaffneten Konflikt Belastungen mit leicht radioaktiver, panzerbrechender Munition aus abgereichertem Uran auftreten. Weiter sind wir für die Weltgesundheitsorganisation WHO tätig. Ebenso für die Internationale Atomenergieagentur IAEA.

Einer unserer wichtigsten Kunden ist die OPCW – die Organisation für das Verbot von chemischen Waffen.

Die OPCW muss das Chemiewaffenübereinkommen überwachen. Hierfür sind wir eines der designierten Labors. Jeder Staat, der dieses Abkommen unterzeichnet – und das sind fast alle auf der Welt mit einigen wichtigen Ausnahmen (z. B. Syrien) –, verpflichtet sich unter anderem, seine eigenen Industrieanlagen regelmässig kontrollieren zu lassen.

Es ist ein grosser Vorteil des LABOR SPIEZ, dass wir sehr interdisziplinär aufgestellt sind. Wir sind zwar klein – rund 100 Mitarbeiter –, verfügen allerdings über hoch spezialisiertes Personal. Im Krisenfall erhalten wir personelle Unterstützung vom Kompetenzzentrum ABC-KAMIR der Armee. Nur so kann bei einer Katastrophe oder einem Notfall ein 24-Stunden-Betrieb des Labors auf Dauer sichergestellt

DR. ANDREAS BUCHER, CHEF STRATEGIE UND KOMMUNIKATION, LABOR SPIEZ

Dr. Andreas Bucher (geb. 1964) studierte nach seiner Schulzeit in Zürich und Santa Barbara (CA), an den Universitäten Genf, Zürich und Berlin-Potsdam Wirtschafts- und Sozialwissenschaften. Anschliessend absolvierte er eine Journalistenausbildung beim «Tages-Anzeiger» in Zürich sowie am Medienausbildungszentrum MAZ in Luzern. 1992 arbeitete er zwei Jahre als EU-Sonderkorrespondent für die «Berner Zeitung», danach als Produzent des «Tages-Anzeigers» sowie als Nachrichtenchef und Redaktionsleiter für die TA-Gruppe. 2001 bis 2007 war er für das Nachrichtenmagazin «FACTS» tätig.

werden. Ich spreche hier das Beispiel der plötzlich epidemisch auftretenden Schweinegrippe bei Soldaten an: Da waren wir zuständig für die Diagnostik der Proben aller Armeeangehörigen in der Schweiz. Hierbei konnten uns die militärischen Spezialisten optimal unterstützen. Wir sind primär ein ziviles Labor mit einem klar definierten Forschungsauftrag.

In der Schweiz unterstützen wir auch das Eidgenössische Departement für auswärtige Angelegenheiten EDA, das EDI mit dem Bundesamt für Gesundheit oder das EVD mit dem Staatssekretariat für Wirtschaft SECO. Und seit 2011 sind wir auch das designierte Labor des Internationalen Komitees vom Roten Kreuz IKRK bei ABC-relevanten Fragen.

Kümmern Sie sich auch um die weltweit grassierende Ausbreitung von Krankheiten, welche von Tieren übertragen werden? Immerhin ist die Asiatische Tigermücke schon bis ins Tessin vorgedrungen.

Ja, hier handelt es sich um sogenannte «neue Vektoren». Gerade im Tessin haben wir ein Forschungsprojekt hierzu am Laufen. Die Klimaveränderungen haben zur Folge, dass laufend neue Übertragungswege für Erkrankungen infrage kommen und entsprechend überwacht werden müssen.

Ähnlich wie das CERN in Genf dürfte das LABOR SPIEZ auch die Fantasien kranker Geister beflügeln, die sich mit schadhaften Absichten und Anschlagideen tragen. Was wird unternommen, um diese Personen konsequent von Ihren sensiblen Einrichtungen und Forschungsarbeiten fernzuhalten?

Der Schutz unserer Forschungseinrichtungen gegen Einflüsse von aussen ist gewährleistet. Mehr kann ich hierzu nicht sagen. Generell werden meines Erachtens die externen Risiken eher überbewertet und die internen Risiken eher unterbewertet. In diesem Zusammenhang erwähne ich den Fall von Anthraxattacken in den USA im 2001. Hier war offenbar ein Angestellter eines staatlichen Labors über Monate an den Wochenenden damit beschäftigt, Anthrax waffenfähig zu machen, ohne dass seine Vorgesetzten davon wussten. Es heisst ja, die Chance, dass sich ein Terrorist zum Wissenschaftler ausbildet, sei wesentlich unwahrscheinlicher, als dass sich ein Wissenschaftler zum Terroristen machen lässt.

Ebenso sensibel wie die physischen Einrichtungen und Mittel selbst dürften die Forschungsergebnisse sein. Gleichzeitig ist es für Ihre Arbeit enorm wichtig, dass Sie sich mit anderen Wissenschaftlern austauschen können. Wie stellen Sie diese Kommunikation im Allgemeinen sicher – technisch und organisatorisch? Können Sie hierzu Stellung beziehen?

In unserer täglichen Arbeit sind wir mit Geheimhaltungsfragen beschäftigt und müssen damit umgehen können. Im internationalen Vergleich weisen wir allerdings einen hohen Grad an Transparenz auf. Wir wollen zeigen, was wir machen. Natürlich gibt es Arbeiten, welche wir nicht publizieren. Jedoch jeder, der will, findet etwa die Rezepte zur Herstellung von chemischen Kampfstoffen im Internet. Da würde eine konsequente Vertraulichkeit nur bedingt nützen. Hier steht eher eine konsequente Aufklärung über die potenziellen Gefahren im Vordergrund. So organisieren wir bei Chemie- und Biologiestudenten verschiedene Awareness-Raising-Programme.

Herr Dr. Bucher, herzlichen Dank für das Gespräch und Ihre spannenden Ausführungen.

www.labor-spiez.ch

Taktischer Richtstrahl: Marktlücke sicher geschlossen

Richtstrahlverbindungen spielen eine Schlüsselrolle im Verbund der netzwerkzentrierten Einsatzführung. Sie eignen sich zur raschen Inbetriebnahme innerhalb weniger Stunden und funktionieren auch in unwegsamen Gegenden, welche nicht anderweitig telematisch erschlossen sind. Crypto AG ergänzt die Richtstrahlwelt nun um eine vom Markt lang ersehnte Lösung: maximalen kryptografischen Schutz, umfassend gehärtet gegen die rauen Natur- und Einsatzbedingungen.

Jahn Koch | Customer Segment Manager Defence

Operative Netzwerke sind in der Regel umso mobiler, rascher verfügbarer und begrenzter in der Übertragungskapazität, je weiter vorne an der Front sie eingesetzt werden. Das Mittel erster Wahl auf taktischer Ebene bis Stufe Kompanie ist folglich HF- und VHF-Funk. Diese Funknetze werden sodann zusammengeführt und integriert in Richtstrahlbündel, welche die Anbindung von Bataillonen an grössere Verbände und darüber hinaus ermöglichen. Deren Führungsstaffeln sind zumeist nur während kurzer Zeit abgesessen und benötigen ab Erreichen ihres Einsatzraumes umgehend eine stabile Anbindung an vorgesetzte Stellen ab Brigadestärke – bei grösstmöglichem Datendurchsatz. Findet der Einsatz auf dem eigenen Territorium statt, so können mobile Kommandoposten sowie durchsatzintensive Sensoren-, Radar-, Steuerungs- und Feuerleitsysteme mit Hilfe von Richtstrahl häufig an das bestehende Festnetz angebunden und so direkt für Führungsinformationssysteme erschlossen werden. Richtstrahl bietet überdies eine relativ hohe Resistenz gegen Störungen und Beeinträchtigungen durch Elektronische Kriegsführung und wird häufig verwendet, um die taktisch-operative Führung vorrückender Kampfverbände durch die Einsatzleitung sicherzustellen. So wichtig der kryptografische Schutz dieser Verbindungen ist, so sehr gilt es auch den rauen Natur- und Einsatzbedingungen Rechnung zu tragen, denen die Übermittlungsmittel im Feld ausgesetzt sind.

