CRYPTO MAGAZINE

TOTAL INFORMATION SECURITY. FÜR DIE KUNDEN DER CRYPTO AG, SCHWEIZ.

3/04

SECURITY MANAGEMENT – DIE HOHE SCHULE DER ANGEWANDTEN KRYPTOGRAFIE

LINK IN DIE GEFAHRLOSIGKEIT

GEBÜNDELTE KRISENBEWÄLTIGUNG

Liebe Leserin, lieber Leser Was verstehen Sie unter Sicherheitsmanagement? Sicherheit und Management sind zwei Begriffe, welche untrennbar miteinander verbunden sein sollen. *Sicherheit* ist der Idealzustand, bei welchem ein System in sich selbst ruht und weder aufgrund äusserer noch innerer Einflüsse aus dem Gleichgewicht gebracht werden kann. Sicherheit beinhaltet ausserdem auch alle Anstrengungen, welche unternommen werden, um solche Beeinträchtigungen gezielt abzuwehren. Und hier kommt das *Management* ins Spiel – ad Manum agere – an die Hand nehmen. Nicht umsonst wird das Sicherheitsmanagement als ein Handwerk bezeichnet.

In einer Zeit, in welcher sich die Technik und mit ihr auch die Sicherheitstechnologie in einem unaufhaltsamen Fortschritt befindet, liegt es nahe, die Sicherheit(sthematik) rein auf der technischen Ebene zu lösen respektive dieser zu überlassen. Mittels Technologie allein kann Sicherheit aber nicht erzielt werden. Denn das Verhalten spielt eine ebenso wichtige Rolle wie die Technologie. Gefragt sind eingespielte Prozesse; gefragt ist aber auch diszipliniertes Handeln. Die Wahrung der Sicherheit muss aktiv an die Hand genommen und «gemanaged» werden.

Das Sicherheitsmanagement ist als eine kontinuierliche Aufgabe zu betrachten, welche mit dem Erstellen von Sicherheitsgrundsätzen beginnt und mit der Vermittlung des Sicherheitsdenkens quer durch alle Hierarchiestufen sowie der kontinuierlichen Überprüfung dieser Grundsätze endet. Die Sicherheitsprozesse sind aufzubauen, zu steuern sowie periodisch wieder anzupassen.

Zu einem stringenten Sicherheitsmanagement zählt der Schutz der Übertragungswege zur Sicherung der darauf zirkulierenden Informationen. Dazu gehört aber auch die Klassierung der Informationen in öffentliche, vertrauliche und geheime Botschaften. Da die Zielsetzungen von Dringlichkeit und Sicherheit in der Regel immer wieder in einem Konflikt stehen, kann dies keine einfache Aufgabe sein. Was nicht mit unlösbar zu verwechseln ist, wie wir Ihnen auf den nächsten Seiten enthüllen werden.

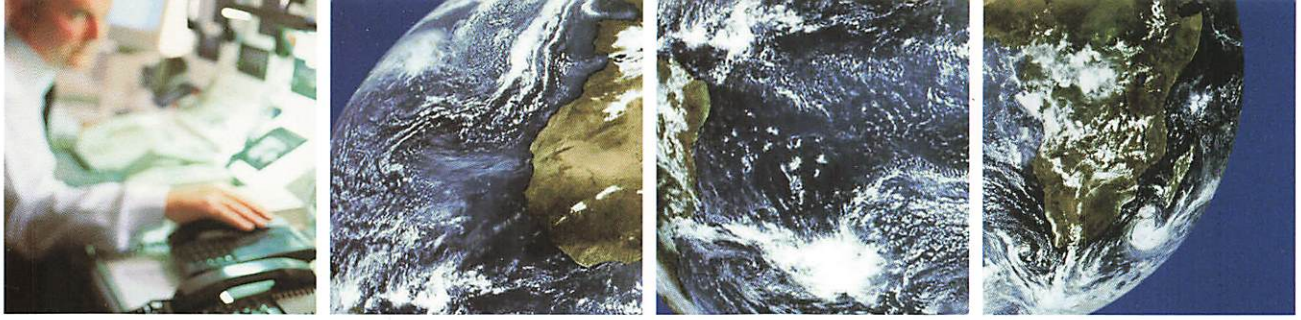
Ich möchte mich gerne an dieser Stelle im Namen der Geschäftsleitung und unserer Mitarbeiter herzlich bei allen unseren Kunden und Partnern für die entgegengebrachte Wertschätzung im Jahr 2004 bedanken. Und auch im nächsten Jahr gilt: Vertrauen ist gut – Crypto ist besser!

Giuliano Otth
President and Chief Executive Officer

Impressum

Erscheinungsweise 3-mal jährlich **Auflage** 1150 deutsch, 3750 englisch, 500 französisch, 700 spanisch **Herausgeber** Crypto AG, Postfach 460, CH-6301 Zug (Schweiz), www.crypto.ch **Redaktionsadresse** Crypto AG, Catherine Frigo, Postfach 460, CH-6301 Zug (Schweiz), Tel. +41 41 749 77 80, Fax +41 41 741 22 72, E-Mail: catherine.frigo@crypto.ch **Konzept/Layout** Heads Corporate Communication AG, CH-8032 Zürich, www.heads.ch **Druck** Druckerei Ennetsee AG, CH-6331 Hünenberg **Nachdruck** Honorarfrei mit Zustimmung der Redaktion, Belegexemplare erbeten,

Bildnachweis S. 12: Corbis; S. 4: Digital Globe; S. 18/19: Engelberg-Titlis Tourismus; Titelbild + S. 3/4/20: ESA European Space Agency; S. 12: Getty Images; S. 17: Keystone; S. 12: Prisma; S. 15: Ringier/RDB, S. 17: VBS Armeefilmdienst; S. 15: Nick Yoon, Zürich; S. 4/5/12/16: zefa blueplanet



HAGELIN-CRYPTOS
CRYPTO AG

SECURITY MANAGEMENT

DAS SECURITY MANAGEMENT – DIE HOHE SCHULE DER ANGEWANDTEN KRYPTOGRAFIE

Inhalt: Jürg Eiholzer
*Redaktion: Dr. Rudolf Meier**

Darf man in öffentlichen Netzwerken kommunizieren, ohne dass Vertraulichkeit, Integrität und Authentizität von sensiblen Informationen gewährleistet sind? Das wäre heute kaum mehr denkbar! Aber ist ebenso unbestritten, welches Niveau an Informationssicherheit es denn sein soll?

Diese Frage ist berechtigt, denn Sicherheit ist nicht gleich Sicherheit. Die Basis jeder Informationssicherheit besteht in der Chiffrierung aller Informationen, die den geschützten Bereich des Anwenders verlassen. Die dazu in der Praxis verwendeten kryptografischen Konzepte sind jedoch sehr verschieden – und sie weisen auch sehr unterschiedliche Leistungspotenziale auf. Komplexe, hochsichere Systeme sind beispielsweise für regierungsnahe oder für militärische Organisationen die Regel. Das, was solche Systeme bieten, muss jedoch letztlich auch voll nutzbar gemacht werden können. Und darüber entscheiden nicht zuletzt die Qualität und die Funktionalität des eingesetzten Security Management, also des Managements von kryptografischen Algorithmen und Schlüsseln und weiteren Parametern.

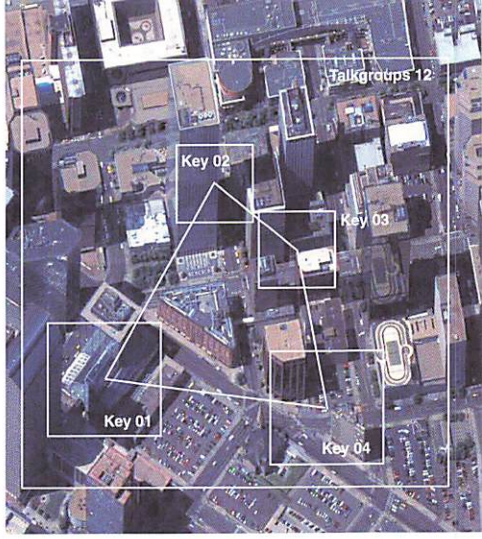
Logischerweise muss das Security Management Sicherheitsprozesse aufbauen, steuern, anpassen. Was die Sicherheit des *Gesamt*systems betrifft, sind diese Managementprozesse genauso relevant wie die kryptografischen Prozesse während der Kommunikation selber. Ein nicht nur funktionales, sondern auch hochsicheres Security Management kann jedoch keine simple Aufgabe sein, denn in der Praxis geht es oft um konkurrierende Zielsetzungen (z.B. Dringlichkeit vs. Sicherheit) und es kommt der Mensch als Benutzer – als «human factor» – ins Spiel.

Wie das Potenzial nutzbar wird

Behörden und militärische Organisationen wählen meist kryptografische Verfahren, die auf einzigartigen, gar geheimen symmetrischen Algorithmen aufbauen – wie es auch Crypto AG mit

INHALT

* Jürg Eiholzer ist Manager Security Architectures, Dr. Rudolf Meier (Forch/ZH), ist Publizist mit den Schwerpunkten Politologie, Wirtschaft und Technologie



dem TIS©-Konzept* anbietet. Dieses ist zwar mathematisch und logisch komplex, aber dafür man kann mit ihm sehr viele zusätzliche Sicherheitsfunktionen integral erfüllen und/oder optimieren. Beispielsweise mehrere «Lines of Defence» gegen Risiken errichten oder mehrere separierte Benutzerebenen («Crypto Groups») etablieren.

Ein solches Potenzial lässt sich im praktischen Alltag in der Regel nicht «im Handbetrieb» wirklich effizient und schnell umsetzen: Man benötigt dazu ein intelligentes Konzept für das Security Management. Damit kann der Anwender seine organisatorischen oder operationellen Bedürfnisse viel einfacher in seinen Sicherheitssystemen abbilden. In der Bedienung nimmt es dem Security-Manager komplizierte kryptografische Eingriffe ab, indem es die vom Anwender gewünschten Funktionen über möglichst einfache Befehle (menügesteuert am Bildschirm) zugänglich macht. Auf betrieblicher Ebene erhöht ein komfortables und flexibles Security Management ausserdem die Systemverfügbarkeit, weil Vorgänge online veranlasst werden können – es entsteht keine Leistungsbeeinträchtigung im Netzwerk.

Kontrollierte Multifunktionalität

Nimmt man das TIS©-Konzept als Referenz, benötigt hochsichere Chiffrierung eine Hardwarebasis, damit sie getrennt und abgeschirmt vom Netzwerk ablaufen kann. Für das Security Management kann dann logischerweise die Anforderung nicht geringer sein: Es muss auf der gleichen Kryptografie- und Hardwarebasis und somit auf dem gleichen Sicherheitsniveau stattfinden wie die Chiffrierung der Informationen. Zusammen mit einer geeigneten PC-Plattform können *alle* Chiffrier- und Managementprozesse so gesteuert werden, dass sie gleichermassen sicher und anwenderorientiert ablaufen. Es gibt also keine Vorgänge, bei denen der Anwender nicht unterstützt wird!

