CRYPTO

CRYPTO MAGAZINE

N° 1 | 2014

e-Government

Vernetzt – aber sicher

Geschätzte Leserin, geschätzter Leser

Regierungs- und Verwaltungsorganisationen setzen heute zur Erfüllung ihrer Aufgaben zunehmend neue Informations- und Kommunikationstechnologien ein, um die Effizienz, Effektivität und Transparenz zu erhöhen. Als Folge davon fördert e-Government das Vertrauen der Öffentlichkeit in die Tätigkeiten der Regierung, wie im vorliegenden CryptoMagazine auch eine Verantwortliche für e-Government-Projekte der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) versichert.

Da im Rahmen von e-Government grosse Mengen an sensitiven Daten bearbeitet, gespeichert und häufig über mehrere staatliche Stellen hinweg ausgetauscht werden, ist der Sicherheitsaspekt bei der Planung von e-Government-Projekten von zentraler Bedeutung – bereits bei der Ausarbeitung von entsprechenden Strategien und Richtlinien.

Ich wünsche Ihnen bei der Lektüre der neusten Ausgabe des CryptoMagazines viel Vergnügen.

Giuliano Otth

President and
Chief Executive Officer

Fokus

Sicheres e-Government erfordert einheitliche Vorgaben

Seite 3

Impressum

Erscheint 3-mal jährlich | **Auflage** | 6'700 (Deutsch, Englisch, Französisch, Spanisch, Russisch, Arabisch)

Herausgeber | Crypto AG, Postfach 460, 6301 Zug, www.crypto.ch
Redaktionsleitung | Tanja Birrer, Crypto AG, Tel. +41 41 749 77 22, Fax +41 41 741 22 72, tanja.birrer@crypto.ch

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

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

Druck | Druckerei Ennetsee AG, Bösch 35, 6331 Hünenberg

Nachdruck | Honorarfrei mit Zustimmung der Redaktion, Belegexemplare erbeten, Copyright by Crypto AG

Bildnachweis | Crypto AG: S. 9 | e-Government Schweiz: S. 16 | OECD: S. 15 | Parlamentsdienste 3003 Bern: S. 3, 4 | Shutterstock: Titelseite, S. 7, 8 | Thinkstock: S. 6 | Urban Zingg: S. 12, 13 | Wikipedia: S. 19, 20

Sicheres e-Government erfordert einheitliche Vorgaben

Setzt eine Regierung zur Erfüllung ihrer Aufgaben auf neue Informations- und Kommunikationstechnologien, profitieren alle Anspruchsgruppen von den zahlreichen Vorteilen von e-Government. Bevor e-Government jedoch erfolgreich implementiert werden kann, ist die Definition von Strategien und verbindlichen, ministeriumsübergreifenden Vorgaben zwingend.

Tanja Birrer | PR & Corporate Communications Manager

Regierungen verwenden heute bei der Erfüllung ihrer Aufgaben verbreitet neue Informations- und Kommunikationstechnologien (IKT), was die entsprechenden Entwicklungen in der Gesellschaft reflektiert. Positive Effekte dieser grundlegenden Veränderungen in den organisatorischen Strukturen, Prozessen und der Infrastruktur sind unter anderem effizientere Arbeitsabläufe, eine bessere Servicequalität und eine erhöhte Transparenz von Verwaltungs- und politischen Prozessen, was schliesslich das Vertrauen des Bürgers in die üblicherweise eher undurchsichtigen Verwaltungsstrukturen und -abläufe erhöht. Somit lässt sich e-Government mit den Worten der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) zusammenfassend als Einsatz von Informations- und Kommunikationstechnologien mit dem Ziel, dadurch besseres und zeitgemässes Regieren und Verwalten zu bewirken, definieren.

Bei der Beschreibung von e-Government lassen sich verschiedene Perspektiven einnehmen: Einerseits wird unter e-Government der auf elektronischen Dienstleistungen beruhende, interaktive Kontakt der Regierung und öffentlichen Verwaltung zum Bürger (Government to Citizen) verstanden. Weiter können mithilfe des e-Government-Konzepts die auf IKT gestützten Beziehungen der Behörden zur Privatwirtschaft (Government to Business) erfasst werden. Und schliesslich meint e-Government auch den virtuellen Zusammenschluss verschiedener Ministerien und Ämter (Government to Government), wobei (klassifizierte) Daten ausgetauscht und zentral in Datenbanken gespeichert werden, um komplexe Aufgaben gemeinsam anzugehen und Wissen sowie die Infrastruktur zu teilen.

Sicherheit als kritischer Faktor

Dabei wird eines sofort klar: Sobald heikle Informationen – seien es schützenswerte Personendaten oder höher klassifizierte Informationen – bearbeitet, übermittelt oder gespeichert werden, ist der Sicherheitsaspekt zentral. Im Kontext von e-Government hat der Faktor Informationssicherheit gemäss OECD sogar einen erheblichen Einfluss darauf, ob ein geplantes e-Government-Projekt in der breiten Öffentlichkeit Unterstützung findet.

Um von den eingangs beschriebenen Vorteilen von e-Government profitieren zu können, muss daher in einem möglichst frühen Projektstadium zunächst die Interoperabilität der zu verbindenden staatlichen Stellen sichergestellt werden, indem konsolidierte, für alle Beteiligten geltende Richtlinien geschaffen werden: Jedes Ministerium und jedes Amt muss gewisse Bedingungen erfüllen, um an das e-Government angeschlossen werden zu können, beispielsweise bezüglich Klassifizierung und daraus abgeleitetem Schutzbedarf von Daten auf der Basis eines Sicherheitszonenkonzepts.

Die vermeintlich rein technische Herausforderung der Implementierung von e-Government ist somit zunächst eine Problemstellung auf der Agenda der Politik. Denn die Definition von einheitlichen Vorgaben wird im Rahmen von komplexen Entscheidungs- und Strategiefindungsprozessen auf Regierungsebene vorgenommen, bevor die dem e-Government zugrunde liegenden technischen Infrastrukturen konzipiert werden können. In einem ersten Schritt werden die gesetzlichen Grundlagen sowie die übrigen notwendigen Rahmenbedingungen für e-Government geschaffen.

Zudem wird festgelegt, wie die Zusammenarbeit der einzelnen staatlichen Stellen genau ausgestaltet werden soll.

Ministeriumsübergreifende Strategien und Vorgaben
Doch welche staatlichen Institutionen und Verwaltungseinheiten agieren als entscheidungstragende Akteure bei der Schaffung von Rahmenbedingungen für e-Government, der Durchsetzung der Vorgaben und dem Betrieb von gemeinsam genutzter Infrastruktur im Bereich der Informationssicherheit? Welche Gremien erlassen Strategien und Vorgaben?

In generischer und modellhafter Form kann das Zusammenspiel der involvierten Akteure wie folgt beschrieben werden: Auf der Basis des Gesetzes (einschliesslich der Verfassung und Verordnungen wie beispielsweise einer Informationsschutzverordnung, jedoch auch internationaler rechtlicher Vereinbarungen) gibt die Exekutivgewalt der Regierung Strategien in Auftrag, welche die Leitlinien für die inhaltliche Ausgestaltung spezifischer Bereiche der Politik beinhalten und Stossrichtungen für die folgenden Jahre vorgeben. Ausserdem verabschiedet sie diese und überwacht deren Umsetzung. Legislative und Exekutive agieren nicht unabhängig, sondern werden in Strategiefragen beraten und beeinflusst durch Meinungsführer, Lobbys, Nichtregierungsorganisationen, Interessengruppen, Medien, Beratungsunternehmen und Fachgremien. Üblicherweise haben die Repräsentanten der Regierung selbst Einsitz in Fachgremien, was den komplexen Charakter der Strategiefindungsprozesse verdeutlicht.
Da e-Government-Projekte einen hohen Grad an Expertise, Wissen und Erfahrung erfordern, werden auch Berater aus Privatwirtschaft und Wissenschaft einbezogen.

Das Resultat dieses iterativen Prozesses sind übergeordnete, ministeriumsübergreifende Strategien wie beispielsweise eine Strategie der nationalen Sicherheit, eine nationale IKT-Strategie oder eine Informationsgesellschaftsstrategie. Daraus werden anschliessend weitere Strategien und Teilstrategien wie eine nationale Strategie zum Schutz vor Cyberrisiken oder eine nationale e-Government-Strategie abgeleitet.

Eine federführende Rolle bei der koordinierten Umsetzung der e-Government-Strategie nimmt die Behörde ein, die hier generisch als Informatiksteuerungsorgan bezeichnet wird. Sie ist üblicherweise einem Ministerium zugeordnet, nimmt jedoch Aufgaben wahr, welche alle staatlichen Stellen und Verwaltungseinheiten betreffen. So erarbeitet das Informatiksteuerungsorgan beispielsweise die Grundlagen der Informatiksicherheit, erlässt Vorgaben zur IKT-Steuerung und -Sicherheit sowie zur Führung von Projekten und Programmen. Zentral ist im Kontext von e-Government die Definition von ministeriumsübergreifenden Richtlinien zum Umgang mit klassifizierten Daten. Das Informatiksteuerungsorgan wird ebenfalls von diversen Fachgremien beraten, und Delegierte nehmen ihrerseits Einsitz in den Gremien der nationalen e-Government-Organisation, welche die e-Government-Strategie gemäss der strategischen Planung implementiert.

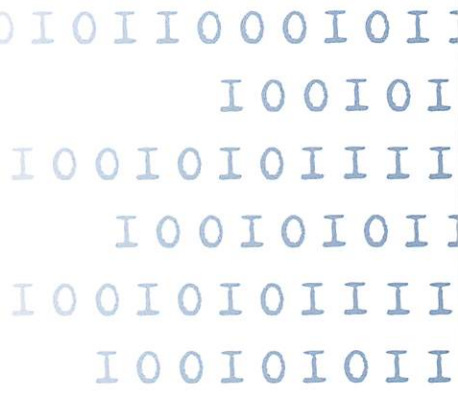
Zusätzlich zum strategischen Informatiksteuerungsorgan erlassen typischerweise auch regulative Organe Vorgaben, welche die Rahmenbedingungen für die Entwicklung von e-Government tangieren: Beispielsweise entscheiden sie, ob internationale Standards übernommen werden oder ob eigene Standards definiert werden müssen. Schliesslich ist ein operatives Organ für den reibungslosen Betrieb gemäss den definierten Vorgaben und Policies verantwortlich – das Sicherheitszonenkonzept kann nun umgesetzt, der geplante Backbone zwischen den Ministerien implementiert werden.

So weit die Theorie. Erfahrungsgemäss stellt die Schnittstelle zwischen funktionalen Anforderungen zur Umsetzung der e-Government-Strategie, der Wahl des bevorzugten Partners und der Berücksichtigung der definierten Mindeststandards zum Schutz der Daten höherer Klassifizierung (vertraulich, geheim usw.) ein Spannungsfeld dar. Dies führt vielfach dazu, dass die e-Government-Lösungen geplant werden, der Sicherheitsaspekt jedoch erst am Schluss berücksichtigt wird.
Die Crypto AG empfiehlt, griffige Standards zumindest für Klassifizierungsstufen ab vertraulich zu definieren und diese konsequent – von Anfang an – in die Planung einzubeziehen. Dies gelingt am besten mit einer IKT-Sicherheitsarchitektur, in der die Mindestanforderungen zum Schutz der klassifizierten Daten, sowohl wenn sie übertragen, bearbeitet als auch auf einem (mobilen) Gerät gespeichert werden, verortet werden.

Quellen

- Informatiksteuerungsorgan des Bundes: www.isb.admin.ch
- Organisation for Economic Co-operation and Development OECD, 2003: The e-Government Imperative
- Organisation for Economic Co-operation and Development OECD, 2010: Good Governance for Digital Policies: How to Get the Most Out of ICT

Immer online, immer mobil: Regieren und Verwalten am Puls der Zeit



Dubai kennt m-Government-Anwendungen und auch Singapur. In Ruanda sind diese zusehends aktuell und auch Brasilien bereitet eine Einführung vor, um die Besteuerung der Bürger und das Wahlsystem zu vereinfachen. Nigeria kennt sie im Zusammenhang mit Dienstleistungen der Polizei, und in der Schweiz ist die Ausweitung eines damit zusammenhängenden Services auf weitere Mobilfunkanbieter im Gang.

