

CRYPTO MAGAZINE

N° 1 | 2018

Die Weichen
für Wachstum
sind gestellt





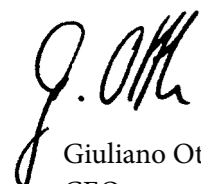
Geschätzte Leserin, geschätzter Leser

Seit der letzten Ausgabe hat sich einiges getan: Die Crypto AG hat in der Zwischenzeit das nationale und internationale Geschäft in zwei neue Gesellschaften aufgeteilt: Crypto International AG und Crypto Schweiz AG.

Was sind die Vorteile? Durch die neuen Strukturen können wir die unterschiedlichen Bedürfnisse der Schweizer und der internationalen Kunden besser bedienen und die Marktleistungen fokussiert auf die Kundenbedürfnisse ausbauen. Die Details dazu erläutern wir auf den folgenden Seiten.

Weiter zeigen wir in dieser Ausgabe auf, wie gross die Abhängigkeit von der Informations- und Kommunikationstechnologie (IKT) für Staaten, zivile und militärische Organisationen ist. Diese sind ohne die immer stärker miteinander vernetzten Systeme kaum mehr funktionsfähig.

Welche Anforderungen haben staatliche Organisationen und Armeen an die IKT? Und welche Herausforderung stellt diese «Vernetzung der Welt» für die Informationssicherheit dar? Details zu diesen Themen finden Sie in dieser Ausgabe des CryptoMagazine.


Giuliano Otth
CEO
Crypto Schweiz AG


Anders Platoff
CEO
Crypto International Group AB

3 | FOKUS

Die Crypto AG auf Wachstumskurs

6 | Informations- und Kommunikationstechnologie als Effizienztreiber

9 | Sicherheit hoch vier – unterwegs in der vernetzten Datenwelt

12 | Armeen brauchen krisensichere IKT-Systeme

14 | INTERVIEW
Die Integrität jederzeit sicherstellen

18 | Estland – das digitale Vorbild

22 | SUCCESS STORY
Hochsicherer Arbeitsplatz als Basis für effiziente Polizeiarbeit

Impressum

Erscheint 2-mal jährlich | **Auflage** | 3'750 (Deutsch, Englisch, Französisch, Spanisch, Russisch, Arabisch)

Herausgeber | Crypto International AG & Crypto Schweiz AG, Zugerstrasse 42, 6312 Steinhausen, www.crypto.ch

Redaktionsleitung | Anita von Wyl, Crypto Schweiz AG, T +41 41 749 77 22, F +41 41 741 22 72, anita.vonwyl@crypto.ch

Nachdruck | Honorarfrei mit Zustimmung der Redaktion, Belegexemplare erbeten. Copyright Crypto International AG & Crypto Schweiz AG

Bildnachweis | Crypto AG: Titelseite, S. 2, 3, 4, 5 | Getty Images: S. 9 | Jean-Paul Theler: S. 15 | Shutterstock: S. 6, 10, 12, 16, 20, 21 | Grisha Bruev/Shutterstock: S. 18 | Maciej Bledowski/Shutterstock: S. 8



Die Crypto AG auf Wachstumskurs

Die Crypto AG spaltet ihr nationales und internationales Geschäft in zwei neue Unternehmen auf. Dabei übernimmt der schwedische Cyber Security-Veteran und Unternehmer Andreas Linde die Verantwortung für das internationale Geschäft, das er mit der Crypto International Group weiterentwickeln wird. Das Schweizer Geschäft, die Crypto Schweiz AG, wird von der Unternehmensleitung unter Federführung des langjährigen CEO der Crypto AG, Giuliano Otth, im Rahmen eines Management-Buyouts zusammen mit dem ehemaligen Schwesterunternehmen InfoGuard AG übernommen.

CryptoMagazine hat mit dem Eigentümer der Crypto International Group, Andreas Linde, dem Miteigentümer und CEO der Crypto Schweiz AG, Giuliano Otth, und Anders Platoff, CEO der Crypto International Group, darüber gesprochen, mit welchem Fokus sie sich und ihre neuen Unternehmen auf das künftige Wachstum vorbereiten.

Wie kam es zu der Entscheidung, das Schweizer und das internationale Geschäft der Crypto AG aufzuspalten?

Giuliano Otth: Innerhalb der Crypto AG haben wir zwei Geschäftsmodelle mit sehr unterschiedlichen Kundenanforderungen bedient. Diese zu trennen ist der logische Schritt, um das ganze Potenzial beider auszuschöpfen. Wir können die verschiedenen Anforderungen unserer Kunden in der Schweiz und im internationalen Bereich besser abdecken, wenn wir uns stärker auf die Angebote beider Märkte konzentrieren können. Dadurch stärken wir beide Unternehmen und beide Kundengruppen.

Was bedeuten die neuen Eigentumsstrukturen für die Kunden?

Giuliano Otth: Die operative Aufteilung in die beiden neuen Unternehmen wird im Laufe des Jahres 2018 vollzogen. Dank der neuen Eigentumsverhältnisse kann sich jedes der beiden Unternehmen auf sein Geschäftsmodell konzentrieren. Beide Unternehmen können jetzt gezielt in Zukunftstechnologien und Vertriebskanäle investieren. Von der Erweiterung ihrer jeweiligen Marktangebote profitiert sowohl das Geschäft in der Schweiz als auch das internationale Geschäft. Unsere Kunden werden feststellen, dass unsere Produkte ihre Bedürfnisse noch besser erfüllen.

Andreas Linde soll das internationale Geschäft vorantreiben. Warum er?

Giuliano Otth: Andreas Linde ist ein Vollblutunternehmer und ein starker strategischer Partner mit viel Erfahrung im Bereich Informationssicherheit. Wir planen, künftig eng zusammenzu-



arbeiten, besonders bei der Produktentwicklung. Die Verantwortung für die internationalen Kundenbeziehungen geht auf die neue Crypto International AG über, eine Tochter der Crypto International Group AB. Dort wird das aktuelle Portfolio an hochsicheren Chiffrierlösungen um umfassende Lösungen im Bereich Cyber Security ergänzt. Seine Visionen für das Unternehmen und seine profunde Branchenkenntnis haben uns davon überzeugt, dass er der Richtige ist, wenn es darum geht, das internationale Geschäft zu führen und weiterzuentwickeln.

Was hat Sie an der Übernahme des internationalen Geschäfts gereizt?

Andreas Linde: Die Mitarbeitenden von Crypto International wie auch von Crypto Schweiz verfügen über ein einzigartiges Know-how, das so nirgendwo sonst zu finden ist. Die Kombination eines hochmodernen Produkt- und Dienstleistungsportfolios mit einem ausgezeichneten globalen Kundenstamm macht die Sache ausserordentlich attraktiv. Die Marke Crypto steht für höchste Sicherheit in allen Belangen, respektvollen Umgang mit der Privatsphäre unserer Kunden und deren Feedback, egal ob es positiv ausfällt oder ob Verbesserungsbedarf besteht. Auf diese Werte bin ich sehr stolz. In den Wochen seit meinem Antritt hat sich dieser positive Eindruck nur noch verstärkt. Wir bringen das Beste schwedischer Innovationskraft und Schweizer Ingenieurskunst zusammen, um unseren Kunden die beste Cyber Security anzubieten.

In welchen Bereichen sind weitere Investitionen geplant?

Andreas Linde: Im internationalen Geschäft wollen wir das Crypto-Angebot weiter stärken und ein umfassendes Cyber Security-Portfolio entwickeln, das auf die komplexer werdenden Cyber Security-Anforderungen unserer internationalen Kunden zugeschnitten ist. Zug, Schweiz, bleibt auch langfristig

der strategische Forschungs- und Entwicklungsstandort der Gruppe. Ein zweiter F&E-Standort wird in diesem Jahr in Lund, Schweden, eröffnet. So wollen wir ein wirklich internationales Cyber Security-Unternehmen schaffen. Die Gruppe wird von Anders Platoff, einer erfahrenen Führungskraft, geleitet.

Wie lautet Ihre Vision für das internationale Geschäft?

Andreas Linde: Wir haben ein neues, spannendes Kapitel einer fast 100-jährigen Geschäftstätigkeit aufgeschlagen, die in Schweden in den 1920er-Jahren begann, als der Textilingenieur Arvid Damm ein schwedisches Unternehmen für Kryptografie gründete. Ein paar Jahre später übernahm ein weiterer bekannter schwedischer Unternehmer, Boris Hagelin, das Unternehmen und machte den kleinen Betrieb zum globalen Marktführer in der Kryptografiebranche. Seitdem ist die Crypto AG in der Branche federführend. Jetzt ist für die Crypto AG die Zeit für eine neue Ära in der Unternehmensgeschichte angebrochen, um die Schweizer Identität mit unseren schwedischen Wurzeln in Einklang zu bringen und tief in die Welt der Cybersecurity vorzustossen. Im internationalen Geschäft wird das Crypto-Angebot weiter gestärkt und ein umfassendes Cyber Security-Portfolio entwickelt, das auf die komplexer werdenden Cyber Security-Anforderungen unserer internationalen Kunden zugeschnitten ist. Indem wir unsere einzigartige Expertise im Bereich höchster Sicherheit mit Cyber Security verschmelzen, schaffen wir für unsere Kunden, die verstehen, wie wichtig der Schutz ihrer Länder und Bürger gegen Angriffe ist, einen grossen Mehrwert.

