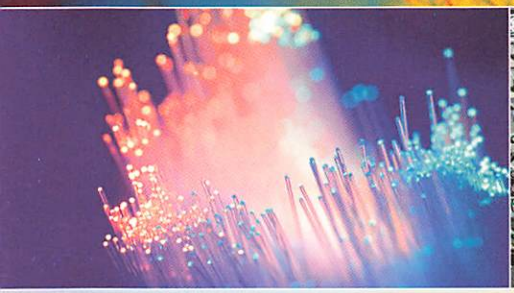
CRYPTOMAGAZINE

HAGELIN-CRYPTOS
CRYPTO AG

Zeitschrift für die Kunden von Crypto AG, Schweiz 2 • 2007



HIGHSPEED NEEDS HIGH PROTECTION

Liebe Leserin, lieber Leser

Der Wissensarbeiter des 21. Jahrhunderts funktioniert – im Gegensatz zum Industriearbeiter des 20. Jahrhunderts – ohne Internet nicht mehr. Das weltumspannende Netz ist der wichtigste Kommunikationskanal und Quelle zur Informationsbeschaffung. Die Datenmengen, welche über die weltweiten Datennetze laufen, steigen exponentiell. Heute spricht man von Datenraten bis 10 Gigabits pro Sekunde – dies würde ungefähr 300'000 A4-Seiten Text entsprechen –, die auf einer einzelnen Verbindung übertragen werden können.

Die Menge an Daten, d.h. an Information steigt gewaltig. Doch nicht jede Information ist gleich wertvoll. Den Wert bekommt sie erst durch Relevanz. Ein guter Weg, um die Relevanz von Information darzustellen und damit wertvolle Information von weniger wertvollen zu trennen, ist Klassifizierung. Wertvoll bedeutet zudem auch schützenswert. Dies gilt für Information – wie beispielsweise auch für Rohstoffquellen. Ein guter Weg, um wertvolle Information auf dem Weg durch die weltumspannenden Datennetze zu schützen, ist Verschlüsselung. Dabei kann Crypto AG Sie unterstützen. Mit unserer neuen Chiffrierlösung, Ethernet Encryption HC-8555 10G, können Sie auch grosse Datenraten bis 10 Gigabits pro Sekunde hochsicher verschlüsseln. Und Ihre wertvolle Information bleibt geschützt.

Ich wünsche Ihnen eine spannende und interessante Lektüre.

Giuliano Otth

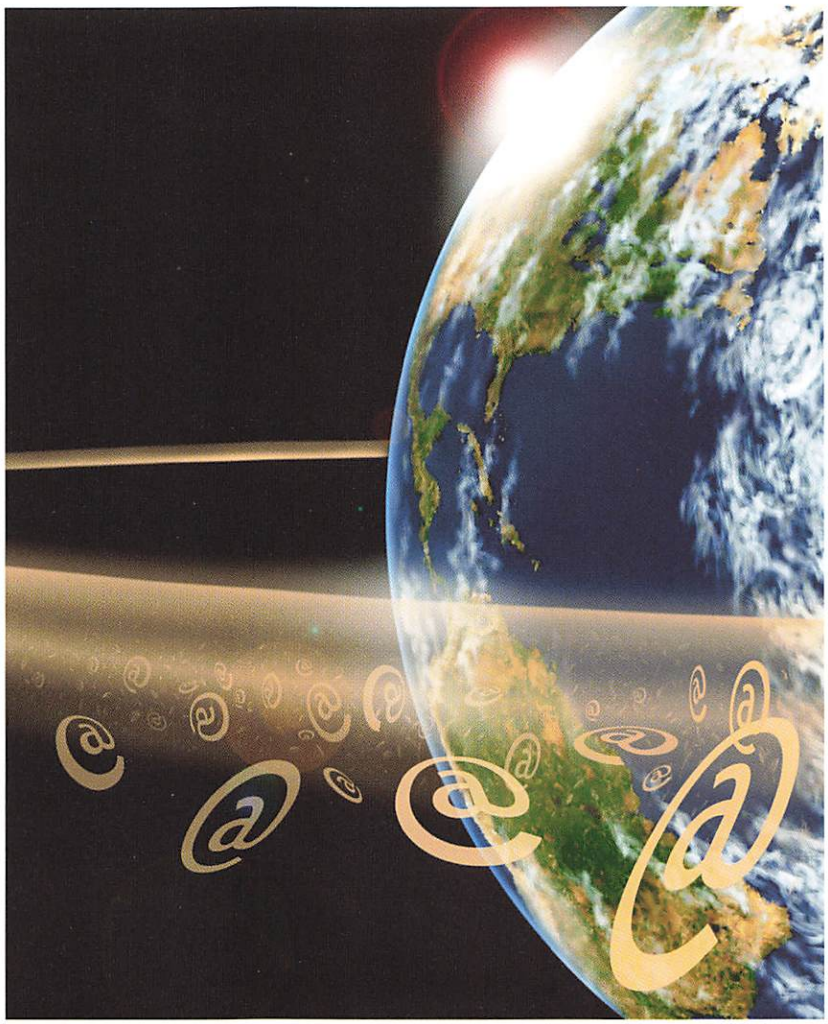
President and Chief Executive Officer

HERAUSFORDERUNGEN BEI DER SICHERUNG KRITISCHER INFORMATIONSINFRASTRUKTUR

«HIGHSPEED NEEDS HIGH PROTECTION»

Die moderne Welt ist in einer noch nie da gewesenen Weise abhängig von Highspeed-Informations- und Kommunikationssystemen und von deren hoher und unterbruchsfreier Verfügbarkeit. Diese so genannten kritischen Informationsinfrastrukturen sind unterschiedlichsten Bedrohungen durch Mensch und Natur ausgesetzt. Dem guten Schutz dieser Infrastrukturen kommt deshalb eine grosse Bedeutung zu.

*Beatrice Huber und Dr. Silvan Frik**



Highspeed ist gefragt. Der moderne geschäftliche und auch private Benutzer von Telekommunikation hat sich sehr schnell daran gewöhnt, dass diese Dienstleistungen highspeed und unterbruchsfrei zur Verfügung stehen und dies, bevorzugt zu günstigen Preisen, immer und überall. Der so genannte Breitband-Internetanschluss gilt vielleicht schon bald als «Menschenrecht». Ein Arbeiten ohne «schnelle Leitungen» wird undenkbar. Die International Telecommunication Union ITU definiert Breitband (im Unterschied zu Schmalband) als Datenübertragungsrate, die schneller ist als die Primärmultiplexrate von ISDN, d.h. 1,5 oder 2,0 Megabits pro Sekunde (Mbit/s). Aktuelle Highspeed-Kommunikationsnetze tauschen Daten bereits mit Raten von über einem Gigabit pro Sekunde (Gbit/s) aus.

In den USA verfügten Ende 2006 fast 80 Prozent der Internetbenutzer zu Hause über einen Breitbandanschluss. Die Schweiz geht noch einen Schritt weiter. Im Herbst 2006 hat der Schweizer Bundesrat beschlossen, dass ab dem 1. Januar 2008 Breitband-Internetanschluss zur Grundversorgung aller Schweizer Haushalte gehört. Zwei weitere Beispiele: Singapur will gemäss dem Masterplan «Next Generation National Broadband Network» bis 2015 Datenraten zwischen 100 Mbit/s bis über 1 Gbit/s für Heimanschlüsse, Schulen und Geschäfte aufbauen. In Australien hat im März diesen Jahres die Oppositionspartei, die Labor Party, ein Projekt vorgestellt, mit dem 98 Prozent aller Australier an Breitbanddienste angeschlossen werden sollen. Der Auf- und Ausbau von Highspeed-Kommunikationsnetzen ist weltweit im Gange.

Die moderne Gesellschaft befindet sich jetzt schon in einer noch nie da gewesenen Abhängigkeit von Highspeed-Informations- und -Kommunikationssystemen und von deren dauernden Verfügbarkeit. Ein längerer Ausfall hätte gravierende Folgen für die Wirtschaft und die innere Stabilität der betroffenen Staaten. Solche Informations- und Kommunikationssysteme werden deshalb kritische Informationsinfrastrukturen (zu Englisch Critical Information Infrastructure CII) genannt. Diese dienen dem Staat und der Wirtschaft als zugrunde liegende und tragende Infrastrukturen. Besonders anfällige Bereiche bei Staat und Wirtschaft sind beispielsweise die Stromversorgung, die Finanzwelt oder das Gesundheitswesen. Diese kritischen Infrastrukturen müssen funktionieren, damit die innere Stabilität und die nationale Sicherheit von Staaten

garantiert werden können und so die Staaten «gedeihen». Staaten sind deshalb am Schutz der Informationsinfrastrukturen (zu Englisch Critical Information Infrastructure Protection CIIP) interessiert.

Gefährdung von aussen und innen

Kritische Informationsinfrastrukturen sind unterschiedlichsten Bedrohungen ausgesetzt: beispielsweise Stromausfällen. Da Informationsinfrastrukturen ohne Strom nicht funktionieren, ist eine ausreichende und vor allem zuverlässige Versorgung mit Elektrizität lebenswichtig. Weitere Bedrohungen sind Naturkatastrophen wie Erdbeben oder Wirbelstürme oder direkte Aktionen von Menschen, bösartig oder «nur» fahrlässig. Informations- und Kommunikationssysteme bieten menschlichen Akteuren mannigfaltige Angriffspunkte, die auch intensiv genutzt werden. So gilt Internetkriminalität als Wachstumsmarkt. Dazu eine Zahl: Gemäss einem Report von IBM wurden im ersten Halbjahr 2005 weltweit mehr als 237 Millionen Attacken auf die Computer-Sicherheit gezählt, wobei die tatsächliche Zahl noch viel höher liegen dürfte. Die häufigsten «Opfer» waren Regierungsstellen.

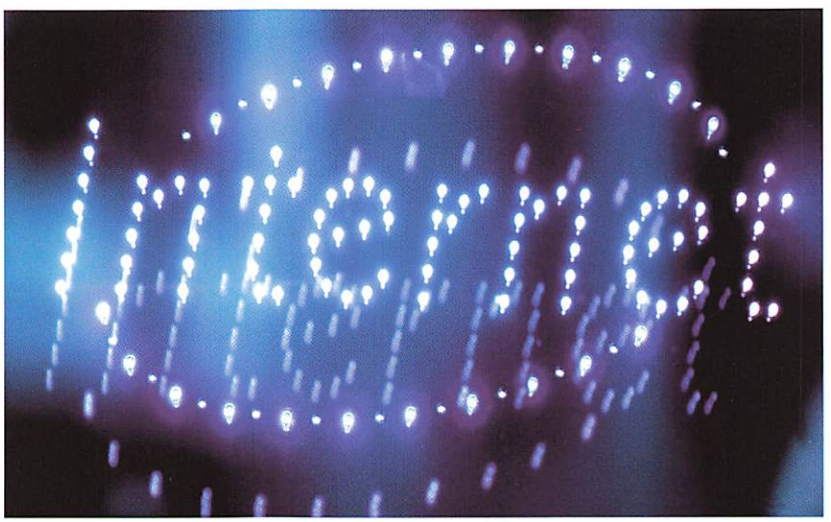
Mögliche menschliche Akteure von bösartigen Operationen sind dabei klassischerweise Hacker und Cracker, die vor allem der Herausforderung und des Ego wegen versuchen, in fremde Systeme einzudringen. Vermehrt sind einzelne Kriminelle oder ganze Organisationen am Werk, welche private und staatliche Computersysteme nach «Leckagen» absuchen, um das Wissen darüber dann gewinnbringend zu verkaufen. Terroristische Gruppen, religiös-fanatische Bewegungen und extreme politische Parteien nutzen das Netz intensiv für Propaganda, Geldbeschaffung und zum Informationsaustausch. Es ist jedoch auch denkbar, dass Terroristen auf diesem Weg versuchen, Staaten oder Organisationen zu «attackieren» und so diesen grossen Schaden zuzufügen. Weitere Akteure sind klassischerweise Staaten, welche feindliche und auch verbündete Staaten ausspionieren. Bösartige Aktionen können auch von innen, d.h. beispielsweise von frustrierten Mitarbeitenden ausgehen, die sich an ihrer Organisation «rächen» möchten. Nicht ausser Acht gelassen werden darf jedoch auch die Tatsache, dass eine Applikation falsch bedient oder ein klassiertes Dokument falsch gehandhabt werden kann. So kann ein Informationsverlust ohne böse Absicht und vermutlich sogar ohne Kenntnis der Betroffenen eintreten. Auch im Falle eines Wechsels der Arbeitsstelle nimmt der Mitarbeitende eine Fülle von Informationen mit. Kritische Informationsinfrastrukturen können sich jedoch auch selbst bedrohen. Diese Systeme wurden vielfach Stück um Stück aufgebaut und vernetzt und haben in der Zwischenzeit einen Komplexitätsgrad erreicht, sodass solche Systeme nicht mehr als inhärent sicher und stabil angeschaut werden können. «Zufällige» Fehlfunktionen werden möglich, die durch Kettenreaktionen zu grossflächigem Ausfall von Infrastrukturen führen können.

Es ist nun mal so, dass gerade moderne Informations- und Kommunikationssysteme entworfen wurden, um die Effizienz oder die Zuverlässigkeit der Kommunikations- und Informationsprozesse zu steigern, und eben nicht mit dem Ziel, die Sicherheit in einem komplexen, heterogenen Umfeld zu verbessern.