Casha Frigo Schmidiger | Publizistin

Die Vorteile von m-Government sind bestechend: Die Kosteneffizienz ist hoch, da es vom Nutzer eine höhere «Beteiligung» und ein grösseres Mitwirken verlangt. Welches dieser jedoch noch so gerne zu geben bereit ist, da sich die genannte Entwicklung dem Benutzer und seinen gewohnten Geräten anpasst und massgeschneidert auf seine Bedürfnisse ist, da von überallher Zugriff besteht. Die Entwicklung führte überdies zu vereinfachten Verifizierungslösungen mit verschiedenen Formen von mobilen Identitäten.

Ja, das mobile Government (m-Government) ist gewaltig auf dem Vormarsch und ist massgeschneidert auf die Lebensart der heutigen «digital nativen» Bürger sowie deren Vorfahren, welche sich zwangsläufig auch mit dem digitalen Fortschreiten auseinandersetzen müssen. Die Bevölkerung ist es sich mittlerweile gewohnt, ihre Kommunikation über mobile Endgeräte abzuwickeln und Dienstleistungen immer mehr auch über solche zu nutzen, vor allem auch via die diversen Apps. Auch die Wirtschaft setzt im Kundenkontakt sowie im internen Einsatz schon länger rund um die Uhr auf Mobilität. Beide erwarten, dass die öffentliche Hand mit diesem Trend mitzieht.

Was nun ist m-Government genau, wie kann man attraktive m-Services designen und wie sieht ein gutes Life Cycle Management für m-Services aus?

Immer näher zum Menschen

M-Government ist die Weiterentwicklung von den behördlichen e-Dienstleistungen noch näher hin zum Kunden. Unser Medienverhalten wandelt sich rasant, im Moment sind mobile Geräte wie Smartphones und Tablets nicht mehr aus dem täglichen Leben wegzudenken. Wir sind immer erreichbar, «always on» und haben konstanten Zugriff auf unsere Daten. Was der Arbeit und Freizeit recht ist, soll auch unserem Informationsaustausch mit und zwischen Verwaltungen und Behörden billig sein. Deren Dienstleistungen müssen heutzutage vermehrt als elektronische Services online angeboten werden, um den modernen Bürger zu erreichen. So wurde aus der Behörde (Government) mit einem bedienten Schalter zunächst e-Government via PC und daraufhin als logische Fortsetzung m-Government mittels Smart Device.

Die im Folgenden verwendete Definition bezieht sich auf den Gebrauch von Informations- und Kommunikationstechnologien (IKT) durch staatliche Stellen: e- und auch m-Government decken alle auf solchen Technologien basierenden Entscheidungs- und Dienstleistungsprozesse in der Politik, der Regierung und der Administration ab.

Zentrales Charakteristikum von m-Government ist die Ortsunabhängigkeit.

Ob Bürger, Unternehmer oder Verwaltungsangestellter: Jeder kann an jedem beliebigen Ort mit anderen kommunizieren, Daten übermitteln und empfangen und Geschäftsprozesse definieren. Diese Arbeitsweise ermöglicht der Verwaltung eine flexiblere und schnellere Aufgabenerledigung und für Bürger und Unternehmen Kommunikationsmöglichkeiten, wann, wo und wie sie es wollen. Dabei geht es vor allem um Anwendungen, welche nicht nur mobil einsetzbar sind, sondern ihren Nutzen erst dadurch erbringen, dass sie mobil verfügbar sind. Neue Dienstleistungen bieten sich vor allem dort an, wo mangels Computer- bzw. Internetzugang bisher keine Lösung möglich war, schwerpunktmässig unter freiem Himmel und bei permanent mobilen Personen.

Der Nutzen ist das wichtigste Kriterium bei der Bestimmung des Sinns einer mobilen Anwendung – die damit zusammenhängenden Vorgänge müssen echt erleichtert werden. Gerade auch verwaltungsintern bestehen sicherlich die vielfältigsten Möglichkeiten für Effizienzsteigerung: Einige Mitarbeiter einer Behörde sind auch aufgrund ihrer Tätigkeiten mobil, gerade die Polizei, die Zollbehörden, Feuerwehr und Katastrophenschutz. Dank mobiler Anwendungen erhalten sie einen ebenso funktionierenden Zugang zu allen Prozessen wie in ihrem Büro. Der Zugang zum Behördennetz ermöglicht das unmittelbare Handeln an Ort und Stelle.

Das hauptsächliche Ziel von digitalem Government ist es, externen Kunden alle Dienstleistungen von öffentlichen Stellen als elektronische oder mobile Angebote zu offerieren. Kunden sind dabei Bürger, Firmen oder andere Stellen der Administration. Somit haben wir drei mögliche Partner oder Anwendungsbereiche, welche in solche e-Government-Prozesse involviert sein können und unterschieden werden müssen:

- **Government to Government (G2G):** Diese Anwendungen decken das grosse Feld der mobilen Beziehungen zwischen verschiedenen staatlichen Behörden und Institutionen ab.
- **Government to Business (G2B):** Dieses Feld umfasst die elektronischen/mobilen Beziehungen zwischen der Administration und Unternehmen.
- **Government to Citizen (G2C):** Diese Situation bezieht sich auf die Interaktionen zwischen Bürgern und der Administration. Dieses Feld umfasst auch die Non-Profit- und die nicht staatlichen Organisationen.

Öffnung der Netze nach aussen

Apps und mobile Anwendungen auf dem Smart Device bedeuten jedoch, dass ein zusätzlicher Kanal eingeführt wird und sich die Komplexität der m-Government-Lösung erhöht, was auch die Sicherheitsrisiken enorm erhöht. Dem Nutzen der mobilen Dienste und Endgeräte stehen also signifikante Gefahren gegenüber. Die Einführung von virtuellen Government-Diensten bewirkt eine Steigerung der bisherigen Sicherheitsproblematik – neue Gefahren kommen hinzu. Immerhin handelt es sich um eine (weitere) Öffnung der bislang geschlossenen Verwaltungsnetze nach aussen.

Deshalb muss ein e- oder m-Government-System, welches entwickelt und eingesetzt werden soll, unter anderem einige zentrale Bedingungen erfüllen, welche in einer frühen Phase der Entscheidungsfindung zu berücksichtigen sind:

- Die **Sicherheit** muss gewährleistet sein: Vertraulichkeit, Integrität, Authentizität sowie Verfügbarkeit müssen beim Gebrauch von m-Government-Anwendungen jederzeit umfassend gewährleistet sein.
- Auch **Flexibilität** ist zwingend: m-Government-Applikationen müssen so gestaltet sein, dass sie ohne grossen Aufwand verändert und erweitert werden können.
- Die **Skalierbarkeit** erhöht die Flexibilität: Eine m-Government-Applikation muss problemlos verteilt werden können.
- **Performanz** ist unumgänglich: Eine kurze Antwortzeit einer Applikation ist äusserst wichtig und vergrössert deren Akzeptanz bei den Anwendern.
- Und die **Fehlertoleranz** erhöht die Akzeptanz: Das System muss fähig sein, unvorhergesehene oder fehlerhafte Systemzustände einfach beheben zu lassen.

Alle Behörden müssen sich in der Informationsgesellschaft behaupten. Apps und mobile Anwendungen auf dem mobilen Endgerät bedeuten, dass sich die Komplexität in der Behördenkommunikation parallel mit den Sicherheitsrisiken erhöht.

Nicht nur G2G, sondern auch G2C schützen

Um Bürgern, Verwaltungsbehörden sowie Aussendienstmitarbeitern öffentliche Informationen und Dienste jederzeit und überall zur Verfügung zu stellen, müssen also nicht nur die richtigen Dienste angeboten und die entsprechende Infrastruktur bereitgestellt werden. Die Sicherheitsproblematik bei der Verwendung mobiler Endgeräte und Infrastruktur stellt Behörden und Anbieter vor die Herausforderung, nicht nur vertrauliche behördliche Daten, sondern auch die Daten der Bürger zu schützen. Dabei ist die Sicherheit von m-Government, die m-Security, ein sehr komplexes Thema, das von leichter Ausspähbarkeit durch Unachtsamkeit beim mobilen Einsatz über erhöhtes Verlustrisiko der Endgeräte, Gefahr durch Viren und Schwachstellen in der Software oder mangelhafte Bluetooth-Implementierung bis hin zum Bruch der softwarebasierten Verschlüsselung durch einen Angreifer reicht.

Im m-Government sind vor allem folgende Risiken zu beachten:

- die permanente Internetverbindung
- ein erhöhtes Verlustrisiko des mobilen Endgerätes
- der Bedarf an hoch entwickelten Betriebssystemen
- mögliche und drohende Angriffe auf VPN-Verbindungen, auf öffentliche Netzwerke und auf den Übertragungsweg
- einfach zu bewerkstelligende Angriffe via Bluetooth, auf WLANs oder auf das GSM-Netz
- physische Attacken und
- das Einschleusen eigener Applikationen[1]

Kein standardmässiger wasserdichter Schutz

Herausforderungen ergeben sich in einer solch vernetzten Umgebung vor allem im Bereich des Datenschutzes und der Datensicherheit. Werden personenbezogene Daten übertragen, so sind diese gegen einen Zugriff Dritter zu schützen. Höchste Sicherheit erreicht man nur mit technischen Massnahmen wie hardwarebasierter Verschlüsselung, für den Schutz der Privatsphäre der Nutzer sowie eine sichere und schnelle Kommunikation der Daten und eine eindeutige Authentifizierung der Beteiligten. Auch der sicheren Speicherung der Daten und der Zugriffskontrolle muss grosses Augenmerk zuteilwerden. Zudem gilt es, den organisatorischen Anordnungen wie vom Gesetzgeber definierten Vorschriften Folge zu leisten.

Mit im Zentrum bei der virtuellen Sicherung der m-Government-Services steht auch die sichere Kommunikation mit mobilen Telefonen. Gerne verweisen wir Sie auf den Artikel «Das Smarte am Phone» in der letzten Ausgabe des CryptoMagazines. Oder in der Quintessenz: m-Government kann nur dann erfolgreich betrieben werden, wenn der Informationssicherheit oberste Priorität eingeräumt wird.

Quelle

[1] DSTGB Dokumentation N 52, www.dstgb.ch; Lothar Fritsch und Kai Rannenberg: Informationstechnische Voraussetzungen von E-Government am Beispiel des Katastrophenschutzes mittels Mobilkommunikation und CryptoMagazine 1|2008.