Anders Platoff: Wir arbeiten intensiv an der Entwicklung umfassender Cyber Security-Lösungen der nächsten Generation, damit sich unsere Kunden sicher fühlen, mehr Kontrolle erlangen und sich auf die neuen Bedrohungen der Cyber Security

«Der Markt für Cyber Security verspricht ein starkes Wachstum. Mit den neu aufgestellten Unternehmen können wir in unseren Kernmärkten eine Spitzenposition einnehmen.»

vorbereiten können. Ziel ist es, bis Ende 2018 das erste Cyber Security-Angebot zu präsentieren. Sollten unsere Kunden in der Zwischenzeit dringende spezifische Anforderungen im Bereich Cyber Security haben, lade ich sie ein, sich umgehend mit uns in Verbindung zu setzen. Wir werden unser Möglichstes tun, um ihre Ideen und Anforderungen zu berücksichtigen.

Welche spannenden Neuigkeiten hat die Crypto Schweiz AG für ihre Schweizer Kunden?

Giuliano Otth: Mit mehr als 150 Mitarbeitenden ist die neu gegründete Gruppe aus Crypto Schweiz AG und InfoGuard AG das grösste rein schweizerische Unternehmen für Cyber Security. Neben unseren bekannten hochmodernen Chiffriersystemen können wir unseren Kunden durch den Zusammenschluss die volle Bandbreite an Lösungen und Leistungen im Bereich Cyber Security anbieten, und zwar stark auf den Schweizer Markt abgestimmt. Künftig wird das Security-Know-how, das wir uns über Jahrzehnte hinweg erarbeitet haben, auch für IoT-Anwendungen nutzbar gemacht. So möchten wir sowohl als Dienstleister für unsere Kunden als auch als Technologiepartner für Unternehmen aus anderen Branchen eine führende Rolle übernehmen.

Mit Blick in die Zukunft haben Kunden also viel zu gewinnen. Sind in der Übergangsphase auch negative Auswirkungen zu erwarten?

Anders Platoff: Wir geben unser Bestes, um die Übergangsphase für unsere Kunden so angenehm wie möglich zu gestalten. Denn das eigentliche Ziel dieses Übergangs ist ja, unseren Kunden künftig noch bessere Leistungen anbieten zu können. Dennoch ist uns bewusst, dass in jeder Übergangsphase Schwierigkeiten überwunden werden müssen, und wir tun selbstverständlich unser Möglichstes, um sicherzustellen, dass wir unsere Kunden nicht über Gebühr strapazieren.

Sollten in der Übergangsphase doch einmal Probleme auftauchen, können unsere Kunden sicher sein, dass sowohl Giuliano als auch ich bereitstehen, um diese schnellstmöglich zu lösen.

In welchen Bereichen werden die beiden neuen Unternehmen zusammenarbeiten und voneinander profitieren?

Giuliano Otth und Anders Platoff: Beide Unternehmen möchten auch künftig eine enge Partnerschaft unterhalten und zusammenarbeiten. Bei der Entwicklung von Crypto-Produkten streben wir eine enge Kooperation an. Beide Unternehmen werden das gesamte Crypto-Produktportfolio anbieten, auch wenn die Schwerpunkte sicherlich auf die Bedürfnisse der jeweiligen Märkte zugeschnitten sind.



Andreas Linde

Der Unternehmer Andreas Linde ist Eigentümer und Vorsitzender des Verwaltungsrats der Crypto International Group AB mit Sitz in Lund, Schweden. Linde verfügt über langjährige Berufserfahrung in der Cyber Security-Branche. Ende 2015 gründete Andreas Linde Famco, ein Unternehmen, das als externer Dienstleister für Regierungsorganisationen schlüsselfertige Projekte im Bereich Cyber Security umsetzt.

Bis 2015 war Linde CEO des schwedischen Unternehmens Advenica, das von seinem Vater in den frühen 1990er-Jahren gegründet wurde. Linde hält das grösste Aktienpaket am IT-Sicherheitsunternehmen Advenica, das verschiedene zertifizierte Cyber Security-Lösungen für Regierungen und Organisationen im Bereich kritischer Infrastrukturen anbietet. Im Jahr 2000 war Andreas Linde Mitbegründer von 4C Strategies, einem Unternehmen, das Lösungen im Bereich Risikomanagement anbietet und Kunden beim Aufbau von Know-how in den Bereichen Risikomanagement, Krisenmanagement und Business Continuity Management unterstützt.

Linde ist Unternehmer aus Leidenschaft mit der Fähigkeit, langfristig erfolgreiche Unternehmen aufzubauen. Seine umfangreiche Erfahrung in den Bereichen Cyber Security und Informationssicherheit erstreckt sich auch auf die Geschäftsentwicklung in dieser Branche.

Linde ist 43 Jahre alt, verheiratet und Vater von zwei Töchtern im Alter von 3 und 4 Jahren.

Informations- und Kommunikationstechnologie als Effizienztreiber

Staat, Wirtschaft und Gesellschaft sind stark von der Informations- und Kommunikationstechnologie (IKT) geprägt. Deren Fortschritte haben sich in den vergangenen Jahrzehnten als Triebfeder für die Modernisierung von Behörden und der dazugehörigen Prozesse erwiesen. Um mit der technologischen Entwicklung Schritt halten und auch davon profitieren zu können, bedarf es einer Strategie, welche der Informationssicherheit Rechnung trägt.

Eine Welt ohne Computersysteme ist heute unvorstellbar. Wie stark die Informations- und Kommunikationstechnologie die Gegenwart prägt, ist im Alltag immer dann spürbar, wenn einmal ein System ausfällt. Funktionieren etwa die Zahlterminals in den Läden nicht, bilden sich vor den Kassen lange Schlangen. Fällt an einer Strassenkreuzung die Steuerung der Lichtsignale aus, kann der Verkehr zeitweilig komplett zum Erliegen kommen.

Ungleich schwerer wiegen Störungen und Pannen bei Systemen auf einer höheren Schutzbedarfsstufe. Je kritischer ein System für das Funktionieren von Prozessen ist, desto deutlicher zeigt sein Ausfall, wie abhängig Staat, Wirtschaft und Gesellschaft heute von der Informations- und Kommunikationstechnologie – kurz IKT oder englisch ICT – sind. Das Spektrum reicht dabei von behördlichen Verwaltungsprozessen, industriellen Fertigungsmaschinen bis hin zu IT-Systemen für die Steuerung in Kernkraftwerken.

IKT-Durchdringung weitet sich aus

In den vergangenen Jahren und Jahrzehnten ist die Bedeutung von IKT-Systemen kontinuierlich gestiegen. Die Rede davon war erstmals Ende der 1970er-Jahre und zu Beginn der 1980er-Jahre, als im Fernmeldewesen im etwas grösseren Stil damit begonnen wurde, digitale Informationen zu übermitteln. Mit der Übertragung digitaler Informationen begannen die traditionelle Informationstechnik (IT) und die Kommunikationstechnik schrittweise näher zusammenzurücken. Inzwischen sind die einst separaten Technologien unumkehrbar miteinander verschmolzen.

Die IKT umfasst im Wesentlichen drei unterschiedliche Grundfunktionen:

- Die Kommunikation, das heisst die Übermittlung von Information von einem Ort zu einem anderen,
- die Speicherung von Information, also eigentlich das Festhalten von Daten von einem Zeitpunkt bis zu einem späteren, sowie
- die Bearbeitung der Information, sprich die Umwandlung von Daten anhand definierter Regeln. Letzteres könnte gemeinhin als Computer-Berechnungen bezeichnet werden.

Für Staat, Wirtschaft und Gesellschaft ist Informations- und Kommunikationstechnik essenziell. Ohne IKT-Systeme sind sie schlicht nicht mehr funktionsfähig. Die Abhängigkeit ist im Laufe der Zeit deutlich angestiegen – parallel zur immer stärkeren Vernetzung der einzelnen Systeme. Die Vorteile einer Vernetzung liegen auf der Hand: Prozesse werden vereinfacht und beschleunigt. Die IKT hat damit wesentlich zur Modernisierung aller Bereiche des Lebens beigetragen.

IKT treibt Modernisierung vorwärts

In Organisationen und im Behördenumfeld hat die IKT auch die Ausgestaltung der Prozesse an sich massgeblich beeinflusst.

Selbst einfachste Handlungen können ohne technische Systeme nicht mehr ausgeführt werden. Ein Grossteil der Informationen wird heute ausschliesslich digital aufbewahrt. Entsprechend können die Daten nur noch mit Hilfe passender Instrumente gelesen und bearbeitet werden. Verstärkt wird die Abhängigkeit dadurch, dass die Menge der Daten, die erfasst, transportiert, gespeichert und verarbeitet werden, mit dem technologischen Fortschritt enorm zugenommen hat. Die Verarbeitung und die Übertragung der heute üblichen Datenmengen sind ohne IKT undenkbar. Im Gegenzug hat die moderne IKT die grossen Datenvolumen aber auch erst geschaffen.

Es gibt keinerlei Anzeichen oder Gründe dafür, dass die technologische Entwicklung sich verlangsamen könnte oder gar ein Ende finden wird. Im Gegenteil: die Informations- und Kommunikationstechnologie dürfte weiterhin ein massgeblicher Treiber für die sich fortsetzende Modernisierung sein – Stichwort: digitale Transformation. In diesem Umfeld ist es für Unternehmen, Organisationen und Behörden unabdingbar, ihren Umgang mit der IKT gut zu durchdenken und zu planen.

In der Schweiz reichen die ersten Bestrebungen, den Umgang mit IKT zu planen, ins Jahr 1998 zurück. Die IKT sei ein wichtiges Mittel, den Wohlstand nachhaltig zu vermehren. Seither wurden zwei IT-Strategien formuliert. Heute steht die Schweiz inmitten der Umsetzung der Strategie (2016 – 2019), mit dem Zielbild, die IKT des Bundes langfristig gesehen

geschäftsorientierter, integraler, verlässlicher und fokussierter zu gestalten.

