Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info 19. Jahrgang, Heft 3, September 2019

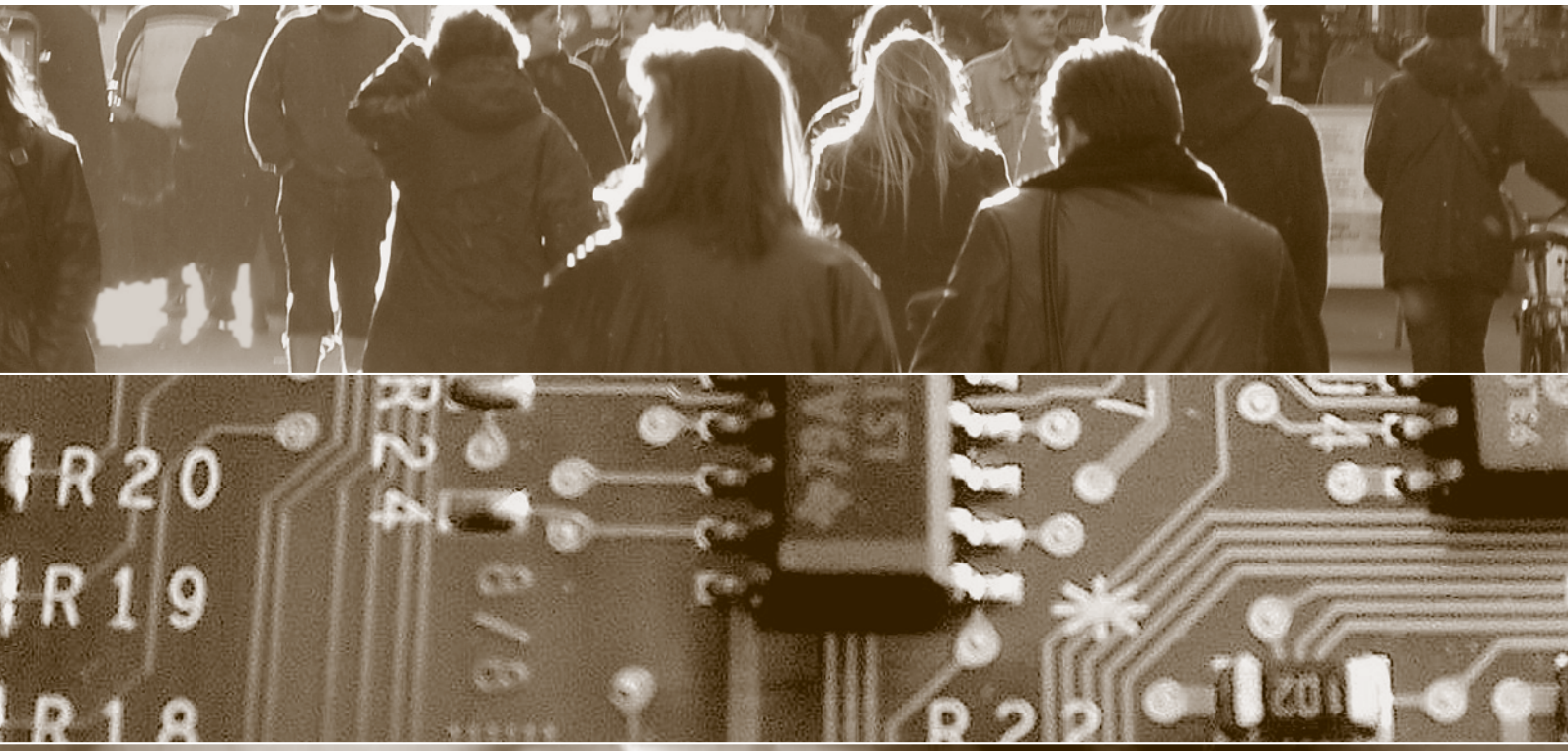
Schwerpunkt:

Auftragsdatenbearbeitung und Verantwortung

fokus: Verschlüsselung in der Cloud

report: Betrugserkennung auf Immobilienportalen

report: Schengen-Evaluation: Kopf in den Sand stecken?