Best Practice im m-Government

Folgende ausgewählte Beispiele zeugen von der weltweiten Relevanz von m-Government in unterschiedlichen Ausprägungen:

Nigeria i-Police: Hierbei handelt es sich um eine App, welche zu einer effektiven Kooperation zwischen der Bevölkerung und den nigerianischen Sicherheitskräften führt. Zudem können die Bürger damit einerseits über die Prävention von Kriminalfällen informiert werden, es andererseits auch direkt zur Meldung von Schäden oder Verbrechen einsetzen. Die Applikation hat im Jahr 2012 den World Summit Award m-Government in Abu Dhabi gewonnen. www.nigeriapolice.org

Singapore SMS70999: Diese ermöglicht registrierten gehörlosen Personen, eine Notfall-SMS-Helpline zu erreichen, um die Polizei und Notfallorganisationen zu kontaktieren. www.spf.gov.sg/sms70999

Estonia Mobile ID: Ist ein Service, welcher einem Nutzer erlaubt, ein Mobiltelefon zur sicheren digitalen Identifizierung zu verwenden. Wie eine Identitätskarte kann die Mobile ID verwendet werden, um Zugang zu sicheren e-Services zu erhalten. Sie basiert auf einer spezialisierten Mobile-ID-SIM-Karte. www.gsma.com/mobileidentity

UAE Kooperation von Etisalat und SAP: Der lokale Operator Etisalat und der deutsche Softwaregigant SAP haben im Jahr 2013 in den Vereinigten Arabischen Emiraten zusammengespannt, um ein m-Government Framework zu etablieren. Die Kooperation ermöglicht mobile Services in den Bereichen Mobilität, Gesundheit, Bildung und Tourismus. Etisalat gewann im selben Jahr den Global Mobile Award für den «Best Mobile Money Service». www.etisalat.ae

Schweden Roadroid: Diese offeriert eine mobile Applikation für Android-Smartphones, um den Strassenzustand zu prüfen, in Kombination mit einer Website, auf welcher die Strassen auf der Karte farbig markiert werden. Die App verwendet ins Mobiltelefon eingebaute Sensoren, die Kamera und GPS. www.roadroid.se

Brasilien My Fun City – Sustainable Cities: Dies ermöglicht die Einflussnahme der Behörden auf verschiedene Lebensbereiche per Online-Befragung mit dem Ziel, eine lebenswertere Umgebung/Stadt zu erhalten. www.myfuncity.org

Suisse ID: Die Suisse ID ist der erste standardisierte elektronische Identitätsnachweis der Schweiz, mit dem eine rechtsgültige elektronische Signatur möglich ist. Mit der als USB-Stick oder Chipkarte erhältlichen Suisse ID können Geschäfte von Privatpersonen mit Verwaltungen (oder auch mit Unternehmen) direkt über das Internet oder per E-Mail abgeschlossen werden. Sie wurde im Mai 2010 im Schweizer Markt lanciert. Zur Anwendung gelangt die Suisse ID, um eine authentifizierte digitale Kommunikation zu ermöglichen – so, wie sie im Mobile Government stattfindet. Mit dem Einsatz der Suisse ID können folgende Voraussetzungen für ein sicheres m-Government erfüllt werden:

- **Elektronischer Identitätsnachweis:** Mit der Suisse ID können elektronische Dienstleistungen in Anspruch genommen werden, die eine sichere Identifizierung der Nutzer bzw. Kunden bedingen.
- **Qualifizierte elektronische Signatur:** Mit der Suisse ID lassen sich auch Dokumente elektronisch unterschreiben. Eine solche digitale Signatur gilt als fälschungssicher und ist gesetzlich der manuellen Unterschrift gleichgesetzt.

www.suisseid.ch

Echter Mehrwert durch Sicherheit in elektronisch abgebildeten e-Government-Prozessen

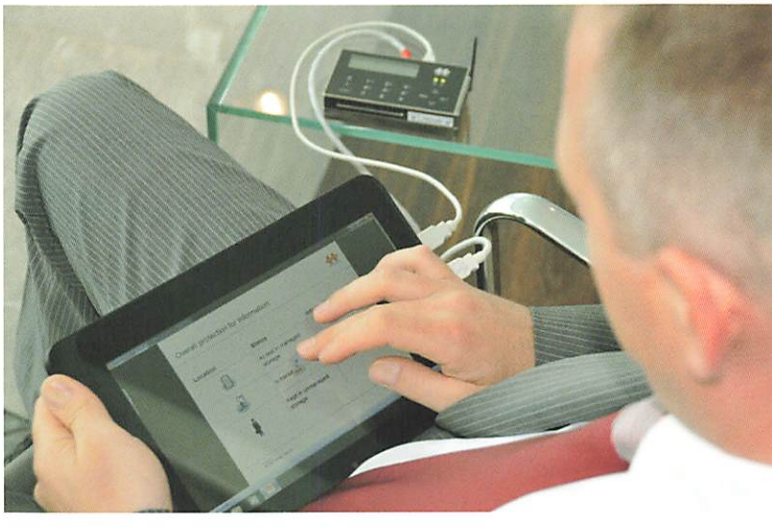
Das Entwickeln von e-Government-Dienstleistungen erfordert eine ganzheitliche Sichtweise: Aufbauend auf einer e-Government-Strategie und klaren Security Requirements wird eine adäquate ICT-Sicherheitsarchitektur erarbeitet. Die daraus abgeleiteten Sicherheitsmassnahmen – seien es technische oder prozedurale Kontrollen – werden schliesslich in die Infrastruktur und Abläufe integriert. Daraus resultieren sichere und verlässliche e-Gov-Workflows.

Urs Kürzi | Customer Segment Manager

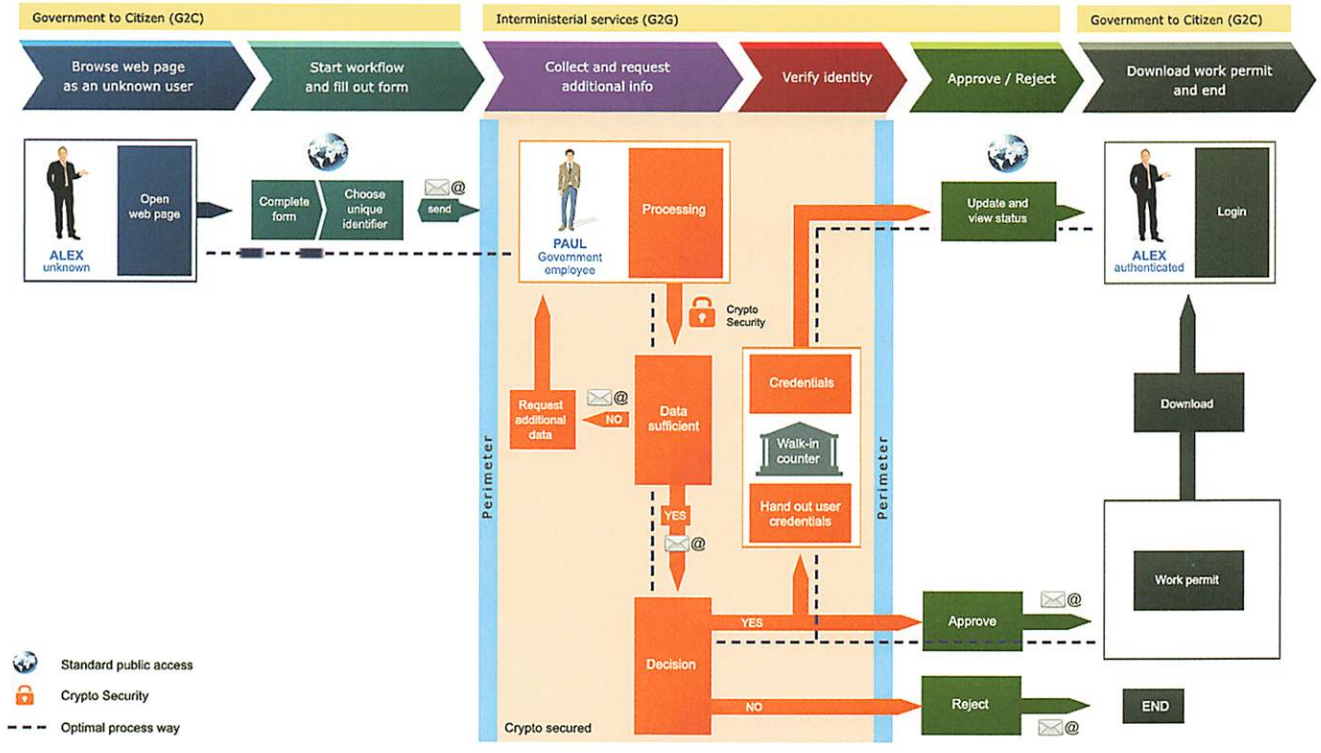
Herr K. aus S. arbeitet im Büro am Computer. Er beabsichtigt, für einen Fachspezialisten eine Arbeitsbewilligung für die nächsten drei Jahre zu beantragen, weshalb er zur Homepage der Regierungsadministration des Landes C surft. Er findet leicht heraus, welche Beamten für Arbeitsbewilligungen zuständig sind, wie er vorzugehen hat und welche Informationen er liefern muss. Herr K. besitzt vom zukünftigen Expat (in der Grafik als «Alex» bezeichnet) je eine Datei des eingescannten Arbeitsvertrages und seines Passes. Die Befürchtungen seines Expats, bei der Einreise wegen unklarer Formalitäten über Stunden am Zoll festzusitzen, oder dass seine persönlichen Daten sogar von unberechtigten Dritten eingesehen werden, kann er entkräften. Das Interesse der Regierungsadministration auf der anderen Seite besteht darin, keine Vergaben von Arbeitsbewilligungen an nicht vertrauenswürdige Personen gutzuheissen.

Dieser elektronische Prozess ist kein Zukunftsszenario, sondern dank umfangreichen Sicherheitsmassnahmen ein realer e-Government-Service von heute. Die Crypto AG nimmt bei solchen Projekten eine beratende Funktion wahr, damit der Zonenübergang (Public / Secure Intranet) angemessen geschützt wird, und bringt ihr Wissen ein, sodass das empfohlene Produkt richtig implementiert und konfiguriert wird und somit dem Schutz des Portals dient.
Der e-Government-Prozess ist dann sicher, wenn Lösungen der Crypto AG zur Verschlüsselung der interministerialen Kommunikation zur Anwendung kommen und die Sicherheitsarchitektur mit den Konzepten der Crypto AG implementiert wird. Denn nur dank einer umfassenden ICT-Sicherheit in perfektem Zusammenspiel von Software- und Hardwareverschlüsselung bestehen weder für Bewerber noch für Behörden Sicherheitslücken.

Praxisorientierte e-Government-Prozesse
Der Prozess sieht im Detail wie folgt aus: In einem ersten Schritt füllt Herr K. das elektronische Formular aus, indem er die persönlichen Angaben des Expats erfasst. Im Anschluss sendet er den Antrag zusammen mit dem eingescannten Arbeitsvertrag und dem Pass elektronisch an die zuständigen Behörden. Zu diesem Zeitpunkt ist der Expat den Behörden noch nicht bekannt:



Vertrauliche Daten können ausserhalb eines abgeschirmten Netzwerks mit der Secure-Remote-Access-Lösung geschützt abgerufen und genutzt werden. Der Beamte hat für die Bearbeitung der Arbeitsvisa volle Flexibilität und nutzt die hardwarebasierten Sicherheitslösungen der Crypto AG.



Kundenspezifische Prozessschritte in einer e-Government-Lösung vom Antrag bis zur Ausstellung einer Arbeitsbewilligung. Es gibt drei Sicherheitsherausforderungen zu bewältigen:

- Zugriff eines nicht autorisierten Antragstellers (in der Grafik «Alex») via Webbrowser auf den e-Service des Büros für «Business Development».
- Der Beamte (in der Grafik «Paul») überprüft in der gesicherten Zone (Secure Governmental Intranet) mit geeigneten Verfahren die Identität des Antragstellers.
- Das Vertrauensverhältnis zwischen Antragsteller und Behörde ist etabliert; der Antrag wird bewilligt und ist als PDF zum Download für den Selfservice bereit.

Der Antrag für dieses Arbeitsvisum könnte für irgendeine beliebige Person gestellt werden.

Aufseiten der Behörden stellt sich nun daher die Aufgabe der Verifikation der Daten. Die persönlichen Daten des Expats sind über eine softwarebasierte Informationssicherheitslösung vom Browser ins Intranet der Migrationsbehörde übertragen worden – es ist also ein Transfer über eine Verbindung mit ausschliesslich kommerzieller Handelsware getätigt worden. Die softwarebasierte Informationssicherheitslösung hat eine sichere Verbindung zwischen zwei Teilnehmern errichtet. Hierzu ist die Verhandlung der Parameter zwischen Client und Server vorgenommen, ebenso die gegenseitige Authentifizierung, der Schutz der Datenintegrität und ein Verfahren zur Verschlüsselung der Übertragung ausgewählt worden. Diese softwarebasierte Informationssicherheitslösung kann verschiedene kryptografische Verfahren unterstützen, wie beispielsweise Triple DES oder AES. Ist die Implementierung sorgfältig erfolgt und generiert der Schlüsselgenerator auch tatsächlich zufällige Schlüssel, die angemessen geschützt sind, so gilt die softwarebasierte Sicherheitslösung durchaus als geeignet, die bis anhin nicht authentifizierten e-Government-Benutzer am e-Government-Service partizipieren zu lassen.

