„Vertrauliche Dokumente müssen sogar vor dem Administrator geschützt werden“

Interview mit Bruno Quint zum Thema „Cloud und Verschlüsselung“

Egal ob für die NSA oder die Konkurrenz – Daten sind das moderne Gold. „Verschlüsselung“ lautet das Zauberwort, das Privatpersonen Privatheit und Unternehmen Geheimhaltung sogar in der Cloud sichern soll. Geheimhaltung mit Open-Source ist nicht neu. Gegenwärtig geht der Trend hin zu starken Verschlüsselungen von Dokumenten und Files, damit sich Unbefugte keinen wirklichen Zugriff verschaffen können. Dr. Bruno Quint, Managing Director der CORISECIO GmbH, spricht darüber, wie digitaler Datenaustausch im Cloud-Zeitalter ohne Security-Striptease funktionieren kann.

OBJEKTspektrum: Herr Dr. Quint, Fraunhofer hat die Volksverschlüsselung ausgerufen. Was halten Sie davon?

Bruno Quint: Es gibt so vieles, was Fraunhofer schon ausgerufen hat. Mit MP3 hatte Frauenhofer einen Riesenerfolg, aber eine Volksverschlüsselung ist eine große Herausforderung.

Also eher weniger?

Alles und jedes zu verschlüsseln, halte ich nicht für das Maßgebliche. Wir wollen ja Daten austauschen. Nur muss ich mir Gedanken machen, welche Daten sensitiv sind. Früher hat man alle Fotos in Facebook geladen. Das hat sich geändert. Wenn im privaten Umfeld einer ein Foto macht, kommt sofort der Satz: „Das veröffentlichst du aber bitte nicht auf Facebook.“ Da ist etwas passiert, man denkt mehr nach.

Sind die Menschen und Unternehmen auch sensibler hinsichtlich der Inhalte geworden, die sie beruflich in die Cloud stellen, etwa personenbezogene Daten?

Jede Firma muss selbst bewerten, wie groß ihr Security-Bedarf ist. Wenn hochbrisante Themen, beispielsweise Informationen über Atomkraftwerke und Patente, in der Cloud lägen, ginge man ein hohes Sicherheitsrisiko ein.

SharePoint-Lösungen sind praktisch, weil die Benutzer einfach und überall damit arbeiten können. Schließlich werden sogar hoch vertrauliche Dokumente dort abgelegt. Man macht einen Vertrag mit dem Cloud-Anbieter. Sichert der nicht über Service-Level-Agreements viele wiederkehrende Dienstleistungen zu, die einem Geborgenheit vorgaukeln?

In den SLA-Agreements geht es um Verfügbarkeit, Service und …

... also um ganz viel Komfort, den man umfassend in Anspruch nehmen möchte. Sie als Security-Experte auch?

Die Vorteile einer Cloud lassen sich nicht mehr aus dem Alltag vertreiben: Denken Sie nur an die komfortable Zusammenarbeit, ohne umständlich Daten auf Papier oder Speichermedien mitschleppen zu müssen. Umso wichtiger ist deshalb unauffällige, nicht störende Sicherheit. Sie muss von jedermann so automatisch und einfach genutzt werden können, dass man sie gar nicht bemerkt.

Wie funktioniert die ideale Security demnach?

Beim Hochladen durchläuft der Datenstrom unser Gateway. Dabei wird er ver- und entschlüsselt. Das war‘s schon. Sogar der Administrator ist außen vor. Er kann sich zwar anzeigen lassen, dass ein Dokument vorhanden ist. Aber er hat keine Chance, es zu entschlüsseln, um es zu lesen.

Foto: Peter Knoll

Dr. Bruno Quint ist Geschäftsführer von CORISECIO, einer Tochterfirma von Allgeier IT Solutions. CORISECIO ist Anbieter von Open-Source-Security-Lösungen und bietet Verschlüsselungen unter anderem für SharePoint, Microsoft Office 365, GoogleDrive und Dropbox.

Hier die Wolke, dort der Mensch. Kann man den menschlichen Faktor absichern?