Für Unternehmen, Organisationen und Behörden ist es unabdingbar, ihren Umgang mit der IKT gut zu planen und die Informationssicherheit zu berücksichtigen.

Die Vision gibt die Massnahmen vor

Eine IKT-Strategie ist auch unverzichtbar mit Blick auf die Kosten. Zwar haben moderne Technologien und die Automatisierung von Prozessen massgeblich dazu beigetragen, dass in den Behörden die Abläufe und Prozesse kostengünstiger und schneller vonstattengehen. Gleichzeitig hat die IKT aber den Bedarf für die Erhebung und Auswertung gewisser Daten auch erst geschaffen. Resultat der ganzen Entwicklung sind riesige Mengen von Daten, die zu verarbeiten, speichern und pflegen sind, aber auch eine Vielzahl von Schnittstellen, die es zu verwalten und überwachen gilt. Die Kosten für IKT sind und bleiben nämlich ein entscheidender Faktor, und dies obwohl mit der technologischen Entwicklung die Preise für die physische Infrastruktur zur Bearbeitung, Übertragung und



Speicherung von Daten und Informationen kontinuierlich gesunken sind.

Angesichts der Kosten bei der Umsetzung von IKT-Projekten und des auch nicht zu unterschätzenden Aufwands für den laufenden Betrieb von IKT-Anwendungen ist die Effizienz und die Wirtschaftlichkeit wesentlicher Bestandteil einer jeden IKT-Strategie. Anzustreben ist dabei immer ein ganzheitlicher Blick, das heisst Wirtschaftlichkeit und Effizienz müssen aus der gesamthaften Perspektive bewertet werden. Zudem soll zur Bewertung von Kosten nicht nur die Dauer eines Projekts im Auge behalten werden, sondern die Aufwendungen, die während der gesamten Lebensdauer eines Systems voraussichtlich entstehen.

Alle Ansprüche berücksichtigen

Neben der Effizienz und der Wirtschaftlichkeit gibt es aber eine Vielzahl von weiteren Aspekten, die in IKT-Strategien mindestens eine ebenso hohe Beachtung verdienen. Einer davon könnte als Zweckmässigkeit umschrieben werden. So gilt es sicherzustellen, dass IKT immer auf die Ansprüche einer Verwaltungs- oder Organisationseinheit ausgerichtet ist und diese beim Erbringen ihrer Leistung unterstützt. Den Ansprüchen der Benutzer ist dabei genauso Rechnung zu tragen wie jenen von anderen Stakeholdern, namentlich Bürgerinnen und Bürger, externe Leistungsempfänger und -erbringer sowie andere Behörden. Ein Interessenskonflikt ist dabei vorprogrammiert: Wenn aus Kosten- und Praktikabilitätsüberlegungen möglichst standardisierte IKT-Lösungen angestrebt werden, können spezifische Anforderungen einzelner Verwaltungseinheiten nicht vollumfänglich erfüllt werden. Zu stark vereinheitlichte Lösungen bergen zudem die Gefahr, dass die IKT ihre Rolle als Treiberin der Effizienz nicht mehr entfalten kann.

Besonderes Augenmerk bei IKT-Strategien gehört der Informationssicherheit. Diese ist der Schlüssel dazu, einen kontinuierlichen störungsfreien Betrieb der Systeme sicherzustellen und die Sicherheit des Staates zu gewährleisten. Die Informationssicherheit ist einer der kritischen Erfolgsfaktoren, dem auch im Risikomanagement die entsprechende Aufmerksamkeit geschuldet ist. Die Auswirkungen eines Systemausfalls, eines Datenverlustes oder auch eines Datendiebstahls können schliesslich gravierend sein.

Zwar hängt die Grösse der Risiken immer auch von den jeweils involvierten Stellen ab, eine Vernachlässigung der Informationssicherheit kann für einen Staat in vielen Bereichen aber geradezu verheerend sein. Es gilt daher, bereits in der Strategie für den Umgang mit IKT den entsprechenden Themenfeldern den nötigen Raum einzuräumen. Wenn es um die Wahrung der Vertraulichkeit und Integrität von Daten geht, das heisst den Schutz vor unberechtigtem Zugriff und Veränderung, dann darf Wirtschaftlichkeit nicht mehr wichtigstes Kriterium sein.

Nach einem Stromausfall muss die Verkehrsregelung gewährleistet werden



Sicherheit hoch vier – unterwegs in der vernetzten Datenwelt

Die Welt steuert in Richtung Hypervernetzung. Mit der zunehmenden IT-Durchdringung steigt auch der Schutzbedarf der dahinterstehenden Systeme sowie der zirkulierenden digitalen Informationen. Die Crypto SmartProtect-Technologie trägt dieser Entwicklung Rechnung. Sie ermöglicht es, auf einem Gerät bis zu vier vollständig isolierte Sicherheitszonen zu betreiben, so dass sensible Daten jederzeit umfassend geschützt sind.

Informationen und Menschen sind heute schneller unterwegs als je zuvor. Bereits haben sich etliche Anwendungen und Tätigkeitsfelder aus ihrer örtlichen Verankerung gelöst und sich in den Cyberspace verlagert. Wegen der dort lauenden Gefahren ist es zwingend, die Systeme der Informations- und Kommunikationstechnologie (IKT) so zu konzipieren, dass sicherheitskritische Komponenten, Prozesse, Schnittstellen und Informationen jederzeit zuverlässig geschützt sind.

Permanenter Wandel steigert Verwundbarkeit

Die moderne IKT bietet grosses Potenzial für Standardisierungen. Dieses Potenzial soll so weit wie sinnvoll ausgeschöpft werden, gibt etwa die IKT-Strategie der Schweizer Eidgenossenschaft vor. Selbstredend lässt sich bei der Fachvielfalt im

Behördenumfeld nie eine durchgehende Standardisierung erreichen. So kommen in der Schweiz aktuell bis zu 6'000 unterschiedliche Fachapplikationen zum Einsatz. Diesen spezifischen Bedürfnissen verschiedener Anspruchsgruppen gilt es gerecht zu werden. Erschwerend kommt hinzu, dass die Zahl vernetzter Systeme und Geräte laufend zunimmt – eine Entwicklung, deren Konsequenzen heute noch kaum abschätzbar sind. Fest steht: Die Digitalisierung hat die Verwundbarkeit insgesamt vergrössert. Selbst Regierungen und Organisationen mit gut ausgebautem IT-Schutz wurden in jüngster Vergangenheit Opfer von Cyberattacken. Mehrfach war es Angreifern gelungen, fehlkonfigurierte Infrastrukturkomponenten oder zu spät identifizierte Schwachstellen auszunutzen, um Zugang zu sensiblen Daten zu erhalten.

Die Gewährleistung der operativen Sicherheit verbunden mit maximaler Benutzerfreundlichkeit ist eine zentrale Herausforderung, die es zu meistern gilt. Dabei muss auch berücksichtigt werden, dass die Strukturen des Internets permanentem Wandel unterliegen. In hohem Tempo ermöglicht der technische Fortschritt neue Anwendungsmöglichkeiten, die es in bestehende IT-Infrastrukturen zu integrieren gilt. In naher Zukunft dürften vermehrt auch noch IT-fremde Komponenten wie Internet of Things, kurz IoT, hinzukommen. Zudem eröffnet die Erfassung und Verknüpfung riesiger Datenmengen (Big Data) bisher unbekannte Möglichkeiten.

Die Gewährleistung der operativen Sicherheit verbunden mit maximaler Benutzerfreundlichkeit ist eine zentrale Herausforderung, die es zu meistern gilt.

Sicherheitsrisiken aus der Welt schaffen

Bereits etabliert hat sich die flächendeckende Verwendung mobiler Technologien. Effizientes Arbeiten ist heute ohne Einbezug mobiler Geräte nicht mehr möglich. Die sichere Vernetzung von stationären und portablen Systemen ist zu einem der wichtigsten Erfolgsfaktoren geworden. Dazu müssen jedoch IKT-Infrastrukturen zur Verfügung stehen, die grenzenlose Kommunikation und uneingeschränkte Zusammenarbeit – Unified Communication and Collaboration, kurz UCC, – ermöglichen und sicherstellen. Anwender brauchen jederzeit und überall Zugriff auf ihre Daten und Dokumente: seien es öffentliche Informationen oder solche, die der Geheimhaltung unterliegen. Diesen gilt es, besonderes Augenmerk zu widmen, speziell wenn sensible Daten situationsbedingt in einem Netzwerk oder mit einzelnen Partnern geteilt werden müssen.

Ein Beispiel: Wird ein Bürger eines Staates im Ausland entführt, ist bei der Lösungsfindung in der Regel das Außenministerium des Heimatstaates der verschleppten Person federführend. Von Fall zu Fall verlangt eine derartige Operation den Einbezug von Instrumenten, die bloss auf loser Basis mit dem Außenministerium verbunden sind. Zum Beispiel externe Berater oder Einheiten der Polizei. Um sicherzustellen, dass der Austausch von Informationen in diesem Netzwerk sicher funktioniert, sind Technologien erforderlich, die parallelen Datenverkehr unterstützen.

Gleiches gilt für Operationen mit Beteiligung des Militärs: So leisten etwa die Militärs subsidiäre Einsätze, für deren Erfolg der sichere Datenaustausch ausschlaggebend ist. Dabei ist es zentral, dass die Armeespitze einerseits auf interne Informationskanäle Zugriff hat, andererseits der Informationsaustausch mit Partnern einwandfrei und sicher funktioniert.