Ein sicheres kryptografisches Netzwerk – im «grenzenlosen Raum»

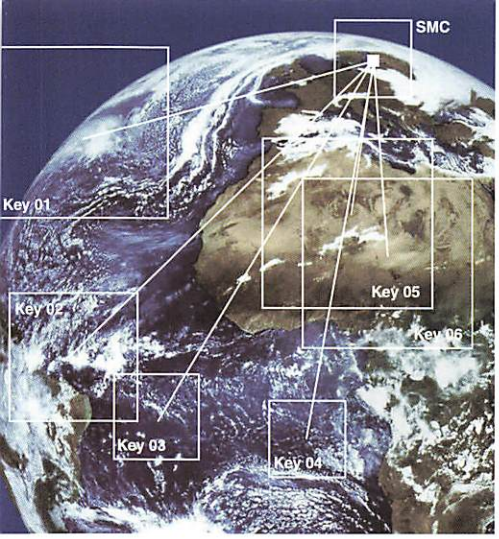
Sicherheit ist dort am leichtesten zu erzielen, wo die Verhältnisse klar und übersichtlich sind. Kommunikation findet heute jedoch in «grenzenlosen» Netzwerken statt. Trotzdem will jeder Netzteilnehmer sicher arbeiten können – egal, wo er sich befindet. Der Security-Manager muss seine Aufgabe entsprechend omnipräsent und flexibel erfüllen können, und zwar von einer zentralen Stelle aus. Sein Wirkungsfeld im Netzwerk ist nach einer logischen Ordnung gegliedert:

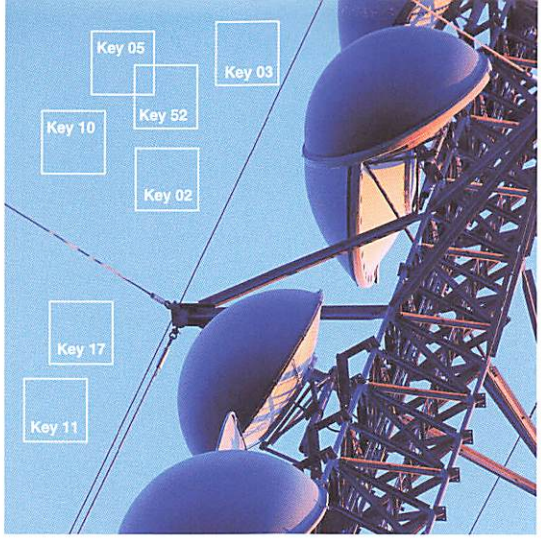
Netzwerkgeografie: Der geografische Raum, in dem sich die Netzteilnehmer befinden. Das kann ein Bürohaus sein oder ein ganzes Land. Die Teilnehmer gehören z.B. einem lokalen Funknetz an oder einem weltweiten Botschafts-VPN eines Staates.

Netzwerktopografie: Das physisch vorhandene, funktionierende Netz. Beispielsweise das weltweit grösste Netz, das Telefonnetz, bei dem alle mit allen im Prinzip ungehindert sprechen können. Sicherheit ist hier noch nicht gegeben, denn als öffentliches Netz ist es für Unbefugte leicht anzapfbar.

Sicherheit durch Unlesbarkeit: Mit Kryptografie will man innerhalb eines Teiles der Topografie Informationssicherheit schaffen: Die Kommunikation soll von Unbefugten nicht mehr abgehört oder verändert werden können. Die Chiffrierung macht Informationen unlesbar – aber die Teilnehmer werden damit zuerst einmal voneinander getrennt: ein babylonischer Zustand. Das ist zwar sicher, aber natürlich nicht zweckmässig.

Sicherheitsmanagement: Damit Sicherheit ***und*** Kommunikation möglich werden («angewandte Sicherheit»), werden *erst jetzt* mit dem Sicherheitsmanagement die «gewollten» Verbindungen kryptografisch ermöglicht. Dazu wird zuerst der Algorithmus und dann der Schlüssel für die erlaubten Verbindungen (in den Teilnehmergeräten) selektiv definiert: Nun haben wir ein sicheres, geregeltes, nur von den einbezogenen Teilnehmern benutzbares Netz zur Verfügung. Es kann mit einem intelligenten Security Management jederzeit online verändert und erweitert werden.





Netzwerktopologie: Sie ist das Resultat des Security Management – also das exklusive Netzwerk, welches mit kryptografischen Mitteln innerhalb einer Topografie gebildet wurde. Die Topologie zeigt, wer mit wem kommunizieren kann/darf. Es lassen sich Gruppen und Hierarchien abbilden – genau so, wie der Anwender arbeiten möchte.

Informationssicherheit als kontrollierter Prozess

«Ordnung im offenen Raum»... diese Sichtweise hat fast etwas Philosophisches an sich. Aber wie entsteht nun *real* mit Hilfe eines modernen Security Management diese «anwendbare» Sicherheit? Mit folgenden Prozessschritten werden alle Elemente zu einem hochsicheren System zusammengefügt:

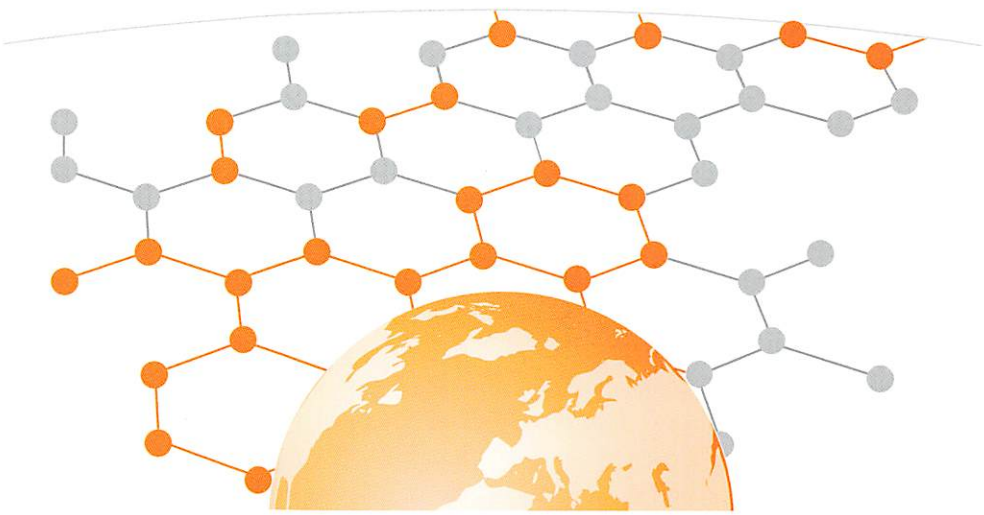
1. Sicherheitshardwareinstallation: Die Netzknoten werden mit einer Hardwarechiffriereinheit ausgerüstet, welche über eigene Rechenkapazität verfügt. Sie kann neben der Chiffrierung auch sichere Funktionen des Sicherheitsmanagements übernehmen.

2. Sicherheitsinstallation: Der komplexe Chiffrieralgorithmus wird vom Anwender selber profiliert. Am einfachsten geschieht dies natürlich mit dem Security Management Centre (SMC). Nur der Anwender kennt jetzt den Algorithmus. Auf dieser geheimen Basis werden alle weiteren Funktionen aufgebaut. Der Algorithmus wird an die Chiffriereinheiten verteilt bzw. in diese geladen. Dieser Vorgang erfolgt bei Systemen von Crypto AG am einfachsten direkt mit dem SMC. Weitere Möglichkeiten sind die Verteilung via Security Data Carrier (SDC), die manuelle Eingabe über das eingebaute Tastenfeld oder der Transfer über das PC-User Interface. Die zu ladenden Daten auf dem SDC sind verschlüsselt. Mit der Sicherheits-Installation ist die Chiffrierung implementiert, aber noch nicht anwendbar.

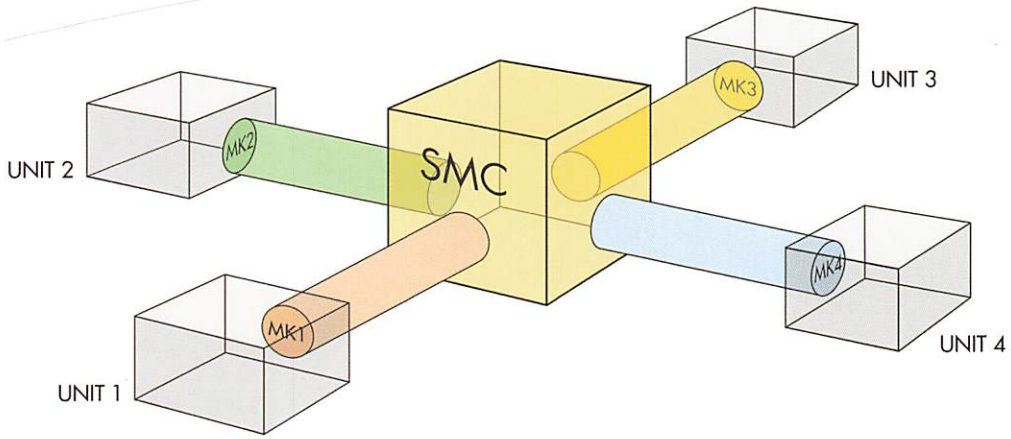
3. Security Registration: Das SMC von Crypto AG erlaubt nun das Etablieren einer weiteren Sicherheitsfunktion: Für jede Einheit im Netz wird ein eigener Management Key (MK) generiert und im SMC registriert. Der MK wird ebenfalls mitttels eines SDC in die Geräte geladen. Mit dem MK steht nun zwischen dem SMC und jeder Einheit ein exklusiver, geschützter Kanal zur Verfügung, über den jederzeit weitere Sicherheitsdaten und Schlüsselinformationen übermittelt werden können – sogar online! Diese geschützten Kanäle – exklusiv zu jeder Chiffriereinheit – erlauben die einfache und dennoch sichere Behandlung von Ausnahmezuständen im Netz.

4. Anwendung der Schlüsselfunktionen: Die Geräte sind nun in der Lage, kryptografische Daten der nächsten Schlüsselhierarchie zu empfangen – die sogenannten Master Communication Keys (MCK). Sie definieren, welche Verbindungen über das Gerät laufen können – d.h. welchen Crypto Groups es zugeordnet ist (sog. Domain-Management). Diese Master Keys werden mit dem SMC definiert und entweder mittels Online-Kommunikation oder SDC den Teilnehmergeräten zugestellt.

Nun ist chiffrierte Kommunikation möglich. Die erlaubten Verbindungen lassen sich via SMC immer wieder beliebig umorganisieren – die Organisation kann so ihre Arbeitsweise jederzeit in der Kommunikationsstruktur abbilden.



EGAL, WO SICH DIE TEILNEHMER IN EINEM KOMPLEXEN PHYSISCHEN NETZ BEFINDEN: MIT DEM SECURITY MANAGEMENT KANN EINE UNABHÄNGIGE TOPOLOGIE GESCHAFFEN WERDEN, IN DER JEDE ERLAUBTE BEZIEHUNG KRYPTOGRAFISCH DEFINIERT IST.



AUFGRUND SEINER REGISTRIERUNG IM SMC WIRD JEDES GERÄT (UNIT) MIT EINEM INDIVIDUELLEN MANAGEMENT KEY (HIER ALS MK1 BIS MK4 DARGESTELLT) AUSGERÜSTET UND VERFÜGT DESHALB ÜBER EINEN INDIVIDUELL CHIFFRIERTEN, GETRENNTEN MITZUHÖREN «MANAGEMENT-KANAL» FÜR DEN EMPFANG VON NEUEN SICHERHEITSDATEN. GEHT Z.B. EIN GERÄT VERLOREN, KANN DIESES AUS DEM NETZ AUSGESCHLOSSEN WERDEN, INDEM ÜBER DIE GESCHÜTZTEN MANAGEMENT-KANÄLE ZU DEN ANDEREN GERÄTEN GEFAHRLOS NEUE SCHLÜSSEL VERTEILT WERDEN. DER ENTSCHEIDENDE SICHERHEITSGEWINN: DAS VERLORENE GERÄT KANN NICHT MISSBRAUCHT WERDEN, UM DABEI «MITZUHÖREN»!