Es gibt Angriffe, die keiner richtig bemerkt, weil sie von innen kommen. Bei der Cloud sind Cloud-Betreiber und Administratoren sowie Rechenzentren im Spiel, die irgendwo in Malaysia und Indien stehen. Ich kann interne Security über Standardmethoden durchführen und sogar Zugriffsberechtigungen erteilen. Der Daten-Administrator in Indien oder Malaysia, den ich nicht kenne, kann sich dann aber doch Zugang zu Dokumenten verschaffen, die unverschlüsselt sind.

Wie muss man sich diese Standard-Security genau vorstellen?

Standard sind Firewalls mit Intrusion Prevention, Malware-Schutz, Application Intelligence and Control, gegebenenfalls verbunden mit Echtzeit-Visualisierung. Hinzu kommen Berechtigungskonzepte, die man mit einer Art Türsteher vergleichen kann: Wer darf rein, wer raus? Aber reicht so ein Standard? Bei der Cyber-Attacke auf den Bundestag offensichtlich nicht. Ein anderer Fall: Edward Snowden war SharePoint-Administrator der NSA. Snowden hat vertrauliche Dokumente der NSA kopiert. Der geht hin und nimmt auf einmal Daten mit, kopiert sie auf seine USB-Festplatte und marschiert nach draußen. Mit so einem simplen Trick wurden die Berechtigungskonzepte der NSA ausgetrickst.

Zugriffsberechtigungen reichen als Zusatzsicherung also nicht aus?

Interne Angriffe, auch von Entwicklern, die Zugriffe haben, sind das Einfachste, um Vertrauliches, Geheimes nach draußen zu tragen. Das heißt, vertrauliche Dokumente müssen auch vor internen Angriffen geschützt werden, sogar vor Administratoren.

Wie lassen sich sensible Daten und Geschäftsgeheimnisse angesichts des „menschlichen Faktors" überhaupt sichern?

Verschlüsselung ist der sicherste Schutz. Das, was Sie jeden Tag machen, wenn Sie aus der Haustür gehen: Sie schließen ab, um Ihr Haus zu sichern. So ähnlich kann man das bei der Kryptographie sehen: Sie haben einen Algorithmus als Haustür und einen Schlüssel, mit dem Sie die Tür auch wieder aufschließen können. Um das Bild fortzusetzen: Bei der symmetrischen Verschlüsselung haben mehrere Familienmitglieder einen Schlüssel, mit dem sie auf- und zuschließen können. Beim asymmetrischen Verfahren können Partygäste abschließen, aber nicht mehr aufschließen. Diese Möglichkeiten gibt es eigentlich seit Jahrzehnten. Die NSA ist jetzt, nach Snowden, auch damit beschäftigt, die Daten zu verschlüsseln. Für die NSA lautet die nächste Anforderung ebenfalls: Wie bleibe ich trotz Verschlüsselung arbeitsfähig? Wie kann ich in verschlüsselten Dateien suchen, einzeln und miteinander geschmeidig arbeiten, trotz aller Security? Natürlich gibt es dafür Wege, so wie wir das Arbeiten mit verschlüsselten Daten bei CORISECIO gelöst haben.

Die Cloud lässt sich also abriegeln. Doch schwindet mit der wachsenden Popularität von Smartphones und Tablets die Sicherheit nicht zwangsläufig?

Jeder muss sich bewusst sein, dass die Sicherheit und das Arbeiten mit verschlüsselten Dateien auf mobilen Geräten schwerer umsetzbar sind, als wenn ich mich im Unternehmen befinde. Mitarbeiter, die über Mobile Devices häufiger auf vertrauliche Dateien zugreifen müssen, stellen für Firmen eine immense, sicherheitstechnische Herausforderung dar.

Wenn dieser Zugriff auf vertrauliche Arbeitsdateien über Smartphones und Tablets schwieriger ist, könnte das ein Grund für Unternehmen sein, auf Sicherheit zu verzichten?