Benutzerfreundliches Arbeiten auf einem Gerät

In derartigen Konstellationen werden üblicherweise auch Informationen unterschiedlicher Klassifizierungsstufen ausgetauscht. Dieser Austausch muss daher zwingend über vollständig voneinander getrennte Netzwerke erfolgen, weil einzig die konsequente Trennung höchste Informationssicherheit gewährleistet. Lange Zeit war dies ausschliesslich möglich, indem mehrere Geräte zum Einsatz gekommen waren. Eine solche Handhabe ist jedoch nicht mehr zeitgemäss. Sie widerspricht einerseits heutigen Benutzeranforderungen und kostet andererseits wertvolle Zeit.

Bis zu vier Benutzerumgebungen – eine Arbeitsstation

Mit der Crypto SmartProtect-Technologie werden die genannten Hürden übersprungen. Sie ermöglicht eine sichere Informationsverarbeitung auf einem einzigen Endgerät. Der Anwender erhält die Möglichkeit, mit bis zu vier vollständig isolierten Sicherheitszonen (Compartments) zu arbeiten. Mit den zwei Standard-Compartments wird einerseits der Zugang zum Internet (Klassifizierungsstufe Public) möglich gemacht. Andererseits werden im zweiten Compartment die Anwendungen betrieben, die für die Bearbeitung interner Informationen benötigt werden (Klassifizierungsstufe Intern). Weiter ermög-

licht die Crypto SmartProtect-Technologie auch Lösungen mit weiteren Compartments: ein drittes Compartment für vertrauliche Dokumente (Klassifizierungsstufe Vertraulich) und ein viertes Compartment für Daten und Applikationen, die als geheim klassifiziert sind (Klassifizierungsstufe Geheim).

Je nach Bedarf können für die Compartments unterschiedliche Restriktionen definiert werden. Beispielsweise kein Druckeranschluss oder USB-Stick-Gebrauch auf der Klassifizierungsstufe Geheim (viertes Compartment). Im zweiten Compartment stehen diese Möglichkeiten dem Anwender jedoch offen. Der Vorteil dieser Lösung liegt darin, dass der Benutzer in seiner vertrauten Benutzerumgebung arbeiten kann und in einer Krisensituation nicht auf ein System zugreifen muss, welches selten bedient wird.

Endgeräte im Visier

Zu wissen, was nötig ist, um Sicherheitsanforderungen zu erfüllen, ist eine Sache – entsprechend zu handeln, eine andere. Wenn Mitarbeitende jedoch über Endgeräte verfügen, die es ihnen ermöglichen, sich in gewohnten Benutzerumgebungen in voneinander isolierten Sicherheitszonen zu bewegen, werden

die Risiken für sensible Informationen konsequent aus der Welt geschafft. Dies ist insofern wichtig, als jüngst vermehrt die Endgeräte ins Visier der Hacker geraten sind und als «Sprungbrett» genutzt wurden, um in weitere Ebenen eines IT-Systems einzudringen.



Armeen brauchen krisensichere IKT-Systeme

Im digitalen Zeitalter gilt es für Armeen mehr denn je sicherzustellen, dass ihre Souveränität unangetastet bleibt. Vertrauenswürdigkeit, Integrität und Verfügbarkeit der Kommunikationskanäle müssen lückenlos unter Kontrolle sein. Diese IKT-Systemsicherheit zu garantieren, ist eine Herausforderung, welche zunehmend an Bedeutung gewinnt, da Sie essenziell ist für die Einsatzfähigkeit.

Eine Armee muss jederzeit und in allen Situationen einsatz- und handlungsfähig sein. Hierbei spielt die Kommunikation innerhalb der Truppe und die sichere Weiterleitung von Informationen eine entscheidende Rolle. Die Führungsunterstützung durch moderne IT-Mittel wird dabei immer wichtiger. Gerade in Krisensituationen muss die vertrauliche Kommunikation funktionieren. Sensible Informationen dürfen unter keinen Umständen in falsche Hände geraten oder manipuliert werden können. Informationen und Lageberichte müssen auch Jahre nach der Mission vertraulich bleiben.

Durch die rasante technologische Entwicklung steigen Informationsdichte und deren Anforderungen an die Verfügbarkeit der Information. Mit der erhöhten Verfügbarkeit steigen auch die Anforderungen an die Informationssicherheit. Gerade Sensoren und Effektoren im Feld – beispielsweise Drohnen, Bodycams oder Radar – liefern heute hochauflösende Bildinformation, welche nach einer höheren Bandbreite der Transportsysteme verlangt. Im taktischen Feld kann dabei auf moderne IP-Radios, Satellitenkommunikation oder militärische Mobilkommunikation 3G oder 4G zurückgegriffen werden.

Feste Netzwerkstrukturen stützen sich derzeit auf Mikrowellen-Netzwerke und vermehrt auch auf schnelle Glasfaserleitungen.

Bislang laufen oft noch verschiedene ältere Systeme parallel, welche auf unterschiedlichen Programmiersprachen und Technologien aufgebaut sind. Zudem werden die Daten meist isoliert und dezentral gespeichert. Das Problem der veralteten Technik ist insgesamt, dass diese zu wenig Integration und Bandbreite für die neuen Anforderungen an umfassende Echtzeit-Führungsinformation liefert.

Handlungsfähigkeit gewährleisten

Damit die Handlungsfähigkeit einer Armee in einem Krisenfall nicht eingeschränkt wird, müssen die Systeme resistent gegen Angriffe von aussen sein. Die Härtung und der Schutz dieser krisensicheren Netzwerke und Rechenzentren wird durch physische Härtung sowie entsprechende Verschlüsselungen und Absicherung der Information erreicht. Zur Verschlüsselung der Kommunikation und Absicherung der Netzwerke bieten die Crypto International AG und die Crypto Schweiz AG verschiedene Lösungen, die den entsprechenden Bedürfnissen

Die Unabhängigkeit des militärischen Netzes ist von grösster Wichtigkeit

gerecht werden. Diese bauen auf der Crypto-Sicherheitsarchitektur auf. Angriffe werden dadurch immer mit den stärksten zur Verfügung stehenden Sicherheitsmassnahmen abgewehrt. Für die Verbindung von Standort zu Standort schützen Crypto cProducts die Information bei der Übermittlung auf Informationslevel mithilfe der Kryptografie (logisch/kryptografisch) gegen Attacken.

Spätestens seit Snowden ist allgemein bekannt, dass relevante Systeme auch innerhalb des Grundnetzes separiert werden sollen, um damit eine Zonierung der Information zu erreichen. Beispielsweise wird das Radarsystem der Luftwaffe gegenüber der Telefonie, gegenüber einem biometrischen Zutrittssystem und gegenüber einem Führungsunterstützungs- und -informationssystem logisch/kryptografisch voneinander separiert. Damit ist garantiert, dass im Störfall, aber auch bei bewusster Manipulation kein zonenübergreifender Informationsaustausch stattfinden kann. Zu guter Letzt wird für einen Teil der Informationen eine End-zu-End-Verschlüsselung gefordert. Hier kommen Lösungen für den End-User zum Einsatz, bei welcher Sprache, Papierdokumente oder elektronische Dokumente bis zur höchsten Geheimhaltungsstufe sicher übermittelt werden können.

Ziel einer Armee ist es, autonom zu sein und sich in Notsituationen nicht von zivilen Anbietern abhängig zu machen. Dieses Denken in Krisenszenarien garantiert auch, dass die gesicherten Netzwerke als Verbindungen zwischen dem Militär und der Regierung sowie zu Betreibern kritischer Infrastrukturen (Kernkraftwerke oder Flughäfen) fungieren, sodass eine Grundversorgung in Krisensituationen einwandfrei funktioniert. Oft sind Systeme untereinander stark vernetzt, um eine optimale Lagebeurteilung und Szenarioplanung zu ermöglichen. Für das Lagebild werden umfassende Informationen zu einer Mission gesammelt und zentral aufbereitet. Dies dient der optimalen Vorbereitung, effektiven Einsatzführung und im Nachhinein als Dokumentation.

Die Armee im 21. Jahrhundert

Viele Armeen gehen derzeit den Schritt ins 21. Jahrhundert. Ein wesentlicher Teil der Modernisierung ist die Gewährleistung der Systemsicherheit. Dazu gehören auch die Überwachung von Netzen und das Erkennen von Cyberattacken auf IKT-Systeme sowie allenfalls die Auslösung notwendiger Gegenmassnahmen

Neben neuen Rechenzentren soll oftmals auch ein eigenständiges Telekommunikationsnetz etabliert werden, welches die verschiedenen Systeme zu einem Netzwerk zusammenführt. Alte Kupferkabel- und Richtfunknetze werden durch Glasfaser abgelöst. Zwischen vielen einzelnen Standorten ist dadurch eine verschlüsselte Datenübertragung möglich. Von diesem Netz soll aber nicht nur die Armee, sondern es sollen auch zivile Organisationen mit sicherheitsrelevanten Aufgaben davon profitieren. Dank der Lösungen der Crypto International AG und der Crypto Schweiz AG können sogar Infrastrukturen gemeinsam genutzt werden, die aber gleichzeitig hochsicher und voneinander getrennt betrieben werden können.

Damit die Handlungsfähigkeit einer Armee im Krisenfall nicht eingeschränkt wird, müssen die Systeme resistent gegen Angriffe von aussen sein.