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth
David Vasella

Schulthess §

inhalt

fokus

Schwerpunkt:
Auftragsdatenbearbeitung und Verantwortung

Auftragsbearbeitung im Privatbereich

Wie ist bei arbeitsteiliger Datenbearbeitung die Verantwortung zuzuordnen? Wie unterscheiden sich die Rollen des Verantwortlichen (allenfalls der gemeinsam Verantwortlichen) von jener des Auftragsdatenbearbeiters? Viele Fragen in diesem Umfeld sind noch wenig geklärt.

Wenn die Rechtsauslegung «nebulös» wird

Die (Informations- und) Datenschutze enthalten Regelungen für die Auftragsdatenbearbeitung. Wenn dann noch Cloud-Technologie verwendet werden soll, wie sind die zusätzlichen oder akzentuierten Cloud-Risiken durch spezifische Massnahmen zu vermeiden oder zu reduzieren?

Verschlüsselung in der Cloud

Bei Cloud-Diensten bietet sich Verschlüsselung als Schutzmassnahme an. Nur: Was meint «Verschlüsselung»? Welchen Schutz bringen die verschiedenen Verschlüsselungslösungen? Was taugen neue Ansätze wie Hardware-basierte sichere Ausführungsumgebungen oder homomorphe Verschlüsselung? Und wie steht es mit der Langzeitverschlüsselung?

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Prof. Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. (em.) Dr. iur. Rainer J. Schweizer, Prof. Dr. Günter Karjoth, Dr. iur. David Vasella

Redaktion: Dr. iur. Bruno Baeriswyl und Prof. Dr. iur. Beat Rudin

Rubrikenredaktor(inn)en: Dr. iur. Barbara Widmer, Dr. iur. Dominika Blonski

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, redaktion@digma.info

Erscheinungsplan: 4-mal jährlich (März, Juni, September, Dezember)

Bezugsbedingungen: Jahresabonnement: CHF 178.00 (für Studierende: CHF 98.00), Einzelheft: CHF 48.00, zzgl. Versandkosten. Alle Abo-Preise inkl. 2,5% MWST, zzgl. Versandkosten von CHF 6.00 innerhalb der Schweiz (Versandkosten für Lieferung ins Ausland: CHF 31.00). Studentenpreis gegen Vorlage eines gültigen Nachweises. Abonnementkündigungen sind mit einer Frist von 8 Wochen zum Ende des berechneten Bezugsjahres möglich.

Anzeigenverkauf und -beratung: Fachmedien Zürichsee Werbe AG, Laubisrütistrasse 44, CH-8712 Stäfa, Tel. +41 (0)44 928 56 17, marc.schaettin@fachmedien.ch

Verlag und Kundenservice: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach 2218, CH-8021 Zürich
Tel. +41 (0)44 200 29 29, Fax +41 (0)44 200 29 28, service@schulthess.com, www.schulthess.com

Betrugserkennung auf Immobilienportalen

Unter der Vielzahl von Anzeigen auf Immobilienportalen befinden sich auch Betrugsinserate. Wie kann man diese unter verschleierter Identität erstellten Inserate automatisch erkennen?

Den (Kantons-) Kopf in den Sand stecken?

Die Empfehlungen zu den bei der Schengen-Evaluation 2018 festgestellten Mängeln sind publiziert. Wäre es gescheit von den Kantonen, jene Empfehlungen nicht zu beachten, welche nur die Datenschutzaufsicht des Kantons Luzern direkt ansprechen? Die nächste Schengen-Evaluation kommt bestimmt und die Prüfpunkte werden dieselben sein.

Der Verwaltungsrat in der Pflicht

Die Nichteinhaltung von Datenschutzvorgaben kann – zurzeit mindestens dann, wenn das Datenbearbeiten durch ein Schweizer Unternehmen unter die DSGVO fällt – Bussen zur Folge haben. Geht das den Verwaltungsrat etwas an?

Outsourcing

Tja, Outsourcing hat so seine Tücken, weiss unser Cartoonist.

report

forum

Verschlüsselung in der Cloud

Möglichkeiten, Perspektiven und Grenzen der IT-Sicherheit aus kryptografischer und technischer Sicht

Michael Herfert, Dipl.-Inform., Abteilungsleiter Cloud-Computing, Identity and Privacy, Fraunhofer-Institut für Sichere Informationstechnologie, Darmstadt, Deutschland michael.herfert@sit.fraunhofer.de

Benjamin Lange, Dr. Dr., wissenschaftlicher Mitarbeiter in der Abteilung Cloud-Computing, Identity and Privacy, Fraunhofer-Institut für Sichere Informationstechnologie, Darmstadt, Deutschland benjamin.lange@sit.fraunhofer.de

Können personenbeziehbare Daten und andere vertrauliche Informationen vor unbefugten Zugriffen durch Verschlüsselung geschützt werden?

