

 CRYPTO

CRYPTO MAGAZINE

N° 2 | 2016



Hochsicherer Dokumentenaustausch
überall und jederzeit



Geschätzte Leserin, geschätzter Leser

Der mobile Zugriff auf Informationen in Form von elektronischen Daten ist für die heutige Gesellschaft Alltag. Diese globale Verfügbarkeit stellt Unternehmen und Behörden gleichermaßen vor grosse Herausforderungen – ein ganzheitlicher Ansatz für Informationssicherheitslösungen ist gefragt.

So hat sich die Methode der Klassifizierung von Informationen weltweit etabliert, um die Integrität und Vertraulichkeit von Dokumenten sicherzustellen. Peter Fischer, Delegierter des ISB, erklärt im Interview, wie die Schweizer Eidgenossenschaft mit diesem Thema umgeht.

Für das Speichern und den Versand von hochsensiblen Daten kommen symmetrische und asymmetrische Chiffriermethoden zum Einsatz. Wie diese funktionieren und ob sie durch Quantencomputer bedroht sind, erfahren Sie in dieser Ausgabe des CryptoMagazine.

Giuliano Otth

President and
Chief Executive Officer

Fokus

Von der Lochkarte zu modernen, hochsicheren Datenbanken

Seite 3

- 7 | Diplomatie in einer vernetzten Welt
- 11 | Schutz von hochsensiblen Daten – wichtiger denn je
- 14 | Interview mit Peter Fischer, Delegierter für die Informatikstrategie der Schweizerischen Eidgenossenschaft
- 16 | Sicheres Cloud-Computing – Tatsache oder Illusion?
- 20 | Quantenrechner: Der Supercomputer der Zukunft

Impressum

Erscheint 2-mal jährlich | **Auflage** | 6'200 (Deutsch, Englisch, Französisch, Spanisch, Russisch, Arabisch)

Herausgeber | Crypto AG, Postfach 460, 6301 Zug, Schweiz, www.crypto.ch

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

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

Bildnachweis | Crypto AG: S. 2 | illugraphic: S. 3 | Keystone: S. 11, 13 | Peter Fischer: S. 15 | Shutterstock: Titelseite, S. 3, 4, 7, 9, 15, 16, 18, 20, 21, 23



Von der Lochkarte zu modernen, hochsicheren Datenbanken

Das sichere Verwalten elektronischer Dokumente wird zu einer immer grösseren Herausforderung. Ein Grund dafür ist die Notwendigkeit, zu jeder Zeit und von überall her auf Datenbanken zugreifen zu können. Das wollen heute auch Ministerien, Nationalbanken und Armeen.

Selbst Grossmächte sind trotz scheinbar unbeschränkter Mittel nicht vor Schäden gefeit. Sogenannte «Enthüllungsplattformen» stellten in den letzten Jahren regelmässig Regierungen kleiner, aber auch grosser Staaten an den Pranger. Sie veröffentlichten streng vertrauliche Dokumente. Sogar Geheimdienstinformationen kamen auf diese Weise an die Öffentlichkeit. Die Skandale sind wegen des rasend schnell voranschreitenden Technologiewandels alles andere als ein Zufall. Und es herrscht Einigkeit darüber, dass mit den richtigen Methoden das Risiko solcher «Datenlecks» deutlich verringert werden kann.

Doch der Reihe nach. Der Schutz von Dokumenten beschäftigt die Menschen, seit es Dokumente gibt. Bereits die Siegel im Mittelalter und in der frühen Neuzeit aus Wachs und Lack dienten zur Beglaubigung von Urkunden. Ein Siegel konnte damals aber auch die Unversehrtheit eines Dokumentes belegen – wenn zum Beispiel ein Briefumschlag auf diese Weise verschlossen war.



Dann aber, als sich die physische zur digitalen Welt veränderte, nahm die Thematik eine völlig neue Dimension an. Ende der Sechziger- und zu Beginn der Siebzigerjahre des letzten Jahrhunderts entstanden die ersten elektronischen Datenbanken. Damit setzte eine Entwicklung ein, deren Ende sich noch nicht einmal richtig erahnen lässt.

Zwei Technologien kommen zusammen

Eine Voraussetzung für das Entstehen von Datenbanken war laut dem emeritierten Informatik-Professor der Eidgenössischen Technischen Hochschule (ETH) Carl August Zehnder, dass zwei technologische Entwicklungsstränge aufeinandertrafen: Durch die Kombination der immer besseren Rechenautomaten und der immer leistungsfähigeren Datenverarbeitung hätten Datenbanken erst entstehen können, schrieb Zehnder in einem Aufsatz.

Bei hochsensiblen Daten ist die Frage nach dem adäquaten Schutzniveau schnell beantwortet.

Die Datenverarbeitung hat ihre Wurzeln im 19. Jahrhundert. Mit sogenannten Lochkarten konnten zunächst Routinearbeiten maschinell erledigt werden, lochkartengesteuerte Webstühle sind ein Beispiel dafür. Bei der Volkszählung von 1890 in den USA kamen Lochkarten dann erstmals nicht als Steuerungselemente, sondern als Datenträger zum Einsatz. Die ersten Rechenmaschinen datieren aus der Zeit des Zweiten Weltkriegs. Als bekanntester Entwickler gilt der Deutsche Konrad Zuse. Sein vollautomatischer Z3 aus dem Jahr 1941 gilt als erster funktionstüchtiger Computer der Welt.

Ab den Sechzigerjahren näherten sich die Technologien der Rechenautomaten und Datenverarbeitung an. Damals wurde es laut Zehnder möglich, dass auf Grossrechnern mehrere Personen gleichzeitig arbeiteten. Die Datenbank als «computer-gestützte Einrichtung zum organisierten Speichern und Abrufen grosser Datenmengen durch mehrere Benutzer» – so Zehnders Definition – war erfunden.

Distanz spielt keine Rolle mehr

Die Computer wurden seither immer kleiner und leistungsfähiger. Und in den Neunzigerjahren begann eine neue Ära: Dank dem Internet spielte räumliche Distanz plötzlich keine Rolle mehr. Was als Austauschsystem zwischen einzelnen Universitäten seinen Anfang nahm, breitete sich rasend schnell über die ganze Welt aus. Heute will jede und jeder zu jeder Zeit auch unterwegs per Computer oder Smartphone im Internet surfen können.

Damit wird auch der Zugriff auf Datenbanken von unterwegs immer mehr zu einer Selbstverständlichkeit. Auch im Home-office, auf dem Arbeitsweg oder beim Kunden will der Nutzer auf die gewünschten Dokumente zugreifen und sie modifizieren können – und dies ohne Abstriche, was die Bedienung angeht. Parallel dazu werden Datenbanken immer komplexer. Aus einfachen Dokumentenarchiven werden Schlüsselemente für Geschäftsprozesse, die auch zur Qualitätssicherung und zur Einhaltung juristischer und finanzieller Vorgaben dienen.

Was ist das adäquate Schutzniveau?

Der Schutz der Daten ist dabei im Bewusstsein jedes Einzelnen angekommen. Doch es herrscht Einigkeit darüber, dass die meisten Alltagssysteme keine 100-prozentige Sicherheit bieten können. Zu viele Hard- und Software-Komponenten sind dafür im Spiel, und zu oft müssen einzelne Elemente ausgetauscht oder aufdatiert werden. Das häufige Auftauchen von Schadprogrammen ist ein Beleg dafür. Grenzen sind einem noch besseren Schutz oft auch durch den finanziellen Rahmen gesetzt: Unternehmen müssen sich daher die Frage stellen: Was ist das adäquate Schutzniveau?

Aus der früheren Kultur des «need to know» hat sich eine Kultur des «need to share» entwickelt.

Diese Frage stellt sich bei hochsensiblen Daten nicht, da ein höheres Schutzniveau automatisch gegeben ist. So müssen auf einem Aussenposten stationierte Diplomaten die Daten in die Zentrale übermitteln können, ohne dass jemand mitliest. Ebenso gilt dies für die obersten Mitglieder von Notenbanken. Sie müssen ebenfalls jederzeit und überall Zugriff auf ihre Datenbank haben, um gegebenenfalls intervenieren zu können. Auch Sicherheitssysteme von Atomkraftwerken oder grossen Staumauern gelten naturgemäss als hochsensibel.

Und das gilt nicht zuletzt für Armeen: In der modernen Kriegsführung ist der schnelle und sichere Zugang zu Informationsmaterial ein entscheidender Faktor. Aus der früheren Kultur des «need to know» hat sich eine Kultur des «need to share» entwickelt, sagen Experten. Der ungehinderte und gesicherte Informationsaustausch gilt somit als Schlüsselement für den Erfolg einer Operation. Vereinfacht gesagt: Ohne gut geschützte und stets zugängliche Datenbanken ist ein Krieg kaum mehr zu gewinnen.

Beim Schutz geht es dabei nicht nur darum, Datenbanken vor Eindringlingen zu sichern und damit Manipulationen zu verhindern. Ebenso wichtig ist der Schutz vor Sabotage. Dazu zählen Angriffe, die den Zugang zur Datenbank für die Nutzer erschweren oder für kurz oder lang sogar verunmöglichen. Zu Sabotage zählen ausserdem Angriffe, die auf die Zerstörung der Daten abzielen.