Mit der Umstellung der Technik der Netzwerke auf den neuesten Stand können, unabhängig von privaten Telekommunikationsanbietern, sowohl Sprache als auch Daten vom festen und geschützten Transportnetz der Armee über die teilmobilen und mobilen Komponenten bis hinaus ins Feld übermittelt werden. Ein weiteres Ziel der Modernisierung von IKT-Systemen besteht in der Reduktion der Vielzahl der Systeme und der Einführung einheitlicher Plattformen.

Für das Funktionieren einer Armee ist eine reibungslose Logistik unabdingbar. Begrenzte Ressourcen wie Fahrzeuge, Truppenmaterial und Verpflegung sollen zeitgerecht und rasch bereitgehalten werden. Pharmazeutische Zentren der Armee können in Notfallsituationen Aufgaben zugunsten der Bevölkerung übernehmen und helfen, die medizinische Versorgung sicherzustellen. Diese Materialbewegungen und Leistungen der Logistik zur Unterstützung der Ressourcenplanung können ohne ERP-basiertes IT-System kaum mehr bewältigt werden. Die Einsatzfähigkeit der Armee ist gegeben, wenn die Logistik die Einsatzmittel zeit- und bedarfsgerecht bereitstellen kann. Dazu gehört natürlich die Verfügbarkeit (Planung und Vorrat der Mittel), aber auch ein funktionierender Logistikprozess inklusive der dazugehörigen IT-Logistik. Die Anbindung dieses Prozesses an krisenresistente Netzwerke erhöht die Verfügbarkeit und garantiert den Logistikprozess. State-of-the-art Technologie und gehärtete IKT-Komponenten mit entsprechendem Schutz auf dem neuesten Stand sichern hier einen effizienten Betrieb.

«Die Integrität jederzeit sicherstellen»

Die Einsätze der Armee werden heutzutage hauptsächlich durch Mittel der Informations- und Kommunikationstechnologie (IKT) unterstützt und können ohne diese nicht mehr wirksam geführt werden. Neben den vielen Vorteilen und Möglichkeiten, welche die IKT bietet, bringt dieser Einsatz aber auch neue Risiken und Gefahren mit sich, mit denen man im militärischen Umfeld sehr bewusst umgehen muss.

Welche Anforderungen stellt ein militärisches Umfeld an die IKT?

Im Vergleich zum zivilen Umfeld werden aus militärischer Sicht die Anforderungen an Robustheit, Verfügbarkeit und Informationssicherheit anders betrachtet und gewichtet. Die Armee muss ihre Aufgaben über alle Lagen und unter Berücksichtigung aller möglichen Bedrohungen erfüllen. Die IKT ist zudem im militärischen Umfeld nie Selbstzweck, sondern unterstützt die militärischen Akteure in der Erfüllung ihrer Aufgaben und Funktionen. Ich betone dies, da als Konsequenz einer fehlerhaften oder fehlenden IKT-Leistung mit grosser Wahrscheinlichkeit Personen zu Schaden kommen. Diese Aspekte definieren im Wesentlichen auch die unterschiedlichen und erhöhten Anforderungen, welche im militärischen Umfeld an die IKT gestellt werden. Konkret bedeutet dies, dass wir im militärischen Umfeld IKT-Infrastrukturen benötigen, welche über alle Lagen, sowohl nach einem militärischen Angriff als auch nach grösseren Naturereignissen oder einer grossflächigen Strommangellage noch funktionieren, sodass die notwendigen IKT-Services weiterhin genutzt werden können.

In welchen Handlungsfeldern sind die Herausforderungen am grössten? Welche Strategien erachtet die Schweizer Armee als zielführend, um jene zu meistern und wie werden diese umgesetzt?

Die Schweizer Armee hat den primären Auftrag, die Schweizer Bevölkerung zu schützen und die Integrität der Schweiz sicherzustellen. Damit will ich sagen, dass die Armee darauf ausgerichtet ist, primär innerhalb der eigenen Grenzen zu agieren. Das bedeutet ebenfalls, dass wir unsere IKT-Leistungen im Wesentlichen auch innerhalb der Schweiz erbringen und sicherstellen müssen. Die grössten Herausforderungen haben wir aktuell in den folgenden Handlungsfeldern: der sicheren und robusten Vernetzung von Systemen und Akteuren, der Sicherstellung der Bereitstellung der benötigten Informationen zur richtigen Zeit und der Cyberdefence, das heisst dem Erkennen und Abwehren von Bedrohungen im Cyberraum.

Da wir als Armee unsere Leistungen über alle Lagen, also permanent erbringen müssen, verfügen wir im Bereich der

IKT-Leistungen über eigene, gehärtete und autonom funktionierende Infrastrukturen und Systeme, welche wir mit eigenem Personal – Mitarbeitenden der Verteidigung und Angehörigen der Miliz – betreiben und nutzen können. Zudem müssen wir sicherstellen, dass unsere Mitarbeiter über das notwendige Wissen und die Erfahrung verfügen, um diese Aufgaben selbständig und autonom wahrnehmen zu können.

Mit dem Programm FITANIA sind wir aktuell daran, unsere IKT-Infrastrukturen zu erneuern und den aktuellen Anforderungen und Bedrohungen anzupassen. Das Programm beinhaltet die drei grossen Projekte für den Bau des Führungsnetzes Schweiz, die Erneuerung der Telekommunikation der Armee und den Bau der neuen Rechenzentren. Im Weiteren hat der Chef des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (kurz: VBS), Bundesrat Guy Parmelin, den Aktionsplan Cyberdefence genehmigt. Mit dessen Umsetzung werden im Departement die Rahmenbedingungen geschaffen, damit die Armee auch in diesem Bereich die geforderten Leistungen erbringen kann.

Der rasante technologische Fortschritt bedingt laufend Anpassungen der IKT-Landschaft. Wo steht die Schweizer Armee allgemein und im Vergleich zum Ausland?

Der technologische Fortschritt macht auch vor der Schweizer Armee nicht halt. Im Gegensatz zur zivilen Welt werden aber die Bedürfnisse in der militärischen Welt, insbesondere in der Schweiz, nicht von den technologischen Trends und Möglichkeiten getrieben, sondern von neuen, sich verändernden Bedrohungen und den daraus resultierenden Bedürfnissen. Selbstverständlich werden auch im militärischen Umfeld neue Technologien und die darauf basierenden Produkte eingesetzt. Dies geschieht im Sinne der Nutzung dieser neuen Möglichkeiten für die Unterstützung der Erfüllung der militärischen Bedürfnisse und Aufträge.

Die Schweizer Armee hat mit ihrem Milizsystem einen gewichtigen Vorteil. Unsere Soldaten beziehungsweise die Angehörigen der Armee wachsen heute mit dem technologischen Fortschritt auf. Für sie ist die Nutzung dieser

Technologien und Produkte nichts Aussergewöhnliches. Auf der anderen Seite wird der Einsatz moderner Systeme immer komplexer und erfordert eine starke und kompetente Berufsorganisation mit Spezialisten, welche diese Systeme konfigurieren, warten und instand halten, damit diese dann durch die Truppe (Angehörige der Miliz) eingesetzt werden können. Die grosse Herausforderung hierbei ist, dass wir für die Gewinnung dieser IKT-Spezialisten der Berufsorganisation am Schweizer Arbeitsmarkt mit den anderen grossen zivilen IT-Unternehmen konkurrieren.

Der Integrität und Authentizität der Daten kommt eine wesentliche Bedeutung zu.

Der Trend zeigt vielerorts in Richtung Standardisierung von IKT-Strukturen und -Prozessen. Trifft dies auch auf das Militär zu?

Korrekt, dies trifft auch auf das militärische Umfeld zu. Eine Standardisierung ist notwendig, um insbesondere die Interoperabilität mit den militärischen und zivilen Partner sicherzustellen. Seit dem zweiten Weltkrieg finden militärische Einsätze meistens im Verbund mit anderen Armeen oder bei der Bewältigung grösserer Naturereignisse mit zivilen Einsatzkräften statt. Damit man gemeinsam erfolgreich sein und zusammenarbeiten kann, war es notwendig, eine gemeinsame Sprache zu finden und Abläufe, Prozesse und auch Schnittstellen zu definieren. Insbesondere für die Zusammenarbeit der Partner in der westlichen Welt war diese Arbeit von Bedeutung, was zu einem grossen Effort im Bereich der militärischen Standardisierung von Strukturen und Prozessen bis hin zu einer grossen Anzahl an technischen Standards geführt hat. Ohne Standardisierung wäre die Nutzung der heutigen Technologien, zum Beispiel der Telekommunikationstechnologien, gar nicht möglich. Dies gilt übrigens auch für die zivile Welt.

Welche Bedrohungsszenarien schliessen eine durchgängige Standardisierung von vornherein aus? Und: Welchen Hauptrisiken sind die IKT-Systeme der Armee grundsätzlich ausgesetzt?

Grundsätzlich dient die Standardisierung primär der Sicherstellung von Interoperabilität und Zusammenarbeit. Damit fördert sie aber auch die Transparenz. Das heisst, ein potenzieller Angreifer weiss, wie ich etwas tue und kann somit auch besser planen, wie er mich angreifen und verletzen kann. Auf der anderen Seite ist es aber auch so, dass, wenn ich ein standardisiertes Verfahren, beispielweise ein bestimmtes Protokoll einsetze, ich auch besser weiss, wo Schwachstellen und Risiken sind. Ich kann folglich je nach Bedrohungslage geeignete Massnahmen ergreifen, um diese Risiken zu minimieren oder sogar zu eliminieren. Wichtig ist, dass ich die Risiken kenne, welche mich bei der Erfüllung meiner Aufgaben



Jean-Paul Theler studierte Volkswirtschaft an der Universität Lausanne. Danach erwarb er einen Master in Science in Wirtschaftsmathematik an der London School of Economics and Political Science und den Dokortitel (oec. publ.) an der Universität Lausanne. 1996 trat Jean-Paul Theler in das Instruktioncorps ein und war in verschiedenen Funktionen, unter anderem der höheren Kaderausbildung und als Chef der militärischen Doktrin, eingesetzt. Als Chef Personelles der Armee wurde er zum Brigadier befördert. Ab dem 01.01.2013 bis zum 31.12.2017 führte er als Divisionär die Führungsunterstützungsbasis und war in der Armee verantwortlich für Leistungen im Bereich der Informations- und Telekommunikations-Technologie sowie der elektronischen Operationen.