Die Kernidee von Cloud-Computing besteht in der Auslagerung einer IT-Infrastruktur zu einem – üblicherweise kommerziellen – Cloud-Anbieter mit dem Ziel, Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung bereitzustellen, um Ressourcen zu bündeln. Durch die Vielzahl der Anwendungsmöglichkeiten einer Cloud nehmen Cloud-Angebote stetig zu. Fast jedes Endgerät in unserer digitalen und vernetzten Welt verfügt über eine optionale Cloud-Anbindung, egal ob Smartphone, Tablet oder Fitness-Armband. Die Daten, die bei der Verwendung und Vernetzung solcher Endgeräte anfallen können, sind heterogen. Im Falle der Fitnessarmbänder werden sogar medizinische Daten in die Cloud übertragen. Werden diese Daten analysiert, erlauben sie die Konstruktion eines Anwenderprofils: Auffälligkeiten im Puls können auf Herzprobleme, Einschlafschwierigkeiten auf psychische Schwierigkeiten hindeuten. Es ist offensichtlich, welche Einschnitte in die Privatsphäre und in das Recht der informationellen Selbstbestimmung eines Anwenders eine böswillige, nicht autorisierte oder nicht zweckmässige Verarbeitung dieser Daten zur Folge hat.

Neben Privatpersonen nutzen auch Firmen immer mehr Cloud-Angebote. Sie übertragen intellektuelles Eigentum, das möglicherweise über Jahre hinweg erarbeitet wurde, in die Cloud. Auch börsenrelevante Informationen über eine geplante Fusion zweier Unternehmen sind sehr schützenswert. Human-Resources-Management-Systeme zur Verwaltung von Personaldaten gehen grundsätzlich mit sehr sensiblen personenbeziehbaren Daten um. Der Schutzbedarf der Daten ist evident. In diesem Beitrag soll untersucht werden, wie dieser sich durch technische, nicht durch juristische bzw. vertragliche Möglichkeiten erfüllen lässt.

Schutz durch Verschlüsselung

Technische Möglichkeiten zum Schutz der Daten sind immer mit einer Verschlüsselung verknüpft. Dabei ist zunächst zu unterscheiden, in welcher Phase Daten verschlüsselt sein sollen:

- erstens auf dem Transportweg vom und zum Cloud-Anbieter,
- zweitens während der Speicherung beim Cloud-Anbieter und
- drittens während der Verarbeitung durch den Cloud-Anbieter.

Im Optimalfall wären die Daten über alle drei Phasen hinweg verschlüsselt. Der Transportweg ist durch das *Transport-Layer-Security-Protokoll (TLS)*, das seit vielen Jahren benutzt wird und das intensiv untersucht wurde, als gut abgesichert zu betrachten. Bei den beiden anderen Phasen ist zu unterscheiden, wer Einblick in die Klartextdaten nehmen kann. Bei einer serverseitigen Verschlüsselung in der zweiten Phase besitzt der Server die für den Klartext notwendigen Schlüssel. Bei einer clientseitigen Verschlüsselung während der dritten Phase werden die Daten durch den Cloud-Kunden derart verschlüsselt, dass der Cloud-Anbieter serverseitig keinen Einblick mehr nehmen kann.

Eine serverseitige Verschlüsselung ist durchaus sinnvoll, denn sie reduziert die Angriffsfläche. Beispielsweise sorgt eine verschlüsselte Festplatte dafür, dass ein Dieb mit den Daten nichts anfangen kann. Auch ist es möglich, durch ein Schlüsselmanagement festzulegen, welche Mitarbeiter und welche Systeme auf welche Daten zugreifen dürfen.