Der Beamte (in der Grafik als «Paul» bezeichnet), der die Bearbeitung der Arbeitsbewilligung im Büro «Business Development» vornimmt, wird durch ein E-Mail über den Erhalt des Antrags in Kenntnis gesetzt. Der Beamte wählt sich über eine Secure-Remote-Access-Verbindung in das gesicherte Intranet der Regierung ein. Hierfür setzt er den Crypto Secure Mobile Client HC-7835 via einen separaten Zugang ein und authentisiert sich via Zweifaktor-Authentifikation. Das Intranet der Regierung ist auf höchstem kryptografischem Niveau mit Hardwareverschlüsselung der Crypto AG gesichert. Hardwarebasierte Chiffrierung bildet die Grundlage für maximale kryptografische Vielseitigkeit – einerseits aus Geschwindigkeitsgründen, andererseits wegen ihrer Mani-pulationssicherheit. Ausserdem laufen die Chiffrierprozesse getrennt von der Netzwerkfunktionalität ab. Die individua-lisiert erzeugten Kundenalgorithmen stehen unter der ausschliesslichen Kontrolle des jeweiligen Kunden, sind keinem anderen Kunden bekannt und werden von niemandem sonst benutzt. Selbst mit einem gleichen Gerät ist kein kryptografischer Angriff möglich. Auch die Crypto AG hat keinen Zugriff.

Für die Bearbeitung des Antrags ist darüber hinaus eigens eine Applikation entwickelt worden, die sich perfekt in die übrige IT-Infrastruktur einfügen lässt. Das Leistungspaket dieser Applikation umfasst die Kontaktaufnahme mit dem Antragsteller, das Akzeptieren und Ablehnen der Arbeitsbewilligung sowie viele Filter- und Berechtigungsfunktionen.

Die Prüfung des Antrags erfolgt auf dem auf höchstem kryptografischem Niveau gesicherten Intranet der Regierung, in der Regel über mehrere Organisationen hinweg, wie beispielsweise Rückfragen ins Arbeitsamt, ins Justiz- und Polizeidepartement (Strafregister) oder ins Ministerium für Migration.

Fehlen gewisse Angaben, kann der Beamte mit dem Antragsteller direkt via E-Mail (Chat) Kontakt aufnehmen und die notwendigen Informationen einfordern. Hierbei führt die Kommunikation über einen Perimeter ins Internet.

Ist die Identität geprüft, meldet der Beamte dem Antragsteller das Ergebnis per E-Mail mit der Instruktion des weiteren Vorgehens. Dies hat zur Folge, dass der Antragsteller bei Ankunft am Flughafen im Land C seine Matrixkarte persönlich auf dem Büro «Business Development» (Walk-in Counter) abholen kann.

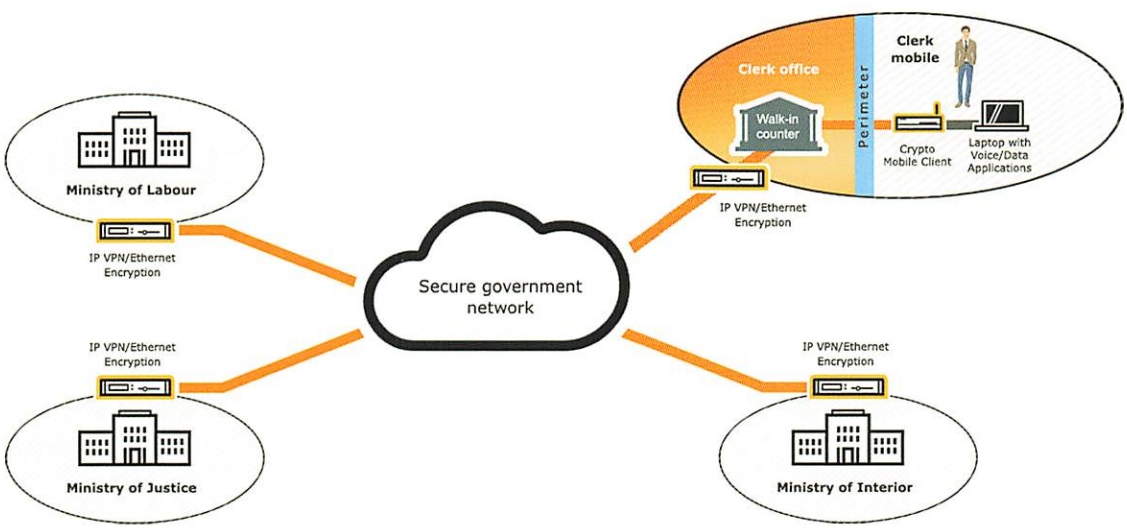
Erfolgreiche Authentifizierung von Antragstellern
Das Kernelement im Prozess der Authentifizierung von Antragstellern ist das Büro «Business Development», der sogenannte Walk-in Counter. Der Antragsteller identifiziert sich dort mit dem Pass und den dazugehörigen Papieren beim diensthabenden Offizier. Ist die Identität klar, bekommt der Antragsteller die Matrixkarte überreicht. Diese Matrixkarte ermöglicht ihm den Zugang mit einer Zweifaktor-Authentifizierung für den Online-Selfservice des e-Gov-Portals. Sein Arbeitsvisum ist dort zum Download in der Form eines PDFs bereit. Das Vertrauensverhältnis zwischen Behörde und dem Antragsteller (Alex) ist etabliert und erlaubt Letzterem die sofortige Nutzung des Selfservices mit klassifizierten Informationen. Das persönliche Erscheinen im Büro «Business Development», dem Walk-in Counter, ist eine einmalige Notwendigkeit und dient ausschliesslich der Authentifizierung.

Entwicklung von e-Government-Service: Nur mit ICT-Sicherheit

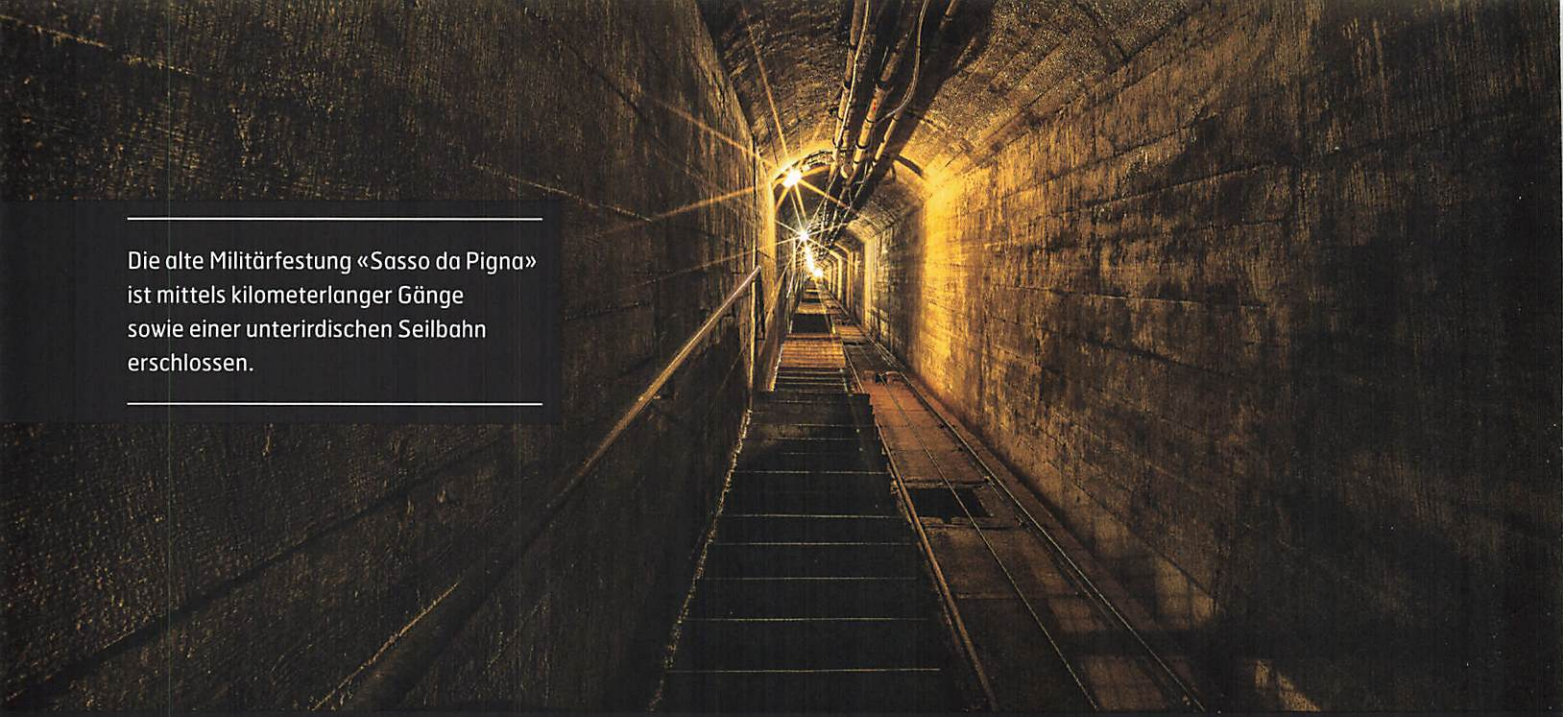
Eine Behörde erbringt Dienstleistungen für das Gemeinwesen als Ganzes wie auch für Privatpersonen und Unternehmen. Basierend auf dem Verständnis, was für eine prosperierende Region wichtig ist, gibt die Regierung Ziele, Aufträge und Vorgehen vor. So hat sie in obigem Beispiel ein Projekt zur Bewältigung von Anträgen für Arbeitsbewilligungen ausgewählt. Im Zuge dessen Bürokratieabbau, Kostenersparnisse und vor allem rasche Entscheidungswege grosse Erleichterungen im täglichen Geschäft bringen.

Für eine moderne Dienstleistungs- und Informationsgesellschaft ist ein einfacher und schneller Kontakt mit den Behörden ein entscheidender Wirtschaftsfaktor. Unternehmen und deren potenziellen Arbeitnehmer erwarten eine an ihren Bedürfnissen orientierte Abwicklung der Geschäfte, im obigen Beispiel eine auf elektronischem und gesichertem Weg geführte Erlangung einer Arbeitsbewilligung.

Das bedeutet für die Behörden: Nur mit einem nachhaltigen Konzept zur ICT-Sicherheit gewinnt der Benutzer Vertrauen in e-Government-Services.



Eine Verschlüsselungslösung der Crypto AG stellt sicher, dass im interministeriellen Kommunikationsnetz die Daten vertraulich, integritätsgeschützt und authentisiert ausgetauscht werden. Der Beamte kann sowohl mobil als auch über seinen Desktop-Computer die Arbeitsbewilligungen bearbeiten.



Die alte Militärfestung «Sasso da Pigna» ist mittels kilometerlanger Gänge sowie einer unterirdischen Seilbahn erschlossen.

Trutzig-informativer Zeitzeuge des Schweizer Wehrwillens und Widerstands

3,5 Tonnen schwere Panzertüren, kugelsichere Einmannschleusen und Spezialkameras in jeder Ecke – was anmutet wie ein Hochsicherheitsgefängnis, das ist das «Swiss Fort Knox». In den Sechzigerjahren wurde der Berg (an einem nicht genannt sein wollenden Ort) von der Schweizer Armee buchstäblich ausgehöhlt und als Festung genutzt. Seit 1996 können sowohl Unternehmen wie auch Privatpersonen ihre Daten dorthin auslagern und buchstäblich bombensicher ablegen.

Casha Frigo Schmidiger | Publizistin

So wie das Swiss Fort Knox existieren in der Schweiz ein Dutzend einzigartige unterirdische Rechenzentren in alten Festungsanlagen der Schweizer Armee: Diese werden als topmoderne Datentresore für sensible Informationen wie Kunden-, Produktions- oder Finanzdaten genutzt. Das stellt eine sinnvolle Art dar, wie in der Schweiz die unzähligen sich in den Alpen befindlichen alten Militärfestungen genutzt werden können. Die ältesten datieren bis auf den Bau der Gotthardbahn von 1872 zurück. Dieser Umstand veranlasste die Schweizer Armee schon weit vor dem Ersten Weltkrieg zum Bau von in den Fels geschlagenen Artilleriewerken nördlich und südlich des bis heute wichtigsten Alpenübergangs. Nach dem Krieg wurden die Befestigungstätigkeiten weiter vorangetrieben und erreichten ihren Höhepunkt während des Zweiten Weltkrieges, als im ganzen Schweizer Alpenraum unter hohem Zeitdruck gewaltige Festungswerke erstellt wurden. Diese wurden auch nach Kriegsende noch Jahrzehntelang – bis 1995 – vom Festungswachtkorps betrieben, einer Berufsformation der Schweizer Armee.