Im Rahmen der Umsetzung der Weiterentwicklung der Armee ist er seit dem 01.01.2018 Projektleiter Unterstützungskommando. Basierend auf dem Entscheid des Parlaments über die Organisation der Armee wird das Unterstützungskommando die aktuellen Aufgaben der Führungsunterstützungsbasis und der Logistikbasis der Armee zusammenführen.



Auch Soldaten verwenden immer mehr technische Hilfsmittel

behindern können oder sogar bewirken, dass ich meine Aufgabe nicht mehr wahrnehmen kann. Wenn ich diese Risiken kenne und mir dann überlege, welchen Bedrohungen und Gefahren ich ausgesetzt bin, dann kann ich geeignete Massnahmen ergreifen, um diesen Gefahren auszuweichen oder sie zu bannen. Wie bereits ausgeführt, dienen die IKT-Systeme der Unterstützung der Erfüllung der Aufgaben der Armee. Kurz zusammengefasst kann man sagen, die IKT-Systeme der Armee dienen dem Generieren, Verarbeiten, Speichern, Transportieren und Präsentieren von Daten beziehungsweise Informationen. Darauf basierend kann man sagen, es gebe grundsätzlich die beiden folgenden Risiken: Einerseits das Risiko, dass Informationen verloren gehen, also nicht mehr nutzbar sind, und andererseits, dass die Funktionsfähigkeit meiner Systeme beeinträchtigt oder zerstört ist. Konkret sind dies Risiken aus dem Cyberraum:

- Datenabfluss oder das Beeinträchtigen softwarebasierter Funktionen und Prozesse,
- menschliches Fehlverhalten, wie das absichtliche Einbauen von Fehlern oder Angriffspunkten in Software (Backdoors),
- bewusstes Manipulieren von Daten und Prozessen,
- physische Bedrohungen durch Naturgewalten und kinetische Gewalten (Erdbeben, Explosionen, Waffenwirkungen, usw.),
- Ausfall der Energieversorgung (elektrische Energie oder Wasser).

Damit will ich aufzeigen, dass für die IKT-Systeme der Armee nicht nur die Risiken im Cyberraum von grosser Wichtigkeit sind, sondern dass andere Risiken gleichwertig sind. Dies ist ein wesentlicher Unterschied zu der Wahrnehmung der Risiken im zivilen Umfeld.

Welche Bedeutung kommt dabei konkret der Informationssicherheit zu?

Die Informationssicherheit ist von grosser Bedeutung, primär natürlich der Schutz der Daten beziehungsweise der Informationen. Im militärischen Bereich wird mit dem System der Klassifizierung von Informationen – GEHEIM, VERTRAULICH, INTERN – eine Struktur geschaffen, welche auch die Stossrichtungen bei der Handhabung der Information prägt. Massnahmen für den Schutz der Informationen auf Stufe GEHEIM beginnend auf der Ebene der IKT-Infrastrukturen bis hin zu den Prozessen der Handhabung sind umfassender und restriktiver als auf der Stufe INTERN.

Daneben kommt auch der Integrität und Authentizität der Daten eine wesentliche Bedeutung zu. Die Entscheide eines Kommandanten basieren auf den Informationen, welche ihm zur Verfügung stehen. Gelingt es beispielsweise einem Gegner die Informationen zu manipulieren, dann kann auch ein Entscheid stark beeinflusst werden. Daraus resultiert, dass die Grundvoraussetzung für die Informationssicherheit integre und funktionierende IKT-Mittel sind.

Welchen konkreten Bedrohungen ist die Informationssicherheit aus Ihrer Sicht am meisten ausgesetzt?

Aus Sicht der Armee können folgende grundsätzliche Bedrohungen unterschieden werden: Erstens der Abfluss von Information, zweitens das Zerstören beziehungsweise Verhindern des Zugriffs auf Information und drittens das Manipulieren oder Korumpieren von Informationen. Mit dem «Stehlen» von Informationen will die Gegenseite zu Informationen gelangen (z. B. Planungsunterlagen, Zugriffsinformationen wie Passwörter, Zertifikate), welche ihr eine Informationsüberlegenheit

verschaffen und den Zugriff zu IT-Systemen erlauben, um dann die Systeme zu übernehmen oder zu manipulieren. Mit dem Zerstören oder Verhindern des Zugriffs auf Informationen wird versucht, den Einsatz von Mitteln des Gegners zu verunmöglichen. Wenn beispielsweise verhindert werden kann, dass Bilder einer Aufklärungsdrohne in die Einsatzzentrale gelangen, kann ein Waffeneinsatz verunmöglicht werden. Mit dem Manipulieren von Informationen und Daten können weiter falsche Entscheide erwirkt oder auch Systeme zum Absturz gebracht werden.

Die aktuellen Richtlinien der Armee verbieten die Vernetzung von privaten Geräten mit den IKT-Infrastrukturen von Armee und Verwaltung.

Technologien wie das Internet of Things (IoT) stecken noch in den Kinderschuhen, werden Geräte in Zukunft aber direkt miteinander kommunizieren lassen. Wo steht die Armee in Bezug auf das IoT? Oder: Wo sehen Sie das grösste Potenzial für das IoT im militärischen Umfeld?

Das IoT ist wie viele andere Themen ein Hype, welcher im militärischen Umfeld nicht von direkter Bedeutung ist. Betrachtet man hingegen das Thema in allgemeiner Form, nämlich in der Vernetzung vieler verschiedener IT-Ressourcen und der direkten Kommunikation dieser Ressourcen untereinander, dann ist dies sicherlich auch im militärischen Umfeld von Bedeutung.

Im militärischen Umfeld spricht man dabei auch vom Sensorto-Effector-Loop, also der Vernetzung der Sensoren mit den Effektoren in einem mehr oder weniger automatisierten Prozess. Heute ist es noch so, dass der Mensch in diesem Loop die zentrale und primäre Intelligenz darstellt und somit die Entscheide fällt. Auch wird der Soldat an der Front mit immer mehr Sensoren ausgerüstet, welche die Daten direkt und autonom an zentrale Kommandostellen übermitteln. Die konsolidierten Informationen werden dann wieder dem Soldaten übermittelt und erlauben einen effizienteren Einsatz der Waffen vor Ort. Im Trend der Reduzierung der Exposition des Menschen als sehr verletzlich und schwächstes Glied an der Front, wird die Automatisierung dieses Loops in Zukunft verstärkt werden. In meinen Augen ist es aber von zentraler Bedeutung, dass beim Waffeneinsatz der Mensch immer den finalen Entscheid fällt und damit seine Verantwortung wahrnimmt. Der vollständig automatisierte Krieg darf nicht Realität werden.

Ich gehe davon aus, dass ähnlich dem zivilen Umfeld das IoT als Technologie primär im Supportbereich eine zunehmende Bedeutung erhalten wird und beispielsweise die Logistikprozesse noch stärker automatisieren könnte.

Mit welchen Sicherheitsrisiken wird die Kommunikation dadurch konfrontiert, und wie könnte ein effektiver Schutz gestaltet sein?

Werden Prozesse durch das IoT stärker automatisiert, dann gewinnt insbesondere die End-zu-End-Sicherheit an Bedeutung. Die Anforderungen an die Sicherstellung der Authentizität und Integrität einer Information werden stark erhöht und parallel dazu wächst auch die Zahl an möglichen Angriffspunkten für einen Cyberangriff massiv. Dies muss dazu führen, dass jegliche Information so eingepackt wird, dass sie Identifikationselemente enthält, welche eine Identifizierung und Authentifizierung ermöglichen und dadurch die Integrität der transportierten Information sichergestellt ist.

Inwiefern stellen private Geräte im militärischen Einsatz ein Sicherheitsrisiko dar? Und welche Schutzmassnahmen trifft die Armee dagegen?

Private IKT-Mittel stellen im militärischen Einsatz per se ein Sicherheitsrisiko dar, weil sie für dieselben Tätigkeiten eingesetzt werden wie die funktionsgleichen oder ähnlichen militärischen Geräte, nicht aber mit denselben oder zumindest gleichwertigen Schutzmassnahmen ausgerüstet sind und eingesetzt werden.

Sicherlich muss bei der Beurteilung der Sicherheitsrisiken bezüglich der Art des privaten Gerätes und dem Einsatzort differenziert werden, aber in den meisten Fällen werden diese Geräte ja nicht isoliert verwendet, sondern sind über irgendeine Infrastruktur mit der Umwelt vernetzt. Ein klares No-Go ist die Vernetzung privater Geräte mit den militärischen IKT-Infrastrukturen, aber auch wenn sie unabhängig von den militärischen IKT-Infrastrukturen verwendet werden, sind sie ein Risiko für unkontrollierten Datenabfluss. Sie sind zudem auch ein Risiko als unkontrollierter Sensor, zum Beispiel über die Ortungsfunktion bei einem Smartphone oder dem Mikrofon oder der Kamera in einem Laptop oder einem Smartphone.