Eine serverseitige Verschlüsselung ist technisch einfacher umzusetzen, hat aber eine Reihe von Nachteilen: Niemand weiss, mit wem dieser Cloud-Anbieter in Zukunft vielleicht fusionieren oder von wem er möglicherweise auf-

gekauft wird. Behördliche Stellen können Zugriff auf die Klartextdaten verlangen, möglicherweise auch auf Basis ausländischen Rechts. Es ist nicht ausgeschlossen, dass Innentäter Zugriff auf die Klartexte erhalten. Nach Aussagen von Microsoft geht ein hoher Teil von Angriffen darauf zurück, dass Schlüsselmaterial oder Administrator-Accounts kompromittiert werden[1]. Auch eventuell vorhandene Schadsoftware, die trotz professioneller Wartung möglicherweise Eingang in die Serverseite fand, hat prinzipiell die Möglichkeit, auf Klartexte zuzugreifen.

Cloud-Anbieter versuchen stets, ihre Ressourcen aus Gründen der Effizienz zu bündeln und mehreren Kunden zur Verfügung zu stellen. Sollte die Abschottung der Kundenkontexte fehlerhaft oder Ziel eines Angriffes sein, könnten Klartexte von einem Kunden zum anderen fliessen. Schliesslich erfordert eine Verarbeitung von Klartextdaten immer ein Vertrauen in den Anbieter, das deutlich über das Vertrauen für die Gewährleistung von Schutzzielen wie Verfügbarkeit, Integrität und Authentizität hinausgeht.

Am sichersten ist es also, wenn die Daten clientseitig verschlüsselt werden. Dabei entsteht jedoch das Problem, wie der Cloud-Anbieter verschlüsselte Daten verarbeiten soll. Wie soll er die Rechtschreibung eines Textes überprüfen, wenn die Inhalte verschlüsselt sind? Wir unterscheiden zunächst zwischen Cloud-Speicherdiensten auf der einen und allen anderen Cloud-Diensten auf der anderen Seite.

Cloud-Speicherdienste

Cloud-Speicherdienste haben die primäre Aufgabe, Daten zu speichern und sie auf Anfrage wieder herauszugeben (Kopierfunktion). Einige Dienste können darüber hinaus Daten versionieren (Backup-Funktion) und sie zwischen verschiedenen Geräten eines Nutzers abgleichen (Synchronisierungsfunktion). Schliesslich können einige von ihnen auch Daten zwischen verschiedenen Nutzern teilen (Kooperationsfunktion). Neben dezidierten Speicherdiensten, von denen Dropbox der bekannteste ist, werden Speicherdienste auch von Anbietern verschiedener Endgerät-Betriebssysteme bereitgestellt, um Kundendaten zu speichern.

Allen Cloud-Speicherdiensten ist gemein, dass Daten nicht inhaltlich verarbeitet werden. Für Cloud-Speicherdienste ist eine gute Lösung zur Verschlüsselung seit vielen Jahren möglich, indem die Daten auf der Clientseite verschlüsselt werden, bevor sie über einen ebenfalls verschlüsselten Kanal zum Cloud-Anbieter übertragen werden. Diese Art der Verschlüsselung kann mit symmetrischen Verschlüsselungsalgorithmen umgesetzt werden. Symmetrische Algorithmen sind effizienter zur Verschlüsselung grosser Datenmengen und benötigen im Gegensatz zu asymmetrischen Verfahren nur einen Schlüssel zum Ver- und Entschlüsseln. Somit ist auch eine Public-Key-Infrastruktur, die aufwändig umzusetzen wäre, nicht notwendig.

Technisch lässt sich clientseitige Verschlüsselung leicht umsetzen, die Methoden dazu sind allgemein bekannt, Programmbibliotheken sind als Open Source kostenlos verfügbar. Die Anforderungen sind also gering. Umso verwunderlicher ist, dass nur sehr wenige Dienste von clientseitiger Verschlüsselung Gebrauch machen. Daran hat sich in den letzten sieben Jahren wenig geändert[2]. Zu den Gründen dafür zählen ein zu gering ausgeprägtes Verlangen der Nutzer nach Vertraulichkeit und der ökonomische Vorteil, den der Cloud-Anbieter aus unverschlüsselten Daten ziehen kann. Durch die gemeinsame Nutzung von Speicherplatz durch mehrere Kunden ist es wahrscheinlich, dass Daten durch unterschiedliche Kunden redundant in die Cloud verschoben werden. Liegt ein Duplikat vor, kann ein Cloud-Anbieter das erkennen und speichert die Datei nur einmal ab, belastet aber das Volumen jedes Kunden. Dieses Verfahren der Deduplikation ist nicht mehr anwendbar, wenn Daten individuell verschlüsselt werden.