5. Periodische Schlüsselwechsel: Ein kryptografisches Prinzip lautet, dass jeder geheime Schlüssel periodisch ausgetauscht werden sollte. Bei grösseren Netzen entsteht dabei ein Problem: Es ist nicht möglich, bei allen Einheiten den Schlüssel simultan online zu wechseln. Das Security Management von Crypto AG verwendet deshalb ein Konzept, das diese Asynchronität der Schlüsselverteilung elegant bewältigt: Für jede Crypto Group (Domain) können zwei Schlüssel gespeichert sein. Der neue Schlüssel erhält mit dem Erreichen seiner Key Activation Time Priorität, allerdings kann das Gerät beide, den neuen und den alten, verwenden, je nachdem, ob die jeweilige Gegenstation ebenfalls schon auf den neuen gewechselt hat oder nicht. Diese Rückfallposition bleibt bis zum nächstfolgenden Wechsel bestehen. Die Häufigkeit der Schlüsselwechsel lässt sich individuell handhaben, sogar unterschiedlich von Crypto Group zu Crypto Group – ein weiterer Sicherheitsfaktor.

6. «Session Keys»: Bei Systemen, die jeweils chiffrierte Verbindungen neu aufbauen (typisches Beispiel: das Telefon), wird jedes Mal zusätzlich ein völlig neuer Verbindungsschlüssel generiert – auf Basis der gespeicherten MCKs. Bei Systemen, die dauernd online sind (wie etwa Datenlinks), wird eine virtuelle Sessionlänge programmiert – nach gewählten Kriterien, z.B. nach einer bestimmten Menge übermittelter Daten.

Das Security Management Centre (SMC) von Crypto AG

Das Instrument, welches alle diese Security-Management-Aufgaben unterstützt, ist das PC-basierte Security Management Centre von Crypto AG. Es ist die benutzerorientierte Plattform, die dank separatem Message Scheduler und Hardwaresicherheitsmodul alle kryptografischen Vorgänge getrennt von der Netzstruktur abwickelt und damit vor Zugriffen schützt, auch wenn die Verteilung der Schlüssel online geschieht. Was das SMC verlässt, ob online oder offline, ist selber immer bereits chiffriert.

Die Arbeit des Security-Managers wird mit einer intuitiven Menüführung erleichtert. Kennt der Security-Manager die Konzepte der Crypto-Geräte, wird er durch das SMC sehr gut unterstützt.

Für Security-Manager und andere Interessierte bietet Crypto AG Grundlagenkurse an in Kryptografie, Informationstechnologie und generellen Sicherheitsthemen. Daneben kann Grund- und Refresher-Training an identischen Geräten, wie sie beim Kunden in Betrieb sind, absolviert werden. Weiterbildung auf diesen Gebieten erhöht letztlich immer die Verfügbarkeit von Chiffriersystemen.

* TIS = Total Information Security©, TIS by Crypto AG. Dieses Konzept auf der Basis von «Multiple Lines of Defence» garantiert systemspezifisch den absoluten Schutz von Informationen in Bezug auf Vertraulichkeit («Information ist für Unbefugte nicht lesbar»), Integrität («niemand kann die Information oder Teile davon in irgendeiner Beziehung verändern»), Authentizität («die Herkunft bzw. der Absender ist immer unzweifelhaft erkennbar») und dauernde Verfügbarkeit («die Bearbeitung und die Verteilung sind jederzeit uneingeschränkt möglich»).

«MANIPULATIONSMASSE» MITTEILUNG

Interview: Catherine Frigo

Es wird nie so viel gelogen wie im Wahlkampf, während eines Krieges oder nach der Jagd, wusste bereits Graf Otto von Bismarck, seines Zeichens erster Kanzler von Deutschland. Heute hat diese Aussage noch immer Gültigkeit und kann sogar noch um das Golfturnier erweitert werden. Im Falle einer kriegerischen Auseinandersetzung werden die Manipulationen an den Medienmitteilungen jedoch auf die Spitze getrieben. Frei nach dem Motto: Wer die Öffentlichkeit auf seiner Seite weiss, hat den Sieg so gut wie in der Tasche. Ein Interview über Information Warfare in all ihren Facetten.

INTERVIEW MIT OBERST DR. PETER FORSTER, PRÄSIDENT DER SCHWEIZERISCHEN KOMMISSION FÜR INNERE SICHERHEIT UND NAHOST-EXPERTE

Wer die Information besitzt, besitzt die Macht. Welche Relevanz hat diese Aussage noch in einem Zeitalter, in welchem im Kriegsfall die Information bei ihrer Ankunft beim Empfänger bereits als veraltet gilt?

Im strategischen Bereich waren gerade im Winter 2002/2003 vor dem dritten Golfkrieg enorme Probleme im Nachrichtenfluss festzustellen. Denken Sie an die Fehlbeurteilungen in Sachen Massenvernichtungswaffen und die mangelnden Nachrichtengrundlagen für den Irak-Krieg. Hingegen im taktischen Bereich bin ich der Meinung, dass diese Aussage nicht ganz richtig ist, wonach die Informationen veraltet sind, wenn sie eintreffen. Hier sind im ganzen Durchlauf Nachricht–Führung–Einsatz Verbesserungen erzielt worden. Man spricht davon, dass sich dieser Durchlauf auf wenige Minuten reduziert hat, und gerade der eigentliche Irak-Feldzug vom Jahre 2003 hat dies gezeigt.

Der Kosovo-Krieg wird wiederholt als Geburtsstunde der Information Warfare genannt. Welchen Einfluss hatte dieser Krieg auf das Informationshandling im militärischen Bereich?

Was die Geburtsstunde der Information Warfare anbelangt, bin ich anderer Ansicht. Für mich fängt diese bei den Trompeten von Jericho an, welche Josua bei der ältesten Stadt der Welt eingesetzt hat. Oder denken Sie an Cäsar, der selber sein bester Propagandist war, oder an Napoleon, welcher ein Meister der Beeinflussung war. Der Kosovo-Krieg war insofern bedeutend, als zu diesem Zeitpunkt der erste *Internet*krieg ausgefochten wurde. Man muss hier beim «kriegerischen» Einsatz der Medien differenzieren:
Der erste *Presse*krieg fand während des Krimkrieges von 1853 bis 1856 statt, mit dem Einsatz der «London Times» an der Front. Der erste *Radio*krieg fand zu Zeiten des Zweiten Weltkriegs statt. Das Radio – 1923 erfunden – wurde von Hitler sowie Goebbels zu Propagandazwecken verwendet. Dank dieses Mediums konnte sich die Ideologie des Nationalsozialismus erst so richtig verbreiten. Der erste Televisionskrieg wurde zweifellos während des Vietnamkriegs

ausgefochten, als die amerikanischen Streitkräfte dem Fernsehen jegliche Freiheiten gaben, von der Front zu berichten. Was enorme Auswirkungen auf die Stimmung in den USA hatte. Noch heute herrscht in den Staaten die Meinung, dass der Vietnamkrieg letztlich am Bildschirm verloren ging.

«Heute können wir einen Raster ziehen zwischen den Psychological Operations und dem Bereich der technischen Operationen.»

Aber unter dem Gesichtspunkt Internet war der Kosovo-Krieg neu. Das Internet ist die Informationswaffe des armen Mannes: sehr einfach zu handhaben, billig, aktuell, direkt. Sowohl die UCK als auch die serbische Opposition haben das Internet intensiv zur Verbreitung von journalistisch aufbereiteten Geschichten angewandt. Denken Sie an die Geschichte des serbischen oppositionellen Radiosenders B92, welcher vom Milosevic-Regime geschlossen wurde: Innert Stunden haben die Regimegegner nachher ihre Radiobotschaften via Internet verbreitet. So gesehen war Kosovo tatsächlich ein Meilenstein im Bereich Information Operations. Eigentlich ein bedeutender Meilenstein, denn seither haben wir vier Medien, welche dauernd zu Propagandazwecken genutzt werden.

Zur besseren Verständlichkeit möchte ich hier eine Zwischenfrage einschieben: In welchem Fall spricht man von Information Operations, wann von Information Warfare?
Der Begriff «Information Warfare» hat meines Erachtens ausgedient. Die «Information Operations» hingegen sind neutraler gefasst und lassen sich wie folgt aufteilen: Command and Control Warfare, welche darauf abzielt, die feindlichen Kommandostrukturen und Kommunikationsverbindungen zu zerstören. Die Intelligence Operations gehen hingegen bereits subtiler zu Werke; wir sprechen hier von geheimdienstlichen Aufklärungen. Electronic Warfare kann auch zu den Information Operations gezählt werden, dessen jüngste Auswüchse in Hacker Warfare – dem Ausnützen der Sicherheitslücken im Internet – gipfeln. Schliesslich gibt es noch *Psychological Warfare* respektive *Operations*. Heute können wir einen groben Raster ziehen zwischen den Psychological Operations einerseits und dem ganzen Bereich der technischen Operationen andererseits. Die Psychological Operations zielen gemäss NATO auf die «Hearts and Minds» der Truppen und auch der Bevölkerung.

Psychological Operations sollen die Herzen und die Köpfe der Bevölkerung erreichen; welcher Mittel bedienen sie sich hierzu?
Gefragt sind Botschaften, welche sich an den Grundsätzen von Sachlichkeit, Wahrhaftigkeit, Aktualität und Verständlichkeit orientieren. Hierzu existieren jedoch unterschiedliche Ansätze: Die schweizerische Doktrin beruht nicht auf den amerikanischen Psychological Operations. Hierzulande haben wir immer nur einen Informationsauftrag gehabt und auch die Nachfolgeorganisation im Führungsstab der Armee wird sich begrenzen auf einen *Informationsauftrag*. Die amerikanische und die NATO-Doktrin hingegen wollen zusätzlich *beeinflussen*. Und diese Beeinflussungen erfolgen in weissen und schwarzen Operationen. Eine weisse Operation geht von einer ehrlich deklarierten Quelle mit einer sachlichen, wahrhaftigen Information aus. Die schwarzen Operationen nennen die Quelle nicht. Beispielsweise gibt «The Voice of the Gulf» sich als arabischer Sender aus, ist in Tat und Wahrheit aber ein CIA-Sender. Somit wird das Zielpublikum irregeführt und «falsch» beeinflusst.
Noch etwas zu den schweizerischen Grundsätzen: Weshalb muss nach hiesigen Gesichtspunkten die Information nicht vollständig sein? Im zivilen Journalismus wird die Vollständigkeit angestrebt. Im Krieg kann es Situationen geben, wo die vollständige Information Leben oder Operationen gefährden kann. Deshalb fehlt in der schweizerischen Doktrin die Vollständigkeit, aber die übrigen Grundsätze entsprechen den zivilen Grundsätzen. Und was die Wahrhaftigkeit anbelangt, da bin ich im lessingschen Sinne der Ansicht, dass wir die absolute Wahrheit nie besitzen können. Und auch in all diesen Operationen können wir nur ringen um die Wahrheit – immer aber im Bewusstsein, dass es gerade im Krisenfall keine absolute Wahrheit gibt. Tragisch, aber wahr: Die Auflagen der Zeitungen und die Einschaltquoten der elektronischen Medien sind nie höher als im Kriegsfall.

Sie sprechen die Medien an: Kann das Konzept der Information Operations auch auf die Medien resp. die Berichterstattung aus Krisengebieten angewendet werden, nämlich dann,

wenn Reporter die «Wahrheit» zugunsten der Berichterstattung verzerrt wiedergeben? Berühmtes Beispiel ist ja CNN mit den Live-Reportagen aus dem Kampfgebiet.
Ich bin nach wie vor davon überzeugt, dass sich die überwiegende Anzahl der Medien unter berufsethischen Aspekten um eine wahrheitsgetreue und korrekte Berichterstattung bemüht. Aber in jedem Krieg ist die Wahrheit das erste Opfer. Die Medien werden von Kriegsparteien ganz bewusst eingesetzt. Gegen Ende des zweiten Golfkrieges beispielsweise hat General Schwarzkopf der irakischen Gegenpartei via Medien vorgespielt, der Angriff auf Kuwait erfolge vom Persischen Golf aus. Derweil hat er starke Verbände in der Wüste nach Westen verlegt und in der Tat hat er dann die «Operation Kuwait» zu Lande ganz im Westen mit einer

grossen Umklammerungsaktion geführt. Tagelang vorher hat er aber den Medien Gerüchte zugespielt, wonach die Operation vom Wasser geführt werde. Die Presse hat das von ihm übernommen und hat mangels besseren Wissens eine Rolle gespielt. Schwarzkopf hat jeden Tag mehrere Stunden mit Information Operations verbracht und hat sie unter seinen Gesichtspunkten meisterhaft eingesetzt. Denn er musste den Krieg mit einem Minimum an eigenen Opfern gewinnen – noch aufgrund des in den

USA herrschenden Vietnamtraumas. Für ihn waren die Information Operations also ein absolut willkommenes Mittel, den zweiten Golfkrieg mit einem Mindestmass an Verlusten zu gewinnen.