Die aktuellen Richtlinien in der Armee verbieten die Vernetzung von privaten Geräten mit den IKT-Infrastrukturen von Armee und Verwaltung. Zudem werden die IKT-Infrastrukturen mit verschiedenen Mechanismen vor dem unbefugten Netzwerkzugriff geschützt. Beim Zutritt in klassifizierte militärische Anlagen erfolgt eine Zutritts- und Gepäckkontrolle wie an Flughäfen. Die effizienteste Schutzmassnahme ist aber immer noch die Selbstdisziplin und die Kontrolle durch die Vorgesetzten und Kameraden.



Estland – das digitale Vorbild

Der kleine osteuropäische Staat Estland gilt als Digitalisierungspionier. Estland setzte früher und konsequenter als andere Länder auf die neuen technologischen Möglichkeiten. Obwohl dieser Weg nicht ohne Risiken ist, gilt Estland als Vorbild – auch beim Schutz von Daten und der IT-Infrastruktur.

Estland nutzte die Gunst der Stunde. Als das Land im Sommer 1991 von der Sowjetunion unabhängig wurde, konnte es auf der «grünen Wiese» neue staatliche Strukturen schaffen. Die jungen Politiker, die an die Macht kamen, erkannten dabei rasch das Potenzial der neuen Technologien und des aufkommenden Internets. Mitte der Neunzigerjahre starteten sie eine erste breite IT-Bildungsoffensive, in deren Rahmen alle Schulen passende Hard- und Software erhielten. Die Regierung selber arbeitet seit Ende der Neunzigerjahre papierlos.

Heute belegt Estland auf der Rangliste der Europäischen Union (EU) zur Digitalisierung der Verwaltung den ersten Platz. Kein Wunder, denn fast die gesamte Interaktion zwischen dem Staat

und seinen Bürgern kann online stattfinden. Als die drei einzigen Ausnahmen gelten Heirat, Scheidung und der Kauf eines Hauses, für die noch eine physische Anwesenheit und eine Unterschrift vor Ort erforderlich sind.

Die Estinnen und Esten nutzen die neuen Möglichkeiten. So haben bei den Europawahlen 2014 knapp 10 Prozent der Wähler über das Internet abgestimmt, bei den nationalen Parlamentswahlen im Jahr darauf waren es schon mehr als das Doppelte. Fast alle Esten geben ihre Steuererklärung inzwischen online ab. Wesentliche Teile davon werden ohnehin automatisch ausgefüllt, weil Steuerbehörden, Banken und Arbeitgeber vernetzt sind.

Als Paradebeispiel für das hohe Niveau der Digitalisierung gilt zudem der Gesundheitssektor. Seit rund zehn Jahren besteht im baltischen Land ein einheitliches System für elektronische Patientenakten, auf denen die Krankheitsgeschichten aller Bewohner gespeichert sind. Auf diese können Ärzte und Patienten gleichermaßen zugreifen. Über die E-Health-Plattform werden auch Arzttermine vereinbart, einfache Konsultationen durchgeführt und Medikamente verschrieben.

Internet als Grundrecht

Die Grundlagen dafür, dass dies alles funktioniert, wurden um die Jahrtausendwende gelegt. Damals schrieb das Parlament in Tallinn ein Grundrecht auf einen Internetzugang in die Verfassung. Und es blieb nicht bei Lippenbekenntnissen. In der Folge wurde eine solide Breitband-Infrastruktur errichtet, die regelmäßig erneuert wird. Sehr gut im relativ dünn besiedelten Land mit gut 1,3 Millionen Einwohnern, ist auch die Abdeckung mit mobilem Internet.

Laut Zahlen der EU liegt das Land bei allen Indikatoren, mit denen das Niveau der Digitalisierung gemessen wird, über dem europäischen Schnitt. So nutzen etwa 86 Prozent der 16- bis 74-Jährigen das Internet regelmässig (EU-Schnitt: 76%), 87 Prozent der Haushalte verfügen über einen Breitbandanschluss (EU-Schnitt: 80%).

Die Regierung steckt nach wie vor auch erhebliche Ressourcen in die Stärkung der digitalen Kompetenzen. In der Schule zum Beispiel ist Programmieren ein normales Fach. Das Land sieht sich ohnehin noch längst nicht am Ziel. Eine digitale Agenda 2020 ist der Fahrplan für weitere Verbesserungen.

X-Road und E-Ausweis

Rückgrat der digitalen Gesellschaft Estland ist die dezentrale Plattform X-Road, an die rund 1'000 Institutionen angebunden sind. X-Road ermöglicht einen sicheren Datenaustausch zwischen autorisierten Datenbanken, wobei zur Speicherung

auch das Blockchain-Prinzip zur Anwendung kommt. Es werden also zum Teil Datenbanksysteme eingesetzt, bei denen die Verwaltung der Daten dezentral erfolgt. Die Datensätze sind dabei durch kryptografische Verfahren miteinander verkettet.

Ausserdem besitzen alle Esten einen elektronischen Personalausweis, der mit einem Lesegerät und einer Zweifaktor-Authentifizierung zur sicheren Online-Legitimierung genutzt und für alle E-Dienste verwendet werden kann. Damit lässt sich auch elektronisch «unterschreiben». Über 90 Prozent der Bevölkerung verwendet die Karte – für staatliche Dienstleistungen über die Plattform E-Estonia, aber auch für Bankgeschäfte.

Lücken und Attacken

Das alles birgt aber auch Gefahren. Prompt wurden im Herbst 2017 Sicherheitslücken beim elektronischen Personalausweis publik. Hacker konnten an die Daten von rund 750'000 Menschen gelangen, hiess es in Medienberichten. Gemäss Fachleuten wurde dem Problem jedoch oberste Priorität eingeräumt. Selbst der Ministerpräsident äusserte sich umgehend dazu. Und innert kurzer Zeit stand eine technische Lösung bereit, mit der die Lücken geschlossen wurden.

Vor mehr als zehn Jahren machte Estland Schlagzeilen mit einer negativen Folge der Digitalisierung. Damals legten Hacker über Wochen immer wieder verschiedene Internetseiten lahm, unter anderem die Online-Plattform des Staates sowie Webseiten verschiedener Banken.

Elektronische Sicherheit wurde daher relativ früh zu einem Teil der Landesverteidigung. Die Behörden führten nach dem Angriff vor zehn Jahren ein neues System zur Sicherung der Daten ein. Ausserdem kann heute jeder Einsehen nehmen, ob und wann jemand auf seine Daten zugegriffen hat – wodurch Angriffe schnell entdeckt werden sollen.

NATO-Zentrale für Cyberabwehr

Estland wurde – wohl auch wegen des damaligen Angriffs – zu einem Pionier in Sachen Cyberdefence. Unmittelbar nach dem Beitritt zur Nato schlug es die Schaffung eines entsprechenden Kompetenzzentrums vor. Seit 2008 hat das Cooperative Cyber Defence Centre of Excellence (CCDCOE) in der Hauptstadt Tallinn seinen Sitz. Es ist eine Art Denkfabrik für Cyberdefence.

Das Schlüsseldokument der Institution ist das «Tallinn Manual», eine Sammlung von Rechtstexten zum Thema. Es gilt für manche Experten als mögliche Grundlage für die Erweiterung des Kriegsvölkerrechts im Bereich der elektronischen Kriegsführung. Das CCDCOE führt aber auch konkrete Verteidigungsübungen durch, während derer die Spezialisten der beteiligten Armeen – Nato-Länder und neutrale Staaten – sich gegen massive Cyberangriffe zur Wehr setzen müssen.

Und nicht zuletzt verfasst das CCDCOE Berichte zu einzelnen Ländern – auch zu Estland selber. Wegen des hohen Stands der Digitalisierung und entsprechender Verletzlichkeit genießt das Thema Cybersicherheit eine höhere Priorität als in den meisten anderen Ländern, heisst es darin.

Bereits die Jüngsten setzen sich intensiv mit den digitalen Hilfsmitteln auseinander



Cyber Security-Strategie

Das Land habe sich als eines der ersten bereits 2008 eine Cybersecurity-Strategie gegeben und diese 2014 erneuert, schreiben die Autoren weiter. Die Massnahmen dieser Strategie sind naturgemäss geheim. Ebenso wenig ist öffentlich, wie viel die Armee für Cyber Security ausgibt. Immerhin gibt es ein Bekenntnis, dass dieses Thema hohe Priorität genießt.

Wichtige Rolle der Partner

Experten sind sich insgesamt jedoch einig, dass Estland als Digitalisierungsvorbild taugt. Sie verweisen unter anderem auf die effizienteren und damit auch finanziell günstigeren Prozesse. Schätzungen gehen davon aus, dass das kleine Land allein dank der breiten Verankerung der digitalen Unterschrift rund zwei Prozent des Bruttoinlandsprodukts einspart.

Laut den Fachleuten müssen Staaten, die Estland nacheifern wollen, aber auch die Risiken einer solchen Digitalisierungsstrategie im Auge behalten. Der Schutz der Daten müsse auf allen Stufen adäquat erfolgen. Bei hochsensiblen Daten, die für das Bestehen des Staates zentral sind, führt dabei kein Weg an hochsicheren Informationssicherheitslösungen vorbei. Das gilt in erster Linie für die Diplomatie und die Kommunikation innerhalb der Sicherheitskräfte, aber auch für die Bereiche State Governance, Defence und Internal Security. Entscheidend ist laut den Experten dabei, frühzeitig die richtigen Partner ins Boot zu holen, die über das entsprechende Know-how verfügen.

Bei hochsensiblen Daten führt kein Weg an hochsicheren Informationssicherheitslösungen vorbei.