Software reicht nicht

Um hochsensible Daten adäquat zu schützen, genügt es oft nicht, sich beim Login und der Datenübermittlung auf Softwarelösungen zu verlassen. Vielmehr braucht es Hardware, die den Datenverkehr chiffriert, also mit individuellen Algorithmen verschlüsselt. Konkret geschieht dies zum Beispiel über Module, die in ein Notebook eingesteckt oder in ein Smartphone eingelegt werden. So wird das Abfragen, Bearbeiten und Versenden der Daten geschützt. Wichtig ist beim Arbeiten ausserhalb eines geschützten Netzwerks, dass auch lokale Speicherungen – zum Beispiel von E-Mails – geschützt werden. Umfassende Systeme tun dies.

Entscheidend für die Sicherheit des Gesamtsystems ist, dass sämtliche Zugänge zu einer Datenbank geschützt sind. Üblicherweise kann über das klassische Kupferkabel, aber auch das moderne Glasfasernetz zugegriffen werden. Dazu kommen im staatlichen Bereich auch Richtfunk- und Satellitenverbindungen, die vor allem in Krisenzeiten und in entlegenen Gebieten effizienter sind. Gerade Funktechnologie ist aber – sofern unzureichend geschützt – besonders anfällig für heimliches Anzapfen und Sabotage.

Und was bringt die Zukunft? Experten sind sich einig, dass der Schutz der Datenbanken zunehmend komplexer wird. Durch die weitere Digitalisierung der Gesellschaft und die Verbreitung des «Internet of Things», bei der immer häufiger auch Maschinen untereinander kommunizieren, sind weitere Angriffsszenarien denkbar. «Die technischen Entwicklungen im Bereich der Informatik werden weitergehen und uns allen noch erstaunliche neue Möglichkeiten eröffnen», blickt ETH-Informatikprofessor Carl August Zehnder in die Zukunft.

Diplomatie in einer vernetzten Welt

Erfolgreiche Aussenpolitik baut im 21. Jahrhundert auf sichere Information und Kommunikation. Neue Technologien haben den Akteuren weltweit Kommunikationskanäle eröffnet, die machtvolle Instrumente sein können. Insbesondere auch für Diplomaten. So findet ihre Tätigkeit vermehrt auch in der digitalen Öffentlichkeit statt. Gleichwohl gilt es, die Geheimhaltung als begrenzender Faktor für komplexe Verhandlungen aufrechtzuerhalten – unabhängig davon, welche Kommunikationstechnologien zum Einsatz kommen.

Das Hashtag (#) ist aus der digitalen Welt nicht mehr wegzudenken. Seit 2007 damit begonnen wurde, das Rautenzeichen zur Verschlagwortung von Begriffen zu nutzen, hat seine Verwendung millionenfach zugenommen. Auch in der Botschaftskommunikation. «Waren Sie je in #Genf?», fragte die Schweizer Botschaft in den USA neulich ihre Follower auf dem Kurznachrichtendienst Twitter. Anlass für den Tweet war eine TV-Reportage über die Schweizer Stadt Genf, die weltweit bekannt ist als Hauptsitz internationaler Organisationen,

und ihre multikulturelle Bevölkerung. Derartige Hinweise, aber auch für eine breite Öffentlichkeit bestimmte Event-Empfehlungen sind gemäss dem Schweizer Aussenministerium im digitalen Zeitalter geeignete Mittel, um ein frisches Image der Schweiz zu vermitteln und neue Netzwerke zu erschliessen.

Die ersten Gehversuche der Eidgenossenschaft auf dem Parkett der E-Diplomatie gehen zurück ins Jahr 2012. Im Rahmen eines Pilotprojektes begannen zehn Schweizer Vertretungen im



Ausland, den Umgang mit sozialen Medien zu erproben. Seinerzeit beschränkten sich die Aktivitäten auf maximal drei Meldungen täglich auf der Facebook-Seite und dem Twitter-Kanal. Vier Jahre später hat sich das Volumen vervielfacht und die Reichweite wurde markant gesteigert. Heute verfolgen über 2'500 Personen, was das Schweizer Botschaftspersonal in Washington (USA) auf dem Twitter-Kanal mitteilt, 50'000 sind es bei Facebook. Die sozialen Medien werden mittlerweile als wichtiges Werkzeug diplomatischer Arbeit bezeichnet.

Digital oder konventionell – der sichere und vertrauliche Informationsaustausch muss jederzeit sichergestellt sein, unabhängig von den eingesetzten Kommunikationsmitteln.

Diplomatie im digitalen Zeitalter

Als Instrument der «public diplomacy» werden neue Technologien genutzt, um eine wachsende und sich wandelnde Gemeinde von Akteuren überall auf der Welt einzubinden, mit dem Ziel, Beziehungen aufzubauen. Dabei gilt es, die Bedürfnisse und Besonderheiten anderer Staaten, Kulturen und Menschen zu verstehen, die eigenen Standpunkte zu kommunizieren und Korrekturen vorzunehmen bei falschen Vorstellungen sowie Regierungspropaganda aktiv entgegenzuwirken. Während sich die klassische Diplomatie auf die Beziehung zwischen Staaten auf formeller Ebene konzentrierte, hat die Zahl relevanter Akteure im diplomatischen Spiel des 21. Jahrhunderts markant zugenommen. Dazu gehören Nichtregierungsorganisationen, kulturelle und akademische Vermittler, Konzerne, Lobbyisten, Medien und neu insbesondere auch die jeweilige Bevölkerung vor Ort. Deren Wahrnehmung beziehungsweise Meinung soll durch gezielte Ausschöpfung der Möglichkeiten der digitalen Diplomatie im eigenen Interesse beeinflusst werden.

Der Wandel im diplomatischen Dienst, der mit der Digitalisierung eingesetzt und dessen Ende nicht absehbar ist, hat bisher dazu geführt, dass die rechtlichen und politischen Funktionen von Diplomaten an Gewicht eingebüsst, symbolische Funktionen in Form von «public diplomacy» hingegen an Bedeutung zugenommen haben. Der Botschafter ist auf allen Kanälen präsent, hält Vorträge, gibt Interviews und erklärt der Öffentlichkeit im Gastland die Politik des eigenen Landes.

Der verstärkte Einsatz von sozialen Medien als Instrument der E-Diplomatie ist aber auch mit Risiken verbunden und erfordert dementsprechend gewisse Richtlinien. Andernfalls kann es zu einem Online-Schlagabtausch zwischen Regierungsvertretern kommen, die beidseitig kontraproduktiv wirken, weil sie für Negativschlagzeilen sorgen können. Und nach wie vor gilt, worauf verschiedene E-Diplomatie-Experten hinweisen: Zum erfolgreichen Abschluss einer internationalen Vereinbarung kann man sich (noch) nicht twittern.

Technologie beschleunigt Tempo in der Diplomatie

Der technologische Fortschritt hat nicht nur den Trend hin zu einer «digital diplomacy» insbesondere in der Öffentlichkeitsarbeit beschleunigt, sondern auch das Tempo in der Diplomatie insgesamt erhöht. Ermöglicht wurde diese Entwicklung durch die fast flächendeckende Ergänzung oder gar Ablösung von analogen leitungsgebundenen Kommunikationskanälen – wie das Telefonnetz, auch als PSTN bekannt – durch schnelle digitale, paketerorientierte Kommunikationskanäle, welche vermehrt auch drahtlos, also funkbasiert sind. In Krisenzeiten hingegen besteht die Gefahr, dass diese lokal vorhandenen terrestrischen Netze wie das PSTN, das Internet oder 3G- bzw. 4G-Mobilfunknetze gestört werden können oder temporär ausfallen. Gewisse Botschaften benutzen deshalb zusätzlich oder als Back-up Kurzwellenfunk und/oder VSAT-Satelliten, um die Kommunikation unabhängig von lokalen Netzwerken sicherstellen zu können.

Heute setzen Botschaften und Missionen der Aussenministerien anstelle des Kurzwellenfunks, der mit erheblichen Infrastruktur-Investitionen verbunden ist und zudem nur langsame und nur bedingt digitalisierte Kommunikation zulässt, vermehrt auf Breitband-Satellitenkommunikation wie Inmarsat BGAN, Global Xpress oder Thuraya IP. Diese ist deutlich günstiger geworden und global verfügbar, sowohl stationär wie auch für unterwegs, und erfüllt somit die Ansprüche, welche in einer weltweit mobilen und vernetzten Gesellschaft an heutige digitale Kommunikationstechnologien gestellt werden.

Vor dem Hintergrund der rasant fortschreitenden Digitalisierung und Vernetzung, der intensivierten Nutzung neuer Kommunikationsmittel sowie der Forderung nach mehr Transparenz gilt es aber auch für die Diplomatie im 21. Jahrhundert, die relative Geheimhaltung als begrenzender Faktor für komplexe Verhandlungen aufrechtzuerhalten. Insofern steht Geheimhaltung als gängige Münze der Diplomatie höher im Kurs denn je. Denn: Digital oder konventionell – der sichere und vertrauliche Informationsaustausch muss sichergestellt sein, unabhängig von den eingesetzten Kommunikationsmitteln.



Auch wenn die Diplomaten-tätigkeit vermehrt im Bereich «public diplomacy» angesiedelt ist, die klassischen Einsatzgebiete der Diplomatie bleiben aktuell. Zum Beispiel die Koordination eines Gefangenenaustausches zwischen zwei Ländern, die keine diplomatischen Beziehungen unterhalten – also über keine Kommunikationswege verfügen – und deshalb auf die Vermittlungsdienste eines Drittstaats angewiesen sind.