«In all diesen Operationen können wir nur ringen um die Wahrheit – immer aber im Bewusstsein, dass es gerade im Krisenfall keine absolute Wahrheit gibt.»

Wie verhielt es sich im dritten Golfkrieg?
Im dritten Golfkrieg 2003 ist es nicht zu übersehen, dass mindestens in der Anfangsphase die Amerikaner sehr patriotisch berichtet haben. Es war eine Berichterstattung im Zeichen einer vaterländischen Pflicht. In der Zwischenzeit haben aber etliche amerikanische Medien ihre Positionen korrigiert. Es gibt auch Zeitungen wie die «New York Times» oder die «Washington Post», welche ausdrücklich eingeräumt haben, sie seien in der Vorbereitung des Krieges und während des anfänglichen Feldzuges falsch gelegen. Die britische BBC verhielt sich hingegen immer distanzierter zur Regierung Blair und zur Kriegsführung. Gerade in den Medien – allen voran CNN – wird ein Krieg immer mehr zu einem Event hochstilisiert, einer Bühne, auf welcher die verschiedensten Inszenierungen stattfinden: Politiker inszenieren sich als vertrauenswürdig, Militärs als Herr der Lage und die Medien inszenieren sich selbst um der Inszenierung willen. Kritische Hintergrundbeleuchtungen bleiben hierbei natürlich auf der Strecke.

Betreiben Dokumentarfilmer wie Michael Moore Ihrer Ansicht nach auch Informationskrieg, wenn – wie im Film «Fahrenheit 9/11» geschehen – die Fakten offensichtlich sehr zuungunsten einer Krieg führenden Partei dargestellt werden?
Ist es denn Zufall, dass dieser Film gerade auf dem Höhepunkt des Wahlkampfes ins Kino kommt? Es ist interessant, dass Bücher und Berichte gegen die Administration Bush gerade jetzt in der heissen Vorwahlphase (Anmerkung der Redaktion – das Gespräch fand Mitte Oktober 2004 statt) erscheinen. Wenn auch hinter diesem Film eine bewusste Planung steckt, dann kann man von Information Operations resp. Information Warfare sprechen. Traditionellerweise stehen viele Film- und Schauspielgrössen in den Staaten auf der Seite der Demokraten.

Denial-of-Service-Attacken, welche die Rechner der zentralen Verwaltungsstellen lahm legen, ein Hackerangriff, welcher den öffentlichen Schienenverkehr fast zum Erliegen bringt, oder das böswillige Eingreifen in den Informationsfluss zwischen einer Zentralbank und weiteren Bankinstituten durch Manipulation der Glasfasern: Welche Zusammenhänge bestehen Ihrer Meinung nach (noch) zwischen der Wahrung der inneren Sicherheit und Information Warfare?

Dr. Peter Forster – zur Person
Dr. Peter Forster wurde 1946 geboren, erwarb die Maturität an der Kantonsschule Winterthur und studierte an der Universität Zürich Geschichte und Staatsrecht (Promotion zum Dr. phil. 1970). 1971/1972 Postgraduate-Studium an der Columbia University New York und der University of California Berkeley.

1972 trat er in die Redaktion der «Neuen Zürcher Zeitung» ein, für die er ab dem Jom-Kippur-Krieg 1973 als politischer und militärischer Korrespondent aus Israel, Zypern, Griechenland und der Türkei berichtete.

Von 1981 bis 2001 war Dr. Forster Chefredaktor der «Thurgauer Zeitung» und Mitglied der Geschäftsleitung der Huber & Co. AG in Frauenfeld. Seit 2001 leitet er im Lilienberg Unternehmerforum das Aktionsfeld Medien.

Er schrieb die beiden Bücher: «Aber wahr muss es sein. Information als Waffe» (Frauenfeld, 1998) und «Fällt Jerusalem? Israel und die Araber: Tage der Entscheidung» (Frauenfeld, 2001).

In der Schweizer Armee war er von 1996 bis 2003 Kommandant des Informationsregimentes 1, vorher Kommandant der Schweren Kanonenbatterie, der Armeestabsabteilungen und -stabsgruppe. Seit dem 1. Januar 2004 ist er Chef Information Operations Astt 370 (Führungsstab der Armee).

Innere und äussere Sicherheit sind heutzutage untrennbar miteinander verbunden. Im modernen Bedrohungsbild steht natürlich die Bedrohung durch Terror und gewalttätigen Extremismus an der Spitze. Auch der ganze Bereich «Hacker Warfare», Denial-of-Service-Attacken etc. muss ernst genommen werden. Viele unserer Lebensbereiche sind direkt abhängig von Informatiksystemen. Man stelle sich einmal eine Attacke auf die Leitsysteme der Eisenbahnverbindungen vor, welche zu einer Zugsentgleisung führt, gekoppelt mit einer Attacke auf die Flugraumüberwachung, welche prompt drei Jumbos zum Absturz bringt. Stellen wir uns vor, die zentrale Lebensmittelversorgung wird gestört, die Elektrizitätsversorgung fällt zusammen. Dieses aufrüttelnde Szenario wurde an der Schweizer Strategischen Führungsübung 1:1 durchgespielt. Seither ist hierzulande die Wachsamkeit stark gewachsen. Leider hinkt sie noch immer den bestehenden Gefahren hintennach. Über «Gedeih oder Verderb» entscheidet beispielsweise,

Fortsetzung auf Seite 10

Fortsetzung der Seite 9

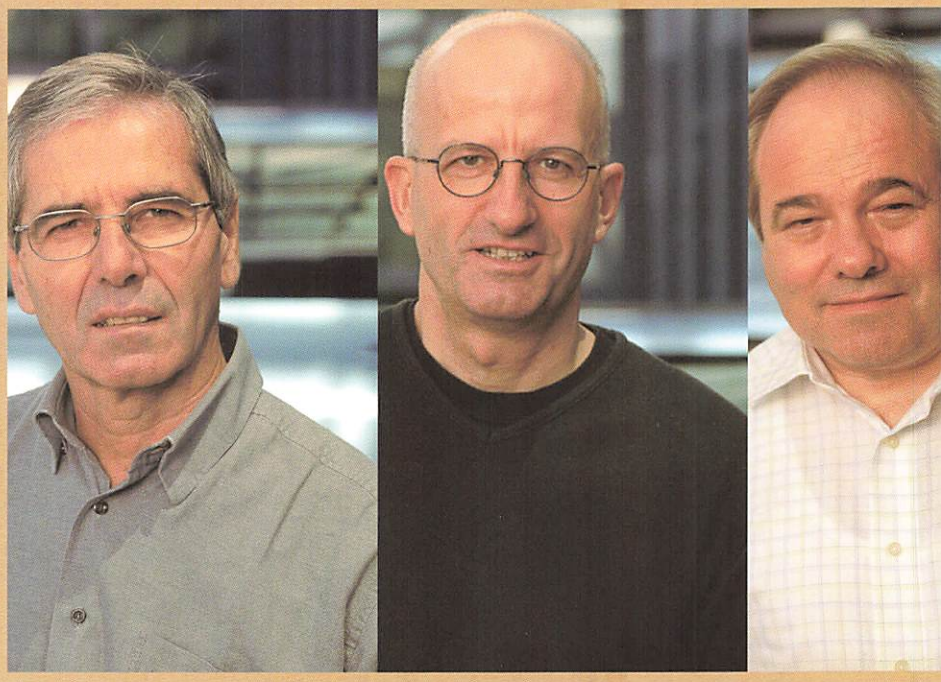
dass die kritischen Systeme auf keinen Fall mit dem Internet verbunden sind.
Ein zentraler Angriffspunkt kann nach wie vor die Elektrizitätswirtschaft bleiben: Ein Stromausfall in einer grösseren Stadt hätte verheerende Auswirkungen auf die Sicherheit.
Andererseits muss man sich nach der möglichen Urheberschaft erkundigen: Wer will denn ein solches Cyber-Pearl-Harbour erreichen? Gerade eine Denial-of-Service-Attacken ist doch mit erheblichem Aufwand verbunden.

Der Schutz der kritischen Infrastrukturen gilt als Kernelement der «inneren Sicherheit»: Inwieweit ist dies Sache eines jeden einzelnen Staates oder inwieweit kommen länderübergreifende Konzepte wie bspw. der CIIP-Ansatz zum Tragen?
Wir haben ein Mehrfaches zu tun: Es beginnt bei den Firmen, bei der Verwaltung, bei der Armee etc.: Es hat jeder in seinem Bereich die nötigen Schutzmassnahmen zu treffen und durchzusetzen. Nun kann das in einem zweiten Schritt sicher nicht isoliert geschehen; es braucht bei allen Betroffenen eine Zusammenarbeit, welche ja bereits eingesetzt hat. Und Sie haben durchaus Recht, das dies auch grenzüberschreitend geschehen sollte. Der Hacker War wird weltweit geführt und kam von den Philippinen, kann aber auch von Buenos Aires oder von Amsterdam aus geführt werden. Hacker War kennt keine Grenzen, sowenig wie das Internet Grenzen kennt. Also haben Sie Recht, es braucht internationale Kooperation.

Besten Dank, Herr Dr. Forster, für Ihre Ausführung.

CRYPTO-SPEDITION *Catherine Frigo*

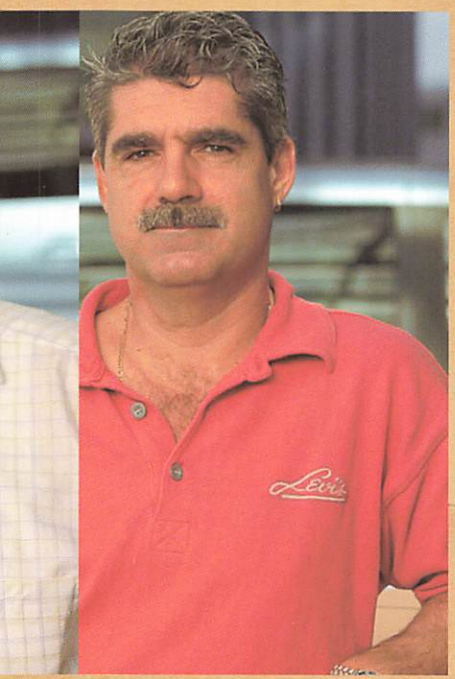
DEM ZUFALL WIRD NICHTS ÜBERLASSEN



VON LINKS: RÖBI STIERLI, ARMIN HOFSTETTER BRUNO ULRICH UND MARTIN WALKE

An die Crypto-Produkte werden höchste Anforderungen gestellt. Unzählige Vorsichtsmassnahmen sorgen deshalb für einen reibungs- und vor allem fehlerlosen Produktionsprozess. Sämtliche Abläufe verlaufen in geordneten Bahnen. Damit die Produkte auch nach Verlassen des Hauses ihren Empfänger in tadelloser Qualität erreichen, dafür sorgen diese vier Herren im Hinter- respektive Untergrund.