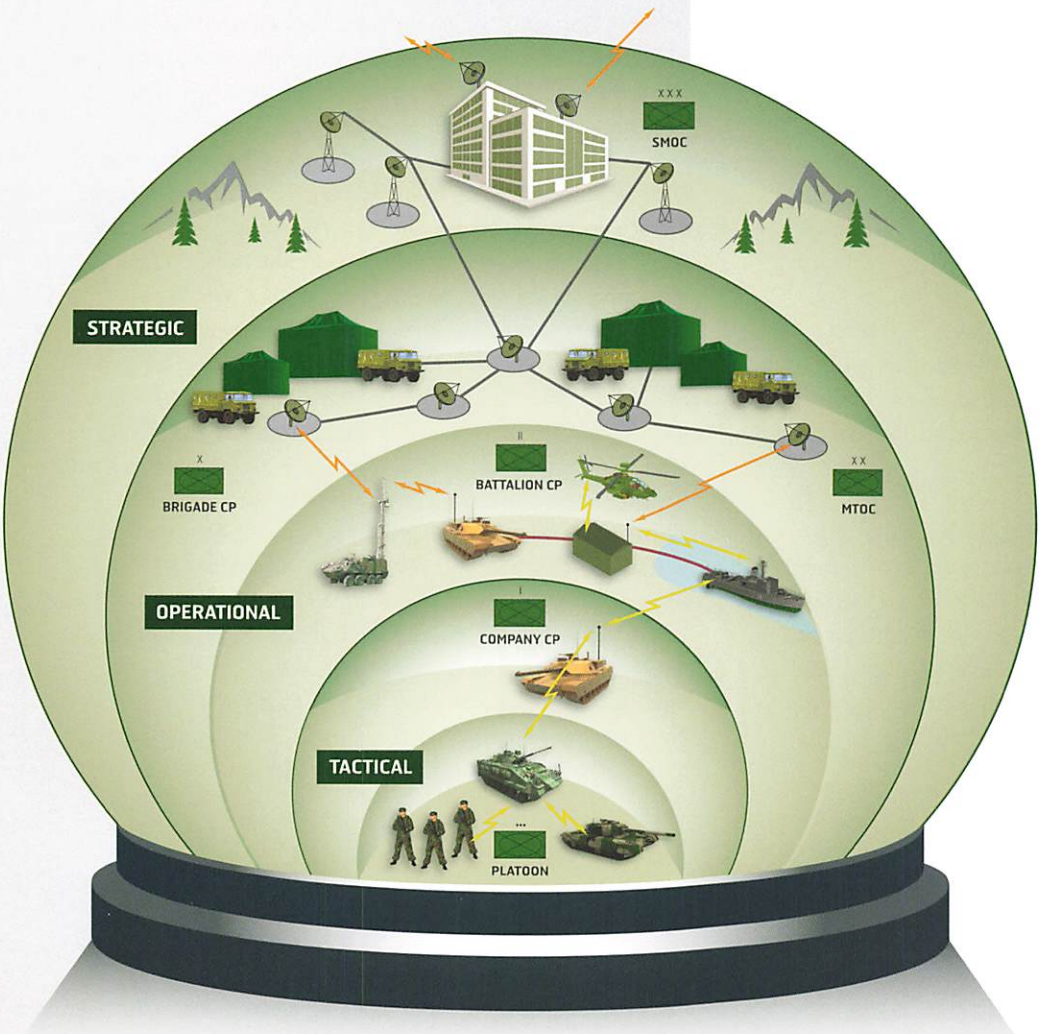
Bandbreite erzielen unter widrigen Umwelteinflüssen

Um sensitive Informationen wirkungsvoll zu schützen, müssen Richtstrahlverbindungen effektiv verschlüsselt und zusätzlichen elektronischen Härtungsmassnahmen unterzogen werden. Zudem muss die Übertragungskapazität auf die taktischen Bedürfnisse ausgerichtet werden. Sie muss hoch genug sein, um den gewünschten Datenstrom zu bewältigen und sollte schlank genug gehalten werden, um eine allzu leichte Detektierbarkeit durch elektronische Aufklärung zu vermeiden. Im Weiteren gilt es, der Robustheit des Übermittlungs- und Chiffrierequipments besonderes Augenmerk zu schenken. Der Einsatz unter Feldbedingungen bedeutet mitunter, dass es über längere Zeit extremer Vibration, Hitze, Kälte, Nässe, feinem Staub und sonstigen Verschmutzungen ausgesetzt ist. Die beste Technologie nützt folglich nichts, wenn die Geräte diesen harten Umweltbedingungen nicht standhalten können. Zu diesem Zweck hat Crypto AG eine neue, leistungsstarke Chiffrierplattform entwickelt.

Gehärtet und leistungsstark: Kryptologische Topsicherheit trifft auf Robustheit fürs Feld.

Die Rugged Ethernet/IP Network Encryption Platform HC-8224 ist speziell geeignet für den Schutz taktischer Richtstrahlverbindungen in Landeinsatzszenarien und ermöglicht eine Hochsicherheitsverschlüsselung von Links mit bis zu 100 Mb/s Bandbreite.

Am Scharnier zwischen Funk- und Netzwerkübertragung
Crypto AG bedient mit dieser neuen Plattform ein in jüngster Zeit rasant gestiegenes Kundenbedürfnis im Bereich Mikrowellenverbindungen. Sie ermöglicht den durchgängigen Schutz taktischer Funknetze, operativen Richtstrahls und fest installierter operativ-strategischer Netzwerke auf dem gleichen Hochsicherheitsniveau eines kundenspezifischen Algorithmus'. So werden optimale Bedingungen geschaffen für den erfolgreichen und sicheren Einsatz militärischer Applikationen und komplexer Führungsinformationssysteme, welche auf diese Art von geschützten, hochverfügbaren und -replizierenden Netzwerkverbindungen angewiesen sind. Die symmetrische Verschlüsselung innerhalb des HC-8224 erfolgt durch eine zugriffsgeschützte (Tamper Proof) Hardware. Kryptologische und mechanische Attacken werden dadurch aussichtslos. Der periodische Austausch von Schlüsseln zwischen den verschiedenen Einheiten erfolgt automatisch und ohne Beeinträchtigung der Nutzungsrate. Die gehärtete Bauart, die auch die Anforderungen militärischer Normen erfüllt, erlaubt den Einsatz der Plattform unter anderem in militärischen Fahrzeugen, Panzern oder mobilen Führungssheltern. Aufgrund der geringen Leistungsaufnahme und passiven Kühlung benötigt die Plattform keinerlei interne Ventilatoren oder Lüftungsöffnungen. Dank eines optionalen Aufsatzes kann sie überdies komplett wasser- und staubdicht gemacht und mit gängigen militärischen Steckern angeschlossen werden.



Crypto AG ermöglicht durchgängigen Schutz taktischer Funknetze, operativen Richtstrahls und fest installierter operativ-strategischer Netzwerke.