Viele Cloud-Anbieter geben an, Daten stets verschlüsselt im Massenspeicher abzulegen, also eine serverseitige Verschlüsselung vorzunehmen. Das ist durchaus sinnvoll, da dadurch die Angriffsfläche reduziert wird. Das Schutzniveau einer clientseitigen Verschlüsselung wird dadurch aber nicht erreicht.

Dominik Spychalski, MSc., wissenschaftlicher Mitarbeiter in der Abteilung Cloud-Computing, Identity and Privacy, Fraunhofer-Institut für Sichere Informationstechnologie, Darmstadt, Deutschland
dominik.spychalski@sit.fraunhofer.de

Kurz & bündig

Ob zum Auslagern von Speicherplatz oder Rechenleistung, Cloud-Dienste sind seit Jahren etabliert und setzen Vertrauen in den Anbieter voraus. Für Speicherdienste existieren Lösungen, die Daten eines Kunden vor ihrer Auslagerung in die Cloud verschlüsseln, wodurch sie in allen Phasen ihres Lebenszyklus geschützt sind. Trotz der Verfügbarkeit werden die Techniken in der Praxis nur selten eingesetzt. Im Kontext von Datenbanken werden Informationen bereits ausserhalb ihrer Verarbeitung verschlüsselt. Soll ein durchgängiger Schutz in einem Szenario etabliert werden, das eine Datenverarbeitung in der Cloud vorsieht, sind neue Ansätze wie Hardware-basierte sichere Ausführungsumgebungen wie Intel SGX oder homomorphe Verschlüsselung notwendig. Letztere ist durch ihre hohe Komplexität jedoch noch nicht praxistauglich. Auch die Langzeitverschlüsselung von Daten in der Cloud ist ein weitgehend ungelöstes Problem.

Verarbeitende Cloud-Dienste

Den Cloud-Speicherdiensten gegenüber stehen Dienste, die Daten direkt in der Cloud verarbeiten. Im Folgenden werden drei typische Beispiele von verarbeitenden Cloud-Diensten beleuchtet.

Ein Schwachpunkt besteht darin, dass Daten während der Verarbeitung stets in unverschlüsselter Form vorliegen müssen und damit aus dem Cloud-Netzwerk des Dienstanbieters im Klartext sichtbar sind.

Cloud-basierte Office-Anwendungen

Eine klassische Domäne von verarbeitenden Cloud-Diensten sind Cloud-basierte Office-Anwendungen wie etwa Microsoft *Office 365*, *Apple iWork* oder *Google G Suite*. Neben der Bereitstellung von Cloud-Speicher zur Ablage von Dokumenten werden dabei häufig webbasierte Office-Applikationen oder mobile Office-Anwendungen angeboten, die direkt in der Cloud ausgeführt werden. Mögliche Dienste sind ausserdem Austausch-Plattformen oder Messenger-Dienste. Die in Cloud-basierten Office-Anwendungen eingesetzten Verschlüsselungstechniken sind häufig ähnlich konzipiert und werden nun am Beispiel von Microsoft Office 365 erläutert.

Eine Verschlüsselung von Daten erfolgt in Office 365 auf den Transportwegen zwischen Gerät bzw. Rechenzentrum des Kunden und dem Cloud-Anbieter. Daneben werden Daten auch verschlüsselt, wenn sie im Cloud-Speicher abgelegt werden. Für den Schutz der gespeicherten Daten verwendet Microsoft eine Methode der Verschlüsselung, die auch bei Cloud-Storage-Providern beliebt ist[3]: Die Daten werden durch die sogenannte hybride Verschlüsselung mit zwei verschiedenen Verschlüsselungssystemen geschützt[4]. Zunächst werden die eigentlichen Nutzdaten mit einem *Datenverschlüsselungsschlüssel (DVS)* symmetrisch verschlüsselt[5] und zusammen mit diesem Schlüssel im Cloud-Speicher abgelegt. Da ein Zugang zum DVS gleichzeitig eine Entschlüsselung der Daten möglich machen würde, wird dieser mit einem zweiten Verfahren unter Verwendung eines *Schlüsselverschlüsselungsschlüssels (SVS)* verschlüsselt und ist damit nur für solche zugänglich, die den SVS kennen. Der SVS wird in einer speziell geschützten Umgebung aufbewahrt[6] und ist nur für besonders privilegierte Administratoren und Nutzer zugänglich. Gelegentlich ist der Ablageort so konzipiert, dass nicht einmal der Cloud-Provider selbst diesen Schlüssel aus der gesicherten Umgebung extrahieren oder einsehen kann.

