INHALTSVERZEICHNIS

END2END-VERSCHLÜSSELUNG – DAS ALLHEIL-MITTEL FÜR DIE CLOUD?

Dass die Cloud neben vielen Vorteilen auch Probleme mit sich bringt ist mittlerweile bekannt. Eines der Hauptprobleme sind Sicherheitsfragen. Sie resultieren daraus, dass bislang in vertrauenswürdigem Kontext wie z.B. dem geschützten Firmennetzwerk, abgelegte Daten nun an einem deutlich weniger vertrauenswürdigen Ort – eben der Cloud – abgelegt werden.

END2END-VERSCHLÜSSELUNG – EINE PILLE OHNE NEBENWIRKUNGEN?

Die Tragweite ist, insbesondere durch das **EuGH-Urteil zu SafeHarbor** und **Spionageenthüllungen durch E. Snowden**, deutlich sichtbar geworden. Der **Druck auf die Anbieter von Cloud-Angeboten** hat diese zum Handeln gezwungen. So weit, so gut.

Die Antwort auf diese Sicherheitsproblematik fällt bisweilen wenig differenziert aus. Die sogenannte **End2End-Verschlüsselung** entwickelt sich zum Allheilmittel: Eine Pille gegen alles und ohne Nebenwirkungen. Das macht stutzig.

Was bei **Instant Messaging Systemen**, wie jüngst bei WhatsApp eingeführt, eine gute Idee sein mag, muss es z.B. **File Sharing-Systemen (EFSS, Enterprise File Sync & Share oder MFT, Managed File Transfer)** noch lange nicht sein. Hier ein paar Beispiele:

> End2End-Verschlüsselung macht z.B. Virenscanner wirkungslos
Wenn nur noch der Eigentümer einer Datei an deren unverschlüsselten Inhalt kommt, kann der Cloud-Dienst nicht mehr damit arbeiten. Damit ist nicht nur eine ungewollte Verarbeitung ausgeschlossen, sondern z.B. auch der Virenscan, der aber auf Fileservern gängige Praxis ist. Man schafft also ein **neues Sicherheitsrisiko durch unerkannte Viren**, insbesondere wenn eine solche Plattform zum Austausch von Dateien über Organisationsgrenzen eingesetzt wird.

> Steigender Ressourcenverbrauch
Gewöhnlich werden die Daten unter Verwendung von **Public-Key Kryptographie** (asymmetrische Verschlüsselung). Das heißt, dass beim Teilen von Dateien mit anderen **nur der Empfänger die Datei entschlüsseln** kann. Was im Umkehrschluss bedeutet, dass seitens des Senders jede Datei einzeln mit dem Schlüssel des Empfängers verschlüsselt werden muss. Man spricht hier von **„Client-Side Fan-Out" statt „Server-Side Fan-Out"**. Das **kostet Netzwerkbandbreite** und **belegt Speicherplatz**. Mehr Speicher wird aber nicht nur durch die mehrfache Ablage benötigt, sondern auch, weil die Duplizierung mit verschlüsselten Dateien nicht mehr greift. Im Endeffekt führt dies zu **steigenden Kosten.**

> Wider den Business-Anforderungen
Im Unternehmen gibt es typischerweise **Abteilungs- oder Projektverzeichnisse**. Die Liste der Zugriffsberechtigten ändert sich mit **Zugehörigkeit und Rolle eines Mitarbeiters**. Betrachtet man das vor dem Hintergrund des letzten Beispiels, stellt sich die Frage, nach einer Lösung. Kommt ein neuer Mitarbeiter hinzu, müssten – bei asymmetrischer Verschlüsselung – alle Inhalte des Projektverzeichnisses Client-seitig mit dem Schlüssel des neuen Mitarbeiters verschlüsselt und nochmals abgelegt werden. Das wird schnell unpraktikabel bei großen Datenmengen. Einfacher geht es zwar bei symmetrischer Verschlüsselung: Hier reicht es den Schlüssel dem neuen Mitarbeiter auszuhändigen. Allerdings müssten bei Wegfall eines Mitarbeiters ebenfalls alle Dateien Client-seitig neu verschlüsselt und der Schlüssel an die berechtigten übermittelt werden. Derartige Lösungen werden in der Praxis schnell unpraktikabel.

FAZIT

Lösungen müssen angemessen sein. End2End-Verschlüsselung ist eine Lösungsmöglichkeit für ein konkretes Problem. Es ist aber mit Sicherheit kein Allheilmittel. Ein Vorgehen Nutzer von Enterprise File Sync & Share bzw. Managed File Transfer Systemen kann wie folgt aussehen:

> Prüfung der Anforderungen:

a. Am Anfang sollte immer eine VIV-Analyse (Vertraulichkeit, Integrität, Verfügbarkeit, siehe z.B. http://www.computerwoche.de/a/it-sicherheit-das-kalkulierte-risiko,3092357) zur Ermittlung des Schutzbedarfes stehen.

b. Prüfung, ob Anforderungen in Richtung Kollaboration und Verarbeitung von Daten vorliegen. Beispiele: Virenprüfung, Durchsuchbarkeit von Inhalten, Konvertierung von Formaten, Erkennung von Inhalten, usw.

> Die Erkenntnisse aus der Schutzbedarfsermittlung und der weiteren Anforderungsanalyse dienen als Grundlage zur Auswahl von Produkten und deren Betriebsmodellen:

a. Wenn keine Anforderungen an die Sicherheit (kommt im Business-Kontext kaum vor) vorliegen, sind die bekannten Public Cloud Angebote ggf. eine Option.

b. Bei Inhalten zum internen Gebrauch oder bei vertraulichen Inhalten können Private Cloud-Lösungen, entweder im eigenen Rechenzentrum (onPremise) oder als Hosted Private Cloud eine Option darstellen. Durch den vertrauenswürdigen Kontext in dem die Daten abgelegt sind, ist meist eine ausreichende Sicherheit gegeben, ohne auf eine End2End-Verschlüsselung setzen zu müssen. Das erlaubt auch die Verarbeitung von Daten.
Hochsicherheitslösung: In diesem Fall führt kaum ein Weg an der End2End-Verschlüsselung vorbei, womit zumeist Einschränkungen in Bezug auf Funktion (z.B. Datenverarbeitung) und Usability verbunden sind.

KONTAKTIEREN SIE UNS

Rebecca Hilebrand
Business Consultant

+49 7541 70078-782
kontakt@business-filemanager.de