Gerade das Tessin sah sich während des letzten Weltkrieges umzingelt von den Achsenmächten – siebzehn Kilometer vom Gotthard entfernt fing bereits das Feindesland an. So wurde beispielsweise das Artilleriewerk «Sasso da Pigna» während des Zweiten Weltkrieges als Teil des nationalen Réduits gebaut und war auch noch während des Kalten Krieges bis 1999 in Betrieb. Damit die Festung «da Pigna» für die Nachwelt erhalten werden kann, wurde 2012 die Stiftung «Sasso San Gottardo» gegründet, an welcher auch die Crypto AG beteiligt ist. So können sich nun Interessierte während der Gotthardpass-Öffnungszeiten im Sommer ein Bild davon machen, wie sich das Leben eines Soldaten oder Offiziers «unter Tag» angefühlt haben muss.

Eindrücklich bis hin zur Ehrfurcht
Den Eingang in die historische Festung, welche nun ebenso «Sasso San Gottardo» heisst, bildet eine quadratische, ins Gestein gezimmerte Öffnung. Dahinter führt ein langer Gang schnurgerade in den Berg hinein. Was zuerst auffällt, ist die eher niedrige Temperatur. Ist es draussen über 30 Grad warm, geht es im Berginnern bis auf 7 Grad hinunter – was gerade im Sommer sehr angenehm ist. Die feuchten Gänge und das schummrige Licht tragen zum einzigartigen Ambiente des Ortes bei. Der vordere Teil der zweieinhalb unterirdische Kilometer umfassenden Anlage beherbergt verschiedene erlebnisreich inszenierte Themenwelten zu den Bereichen «Mobilität», «Verkehr», «Energie» und «Sicherheit». Die Inhalte wurden in Zusammenarbeit mit Wirtschaftspartnern sowie der Wissenschaft entwickelt und orientieren sich an Erkenntnissen aus der aktuellen Forschung. Sie tragen klar die Handschrift ihrer Macher, welche ebenso für die Landesausstellung EXPO 02 verantwortlich zeichneten.

Der Sicherheit ist ein eigener Stollen gewidmet

Täglich werden weltweit über 294 Milliarden E-Mails versendet und 3 Millionen Bilder bei flickr hochgeladen, mit welchen man 375'000 Seiten eines Fotoalbums füllen könnte. Dazu werden pro Tag 43'339'547 Gigabyte Daten via Mobiltelefon versendet, damit könnte man 1,7 Millionen Blu-Ray-Discs füllen oder 9,2 Millionen DVDs. Das erfährt beispielsweise der erstaunte Besucher im Raum «Sicherheit» – während er Lichtschranken überschreitet und ihm von der Decke entgegenleuchtet, dass er gerade über sein Mobiltelefon geortet wird. Zudem erfährt man einiges über Robin Sage, die fiktive, hübsche Amerikanerin, welcher es gelang, mittels Social Engineering sensible Daten der US-Regierung auszuspionieren, und vieles mehr. Die Diskrepanz zwischen der digitalen Welt und der sich darin befindlichen Gefahren und dem Bollwerk Berg mit integrierter Festung könnte nicht grösser sein, und doch hängen die beiden – digitale und reale Sicherheit – eng zusammen. Auch im Zeitalter des Cyberwars, wie aktuelle Beispiele des Weltgeschehens einem wieder plastisch vor Augen führen.

Pulverdampf und Kanonendonner
Diese Themenwelten stellen das erste Highlight von «Sasso San Gottardo» dar. Wer diese verlässt, muss zuerst einen fast einen Kilometer langen unterirdischen Weg zurücklegen, bis er zu einer nostalgischen Seilbahn im Innern des Berges gelangt, welche ihn zur historischen Festung bringt.
Der Rundgang durch diese ist ein Erlebnis für sich. Man bewegt sich nicht in einem Museum, sondern tritt in die Geschichte ein, welche hier konkret erlebbar wird. Noch heute können die zwei 15-cm-Bunkerkanonen der Batterie West Richtung Nufenenpass besichtigt werden. Man riecht förmlich noch den Pulverdampf und hört das Donnern der Kanonen. Die Bedeutung der Alpenübergänge war so hoch, dass die strategisch wichtigen Festungen erst nach Ende des Kalten Krieges geschlossen wurden.

In «Sasso San Gottardo» wird den Besuchern plastisch vor Augen geführt, welche Werte bis heute zum grundlegenden Selbstverständnis aller Nationen und somit auch der Schweiz zählen: Unabhängigkeit und kulturelle Selbstständigkeit. Ein absolut lohnenswerter Besuch.

In der Ausstellung «Sasso San Gottardo» werden Themen wie «Sicherheit», «Energie» oder «Mobilität» plastisch veranschaulicht.

«E-Government fördert das Vertrauen der Öffentlichkeit in die Tätigkeiten der Regierung»

Interview mit Barbara-Chiara Ubaldi, OECD e-Government Project Manager

Das Interview führte Tanja Birrer | PR & Corporate Communications Manager

Frau Ubaldi, welche Treiber von e-Government-Projekten können unabhängig von länderspezifischen Rahmenbedingungen identifiziert werden und welchen Mehrwert bietet e-Government aus Sicht der Regierung und der Bürger?
Barbara-Chiara Ubaldi: Unterschiedliche Treiber politischer, sozialer und ökonomischer Natur beeinflussen in den Mitgliedstaaten der OECD (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung) die Entwicklung und Implementation von e-Government-Strategien. So können der Einsatz von neuen IKT (Informations- und Kommunikationstechnologien) und ein verbessertes Management der internen Prozesse zu einer Erhöhung der Effizienz im öffentlichen Sektor führen, beispielsweise im Erbringen von behördlichen Dienstleistungen. E-Government ermöglicht es, Dienstleistungen über verschiedene Kanäle (Internet, Mobiltelefon usw.) anzubieten, was dem Bedürfnis des modernen Bürgers entspricht.

Der dank neuen IKT und der darauf basierenden Entwicklung von Mobile Government verbesserte Zugang zu behördlichen Dienstleistungen (zu jeder Zeit und an jedem Ort) führt seinerseits zu einer erhöhten Transparenz der Regierungsgeschäfte. E-Government-Strategien heben meist den vereinfachten Zugang zu Informationen über Projekte, Programme und sonstige Aktivitäten der Regierung hervor. Dabei besteht das Ziel darin, das Verständnis der Bevölkerung den Aufgaben der Regierung gegenüber zu erhöhen, damit deren Leistungen schliesslich bewertet werden können.

Das aktive Mitwirken der Öffentlichkeit bei der Ausgestaltung der behördlichen Dienstleistungen sowie bei Entscheidungs- und Strategiefindungsprozessen ist ebenfalls ein wichtiger Treiber.

E-Government kann zudem zum ökonomischen Wachstum und zur Konkurrenzfähigkeit eines Landes beitragen: In einem transparenten Umfeld ist es einfacher, Geschäfte zu tätigen. So ist zum Beispiel die Gründung eines neuen Unternehmens schneller und unkomplizierter möglich. Nicht zuletzt bilden sich dank neuen Kommunikations- und Interaktionsformen auch neue Wirtschaftszweige heraus. Schlussendlich und zusammenfassend kann e-Government wesentlich dazu beitragen, das Vertrauen der Öffentlichkeit in die Tätigkeiten der Regierung zu fördern.

Welche Hindernisse erschweren im Allgemeinen die Entwicklung von e-Government-Projekten?
Die Hindernisse sind verschiedener Art: Einige beeinflussen die Entwicklung von e-Government negativ, während andere die Erreichung der erwarteten Ziele tangieren. Zu Ersteren würde ich zum Beispiel inadäquate rechtliche und regulative Frameworks zählen, jedoch auch eine fehlende Kultur der Koordination, Zusammenarbeit und des Teilens von Informationen innerhalb der Verwaltung, und nicht zuletzt geringes spezifisches Fachwissen in diesem Bereich bei den staatlichen Stellen. Betrachten wir die Faktoren, die einen direkten Einfluss auf die Zielerreichung haben, können die träge Adaption von online verfügbaren Dienstleistungen durch die Bürger und Unternehmen, inadäquate Infrastrukturen (beispielsweise eine geringe Verbreitung von hohen Bandbreiten) sowie der geringe Einsatz von Business-Case-Modellen und/oder die fehlende Berücksichtigung von Richtlinien bei der Implementation von e-Government-Strategien und bei der Messung von Resultaten Hindernisse darstellen.

In welchen geografischen Regionen identifizieren Sie aufgrund welcher Rahmenbedingungen besonderes Potenzial für zukünftige e-Government-Projekte?
Diese Frage lässt sich nicht generell beantworten; vielmehr müssen die unterschiedlichen Phasen der e-Government-Entwicklung, in denen sich die verschiedenen Länder befinden, in die Analyse mit einbezogen werden, um Faktoren, welche einen Einfluss auf die Entwicklung haben, identifizieren zu können. Wir wissen, dass bestimmte

Kategorien von Ländern mit jeweils ähnlichen Problemstellungen konfrontiert sind. So beschäftigen sich die in e-Government-Projekten fortgeschrittenen Länder hauptsächlich mit der Frage, wie sie die Zielerreichung mittels Einsatz von bereits existierenden Technologien noch optimieren können (Stichworte Open Data, Mobile Government). Für Länder, die mit der Implementation von e-Government-Projekten noch wenig Erfahrung haben, ist es hingegen wichtiger, zunächst die Lücke zu den fortgeschrittenen Ländern zu schliessen und damit zusammenhängend die digitale Kluft, das heisst den Ausschluss von Teilen der Bevölkerung von der Nutzung des Internets und allgemein IKT, zu überwinden.

Welche Erfolgsfaktoren für das Design der IKT Policy und deren Implementation in einem Land stufen Sie als besonders bedeutend ein?

Einige der zahlreichen Erfolgsfaktoren sind das Vorhandensein eines adäquaten rechtlichen und regulativen Frameworks, die Definition von Business Cases, um Investitionen in IKT-Projekte zu generieren und die zu erreichenden Ziele festzulegen, die Förderung einer angemessenen Organisationskultur sowie des Verständnisses der Bedürfnisse der modernen Bürger bei den staatlichen Stellen. Zudem ist es essenziell, über verschiedene Regierungsebenen hinweg eine klare gemeinsame Richtung einzuschlagen, einen einheitlichen Massnahmenplan zu erstellen, um die definierten Ziele erreichen zu können sowie ein adäquates Governance Framework zu erarbeiten, welches die Zusammenarbeit der verschiedenen Akteure innerhalb und über verschiedene Regierungsebenen hinweg festlegt. Diese Massnahmen ermöglichen einerseits die Steuerung und politische Verankerung von e-Government-Projekten, während andererseits die gemeinsame Verantwortung und Ausgestaltung der Prozesse und Massnahmen die Ergebnisse positiv beeinflussen.

Das in der OECD-Publikation «Good Governance for Digital Policies: How to Get the Most Out of ICT» beschriebene Mehrebenen-Governance-Framework verdeutlicht die Komplexität der Entscheidungsfindungs- und Strategiedefinitionsprozesse. Welche Behörden nehmen in diesem Framework eine entscheidende Rolle ein und wie kann eine optimale Koordination der verschiedenen Akteure sichergestellt werden?