Trend der Privatisierung und Aufgabe des Staates

In den 90er-Jahren des letzten Jahrhunderts setzte weltweit – gefördert und beschlossen durch die Welthandelsorganisation WTO – eine Privatisierungswelle von Wirtschaftsbereichen ein, die bislang vom Staat betrieben und kontrolliert wurden. Dazu zählt neben der Wasser- und Stromversorgung sowie dem Transportwesen auch der Bereich Telekommunikation. Die Privatisierung führte zu einer Fragmentierung beim Besitz, d.h. statt einem Besitzer – dem Staat – gibt es nun viele. Dies generiert Koordinationsbedarf, um das reibungslose Funktionieren der Wirtschaftsbereiche zu garantieren. Der Trend der Privatisierung wurde und wird zudem durch die Globalisierung verschärft, da die privaten Besitzer nicht nur aus der entsprechenden Nation selbst stammen, sondern auch aus anderen Ländern – benachbart oder vom anderen Ende des Globus.

Staaten sind am Schutz von Informationsinfrastrukturen interessiert – auch wenn oder gerade weil sie nicht die Besitzer sind –, um die innere Stabilität und die nationale Sicherheit zu garantieren und so Staat und Wirtschaft gedeihen zu lassen. Für diesen Schutz sind Konzepte, so genannte Critical Information Infrastructure Protection Policies, gefragt. Diese widmen sich dem Schutz ganzheitlich und strategisch.



Damit solche Konzepte überhaupt formuliert werden können, müssen zuerst mögliche Risiken und Bedrohungen im Detail beurteilt und geeignete Antworten gefunden werden. Zahlreiche Nationen sowie internationale Organisationen haben sich in den letzten Jahren dem Schutz von Informationsinfrastrukturen gewidmet und Konzepte erarbeitet. Die Herangehensweise ist unterschiedlich, ebenso wie der Erfolg. Dieser ist, so zeigen Untersuchungen, stark davon abhängig, ob und wie gut die Zusammenarbeit zwischen Staat und Wirtschaft in so genannten Public-Private-Partnerships funktioniert.

* Beatrice Huber ist Corporate Editor bei Crypto AG und Redaktionsleiterin des Crypto Magazines, Dr. Silvan Frik ist Head of Marketing Services bei Crypto AG und Lehrbeauftragter für Schweizerische Aussenpolitik an der ETH Zürich.

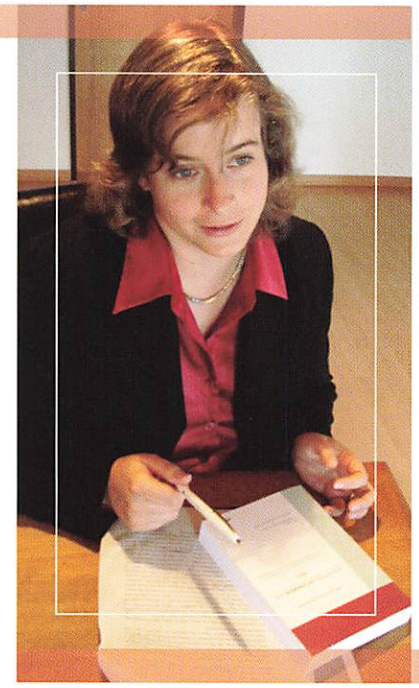
Quelle: Isabelle Abele-Wigert and Myriam Dunn, International CIIP Handbook 2006, Vol. I, Center for Security Studies at ETH Zurich; Myriam Dunn and Victor Mauer (eds.), International CIIP Handbook 2006, Vol. II, Center for Security Studies at ETH Zurich

INTERVIEW MIT DR. MYRIAM DUNN CAVELTY ZU SICHERHEIT IM INFORMATIONSZEITALTER

«ABSOLUT ZENTRAL SIND PUBLIC-PRIVATE-PARTNERSHIPS»

Das Informationszeitalter eröffnet neue Möglichkeiten, birgt aber auch neue Risiken. Was sind das für Risiken? Was sollen bzw. können Staaten für die Informationssicherheit tun? Warum ist die Zusammenarbeit mit der Wirtschaft so wichtig? Das Crypto Magazine sprach mit Dr. Myriam Dunn Cavelty, Leiterin des Forschungsteams «Neue Risiken» am Center for Security Studies der ETH Zürich, über Sicherheit im Informationszeitalter.

Interview: Beatrice Huber



Frau Dunn, Sie beschäftigen sich mit «neuen» Risiken im Informationszeitalter. Was soll man sich unter diesen Risiken vorstellen?

In meiner Forschungstätigkeit beschäftige ich mich mit verschiedenen Aspekten von Risiken und Schutzpraktiken, die im Zusammenhang mit der Informationsrevolution stehen. Solche Risiken werden im Englischen Cyberthreats genannt. Damit sind Aktivitäten gemeint, welche Informationsinfrastrukturen – physische oder virtuelle – entweder zum Ziel haben oder diese als «Waffe» einsetzen. Beispiele für physische Ziele sind Kommunikationssatelliten oder Rechenzentren, Beispiele für virtuelle sind Datenflüsse. Eine «klassische» physische Waffe wäre ein Hammer, mit dem man einen Server zertrümmert. Eine virtuelle «Waffe» wäre ein Computervirus.

Das Forschungsgebiet «Information Age Risks and Countermeasures» untersucht speziell die Risiken, welche der Gesellschaft durch das Informationszeitalter erwachsen, und staatliche Gegenmassnahmen zum Schutz vor diesen Risiken. Dabei stehen gesellschaftliche – und nicht technische – Aspekte im Vordergrund.

Was ist neu an diesen neuen Risiken? Gab es diese früher nicht?

Im Falle der Cyberthreats ist einiges (aber nicht alles) neu: Schon in den 80er-Jahren wurde Datensicherheit als sicherheitspolitisches, jedoch hauptsächlich den Staat betreffendes Problem diskutiert. Neu ist, dass wir es heute mit einem Problem zu tun haben, das die gesamte Gesellschaft betrifft. Die Datenmengen sind in den letzten Jahren enorm gewachsen. Das Internet hat sich durch die Kommerzialisierung stark gewandelt, und die Vernetzung ist seit den 90er-Jahren sozusagen explodiert. Ganz zentral ist, dass es so zu einer Abhängigkeit der gesamten Gesellschaft von nationalen und internationalen kritischen Informationsinfrastrukturen gekommen ist. Diese sind zu verstehen als materielle und informationstechnologische Einrichtungen, Netze, Dienste und Anlagegüter, deren Störung oder Vernichtung gravierende Auswirkungen auf die Gesundheit, die Sicherheit oder das wirtschaftliche Wohlergehen der Bürger sowie auf das effiziente Funktionieren der Regierung eines Landes hätte. Diese Infrastrukturen gelten nicht nur aufgrund technischer Unzulänglichkeiten als inhärent unsicher; sie sind auch besonders anfällig für asymmetrische Attacken seitens staatlicher und nicht-staatlicher Organisationen oder Einzeltäter. Solche Akteure könnten durch die Nutzung weiterverbreiteter Angriffsmöglichkeiten beträchtlichen Schaden anrichten.

Wie hat sich die Wahrnehmung verändert?

Durch die alltägliche Nutzung des Internets, d.h. von vernetzten Rechnern, macht heute jedes Individuum eigene Erfahrungen mit Cyberthreats, beispielsweise mit Computerviren oder Würmern. Das hat die Perzeption der Bedrohung steigen lassen. Darüber hinaus haben die Terroranschläge vom 11. September die Angst verstärkt, dass Gegner ohne jegliche Rücksicht auf zivile Verluste die Gesellschaft da zu treffen versuchen, wo es am meisten weh tut: bei den kritischen Infrastrukturen.

Die Informationsinfrastrukturen, auf denen moderne Gesellschaften ihre wirtschaftlichen und politischen Prozesse aufbauen, sind im Zuge von Liberalisierungen immer mehr in private Hände übergegangen. Was sollte aus Ihrer Sicht der Staat dennoch oder erst recht für die Informationssicherheit tun?

Die Liberalisierung hat bereits vor den 90er-Jahren eingesetzt. Vielen Staaten ist jedoch erst später klar geworden, dass sie damit einen substanziellen Teil ihrer Autorität für das Kollektivgut Sicherheit an die Wirtschaft verloren haben. Der Wirtschaft kommt nun sowohl bei der Definition als auch bei der Umsetzung einer Schutzpolitik eine bedeutende Rolle zu. Zentral ist deshalb, dass die Informationssicherheit nur in Zusammenarbeit von Staat und Wirtschaft, in so genannten Public-Private-Partnerships, gewährleistet werden kann.

Die Verantwortlichkeiten sollten wie folgt verteilt sein: Um den Schutz vor Gefahren im «normalen» Rahmen – dazu gehören neben Hackerangriffen auch kleinere

natürliche Katastrophen – muss der Infrastrukturbetreiber selber bemüht sein. Vom Staat hingegen wird erwartet, dass er Schutz vor Gefahren einer höheren Stufe bieten kann, wie zum Beispiel Angriffe von Terroristen und durch andere Staaten.

Dem Staat kommt auch eine Vorbildfunktion zu. Seine sensiblen Daten muss er natürlich rigoros schützen. Jede grössere Hacker-Attacke in Regierungsrechner – so zeigt das Beispiel USA – führt zu riesigem Imageschaden in der Bevölkerung. Zudem sollte sich der Staat um Awareness-Schulung in der Bevölkerung und um Forschung im Bereich Cyberthreats kümmern, denn viele Aspekte sind noch unklar. Die EU hat dies erkannt und in ihrem 7. Rahmenprogramm zur Forschungsförderung einen Schwerpunkt «Sicherheit» definiert, in dem kritische Infrastrukturen eine grosse Rolle spielen.

Was tun Staaten bereits für die Sicherheit von Informationen und Informationsinfrastrukturen?

Generell umfasst die Sicherung kritischer Informationsinfrastrukturen Programme, Institutionen und Massnahmen zum Schutz von Organisationen oder Einrichtungen mit (lebens-)wichtiger Bedeutung für das staatliche Gemeinwesen. Das primäre Schutzziel sind dabei nicht in erster Linie die Objekte der Infrastruktur, sondern hauptsächlich die Sicherstellung der Robustheit kritischer Dienstleistungen. Dabei muss die langfristige Überlebensfähigkeit aller relevanten Netzwerke gewährleistet werden. Allen bestehenden Initiativen ist infolgedessen die Anlage eines Kooperationsprogramms gemein, welches die Partnerschaft von Staat und Privatwirtschaft beinhaltet. Der Erfolg dieser Programme – dies zeigen die Initiativen in den einzelnen Staaten, beispielsweise der Schweiz – hängt stark vom Vertrauen ab, das zwischen den Partnern aufgebaut werden kann. Der Staat kann der Privatwirtschaft keine «Befehle» erteilen. Das funktioniert nicht. Im Gegenteil: Er muss sich sehr stark als Dienstleister für die Unternehmer verstehen, damit diese auch einen Nutzen in den Schutzmassnahmen sehen. Dann kann der Staat im Endeffekt auch die nationale Sicherheit gewährleisten.

Herzlichen Dank, Frau Dunn, für die Ausführungen!

Dr. Myriam Dunn Cavelty
Leiterin des Forschungsteams «Neue Risiken» am Center for Security Studies der ETH Zürich

Dr. Myriam Dunn Cavelty hat an der Universität Zürich Geschichte, Politikwissenschaft und Völkerrecht studiert. Seit einigen Jahren erforscht sie Risiken und Verwundbarkeiten der Gesellschaft im Informationszeitalter. Seit 2005 leitet sie am Center for Security Studies der ETH Zürich ein Forschungsteam, das sich mit «neuen Risiken» beschäftigt, und koordiniert das internationale Crisis and Risk Network (CRN). Das CRN ist eine Initiative zur Förderung des internationalen Dialogs über Risiken und Verwundbarkeiten. Die Mitarbeitenden ihres Forschungsteams erarbeiten wissenschaftliche Expertisen zu gegenwärtigen und künftigen sicherheitspolitischen Risiken im euro-atlantischen Umfeld und moderieren den diesbezüglichen Dialog zwischen Experten aus Politik, Wissenschaft und Wirtschaft in der Schweiz und auf internationaler Ebene im Rahmen des CRN. Zu diesem Zweck unterhält das CRN ein Beziehungsnetz zu Regierungsstellen und Expertengruppen in Verwaltung, Wirtschaft, Wissenschaft und Gesellschaft, führt Workshops und Konferenzen im Bereich der strategischen Risikoanalyse durch, publiziert auf die Bedürfnisse der Netzwerkpartner zugeschnittene Handbücher und tauscht Wissen mit Hilfe einer elektronischen Plattform aus.

Crisis and Risk Network (CRN): www.crn.ethz.ch
Center for Security Studies: www.css.ethz.ch
7. Rahmenprogramm der Europäischen Union: cordis.europa.eu/fp7/home_de.html

INFORMATIONSTHEORIE: EINE WISSENSCHAFT MIT PRAXIS-RELEVANZ

SYSTEMATIK MACHT INFORMATION BESSER NUTZBAR

Viele Vorgänge in Politik, Wirtschaft und Gesellschaft sind heute explizit informationsgesteuert. Informationen können also sehr wertvoll sein, ja geradezu Macht verkörpern. Aber die moderne Informationsgesellschaft produziert auch sehr viel Triviales. Das Wertvolle in der unübersehbaren Flut zu erkennen, zu bewerten und vor allem richtig zu verwenden, ist also eine Daueraufgabe. Systematisches Vorgehen ist dabei unverzichtbar – die Wissenschaft «Informationstheorie» stellt dafür sehr nützliche Instrumente zur Verfügung. Systematik in der Bewertung oder Klassifikation erleichtert es auch, die Informationen ihrem wahren Wert entsprechend gegen Missbrauch zu schützen.