Obwohl diese Vorgehensweise suggeriert, dass der Cloud-Anbieter keinerlei verschlüsselte Daten im Klartext einsehen kann, ist dies nicht der Fall: Da jeder Vorgang der Ver- und Entschlüsselung von Daten in den Datenzentren des Dienstanbieters durchgeführt wird, hat dieser zwangsläufig Zugriff auf die verwendeten Datenverschlüsselungsschlüssel (DVS) sowie auf die unverschlüsselten Daten selbst.

Ein weiterer Schwachpunkt besteht darin, dass Daten während der Verarbeitung stets in unverschlüsselter Form vorliegen müssen[7] und damit aus dem Cloud-Netzwerk des Dienstanbieters im Klartext sichtbar sind. Sollte der Cloud-Provider oder eine andere Partei mit Zugang zum internen Netzwerk des Cloud-Providers diese Schlüssel und/oder Daten im Klartext einsehen, kopieren oder weitergeben, so könnte dies in einer Weise geschehen, von der der Kunde nichts mitbekommt. Dies ist nicht nur deshalb problematisch, weil ein Angreifer von aussen in das Netzwerk des Cloud-Providers einbrechen und sich damit Zugang zu den Daten verschaffen könnte, sondern weil sich auch Administratoren (mit Absicht oder aus Unachtsamkeit) sowie staatliche Stellen

Literatur, weiterführende Links

- Bundesamt für Sicherheit in der Informationstechnik (2019), Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI TR-02102-1, Version 2019-01.
- Costan Victor/Devadas Srinivas (2016), Intel SGX Explained. IACR Cryptology ePrint Archive 2016.086, 1–118.
- Borgmann Moritz/Hahn Tobias/Herfert Michael/Kunz Thomas/Richter Marcel/Viebeg Ursula/Vowé Sven (2012), On the Security of Cloud Storage Services. Fraunhofer Verlag, <https://www.sit.fraunhofer.de/de/cloud-security>.
- Kraft Reiner/Weber Frank/Marx Ronald/Stöwer Mechthild/Grosse-Onnebrink Hubert/Larbig Pedro/Oberle Alexander (2015), Vertraulichkeitsschutz durch Verschlüsselung. Strategien und Lösungen für Unternehmen. Fraunhofer Verlag.
- Kogos Konstantin G./Filippova Kseniia S./Epishkina Anna V. (2017), Fully Homomorphic Encryption Schemes: the State of The Art. IEEE Xplore 2017, 463–466.
- Odun-Ayo Isaac/Misra Sanjay/Omoregbe Nicolas/Onibere Emmanuel/Bulama Yusuf/Damasevičius Robertast (2017), Cloud-Based Security Driven Human Resource Management System. Advances in Digital Technologies, IOS Press, 96–106.
- Oracle, Oracle E-Business Suite HCM. Data Privacy-challenges and Solutions. Oracle White Paper 2010.
- Patterson David A./Gibson Garth/Katz Randy H. (1988), A case for redundant arrays of inexpensive disks (RAID). Proceedings of the 1988 ACM SIGMOD international conference on Management of data (SIGMOD '88), ACM, 109–116.

über interne Berechtigungen Zugang zu den Daten verschaffen könnten.

Trotz der Verwendung einer Verschlüsselung in der Transport- und Speicherphase sind Daten somit während der Ver- und Entschlüsselung sowie während der Verarbeitung stellenweise ungeschützt und nicht vor einem unberechtigten Zugriff aus dem Netzwerk des Cloud-Anbieters sicher.