Die Charakteristika eines adäquaten Frameworks sind sehr kontextabhängig. Es gibt daher nicht nur ein erfolgversprechendes Modell. So bedürfen eher zentralisiert oder dezentralisiert organisierte Regierungen unterschiedlicher Frameworks. Für alle Länder gültig ist jedoch die Notwendigkeit, ein Mehrebenen-Governance-Framework zu erarbeiten, woraus schlussendlich eine klare einheitliche e-Government-Vision für das betreffende Land resultiert, welche über die Regierungsebenen hinweg geteilt wird. Zentral sind zudem die Institutionalisierung der Steuerung und der politischen Verankerung in den entsprechenden Regierungsebenen, und nicht zuletzt der Mechanismen, welche die Koordination und

Barbara-Chiara Ubaldi

Seit Oktober 2010 leitet Barbara-Chiara Ubaldi das e-Government-Projekt in der Abteilung Public Governance and Territorial Development der OECD. Dabei koordiniert sie die Analyse des Einsatzes von neuen Technologien in der öffentlichen Verwaltung. Zuvor arbeitete Barbara-Chiara Ubaldi einige Jahre als Programme Officer für die Vereinten Nationen in New York, wo sie für die Entwicklung und das Management von e-Government-Programmen und -Instrumenten verantwortlich war. Barbara-Chiara Ubaldi studierte unter anderem Politikwissenschaft, Internationale Beziehungen, Öffentliche Verwaltung und Entwicklung sowie Rechtswissenschaft in Rom und Boston.

Im Oktober 2013 fand in Bern (Schweiz) das OECD High Level Meeting zum Thema e-Government statt.

Zusammenarbeit über die Regierungsebenen hinweg ermöglichen. Die staatlichen Stellen, die für die Informationsgesellschaft, e-Government, Cyber Security oder IKT-Sektorprogramme (z. B. e-Health) usw. verantwortlich sind, müssen zusammenarbeiten, um ihre Ziele zu erreichen.

Inwiefern ist die OECD selber in politische Strategiedefinitionsprozesse der Regierungen der Mitgliedstaaten im Bereich der IKT-Governance involviert? Setzt die OECD auf die Eigenverantwortung der Mitgliedstaaten bei der Umsetzung der Richtlinien oder verabschiedet sie für staatliche Stellen verbindliche Standards (analog dem US-amerikanischen FISMA-Standard [Federal Information Security Management Act of 2002], einem Informationssicherheits-Compliance-Framework)?

Die OECD gibt Normen und Standards für die Übernahme von Policy-Instrumenten vor, welche rechtlich nicht bindend sind, jedoch den politischen Entscheidungsträgern als Richtlinien dienen sollen. Da diese Richtlinien auf Best Practices in den OECD-Ländern basieren, ist es üblich, dass die Regierungen diese bei den Entscheidungsfindungs- und Strategiedefinitionsprozessen berücksichtigen, nicht zuletzt auch, um ihre e-Government-Fortschritte beurteilen zu können. Die OECD verwendet diese Richtlinien als Grundlage, um die Performance der Länder zu vergleichen. Die OECD entwickelt beispielsweise eine Reihe von e-Government-Strategie-Prinzipien und erstellt einen regelmässigen Report über den Projektstatus und die Erfüllung der Kriterien: Sind diese bei der Definition von neuen Strategien, bei der Übernahme von neuen Policies berücksichtigt worden? Können Fortschritte in der Strategie-Implementation verzeichnet werden?

In der OECD-Publikation «The e-Government Imperative» wird die Relevanz der Informationssicherheit im Zusammenhang mit e-Government hervorgehoben: «Öffentliche Verwaltungen werden weiterhin Policies und technische Lösungen rund um die Sicherheit, Authentisierung und Datenspeicherung definieren müssen, um den Schutz der Personendaten wahren zu können. Wenn dieses Thema vernachlässigt wird, hat es – mehr als jedes andere – das Potenzial, dass e-Government-Projekte keine Unterstützung finden.» Welche hauptsächlichen Herausforderungen in der Informationssicherheit stellen sich einem Land, um e-Government erfolgreich implementieren zu können?

Regierungen müssen Massnahmen ergreifen, um allfällige Verletzungen der Informationssicherheit (inklusive des Schutzes von sensitiven Daten) zu umgehen. Dazu sind nicht nur entsprechende Gesetze und der Einsatz von sicheren IT-Systemen notwendig, sondern auch die Förderung einer entsprechenden Kultur unter den Beamten, welche Zugang zu sensitiven Daten haben. Der letzte Punkt wird in Zukunft an Relevanz gewinnen, weil Open Data in den OECD-Ländern immer mehr zum Thema werden und der Einsatz von Social Media im öffentlichen Sektor weiter zunehmen wird.

Frau Ubaldi, herzlichen Dank für diese spannenden Ausführungen.

Die Verwundbarkeit des Internets liegt in seiner heutigen Natur

Das Internet hat in fast alle Lebensbereiche Einzug gehalten und ist aus unserer modernen Welt nicht mehr wegzudenken. Gleichzeitig machen sich hochtechnologische Gesellschaften nicht nur immer abhängiger von der ständigen Verfügbarkeit des Cyberspace, sondern sie setzen sich auch seinen nicht zu unterschätzenden Risiken aus. Woher genau rührt unsere neue Verwundbarkeit jedoch aus technischer Sicht? Ein Exkurs.

Jahn Koch | Customer Segment Manager

Wer die Angriffsflächen und insbesondere die Abhörgefahr des Internets verstehen will, kommt nicht umhin, sich mit dessen Aufbau zu befassen. Dabei fällt es zunächst schwer, das Internet einzugrenzen oder griffig zu beschreiben. Der Grund dafür ist, dass das Internet nicht strukturiert oder kontrolliert nach Plan, sondern historisch und organisch gewachsen ist. Das Wort «Internet» beschreibt daher keine in sich abgeschlossene Entität, sondern ist heute vielmehr ein Sammelbegriff für eine Vielzahl von Unternetzen, Übertragungsmedien, Übermittlungsarten und -geschwindigkeiten. Eines jedoch verbindet alle Anwendungen, Geräte und Netzinfrastrukturen, die im Kommunikationsverbund des Internets zusammenspielen: Sie sprechen alle die gleiche Sprache.

Am Anfang stand eine Universalsprache

Die bescheidenen Anfänge des Internets liegen in den 1960er-Jahren, als das US-Verteidigungsministerium die Schaffung eines Führungs- und Kommunikationsnetzes in Angriff nahm, das dezentral organisiert und somit militärisch schwer angreifbar sein sollte. Im Laufe der 1970- und 1980er-Jahre entstanden nach dem gleichen Muster Computernetze für die zivile Welt, vorab zwischen amerikanischen Universitäten für den wissenschaftlichen Austausch. Hauptsächlich wurden dazu die bereits vorhandenen, internen Computernetze verschiedener Forschungsinstitutionen miteinander verbunden. Dass diese heterogenen Netze und Topografien überhaupt miteinander Daten austauschen konnten, setzte die Entwicklung einheitlicher Verarbeitungsregeln, sogenannter Kommunikationsprotokolle voraus. Dies war die Geburtsstunde einer ganzen Protokollfamilie unter dem Oberbegriff ihrer beiden wichtigsten Vertreter: des Transmission Control Protocol (TCP) und des Internet Protocol (IP). Zu dieser Familie zählt ein gutes Dutzend weiterer Protokolle, darunter finden sich auch Prominenzen wie etwa das HTTP-, das FTP- oder das Telnet-Protokoll. Alle Angehörigen der TCP/IP-Protokollfamilie haben gemeinsam, dass sie von der physikalischen Realisierung des Datenverkehrs unabhängig sind. Mit anderen Worten: Für die Übermittlung von Information über elektrischen Strom, Lichtwellen, Funk oder Laser sind andere Protokolle zuständig, die nicht zur Familie von TCP/IP gehören. Es sind dies die Übertragungsprotokolle aus den beiden untersten Layern des OSI-Referenzmodells, die TCP/IP-Protokolle folgen basierend darauf erst auf Layer 3. Da die Schnittstellen für die reibungslose Zusammenarbeit zwischen den Layern jedoch genau definiert wurden, liegt der grosse Vorteil dieser Gliederung auf der Hand: Praktisch alle Arten von Übertragungsmedien können im Internet verwendet werden.

Eindeutige Navigation trotz Chaostopologie

Das Internet ist also ein einziges grosses Chaos, dessen Struktur man sich grob vereinfacht als ein weltweit verflochtenes Leitungssystem vorstellen kann. Seine Knoten- und Endpunkte bilden einzelne Computer, alleinstehend oder integriert in andere Geräte (Fahrzeuge usw.). Gemeinhin werden sie unterteilt in Router, Switches und Endsysteme, auch Hosts genannt. Während Router Knotenpunkte sind, die über eine seiner Schnittstellen eintreffende Daten nur entgegennehmen, um sie auf anderen Schnittstellen wieder weiterzuschicken, nehmen Endsysteme Daten zum eigenen Gebrauch über das Internet entgegen oder senden sie als verarbeiteten Payload ins Netz hinaus. Switches verbinden alle Endsysteme in einem Netzwerk. Verglichen mit der Welt der klassischen Telefonie haben Router/Switches den Stellenwert einer Vermittlungsanlage, Endsysteme hingegen denjenigen eines Telefons. Dank diesem Aufbau ist es möglich, dass von jedem beliebigen Endsystem aus Daten an jedes beliebige andere Endsystem im Netz gesendet werden können.

Voraussetzung ist jedoch, dass jedes Endsystem eine eigene Adresse besitzt, die es eindeutig als den richtigen Adressat identifiziert. Diese sogenannten IP-Adressen entsprechen den Telefonnummern in der Welt der Telefonie. Sie bestehen aus einer 32-Bit-Zahl, die nach dem Schema von «123.345.67.190» geschrieben wird. Da sich Benutzer solche Zahlen nur schwer merken könnten, erlaubt die TCP/IP-Protokollfamilie eine

Umschrift von IP-Adressen als Textadressen nach dem Schema «endpunkt.muster-organisation.ml». Dieser Verzeichnisdienst nennt sich Domain Name Services (DNS) und ordnet einen Namen der richtigen IP-Adresse zu. Ein Router hat zwei oder mehr Schnittstellen zum Verbinden unterschiedlicher Netzwerke. Die IP-Adresse ist unterteilt in eine Netzadresse (vorderer Teil) und eine Endpunktadresse (hinterer Teil) – ähnlich wie bei der Wohnadresse einer Person, welche die Strasse und die Hausnummer beinhaltet.

Router leiten die Datenpakete aufgrund konfigurierter oder aus dem Netz gelernter Regeln von einer Schnittstelle auf eine andere weiter. Router verbinden einerseits die unterschiedlichen Netzwerke der Internet Service Provider weltweit und andererseits firmeneigene Computernetze mit dem restlichen Internet. Diese lokalen Netze werden daher als Local Area Networks (LAN) bezeichnet, während die grossflächigen Bestandteile des Internets zur Familie der Wide Area Networks (WAN) gehören. Ein Router zwischen LAN und WAN ist somit in der Regel der Anschluss einer Firma (oder sonstigen Organisation) an das Internet. Oft werden LANs nicht speziell für das Internet aufgebaut, sondern man schliesst bereits existierende LANs an. Das Internet dehnt sich infolgedessen – gleichsam wie das virtuelle Abbild unseres Universums – unaufhörlich aus.

Der leistungsfähigste Paketdienst der Welt

Ob über Mobilfunk (z. B. UMTS), ADSL, LAN, WAN oder einen anderen Übertragungskanal: Wenn eine Nachricht im Internet von A nach B übertragen wird, kommt die TCP/IP-Protokollfamilie zum Einsatz. Die Daten werden dazu vom Rechner des Absenders in Blöcke variabler Länge, sogenannte Pakete, gepackt. Jedes Paket enthält neben den eigentlichen Daten die IP-Adressen von Sender und Empfänger sowie einige weitere Versandangaben. Anhand dieser Information entscheidet jeder Router, an welchen anderen Router oder an welches Endsystem er ein erhaltenes Paket weiterleitet. In der Regel wandert jedes Paket über mehrere Router an seinen Bestimmungsort. Welchen Weg das geroutete Paket einschlägt, hängt davon ab, wo sein Empfänger sitzt, wie sich die Kapazität und die Auslastung der möglichen Verbindungen zu anderen Routern zum Zeitpunkt seines Versands präsentieren und welche Konfigurationseinstellungen gewählt wurden (Vorgaben analog zu einem Navigationsgerät, welche Datenstrassen bevorzugt benutzt oder vermieden werden sollen). Dabei kommt es vor, dass einzelne Pakete etwa infolge Netzüberlastung verloren gehen oder absichtlich weggeworfen werden. Solche Verluste werden von TCP/IP jedoch registriert und wenn immer möglich durch eine erneute Übertragung der fehlenden Partien behoben. Hat der Zielrechner schliesslich alle Teilsendungen erhalten, setzt er die Pakete wieder zur ursprünglichen Information zusammen. Die Benutzer merken von diesen Vorgängen nichts – jene werden automatisch, still und unaufhörlich im Hintergrund von ihrer Software erledigt.