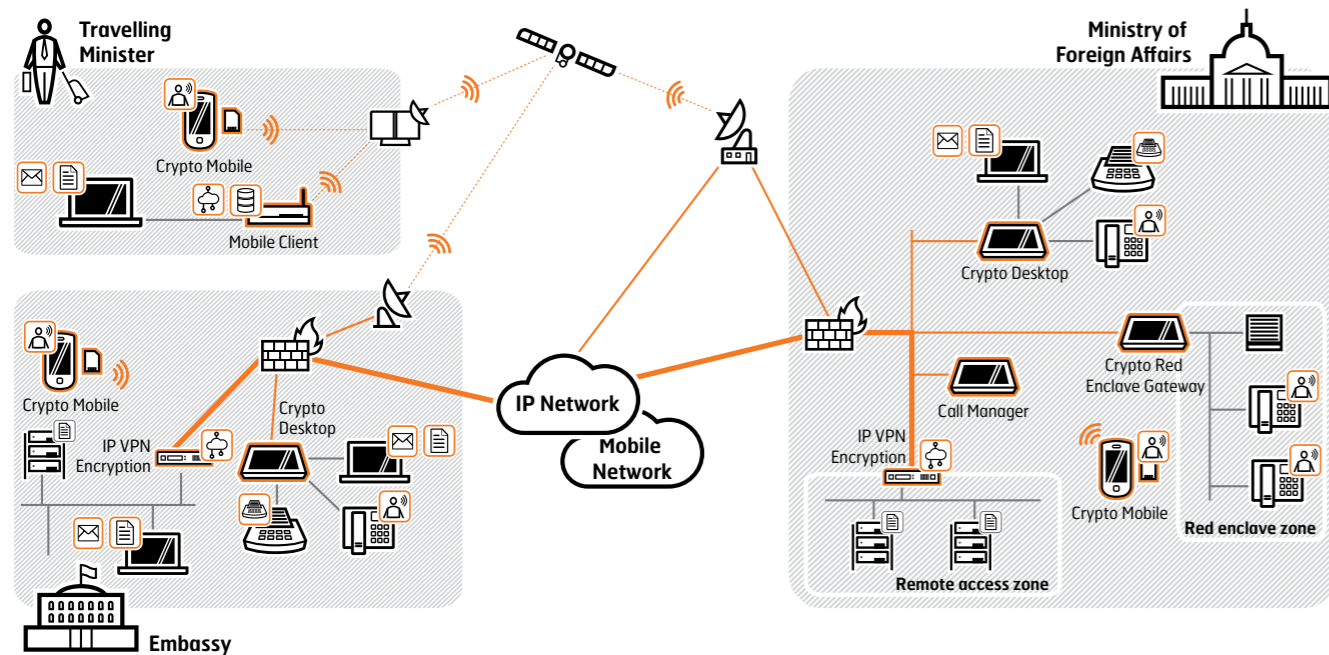
Komplizierte Dreiecksbeziehung

Der vermittelnde Staat hat in einer solchen Konstellation die Aufgabe, sämtliche Details zum Tauschhandel mit beiden Seiten abzustimmen: Von den Verhandlungspositionen der Parteien über die Dokumentation der Zwischenergebnisse bis hin zum Ablauf des Transfers laufen alle Koordinationsarbeiten über den Vermittler. Ein solches Unterfangen erfordert hohe Sicherheitsstandards bei der Kommunikation, denn keiner der beiden Parteien darf es gelingen, Einblick in die Korrespondenz oder die Entscheide der Gegenseite zu bekommen. Hinzu kommt, dass auch die Öffentlichkeit in keinem der beteiligten Länder etwas mitbekommen darf.

Der Vermittler muss deshalb für alle Formen der Korrespondenz eine Verschlüsselungstechnologie verwenden. Benutzen alle Mitarbeiter einen solchen Algorithmus zum Transport von geheimen Nachrichten, ist es keinem der Staaten möglich, die Inhalte ausserhalb der «offiziellen» Kommunikation zu erfahren.

«Kommunikation bleibt in der Diplomatie das zentrale Element. Und deren Schutz muss jederzeit garantiert sein, unabhängig davon, welche Technologien zum Einsatz kommen.»

Doch nicht alles, was an Informationen zwischen den Vertragsparteien über die Vermittlernation hin- und hergeschickt wird, unterliegt der gleichen Geheimhaltung. Damit nicht jede Nachricht verschlüsselt werden muss, lohnt es sich, Mitteilungen nach unterschiedlichen Vertraulichkeitsgraden zu klassifizieren und eine kodierte Übertragung entsprechend den Geheimhaltungsstufen vorzunehmen – wie dies seit den Anfängen der diplomatischen Kommunikation praktiziert wird. Ein ehemaliger Schweizer Top-Diplomat hat den Wandel in der Diplomatie so zusammengefasst: «Kommunikation bleibt in der Diplomatie das zentrale Element. Und deren Schutz muss jederzeit garantiert sein, unabhängig davon, welche Technologien zum Einsatz kommen.»



Schutz von hochsensiblen Daten – wichtiger denn je

Informationen sind oft so sensibel, dass ihr Bekanntwerden enorme Risiken mit sich bringt – für staatliches Handeln, für die nationale Sicherheit, für Unternehmen. Das Speichern, Bearbeiten und Übertragen digitaler Dokumente erfordert deshalb einen ganzheitlichen Ansatz.

Informationssicherheit für die Office-Kommunikation

Die schriftliche Kommunikation hat in der Diplomatie aus verschiedenen Gründen einen hohen Stellenwert: schriftliche Verbindlichkeit, Archivierbarkeit und die Überbrückung von Zeitzeonen. Fax und/oder E-Mail sind daher wichtige Anwendungen, aber auch die Telefonie ist im operativen Einsatz sehr wichtig. Die End-user-Produkte der Crypto AG für Voice, Fax, Messaging und Remote Access sind bestens geeignet, um diese Kommunikationsarten mit höchster Informationssicherheit zu schützen.

Die Plattform Crypto Desktop HC-9300 ermöglicht mit den End-user-Applikationen eine hochsichere Botschaftskommunikation. Faxnachrichten können nicht nur über klassische PSTN-Netzwerke, sondern verschlüsselt auch als E-Mail übermittelt werden. E-Mail-, Daten- und VoIP-Telefoniever-schlüsselung runden das Produkt als Bürosicherheitslösung ab. Bei Bedarf nach mehr Mobilität bietet das Deployable Secure Mobile Office DSSS-1031 mit integriertem HC-9300 ein betriebsbereites mobiles Büro mit allen notwendigen Komponenten und Kommunikationsmitteln.

Das Secure Mobile Phone mit dem Crypto Mobile HC-9100 ist das mobile Mitglied des Crypto Secure VoIP-Systems. Es nutzt zur Kommunikation Paketdatendienste von Mobilnetzwerken, mittels WiFi aber auch andere IP-Netzwerke. Wird zusätzlich ein mobiles Satelliten-Terminal wie beispielsweise das Inmarsat BGAN Terminal iSavi verwendet, kann zusätzlich via Satcom auf das Kommunikationsnetz zugegriffen werden.

Der Crypto Mobile Client HC-7835 ermöglicht Reisenden des diplomatischen Dienstes Remote Access auf die zentrale ICT-Infrastruktur. Diese Plattform ist für Benutzer unterwegs das perfekte Werkzeug, um die Daten verschiedenster ICT-Applikationen lokal oder mittels VPN-Verschlüsselung für die Übermittlung zu schützen. Auch mit dem Mobile Client gibt es mit dem Deployable Secure Mobile Office DSSS-102x ein betriebsbereites mobiles Bürosystem.



Crypto Desktop HC-9300

Die Chiffrierplattform für das moderne Büro. Individuelle Sicherheitsanwendungen sorgen für höchste Sicherheit bei Sprach-, Fax- und Datenübermittlung.



Crypto Mobile HC-9100

Das Crypto Mobile HC-9100 ist eine vollständige, universelle Chiffrierplattform mit beeindruckender Leistungsfähigkeit im Format einer Micro-SD-Card.



Crypto Mobile Client HC-7835

Diese Plattform ist für Benutzer unterwegs das perfekte Werkzeug, um die Daten mittels Verschlüsselung für die Übermittlung und das Speichern zu schützen.

Sie war revolutionär und sie galt als nicht zu knacken – die Verschlüsselungsmaschine Enigma. Die deutsche Wehrmacht verwendete das Gerät im Zweiten Weltkrieg, um ihre Kommunikation zu chiffrieren. Lange mit Erfolg. Mit einem riesigen technischen und personellen Aufwand schafften es die Alliierten dennoch, den Code zu entschlüsseln. Plötzlich hatten die Militärs und Nachrichtendienste Einblick in die chiffrierten Funksprüche. Dies war entscheidend für den Sieg der Alliierten. Historiker sind sich einig: Die nachrichtendienstlichen Erkenntnisse durch das Kompromittieren von Enigma verkürzten den Krieg um Jahre und retteten vermutlich Millionen Menschenleben.