Subsidiäre Einsätze von militärischen Spezialeinheiten auf hoher See

Terroristische Aktivitäten – beispielsweise in Form von Hochseepiraterie – können nur durch schlagkräftige Organisationen und mit einsatzspezifischer Technologie bekämpft werden. Zu Letzterer gehören auch die sehr spezifisch konzipierbaren Radio Security Solutions MultiCom und Messenger. Sie haben operativen Modellcharakter und können von Projektbeginn an genau auf ihr geplantes Szenario hin aufgebaut werden.

Casha Frigo Schmidiger | Publizistin

«Sollen Japans Soldaten im Ausland Landsleute retten?» So titelte die «Neue Zürcher Zeitung» vom 26. Januar 2013. Zehn Japaner hatten bei einem Geiseldrama in Nordafrika ihr Leben verloren. Um japanische Bürger im Ausland besser zu schützen, wollen nun die Politiker das Gesetz über die Selbstverteidigungsstreitkräfte ändern. Was sicher damit zusammenhängt, dass noch bei weiteren Anschlägen der letzten Jahrzehnte – beispielsweise «Nine-Eleven» und Luxor – zahlreiche Bürger Nippons im Ausland ihr Leben verloren haben. Die Frage kam auf, ob Japan die nötigen Instrumente habe, um seine Bürger im Ausland zu schützen und notfalls aus gefährlichen Situationen zu befreien. Gegenwärtig dürfen die japanischen Selbstverteidigungsstreitkräfte ihre Bürger nur auf dem See- und Luftweg befreien. Die Ausweitung der gesetzlichen Vorgaben ist in Planung.

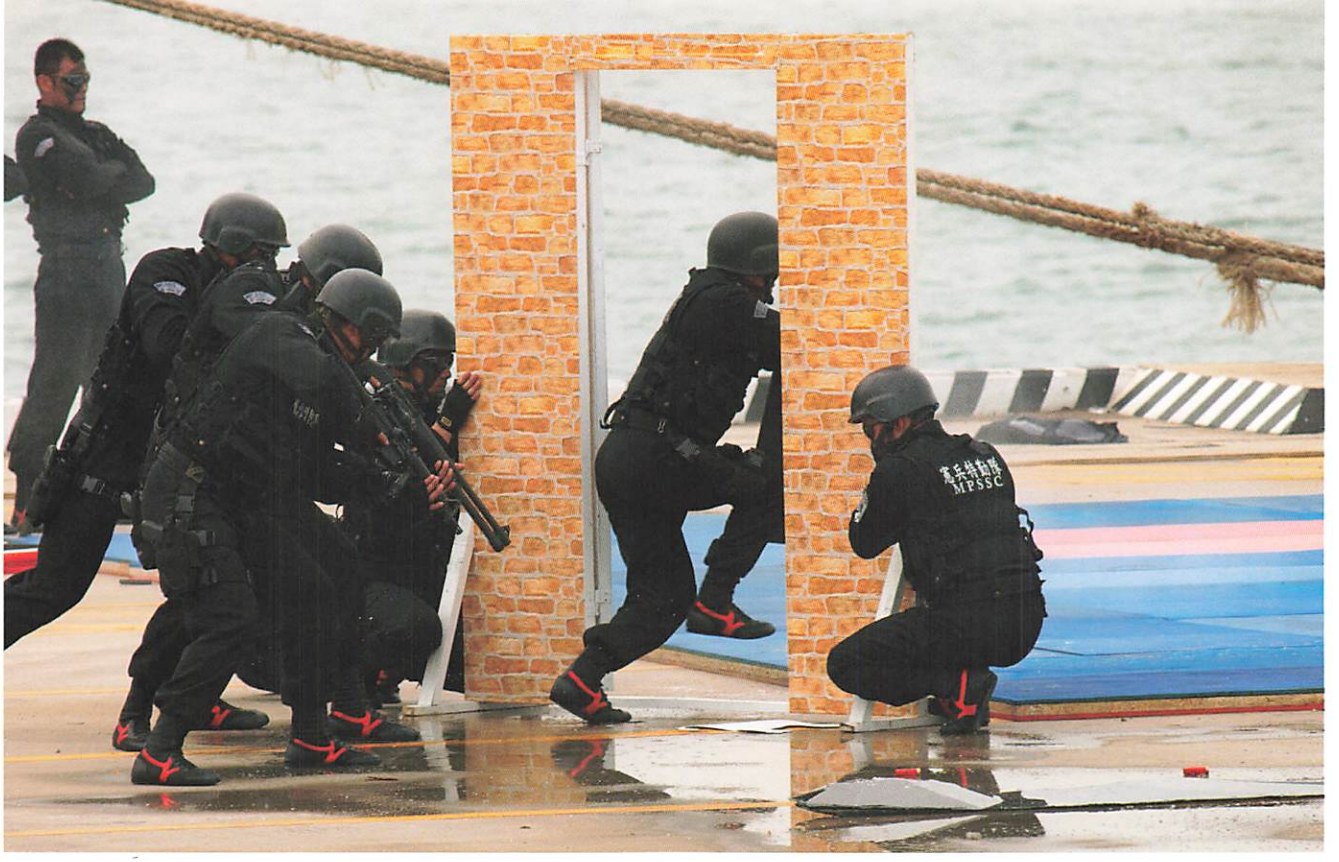
Im Prinzip tut allerdings jedes Land gut daran, sich Gedanken zu machen, wie es im Falle von Übergriffen gegen seine Landsleute reagieren soll. Nebst politischen gibt es auch militärische Optionen, die im Rahmen der Möglichkeiten geprüft werden können.

Die Gefährdung würde sich bestimmt anders darstellen, wäre nicht der internationale Terrorismus im Aufbruch. Dazu zählt naturgemäss auch die Piraterie. So gab es im 1. Quartal 2010 über 80 Piratenvorfälle. Vor allem im Golf von Aden und im südostasiatischen Raum. Hauptsächliches Ziel sind Frachtschiffe – jedoch auch Autotransporter, Chemikalien- und natürlich Öltanker und sogar Fischereischiffe.

Grassierende Seeräuberei

Stellte die Piraterie gemäss dem Center for Security Studies der ETH Zürich[1] die Piraterie lange Zeit ein lokales Problem dar, so hat sie sich seit Anfang 2008 zu einer Herausforderung für die internationale Sicherheit entwickelt. Dies hat vor allem mit der dramatischen Ausweitung des Aktionsradius der Piraten zu tun. Die Entführung von Handelsschiffen und privaten Booten ist zu einem lukrativen Geschäft geworden. Mehrfach sind Lösegelder in Millionenhöhe gezahlt worden. Der Golf von Aden gehört zu den wichtigsten globalen Transportrouten. Seit die Bedeutung des Seeverkehrs aufgrund der Globalisierung generell stark zugenommen hat, können Störungen der Verbindungswege zwischen Europa, der arabischen Halbinsel und Asien besonders gravierende Auswirkungen auf die Weltwirtschaft, die Rohstoffversorgung und die Versorgung mit Energieträgern nach sich ziehen. Die Seeräuberei verschärft auch die Situation in Somalia selbst, die vom UNO-Sicherheitsrat als «eine Bedrohung für den internationalen Frieden» eingestuft wird. Nach einer ersten NATO-Operation zum Schutz der Schiffe des UNO-Welternährungsprogramms 2008 hat die EU das Zepter übernommen und am 8. Dezember 2008 die Operation Atalanta zur Abschreckung, Prävention und Bekämpfung seeräuberischer Handlungen lanciert. Im Mai 2009 verfügte Atalanta über 13 Schiffe und drei Aufklärungsflugzeuge. Dem Projekt haben bisher Deutschland, Frankreich, Griechenland, Grossbritannien, Italien, die Niederlande, Schweden und Spanien ihre Streitkräfte zur Verfügung gestellt. Belgien sowie Norwegen werden bald hinzukommen. Kroatien und die Ukraine haben ein Engagement angekündigt.