*Dr. Rudolf Meier**

Was sind Informationen? Eine nur scheinbar einfache Frage, denn wenn man alles, was sich mit menschlichen Sinnen aufnehmen lässt, dazuzählt (was grundsätzlich richtig wäre), wird eine Definition sehr kompliziert. Informationswissenschaftler arbeiten deshalb häufig mit mathematisch-theoretischen Überlegungen in Bezug auf Formen und Inhalte, um die Abhängigkeit der menschlichen Entscheide von Informationen nachzuweisen. Das ist keine brotlose Tätigkeit, denn wenn man die Wirkung von Informationen immer genau kennen würde, wären sie das allmächtige Steuerungsmittel für alle Bereiche von Politik, Wirtschaft und Gesellschaft. In der Realität ist der Umgang mit der Bedeutung und der Wirkung von Informationen ziemlich komplex und deshalb immer ein Mix aus Theorie und Pragmatik. Als Richtlinie kann dabei gelten: Je besser man (im Voraus) die Entscheid- und Handlungsrelevanz einer Information für eine bestimmte Entscheid- oder Handlungskonstellation kennt, umso effizienter lässt sich mit ihr arbeiten. Die Beschäftigung mit einigen grundlegenden Erkenntnissen der Informationstheorie kann deshalb für den effizienten Umgang mit Informationen durchaus sinnvoll sein.

Militär und Diplomatie als Wegbereiter der Systematisierung

Historisch gesehen waren es zuerst militärische und diplomatische Organisationen, die sich zumindest in Ansätzen mit Informationstheorie beschäftigten: Man versuchte beispielsweise zu ermitteln, wie man je nach Situation klar/eindeutig formulieren kann, wie viel man notfalls weglassen darf (zwecks Vermittlungs-Beschleunigung) oder ob es eher Redundanz (Wiederholung, Erklärung) braucht, um Fehler zu vermeiden – und wie man Informationen schnell/effizient verarbeiten kann.

Diese Fragen haben im Grunde bis heute nichts von ihrer Bedeutung eingebüsst. Nur dass in der modernen, arbeitsteiligen Gesellschaft alles Produktive auf der totalen informatorischen Vernetzung basiert und deshalb die Wirkung von Informationen als Steuerungselemente viel umfassender, breiter ausfällt. Mit der weiteren Folge, dass Informationen – oder gespeichertes Wissen – heute systematisch verwaltet, «gemanaged» werden müssen. Dafür sind taugliche Kriterien nötig, denn je grösser die Informationsflut, umso wichtiger die Selektion der wirklich entscheidungsrelevanten unter ihnen. Diese Informationsbewertung ist eine Daueraufgabe, die zunehmenden Aufwand verursacht – aber gerade darum viel Sorgfalt verlangt und mit technischen Hilfsmitteln unterstützt werden muss. Ist die Selektion/Bewertung erfolgt, können sich die Voraussetzungen für den weiteren Umgang mit den als wertvoll erkannten entscheidend verändern.

Mehr Informationswert gleich mehr Schadenpotenzial

Diese Zusammenhänge machen die ganze Gesellschaft immer verletzlicher, denn je mehr Bedeutung, also Wert, bestimmte Informationen für das Funktionieren von Wirtschaft und Gesellschaft erhalten, umso mehr Schaden lässt sich mit dem Missbrauch von Informationen anrichten – vor allem in den Bereichen, in denen höchst sensible Informationen zum täglichen «Geschäft» gehören.

Wie aber bestimmt sich der «Wert» einer Information? Vereinfacht gesagt: Er steigt, je mehr direktbestimmenden Einfluss sie auf wichtige bevorstehende Entscheide und Handlungen haben kann. Die bereits erwähnten militärischen und diplomatischen Organisationen waren denn auch führend in der systematischen Bewertung und Klassierung von Informationen – was den «werterichtigen» Umgang mit ihnen enorm vereinfacht. Pannen im Umgang mit vertraulichen Informationen in allen Bereichen von Gesellschaft und Wirtschaft passieren trotzdem auch heute immer wieder, weil längst nicht überall die nötige Sensibilisierung für dieses Problem besteht.

Man muss daraus ableiten, dass das Problem der Skalierung des Informationswertes oft unterschätzt wird: Man übersieht in der Fülle der Daten leicht die Sensibilität einzelner Informationen oder kennt weitere relevante Kontexte/Wirkungsfelder der Information nicht. Das Resultat kann sei, dass der «Nutzen» für unbefugte Dritte, zum Schaden der eigenen Tätigkeit, nicht erkannt wird und die nötigen Sicherheitsmassnahmen unterbleiben. Der heute übliche Informations-Mix aus Sprache, Daten, Bildern, Grafiken und Filmen/Video erschwert natürlich ebenfalls den Überblick über die Werthaltigkeit einzelner Informationen oder sogar Informationsfragmente.

Klassifizierung als Führungsinstrument

Klassifizierungen besitzen ja nicht nur Relevanz für einzelne Empfänger, sondern, wenn der Informationswert hoch genug ist, sogar für ganze Staatsgebilde. Nehmen wir das Beispiel von Verhandlungen über einen internationalen Handelsvertrag: Eine geschickte Verhandlungsstrategie kann unter Umständen entscheidende Vorteile verschaffen – wenn sie denn geheim bleibt bis zum genau richtigen Moment der Präsentation am Tisch! Gerät sie vorher der anderen Seite in die Hände, kann das verheerende Folgen haben. Information kann also «Macht» sichtbar machen, indem sie «Fakten bewegt», Leistungen ermöglicht/alimentiert oder anstösst – sie kann aber auch Macht unterlaufen, wenn sie missbraucht wird. Stringente Klassifizierungsvorschriften sind deshalb auch ein «führungspsychologisch» wichtiges Element einer Security Policy.

Wo also Informationen ein wichtiges Instrument bei der Erfüllung von existenziellen Aufgaben sind, stellen sich zwei entscheidende Erfordernisse: Erstens muss der Zugriff darauf konsequent auf die autorisierten Personen und Personenkreise beschränkt werden – innerhalb einer Organisation heisst das, dass sowohl vertikal wie horizontal abgegrenzte Autorisierungsbereiche geschaffen werden müssen – und zweitens darf der Transport durch Kommunikations-Netzwerke nur in chiffrierter Form (zwischen geschützten Zonen oder zwischen End-Empfängern) erfolgen. Für die Sicherheit im Netzwerk gilt im Grundsatz das Prinzip «always on» – chiffrierter Verkehr ist der Normalfall, Klartextverkehr wenn überhaupt nur der Wahlfall.

Diese Prinzipien lassen sich mit den nötigen technologischen, kryptografischen und operativen Massnahmen im Rahmen einer durchgängigen Security Policy praktisch immer realisieren. Die Frage ist also eher, ob die Nutzer sich im Einzelfall des Werts ihrer Informationen als Entscheidgrundlage bewusst sind. ■

* Dr. Rudolf Meier (Küsnacht-Forch) ist Publizist mit den Schwerpunkten Politologie, Wirtschaft und Technologie.

INTEGRALES ARBEITSINSTRUMENT FÜR KLASSIFIZIERTE INFORMATIONEN

CRYPTO HIGH SECURITY MESSAGING SYSTEM

Peer-Messaging-Systeme sind vor allem in geschlossenen Nutzergruppen ideale Instrumente für den Austausch von Meldungen und unterschiedlichen Dokumenten. Sie gewährleisten ständige Erreichbarkeit, eindeutige Definition des Empfängerkreises und auch die Benutzung von geschützten Klassifikations-Hierarchien. Dank kryptografischer Verfahren zur Informationssicherheit und Benutzer-Authentifizierung werden die Systeme zu optimalen Arbeitsinstrumenten für Behördenorganisationen. *Dr. Rudolf Meier**

Peer Messaging ist eine Technologie, die zunehmende Verbreitung findet, weil sie einige wichtige operative Vorteile gegenüber anderen Kommunikationsarten besitzt. Messaging kommt im Gegensatz zu E-Mail ohne einen zentralen Server aus – die Meldungen werden im Push-Verfahren direkt in eine Mailbox geschickt. Der Empfänger ist folglich zuverlässiger erreichbar, weil er selbst nach einer Abwesenheit seine Meldungen in der Mailbox sofort verfügbar hat. In einem modernen Messaging-System lassen sich mehrere Mailboxen für unterschiedliche Benutzer einrichten – der Zugriff darauf kann mit einer persönlichen Authentifizierung verknüpft werden. So lässt sich auf einfache Weise ein individualisierbares, geschlossenes Kommunikationsinstrument realisieren.

Ideal für den Umgang mit sensiblen Informationen

Für den Umgang mit sensiblen Informationen genügt es jedoch nicht, ein komfortables Austausch-Instrument einzusetzen – durchgängige Informationssicherheit ist eine Pflichtvorgabe: Neben einer sicheren, zugriffsgeschützten Kommunikation der Meldungen über öffentliche Netze ist der Schutz der Informationen während der Bearbeitung und Speicherung unerlässlich. Sensible Informationen sind ausserdem oft verschiedenen Vertraulichkeitsstufen zugeordnet – was zusätzlich die Möglichkeit einer Klassifikation erfordert. Solche Sicherheitsbedürfnisse lassen sich nur durch hochsichere kryptografische Verfahren mit der für Behördenanwender nötigen Konsequenz erfüllen.

Ein weiteres Sicherheitsproblem kann durch die ungewollte elektromagnetische Abstrahlung von Geräten entstehen. Oft werden deshalb abgeschirmte Kommunikationsräume gebaut. Eine weitaus elegantere und kostengünstigere Lösung würde darin bestehen, komplett abstrahlfreie Systemkomponenten zu verwenden.

Messaging – optimiert für Behördenorganisationen

Aufgrund verschiedener Kundenanfragen hat Crypto AG ein komplettes Arbeitsinstrument entwickelt, das als geschlossenes System den einfachen, risikolosen Umgang mit höchst sensiblen Informationen erlaubt, ausserdem «beweglich» ist und redundante Kommunikationskanäle benützen kann.

Das System basiert auf kompakten, integralen Kommunikationseinheiten für Arbeitsgruppen. Eine Einheit besteht aus mehreren mobilen Workstations und einem Messaging-Server, der alleine Netzanschluss hat und auch als Router für wählbare Übermittlungskanäle dient.

Meldungen werden in der Workstation erstellt oder bearbeitet – ohne Speicherungsmöglichkeit – und anschliessend an den Messaging-Server geschickt. Dort werden sie chiffriert gespeichert. Erst dann können sie vom Server über einen der angeschlossenen Kanäle selbstständig versandt werden. Umgekehrt werden eintreffende Meldungen vom Messaging-Server empfangen und in Mailboxen gespeichert. Von dort holt sie die Workstation. Es gibt im gesamten System keine unchiffriert gespeicherten Nutzdaten, die «lokale Sicherheit» ist somit vollständig

gewährleistet. Eine beliebige Anzahl von Kommunikationseinheiten können zu einem geschlossenen, sicheren System vernetzt werden.

Eine elegante technische Lösung ...

Als bevorzugte praktische Lösung haben sich in der Diskussion mit Kunden komplette, fahrbare Arbeitsstationen mit PC, Monitor, Drucker und Scanner herauskristallisiert. Alle Komponenten sind abstrahlungsfrei – eine Raumabschirmung ist also nicht nötig. Mit Wireless-Modulen wird ein chiffriertes LAN mit dem Messaging-Server hergestellt.

Der PC ist als Security Workstation ausgeführt, die keine eigene Harddisk (und somit keine eigene Speichermöglichkeit) aufweist – das Betriebssystem wird jeweils von einer CD geladen. Virenattacken oder andere Beeinflussungen von aussen sind deshalb unmöglich. Für den Benutzer steht eine vertraute Office-Oberfläche (Text, Tabellenkalkulation, Präsentation, Scanning) zur Verfügung. Der Messaging-Server ist Router für redundant anschliessbare Kommunikationsnetze wie PSTN, Funk oder SatCom. Er wählt aufgrund von Prioritätsvorgaben den Kanal automatisch aus, kann jedoch manuell übersteuert werden.

... für den komfortablen Umgang mit klassifizierten Informationen

Jede Meldung wird einer Klassifizierungsstufe zugeordnet. Für jede dieser Stufen wird ein separater Schlüssel benutzt – die Schlüsselwahl erfolgt automatisch mit der Adressierung der Meldung an einen entsprechend authentifizierten Empfänger. Eine Meldung kann ausserdem mit einer Priorität versehen werden. Eintreffende Meldungen werden am Messaging-Server optisch signalisiert, inklusive Prioritätsstufe. Zusätzlich können externe Dateien als Attachments transportiert werden – sie sind aus Sicherheitsgründen (vor allem Virenschutz) auf dem System jedoch nicht bearbeitbar. Das Einlesen erfolgt mittels USB-Stick.

Jeder Benutzer kann pro Workstation für eine oder mehrere Mailboxen authentifiziert werden. Jede Mailbox darf Meldungen verschiedener Klassifizierungsstufen enthalten. Klassifizierte und unklassifizierte Meldungen sind immer kryptografisch separiert. Das Kopieren von Meldungen von einer Stufe oder Mailbox in eine andere ist im Interesse der Sicherheit nicht möglich.
Das System liefert jeweils automatisch Bestätigungen für Versand, Zustellung (in die Empfänger-Mailbox) und Öffnen der Meldung («Non repudiation»-Nachweis).