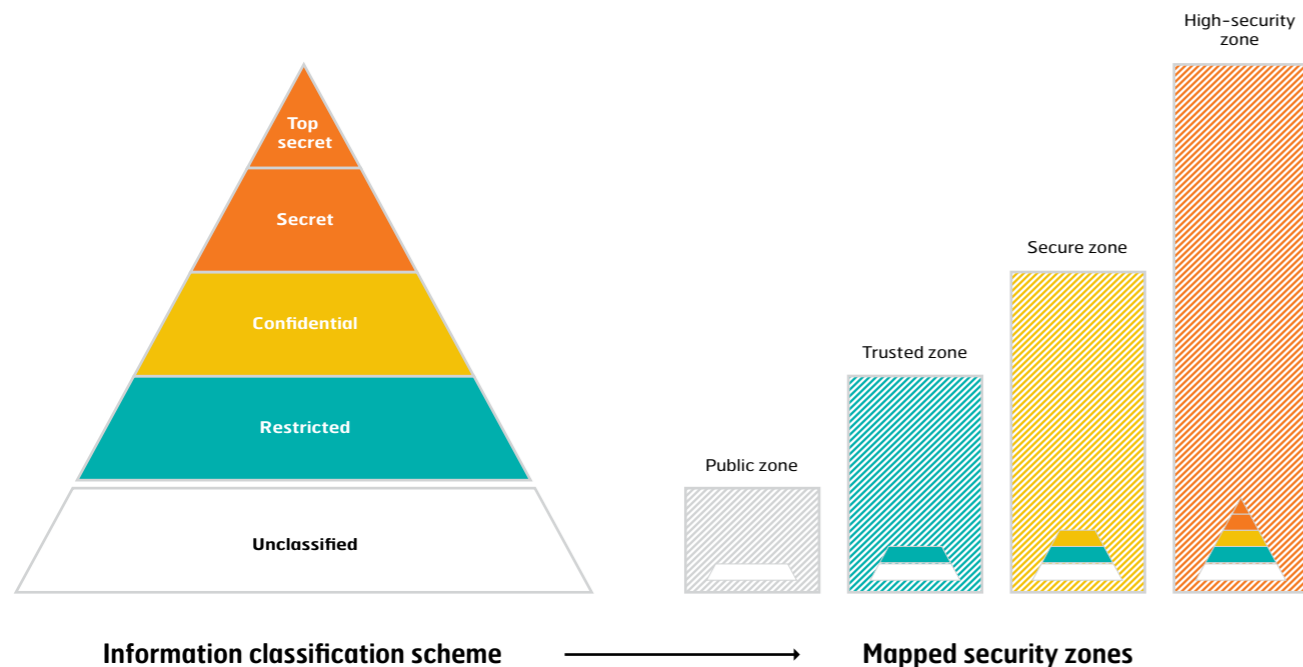
Die Verschlüsselung geheimer Informationen spielt bis heute eine Schlüsselrolle zum Schutz vor unberechtigtem Zugriff und Manipulation. Das Chiffrieren von Daten bedeutet, sie so zu verändern, dass ihr Inhalt nicht mehr erkenntlich ist. Klartext wird in Geheimtext umgewandelt.

Der Begriff «Text» ist jedoch überholt. Enigma chiffrierte zwar noch ausschliesslich Buchstaben, Verschlüsselungssysteme des 21. Jahrhunderts speichern und übermitteln Daten hingegen fast ausschliesslich in digitaler Form. Dies umfasst Textdokumente und Daten-Files ebenso wie Sprache, Videos, E-Mails, Programmcodes, Fax oder Telefonate.

Der Vorteil der Chiffrierung: Selbst wenn Unbefugte Daten abgreifen, bleiben deren Inhalte vertraulich. Moderne Verschlüsselungstechniken beruhen auf so komplexen mathematischen Prozessen, dass das Rekonstruieren des Klartextes – selbst mit Zuhilfenahme der schnellsten Computer der Welt – unzählige Jahre dauern würde.

Chiffriert bis zum Empfänger

Das Chiffrieren der Informationen stellt nur eine Seite eines ICT-Sicherheitssystems dar. Entscheidend ist, dass alle berechtigten Nutzer wieder Zugang zu den sensiblen Daten haben. Das Ziel eines hochsicheren Dokumentenmanagements: Die Dokumente bleiben chiffriert, bis sie der Endnutzer auf seinem Gerät abrufen. Nur der berechtigte Empfänger kann die Informationen entschlüsseln. Fängt eine dritte Person die geheimen Daten unterwegs ab, kann er mit ihnen nichts anfangen.



Regierungsorganisationen unterhalten ein Klassifikationsschema zur Schwärze ihrer Information. Klassifizierte Information wird vielfach nach dem 4-Stufenmodell eingereiht. Jegliche Information, die nicht in eine dieser Klassifikationsstufen eingereiht ist, wird als «unclassified» betrachtet. Die verschiedenen Klassen von Information und informationsverarbeitender Infrastruktur werden ihren Sicherheitszonen zugewiesen.

Bei dieser End-zu-End-Verschlüsselung kommen Schlüssel zum Einsatz, die durchaus mit Türschlüsseln vergleichbar sind, die man aus dem Alltag kennt: Mit dem Schlüssel verschliesst man den Zugang zum Dateninhalt, und der Endnutzer braucht wiederum einen Schlüssel, um Zugriff zu den Informationen zu erhalten.

Für das Speichern und Senden hochsensibler Dokumente wird die Methode der symmetrischen Verschlüsselung angewendet. Bei dieser nutzen alle Kommunikationspartner denselben geheimen Schlüssel – mit diesem wird die Information beim Sender chiffriert und beim Empfänger dechiffriert. Ein grosser Vorteil dieses Verfahrens ist zudem: Selbst Dokumente mit grossen Datenmengen lassen sich auf diese Weise rasch verschlüsseln und übermitteln.

Der hochsichere Umgang mit Dokumenten verlangt eine ganzheitliche Architektur.

Bei asymmetrischen Kryptoverfahren nutzen die Beteiligten hingegen ein mathematisch kreierte Schlüsselpaar: Einer dieser Schlüssel ist öffentlich erhältlich – beispielsweise im Internet und über authentifizierte Kanäle abrufbar – und ermöglicht es, Daten so zu chiffrieren, dass sie nur mit dem passenden privaten Schlüssel entziffert werden können. Die asymmetrische Verschlüsselung ist jedoch langsam, sie eignet sich nur für kleine Datenmengen. Deshalb kommen auch hybride Kryptoverfahren zum Einsatz: Eine Kombination aus symmetrischer und asymmetrischer Verschlüsselung, die die Vorteile der jeweiligen Methode nutzt. Angewendet wird hybride Chiffrierung zum Beispiel beim E-Banking, bei



Bezahlssystemen im Internet oder bei gesichertem E-Mail-Verkehr. Mehr zu diesen beiden Methoden erfahren Sie im Artikel «Quantenrechner: Der Supercomputer der Zukunft» auf Seite 20.

Ganzheitlicher Sicherheitsansatz

Je sensibler Daten sind, desto besser müssen ihre Integrität und Vertraulichkeit geschützt werden. Angriffsmöglichkeiten gibt es viele: Informationen können an ihrem Speicherort abgegriffen werden oder während ihrer Übermittlung über einen verdeckten Kanal; Schlüssel können geklaut, manipuliert und missbraucht werden; es besteht zudem das Risiko, dass Personen ohne Zugriffsrecht an klassifizierte Dokumente gelangen. Die geheimen Datenströme verlaufen über unterschiedliche Medien: Kabel, Glasfaser, Satelliten, Funknetzwerke oder Mikrowellen.

Die vertraulichen Informationen bewegen sich dabei nicht nur über vertrauenswürdige Pfade. Innerhalb kleinerer Arbeitsnetzwerke sind die Übertragungswege meist noch übersichtlich und sicher. Bei grossen Netzwerken sind die Kommunikationspartner räumlich oft weit entfernt und die Datenübermittlung läuft über nicht vertrauenswürdige Wege wie das Internet – damit steigt die Herausforderung an die Sicherheitsmassnahmen.

Die sichere Übertragung hochsensibler Dokumente ist zwar mit einem entsprechend höheren technischen Aufwand verbunden, doch er zahlt sich aus: Der Verlust von Dokumenten höchster Geheimstufe stellt für einen Staat oder ein Unternehmen ein oft schweres Risiko dar. Gleiches gilt für die Kompromittierung von Dateien. Deren Wiederherstellung beziehungsweise die Einrichtung eines neuen Sicherheitssystems ist mit einem Arbeitsaufwand und mit Kosten verbunden, die rasch die Betriebskosten der ursprünglichen Sicherheitsmassnahmen übersteigen.

Aufgrund der vielfältigen Risiken und Datenübertragungswege muss der hochsichere Umgang mit Dokumenten breit aufgestellt sein, was eine ganzheitliche Architektur verlangt. Neben technischen Massnahmen und Kryptoverfahren erfordert dies auch organisatorische Massnahmen, wie geordnete Rechtevergabe für den Zugriff. Die zu schützenden Daten werden gemäss dem Grad ihrer Vertraulichkeit klassifiziert und in Sicherheitszonen eingeteilt, zu denen nur befugte Personen Zugriffsrecht besitzen. So werden beispielsweise Daten der Sicherheitsklassifizierung «geheim» in Hochsicherheitszonen verarbeitet, zu denen nur eine Gruppe mit wenigen Personen Zugriff hat. Oder Daten der Stufe «restricted» werden in Sicherheitszonen tieferen Schutzgrades verarbeitet, zu denen wesentlich mehr Personen Zugriff haben.

Innerhalb dieser Zonen können Nutzer die geschützten Dokumente sicher lesen, bearbeiten und wieder abspeichern. Zwischen den Zonen werden technische Schutzwälle wie Gateways aller Art errichtet, die den Datenfluss kontrollieren und wenn nötig unterbinden. Denn die Übergänge zwischen den einzelnen Schutzzonen sind meist die grösste Schwachstelle eines Sicherheitssystems – hier finden Angreifer die Brechen, durch die sie eindringen können.

Daten, deren Vertraulichkeit und Integrität allerhöchsten Sicherheitsansprüchen genügen müssen, werden deshalb sogar physisch von den anderen Zonen und dem Internet getrennt. Dies schränkt zwar die Zugriffsmöglichkeiten drastisch ein, aber ebenso die Chancen auf Datenklau.