Betrachtet man eine Warenkette als Ganzes, so sind auf dem Weg vom Produktionsbeginn bis zur Auslieferung des fertigen Produktes einige Hürden zu meistern. Vor allem am Anfang und am Ende des Produktionsprozesses lauern Fussangeln, welche ein industriell erzeugtes Produkt massiv entwerten könnten. Diesen Funktionen kommen also Schlüsselrollen zu. Was für die ganze Industrie gilt, ist besonders für die Crypto AG gültig: Beim Wareneinn- als auch beim Warenausgang hat «Feind Zufall» keine Chance. Damit dies so ist, braucht es Mitarbeiter, welche auch an sich Höchstanforderungen stellen.



Konzentration auf das Wesentliche

In einem 230-Personen-Betrieb wie der Crypto AG werden tagtäglich mehrere Dutzend Warensendungen angeliefert – von der kleinsten Schraube bis hin zu meterhohen Paletten von Prints. Damit hier kein unerwünschtes und nicht angemeldetes Paket durchschlüpfen kann, existiert ein rigoros enges Filtersystem. Was zu mühseliger, detektivischer Kleinarbeit führen kann, müssen doch die angekommenen mit den erwarteten Sendungen verglichen werden. Dabei lässt Armin Hofstetter «Intelligence» walten oder zieht auch mal die Personen vom Wareneinkauf zu Rate, mit welchen er eng kooperiert. Strikt einhalten muss er auch das Prozedere, wie man sich bei unidentifizierbaren Waren verhalten soll. Jede Nachlässigkeit kann schliesslich unvorhersehbare Folgen haben.

Schnittstelle zum Kunden

Ist der Wareneingang die Tür ins Unternehmen, so stellt der Warenausgang die Schnittstelle zum Kunden dar. Dies ist bei der Crypto AG die Spedition, welche die fertigen Chiffrierprodukte so versandfertig macht, dass ihnen unterwegs buchstäblich nichts passieren kann. Röbi Stierli und Martin Walker machen die Maschinen versandbereit, indem sie die Geräte in eigens für sie angefertigte und im Umweltlabor überprüfte Verpackungen stecken, welche schliesslich teilweise sogar versiegelt werden. Dabei wird von beiden ein grosses Mass an Flexibilität gefordert – nicht selten werden die beiden zehn Minuten vor «Ladenschluss» noch mit wichtigen Versandaufträgen konfrontiert. Just in Time in Reinkultur also. Trotz aller Hektik wickeln sie die Speditionsformalitätenin Zusammenarbeit mit der Export-Administration in grösster Perfektion ab. Die Pakete sind so entworfen, dass ihnen keine Einwirkungen von aussen etwas anhaben können. Die versandfertigen Pakete gehen im Anschluss nicht den üblichen Postweg, sondern werden entweder direkt an die Botschaften der jeweiligen Kundenländer geliefert oder aber einem Vertrauens-spediteur übergeben. Während des Transportes an den Zielort darf dann die Lieferung in keinem Moment aus den Augen gelassen werden – was dann eine Toilettenpause zu einem schwierigen Unterfangen werden lässt ...

Humanfaktor

Die «Spedi» macht die Crypto-Produkte nicht nur versandfertig, sondern liefert sie zum Teil auch noch eigenhändig an die Kunden aus. Die Abteilung hat indes nicht nur die Waren-, sondern auch noch die Personentransporte unter sich. Und hier kommt Bruno Ulrich ins Spiel. Auch er ist ein seit Jahren treuer Cryptoianer, welcher Tag und Nacht zur Verfügung steht, um Kunden und Partner der Crypto AG zu deren gewünschten Destination zu chauffieren. Nicht selten gehen Meetings länger als geplant und die Zeit, bis der Flieger abgeht, wird immer kürzer. Da kommt ihm sein Wissen um die Schleichwege zum Flughafen jenseits des Feierabendverkehrs sehr gelegen. Denn auch die Schweiz bleibt vom ständig zunehmenden Privatverkehr nicht verschont. Aller guten Dinge sind vier: Röbi Stierli, Martin Walker, Armin Hofstetter und Bruno Ulrich sind bestrebt, dass sich weder am Anfang noch am Schluss des Produktionsprozesses Fehler einschleichen können.

NETWORK SECURITY

*Inhalt: Markus Baumeler und Urs Kürzi**
*Redaktion: Catherine Frigo**

LINK IN DIE GEFAHRLOSIGKEIT

Datennetzwerke sind das Rückgrat sämtlicher Kommunikation. Technologisch als Bitübertragungsebene gekennzeichnet, bildet eine Verbindung zweier Teilnehmer die kleinste Einheit, auf welche schliesslich jedes Netzwerk reduziert werden kann – sei es das Internet, die Verbindung mehrerer Organisationen untereinander oder ein militärisches Netz. Aus diesem Grund stellen zuverlässige und sichere Verbindungen in einem Netzwerk die Grundlage für den Aufbau einer jeden Kommunikationsinfrastruktur dar. Punkt zu Punkt.

Hacking, Cracking, Cyberwar: Die alte Leier muss einfach immer wieder gespielt werden. Denn der «Feind» ist immer einen Schritt voraus. Ist Ihnen auch schon passiert, dass Sie während einer Recherche im Internet eine Message erhielten, welche Ihre URL sowie Ihren genauen Standort samt freundlichen Grüssen enthielt? Okay, das Internet zählt zu den berühmtesten Beispielen für eine unsichere öffentliche Kommunikationsplattform. Genauso unsicher sind jedoch auch private sowie weitere dem Publikum offene Netze. Exemplarisch, quasi der Rolls-Royce unter den Beispielen, ist der Fall vom World Economic Forum Davos. Da gelang es vor drei Jahren Globalisierungsgegnern, «dank» eines ungeschützten Back-up-Prozesses auf die Daten der Forumsteilnehmer zuzugreifen. Weitere prominente Fälle sind natürlich die UNO- und Waffeninspektoren-Abhör-Geschichten vom Anfang dieses Jahres. Aber auch spektakuläre «Einzelschicksale» spielen sich aufgrund liederlichen Umgangs mit Netzwerken ab: Ein deutscher Ingenieur wurde mit einer Milliardenklage eines US-Unternehmens konfrontiert, welche ihn des Diebstahls von geistigem Eigentum bezichtigte. Ursprünglicher Erfinder der neuen Technologie im Umgang mit Windenergie war jedoch er selbst. Er hatte es jedoch versäumt, seine Erfindung rechtzeitig zum Patent anzumelden, und wie erwähnt seine Daten nicht geschützt: Das kam ihn sowie seine Mitarbeiter teuer zu stehen.[1]

Look back without anger

Was wäre geschehen, wenn ...? Um zu verstehen, wie man sich umfassend auf der Stufe der Links, der Verbindungen zwischen zwei Netzteilnehmern, schützen kann, soll der Begriff «Link» an dieser Stelle zunächst eingeführt werden.

Die als Links bezeichneten Punkt-zu-Punkt-Verbindungen bilden die Grundlage für sämtlichen Datenverkehr. Sie werden da eingesetzt, wo grössere Datenmengen ge-

*Markus Baumeler ist Product Manager Link and Broadband Systems, Urs Kürzi Marketing Manager und Catherine Frigo Corporate Editor.

[1] Schmeh, Klaus. Die 55 grössten Flops der Wirtschaftsgeschichte. Ueberreuther Verlag.

bündelt zwischen selbstständigen Netzwerken zirkulieren müssen. Die Links basieren 0auf einem physischen Trägermedium (Kupferkabel, Glasfaser, Mikrowelle bzw. Richtstrahl oder Satellitenverbindung) sowie einem Übermittlungsprotokoll, das gleich die Nutzungsmöglichkeiten vorgibt. Punkt-zu-Punkt-Verbindungen führen dabei zwei Netzteilnehmer zusammen, Multipunkt-Links vernetzen mehrere Teilnehmer.

Links noch lange nicht überholt

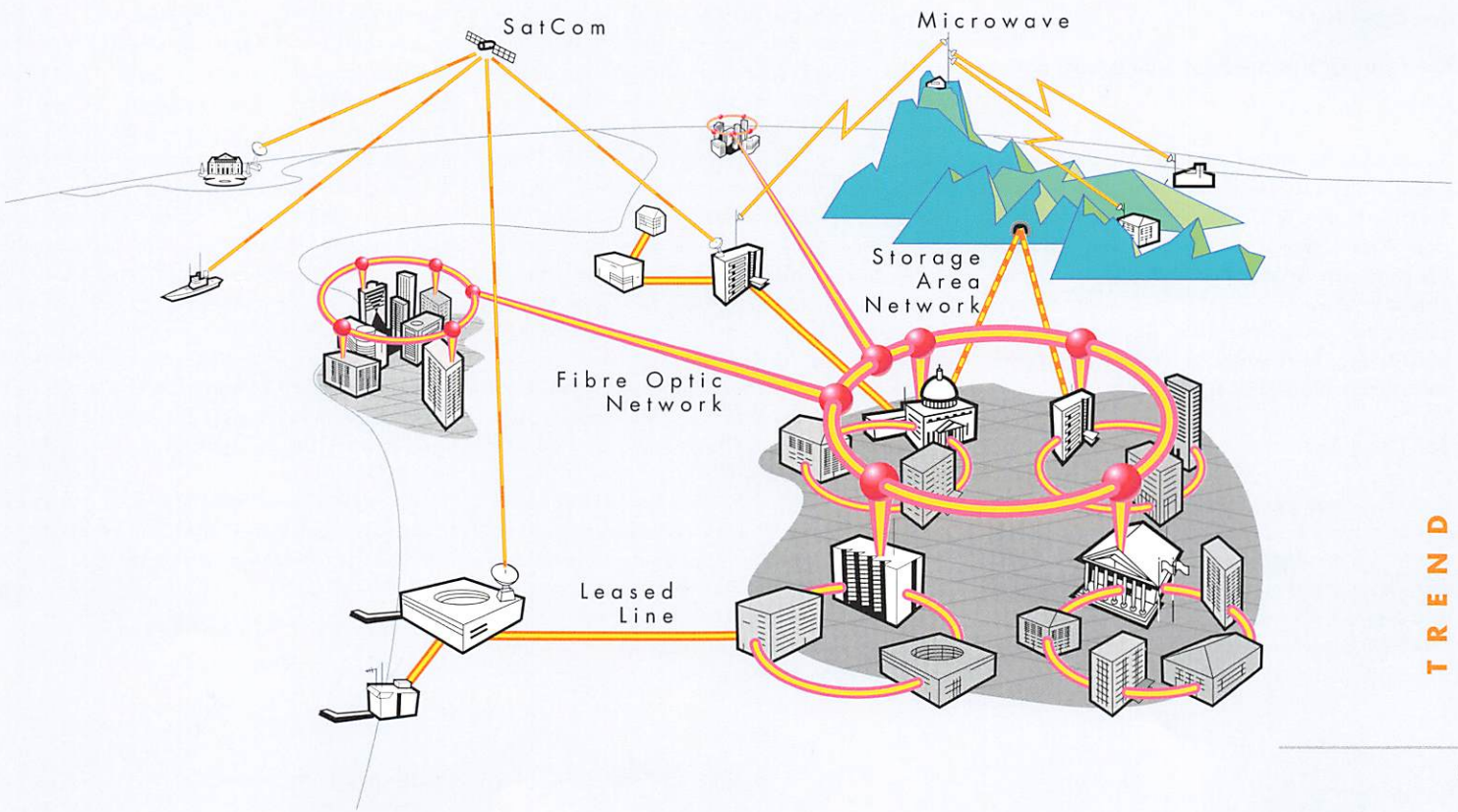
Dass das transportierte Datenvolumen jährlich um 30 Prozent zunimmt, ist bekannt. Gefragt sind deshalb hohe Durchsatzraten zu selbstverständlich niedrigen Preisen. Erwartet werden skalierbare Bandbreiten auch zu abgelegenen Kommunikationspartnern hin. Gesucht sind hohe Verfügbarkeit der Daten in Echtzeit und Zuverlässigkeit. Was liegt denn da näher, als die Infrastruktur möglichst zu vereinfachen. Die Kapazität der Linkübertragung kann heute mehrere Gigabytes/Sekunde erreichen, beispielsweise für Multimediaanwendungen, militärische Lagedarstellungen, Brücken zwischen Grossnetzen oder dezentrale Datensicherungen. Netzwerke und deren Untereinheiten beschränken sich nicht auf erdgebundene Kupfer- und Glasfaserleitungen. Auch ätherische Medien wie Mikrowellen/Richtstrahl und Satelliten kommen vermehrt zum Einsatz, sei es aufgrund des Fehlens drahtgebundener Übertragungsmedien oder um weite Strecken in unwegsamen Geländen zu überbrücken.