Human-Resources-Management-Software

Ein weiteres Anwendungsszenario für verarbeitende Cloud-Dienste sind *Human-Resources-Management-Systeme (HRMS)*. Häufig werden diese in die Cloud ausgelagert, um grosse Mengen von Personaldaten kostengünstig, zentralisiert und effektiv verwalten und damit auf eine lokale Administration verzichten zu können. Damit liegen jedoch sehr sensible persönliche Daten unter der Hoheit eines Cloud-Dienstanbieters. Während viele HRMS-Anbieter gar keine Verschlüsselung anbieten[8], verwenden andere Anbieter bereits eine Verschlüsselung sowohl für die Transport- als auch für die Speicherphase. Eine solche Verschlüsselung sichert die von einem Unternehmen zum HRMS-Anbieter übertragenen Daten während des Transportweges und während der Ablage in der Cloud vor externen Angriffen, etwa aufgrund von Datendiebstahl[9]. Ferner kann durch organisatorische Massnahmen wie Zugriffskontrolle oder Audits die Gefahr von internen Angreifern reduziert werden. Eine verschlüsselte Verarbeitung wird dabei jedoch noch nicht angewandt.

Datenbankanwendungen

Innerhalb eines Informationsverbundes werden Datenbanken *(Datenbank-Management-Systeme, DBMS)* zum zentralen Aufbewahren und Organisieren von Daten, die aus beliebigen Informationssystemen stammen können, eingesetzt. Das Auslagern einer Datenbankinstanz in die Cloud bietet vor allem Vorteile in den Bereichen Wirtschaftlichkeit und Ressourceneffizienz, jedoch auch Gefahren in Sachen Sicherheit und Datenschutz. Datenbankhersteller wie Microsoft, IBM und Oracle z.B. führten für ihre Produkte unter anderem den Mechanismus der *transparenten Datenverschlüsselung (Transparent Data Encryption, TDE)* ein, welche eine Verschlüsselung der gesamten Datenbank auf Dateiebene erlaubt. TDE schützt die Daten durch eine ergänzende Sicherheitsschicht um eine AES-Verschlüsselung in ihrer Ruhephase, nicht jedoch während ihres Transports oder ihrer Verwendung. Die Ver- und Entschlüsselung der Daten erfolgt transparent gegenüber den konsumierenden Anwendungen.

Werden die Daten zu ihrer Verwendung entschlüsselt und in den Arbeitsspeicher geladen, können Plattform- und Datenbankadministratoren sowie alle Anwendungen oder Rollen mit entsprechenden Rechten und Zugriff auf das DBMS die Daten im Klartext einsehen. Enthält eine Datenbank vertrauliche Informationen, sind diese auch gegenüber dem Cloud-Anbieter und seinen Angestellten zu schützen. Microsoft bietet aus diesem Grund für SQL-Server im Rahmen von *Microsoft Confidential Computing* an, dass ganze Datenbankspalten mit sensiblen Inhalten auch im Arbeitsspeicher zur Verarbeitung verschlüsselt vorgehalten werden können und somit auch für den Cloud-Anbieter nicht einsehbar sind. Der Schutz der Daten erfolgt dabei über die Intel-SGX-Erweiterung für Intel-Prozessoren und ihre sichere Ausführungsumgebung.

Werden die Daten zu ihrer Verwendung entschlüsselt und in den Arbeitsspeicher geladen, können Plattform- und Datenbankadministratoren sowie alle Anwendungen oder Rollen mit entsprechenden Rechten und Zugriff auf das DBMS die Daten im Klartext einsehen.

Schutz während der Verarbeitung

Intel Software Guard Extensions (SGX)

Intel SGX[10] ist eine Befehlssatzerweiterung der Intel-Prozessorarchitektur, welche als Trusted Execution Environment (TEE) vertrauenswürdige Berechnungen in einer potenziell nicht vertrauenswürdigen Umgebung ermöglicht. Intel SGX gewährleistet die Schutzziele Vertraulichkeit und Integrität, auch dann, wenn der gesamte höherprivilegierte Softwarestack möglicherweise kompromittiert wurde. Intel SGX lagert sicherheitskritische Berechnungen in *Enklaven* aus. Enklaven sind geschützte Speicherbereiche innerhalb des Adressraums des Prozessors und beinhalten neben dem Programmcode auch die den Berechnungen zugrunde liegenden Daten. Um die Schutzmechanismen von Intel SGX nutzen zu können, müssen Anwendungen auf die SGX-Architektur portiert werden. Eine SGX-Anwendung besteht aus einem nicht vertrauenswürdigen Teil, betrieben auf dem Host-System, und einem vertrauenswürdigen Teil, betrieben in einer Enklave. Innerhalb einer Enklave anfallende Daten während des Berechnungsprozesses (Ursprungsdaten, Zwischen- und Endergebnisse) verlassen diese niemals im Klartext. Terminiert

eine Enklave, werden die Daten entweder gelöscht oder für eine zukünftige Verwendung über den *Data Sealing*-Mechanismus verschlüsselt auf die Festplatte geschrieben.