«Je höher der Schutzgrad, desto höher auch der Grad der Personensicherheitsprüfung»

Das Informatiksteuerungsorgan des Bundes (ISB) sorgt für die Umsetzung der Strategie zur Informations- und Kommunikationstechnik (IKT) in der Bundesverwaltung. Es erlässt hierzu Vorgaben für die Verwaltungseinheiten und führt die IKT-Standarddienste. Das ISB hat zudem die Leitung der Geschäftsstelle E-Government Schweiz sowie der Melde- und Analysestelle Informationssicherung (MELANI) inne.

Herr Fischer, was bedeutet Klassifizierung sensibler Daten und welchen Nutzen hat sie?

Darunter versteht man, dass Daten nach deren Schutzwürdigkeit eingestuft werden. Zuständig für die betreffenden Vorgaben ist in der Schweiz die Abteilung Informations- und Objektsicherheit im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS). Mit der Klassifizierung wird Schutzwürdiges von weniger Schutzwürdigem unterschieden. Darauf gestützt können gezielte vorbeugende Massnahmen getroffen werden, um schutzwürdige Informationen vor der Kenntnisnahme durch Unbefugte zu bewahren.

Welche Geheimhaltungsstufen kommen beim Bund zur Anwendung? Und: Bestehen Unterschiede zum Ausland?

In der Schweiz wird folgendermassen klassifiziert: INTERN, VERTRAULICH und GEHEIM. Andere Länder wie zum Beispiel Deutschland kennen noch zusätzlich die Stufe STRENG GEHEIM.

Klassifizieren bedeutet auch, Zugriffsrechte zu vergeben. Nach welchen Kriterien werden diese verteilt?

Grundsätzlich sollten diejenigen Personen Zugang zu einem Dokument haben, die es für die Wahrnehmung ihrer Aufgabe benötigen. Sie müssen aber je nach Klassifikationsstufe bestimmte Bedingungen einschliesslich der nötigen Auswahl und Ausbildung erfüllen. Je höher der Schutzgrad, desto höher zum Beispiel auch der Grad der Personensicherheitsprüfung.

Früher wurden geheime Schriftstücke mit einem entsprechenden Stempel markiert. Wie wird bei digitalen Dokumenten deren Geheimhaltungsgrad erkenntlich gemacht?

Klassifizierungsvermerke VERTRAULICH und GEHEIM werden auf jeder Seite jeweils oben angebracht und das Dokument verschlüsselt.

Identifikation beim Zugriff: Wie stellt man sicher, dass die Person, die auf klassifizierte Dokumente zugreifen will, tatsächlich die berechnigte Person ist?

Durch entsprechende Berechtigungskonzepte und Zugriffssysteme, die eine sichere Identifikation erlauben. Die klassifizierten Informationen sollen gemäss dem Grundsatz «Kenntnis nur, wenn unbedingt nötig» nur jenen Personen zugänglich gemacht werden, welche diese auch tatsächlich benötigen.

Welche Formen klassifizierter Informationen sind verbreitet?

Primär Text, Grafik und E-Mail.

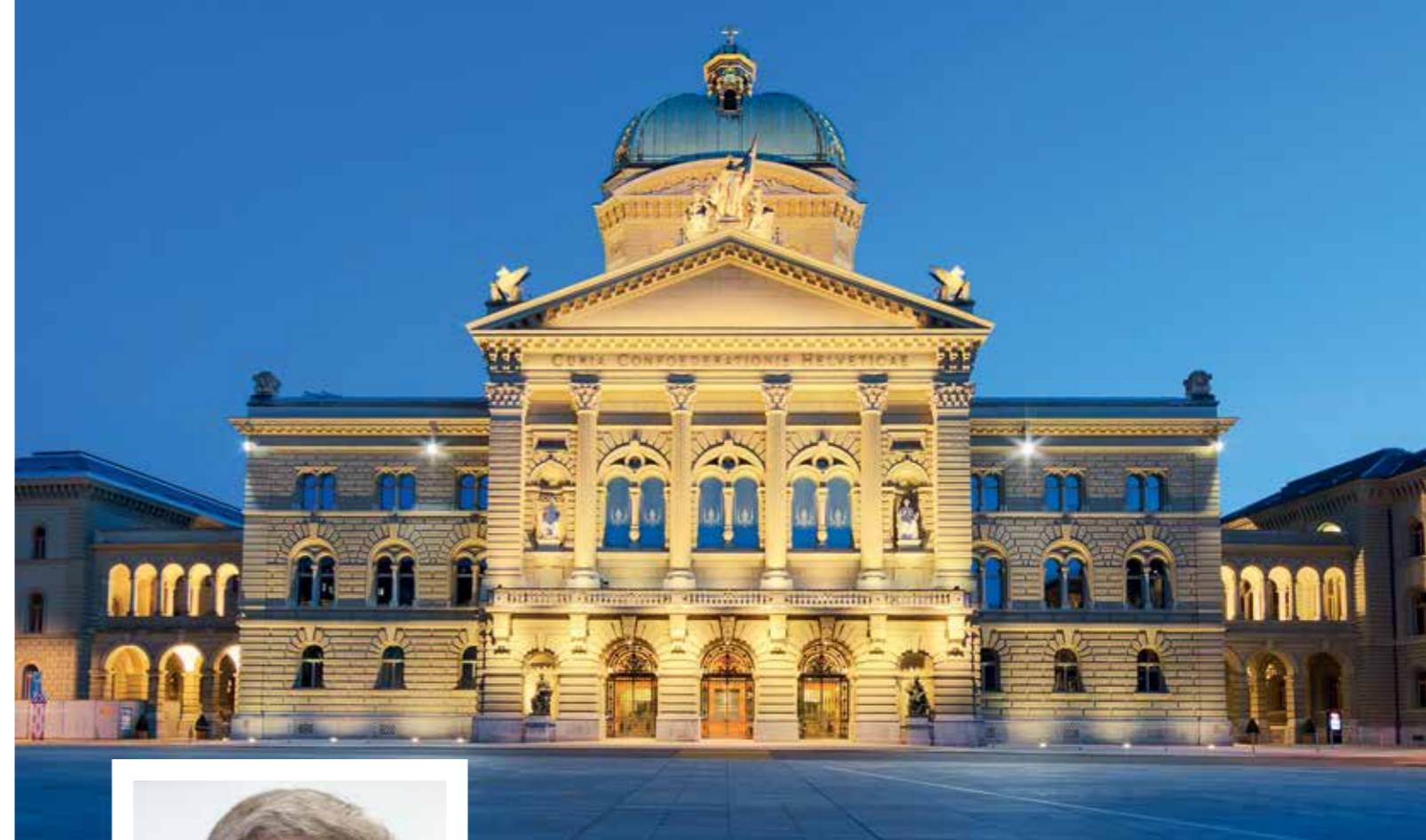
«DRM-Lösungen haben ihre Grenzen, wie Attacken in der Unterhaltungsindustrie zeigen.»

Wie gewährleistet die Bundesverwaltung das sichere Transferieren sensibler Daten?

Ab VERTRAULICH müssen die Daten verschlüsselt übertragen werden.

Wie vermeiden Sie den Verlust sensibler Daten?

Durch regelmässige Datensicherungen gegen Verlust. Gegen Datenabfluss werden die Netzübergänge überwacht. Überhaupt müssen gegen und zum Erkennen von Cyber-Angriffen neben dem «Perimeterschutz» vermehrt auch Verhaltensanalysen in den Systemen erfolgen.



Peter Fischer ist Delegierter für die Informatiksteuerung des Bundes (ISB) und somit der oberste Informatik-Verantwortliche in der Bundesverwaltung. Auf Stufe Amtsdirektor verantwortet er die gesamte Informations- und Kommunikationstechnik. Fischer übt diese Tätigkeit seit 2011 aus und rapportiert direkt an den Bundesrat.

Wie schützt die Bundesverwaltung sensible Daten? Und: Wie kann Datendiebstahl aufgedeckt werden?

Einen absoluten Schutz gibt es fast nicht. Manchmal wird man eines Datendiebstahls, wenn überhaupt, erst im Falle des Missbrauchs gewahr. Feststellen lässt es sich zum Beispiel durch Prüfen von Logfiles auf Auffälligkeiten. Digital-Rights-Management-Lösungen, kurz DRM, haben ihre Grenzen, wie Attacken in der Unterhaltungsindustrie zeigen.

Welche Herausforderungen an die Sicherheit erwachsen dem heutigen Anspruch, dass Daten unabhängig von Ort und Zeit verfügbar sein müssen?

Entscheidungsträger haben das Bedürfnis, immer und überall Zugriff auf die für ihre Tätigkeit nötigen Daten zu haben. Nach Möglichkeit sogar von ihren Smart Devices aus, die sie im täglichen Gebrauch haben. Das kollidiert mit den Sicherheitsanforderungen und -massnahmen. Eine grosse Herausforderung besteht darin, in mobile Standardgeräte eine adäquate

Sicherheit einzubauen, siehe das Mobiltelefon der deutschen Bundeskanzlerin Angela Merkel. Ganz auflösen kann man heute diesen Interessenkonflikt nicht. Vielmehr ist eine Optimierung anzustreben, je nach Gewichtung der Interessen. Die Psychologie spielt eine grosse Rolle. Häufig ist eine «nur» sichere benutzte Lösung einer sehr sicheren, aber nicht benutzten Lösung vorzuziehen.