Sicherheitslösungen à la Kanzler-Handy sind schwer handhabbar und als Insellösungen für normale Unternehmen teuer und schwer einführbar. Für Frau Merkel und ihre Politikerkollegen oder auch für Spitzenmanager von börsennotierten Unternehmen sind sie wichtig. Normale Unternehmenshandys jedoch haben schlicht Sicherheitslücken. Jedes Betriebssystem eines Herstellers kann die Inhalte mitlesen und hat so Zugriff auf alles, was auf diesem Handy passiert. E-Mails und Files sind daher schwach bis gar nicht gesichert. Viele Hersteller bieten Backup-Lösungen mit einer Spiegelung aller Daten in der Cloud an. Damit haben sie kompletten Zugriff. Da sind wir wieder beim Komfort: Die Sicherung gegen Datenverlust als automatisches Backup des Herstellers ist nicht zu verwechseln mit inhaltsbasierter Sicherheit, mit Security. Sie sind sogar Konkurrenten.

Von amerikanischen Herstellern wird von Rechts wegen gefordert, Backdoors in die Verschlüsselung einzubauen. Kauft man die Spionage dann mit der Hardware?

Eine Backdoor ist wie eine Katzenklappe in der Haustür, durch die ein Secret-Service-Agent mit durchpasst. Oder wie ein Extra-Schlüssel unter dem Blumentopf, mit dem er aufschließen kann. Nur zu unserem Besten … IT-Unternehmen, Kryptologen und Politiker fordern von US-Präsident Obama, sich gegen solche Hintertüren in Kommunikationsgeräten zu stellen. Sie wollen nicht, dass die Backdoor als Hintertür dient, die bestimmte amerikanische Dienste für sich aufsperren können.

Mittelständische Unternehmen fragen oft: Warum verschlüsseln, wir haben doch nichts zu verbergen?

Datenschutz ist ein Grundrecht, das wir mit beachten müssen. Jeder hat das Recht, gewisse persönliche Daten für sich zu behalten. Möchte eine Firma komplett gläsern sein, ihre Patente, Strategiepapiere, Personal- und Krankenakten beliebigen Augen preisgeben? Börsenbezogene Unternehmen dürfen das gar nicht.

Wird man mit Clouds, die bei amerikanischen Unternehmen angesiedelt sind, nicht automatisch gläsern?

Amerikanische Unternehmen wurden dazu verurteilt, alle Informationen auf ihren Servern an amerikanische Dienste auszuhändigen – auch Infos über ausländische Kunden. Sie können jederzeit dazu verpflichtet werden, selbst wenn sich die Server in Europa befinden. Deshalb arbeiten beispielsweise Microsoft und andere amerikanische Unternehmen gerne mit deutschen und europäischen Anbietern zusammen, um ihren Kunden Security anzubieten. Wenn ein deutsches Unternehmen die Verschlüsselung der Informationen übernimmt, kommt da niemand mehr ran. Ein deutsches Unternehmen braucht nichts offenzulegen.

Welche Anforderungen müssen Lösungen für Verschlüsselungen erfüllen?

Hohe Sicherheit, hohe Verfügbarkeit, die Integration externer Partner, keine Clients sowie Suche in verschlüsselten Dokumenten als SharePoint-Security. Was immer hilft, ist eine Open-Source-Lösung: So kann man sicherstellen, dass keine Backdoors drin sind. Über einen Encryption-Gateway wird echte Security praktiziert, indem jedes Dokument eines Benutzers verschlüsselt und entschlüsselt wird, unabhängig von File-Berechtigungen. Der Administrator kann Zugriff auf meine vertraulichen Dokumente haben, kann sie aber nicht entschlüsseln. Nicht einmal der Security-Administrator, der die Sicherheitsregeln für ein Unternehmen verwaltet, darf an vertrauliche Inhalte herankommen.

Ist bei CORISECIO denn alles Open-Source?

Unser Know-how schützen wir natürlich mit einer Enterprise-Lösung. Auch wir wollen mit unserem Wissen Geld verdienen.

Ihr Fazit zur Security für jedermann?

Security ist etwas Handgreifliches und Verschlüsselung kein Teufelszeug. Man nutzt sie einfach wie den Schlüssel an der Haustür und am besten schon automatisch.

Herr Quint, vielen Dank für das Gespräch.

Das Interview führte OBJEKTspektrum-Redakteurin Annegret Handel-Kempf.