Pünktlich dank Punkt-zu-Punkt-Verbindungen

Müssen Radardaten blitzschnell zur Lageanalyse herbeigezogen werden? Stehen am Zoll verdächtige Personen, deren Identifikation rasch überprüft werden muss? Müssen Minister vor einem staatspolitisch bedeutsamen Meeting noch mit den aktuellsten Informationen versorgt werden? Sind im Falle einer Staatskrise alle Diplomaten schnell zu informieren? Alles Situationen, in welchen Informationen ohne Verzögerung zu ihren Empfängern gelangen müssen. Schnell, und sicher.

Grundsätzliche Voraussetzung für Aufbau einer zentralen, kostengünstigen und effizienten IT-Infrastruktur ist eine leistungsfähige, zuverlässige und sichere Verbindung zwischen allen Verbundsteilnehmern (Backbone). Auf der Linkebene kann dies einfach erreicht werden: Auf dieser Basisübertragungsstufe können Synergien genutzt werden und vor allem ist die Performance für Echtzeitapplikationen vollständig gewährleistet.

Im Gegensatz zu IP-VPN-Lösungen tritt bei reinen Linklösungen auch die Verzögerungsproblematik in den Hintergrund: Dies fällt vor allem bei allen zeitkritischen Applikationen ins Gewicht, insbesondere bei Sprachanwendungen, sowie auch bei der Übermittlung biometrischer Daten anlässlich von Zollkontrollen oder Videokonferenzen. Beim Übertragungsweg auf der Linkebene (Link Layer) drängt sich der Vergleich mit einer Schnellstrasse auf, welche direkt von A nach B führt und auf welcher grosse Informationsmengen ohne zeitliche Verzögerung übermittelt werden. Im Gegensatz dazu werden die Informationen auf IP-(VPN-)Ebene paketweise übermittelt, was insbesondere bei grossen Datenmengen zu Verzögerungen führen kann, weswegen Links im Bereich Quality of Service besonders auftrumpfen können. Gerade staatliche Organisationen fahren mit der Linkkommunikation gut, da sie sich perfekt in das



organisationseigene Kommunikationsnetzwerk integrieren lässt, die hierarchischen Abläufe respektiert und niedrige Übertragungskosten nach sich zieht.

Unspektakulärer Schutz – spektakuläre Wirkung

Sogar zuverlässige Kommunikationssysteme funktionieren nicht reibungslos während einer Krise, falls konventionelle Übertragungsmedien wie das Internet, das Telefon oder Satellitenkommunikation verwendet wird. Zum Beispiel hat der zweite Irak-Krieg gezeigt, dass US-Behörden nicht zögern, Kapazitäten in der Satellitenübertragung zu blockieren oder sich der Kontrolle über das Internet zu bemächtigen. Wer während Krisenzeiten kommunizieren will, soll dies in einem geschützten Rahmen tun.

Die Links laufen über die öffentliche Infrastruktur, auf welche relativ einfach zugegriffen werden kann. Die Ortung des Funkstrahls bei Satellitenkommunikationsanwendungen oder der Dispersionsverlust der Strahlung bei Mikrowellen und Glasfaserverbindungen stellen weitere Gefahren bzw. Angriffspunkte dar. Aber wie eingangs erwähnt, stehen so auch Hackern, Viren und Trojanischen Pferden sowie der ganzen übrigen Menagerie Tür und Tor offen, ganz zu schweigen von Denial-of-Service Attacken, Traffic Analysis und Abfangen von optischen Informationen.

So unkompliziert sich die Übertragung auf der Linkebene gestaltet, so einfach ist auch die Chiffrierung auf dieser Ebene. Seien es Kupfer- oder Glasfaserkabel, seien es Satelliten- oder Mikrowellenverbindungen – die Sicherung der übertragenen Informationen kann bequem gewährleistet werden. Und das ohne Zeitverzögerung, auch bei grossen Datenmengen. Linkchiffriergeräte sind einfach zu bedienen und zeichnen sich durch eine hohe «Benutzerfreundlichkeit» aus. Das Sicherheitsmanagement erfolgt zentral, was für die Benutzer keine aufwändigen Sicherheitsaufgaben nach sich zieht.

Secure Voice over IP

Der Sprach*fehler* ist vorprogrammiert

Voice over IP ist tot. Es lebe Voice over IP. Denn VoIP war und ist nicht gleich VoIP. Nachdem die Telefonie via IP-Netzwerk in den 90er- Jahren des letzten Jarhunderts nach einem anfänglichen Hype aufgrund Quality-of-Service-Problemen wieder verschwand, so erlebt das Kommunizieren via IP-Netz nun einen veritablen Ansturm. Allerdings einen mit Pferdefuss.

Von Beat Püntener

Das Telefonieren über Datennetze ist wieder in aller Munde – zum zweiten Mal nach dem ersten Hype in den 90er- Jahren. Telefonieren via Internet oder IP-Netz findet heute nicht zuletzt dank Breitbandanschlüssen und Freeware-Tools wie Softphones, NetMeeting, Messengers etc. wieder vermehrt seine Anhänger.

Nicht umsonst haben ADSL sowie die weiteren Breitbanddienste nun den Siegeszug der IP-Telefonie eingeläutet. Die von vielen Organisationen aus Kostengründen avisierte Sprachübermittlung via Computernetze hat unbestreitbar viele Vorteile: Der Arbeitsplatz ist plötzlich mobil geworden. Einen Mehrwert gegenüber der konventionellen Telefonie stellt auch die Erreichbarkeit dar, welche mittels VoIP gewährleistet werden kann. Dies kommt vor allem in unwegsamem Gelände zum Tragen, wo kein IP-Netzwerk vorhanden ist. Ausserdem fallen wie erwähnt die hohen Sprachgebühren weg und nur noch ein einziges Netz muss organisationsweit betrieben werden. Damit die so eingesparten Kosten nicht durch die Hintertüre wieder ins Haus flattern, bleibt eine einzige Frage noch zu beantworten: Wie steht es mit der Sicherheit?

Anders als bei Computernetzwerken geht man landläufig beim Telefon als von einer sicheren Kommunikationsinfrastruktur aus. Was jedoch, wenn beide Anwendungen konvergieren, d.h. die Telefonie über das IP-Netz abgewickelt wird? Je mehr sich die IP-Telefonie ausbreitet, desto wichtiger wird das Thema «Security». Das grundsätzliche Problem der IP-Telefonie ist gleichzeitig deren Hauptvorteil – nämlich die Konvergenz der Netze. Das Telefonieren läuft hier über dasselbe Datennetz, auf welches sich Hacker schon seit Jahren eingeschworen haben. Analysten der Gartner Group warnen davor, dass VoIP die Gefahren von Cyber-Kriminalität erhöhen wird. Vor allem Denial-of-Service-Attacken können auch mittels VoIP Tür und Tor offen stehen. Eine weitere Knacknuss stellen Viren und Hackerangriffe dar. Durch einen gezielten Angriff lässt sich via Eindringen in das Computernetz eines Unternehmens die gesamte Kommunikation offen resp. lahm legen. Ganz zu schweigen von der via Internet relativ günstig erhältlichen Freeware, welche den sprachlichen Datenpaketen auf die Schliche kommt. www.ethereal.com zum Beispiel.

Die gute Nachricht zuletzt: Sie können sich und Ihre IP-Telefonie schützen – *rufen* Sie uns einfach an, und wir *sagen* Ihnen, was Sie tun können.
++41 41 749 22 77

*Beat Püntener ist Product Manager VoIP.

CRYPTO-TETRA-LÖSUNGEN *Inhalt: Martin Maron, Redaktion: Catherine Frigo**

GEBÜNDELTE KRISENBEWÄLTIGUNG – AUF NUMMER SICHER

Ein Krisengipfel mit Beteiligung von mehreren Staatspräsidenten, der Zusammenbruch eines Bankenkonglomerats oder der Amoklauf eines Todesschützen: verschiedene Ereignisse, welche eines gemeinsam haben: Sie müssen von Behörden reibungslos verarbeitet werden und stellen auch spezielle Anforderungen an deren Netzwerke. Anspruch Nummer eins an ein mobiles Behördennetzwerk ist die unter allen Umständen zu gewährleistende Funktionalität. Eine Anforderung, der TETRA bestimmt genügen kann. Anspruch Nummer zwei: der Schutz der übermittelten Botschaften. Und hier kommt die Crypto(logie) ins Spiel. Eine Übersicht.

Die Veranstalter der Olympischen Spiele in Peking ebenso wie Europas grösster Flughafen London Heathrow oder die Polizeiverbände von Hong Kong stellen hohe Ansprüche an die mobile Kommunikationstechnik. Ansprüche, welche GSM, GPRS resp. UMTS nicht mehr erfüllen können. Den spezifischen Anforderungen wie bedingungsloser Funktionalität auch beim Totalausfall des Netzes, der Möglichkeit für Gruppenrufe sowie der Priorisierung der Anrufer genügt nur das TETRA-System, welches auch eigens zu diesem Zweck entwickelt wurde. Das digitale Bündelfunksystem kommt nicht nur zum Einsatz, wenn regionale Krisen wie beispielsweise ein Absturz einer Linienmaschine bewältigt werden müssen, sondern findet seine Verwendung mehr und mehr auch in der grenzüberschreitenden Verbrechensbekämpfung. Auch das organisierte Verbrechen macht die Globalisierung mit und hat grosse finanzielle Mittel zur Verfügung. Dementsprechend sind eine enge Kooperation und eine funktionierende Kommunikation unerlässlich für die Arbeit von Rettungs- und Sicherheitsdiensten auf lokaler, nationaler und internationaler Ebene. Die gemeinsame Nutzung von TETRA-Infrastrukturen bringt es mit sich, dass alle beteiligten Organisationen ein hohes Sicherheitsrisiko eingehen. Die Wege sind leicht zugänglich und Missbräuchen Tür und Tor geöffnet. Die Wahrung der Kommunikationssicherheit ist trotz gemeinsamer Nutzung der Infrastruktur kein Ding der Unmöglichkeit, indem im TETRA-Netz zirkulierende Gespräche und Daten mit einem jeweils eigenen Chiffriersystem geschützt werden können. End zu End oder Punkt zu Punkt. Etwas, was die defaultmässig integrierten TETRA-Sicherheitsfunktionen nicht zu bieten vermögen.

Aber schön der Reihe nach: Befindet sich Ihr TETRA-Netz noch in der Planung? Verfügen Sie zwar über ein Bündelfunknetz (TETRA), doch noch über keine Ihren Ansprüchen genügende Hochsicherheitslösung? Oder sind Sie am Schutz Ihrer TETRA-Infrastruktur und Ihrer -Links interessiert?