[1] Quelle: Eidgenössische Technische Hochschule ETH Zürich, Center for Security Studies, Nr. 55, Operation Atalanta 2009



Am 29. Juni 2011 wurde im Hafen von Taipeh, Taiwan, die gross angelegte Terrorismusabwehr- und Katastrophenschutzübung Jinhua abgehalten.

Zivile und militärische Kräfte agieren im Verbund

Bei der Mission Atalanta handelt es sich also einerseits um einen gemischten multinationalen Marineverband (und die erste gemeinsame Marineoperation der EU). Gleichzeitig ist sie ein Paradebeispiel dafür, wie militärische und zivile Behörden zusammen operieren. Unter zivil-militärischer Zusammenarbeit (Civil-Military Co-Operation – CIMIC) versteht man das Zusammenwirken von staatlichen und/oder nicht staatlichen zivilen Organisationen. Materiell fallen darunter Planungen, Vereinbarungen, Massnahmen, Kräfte und Mittel, welche die Beziehungen zwischen militärischen Institutionen, zivilen Organisationen, Behörden sowie der Zivilbevölkerung unterstützen, erleichtern oder fördern sollen. Erfolgreiche Kooperationen beider Kräfte stehen indes nicht immer unter einem guten Stern. Bei Vorsorge- und Versorgungsmassnahmen für die Zivilbevölkerung in Katastrophenfällen wie beim Hurrikan Sandy in den USA oder der Bekämpfung der Feuersbrunst im Osten Australiens erfolgte zwar jeweils ein Arbeiten Hand in Hand. Auch die Zusammenarbeit zwischen Militär und zivilen Kräften im Rahmen internationaler Militäreinsätze, beispielsweise im Rahmen der Provincial Reconstruction Teams in Afghanistan, verlief problemlos. Doch treten oft massive Kompetenzstreitigkeiten auf. Wie etwa beim missglückten Befreiungsversuch des deutschen Frachters Hansa Stavanger durch die GSG-9 Deutschlands.

Oberste Priorität kommt demzufolge bei Joint Operations der Klärung der Aufgaben und der Zuweisung von Kompetenzen zu. So hiess es im erwähnten Fall, dass es sich bei der Piraterie um Kriminalität handle, welche in den Zuständigkeitsbereich der Polizei fällt. Das Militär dürfe nicht zum Vollzug sonstiger hoheitlicher Befugnisse auf hoher See herangezogen werden.

Gerade in einem solchen Fall wäre es sinnvoll, wenn das Militär subsidiäre Einsätze leisten könnte. Den Opfern der Piraterie ist es egal, ob tausende Kilometer von zu Hause auf hoher See die Polizei zuständig wäre – allerdings nur, wenn das Militär mit Marineschiffen in der Nähe überhaupt aktiv werden kann. In diesem Fall wurde in einigen Ländern eine dritte Kraft geschaffen – die Bundespolizei –, welche solche Einsätze in Zukunft führen soll. Noch immer ist es rechtlich nicht geklärt, wann und ob in Hoheitsgebieten fremder Staaten militärische Kräfte anderer Staaten aktiv werden dürfen – siehe auch den Fall Japan.

Aufrüstung im «Hardware-Bereich»

Nicht zuletzt ist es auch ein «Problem», dass dem Militär vielfach die bessere und robustere Infrastruktur zur Verfügung steht. Die zivilen Kräfte holen jedoch auf. Stichwort: Hochsee-Patrouillenboote oder OPV (Offshore Patrol Vessels). Deren Grösse, Ausstattung und Bewaffnung unterscheiden sich je nach den vielfältigen Einsatzbedingungen gegen Piraten, Terroristen oder illegale Einwanderer. Sie sind für längere Fahrten ausgelegt und verfügen zum Teil auch über Hubschrauberlandeplätze. Sie werden unter anderem zur Aufklärung, Überwachung und Sicherung im Küstenvorfeld genutzt.

OPVs sind wie gesehen eher im paramilitärischen Umfeld im Einsatz und haben für die maritime Sicherheit mehr Bedeutung als für den konventionellen Krieg zwischen Streitmächten. Sie eignen sich hervorragend für eine längere Überwachung und Präsenz im küstennahen Gebiet, verfügen jedoch demzufolge nicht über die gleichen Fähigkeiten wie die eigentliche Marine. Notwendig hingegen sind die Möglichkeiten zur Seegebietsüberwachung mittels Radar, zum effizienten Eingreifen gegen kleinere, schnelle Beiboote, oder Helikopter sowie Waffen zur Durchsetzung von Gebietsansprüchen und zur Verteidigung.

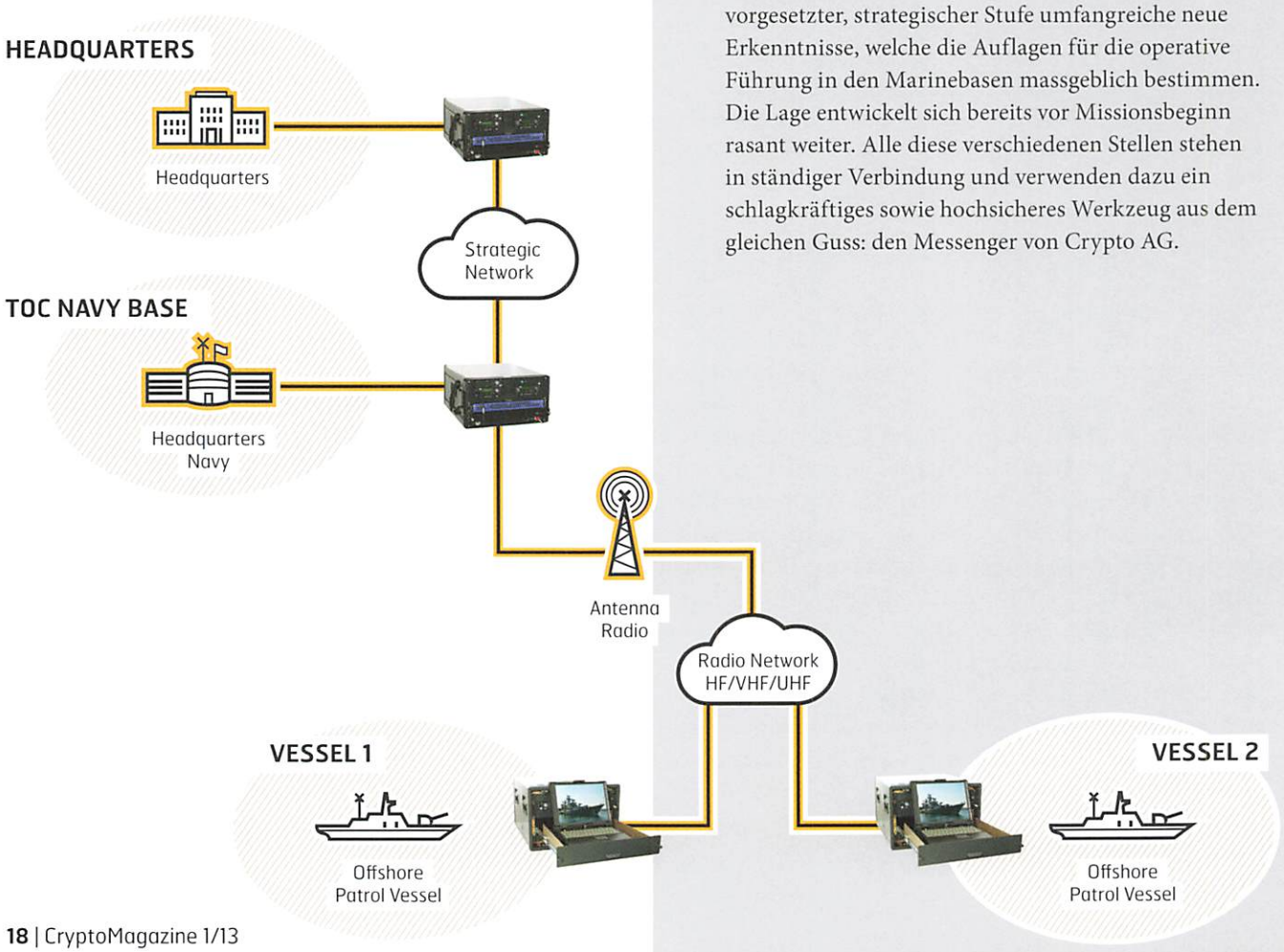
Die Kommunikation zwischen der Marinebasis und den fixen Radaraufklärungssystemen an Land – sowie zwischen der Marinebasis und dem HQ mit dem Datenserver – ist ins Bereitschaftsnetz integriert. Gerade dieses braucht einen «wasserdichten» Schutz der darauf zirkulierenden Informationen. Die Sicherheit der während des Einsatzes kommunizierten Sprach- und Dateninformationen ist für einen erfolgreichen Einsatz entscheidend. Man stelle sich vor, sie würden abgehört oder verfälscht: Dies könnte ganze Einsätze komplett vereiteln oder fehlleiten.