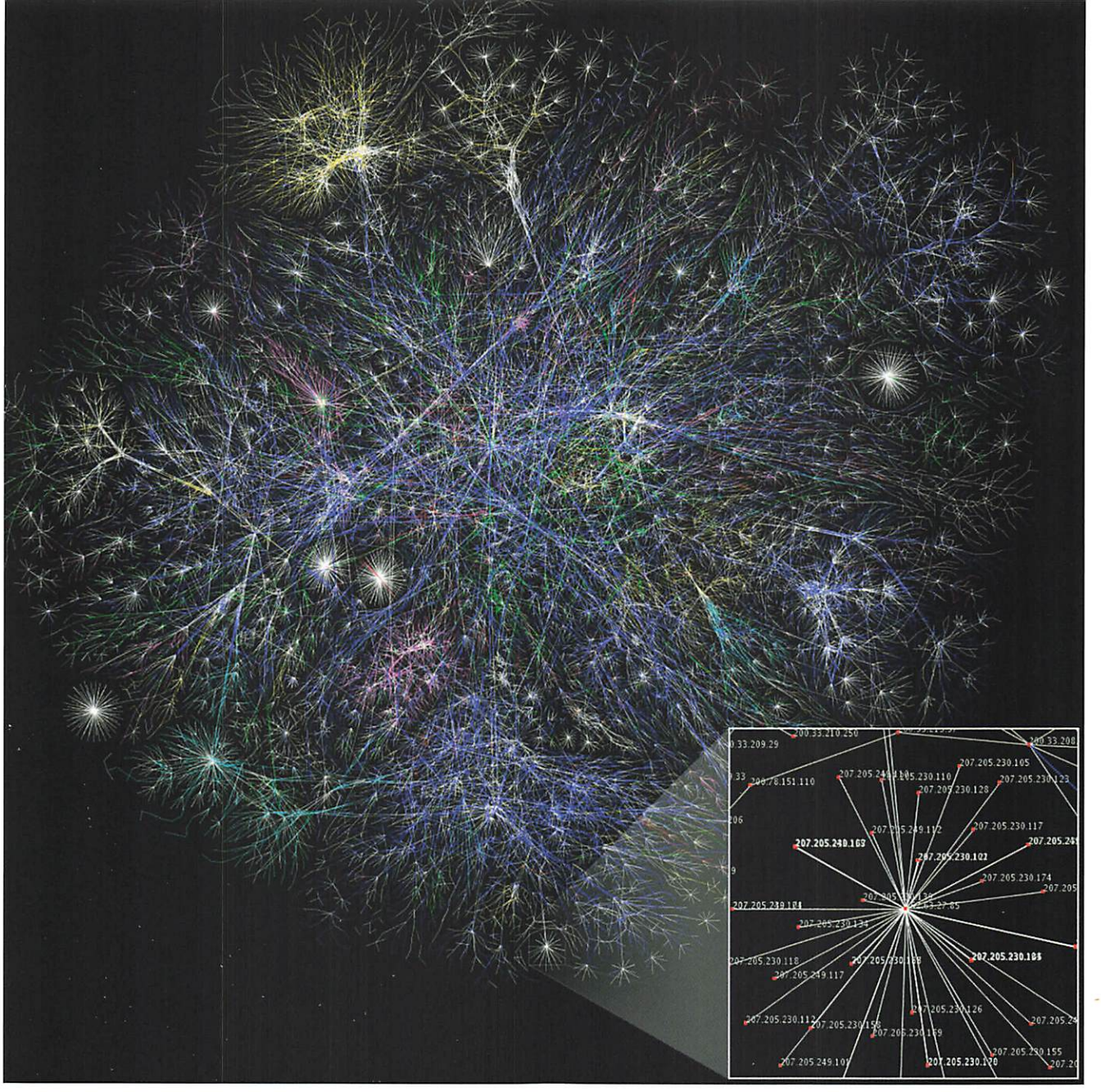
Sicherheit als späte Zutat

Genauso wenig wie das Internet selbst ist TCP/IP nicht über Nacht entstanden. Vielmehr wurden die Protokolle grösstenteils in den 1970er- und 1980er-Jahren geschrieben, als für die zahlreichen bereits existierenden Netzwerke im Laufe der Zeit eine gemeinsame Sprache entwickelt werden musste. Während TCP und IP noch relativ durchdacht waren, entstanden die Originalversionen der meisten anderen Protokolle meist als Produkt eines schnellen Hacks und wiesen dadurch zahlreiche Mängel auf, die sich erst nach und nach in der Praxis zeigten. Zu diesem Zeitpunkt waren jedoch bereits vollendete Tatsachen geschaffen worden: Die Protokolle wurden bereits von Millionen von Computern verwendet und konnten nicht mehr ohne Weiteres durch neue ersetzt werden, ohne ein babylonisches Sprachgewirr gewaltigen Ausmasses zu provozieren und damit den Zusammenbruch des Internets zu riskieren. Man entschied sich deshalb für den Weg sanfter Reparaturen statt für einen radikal neuen Wurf und lebt bis heute mit den Folgen: Neuere Versionen der Protokolle konnten zwar gewisse Mängel beheben, in ihren Grundzügen ist die TCP/IP-Familie jedoch noch gleich aufgestellt wie zu Anbeginn. Dies bestärkt leider den Verdacht, dass der Drang nach Kompatibilität und Netzerschliessung in der Computerfachwelt seit jeher grösser war als das Qualitätsbewusstsein. Die Kehrseite dieser Mentalität rächt sich heute mehr denn je, denn der grösste Qualitätsmangel von TCP/IP ist derjenige an Sicherheit. Als diese Protokolle entstanden, war die Welt freilich noch weit entfernt von der heutigen Realität mit ihren Hackern, Spionen, Internetkriminalität, Cyberterroristen und computerbasierter Kriegsführung. Damals war noch nicht vorhersehbar, dass das Internet spätestens um das Jahr 1995 zu einem sicherheitsrelevanten Massenmedium und bald zum vitalen Nerv ganzer Gesellschaften werden sollte, die sich seiner in allen Lebenslagen bedienen – angefangen vom e-Banking bis hin zur Steuerung kritischer nationaler Infrastrukturen.

TCP/IP bietet viele Angriffsflächen, die immer neue Attacken ermöglichen.

Die gängigsten Sicherheitsschwachstellen sind:

- Bei TCP/IP wird standardmässig nichts verschlüsselt, nicht einmal die Passwörter.
- Die Absenderadresse einer Information kann problemlos gefälscht werden (IP-Spoofing, Mail-Spoofing).
- Nachrichten, die sich Router zu Informationszwecken gegenseitig zuschicken, können gefälscht werden. Damit lässt sich ein Router fast nach Belieben manipulieren. Allerdings gibt es heute moderne Routingprotokolle, welche die Authentisierung unterstützen.
- Die Umwandlung von für Menschen leserlichen Endpunktadressen (Domain Names) in IP-Adressen kann vor allem



bei der Verwendung von älteren Versionen manipuliert werden (DNS-Spoofing). Neue Versionen verhindern dies.
- Viele Implementierungen von TCP/IP-Protokollen haben Schwachstellen und bieten spezielle Sicherheitslücken für versierte Angreifer.

Der Kampf um die Behebung dieser Sicherheitslücken und gegen immer neue Arten von Angriffen auf den weltweiten Datenaustausch per Internet dauert bis heute an. Da TCP/IP in der Zukunft eine noch tragendere Rolle zukommen wird, da alles – angefangen von der Lichtquelle bis zum Kraftwerk – ans Internet angeschlossen wird, kann die Bedeutung von Informationssicherheit im Netzverkehr nicht genug hervorgehoben werden. Dass das Sicherheitsrisiko schliesslich eines Tages in den Griff zu bekommen ist, halten Informatiker und Entwickler mit Verweis auf «Netzwerke der nächsten Generation» für möglich. Bis diese jedoch Wirklichkeit werden und den Tatbeweis antreten müssen, gilt es, die Nutzung der heute schon fast unbegrenzten Möglichkeiten des Internets mit grösstmöglichen Sicherheitsbemühungen zu kombinieren.

Trotz Sicherheitslücken lassen sich dank den TCP/IP-Protokollen sämtliche Knoten- und Endpunkte im Internetuniversum adressieren – ungeachtet seiner ungeheuren Komplexität.

Einige der Schwachstellen können durch die Migration von IPv4 auf IPv6 behoben werden. Letzteres wird in einer der nächsten Ausgaben des CryptoMagazines thematisiert werden.

Neue Architekturen – welchen Preis zahlen wir für «offene Netzkonzepte»?

Alles wird besser, jedoch nichts wird gut

Eine zukünftige Architektur für Kommunikationsnetze sollte auf dem aktuellen Erkenntnisstand der Softwareentwicklung und den bewährten Mechanismen des heutigen Internets basieren. Die Architekturen und Mechanismen dieser Netze sind allerdings nicht mit denen im klassischen Internet identisch. Dass solche Netze auf dem Internet und seinen Protokollen basieren, steht ausser Frage, aber diese Protokolle werden um spezielle Anforderungen erweitert, müssen sicherer und – gegenüber den heutigen – robuster werden. Eine nicht abschliessende Reihe wichtiger Forderungen an Kommunikationsnetze der Zukunft wäre:

- Wichtige Funktionen werden einmal im Netz bereitgestellt und sind für alle anfragenden Elemente gleich verwendbar (Wiederverwertbarkeit).
- Universelle Protokolle (internetbasiert) werden anstatt hoch spezialisierter Signalisierung genutzt.
- Die Unterstützung für eine einfache, integrierte Art der Einführung neuer Funktionen statt sogenannter Balkonarchitektur; denn heutige Netze unterstützen meist zu viele Dienste und Funktionen, für die sie nicht ausgelegt waren.
- Die Architektur muss eine tragfähige Basis für sehr grosse Netze mit einer hohen Verfügbarkeit und Sicherheit liefern.
- Das Netzmanagement muss flexibel genug für die Integration weiterer Funktionen sein. Es muss auf der anderen Seite eine hohe Grundsicherheit gegen potenzielle Angriffe gewährleisten.
- Die Zusammenarbeit mit bestehenden Systemen ist erforderlich, es muss sogar eine Integration von bestehenden Funktionen der herkömmlichen Netze möglich sein. Was immer neu entsteht, kann nicht schlagartig weltweit verfügbar sein und muss auf absehbare Zeit mit bestehenden Systemen zusammenarbeiten können (Rückwärtskompatibilität).

Potenziale und Risiken

Neue Architekturen könnte man als Flexible Universal Networks (FUN) bezeichnen, die offene Schnittstellen zur Verfügung stellen. Sie werden charakterisiert durch eine klare Objektorientierung. Objektorientierte Programmiersprachen zeigen bereits heute in vielen Anwendungen ihre Leistungsfähigkeit und Flexibilität gegenüber veränderten Aufgabestellungen. Als konsequente Weiterentwicklung werden sie die Basis der modernen Kommunikationssysteme und lösen damit Entwicklungsprinzipien aus dem Anfang der 1980er-Jahre ab, mit denen die Architekturen der hergebrachten Telekommunikation realisiert wurden. Statt aufwendige Spezialentwicklungen können frei verfügbare Standardlösungen (Datenbanken, verteilte Systeme, Speichernetze usw.) verwendet werden. Für die Netzbetreiber bedeutet dies keine Bindung an einen Hersteller und günstige Preise. Der grösste Vorteil dieser Architektur ist ihre Offenheit, doch die Erweiterbarkeit gegenüber zukünftigen Anwendungen stellt zugleich auch ihren grössten Schwachpunkt dar: Denn die Sicherheitsrisiken dürften mit offenen Netzkonzepten deutlich zunehmen.

Quelle

Gerd Siegmund: Einführung in die Telekommunikation, Heidelberg (2007)

UNSER ZIEL: IHRE HÖCHSTE INFORMATIONS-SICHERHEIT.