Hat sich durch die Digitalisierung geheimer Daten deren Schutz eher verbessert oder verschlechtert?

Eher verschlechtert, da die Hürde des physischen Eindringens mit der Digitalisierung entfällt. Deshalb werden zum Beispiel geheime Daten in der Bundesverwaltung nur auf isolierten Systemen und Netzen bearbeitet. Aber die Digitalisierung bringt im Gegenzug neue Chancen in der Nutzung von Daten. Das ist entsprechend zu gewichten.



Sicheres Cloud-Computing – Tatsache oder Illusion?

Cloud-Computing wird für immer mehr Unternehmen und Organisationen zu einem wichtigen Arbeitsinstrument: Daten sind nahezu überall verfügbar und hohe IT-Kosten fallen weg. Knackpunkt jedoch ist die Informationssicherheit. Nicht alle Cloud-Dienste sind für hochsichere Kommunikation geeignet.

Informationstechnologien verändern sich rasant und damit auch die Möglichkeiten für die Nutzer. Eine wichtige Rolle spielt dabei das sogenannte Cloud-Computing, also die Nutzung von IT-Ressourcen über das Internet. Daten werden nicht mehr in einer lokalen Infrastruktur gespeichert und bearbeitet, sondern in der Rechnerwolke, besser bekannt als Cloud. Der Nutzer kann dabei von unterschiedlichen Geräten aus (Laptop, Tablet, Handy etc.) auf die eigene, persönliche Arbeitsumgebung zugreifen. Eine Verbindung zur Cloud wird über IP(Internetprotokoll)-Netze hergestellt.

Verschiedene Modelle und Services

Wolke ist jedoch nicht gleich Wolke. Cloud-Computing umfasst verschiedene Modelle und Angebotsformen (Services). Die Fachliteratur nennt vier gängige Modelle.

- **Public Cloud**
Die Public Cloud ist eine öffentlich zugängliche Rechnerwolke. Dabei stehen die Services eines externen Anbieters allen Nutzern offen. Mit welchen anderen Nutzern die Hardware dieser Cloud geteilt wird, kann ein Nutzer nicht selber entscheiden. Eine virtuelle Abgrenzung ist jedoch gegeben. Das heisst, jeder Nutzer legt sich ein Profil an, das vor dem Zugriff anderer Nutzer geschützt ist.
- **Private Cloud**
Die Private Cloud hingegen ist nicht öffentlich zugänglich. Die Services sind nur für Anwender innerhalb eines Betriebes oder einer internen Abteilung nutzbar. Die Private Cloud ist genau auf die spezifischen Bedürfnisse des Nutzers ausgerichtet und physisch von anderen Systemen getrennt.

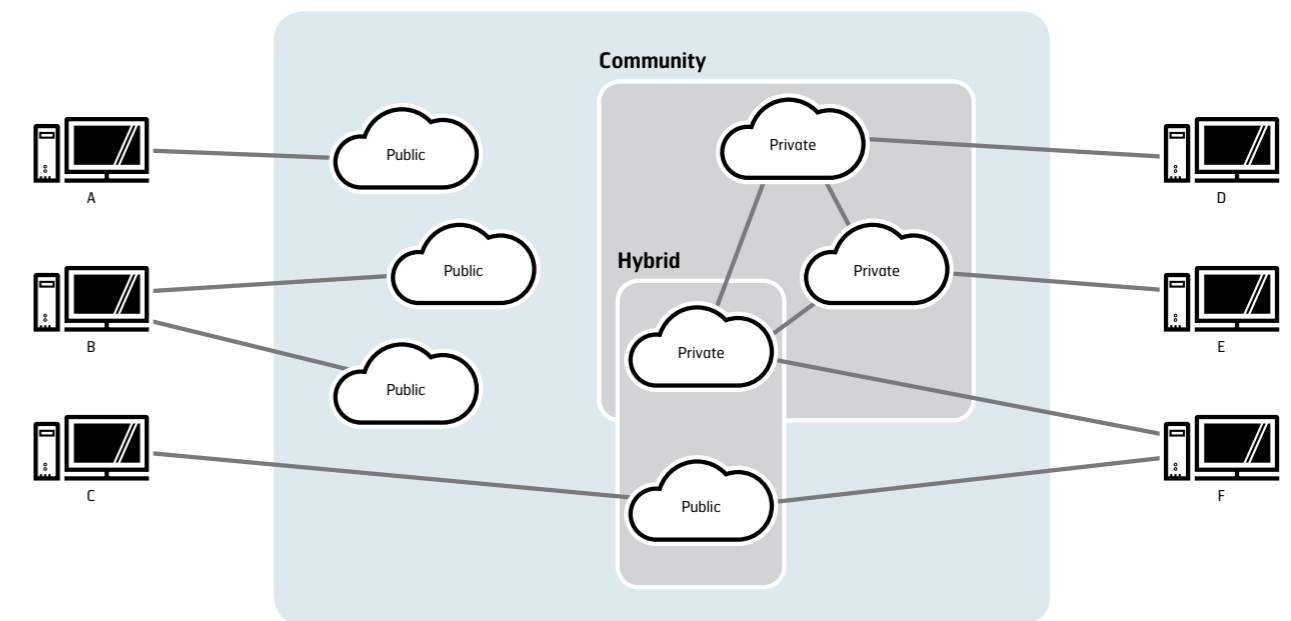
- **Community Cloud**
Schliessen sich mehrere Private Clouds zusammen, spricht man von einer Community Cloud. Der Zugang der Nutzer auf unterschiedliche Private Clouds kann mittels Zugriffsrechten gesteuert werden.
- **Hybrid Cloud**
Die Kombination von mehreren Clouds (Public, Private und/oder Community) wird als Hybrid Cloud bezeichnet. Solche Kombinationen entstehen, wenn beispielsweise aus einer Private Cloud heraus auf die Dienste einer Public Cloud zugegriffen wird oder Organisationen und Unternehmen zwar Anwendungen in Public Clouds nutzen, einen Teil ihrer Daten jedoch in der Private Cloud behalten.

Bei den Services existieren drei unterschiedliche Arten. Diese bauen zwar aufeinander auf, werden jedoch als eigenständige Bereiche betrachtet. Dabei handelt es sich um die Bereiche Hardware (IaaS), Betriebssystem (PaaS) und Anwendung (SaaS).

IaaS steht für «Infrastructure as a Service» und bezeichnet das Fundament innerhalb eines Cloud-Systems. Der Cloud-Anbieter ist verantwortlich für das Funktionieren des Netzes (virtuelle Ressourcen) und für den Zugang zu der angebotenen Hardware (physische Ressourcen). Der Nutzer hat allerdings Zugriff auf die Recheninstanzen, die je nach Anforderungen erweitert oder verkleinert werden können.

Beim «Service Platform as a Service» (PaaS) stellt der Anbieter eine von ihm entwickelte Anwendung zur Verfügung. Dieser Service wird vor allem von Softwareentwicklern genutzt. Die Programmiersprachen und Schnittstellen werden allerdings vom Anbieter vorgegeben.

Auf der Anwendungsebene wird dann von «Software as a Service» (SaaS) gesprochen. Der Benutzer muss sich weder um die Applikation noch um die Skalierbarkeit oder die Datenhaltung kümmern, sondern nutzt lediglich die zur Verfügung gestellten Funktionen der Cloud. Allerdings hat der Nutzer auch keinen Einfluss und Zugriff auf die Infrastruktur und Ressourcen des Cloud-Anbieters.



Schematische Darstellung der verschiedenen Cloud-Computing-Modelle



In der Cloud werden unter anderem IT-Infrastrukturen zur Verfügung gestellt

Risiken in der Cloud

Cloud-Computing bietet für Unternehmen und Organisationen unter gewissen Gesichtspunkten verschiedene Vorteile: Investitionen in Hardware und Software-Lizenzen verringern sich stark oder fallen ganz weg. Trotzdem erhalten die Nutzer Zugriff auf eine hochflexible Infrastruktur, die jederzeit an neue Anforderungen angepasst werden kann. Die Installation und Wartung der IT-Systeme wird vom Cloud-Anbieter übernommen, womit hohe Personalkosten wegfallen und die Nutzer sich stärker auf ihre Kerngeschäfte konzentrieren können. Auch bei Private Clouds können Kosten gesenkt werden, wenn beispielsweise Services zentral genutzt werden und nicht auf jedem einzelnen Gerät installiert sind.

Neben all den Vorteilen existieren bei der Nutzung von Cloud-Diensten auch Nachteile, insbesondere was die Sicherheit angeht. Dies betrifft vor allem Public und Hybrid Clouds. In derartigen Wolken steht die Vertraulichkeit, Integrität und Authentizität von Daten unter Umständen auf sehr wackligen Füßen. Bei der Nutzung einer Public oder Hybrid Cloud weiss der Anwender in der Regel nicht, wo die Daten gespeichert sind. Auf den Schutz seiner Daten gegen unbefugte Einsichtnahme (Vertraulichkeit) und gegen unerwünschte Veränderungen oder Beschädigungen (Integrität)

hat der Nutzer daher wenig bis keinen Einfluss. Es bleibt ihm also nichts anderes übrig, als dem Anbieter zu vertrauen. Die sichere Zuordnung einer Information zum Sender (Authentizität) ist unter Umständen ebenfalls schwierig zu überprüfen und gerade in sensiblen Bereichen mit Sicherheitsrisiken verbunden.

Public und Hybrid Clouds sind für sichere Kommunikationslösungen eine risikobehaftete Option.