Militärisches Nachrichtensystem im Liveeinsatz bei unseren Kunden

Crypto AG unterstützt ihre Kunden in über 130 Ländern weltweit von der Konzipierung bis zur Umsetzung ihrer Projekte. Gerade die Analyse- und Planungsphase bei komplexen Vorhaben verlangt allen Projektpartnern viel Vorstellungskraft ab. Häufig können spätere Realbedingungen «ab dem Reissbrett» schlicht nicht erkannt werden. Das neue Demoset zum militärischen Messaging von Crypto AG schafft hier Abhilfe.

Jahn Koch | Customer Segment Manager Defence

Stellen wir uns folgendes alltägliches Szenario vor: Zwei Flottenverbände müssen zeitgleich vom Tactical Operations Center (TOC) einer Marinebasis angesteuert und in ein Einsatzgebiet gelotst werden. Sie erhalten ihre Aufträge für die bevorstehende Mission mit detaillierten Instruktionen und Zusatzinformationen etwa meteorologischer oder logistischer Natur. Dieser Wissensstand ändert sich fortlaufend, die Flotten müssen jederzeit unverzüglich in Kenntnis darüber gehalten werden. Gleichzeitig ergeben sich auf vorgesetzter, strategischer Stufe umfangreiche neue Erkenntnisse, welche die Auflagen für die operative Führung in den Marinebasen massgeblich bestimmen. Die Lage entwickelt sich bereits vor Missionsbeginn rasant weiter. Alle diese verschiedenen Stellen stehen in ständiger Verbindung und verwenden dazu ein schlagkräftiges sowie hochsicheres Werkzeug aus dem gleichen Guss: den Messenger von Crypto AG.



Kundenfreundlicher als von den Grossen

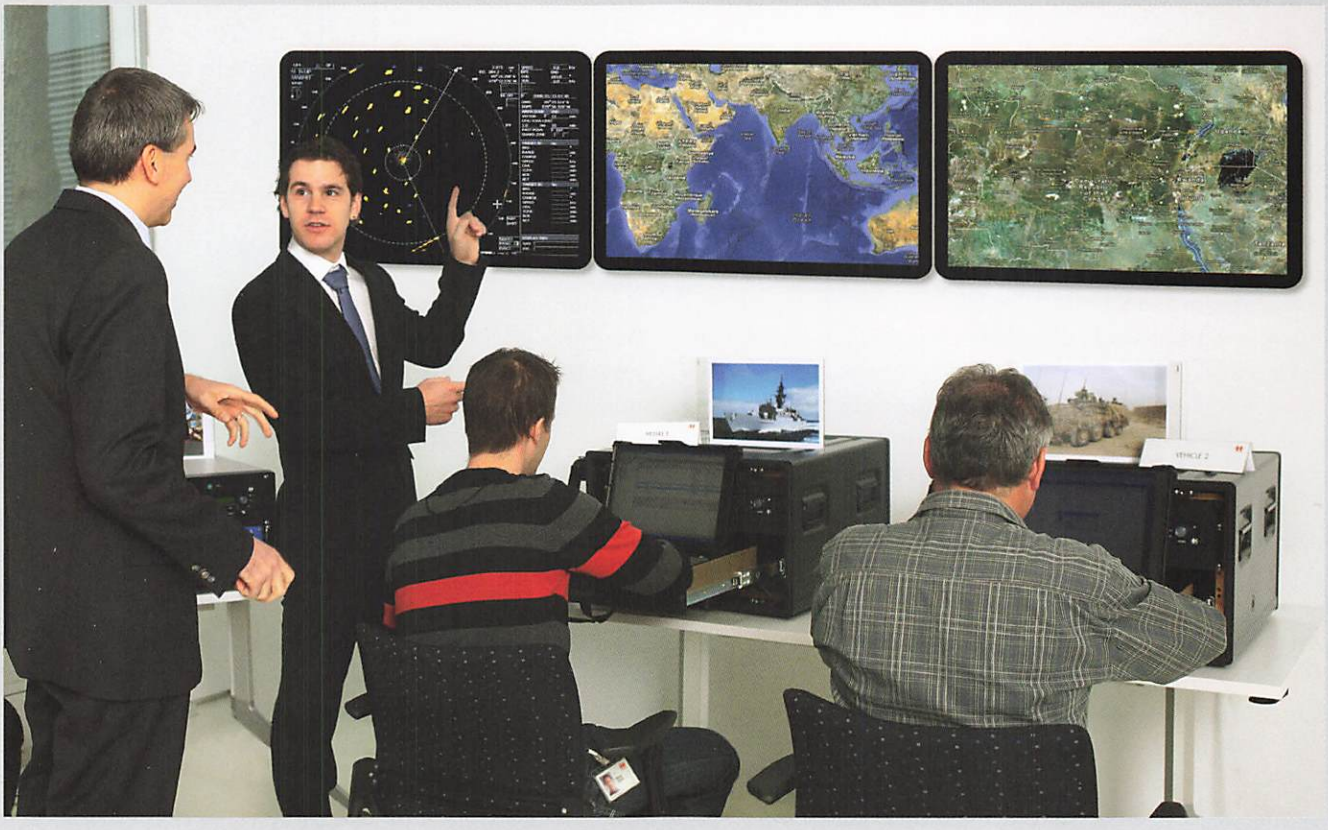
Während die landbasierten Führungsinfrastrukturen wie Hauptquartier und Marinebasen in der Regel über fest installierte IP-Netze verbunden sind, muss die Kommunikation zu den mobilen Flottenverbänden und allfälligen Nachbarstreitkräften zu Land und in der Luft mit Führungsfunk erfolgen. Diese Übertragungsarten stellen die Akteure in der Regel vor völlig verschiedene Ausgangslagen – sei es hinsichtlich der Art oder des Umfangs an Information, die innert nützlicher Frist übermittelt werden kann, sei es aufgrund der unterschiedlichen Ansprüche an verwertbare Sprach- oder Datenkommunikation. Allen Übertragungsarten gemeinsam ist der Bedarf an höchster Sicherheit: Operativ-taktische Informationen, die missionsentscheidend sind, müssen nach dem Willen vieler Kunden ebenso sicher vor fremdem Zugriff und der Manipulation durch Dritte sein wie die strategischen, deren Geheimhaltung häufig nichts weniger als die Wahrung nationaler Interessen bedeutet. Zu diesen Aspekten gesellt sich die Frage der Benutzerfreundlichkeit und der kundenspezifischen Gestaltung eines hoch automatisierten Nachrichtensystems für den Einsatz. Grosse, auf dem Weltmarkt etablierte Hersteller bieten ihren Abnehmern meist keine Lösung, die auf ihre besonderen nationalen Bedürfnisse eingehen würde oder auf ihre bewährten Prozesse zugeschnitten ist. Statt sie zu unterstützen, schwächen sie so die Effizienz der betreffenden Streitkräfte, die sich aufwendig auf das Standardsystem eines Weltmarktanbieters umschulen lassen und auf spezifisch benötigte Anwendungen weitgehend verzichten müssen.