Öffentlich sind jedoch die Ziele. Angepeilt werden unter anderem ein schärferes Bewusstsein für Cyberattacken und verbesserte Fähigkeiten, diesen zu begegnen. Bekannt ist auch, wie die Cyberabwehr organisatorisch aufgebaut ist. Estland erhielt dabei im Bericht des CCDCOE nicht nur Lob. So wurde festgehalten, dass das oberste Cyber Security-Gremium seine Aufsichtsrolle phasenweise nicht sehr gut ausgeübt und es am entsprechenden Support von politischer Seite gefehlt habe.



Sichere Zutrittskontrolle mittels Lesegerät

Hochsicherer Arbeitsplatz als Basis für effiziente Polizeiarbeit

Polizeiorganisationen operieren häufig landesweit. Der Austausch von sensiblen Informationen muss dabei zu jeder Zeit sichergestellt sein, um handlungsfähig zu bleiben. Effiziente Polizeiarbeit setzt weiter voraus, dass unabhängig von Ort und Zeit auf klassifizierte Informationen im Core Network zugegriffen werden kann. Dabei dürfen die Vertraulichkeit, Authentizität und Integrität dieser Informationen keinesfalls gefährdet werden.

Die Anforderungen von Polizeiorganisationen sind vielfältig und die Relevanz von Informationen für deren Handlungsfähigkeit hoch. Wenn beispielsweise Polizisten bei ihrer täglichen Arbeit unterwegs sind und Kontrollen durchführen, benötigen sie Datenzugriff auf eine zentrale Stelle. Sensible Informationen wie Personendaten müssen somit zu jeder Zeit und überall schnell abgerufen, einfach bearbeitet und hochsicher übermittelt werden können, gleichzeitig soll aber auch der Zugriff auf öffentlich zugängliche Informationen möglich sein.

Informationssicherheitslösungen, die den neuen Bedrohungsszenarien mit Endgeräten als primäres Angriffsziel Rechnung tragen und sowohl innerhalb als auch ausserhalb der Organisation das Arbeiten in einer hochsicheren Umgebung ermöglichen, sind gefragt.

Die beiden Compartments können gleichzeitig betrieben werden. Die höchste Informationssicherheit ist dabei durch deren konsequente Trennung jederzeit gewährleistet.

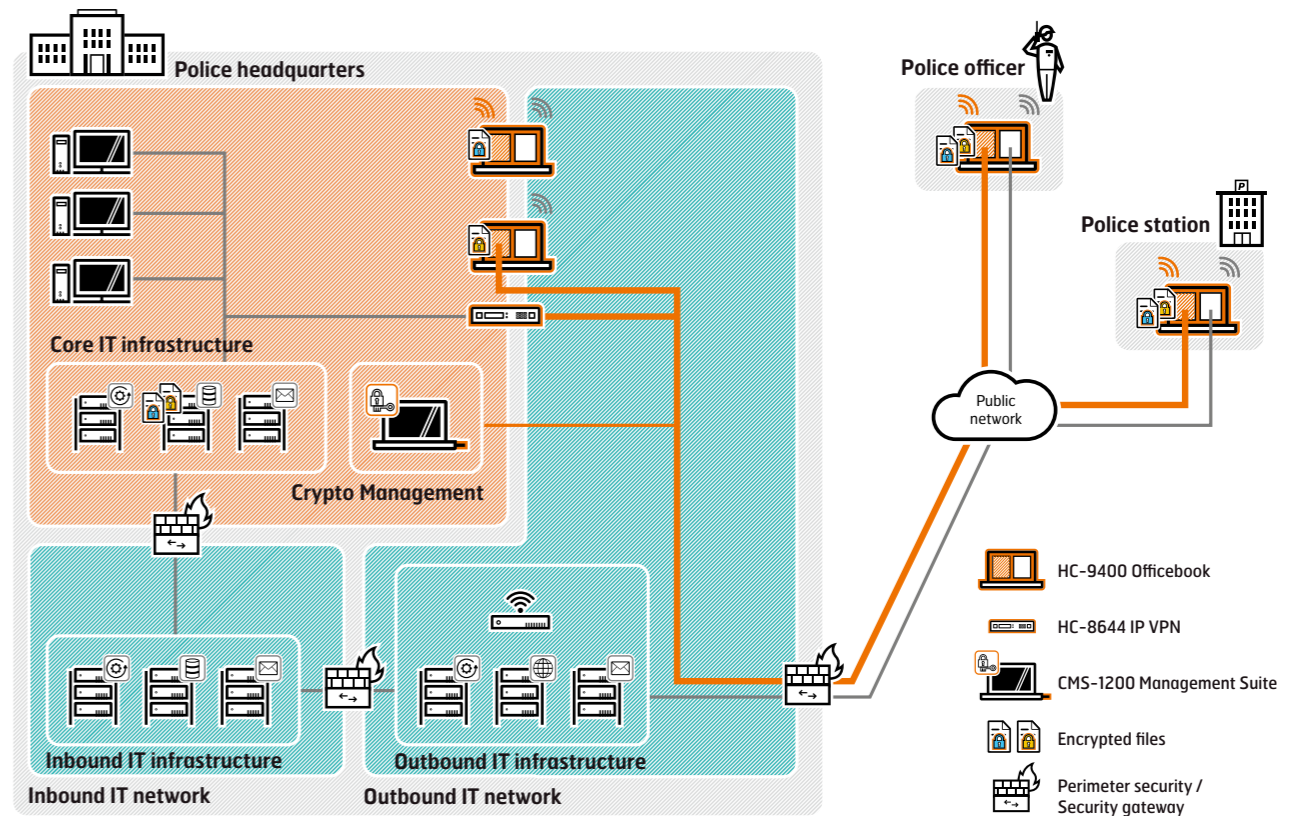
Polizeiorganisationen wollen deshalb eine Lösung, die das Arbeiten ohne Beeinträchtigung des Bedienkomforts sowie die Nutzung von gängigen Betriebssystemen wie Windows, Microsoft-Office-Applikationen und Webbrowsern ermöglicht. Mittels eines zentralen Sicherheitsmanagements sollen zudem die Kommunikationsbeziehungen und Benutzer verwaltet werden können. Auch wird nach einer massgeschneiderten Managementinfrastruktur zur Konfiguration und Verwaltung des Systems verlangt.

Die Lösung heisst cOffice Workplace

Das auf der Crypto SmartProtect-Technologie basierende System cOffice Workplace erfüllt all diese Anforderungen vollumfänglich und ermöglicht jederzeit hochsicheres und komfortables Arbeiten in vertrauter Benutzerumgebung – sowohl innerhalb als auch ausserhalb der Organisation. Das bedeutet, dass die hochsichere Kommunikation in einem flächendeckenden, landesweiten Netzwerk mit angeschlossenen Aussenstellen permanent funktioniert.

Das HC-9400 Officebook ist eine zentrale Systemkomponente des cOffice Workplace, das sich für den stationären wie auch den mobilen Einsatz eignet. Es verfügt über zwei Compartments, welche zwei vollständig voneinander getrennte Benutzerumgebungen bieten. Mit dem ersten Compartment kann auf zentrale Informationen und Applikationen der Organisation zugegriffen werden, die mittels der performanten Chiffrierlösung HC-8644 IP VPN den sicheren Zugriff zur IT-Infrastruktur der Polizeizentrale ermöglichen. Mit dem zweiten Compartment kann der Benutzer über einen Webbrowser auf öffentlich zugängliche Informationen zugreifen. Die beiden Compartments können gleichzeitig betrieben werden. Die höchste Informationssicherheit ist dabei durch deren konsequente Trennung jederzeit gewährleistet. Die Konfiguration und Verwaltung des Gesamtsystems wird mit der CMS-1200 Management Suite und dem Gateway HC-8644 IP VPN sichergestellt.

Die Crypto International AG und die Crypto Schweiz AG bieten mit cOffice Workplace kompromisslosen Schutz vor Cyberattacken.



cOffice Workplace ermöglicht sicheres und komfortables Arbeiten in sicherer Benutzerumgebung – innerhalb und ausserhalb der Organisation

Kompromissloser Schutz vor Cyberattacken

Höchste Sicherheit

Auf der Crypto SmartProtect-Technologie basierend schützt cOffice Workplace die sensiblen Informationen bestmöglich vor dem Zugriff durch Dritte, ohne den Arbeitsprozess zu beeinträchtigen.

Hohe Effizienz und Flexibilität

Für effizientes und flexibles Arbeiten können gleichzeitig zwei vollständig voneinander isolierte Benutzerumgebungen be-

trieben werden. Sensible interne Informationen sind auch dann nicht gefährdet, wenn gleichzeitig auf ein Public Network zugegriffen wird.

Maximaler Bedienkomfort

Die Benutzer können ortsunabhängig in gewohnter Benutzerumgebung arbeiten. Zudem ist der Wechsel zwischen den Compartments auf einfache Weise möglich, ohne die sensiblen Informationen zu gefährden.

Einfache Integration

Die Integration in die IT-Umgebung erfordert keine grundlegende Änderung der Infrastruktur.



Crypto International AG
Zugerstrasse 42
6312 Steinhausen
Schweiz

Crypto Schweiz AG
Zugerstrasse 42
6312 Steinhausen
Schweiz

T +41 41 749 77 22
F +41 41 741 22 72
crypto@crypto.ch
www.crypto.ch

Crypto cSeminars

cSeminar Information Security Specialists

10. bis 14. September 2018

cSeminar Contemporary Cryptography

17. bis 21. September 2018

Die Seminare finden in der Crypto Academy
in Steinhausen statt.

Kontakt und weitere Informationen unter

www.crypto.ch/seminars