Auch was die Verfügbarkeit von Services betrifft, ist ein Nutzer von Public und Hybrid Clouds dem Anbieter ausgeliefert. Er muss sich auf die Angaben des Anbieters verlassen, dass dieser seine Infrastruktur physisch (zum Beispiel vor Naturkatastrophen) und virtuell (funktionierende Netze) genügend schützt. Folglich sind Public und Hybrid Clouds aus sicherheitsrelevanter Perspektive eine risikobehaftete Option, sprich: für höchste Ansprüche bezüglich sicherer und hochsicherer Kommunikationslösungen ungeeignet.

Die Architektur der Sicherheit

Private Clouds hingegen können mit entsprechenden Vorkehrungen hohen Sicherheitsstandards genügen. Eine Möglichkeit ist, die Cloud selber zu betreiben. Das heisst, das Unternehmen oder die Organisation verfügt über eigene Server, Technologien, Anwendungen und entsprechend qualifiziertes IT-Personal. Ob die Private Cloud intern oder extern (oder in einer Mischform) betrieben wird – die Anforderungen an die Sicherheit sind dieselben. Idealerweise werden die Sicherheitsaspekte bereits beim Design der Informationslösung miteinbezogen. Das heisst, die Architektur des Netzwerkes orientiert sich an verschiedenen Informationssicherheitszonen. Diese wiederum werden anhand verschiedener Klassifizierungsstufen gebildet – beispielsweise CONFIDENTIAL, SECRET und TOP SECRET. Diese Schutzzonen werden kryptografisch voneinander getrennt. Für die Übermittlung von sensiblen und hochsensiblen Daten bedeutet dies, dass sie vor der Übertragung mit einer End-zu-End-Verschlüsselung geschützt werden. So werden nur kryptografisch geschützte Daten in die Cloud geladen. Die Verschlüsselung respektive Sicherung der Verbindung von der Cloud über das Internet wird mit kryptografischen Mitteln vollzogen.

Um einen hohen Sicherheitsgrad zu erreichen, muss die Kryptografie auf einer geschützten Hardware-Plattform umgesetzt sein. Solche Geräte sind nicht grösser als eine Zigarettenschachtel und können auch auf Reisen zum Einsatz kommen. Um eine hoch gesicherte Private Cloud betreiben zu können, sind noch weitere Faktoren zu berücksichtigen. Die Cloud-Hardware beispielsweise muss in hochsicheren Räumen untergebracht werden. Das Fachpersonal – intern wie extern – wird einer Sicherheitsprüfung unterzogen. Und mit etwas vom Wichtigsten: Mitarbeitende, die mit Cloud-Diensten arbeiten, brauchen die nötige Sensibilisierung dafür, dass sie in einem hochsicheren Bereich arbeiten. Denn achtsames Verhalten ist ein zentraler Schlüssel für optimale Sicherheit.



Quantenrechner: Der Supercomputer der Zukunft

Quantencomputer lösen gewisse Rechenaufgaben um ein Vielfaches schneller als digitale Rechner – theoretisch. Von einer tatsächlichen Anwendung und praktischem Nutzen ist Quantencomputing noch weit entfernt. Trotzdem lohnen sich Überlegungen, was real existierende Quantencomputer für die Sicherheit von kryptografischen Systemen bedeuten würden.

Ein Quantenrechner ist ein Computer, dessen Funktion auf den Gesetzen der Quantenmechanik beruht. Die Theorie wurde Mitte der 1920er Jahre mit dem Ziel entwickelt, die Welt des Allerkleinsten zu verstehen. Die charakteristische Eigenschaft der Quantenwelt ist die Dualität von Welle und Teilchen: Subatomare Teilchen können sich wie Wellen verhalten und Lichtwellen können sich wie Teilchen verhalten. Ein weiterer Aspekt ist das Phänomen Superposition. Das heisst: Partikel können zwei oder hundert oder eine Million Dinge gleichzeitig tun. Die Quantenwelt besteht daher aus einer Vielzahl sich überlappender Wahrscheinlichkeiten.

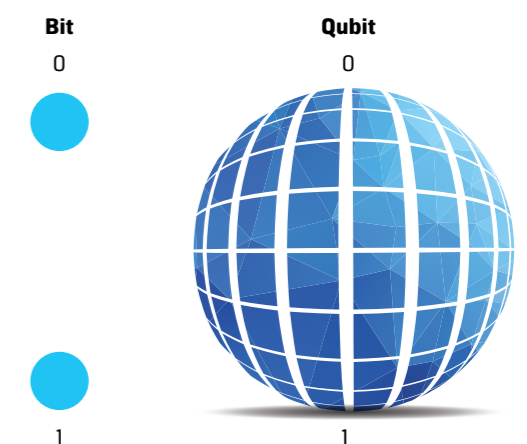
Diese Komplexität lässt sich nicht durch einen herkömmlichen Computer berechnen. Deshalb schlug der Physiker und Nobelpreisträger Richard Feynman vor, die Berechnungen der Quantenwelt mit einem Quantencomputer auszuführen. Im Unterschied zum Digitalrechner arbeitet ein solcher Quantencomputer nicht auf der Basis der Gesetze der klassischen Physik beziehungsweise Informatik, sondern auf der Basis quantenmechanischer Zustände, was wesentlich über die Regeln der klassischen Theorien hinausgeht.

Unbeschränkte Bewegungsmöglichkeiten

Um zu verstehen, wie Quantencomputer funktionieren könnten, ist es nützlich, zunächst das Bit eines klassischen Computers als eine Art kugelförmiger Kompass darzustellen,

dessen Nadel entweder auf die 1 (den Nordpol) oder auf die 0 (den Südpol) weist und durch eine Drehung um 180 Grad zwischen diesen beiden Zuständen wechseln kann. Die Zentraleinheit eines Computers besteht aus vielen Millionen solcher Ein-Bit-Schalter. Im Quantencomputer heisst die Entsprechung zum Bit «Qubit». Das Qubit ähnelt der klassischen Kugel. Seine Bewegungsmöglichkeiten beschränken sich aber nicht nur auf eine Drehung um 180 Grad. Das Qubit kann sich um jeden beliebigen Winkel im Raum drehen.

Die quantenmechanische Kugel kann auch in mehrere Richtungen gleichzeitig weisen (Superposition). Aufgrund dieser extremen Flexibilität kann ein Qubit mehr Informationen kodieren als ein klassisches Bit. Und die Rechenleistung wird zusätzlich erhöht, weil Qubits quantenverschränkt arbeiten – so als wäre jede Qubit-Kugel durch elastische Fäden mit jedem anderen Qubit verbunden – auch Quantenkohärenz genannt. Die Konsequenz: Die Leistung eines Quantencomputers verdoppelt sich durch das Hinzufügen eines einzigen Qubits. Im Gegensatz dazu wächst die Leistung eines klassischen Computers linear mit der Zahl der Bits.



Ein Bit ist entweder 1 oder 0. Das Qubit spielt dabei die analoge Rolle und dient als kleinstmögliche Speichereinheit

Theoretische Studien legen nahe, dass unter Ausnutzung dieser Effekte bestimmte Probleme der Informatik, zum Beispiel die Suche in extrem grossen Datenbanken und die Faktorisierung (das Zerlegen eines Produkts in seine Primfaktoren) extrem langer Zahlen, wesentlich effizienter gelöst werden können als mit klassischen Computern. Dies würde das mathematische Problem, das die Basis für die Sicherheit einiger kryptografischer Verfahren darstellt, lösbar machen.

Chinesen bauen ersten Quantencomputer

Der Quantencomputer ist gegenwärtig allerdings noch ein theoretisches Konzept. Denn damit ein Quantencomputer funktioniert, dürfen die Qubits zur Ausführung von Berechnungen ausschliesslich untereinander interagieren (Quantenkohärenz). Das bedeutet, dass sie völlig von der Umwelt abgeschirmt sein müssen. Um das zu bewerkstelligen, bedienen sich Quantenphysiker physikalischer Systeme: Sie kodieren die Qubits in einer Handvoll Atome, kühlen das System bis auf den Bruchteil eines Grades über dem absoluten Nullpunkt ab und umgeben ihre Apparaturen mit einer Fülle von Isoliermaterial, um alle Einflüsse aus der Umwelt abzuschirmen.

In kleinem Massstab wurden einige solcher Konzepte im Labor erprobt und Quantencomputer mit wenigen Qubits realisiert. So gelang es etwa chinesischen Wissenschaftlern 2011, die Zahl 143 mit Hilfe von nur vier Qubits in ihre Primfaktoren (13 und 11) zu zerlegen. Damit ist klar, dass die Weiterentwicklung der heutigen Generation von Quantencomputern zu nützlichen Geräten eine sehr grosse Herausforderung bleibt. Von einer tatsächlichen Anwendung und praktischem Nutzen ist man noch weit entfernt.

Das Hindernis: Mit jedem zusätzlichen Qubit vergrössert sich zwar die Rechenleistung, gleichzeitig werden aber auch die Probleme grösser, wenn man die Quantenkohärenz aufrechterhalten will. Mit anderen Worten: Die Dekohärenz setzt ein, lange bevor es dem Computer gelungen ist, auch nur die einfachste Berechnung abzuschliessen.

Es werden Anstrengungen unternommen, in der Quantentechnologie weiterzukommen. So hat zum Beispiel die EU-Kommission beschlossen, die Entwicklung von Quantentechnologien zu fördern. Das Programm soll ab 2018 anlaufen und einen Umfang von einer Milliarde Euro haben. Zu den Technologien, die im Rahmen des Programms entwickelt werden sollen, gehören unter anderem Quantencomputer.