Der Link zum sicheren TETRA-Netz

Ihr TETRA-Netz befindet sich noch in der Planungsphase

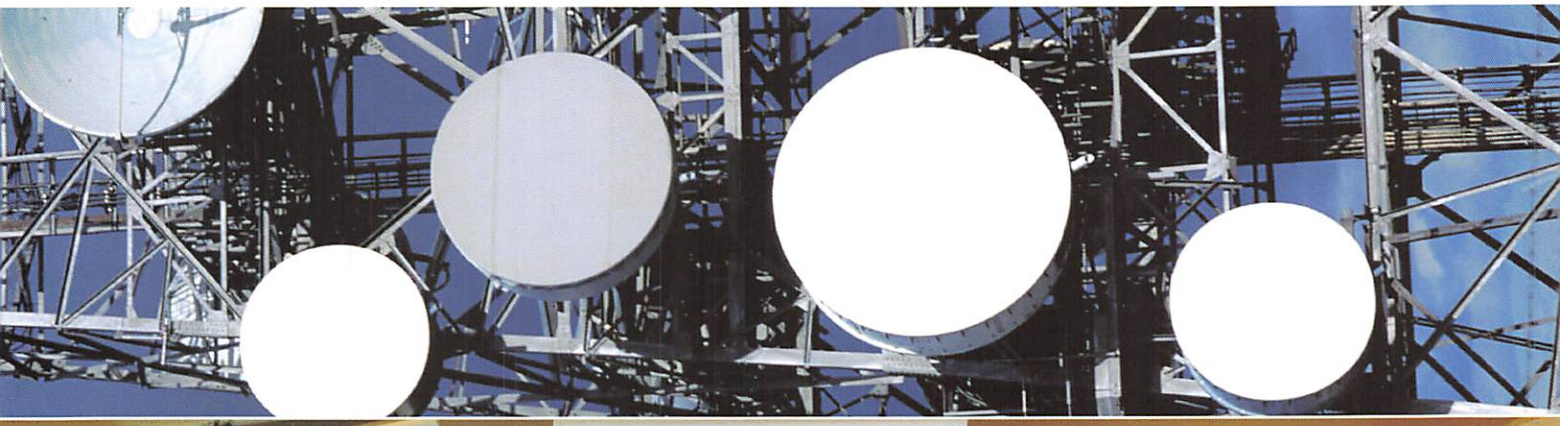
Viel Ehr bringt auch viel Feind mit sich. Nicht umsonst umgeben sich Regierungsmitglieder und Staatspräsidenten zu ihrem persönlichen Schutz mit Garden, welche sich jederzeit untereinander verständigen können müssen. Dabei weisen die grösstenteils per Funk zirkulierenden Mittei-

lungen einen hohen Sensibilisierungsgrad auf: Welcher Minister will denn schon, dass seine genaue Reiseroute durchsickert …

Sichere Bündelfunksysteme bestehen nicht nur aus Terminals und Infrastruktur, also Hardware. Ebenso benötigt wird auch eine geeignete «Software» – umfassendes Know-how genannt. Know-how in der Planung und der Implementierung von Systemen und dem dazugehörenden Security Management. Dazu gehören eine Bedarfsanalyse ebenso wie Vor-Ort-Abklärungen. Und Feldversuche ebenfalls wie System-Engineering. Die Crypto AG verhilft somit zur Planung und zum Aufbau eines hochsicheren TETRA-Systems SEETRA mit mehreren Basisstationen. Wir liefern die Infrastruktur inklusive Managementsystem. Wobei TETRA-Netze von einer bis zu einer Vielzahl von Zellen möglich sind, Zellen, welche auch mobil eingesetzt werden können. Mit SEETRA erhalten die Elitetruppen der Regierungsmitglieder also die «Lizenz» zum Kommunizieren – sicher kommunizieren. Und das bei skalierbarer Verfügbarkeit, denn die gesicherten (chiffrierten) Anrufe und Daten können global übermittelt werden.

Das TETRA-Netz besteht – jedoch nur mit Default-Schutz

Antiterroreinheiten haben die Besonderheit, dass sie vorzugsweise keine Schreibtischtäter sind, das heisst einer mobilen Erreichbarkeit in einem sehr flexiblen Aktionsra-



dius bedürfen. Ausserdem muss der Anschluss an existierende Netzwerke ständig gewährleistet sein.
TETRA-Netze – egal welcher Provenienz – sind in der Regel optional mit «Air Interface Encryption», dem Schutz der Funkstrecke, ausgestattet. Was für Hochsicherheitszwecke nicht ausreicht. Gerade Antiterroreinheiten brauchen einen End-End-Schutz über die gesamte Kommunikationsstrecke hinweg, um den weit verzweigten und autonom agierenden Terrorgruppen Einhalt zu gebieten. Und dies für existierende öffentliche als auch für private Netzwerke. Dabei werden zur Bekämpfung des organisierten Verbrechens absolut vertrauenswürdige Kommunikationskanäle benötigt, welche gemeinsam oder in verschiedene Gruppen aufgeteilt genutzt werden können. Ein solcher gemeinsamer Kommunikationskanal kann mit Crypto TETRA Terminals geschaffen werden. Denn diese Kanäle werden aus nahe liegenden Gründen nicht im Klartextmodus, sondern auf einer gemeinsamen kryptografischen Basis betrieben, wobei die Umschaltung wie ein normaler Gruppenwechsel erfolgt. Das Security Management erfolgt dabei physisch getrennt vom bereits bestehenden Netz. Informationssicherheit ist immer kompromisslos.

Das TETRA-Netz ist End-End-geschützt – die Infrastruktur und die Links jedoch noch nicht
Wenn die Finanzpolizei gegen Steuersünder ihre Tätigkeit aufnimmt und verdächtige Kapitaltransaktionen und Finanzströme überwacht, um fiskalischen Delinquenten auf die Schliche zu kommen, bedarf sie eines sowohl physisch getrennten als auch hochsicheren Netzwerkes. Dies als Schutz gegen eine unerwünschte (Fremd-)Analyse des zirkulierenden Datenstromes sowie das Abhören der Linkverbindungen (Link Eavesdropping). Denn wenn auch «Air Interface Encryption» und «End-End-Schutz» bestehen, so kann die verwundbare Stelle noch immer in der Infrastruktur lauern. Wo auch Schutz gegen Traffic-Analyse benötigt wird (wie das Auslesen von Steuer- und Kontrollinformationen; z.B. von temporären Benutzeridentifikationsnummern, Standorten, Verbindungshäufigkeiten etc.), kann der Schutz der TETRA-Infrastruktur mit zusätzlicher Linkchiffrierung – ebenfalls im Angebot von Crypto AG – realisiert werden. So können keine Rückschlüsse auf operationelle Aktivitäten, Wichtigkeit und Bewegungsprofile von einzelnen Teilnehmern oder gar Organisationen im Netzwerk aus den abgehörten Daten gezogen werden.

Was Sie zudem erwartet
Weitere Vorzüge machen die Crypto-Chiffrierung einzigartig: Sie erhalten Ihre eigene nationalisierbare kryptografische Lösung und Ihren eigenen geheimen Algorithmus – den Sie jederzeit verändern können. Die Abdeckung des Netzes wird zu keiner Zeit beeinträchtigt und die Sprecherkennung funktioniert tadellos. Was wollen Sie mehr …

*Martin Maron ist Senior Program Manager und Catherine Frigo Corporate Editor.

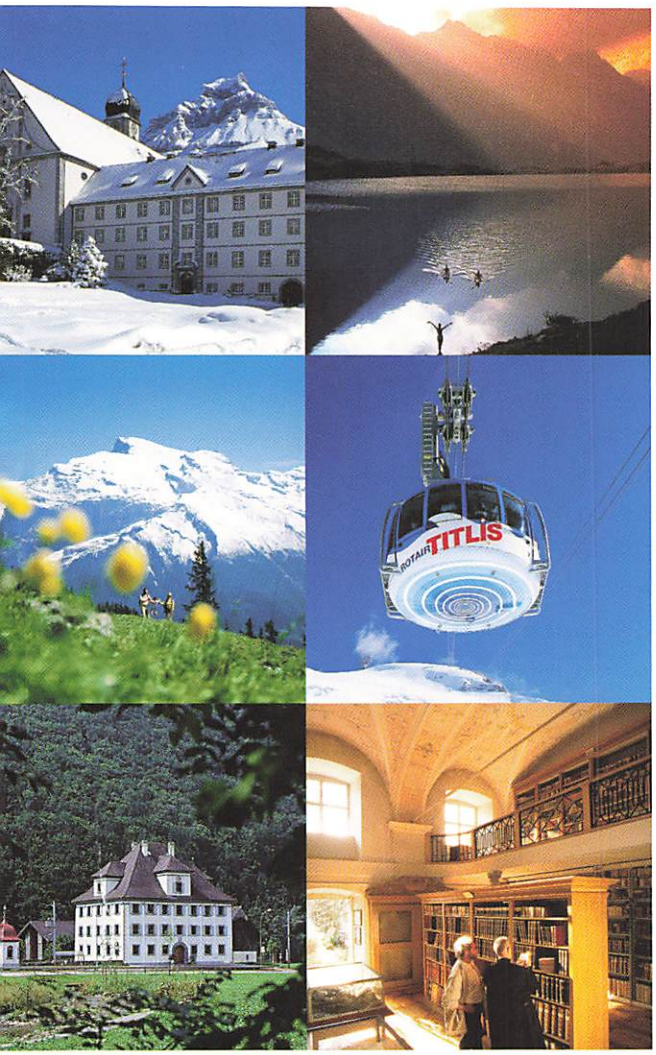
VIER WALDSTÄTTEN *Catherine Frigo*

UND EWIG LOCKT DER TITLIS

Mount Titlis – zweitberühmtester Schweizer Berg und einer der zentralen Anziehungspunkte der Grossregion Luzern. Die erste drehbare Luftseilbahn der Welt bietet auf dem Weg nach oben eine atemberaubende Aussicht auf das Dorf Engelberg sowie den ganzen Kanton Nidwalden und die Berner Alpen. Für viele Urlauber ist die Ankunft auf dem Gipfel auf 3239 Metern über Meer auch gleichbedeutend mit dem erstmaligen Anblick von (ewigem) Schnee.

Abweisend und anziehend zugleich, erhebt sich im Talkessel von Engelberg der felsige Gipfel des Titlis über einem vergletscherten, mit ewigem Schnee bedeckten Bergmassiv. Die Gondelbahn, die zum höchstgelegenen Aussichtspunkt der Zentralschweiz führt, schwebt über zerklüftetes Eis und dreht sich während der fünfminütigen Fahrt um die eigene Achse und bietet eine einzigartige Rundumsicht auf die halbe Schweiz. So viel zur Prospektsicht.[1]

Der Titlis ist natürlich als eine der Hauptattraktionen der Zentralschweiz vor allem Ziel von unzähligen Ausflüglern und Sportlern. Der Gipfel lockt sommers wie winters mit ewigem Schnee, welcher sowohl von innen wie auch von aussen bewundert werden kann. Eine Eisgrotte führt in das Innere des Titlisgletschers – ein gut gesicherter Gletscherweg ein Stück weit in diesen hinein. Mutig, wer mit den Skis oder dem Snowboard trotz sich öffnenden Spalten darüber hinwegflitzt.



Den Titlis als reinen Anziehungspunkt für Touristen zu gewichten, da täte man dem «Wendenstock» jedoch Unrecht. Der Berg spielt auch im Bereich der Energiegewinnung eine nicht zu unterschätzende Rolle. Gerade in Zeiten der steigenden Erdölpreise wird der auf dem Gipfel des Berges befindlichen höchsten Windkraftanlage Europas eine steigende Bedeutung zukommen. Die Anlage produziert 30 Kilowattstunden Energie, was ausreicht, den Betrieb der Drehbahn zu unterhalten. Die Anlage ist zwar bereits 12 Jahre im Betrieb, arbeitet jedoch nach den modernsten Auftriebsprinzipien: Die Rotoren arbeiten nach demselben System, wie es auch im Flugzeugbau zur Anwendung gelangt. Noch eine weitere Alternativenergie wird auf dem Titlis gewonnen: Bei der Zwischenstation Stand befindet sich die höchstgelegene fotovoltaische Versuchsanlage überhaupt.