Einheitliche, hochsichere Kryptografie

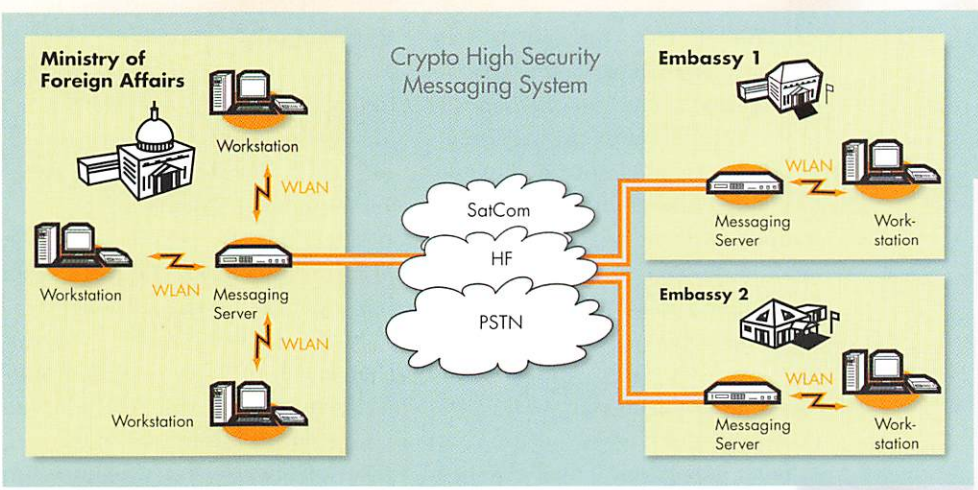
Jeder Chiffriervorgang im System erfolgt konsequent auf höchstem kryptografischem Niveau in einem geschlossenen tamper-proof Hardware-Chiffriermodul. Die Sicherheitsdaten (inkl. Schlüssel) sind dadurch mechanisch und elektrisch gegen Zugriff, Auslesen und Verändern geschützt. Die Kryptografie basiert auf einer geheimen, anwenderspezifischen, vom Security Manager jederzeit veränderbaren Algorithmusbasis. Das Security Management wird durch ein zentralisiertes Security Management Centre unterstützt.

Individuelle Konzepte sind mit wenig Aufwand realisierbar

Das Crypto High Security Messaging System ist in Modulform aufgebaut und lässt sich an individuelle Arbeitsweisen anpassen. So können die Arbeitsstationen auch als fixe Desktop-Versionen mit Anschluss über Kabel an den Messaging-Server konfiguriert sein. Die Sicherheitsprozeduren und/oder Klassifizierungsstufen sind entsprechend der jeweiligen Security Policy gestaltbar. Für die Anschaltung an unterschiedliche Übermittlungskanäle stehen individuelle Schnittstellen zur Verfügung.

Damit wird Messaging nicht nur zur einfachen und zuverlässigen Kommunikationsart, sondern kann auch die höchsten Vertraulichkeitsbedürfnisse von Behördenorganisationen erfüllen.

* Dr. Rudolf Meier (Küsnacht-Forch) ist Publizist mit den Schwerpunkten Politologie, Wirtschaft und Technologie.



TECHNISCHE ASPEKTE VON HOCHLEISTUNGSNETZWERKEN

HOHE VERFÜGBARKEIT BRAUCHT HOHE ZUVERLÄSSIGKEIT

An die Technologie von Hochleistungsnetzwerken werden hohe Anforderungen nicht nur bezüglich der Leistung, sondern auch bezüglich der Zuverlässigkeit, der Skalierbarkeit und der Administrationsfähigkeit gestellt. So legt man, um die Zuverlässigkeit zu garantieren, Kommunikationsverbindungen redundant aus, beispielsweise in einem Ring. Im Laufe der Zeit wurden verschiedene Technologien verwendet, um die jeweils aktuellen Anforderungen an Leistung und Interoperabilität zu erfüllen. Am erfolgreichsten ist Ethernet, das mittlerweile durchgängig in lokalen, aber auch landesweiten Netzen zum Einsatz kommt.

*Beat Kühne und Willy Landolt**

Die moderne Kommunikationswelt mit ihren stetig wachsenden Bedürfnissen an Verfügbarkeit und Bandbreite ist ohne Hochleistungsnetzwerke nicht mehr denkbar. Die Technologie, welche dafür notwendig ist, hat ihren Platz in der Infrastruktur und ist damit meistens wenig sichtbar. Die verwendeten Komponenten wie Multiplexer, Switches und Router sind weit entfernt vom eigentlichen Benutzer von Daten und Dienstleistungen, welcher sich darauf verlässt beziehungsweise verlassen will, dass alles reibungslos funktioniert.

Die grundsätzlichen Anforderungen an solche Netzwerke sind ebenso schnell aufgezählt, wie sie zentral sind:

- Leistung
- Zuverlässigkeit
- Skalierbarkeit
- Administrationsfähigkeit

Um die notwendigen Übertragungskapazitäten zu erreichen, welche sich bereits im Bereich von Terabits pro Sekunde (d.h. eine Billion Bits pro Sekunde) befinden, wird heutzutage für Hochleistungsnetzwerke fast ausschliesslich faseroptische Kommunikation verwendet. Dazu sind inzwischen bereits viele Städte, Länder und Kontinente mit ausgedehnten Glasfasernetzen versehen worden. Der Einsatz von Modulationsverfahren wie WDM (Wavelength Division Multiplexing) erlaubt dabei, auf einer einzigen Faser eine Vielzahl von Hochleistungs-Übertragungskanälen zu realisieren.

Zentral für jedes Netzwerk ist die hohe Verfügbarkeit (99,999%) rund um die Uhr (24x7), welche eine entsprechend hohe Zuverlässigkeit bedingt. Erreicht wird dies durch redundante Konfiguration und Realisierung von Kommunikationsverbindungen, beispielsweise in Form eines Ringes. Ein Unterbruch einer Verbindung wird sofort in alle Richtungen signalisiert, damit eine alternative Leitung geschaltet werden kann. Nebst der Verwendung von qualitativ hochwertigen Komponenten werden diese möglichst ausfallsicher ausgelegt. Dies geschieht etwa durch Verwendung von doppelten Stromversorgungen, welche einzeln ausgewechselt werden können, während der Betrieb unterbruchsfrei weiterläuft.

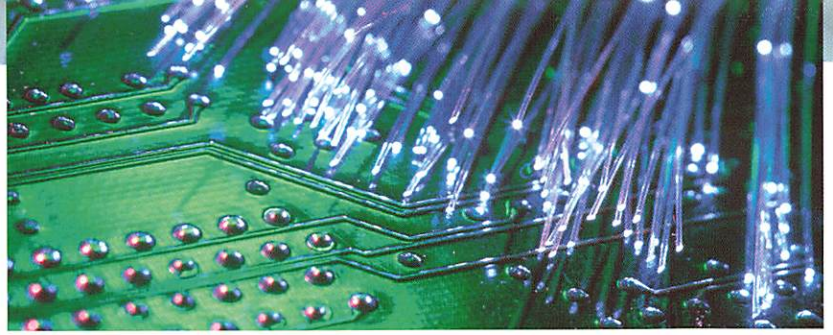
Verschiedene Technologien für Übertragung

Für die Datenübertragung sind die tiefen Schichten des OSI-Layer-Modells relevant, d.h. Layer 1 bis 3. Im Laufe der Zeit wurden dafür verschiedene Technologien verwendet, um die jeweils aktuellen Anforderungen an Leistung und Interoperabilität zu erfüllen:

- **PDH (Plesiochrone Datenhierarchie)** Verfahren zum Multiplexen von vielen kleinen Kommunikationsverbindungen, beispielsweise Telefonleitungen, auf einen einzelnen leistungsfähigeren Übertragungsstrang
- **SDH (Synchrone Datenhierarchie)** Verfahren zum Multiplexen für höhere Übertragungsleistungen mit einfacherer Ein- und Auskopplung von einzelnen Diensten in Kombination mit besserer redundanter Auslegung
- **Ethernet** Verbreitete, günstige und leistungsfähige Technologie mit einem breiten Anwendungsspektrum

Ethernet setzt sich durch

Der Ursprung von Ethernet liegt im lokalen Netzwerkbereich (LAN), wo es zur einfachen Verknüpfung

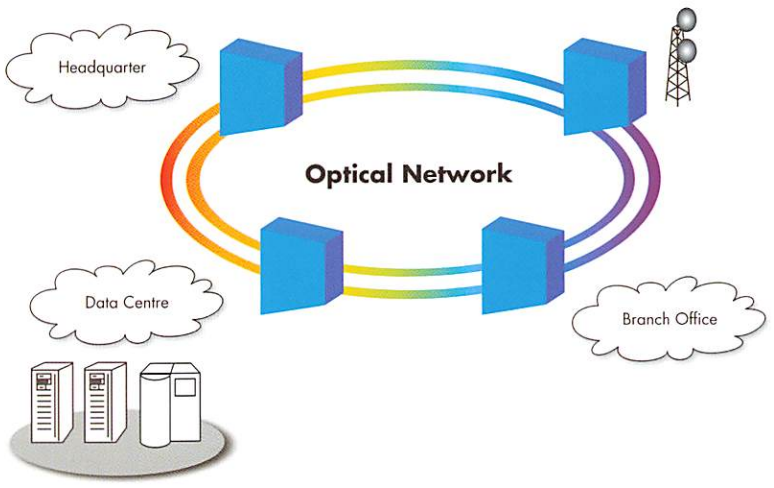


von mehreren Rechnern diente. Inzwischen ist das Protokoll erwachsen geworden und bietet die notwendigen Leistungsmerkmale für einen breiten Einsatz:

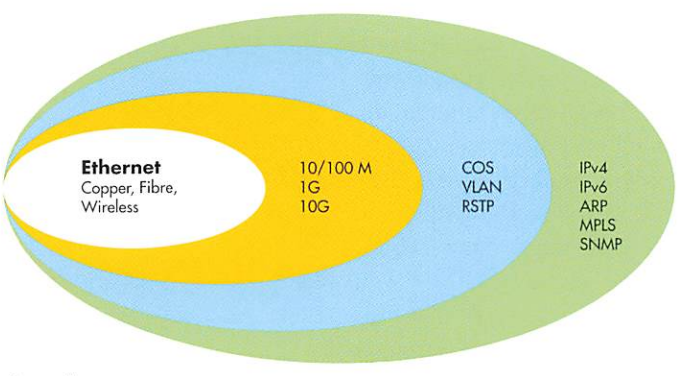
- Bandbreite zwischen 10 Megabits und 10 Gigabits pro Sekunde
- Priorisierung einzelner Dienstleistungen wie beispielsweise Sprache (VoIP) durch COS (Class Of Service)
- Bildung von Subnetzen mit VLANs (Virtual Local Area Network)
- Administrierbarkeit, beispielsweise mit SNMP (Simple Network Management Protocol)

Die Konvergenz von Netzwerkfunktionalitäten zeigt sich eindrücklich daran, dass unterschiedliche Dienste (Daten, Sprache, Fax, Video Conferencing ...) über eine einzige Leitung übertragen werden. Dazu gehört, dass bestehende Schnittstellen (etwa ein PDH-Interface einer Mobiltelefonantenne) vermehrt auf einer Ethernet-Infrastruktur übertragen werden. Mittlerweile wird Ethernet durchgängig in LAN / MAN (Metropolitan Area Network) und in landesweiten WAN (Wide Area Network) verwendet und kommt auch immer mehr zur Verknüpfung von SANs (Storage Area Network) zum Einsatz. Die Verwendung nur einer Technologie für die unterschiedlichsten Einsatzbereiche und Distanzen hat gewichtige Vorteile. Sie eliminiert teure und komplexe Übergänge zwischen den Netzen, reduziert die notwendigen Technologiekenntnisse und vereinfacht damit die Wartung eines solchen Netzwerkes beträchtlich.

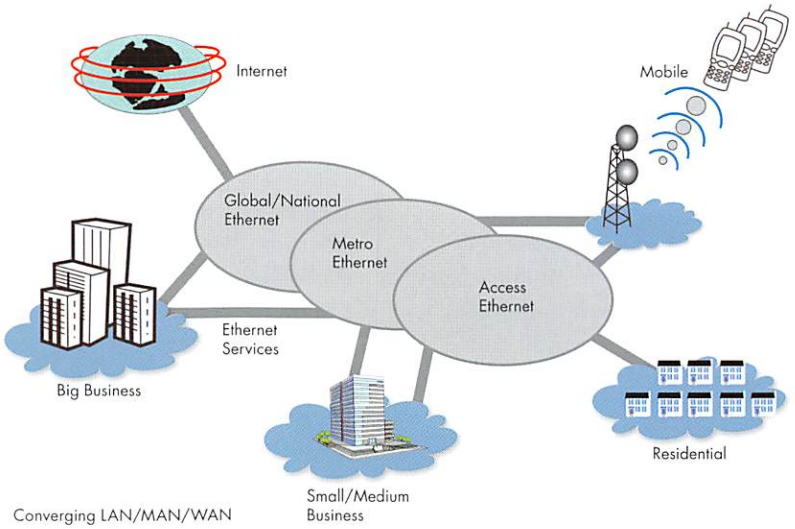
* Beat Kühne und Willy Landolt sind Product Manager.