Von Anfang an mit dem lebensechten Modell arbeiten

Der Messenger von Crypto AG ist demgegenüber einfach in der Bedienung, kann optimal auf die Bedürfnisse des Kunden und seines Betriebspersonals zugeschnitten werden und bietet ihm den gewohnt maximalen Schutz einer Lösung von Crypto AG.

Er verbindet die Welt der IP-Netze via Glasfaser und Draht mit derjenigen von HF- und VHF-Funk. Er schafft den nahtlosen Übergang von den zivilen Büroanwendungen der Militärverwaltung zu den taktisch-operativen Übertragungssystemen und Terminals der Einsatzverbände auf hoher See. Und das Beste: Er kann auf Kundenwunsch jederzeit im Zielland unter realistischen technischen Bedingungen aufgebaut und vorgeführt werden. Damit ist der Entscheid für den Messenger von Crypto AG nicht nur ein Entscheid für eine souveräne Kundenlösung nach Mass, sondern auch für die grösstmögliche Test- und Evaluierbarkeit eines Beschaffungsprojektes bereits ab der Planungsphase.

Üben, Erproben und Optimieren wie im Liveeinsatz: Das Demoset «Messaging» simuliert die taktisch-operative Kommunikation von Flottenverbänden und deren wirksamen Schutz.



Mit Serviceleistungen zu optimalen Sicherheitslösungen

Nie war die Sicherheit der geschäftlichen und behördlichen Informationssicherheitssysteme so wichtig wie heute – und noch nie so unterbewertet. Wie bitte? Will heissen, dass die Relevanz noch immer zu wünschen übrig lässt.

Casha Frigo Schmidiger | Publizistin

Das gesamte Informationssystem einer Organisation ist sowohl von innen als auch von aussen bedroht. Bedrohungen können durch verschiedene Bedienfehler entstehen oder durch Dritte, die Unmengen an Zeit und Geld dazu verwenden, um in ein System einzudringen. Jüngst wieder passiert beim Industriekonzern Lockheed, der erneut Opfer von Attacken wurde, ebenso das britische Aussenministerium. Nicht umsonst hat die Europol das neue Abwehrzentrum für Cyberkriminalität EC3 gegründet, welches aufgrund internationaler Zusammenarbeit nun mit den Angreifern Schritt halten will und muss.

Das Verstehen der Risiken in Verbindung mit dem Zugang zu diesen Informationen und deren Schutz kann eine echte Herausforderung darstellen. Unternehmen haben meist den nötigen Schritt von der klassischen IT-Sicherheit zur umfassenden Informationssicherheit noch vor sich. Oft denken Führungsverantwortliche, dass es sich bei beiden Begriffen um Synonyme handelt. Was so nicht zutrifft. Der springende Punkt ist, dass eine Behörde perfekte IT-Sicherheitsmassnahmen eingerichtet haben kann, diese allerdings nur schon durch eine böswillige Handlung eines Administrators lahmgelegt werden kann. Denn das Risiko ist oft nicht technikgemacht, sondern auf «menschliches Versagen» oder mangelhafte Überwachung der Prozesse zurückzuführen. IT-Sicherheit macht nur 50 % der Informationssicherheit aus. Letztere umfasst immer auch physische Sicherheit, Personalmanagement und die Implementierung von überprüfbaren Sicherheitsprozessen. Der Zweck der Informationssicherheit besteht darin, ein System aufzubauen, welches sämtliche Risiken abdeckt. Und hier setzt der ADBO-Gedanke der Crypto AG ein.

Analyse, Design, Build und Operate (ADBO) einer Informationssicherheitslösung
Das heisst, die stets gleichzeitige Prüfung und Anpassung des People-, Process- und Technology-Verfahrens. All diese Punkte umfassen die Lösungen der Crypto AG.

Die Crypto AG setzt zunehmend auf globale und umfassende Sicherheitslösungen – angefangen bei der Analyse mit Security Assessments bis hin zur Implementation und Abwicklung des Projektes inklusive periodischer Systemüberprüfung gemäss vertraglicher Basis. Das Angebot an Services und Dienstleistungen hat nochmals bedeutend mehr Gewicht im gesamten Leistungsspektrum erhalten. Bei integralen Systemen beträgt der Serviceanteil vielfach bis zu 50 %. Bei Drittkomponenten (Firewalls oder Datenschleusen) kommen vertrauenswürdig geltende Drittanbieter von ICT-Komponenten zum Zug. So kann die Crypto AG zunehmend als Generalunternehmer Komplettlösung aus einer Hand anbieten.

Im Folgenden wird das Serviceverständnis der Crypto AG aus der Optik von vier Personen dargestellt, die täglich damit konfrontiert sind.

Mike Rohrer, Service Designer, mit einem Gesamtüberblick

Um eine Informationssicherheitslösung zu implementieren, braucht es ein Maximum an Kompetenz in Bezug auf die verwendeten Technologien und Protokolle. Denn mit der Auslieferung der Crypto-Lösungen und -Systeme ist es nicht getan. Wir wollen sicherstellen, dass deren Integration optimal verläuft und die verantwortlichen Anwender optimal auf die Systeme geschult sind. Zudem soll die Verfügbarkeit der verwendeten ICT-Funktionen in keiner Weise tangiert sein – damit sich die Nutzer weiterhin auf ihre Tagesgeschäfte konzentrieren können.

Von der Analyse bis zum After Sales Support und Training
Im Grundsatz hat der neue Crypto-Bereich Security Services und Solutions zum Ziel, den Kunden beim erfolgreichen Zusammenspiel von Mensch und Prozess optimal zu unterstützen. Dieser fusst auf den Säulen «Consulting Services»,

Mike Rohrer,
Service Designer

den «Implementation Services», den «Education Services», dem «Operational Support Services» sowie dem «Lifecycle Management Service». Mit den **Crypto Consulting Services** holen sich die Sicherheitsverantwortlichen des Kunden Expertenwissen ins Haus und können überprüfen, ob ihre organisatorischen Abläufe keinem Sicherheitsproblem Vorschub leisten und ob ihre Prozesse professionell geplant sind. Mit den **Crypto Implementation Services** stellen sie sicher, dass ihr Security System in heterogenen Umfeldern und unter Einbezug höchster Sicherheitsstandards und in Übereinstimmung mit ihrer Zielsetzung implementiert wird. Die mit dem Gütesiegel der «Premium Class» versehene Crypto Academy mit ihrem ganzheitlichen Schulungsansatz – zusammengefasst unter den Crypto Education Services – befähigt sie, den Anforderungen an die gestiegene Bedrohungslage zu begegnen und die Crypto-Produkte gezielt zu konfigurieren und einzusetzen. Mit den **Crypto Operational Support Services** können die Sicherheitsverantwortlichen auf eine Rundumbetreuung für ihre installierten Produkte und Lösungen zurückgreifen – wenn erforderlich über eine vertraglich vereinbarte Lebenszyklusdauer.