Geheimnisvolles Goldloch Arnialp

Etwa 300 Meter über dem Talboden liegt eine kleine Hochebene, die Arnialp, welche im Sommer von den Sennen und dem weidenden Vieh bevölkert wird, im Winter aber den Steinböcken, Murmeltieren und Berggeistern gehört, damit diese dort ungestört ihr Dasein fristen können.

Irgendwo am Hang über der Arnialp befand sich eine grosse Höhle. Niemand wagte es, sich dieser zu nähern, wusste man doch, dass dort geheimnisvolle Geister ihr Unwesen trieben. Diese verstanden es jedoch, grosse Reichtümer aus den Tiefen des Berges zusammenzutragen; gold- und silberhaltige Erze, welche sie in Barren umgossen. In einsamen Nächten hörte man das Klopfen und Hämmern weit herum.

Eines Abends sassen Sennen in ihrer Hütte auf der Arnialp beim Nachtessen, als ein kleines, schwarz gewandetes Männchen eintrat. Die Älpler wollten mit dem seltsamen Gast nichts zu tun haben; schon gar nicht, als er mit den Sennen zum Arniloch, der berüchtigten Höhle, aufbrechen wollte. Ein jugendlicher Gehilfe der Sennen anerbot sich dann trotzdem, den schwarz Gekleideten zu begleiten. Er erhoffte sich, so zu einem sagenhaften Goldreichtum zu gelangen.

Der langen Rede kurzer Sinn: In der Höhle angekommen, nahm der Fremde dem Jüngling das Versprechen ab, kein Wort mehr zu sagen. Dann begann er, beschwörende Formeln zu murmeln, worauf innerhalb des Berges ein Getöse anschwoll, welches immer näher kam. Sein Versprechen vergessend, stiess der Jüngling alsbald einen gellenden Schrei aus. Daraufhin wurde er aus der Höhle geschleudert, wo er von den nachkommenden Sennen gefunden wurde. Er konnte jedoch nichts mehr berichten und musste alsbald sein Leben aushauchen. Seine Goldgier wurde ihm so zum Verhängnis. Die Höhle aber stürzte ein und blieb bis heute verschüttet.

Quelle: Engelberger Sagen

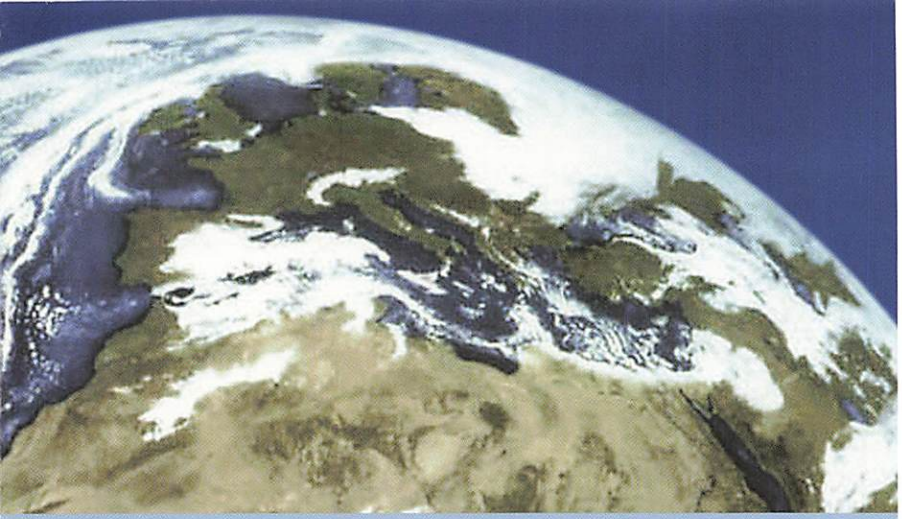
Engelberg

Die Geschichte Engelbergs geht auf die Gründung des Benediktinerklosters zurück. Einer Sage gemäss hatte der Gründer des Klosters, Konrad von Sellenbüren, Engelsstimmen gehört, welche ihm verkündeten, eine «Gott geweihte Stätte» zu gründen. Nach dem Bau des Klosters um 1120 standen Abt Adelhelm und Konrad von Sellenbüren auf der oberen Erlenmatte in der Nähe der Adelhelmsquelle. Sie suchten nach einem Namen, der zu diesem Kloster sinnvoll passen sollte.

Plötzlich hörten sie wiederum Engelsstimmen, und als sie zum nahegelegenen Berg emporblickten, sahen sie einen Chor von Himmelsboten, welcher mit zauberhafter Stimme ein Lob auf den Berg der Engel sang: Von da an sollte das Kloster und das dazugehörende Dorf Engelberg heissen.

Quelle: Engelberger Sagen

[1] Quelle: Engelberg-Titlis Tourismus AG



Messen

IDEX, 12.–17. Februar 2005 in Abu Dhabi.

Neue Publikationen

Crypto TETRA Terminals
«Eine TETRA-Infrastruktur ist teilbar – Ihre Sicherheit nie!»

Crypto SEETRA
«Ein absolut sicheres TETRA-System erhalten Sie nur, wenn Sie auch die Infrastruktur selber kontrollieren.»

Crypto Broadband
«Uneingeschränkte Breitbandkommunikation. Netzwerk-Sicherheitslösungen von Crypto AG.»

Bestellungen unter: marketing@crypto.ch

Pressespiegel

Putting a Face to Big Brother

Literally putting a face on technology could be one of the keys to improving our interaction with high-tech gadgets.

Imagine a surveillance system that also presents a virtual embodiment of a person on a screen who can react to your behaviour and perhaps even alert you to new e-mails. Basic versions of these so-called avatars already exist. Together with speech and voice recognition systems, they could replace the keyboard and mouse in the near future.
Some of these ideas have been showcased at the London's Science Museum, as part of its Future Face exhibition. One such avatar is Jeremiah. It is a virtual man, which you can download for free and install in your computer. "I am interested in the interaction, providing the ability of a system to watch what's going on and make decisions based on that," explained his creator, Richard Bowden, lecturer at the Centre for Vision, Speech and Signal Processing at the University of Surrey... Jeremiah is a virtual face that attempts to emulate humans in the way it responds to activity. ... It works on vision, reacting in a preset way to the information provided by a surveillance tracker system. The research comes at a time when people are having to cope with an increasing numer of high-tech gadgets. Experts say a much more natural way to interact with these devices, such as a virtual human, could make it much easier to make the most of all those new gizmos. "If you get up at three o'clock in the morning and go downstairs, there are probably two things you are going to do: either going to the bathroom or maybe you are going to make a cup of tea," said Dr. Bowden. "Now if the system can watch your behaviour over time, it can learn this, so it would predict what you are going to do, turn on the lights for you, or, before you even get to the kettle, it could have switched it on." You might even be able to tell your home surveillance system that you will be going away on holiday, and ask if it could make sure that the house is secure once you have left. This might sound like a scary vision of an Orwellian future. But it might all depend on the face that is watching you. "When we put the surveillance cameras in our centre, a lot of people were very unhappy about the fact that there was a system watching them," said Dr. Bowden. "But when Jeremiah's camera went in, nobody minded, because although it's still watching them, they could see what it was watching."

BBC News 8 November, 2004

HAGELIN-CRYPTOS
CRYPTO AG

Crypto AG, Hauptsitz

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

Crypto AG, regionale Büros

Abidjan
Crypto AG
01 B.P. 5852
Abidjan 01
République de Côte d'Ivoire
Tel. +225/22 41 17 71
Fax +225/22 41 17 73

Abu Dhabi
Crypto AG
Regional Office Middle East
P.O. Box 41076
Abu Dhabi (UAE)
Tel. +971 2/44 55 737
Fax +971 2/44 55 151

Buenos Aires
Crypto AG
Maipu 1256 PB «A»
1006 Buenos Aires (Argentina)
Tel. +54 11/4312 1812
Fax +54 11/4312 1812

Kuala Lumpur
Crypto AG
Regional Office Pacific Asia
No. 2 Jalan SS7/11 Kelana Jay
47301 Petaling Jaya (Malaysia)
Tel. +60 3/7872 2150
Fax +60 3/7872 2140

Riyadh
Crypto AG Representative Offic
P.O. Box 59701
Riyadh 11535
Kingdom of Saudi Arabia
Tel. +966 1/454 1011
Fax +966 1/454 9030

Sultanate of Oman
Crypto AG Representative Offic
P.O. Box 2911
Postal Code 111
Seeb
Sultanate of Oman
Tel. +968 504 966
Fax +968 504 929

Um wen handelt es sich?

Die gesuchte Person ist ...

Diesmal suchen wir eine Person, welche im Jahre 1912 in London geboren wurde. Der Vater arbeitete bei einer indischen Zivilverwaltung; die Eltern kamen jedoch zur Geburt der gesuchten Person eigens nach England. Einige Wochen nach der Geburt kehrte die ganze Familie wieder nach Indien zurück. Mr. oder Mrs. «Unknown» wuchs in der Obhut von Kindermädchen und im Internat auf, wo bei der Person eine gewisse Schüchternheit und Ungeschicklichkeit, indes auch ein grosses Talent auf naturwissenschaftlichem Gebiet festgestellt wurde. Bereits im zarten jugendlichen Alter folgten Experimente und Forschungen in Kooperation mit einem Freund, mit welchem die Person mehr als freundschaftliche Gefühle verbanden.

Zur Zeit des Eintritts in das Cambridge Kings College im Jahre 1931 wurde auch gleich die Mathematik als allmächtige Wissenschaft entthront, was unsere gesuchte Person dazu bewog, einen einflussreichen mathematischen Aufsatz «on computable numbers» zu verfassen. Darin war von einer imaginären Maschine die Rede, welche eine bestimmte rechnerische Operation ausführen konnte, indem man in diese Maschine über einen Papierstreifen Zahlen einlas und das Ergebnis über einen Papierstreifen ausgegeben wurde. Diese ausbauend entstand das Konzept einer universellen Maschine, welche in der Lage war, auf jede logisch beantwortbare Frage eine Entgegnung zu finden. Die Zeit war damals nur noch nicht reif, das Konzept technisch auch umzusetzen. Trotzdem wurde diese Maschine als Erfindung des Jahrhunderts gewertet und verschaffte der gesuchten Person die benötigte Anerkennung.

Zu Beginn des Zweiten Weltkriegs begann für die gesuchte Person eine neue Ära, nämlich die Aufnahme der Arbeit ausserhalb Londons – in aufklärerischer Mission. Dabei beschäftigten sich die dort angesiedelten Wissenschaftler vor allem mit einer Frage: Was, wenn der Feind den Code statt zwei- nur noch einmal übermitteln würde? Die Hauptaufgabe der gesuchten Person bestand nun darin, für diesen Fall eine neue Taktik zu erarbeiten. Dies gelang ihr, indem sie eine aus verschiedenen Maschinen gekoppelte «Super-Maschine» entwickelte, welche dank ihrer durchschlagenden Wirkung auch «Sprengkörper» genannt wurde. Diese Erfindung soll wesentlich zum Erfolg der Alliierten gegen Deutschland beigetragen haben.

Trotz dieser bahnbrechenden Erfindung und des damit verbundenen Erfolges hatte die gesuchte Person in der Gesellschaft einen schweren Stand: Angezeigt wegen Sittenlosigkeit und nach einer aufgezwungenen Hormonbehandlung in schwere Depressionen verfallend, nahm sie sich im Jahre 1954 das Leben.

Um wen handelt es sich?

Senden Sie die Lösung bis am 31. Januar 2005 an catherine.frigo@crypto.ch. Ab 1. Februar wird die Lösung auf unserer Website www.crypto.ch publiziert.

Zu gewinnen gibt es 3 USB Memory Sticks Cruzer Mini 256 MB PC und Mac-kompatibel.

Der Rechtsweg ist ausgeschlossen. Nicht offen steht der Wettbewerb den Mitarbeitern der Crypto AG.

Die Gewinner des CryptoMagazine-Wettbewerbs 2/2004 kommen aus der Schweiz, Chile und aus Oman.