Highspeed Networking Infrastructure



Ethernet has it all



Converging LAN/MAN/WAN

LAUSCHANGRIFFE AUF GLASFASERKABEL MIT EINFACHEN MITTELN MACHBAR

«ABHÖREN» VON LICHT

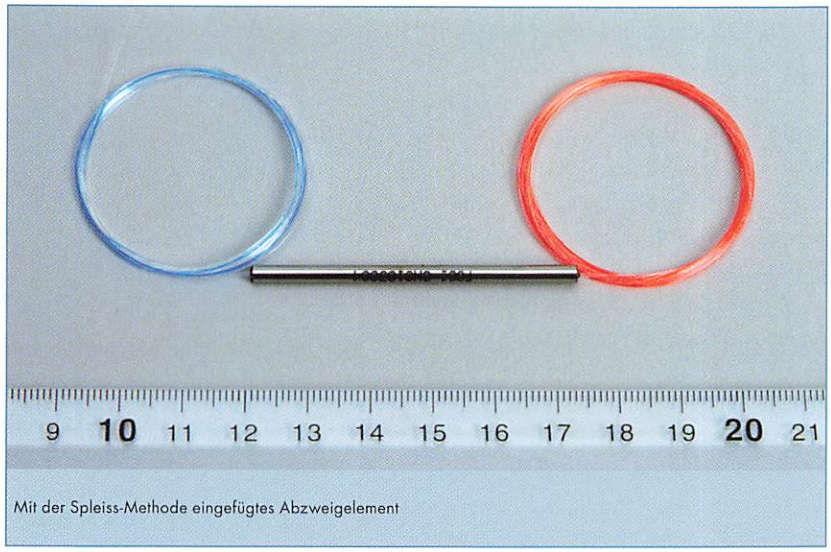
Bis vor kurzem nahm man an, dass Glasfasernetzwerke zwar theoretisch abgehört werden können, jedoch nur mit sehr grossem Aufwand, was Lauschangriffe praktisch undurchführbar machte. In der Zwischenzeit hat sich dies geändert, wie der folgende Artikel zu «Optical Tapping» zeigt. *Markus Moser**

Seit die Glasfasernetzwerke in der modernen globalen Kommunikations-Infrastruktur eine zentrale Rolle einnehmen, ist auch bekannt, dass die Informationen in Glasfasernetzwerken angezapft werden können. Bis vor kurzem galt allerdings dieses Abhören als aufwändig und praktisch nicht durchführbar. Lauschangriffe auf Glasfaserkabel sind jedoch heute mit einfachen Mitteln machbar, ohne dass dies auffällt. Der Zugang zu den Fasern ist auf die gleiche Art und Weise möglich wie bei Kupferleitungen. Die Glasfaserkabel werden in Verzweigkästen des Providers in so genannten Spleisskassetten in die einzelnen Fasern aufgetrennt und mit den Fasern verbunden, die das Gebäude erschliessen. Zusätzlich werden vielfach zu Servicezwecken Abzweigelemente, so genannte Y-Bridges, dazwischengeschaltet. Welche Glasfaser von wem benutzt wird, lässt sich einfach ermitteln, da die Leitungen eines Glasfaserkabels zu Wartungszwecken markiert sind.

Grundsätzlich lassen sich optische Abhörmethoden («Optical Tapping») in drei Gruppen aufteilen: Spleiss-Methoden, Abgreif-Methoden und berührungslose Methoden.

Spleiss-Methoden («Splice»)

Bei der einfachsten Methode, der Spleiss-Methode, wird die Glasfaser-Strecke aufgetrennt, um ein entsprechendes Abzweigelement («Splitter») dazwischenzuschalten. Während dem Spleissen ist die Verbindung unterbrochen, was relativ einfach zu detektieren wäre. Da bei der Spleisstechnik heute grosse Fortschritte gemacht wurden, ist die Zeit der Unterbrechung jedoch sehr kurz und wird von einem Betreiber nur bemerkt, wenn er entsprechende Verfahren zur systematischen Überwachung der Glasfaser-Strecken in Betrieb hat. Die Abzweigelemente, die mit dieser Methode eingefügt werden können, sind heute sehr klein und fallen in einer Installation nicht auf.



Mit der Spleiss-Methode eingefügtes Abzweigelement

Abgreif-Methoden («Coupler»)

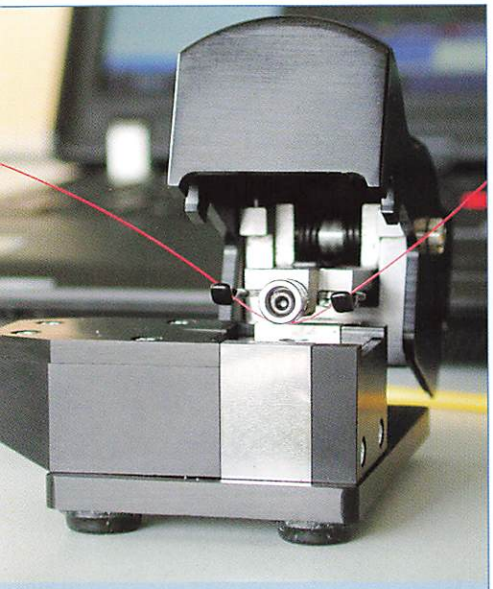
Wird eine Glasfaser gebogen, folgt das transportierte Licht grösstenteils der Biegung. Ein Teil strahlt allerdings aus der Faser heraus. Mit den heute verfügbaren Empfängern genügen schon wenige Prozente des Lichts, um das vollständige Signal zu reproduzieren und in seine digitale Form zu wandeln.

Berührungslose Methoden («Non Touching»)

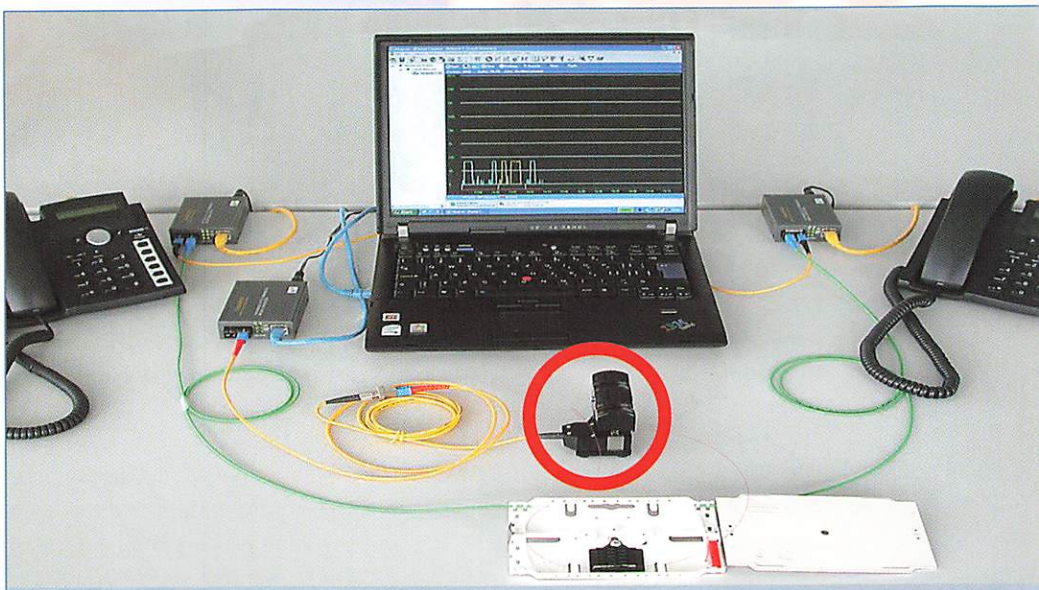
Mit dem heutigen Stand der Technik sind grobe und damit grundsätzlich nachweisbare Eingriffe ins Kabelnetz – wie die oben geschilderten Methoden – überflüssig geworden. Ein Verfahren ist bereits zum Patent angemeldet, welches mit empfindlichen Fotodetektoren arbeitet, die minimale Lichtmengen auffangen, die auf natürliche Weise aus dem Glasfaserkabel strahlen. Diese so genannte Rayleigh-Streuung lässt sich mittels fokussierenden Elementen auf dem Fotodetektor bis zur notwendigen Intensität verstärken. Damit ist ein Abhörverfahren patentiert, bei dem die Glasfaser nicht einmal berührt werden muss.

Analyse der extrahierten Daten mittels Packet Sniffer

Entgegen der verbreiteten Meinung bieten sehr schnelle Datenübertragung und riesige Datenmengen allein keinen Schutz vor Abhörattacken. Um einzelne Informationen aus einer grossen Datenmenge zu extrahieren, reichen bereits einige Adressinformationen oder ein paar Schlüsselbegriffe. Mit solchen Angaben lässt sich mit einem Sniffer-Programm die gewünschte



Abgreif-Methode (Biegekoppler)



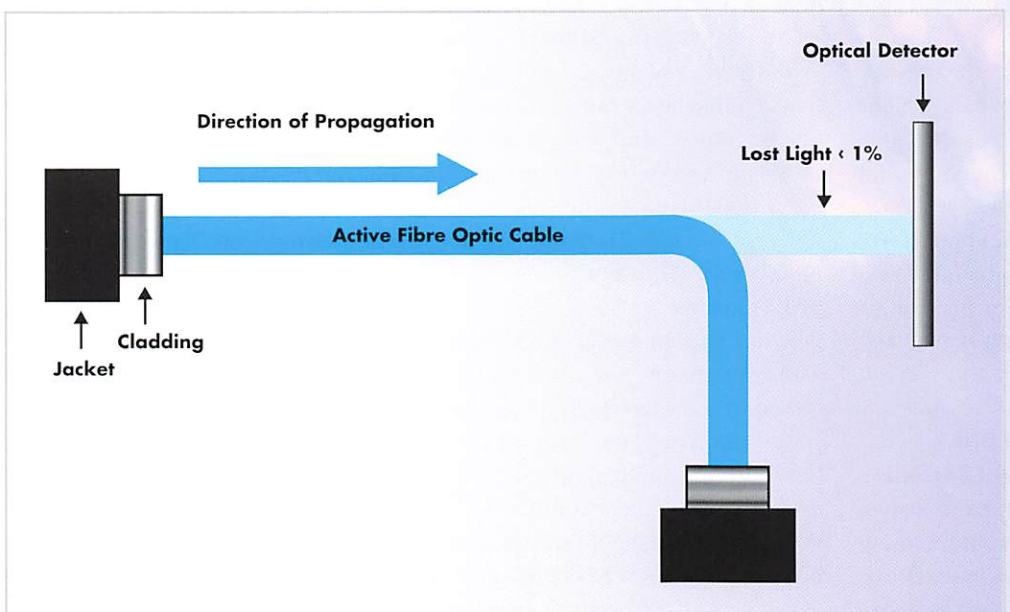
Testaufbau für weniger als 1000 USD: Mit einem Sniffer-Programm wird aus einem Gigabit-Datenstrom ein Gespräch zwischen zwei VoIP-Telefonapparaten aufgezeichnet und als PC-Datei gespeichert. Die Daten werden mittels Biegekoppler (Kreis) aus der Faser angezapft.

Information sehr einfach aus dem Datenstrom herausfiltern und aufzeichnen. Für weniger als 1000 USD kann mit einem solchen Programm ein Gespräch zwischen zwei VoIP-Telefonapparaten aufgezeichnet und als PC-Datei gespeichert werden.

Sicherheitslösung für Glasfasernetzwerke

Wenn sensitive Daten über Glasfasernetzwerke übertragen werden, bei denen die Integrität, Vertraulichkeit und Authentizität garantiert werden soll, ist es notwendig, dies auf der gesamten Übertragungsstrecke zu sichern. Die einzige in jedem Fall effektive Methode ist das Verschlüsseln der Information beim Übergang des privaten Netzwerkes auf öffentlichen, physisch ungeschützten Grund.

* Markus Moser ist Head of Product Management.



ETHERNET ENCRYPTION SOLUTIONS VON CRYPTO AG

BIS 10 GIGABITS MIT 100 PROZENT DURCHSATZ

Ethernet ist ein geeignetes Protokoll für die breite Anwendung in Hochleistungsnetzwerken. Werden sensible Daten durch die Netze gesendet, muss die Vertraulichkeit der Übertragung sichergestellt werden. Crypto AG bietet dazu passende Chiffrierlösungen mit bis zu 10 Gigabits pro Sekunde Leistung.

*Beat Kühne, Willy Landolt und Urs Kürzi**

Die durchgängige Verwendung von Ethernet in lokalen bis länderübergreifenden Netzen, d.h. in LAN / MAN und WAN, macht das Protokoll attraktiv für die breite Anwendung in Hochleistungsnetzwerken. Die unterschiedlichen Dienste (Daten, Sprache, Fax, Video Conferencing ...), welche das Funktionieren von Regierungen, Verwaltung, Wirtschaft und vielen anderen Bereichen gewährleisten, werden so über eine einheitliche Infrastruktur zur Verfügung gestellt. Entsprechend wichtig ist, dass auch die Vertraulichkeit der Datenübertragung mit dieser Technologie sichergestellt werden kann.

Mit der Chiffrierung auf dem tiefsten OSI-Layer, dem Layer 1, wird eine totale Übertragungssicherheit erreicht, welche für alle Dienste gilt, die höhere Schichten verwenden. Gleichzeitig ermöglicht die Chiffrierung der Daten auf der Ethernet-Protokoll-Schicht eine vollständige Transparenz für alle Applikationen und Services, welche höhere Kommunikationsschichten verwenden. Die Sicherung der Übertragung wird ohne jeglichen Overhead realisiert und in Hardwaremodulen ausgeführt, was zusammen eine hundertprozentige Leistung im Vergleich zur Netzkapazität garantiert.