Wir erklären diese Thematik gerne mit der Analogie des Hausbaus: Ein ICT-Security-Projekt besteht ebenso aus verschiedenen Phasen und deren Aktivitäten. In der Need-Phase weiss man, dass man ein neues Haus bauen will, jedoch sind die Vorstellungen noch sehr vage. Genau so beginnt auch der Prozess bei unseren Kunden. Der Kunde weiss, dass etwas gemacht werden muss, die Umsetzung ist für ihn jedoch unklar. Deshalb sucht er einen starken Partner, der ihm diese Unsicherheiten nehmen kann. Somit muss man sich sowohl beim Hausbau als auch beim Aufbau einer Sicherheitsarchitektur eine Strategie, ein Grobkonzept und deren Absicht festlegen, um die entsprechende Vorgehensweise zu definieren. Die Crypto AG unterstützt Sie, um bei diesem Bild zu bleiben, beim ganzen Prozess – vom Legen des Fundaments bis zum Innenausbau.

Christof Eberle, Head of Customer Projects, zu den Implementation Services

Worin bestehen die Implementation Services der Crypto AG?
Unsere Unterstützungsleistungen erstrecken sich von der ersten Idee (dies in Zusammenarbeit mit der Abteilung Bid Management unter Markus Baumeler) bis zur Übergabe des schlüsselfertigen, sicheren Informations- und Kommunikationssystems. Bei komplexen Projekten agiert ein zuständiger Projektmanager als Anlaufstelle und koordiniert den Arbeitsfortschritt mit den kundeneigenen Experten. Somit hat der Auftraggeber die Gewissheit, dass sein System rechtzeitig, budgetgemäss und übereinstimmend mit seinen Technologie- und Sicherheitszielsetzungen realisiert wird. Der Implementation der Sicherheitsfunktion und demzufolge auch dem Sicherheitsmanagement muss dabei die nötige Aufmerksamkeit geschenkt werden. Für die Crypto AG hat die Sicherheit bei einer Projektrealisierung in Zusammenarbeit mit den komplexen Projekten unserer Kunden oberste Priorität.

Dabei ist eine der Hauptaufgaben der Projektmanager die Sicherstellung reibungsloser Prozesse und Abläufe bei Kundenprojekten und -anfragen sowie die Gewährleistung des Informationsflusses vom Markt zurück an die Crypto AG. Wir übernehmen Verantwortung für das Projekt. Das Motto unserer Arbeit ist und bleibt «Security first».

Wie gestaltet sich die Kooperation mit dem Kunden? Bei welchen Projekten tritt die Crypto AG als Turnkey Provider auf, bei welchen als Supporter?
Zunächst halte ich fest, dass wir keine Tätigkeiten vornehmen, bei welchen wir mit den Sicherheitsschlüsseln der Kunden in Berührung kommen. Trotz allen benötigten Einblicke in das System und Netzwerk. Bei rund zwei Dritteln der Projekte nehmen wir die Rolle des Supporters ein. Hier liegt die Hauptverantwortung beim Kunden und wir unterstützen ihn im Engineering und in der Implementation unserer Systeme und Solutions. Bei einem Drittel sind wir hingegen als Turnkey Provider tätig und implementieren ein Projekt bis zur Übergabe. Bei jedem Projektbeginn wird je ein Projektleiter des Kunden und des Lieferanten benannt. Diese sind für den reibungslosen Ablauf des Projektes verantwortlich. Das Projekt muss die abgemachte Sicherheit, die definierte Funktionalität in der geforderten Zeit, zu den vereinbarten Kosten erfüllen. Beide Projektleiter sind primäre Ansprechpartner in den jeweiligen Organisationen. Sie stehen je einem Projektteam vor, das die geforderten Leistungen gemäss dem obigen Ablauf erbringt und aus verschiedenen Fachspezialisten zusammengesetzt ist.

Christof Eberle, Head of
Customer Projects

David Herzig, IT Security Education and Training Engineer

Inwiefern ist die Leistung der Crypto AG einzigartig?
Jedes auf Informationssicherheitssysteme spezialisierte Unternehmen kann ein solches Projekt realisieren, wir jedoch setzen kompromisslos auf Höchstsicherheit. Dies ist nicht immer kompatibel mit Einfachheit und zieht eine gewisse Komplexität beim Einbau unserer Systeme in die Kundennetzwerke nach sich – geht jedoch nicht auf Kosten der Geschwindigkeit des Betriebes. Die Implementierung von Höchstsicherheit mag auf den ersten Blick aufwendiger erscheinen als eine standardisierte Lösung, das Resultat rechtfertigt jedoch allen Aufwand. Zudem haben wir mit unserem Know-how und unserer über 60-jährigen Erfahrung in Hochsicherheitsprojekten diese «State of the Art»-Methoden mit sicherheitsrelevanten Aufgaben und Prozeduren erweitert und an die verschiedenen Kundenanforderungen adaptiert.

Welche Rolle spielt die Technologie, welche der Mensch?
Es geht schlussendlich darum, in ein bestehendes Netzwerk ein vollständig kompatibles Sicherheitssystem zu implementieren. Das läuft nach international gültigen Prozessstandards ab, die wir für unsere Hochsicherheitslösungen adaptiert haben. Die technologische Herausforderung bei solchen Systemen ist, die Sicherheit, die Anbindung an verschiedenste Übertragungskanäle, die Funktionssicherheit und gute Bedienbarkeit sowie das einfache Management unter «einen Hut zu bringen». Allerdings sind auch die Befähigung des Betriebs- und Wartungspersonals und dessen sicherheitsrelevanten Arbeitsabläufe häufig Schlüsselkriterien für die erfolgreiche Umsetzung eines grösseren Infrastrukturprojektes. Ohne Projektleiter und seine Mitarbeiter auf der Höhe ihrer Aufgabe ist dies unmöglich. Deshalb haben wir für die einzelnen Projekte hoch spezialisierte Mitarbeiter. Der für die Durchführung gewählte Crypto-Mitarbeiter muss dabei nicht nur über das theoretische Wissen, sondern auch über die praktische Erfahrung bei der Implementation von Hochsicherheitsprojekten verfügen.

David Herzig, neuer IT Security Education and Training Engineer, zur Ausbildung im zertifizierten Trainingscenter

Kundenprojekte durchlaufen bei Crypto AG das ADBO-Phasenmodell und es liegt nahe, dass dieses Modell im hauseigenen Training ebenfalls zum Einsatz kommt. Meist ist es im Vorfeld nicht möglich abzuklären, welche Vorkenntnisse, Trainingsanforderungen oder Zielsetzungen die Teilnehmer haben. Ebenso wenig ist klar, ob der Kunde bereits alle Anforderungen an seine Infrastruktur im Vorfeld geklärt, ein Design der Solllösung erstellt hat, und in welcher Form er gedenkt, die Produkte oder Systemlösungen von uns zu installieren und zu warten. Häufig fehlt dem Kunden das Verständnis für Bedrohungen, einer übergreifend notwendigen Security Governance und der konkreten Umsetzung in einem Security Process Framework. Solche Fragen müssen zu Beginn eines Trainings adressiert werden und haben einen grossen Einfluss auf den Ablauf und die Involvierung von weiteren Experten. Jedes Training ist ein eigenständiges Projekt und individuelle Trainings finden je nach Wunsch einmal oder in wiederkehrenden Abständen (in der Schweiz oder beim Kunden) statt und sind modular aufeinander aufbauend abgestimmt. Wenn Kunden unser Training besuchen, ist dies ein Zeichen der Wertschätzung und häufig Teil der Karriereplanung. So ist es nicht verwunderlich, dass Trainees nach einem absolvierten Training und einer erfolgreichen Implementation in ihrem Land befördert werden.