Kryptosysteme

Es stellt sich also die Frage, welche Informationssicherheitslösungen durch Quantencomputing bedroht sein könnten. Es gibt prinzipiell zwei Arten von Verschlüsselung: symmetrische und asymmetrische.

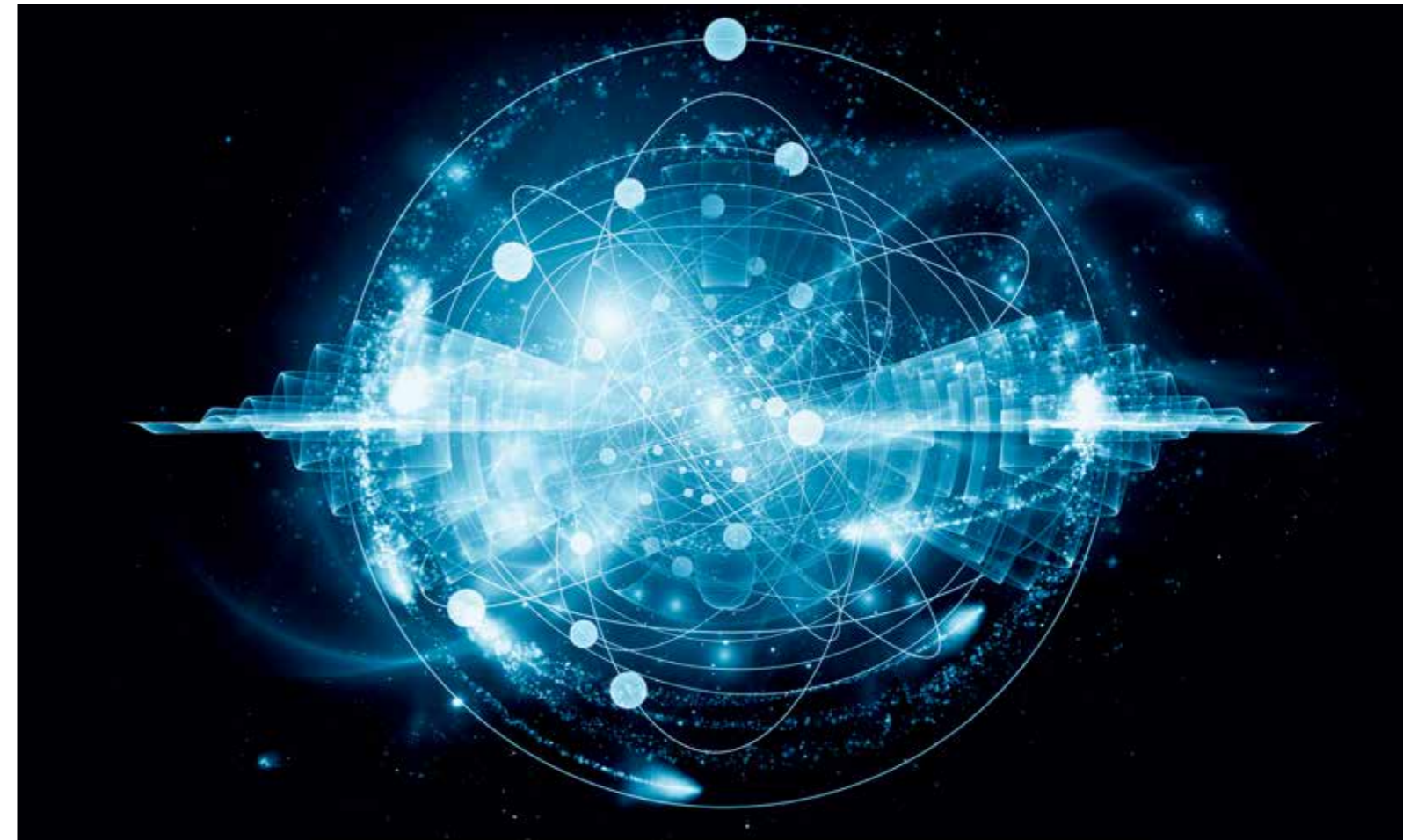
- **Symmetrische Kryptosysteme:** Die Schlüssel zum Ver- und Entschlüsseln einer Nachricht sind identisch – beide Teilnehmer verwenden denselben Schlüssel. Symmetrische Kryptosysteme ermöglichen hohe Verschlüsselungsleistungen: Der Advanced Encryption Standard (AES) ist beispielsweise 1000-mal schneller als das asymmetrische Kryptosystem RSA. Für symmetrische Verschlüsselungsverfahren sind Quantencomputer eine relativ kleine Bedrohung, da hier mittels des Grover-Algorithmus die in Bit gemessene Sicherheit eines Schlüssels maximal um die Hälfte reduziert würde. Der gestiegenen Rechenleistung liesse sich mit entsprechend längeren Schlüsseln entgegenwirken.
- **Asymmetrische Kryptosysteme:** Die Schlüssel zum Ver- und Entschlüsseln einer Nachricht unterscheiden sich. Diese Verfahren werden auch als Public-Key-Verfahren bezeichnet. Das Prinzip der asymmetrischen Verschlüsselung beruht im Wesentlichen darauf, dass sich jeder Kommunikationspartner jeweils ein Schlüsselpaar (bestehend aus zwei Schlüsseln) erzeugt. Einer der Schlüssel wird geheim gehalten, das ist der sogenannte private Schlüssel. Der zweite Schlüssel wird jedem kommunikationswilligen Teilnehmer zugänglich gemacht. Der zweite Schlüssel heisst deshalb öffentlicher Schlüssel. Das heisst, dass jeder, der den öffentlichen Schlüssel kennt, eine Nachricht chiffrieren kann, aber nur, wer den privaten Schlüssel kennt, kann diese auch wieder dechiffrieren. Die Sicherheit beruht darauf, dass es nicht möglich ist, nur aufgrund des öffentlichen Schlüssels den privaten Schlüssel zu berechnen.

Von einer tatsächlichen Anwendung und praktischem Nutzen ist man beim Quantencomputer noch weit entfernt.

Beim asymmetrischen Verschlüsselungsverfahren wird heute RSA genutzt. RSA hat den Namen nach den Anfangsbuchstaben der Nachnamen seiner Erfinder Rivest, Shamir und Adleman bekommen. Sie haben das Verfahren 1977 entwickelt. Die RSA-Verschlüsselung nutzt sogenannte Einweg-Funktionen. Man kann sich diese Funktionen als mathematische Einbahnstrassen vorstellen. In die eine Richtung (Verschlüsseln) ist die Berechnung ganz einfach. Versucht man den Rechenweg jedoch rückwärts zu beschreiten (Entschlüsseln ohne Schlüssel), wird es sehr schwierig.

Für die Praxis untauglich

Eine solche Einweg-Funktion ist die Multiplikation von Primzahlen. Es ist sehr einfach, zwei Primzahlen zu multiplizieren. Beispiel: 3259 mal 5431 ergibt 17'699'629. Wenn die



Quantencomputer brauchen tausende von Qubits, um komplexe Rechnungen zu lösen, und bilden damit eine grosse Angriffsfläche für Störungen

Frage aber lautet: «Welche Teiler der Zahl 17'699'629 existieren?», wird die Lösung sehr aufwendig. Das Problem dabei ist, dass für das Zerlegen einer grossen Zahl in ihre Primfaktoren kein schneller Algorithmus bekannt ist. Schon bei einem 100-stelligen Produkt scheitert ein gängiger Computer. In der Praxis werden aber 300- bis 600-stellige Produkte verwendet, die selbst die schnellsten Hochleistungsrechner auch im Verbund nicht wieder zerlegen können.

Diese Sicherheit ist jedoch nur praktisch und nicht theoretisch. Würde ein effizienter Algorithmus für das Problem der Faktorisierung gefunden, wäre die RSA-Verschlüsselung geknackt. Peter Shor hat 1994 einen Algorithmus erfunden, der auf einem Quantencomputer benutzt werden kann, um RSA und andere gängige Public-Key-Systeme zu knacken. Nur sind die existierenden Quantencomputer nicht schneller als herkömmliche Computer und für die Praxis bisher unbrauchbar.

Trotzdem bleibt die Frage: Wie können asymmetrische Kryptosysteme in Zukunft geschützt werden? Mit dieser Frage beschäftigt sich die Post-Quanten-Kryptografie (PQC). Das ist ein Teilgebiet der Kryptografie, das sich mit kryptografischen Primitiven befasst, die im Gegensatz zu den meisten aktuell verwendeten asymmetrischen Kryptosystemen selbst unter Verwendung von Quantencomputern nicht zu entschlüsseln sind.

Quantencomputing verändert zwar die Kryptografie, doch die Folgen für bestehende Kryptosysteme sind sehr unterschiedlich: Für die meisten asymmetrischen Kryptosysteme könnten die aktuellen Entwicklungen eine Gefahr bedeuten, symmetrische Kryptosysteme wird dies hingegen nicht beeinflussen.



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

Messen

IDEX

19. bis 23. Februar 2017 in Abu Dhabi

CRYPTO cSEMINARS

cSeminar Information Security Specialists

13. bis 17. März 2017

2. bis 6. Oktober 2017

cSeminar Technical Vulnerability Testing

20. bis 24. März 2017

9. bis 13. Oktober 2017

cSeminar Contemporary Cryptography

27. bis 31. März 2017

16. bis 20. Oktober 2017

Die Seminare finden in der Crypto Academy
in Zug/Steinhausen statt.

Kontakt und weitere Informationen unter

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