Lösung für 1 Gigabit pro Sekunde erfolgreich in Betrieb

Abhängig vom Einsatzort der Datenkommunikation sind unterschiedliche Leistungsstufen notwendig. Innerhalb von Gebäuden werden inzwischen häufig Leitungen von bislang 100 Megabits pro Sekunde auf 1 Gigabit pro Sekunde aufgerüstet. Diese Bandbreite genügt meist auch zum Anbinden von kleineren bis mittleren Aussenstellen.

Vor einigen Jahren entsprachen Gigabit-Datenverbindungen dem neusten Stand der Technik. Crypto AG kann ihren Kunden bereits seit vielen Jahren mit dem Ethernet Encryption HC-8440 1G die passende Chiffrierlösung anbieten.

Diese Kombination einer Hochsicherheitslösung mit grosser Leistung und höchster Verfügbarkeit hat von Anfang an überzeugt und wird in der Zwischenzeit von vielen zufriedenen Kunden eingesetzt. Die einfache Installation folgt dem «Plug&Play»-Prinzip und beschränkt sich auf das Einbringen in die optische Verbindung. Für verschiedene Übertragungsdistanzen sind passende, leistungsfähige Laser erhältlich, welche in austauschbaren optischen Transceivermodulen verfügbar sind und damit eine einfache Anpassung an das jeweilige Einsatzszenario erlauben.

Neu bis 10 Gigabits pro Sekunde

Parallel zu den stetig wachsenden Anforderungen an die Dienste haben die Netzwerkbetreiber die Leitungskapazitäten erhöht. Mittlerweile sind 10 Gigabits pro Sekunde für längere Strecken im MAN / WAN und Inter-SAN-Bereich (Verbindungen zu Rechenzentren) bereits weit verbreitet. Auch für diese Übertragungsleistung kann Crypto AG wiederum eine ideale Chiffrierlösung anbieten, das Ethernet Encryption HC-8555 10G. Der bewährte Ansatz, die Daten auf dem OSI-Layer 1 mit 100 Prozent Durchsatz und Sicherheit zu chiffrieren, wird erneut verwendet. Damit erhält der Kunde eine potente Ethernet-Chiffrierlösung mit 10 Gigabits pro Sekunde Leistung, welche komplett transparent für alle Applikationen und Dienste die höchste Vertraulichkeit garantiert.

Grosse Aufmerksamkeit wurde bei der neuen Lösung auf die hohe Ausfallsicherheit gelegt. Redundante Stromversorgung und Kühlung des Gerätes und die Möglichkeit, diese Module im laufenden Betrieb auswechseln zu können, garantieren ein Maximum an Ausfallsicherheit.

Nebst der einfachen «Bump-in-the-Wire»-Installation, d.h. dem Einbringen in die optische Verbindung, wird auch der Betrieb des Gerätes auf vielfältige und praktische Art und Weise unterstützt. Dazu gehört die Bedienung mit einer Browserbasierten Benutzeroberfläche, welche sowohl vor Ort wie auch aus der Zentrale verwendet werden kann. Eingebaute Testfunktionen ermöglichen unabhängig von der restlichen Infrastruktur sicherzustellen, dass die Kommunikationsverbindung sowohl ungeschützt wie auch chiffriert funktioniert.

Die Geräte lassen sich mittels SNMP einfach in eine bestehende Netzwerk-Management-Umgebung

integrieren. Damit können bereits etablierte Überwachungsmechanismen verwendet werden.

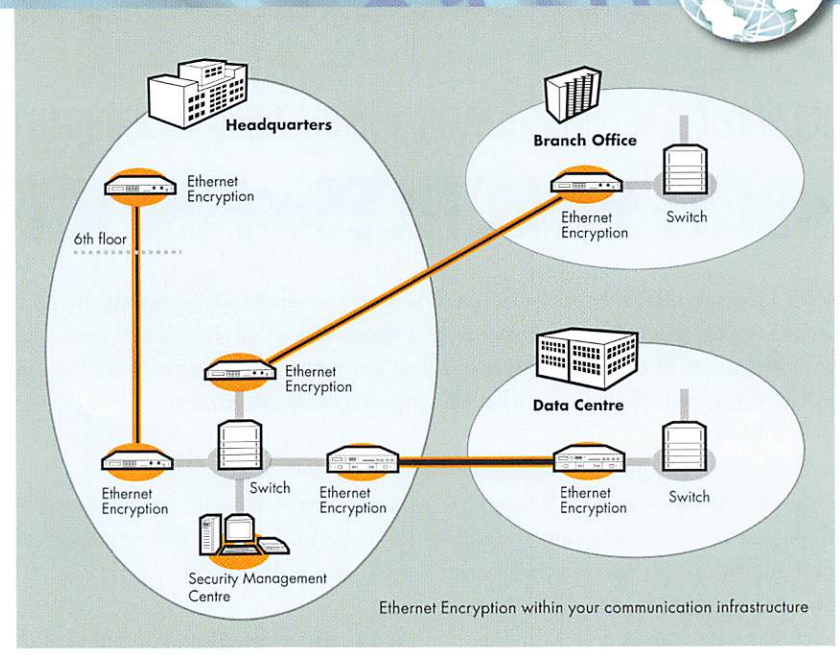
Für beide Ethernet-Encryption-Produkte gelten wie für alle Geräte von Crypto AG:

- Kundenindividueller Hardwarebasierter symmetrischer Algorithmus
- Durchgängige, umfangreiche Sicherheitsarchitektur
- Ausgeklügeltes, gesichertes Verfahren zum Aushandeln des verwendeten Chiffrierschlüssels zwischen zwei Geräten
- Benutzerspezifischer Zugangsschutz mit Passwörtern
- Manipuliergeschützte Gehäusekonstruktion
- Emergency-Clear-Funktion

Security Management Centre

Zentrales Element jeglicher Chiffrierlösung und damit auch der Ethernet-Encryption-Produkte ist das Security Management, welches erlaubt, Algorithmus, Schlüssel, Passwörter und andere Sicherheitseinstellungen entsprechend der Security Policy des Anwenders zu definieren. Dabei werden die grundlegenden Geheimnisse zum Algorithmus bereits bei der Installation des Chiffriersystems eingebracht. Während des Betriebs der Chiffriergeräte soll es auf eine einfache Art und Weise möglich sein, regelmässige Schlüsselwechsel zu konfigurieren und im System selbstständig durchführen zu lassen.

Crypto AG ermöglicht dies mit dem Security Management Centre SMC-1100, einer modernen PC-Applikation, welche einfach zu bedienen ist und ein Höchstmass an Sicherheit bezüglich Definition, Verwaltung und Verteilung der Sicherheitsdaten bietet. Das SMC-1100 beinhaltet ein hardwaremässig ausgeführtes Security Module, welches die komplette Chiffrierung wie auch den Zugangsschutz in einer manipuliergeschützten Umgebung realisiert.



Ethernet Encryption within your communication infrastructure

Die intuitive, grafische Benutzeroberfläche ermöglicht dem Security Manager, auf einfache und übersichtliche Art und Weise das Chiffriersystem abzubilden und die notwendigen Sicherheitskonfigurationen durchzuführen. Chiffrierte Management-Meldungen können auf Smart Cards oder komfortabler mittels einer Ethernetverbindung zum Chiffriergerät verteilt werden. Dabei übernimmt ein externer Message Scheduler (MS-1100) die termingesteuerte Online-Verteilung und sorgt zusätzlich für eine physikalische Trennung der Security-Management-Plattform vom potenziell öffentlichen Management-Netz. Um auch Link-orientierten Topologien Rechnung zu tragen, genügt es, Verbindung nur zu einem Chiffriergerät zu haben. Dieses kann dann mittels eines Inband-Verfahrens die Management-Meldungen an die Partnerstation weiterleiten.

Für die Routineüberwachung, beispielsweise um das Einhalten der Security Policy zu überwachen und zu beweisen, oder für allfälliges Diagnostizieren von Problemen im Kommunikationssystem ist es äusserst nützlich, mit dem SMC-1100 von einem zentralen Ort aus Zugang zu Informationen eines Chiffriergeräts zu erhalten. Online-Abfragen von Geräteeinstellungen und Log-Einträgen ermöglichen dies auf einfache und effiziente Art.

* Beat Kühne und Willy Landolt sind Product Manager. Urs Kürzi ist Customer Segment Manager Government.


Ethernet Encryption HC-8440 1G


Ethernet Encryption HC-8555 10G


Security Management Centre SMC-1100

ICT-SERVICES MITENTSCHEIDEND FÜR DIE ZIELERREICHUNG IN ORGANISATIONEN

«BEST PRACTICES» FÜR ICT-SERVICES

Wie können diejenigen Personen, welche in einer Organisation für die Informations- und Kommunikationstechnologie (ICT) verantwortlich sind, einen ausgezeichneten Service bereitstellen, der ihre Kunden zufrieden stellt und der Organisation erlaubt, ihre operativen Ziele zu erreichen? Dazu haben sich in der ICT-Welt in den letzten Jahren «Best Practices» etabliert.

*Paolo Fanuli**

Noch vor 30 Jahren bedeuteten ICT-Services im Wesentlichen Rechenzeit auf einer – oft wie ein Heiligtum beschützten – Maschine und Papierstapel mit den ausgedruckten Resultaten der Berechnungen. Dies hat sich grundlegend geändert: Die technologische Entwicklung und die Rationalisierung der Abläufe haben dazu geführt, dass heute ICT-Mittel überall eingesetzt werden und dass diese einen entscheidenden Einfluss auf die Qualität und den Inhalt unserer Arbeit haben. Mit ICT-Services wird heute die ganze Administration erledigt, operative Abläufe werden unterstützt, wichtige Daten verwaltet. Mit den Möglichkeiten hat auch die Komplexität stark zugenommen. Die grosse Fülle an Geräten und Abläufen (um die Geräte wiederum zu verwalten und optimal einzusetzen) stellt eine grosse Herausforderung für ICT-Manager dar. Diese tragen deshalb eine hohe Verantwortung. Meistens sind sie heutzutage anderen oberen Kadern gleichgestellt und entsprechend als Chief Information Officer CIO eingestuft. Mit ihren ICT-Services tragen sie entscheidend dazu bei, dass die Organisation ihre Ziele erreicht ... oder auch nicht!

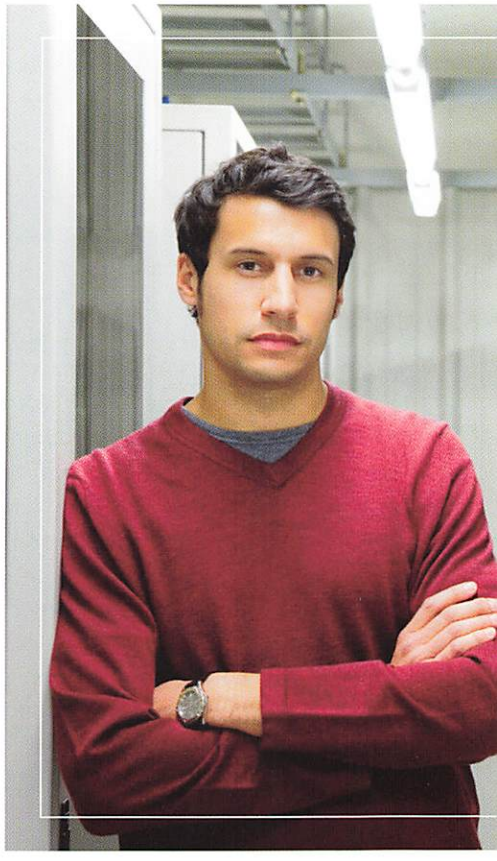
In vielen Ländern kann schlechtes Management von ICT-Services als Straftat belangt werden, wenn es zu einem vermeidbaren Schaden für die Organisation kommt. Oft kann der ICT-Manager sogar als Privatperson zur Verantwortung gezogen werden. Wie kann sich dieser also schützen und, vor allem, wie kann er einen ausgezeichneten Service bereitstellen, der seine Kunden zufrieden stellt und der Organisation erlaubt, ihre operativen Ziele zu erreichen?

Was sind eigentlich ICT-Services?

Die Bereitstellung eines PCs mit allen nötigen Anwendungen ist ein ICT-Service, aber auch die Möglichkeit, an einer Dose in der Wand ein Telefon einzustecken und darüber zu telefonieren. Meist ermöglicht ein solcher Anschluss dann auch, Fax-Nachrichten und Daten über ein Modem zu senden. Diese zusätzlichen Anwendungen stellen auch ICT-Services dar. Ebenso entstehen diese durch Arbeitsabläufe und die Arbeit von Personen, beispielsweise ist die Reparatur eines defekten Gerätes ein ICT-Service.

ICT-Services können auch am OSI-Layer-Modell orientiert definiert werden, d.h. Infrastruktur-Services (Layer 1 bis 6, beispielsweise das Routing) oder Anwendungsservices (Layer 7, beispielsweise E-Mail). Dazu kommen dann noch die Services, die – wie oben erwähnt – durch Arbeitsabläufe oder menschliche Arbeit entstehen.

ICT-Services verfolgen primär das Ziel, die Wertschöpfung der Organisation optimal zu unterstützen beziehungsweise zu ermöglichen. Damit sind auch gleich die Risiken absteckbar. Fehlerhafte oder schlechte ICT-Services beeinträchtigen die gesamte Wertschöpfungskette, angefangen bei der strategischen ICT-Ausrichtung (Positionierung) über die ICT-Entwicklung (Anwendungen) bis hin zur ICT-Produktion (Projekte). Des Weiteren können auch die Finanzen (Kosten, Ertragsausfälle), die Organisation (Personal) und die rechtliche Situation unter mangelhaften ICT-Services leiden.