Kontinuität, Präzision, Vertrauen und Unabhängigkeit: Regierungen und Streitkräfte in mehr als 130 Ländern verlassen sich seit über 60 Jahren auf unsere Expertise in der Informationssicherheit. Vertrauen auch Sie auf unsere kundenspezifischen Lösungen zum Schutz Ihrer wertvollen Daten.

Crypto AG | 6301 Zug | Schweiz | www.crypto.ch

CRYPTO

Link-Chiffrierung: Einfach sicher

Das Internet-Protokoll und Ethernet sind die dominierenden Protokolle heutiger Kommunikationsnetzwerke – lokal, regional oder weltweit. Nicht nur, aber besonders auch bei Regierungsorganisationen mit eigenen Netzen kommen ausserdem häufig SDH und PDH für den Datenaustausch sowie Sprach- und Videokommunikation zum Einsatz. In diesen Fällen stellt sich jeweils die Frage, auf welcher Protokollschicht chiffriert werden soll.

Michael Lauffer | Product Manager

In der Welt der Kommunikationsnetzwerke wird häufig auf das OSI-Referenzmodell mit seinen sieben Schichten (Layers) verwiesen. Jeder Schicht sind entsprechende Aufgaben in ihrem Netzwerk zugeordnet, und für alle Aufgaben gibt es dedizierte Hardware oder Software, welche diese Funktionen übernehmen. Dabei kann es allerdings auch vorkommen, dass die Schichten bzw. ihre Funktionen überlappen oder anders aufgeteilt werden. Grundsätzlich hat jedoch das OSI-Modell nach wie vor seine Gültigkeit.

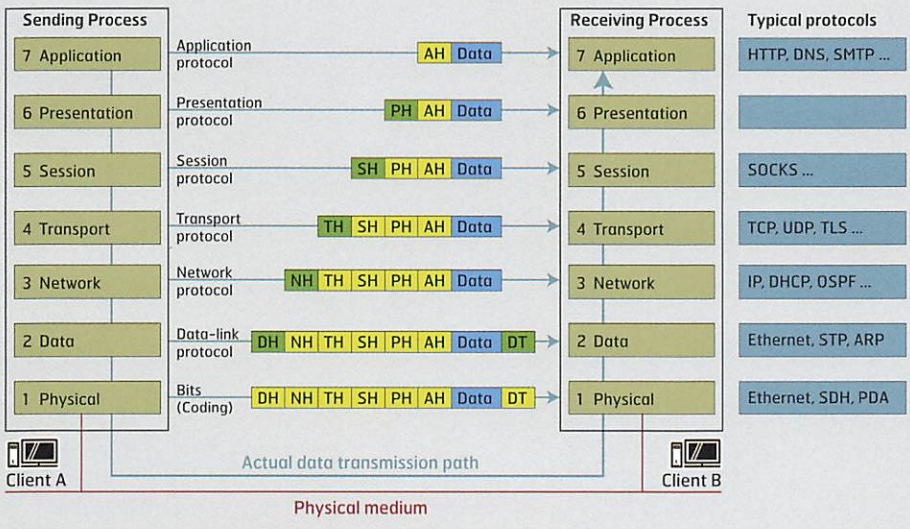
Heutzutage dominiert sicherlich der TCP/IP-Protokollstack (Transport Control Protocol / Internet Protocol) die Layer 3 und 4 sowie Ethernet die tieferen beiden Layer. Allerdings kommen oft noch weitere Protokolle wie SDH und PDH zum Einsatz – sei es für hohe Bandbreiten über Glasfaser im Core-Netzwerk oder auch für die Verbindung abgesetzter Standorte beispielsweise über Richtfunk. Die Crypto AG bietet Systeme, die eine Sicherung wertvoller Daten auf einer beliebigen Schicht ermöglichen. Welche nun jedoch die geeignetste ist, hängt von vielen Faktoren ab und ist nicht in jedem Fall einfach zu bestimmen.

Während IP-VPN-Chiffrierung vor allem in Fällen zum Einsatz kommt, in denen Daten über das öffentliche Internet transportiert werden und es somit besonders auch für die weltweite Vernetzung geeignet ist, sind die Einsatzgebiete von Layer-2- und Layer-1-Chiffriergeräten nicht immer so klar und einfach abzugrenzen. Für Ethernet-Netzwerke stellt sich diese Frage besonders, da hier verschiedene Ansätze möglich sind: Chiffrierung eines vermaschten Netzes als auch der einzelnen Punkt-zu-Punkt-Verbindungen (Links).

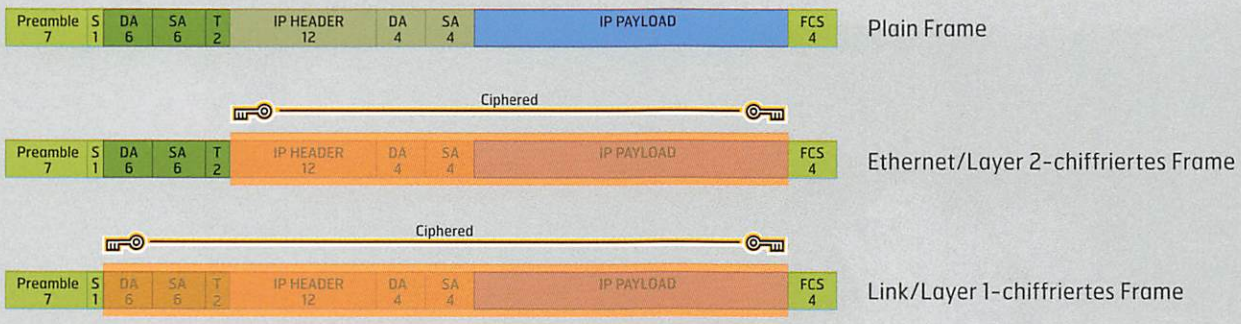
Doch betrachten wir erst einmal die Hauptunterschiede der Chiffrierung auf Layer 1, 2 oder 3. Ein wesentlicher Unterschied ist der Umfang der Daten, welche chiffriert werden bzw. werden können. Am besten lässt sich dies anhand eines gewöhnlichen Ethernet Frames mit IP als Payload erklären.

Bei einer Layer-1-(Link-)Chiffrierung wird beginnend mit der Ethernet-Zieladresse (Destination Address DA) der ganze Paketinhalt verschlüsselt. Die Frame Check Sequence (FCS) wird mit den chiffrierten Daten neu berechnet und am Ende des Paketes eingesetzt. Diese Chiffrierart ist also nur für Punkt-zu-Punkt-Verbindungen (Links) geeignet.

Im Gegensatz zu einer Layer-1-Chiffrierung ist die Layer-2-Chiffrierung für den Einsatz in vermaschten Ethernet-Netzwerken konzipiert. Dies bedeutet, dass der Ethernet Header unchiffriert bleiben muss, damit das Frame von einem Ethernet Switch verarbeitet werden kann. Auch bei einer Layer-3-Chiffrierung müssen die Adressinformationen, sprich der Header, zwecks Routing unchiffriert bleiben, allerdings



Das OSI-Referenzmodell geht auf die 1970er-Jahre Jahre zurück. Es schuf einheitliche Standards für die damals entstehenden unterschiedlichen Netzwerktechnologien, Protokolle und Konventionen.



wird hier das ursprüngliche IP-Paket vollständig chiffriert und in ein neues Paket mit eigenem Header verpackt. Dieses Verfahren wird auch «Tunnel Mode» genannt.

Damit können also auch chiffrierte Punkt-zu-Multipunkt (Star) und Multipunkt-zu-Multipunkt (Mesh) problemlos realisiert werden. Selbstverständlich können innerhalb des Crypto Ethernet- bzw. IP-VPN-Systems die verschiedenen Geräte unterschiedlicher Leistungsklasse miteinander kombiniert werden, sodass die Chiffrierleistung auf die verfügbare Bandbreite der entsprechenden Netzwerkabschnitte abgestimmt ist.

Damit sind Crypto Ethernet- und auch IP-VPN-Systeme universeller und flexibler als eine Link-Chiffrierung, insbesondere auch für all diejenigen Fälle, in denen die benötigte Kommunikationsbandbreite über einen gemieteten Service eingekauft werden muss (beispielsweise öffentliches Internet oder Ethernet Services).

Ist jedoch eine eigene Infrastruktur vorhanden oder kann ein Bittransparenter Service gemietet werden, bietet das Link-System einige Vorteile, welche in gewissen Szenarien entscheidend sein können. Einerseits betrifft dies die Performance und besonders auch die Verzögerung in der Verarbeitung: ein Link-Chiffriergerät kann sofort mit der Verarbeitung sprich Verschlüsselung der Daten beginnen, sobald diese an der Schnittstelle eintreffen, und muss nicht erst das ganze Frame einlesen. Damit kann die Latenz minimal gehalten werden und beträgt zum Beispiel bei der aktuellen Generation weniger als eine Mikrosekunde – eine Eigenschaft, die zusammen mit dem entsprechenden Systemverhalten wesentlich dazu beiträgt, dass sich ein Link-Chiffriergerät (fast) wie ein Lichtwellenleiter verhält.

Durch den relativ einfachen Verarbeitungsprozess bei der Link-Chiffrierung – im Gegensatz zu Layer 2 und 3 müssen die Daten nicht abhängig vom Empfänger unterschiedlich chiffriert werden – wird entscheidend weniger Rechenpower in Form von Hardware benötigt. Datenraten von 100 Gbit/s oder noch höher werden deshalb als Erstes auf Basis der Link-Technologie chiffriert werden können.

Da der ganze Datenstrom inklusive Header/Overhead chiffriert werden kann, kann ein potenzieller Angreifer aus übertragenen Netzwerkadressen keine Rückschlüsse auf die Topologie des Netzwerkes ziehen. Bei synchronen Protokollen wie SDH und PDH werden zudem auch leere Frames chiffriert, wodurch ein Angreifer nicht einmal feststellen kann, ob Nutzdaten transportiert werden oder nicht – eine Eigenschaft, die auch unter dem Begriff «Traffic-flow Security» bekannt ist.

Link-Verschlüsselung verhält sich gegenüber darüberliegenden Applikationen und Services vollkommen transparent und ist deshalb äusserst einfach zu installieren und zu konfigurieren (Bump-in-the-wire). Ist die Verschlüsselung einmal in Betrieb genommen worden, läuft diese in der Regel für die Lebensdauer des Links – auch über Jahre hinweg – unauffällig im Hintergrund. Änderungen an der Konfiguration sind selten nötig, womit die Betriebskosten auf einem Minimum gehalten werden können.

Vorteile Layer 1 Encryption
- Voll protokolltransparent
- Overhead wird mitverschlüsselt
- Höchste Performance
- Einfache Installation und Betrieb

Vorteile Layer 2 Encryption
- Für alle Netzwerktopologien geeignet
- Weniger benötigte Geräte für Star- und Mesh-Szenarios

Fazit: Die Auswahl der richtigen Verschlüsselung hängt nicht nur von der verwendeten Kommunikationstechnologie, sondern auch von ihrem Einsatzzweck ab. Je nach Anforderung der zu schützenden Applikation können Layer-1-Verschlüsselungsgeräte Vorteile gegenüber Layer-2- und Layer-3-Produkten haben – oder umgekehrt. Die Crypto AG bietet für alle Anforderungen das passende System, sodass weder bei der Performance und schon gar nicht bei der Sicherheit Kompromisse eingegangen werden müssen. Wenn die Verschlüsselung frühzeitig beim Netzwerk-Design miteinbezogen wird, kann sichergestellt werden, dass das Netzwerk schlussendlich sowohl die funktionalen Anforderungen als auch den notwendigen logischen Schutz bestmöglich erfüllt.

Hauptsitz

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

Regionale Büros

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

Seminare 2014

Professional Seminar for Information Security Specialists
5. bis 9. Mai | 29. September bis 3. Oktober

Professional Seminar on Technical Testing for Vulnerabilities
12. bis 16. Mai | 6. bis 10. Oktober

Professional Seminar on Contemporary Cryptography
19. bis 23. Mai | 13. bis 17. Oktober

Die Seminare finden in den Räumlichkeiten
der Crypto AG in Steinhausen (Schweiz) statt.

Kontakt und mehr Informationen
www.crypto.ch/de/produkte-und-dienstleistungen#seminare