Falls im Training zuerst das Kundensystem entworfen werden muss – Phase Design –, müssen wir uns intensiv mit der lokalen Situation und deren Anforderungen befassen. Allfällige Inkompatibilitäten, Schnittstellenproblematiken oder Sicherheitszonenübergänge müssen erkannt und gleich zu Beginn angegangen werden. Die Phase Build kann je nach Kunde in einem Training/Workshop bei uns simuliert werden oder findet direkt beim Kunden statt. Eine Komponente, die ebenso zu unserem Prozessverständnis zählt und unsere Kundenorientierung widerspiegelt. Unter Operate verstehen wir die Anwendung und Wartung unserer Crypto-Systeme. Diese können ebenfalls vertieftes Troubleshooting und Maintenance beinhalten.

Welches sind Ihre Ziele in der Ausübung Ihrer neuen Tätigkeit, was wollen Sie erreichen?
Ganz wichtig ist für mich, die bestehenden Werte weiterzuführen. Zusätzlich möchte ich unser Ausbildungsangebot klarer, strukturierter und nutzenorientierter gestalten, die Kundenbindung stärken, die Lernprozesse verschlanken und die Feedback-Kultur vertiefen.

Integraler Bestandteil unserer Aufgabe ist auch die interne Schulung – gerade von neuen Mitarbeitenden. Zu diesem Zweck bilden wir uns auch selbst laufend weiter aus. Produkt- und Systemkompetenzen erwerben wir in enger Kooperation mit dem Produktmanagement.

Wie sieht die Ausbildung im Detail aus?
Die Ausbildung soll unseren Kunden erlauben, sich ein profundes Wissen sowie die nötigen Qualifikationen für die Tätigkeit eines Sicherheitsbeauftragten anzueignen. Nicht nur das Vermitteln von Lerninhalten, sondern auch das Durchführen von Analysen und die Identifikation von wirksamen Strategien stehen im Zentrum der Ausbildung. Dabei werden sowohl Sicherheitsmassnahmen auf physischer als auch auf organisatorischer (Arbeitsabläufe) und auf kryptologischer Ebene (Chiffrierung) betrachtet.

Die Lehrgänge sind modular aufgebaut und lassen sich dem Wissensstand der Teilnehmer beliebig anpassen, damit die Wissensvermittlung in kurzer Zeit und nachhaltig erfolgen kann. Nach Abschluss der Ausbildung erhalten die Absolventen ein Diplom.

Alan Gibson, Maintenance Manager, zum Lebenszyklus-Management

Eine der Herausforderungen, welcher man beim Lebenszyklus-Management gegenübersteht, betrifft die Frage, wie man mit dem sich immer schneller entwickelnden Fortschritt der Technologie mithalten kann. Dies lässt sich gut anhand von Mobiltelefonen erklären. Vor noch nicht langer Zeit kaufte man ein Mobiltelefon für die nächsten drei bis vier Jahre. Heutzutage werden jedoch bessere und schnellere Modelle in so kurzer Zeit auf den Markt gebracht, dass man bereits nach einem oder zwei Jahren das Bedürfnis hat, sich ein Gerät der neuen Generation anzuschaffen, um von den neusten Entwicklungen profitieren zu können. Dass sich die Lebenszyklen vieler anderer Produkte in den letzten Jahren stark verkürzt haben, können wir ebenfalls bei den Laptops oder Computern beobachten.

Die Crypto AG ist immer auf der Suche nach innovativen Prozessen, um die Lebenszyklusübergänge der verschiedenen Produkte, Systeme und Technologien für die Kunden so einfach wie möglich zu machen. Eine Möglichkeit ist, dass man die Zeitspanne definiert, für welche Ersatzteile erhältlich sein werden ab dem Zeitpunkt, an dem die Produkte gekauft werden. Auf spezifische Bedürfnisse kann jedoch auch mit unkonventionelleren Methoden eingegangen werden, wie dies beispielsweise vor Kurzem für einen Kunden mit einem Militärnachrichtensystem gemacht worden ist. Die genaue Planung des Lebenszyklus war hier speziell wichtig, weil dieses System auf der PC-Technologie basiert, wo die Lebenszyklen viel kürzer sind als in anderen Bereichen. Keiner will ein Kommunikationsterminal kaufen, dessen Prozessoren auf dem technologischen Stand sind, wie er vor drei oder vier Jahren geherrscht hatte. Wenn Produkte mit PC-Technologie für Kunden attraktiv sein und bleiben sollen, müssen solche Produktspezifikationen deshalb häufiger aktualisiert werden als diejenigen für andere Crypto-Produkte. Dies hat zur Folge, dass Kunden, die ein hohes Mass an Autonomie benötigen, Ersatzteile verschiedener Generationen für dieses Produkt kaufen müssen. Dies wirkt sich auch auf die Art und Weise aus, wie mit ihrer Hardware- und Softwarekompatibilität umgegangen werden muss.

Im betreffenden Angebot wurde festgehalten, dass eine gewisse Anzahl ältere Geräte innerhalb eines festgelegten Rahmens kontinuierlich ersetzt würden. Da so nur Hardwareteile ersetzt werden mussten (und nicht Hard- und Softwareteile), konnte Crypto AG diese Option zu einem substanziell tieferen Preis anbieten, als wenn man ganze Geräte hätte ersetzen müssen. Diese «Ersetzen statt Reparieren»-Methode bietet zudem weitere Vorteile. So kann die Anzahl der benötigten Ersatzteile vor Ort reduziert werden, da so das Reparieren meist nicht mehr auf Modulebene stattfindet, sondern auf Gerätebene. Dies erlaubt nicht nur, die Aufwendungen für die Ersatzteilbeschaffung und die Kosten für die Bewirtschaftung des Ersatzteillagers zu reduzieren, sondern erleichtert auch die Logistik, da es mit diesem System auf Modulebene weniger Hardwarevariationen gibt.

Alan Gibson,
Maintenance Manager

Die Methode «Ersetzen statt Reparieren» wird nicht für alle Kunden eine Ideallösung darstellen, da sie eine engere Kooperation zwischen den Parteien verlangt. Das Beispiel dieser Methode zeigt jedoch, wie Lösungen im Bereich von Lebenszyklen gefunden werden können, wenn man eingespielte Abläufe und Denkspuren verlässt oder wenn man Lösungen aus anderen Industriestandards auf diesen Bereich überträgt.

Allfällige Anregungen zu dieser Thematik nehmen wir sehr gerne von Ihnen entgegen.

CRYPTO

Hauptsitz

Crypto AG
Postfach 460
6301 Zug
Schweiz
Tel. +41 41 749 77 22
Fax +41 41 741 22 72
crypto@crypto.ch
www.crypto.ch

Regionale Büros

Argentinien, Buenos Aires
Elfenbeinküste, Abidjan
Malaysia, Kuala Lumpur
Sultanat Oman, Muscat
Vereinigte Arabische Emirate, Abu Dhabi