ICT Service Management

Damit ICT-Services in bester Weise die Zielerreichung einer Organisation unterstützen, sollten die üblichen Prinzipien der Führung und Steuerung genügen. Die Führung entsteht zunächst durch eine klare Formulierung der strategischen und operativen Ziele der ICT-Organisation. Anschliessend gilt es, die Umsetzung der Ziele durch operative Pläne voranzutreiben und mit einem effizienten Controlling sicherzustellen, dass bei



Bedarf steuernd eingegriffen wird. Oft wird das auch mit der Sequenz «Plan-> Do-> Check-> Act->» prägnant beschrieben. Ziel des Managements ist es, ICT-Services anzubieten, die

- eine gute Beziehung zu den Kunden der ICT-Organisation aufbauen und aufrechterhalten,
- die ICT-Anforderungen der Organisation erfüllen,
- einfach entwickelt und gewartet werden können,
- alle ICT-Ressourcen effizient und effektiv nutzen,
- zur Gesamtqualität der ICT positiv beitragen im Rahmen der Kostenvorgaben.

Im Verlauf der letzten rund zehn Jahre haben sich in der ICT-Welt «Best Practices» etabliert. Diese wurden zum Teil durch internationale Organisationen zu Standards erhoben. Es hat sich dabei als nützlich erwiesen, ICT-Services unter zwei hauptsächlichen Gesichtspunkten zu betrachten. Einerseits kann mit dem Referenzmodell «COBIT» die strategische Führung der ICT-Services umschrieben werden. Anderseits benutzt man heute ein Modell namens «ITIL» für die Beschreibung der operativen Führung der ICT-Infrastruktur.

COBIT (Control Objectives for Information and related Technology) und ITIL (IT Infrastructure Library) stellen einen Rahmen dar für eine effiziente ICT Governance, d.h. für die Führung der ICT als Organisation und für das Management der ICT-Services. Die Ziele der ICT Governance sind:

- ICT laufend auf Ziele und Mission der Organisation ausrichten
- Optimierung des Nutzens in der Wertschöpfungskette ermöglichen
- ICT-Ressourcen auf bestmögliche Art und Weise einsetzen
- ICT-Risiken minimieren

COBIT

COBIT, erstmals 1996 durch die Information Systems Audit and Control Foundation (ISACF) beschrieben und heute durch das IT Governance Institute weiterentwickelt, definiert als wichtigstes Element 34 übergeordnete Steuerziele (Control Objectives) – je eines für 34 wichtige ICT-Abläufe. Diese Abläufe sind in vier Gruppen eingeteilt: Planung und Organisation, Beschaffung und Implementierung, ICT-Service-Erbringung und Support sowie Überwachung.

Ein «Control» beschreibt eine zusammengehörende Menge von Richtlinien, Teilprozessen, Praktiken und Aufbauorganisationen, die dazu dienen, die Erreichung der Ziele und der Mission der Organisation zu unterstützen. Ein «Control Objective» beschreibt den gewünschten Endzustand für den beschriebenen Ablauf. Für jeden Ablauf enthält COBIT eine Audit-Guideline mit Empfehlungen. Die Management-Guidelines beinhalten praktische Hinweise, wie die ICT-Organisation geführt werden kann. Die wichtigsten dieser Guidelines werden auch als «Critical Success Factors» bezeichnet. Zu guter Letzt beschreiben die Messgrössen «Key Goal Indicators» und «Key Performance Indicators», wie gut ein Ziel erreicht beziehungsweise ein Ablauf geführt wird. COBIT ist damit ein umfassendes Werk, gleichzeitig aber doch kompakt.

ITIL

ITIL, in den frühen 80er-Jahren von der britischen Regierung (OGC Office of Government Commerce) erstmals beschrieben, hat sich seither ständig weiterentwickelt. 2003 entstand daraus der British Standard BS 15000 und 2006 schliesslich der ISO-Standard ISO/IEC 20000. ITIL konzentriert sich auf die Beschreibung von Best Practices für das Management von ICT-Services, d.h. für die operative Führung zur Entwicklung und Erbringung von ICT-Services. ITIL beschreibt Verfahren für die Bereiche «People», «Processes», «Products» sowie «Partners» im Management von ICT-Services. Die sieben Hauptelemente sind:

- Service Delivery: deckt die Prozesse für die langfristige Planung und Entwicklung der Service-Erbringung ab. Teilprozesse dazu sind: Service Level Management, Availability Management, Capacity Management, Continuity Management, Financial Management
- Service Support: deckt die kurzfristigen Tagesabläufe ab, die für die Erbringung der Services nötig sind. Die Service-Support-Funktion dient als Tor zu den folgenden Teilprozessen: Incident Management, Problem Management, Change Management, Release Management, Configuration Management
- ICT Infrastructure Management: deckt die Bereiche Bedarfserfassung bis Bereitstellung der Infrastruktur ab
- Planning to Implement Service Management: Planung und Einführung der Abläufe für die Implementierung des Service-Managements
- Application Management: beschreibt die Behandlung von Anwendungen in deren gesamten Lebenszyklus
- Business Perspective: liefert Hilfsmittel für die ICT-Mitarbeiter, welche die Ausrichtung auf die Organisationsziele erleichtern
- Security Management: definiert Sicherheitspolitik, Erkennen und Management der Bedrohungen und Gefahren. Wichtige Elemente dazu sind: Security Controls Management, Security Incident Management, Audit Results, Reporting

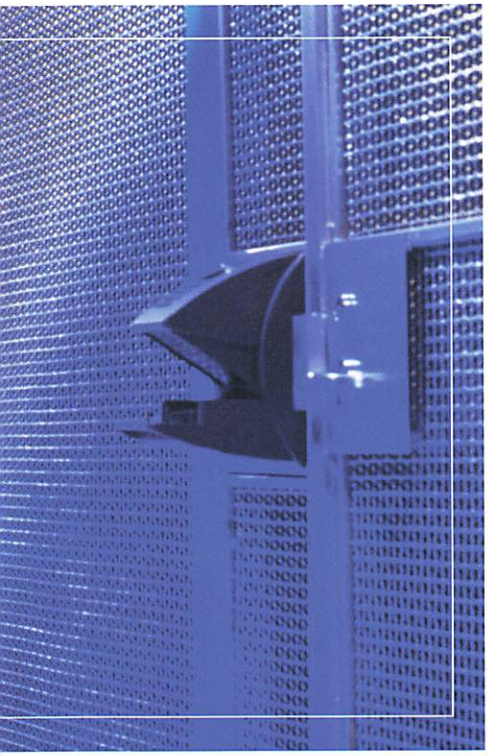
Nutzen und Vorteile eines guten ICT-Service-Managements

Eine effiziente Führung der ICT-Services ist heute und in Zukunft nur möglich, wenn dafür bewährte Best-Practice-Modelle eingesetzt werden. COBIT und ITIL sind nicht die einzigen Modelle, aber am weitesten verbreitet und am besten erprobt – und deshalb empfehlenswert, wenn dabei pragmatisch vorgegangen wird. Daraus kann folgender Nutzen entstehen:

- Bessere Ausrichtung der ICT-Abläufe, Produkte und Services auf die Bedürfnisse der Anwender
- Bessere Erfüllung der Ziele und Mission der Organisation
- ICT-Mitarbeitende, die sich bewusst sind, welchen Einfluss ICT auf die operative Mission hat
- Verringerungen der Gesamtkosten für ICT-Management und Support
- Bessere Verfügbarkeit der ICT-Services
- Bessere Service-Levels und Gesamtqualität der ICT-Services

Die Rolle von Crypto AG

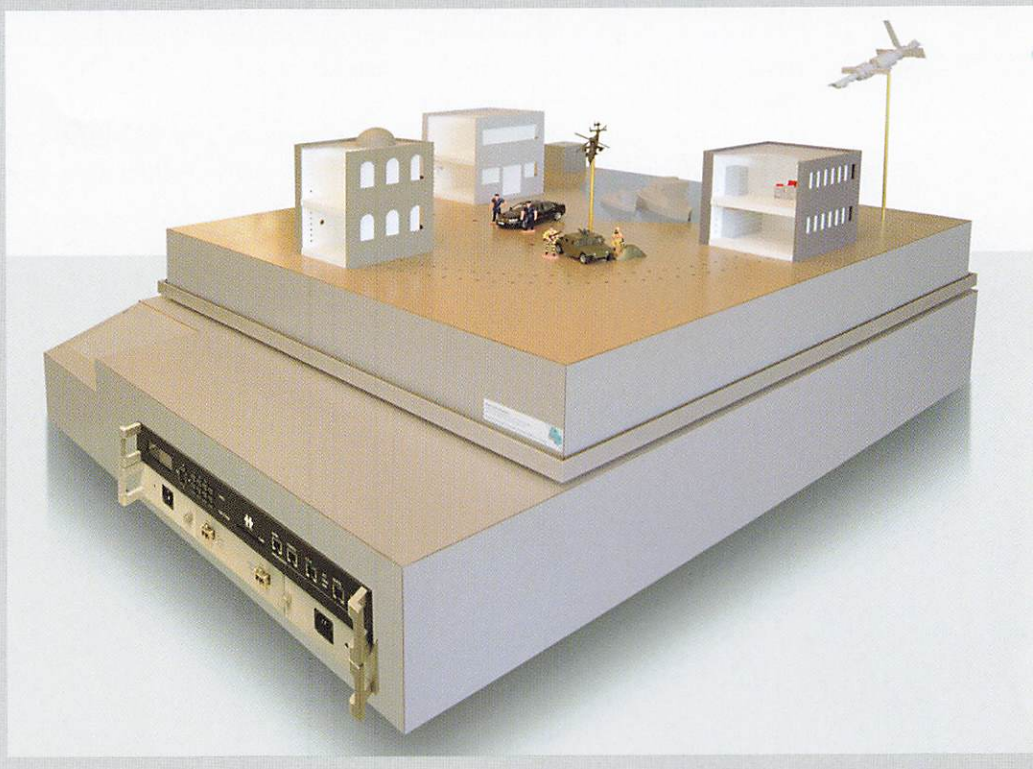
Die direkten Crypto-Kunden sind fast immer selbst auch Service-Lieferanten für ihre internen Benutzer. Auch für unsere Kunden wird es deshalb immer wichtiger, ihre eigenen ICT-Services optimal auf die Erfüllung der Mission ihres Auftraggebers auszurichten. Die Einführung optimaler ICT-Service-Abläufe aus bestehenden, manchmal viele Jahre alten Abläufen ist schwierig. Viele unserer Kunden wünschen Unterstützung bei der Einführung optimaler Lösungen im Information-Security-Bereich. Crypto AG hat seit vielen Jahren die Bedeutung der ICT-Services erkannt und liefert deshalb Produkte und Services, die zusammen eine optimale Lösung darstellen. An erster Stelle stehen dabei, unter anderem, Ausbildung und Engineering-Services. Künftig



wird Crypto AG weiter an das noch zunehmende Bedürfnis nach «Best Practices» anknüpfen und noch in diesem Jahr neue zusätzliche Services ankünden, die einen weiteren Schritt darstellen auf dem Weg zum Anbieter integrierter Sicherheitslösungen. In kommenden Ausgaben des Crypto Magazines werden wir diese neuen Services vorstellen. ■

* Paolo Fanuli ist Head of Direct Sales International.

CRYPTO AG AN DER MILIPOL PARIS 2007



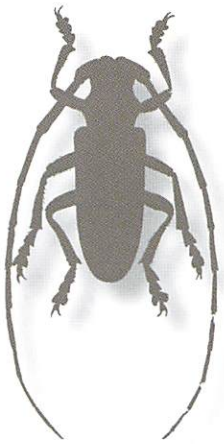
Der mobile Showroom entsteht: Dank diesem sollen sich Besucher des Crypto-Stands innerhalb weniger Minuten ein Bild über die Sicherheitslösungen von Crypto AG machen können.

Crypto AG präsentiert sich an der Milipol Paris 2007 vom 9. bis 12. Oktober. Die Messe findet auf der Paris Expo Porte de Versailles (Frankreich) statt. Die Milipol Paris – unter der Schirmherrschaft des französischen Innenministeriums – ist die führende Messe zu Innerer Sicherheit und ermöglicht – gemäss Veranstalter – einen Überblick über technische Entwicklungen im Bereich öffentliche Sicherheit und Verbrechensbekämpfung. An der Milipol Paris 2005 kamen rund 800 Aussteller und knapp 24'000 Besucher zusammen.

Mobiler Showroom als One-Stop-Shop

An der Milipol Paris kann der Crypto-Stand mit einem neuen Eye-Catcher aufwarten. Basierend auf den Showrooms am Hauptsitz von Crypto AG wurde ein Modell eines mobilen Showrooms entwickelt. Dieser zeigt alle Sicherheitslösungen von Crypto AG auf eine einfache und verständliche Art und Weise. Dargestellt werden sowohl zivile wie auch militärische Anwendungsszenarien. Auf Anschaulichkeit und Detailtreue wird viel Wert gelegt. Lichterketten aus LED-Lämpchen symbolisieren den Weg, über den verschlüsselte Informationen zwischen den verschiedenen Stationen geschickt werden.

Besucher des Crypto-Stands sollen sich dank des mobilen Showrooms innerhalb weniger Minuten ein Bild über die Sicherheitslösungen von Crypto AG machen und so den Zugang zu diesen finden können. Der mobile Showroom soll dem Interessierten zeigen, dass er als Kunde bei Crypto AG einen One-Stop-Shop für Sicherheitslösungen betritt.



DIE GESUCHTE PERSON ...

... brachte in einer Kurzgeschichte, 1843 veröffentlicht, ihr grosses Interesse an der Kryptologie zum Ausdruck. In der Geschichte um einen goldenen Käfer finden die Protagonisten ein Pergamentstück mit einem Geheimtext ...

«Hier zeigte mir Legrand das Pergamentstück, das er eben wieder erwärmt hatte. Zwischen dem Totenkopf und dem jungen Bock erblickte ich folgende, anscheinend von ungeübter Hand geschriebenen Zeichen:

53 ≠ ≠ † 305)) 6 * ; 4826) 4 ≠ .) 4 ≠) ; 806 * ; 48 † 8] / 60)) 85 ; 1 ≠ (; : ≠ * 8 † 83 (88) 5 * † ; 46 (; 88 * 96 * ? ; 8) * ≠ (; 485) ; 5 * † 2 : * ≠ (; 4956 * 2 (5 * - 4) 8] / 8 * ; 40 69 285) ;) 6 † 8) 4 ≠ ≠ ; 1 (≠ 9 ; 48 0 81 ; 8 : 8 / 1 ; 48 † 85 ; 4) 485 † 52 8806 * 81 (/ 9 ; 4 8 ; (88 ; 4 (≠ ? 34 ; 48) 4 ≠ ; 161 ; : 188 ; ≠ ? ;

‹Ich bin allerdings noch gerade so im Unklaren wie früher›, antwortete ich und gab Legrand das Blatt zurück ... »

Im Gegensatz zum Erzähler kann Legrand den Geheimtext entschlüsseln und findet so den verborgenen Schatz des Piraten Captain Kidd.

Die gesuchte Person liess jedoch nicht nur die Figur Legrand Geheimschriften entschlüsseln, sondern tat dies auch selber. In der Zeit, als die gesuchte Person für den «Alexander Weekly Messenger» in Philadelphia schrieb, rief sie ihre Leserschaft dazu auf, monoalphabetische Geheimschriften einzusenden, um diese dann zu entschlüsseln. Der Aufruf stiess auf grosses Interesse, hunderte sendeten Geheimtexte ein. Die gesuchte Person konnte alle entschlüsseln. Dies war zwar dank der Frequenzanalyse relativ einfach, verblüffte damals die Leser dennoch sehr.

Die gesuchte Person wurde allerdings nicht wegen der Kryptologie berühmt, sondern wegen ihres literarischen Schaffens. Sie gilt als Begründerin des Genre der Kriminalliteratur, der Science-Fiction und der Horrorstory und hatte mit ihren Werken grossen Einfluss beispielsweise auf die Autoren Jules Verne, Arthur Conan Doyle und Herbert George Wells.

Die gesuchte Person starb 1849 im noch jungen Alter von bloss 40 Jahren. Über die Todesursache gibt es verschiedene Theorien, jedoch keine Beweise ...

Um wen handelt es sich?

Senden Sie die Lösung bis am 2. Oktober 2007 an beatrice.huber@crypto.ch.

Ab 3. Oktober wird die Lösung auf unserer Website www.crypto.ch publiziert.

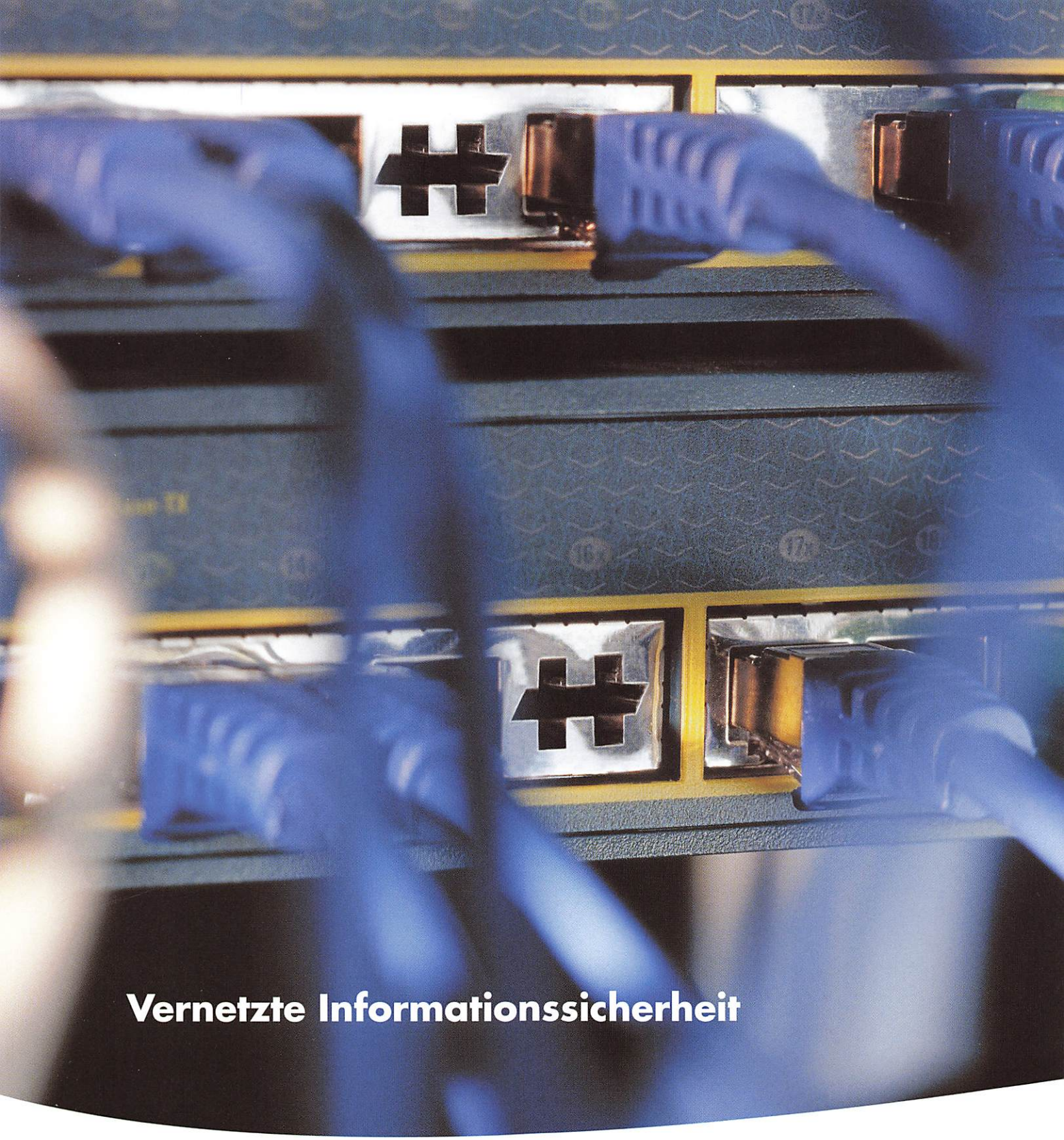
Unter den Einsendern verlosen wir dreimal Literatur der gesuchten Person.

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

Die Lösung des Wettbewerbs Nr. 1/2007 lautet «Max Planck».

IMPRESSUM

Erscheinungsweise 3-mal jährlich **Auflage** 6000 (deutsch, englisch, französisch, spanisch, arabisch) **Herausgeber** Crypto AG, Postfach 460, CH-6301 Zug (Schweiz), www.crypto.ch **Redaktionsleitung** Beatrice Huber, Crypto AG, Tel. +41 41 749 77 80, Fax +41 41 741 22 72, E-Mail beatrice.huber@crypto.ch **Konzept/Layout** illugraphic, Sonnhalde 3, CH-6332 Hagendorn, www.illugraphic.ch **Druck** Ennetsee AG, Bösch 35, CH-6331 Hünenberg **Nachdruck** Honorarfrei mit Zustimmung der Redaktion, Belegexemplare erbeten, Copyright by Crypto AG **Bildnachweis** Corbis: Titelseite, S. 3, 9, 18, 20, 24 · Crypto AG: S. 2, 4, 10, 11, 14, 15, 17, 21 · Dr. Myriam Dunn Cavelty: S. 6, 7 · Imagepoint: Titelseite, S. 3, 4, 5, 12, 14, 15, 18, 19, 20, 21 · Kursiv: S. 9, 13



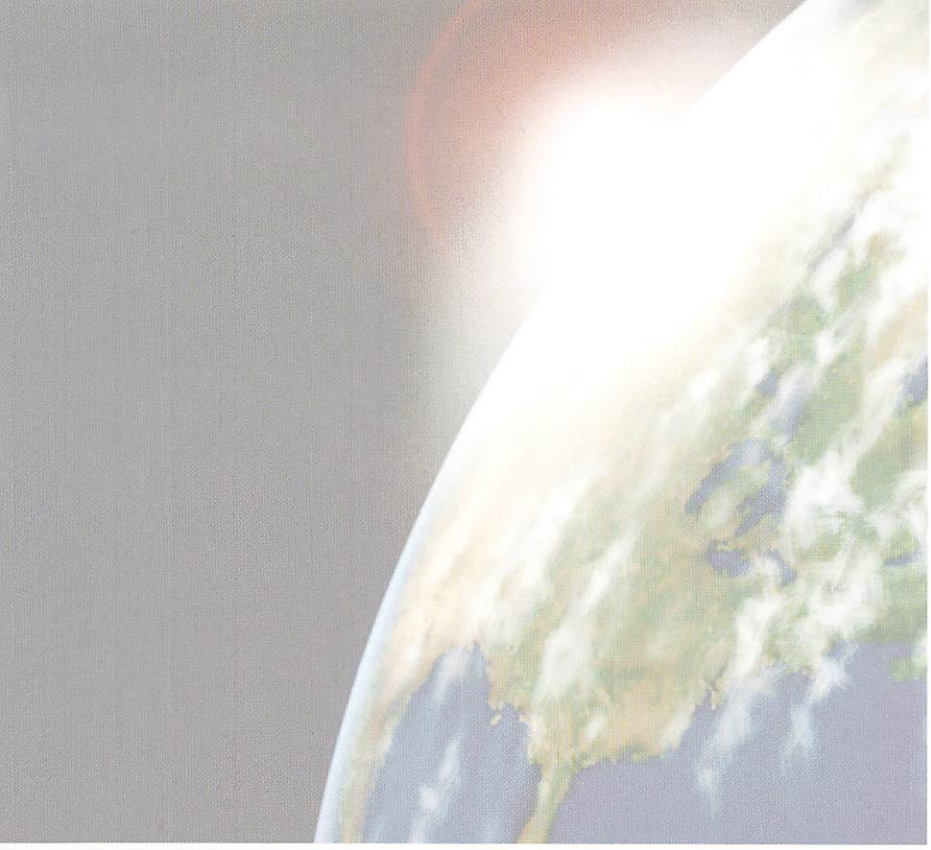
Vernetzte Informationssicherheit

Seit über 50 Jahren konzentrieren wir uns auf die Entwicklung, Produktion und Implementation von anspruchsvollen Informationssicherheits-Lösungen. Weil wir wissen, dass vertrauliche Information Wertsache ist. Vertrauen deshalb auch Sie auf die Kompetenz und Leistungsfähigkeit von Crypto AG, genauso wie unsere Kunden aus über 130 Ländern.

To Remain Sovereign

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

HAGELIN-CRYPTOS
CRYPTO AG



MESSEN

Milipol, 9. bis 12. Oktober 2007
Paris Expo Porte de Versailles, Frankreich

NEUE PUBLIKATIONEN

Die Sicherheitsarchitektur für höchste Ansprüche designed by Crypto AG

Machen Sie den Himmel sicher mit Satellite Security Solutions von Crypto AG

PRESSESPIEGEL

Auf der Suche nach der absoluten Sicherheit

Für quantenkryptografische Verfahren lässt sich – im Gegensatz zu heute eingesetzten kryptografischen Verfahren – mathematisch beweisen, dass diese Verfahren absolut sicher sind. Heute eingesetzte Verfahren basieren auf grossen Primzahlen und erzielen eine relativ hohe bis sehr hohe Sicherheit, weil das Zerlegen von grossen Zahlen in Primzahlen auch für sehr leistungsfähige Rechner äusserst aufwändig ist.

Absolut sicher sind allerdings im Fall der quantenkryptografischen Verfahren auch nur idealisierte und keineswegs reale. Das Wissenschaftsmagazin «Nature» berichtete im Mai über Forschungsarbeiten zum «Hacken» von Quantenkryptografie. Die Geräte, wie sie heute auch von den Forschenden für ihre Experimente eingesetzt werden, sind alles andere als perfekt und weisen deshalb Schwächen auf, die geknackt werden können ...

Quelle: Nature, Vol. 447, 24. Mai 2007

CRYPTO AG – TO REMAIN SOVEREIGN

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
Elfenbeinküste
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
Vereinigte Arabische Emirate
Tel. +971 2 64 22 228
Fax +971 2 64 22 118

Buenos Aires
Crypto AG
Maipu 1256 PB «A»
1006 Buenos Aires
Argentinien
Tel. +54 11 4312 1812
Fax +54 11 4312 1812

Kuala Lumpur
Crypto AG
Regional Office Pacific Asia
Level 9B Wisma E&C
2, Lorong Dungun Kiri
Damansara Heights
50490 Kuala Lumpur
Malaysia
Tel. +60 3 2080 2150
Fax +60 3 2080 2140

Muscat
Crypto AG
Regional Office
Seeb PC 111
Sultanat Oman
Tel. +968 2449 4966
Fax +968 2449 8929

A member of
The Crypto Group