Neben Data Sealing unterstützt SGX auch den Mechanismus der *Attestierung*. Die Attestierung dient der Bescheinigung der Integrität sowie des ordnungsgemässen Betriebs einer Enklave auf einer validen SGX-Plattform gegenüber anderen Enklaven (*local attestation*) oder gegenüber entfernten Dritten *(remote attestation*). Intel SGX ist eine recht junge Technologie, die in der Vergangenheit Ziel erfolgreicher kryptografischer Angriffe wie *Foreshadow* oder *ZombieLoad* war. Berichte über erfolgreiche auf Produktivsystemen ausgeführte Angriffe existieren jedoch nicht.

Homomorphe Verschlüsselung

Eine mögliche Alternative zu geschützten Ausführungsumgebungen ist die Verwendung einer vollständig verschlüsselten Verarbeitung durch Techniken homomorpher Verschlüsselung. Diese Art der Verschlüsselung macht es möglich, einfache Berechnungen auf Daten in verschlüsselter Form durchzuführen und dabei dasselbe Ergebnis zu erhalten, das bei einer Berechnung in unverschlüsselter Form und anschliessender Verschlüsselung des Ergebnisses entstanden wäre. Homomorphe Verschlüsselung ist ein bahnbrechender und vielversprechender Ansatz in der geschützten Verarbeitung von Cloud-Daten, jedoch von einer für die Verwendung in komplexen verarbeitenden Cloud-Diensten notwendigen Praxisreife noch weit entfernt[11].

Der Schutz verschlüsselter Daten lässt im Laufe der Zeit nach. So bleibt zurzeit nur, den Transfer von Daten mit langem Schutzbedarf in die Cloud sehr gut zu überlegen.

Grenzen der Verschlüsselung

Der Schutz verschlüsselter Daten lässt im Laufe der Zeit nach. Symmetrische Algorithmen sind durch die zunehmende Rechnerleistung gefährdet, insbesondere durch Spezialhardware und die zunehmende Vernetzung vieler Rechner. Beide Gefährdungen machen die Erfolgsaussichten einer Brute-Force-Attacke, die einfach alle möglichen Schlüssel testet, zunehmend wahrscheinlicher. Dieselbe Bedrohung trifft auch die asymmetrischen Algorithmen. Sie basieren auf schwierigen mathematischen Referenzproblemen, wie beispielsweise dem Faktorisierungsproblem. Bei ihnen besteht darüber hinaus die Gefahr einer Schwächung durch mathematische Kryptoanalyse. Es ist unwahrscheinlich, dass das einem Kryptosystem zugrunde liegende Referenzproblem vollständig gelöst wird. Jedoch ist es unvorhersehbar, inwieweit der zu testende Schlüsselraum in Zukunft einzugrenzen ist, um effizienter an die Klartexte zu gelangen. Das *Bundesamt für Sicherheit in der Informationstechnik (BSI)* sieht es als schwierig an, eine Prognose für die Sicherheit kryptografischer Algorithmen zu erstellen, die einen Zeitraum von sieben Jahren übersteigt[12].

Im Kontext der Cloud hilft es nicht, Daten später mit einem neuen Algorithmus und neuen Schlüsseln erneut zu verschlüsseln, denn die vormals verschlüsselten Daten sind weiterhin vorhanden.

Bei Ablage verschlüsselter Daten in der Cloud sollte also immer der Zeitraum der Vertraulichkeit bedacht werden. Staatliche Dokumente können einen Schutzbedarf von 60 Jahren haben[13], in Sonderfällen sogar noch mehr. Gesundheitsdaten sollten über die Lebenszeit hinweg vertraulich bleiben. In der Schweiz sind das für die 2018 Geborenen mehr als 80 Jahre[14]. Für diese Fristen kann heute niemand eine Gewähr übernehmen.

Bei Cloud-Storage-Diensten würde es helfen, die verschlüsselten Daten auf *n* (z.B. 5) Dienste zu verteilen, von denen *m* (z.B. 3) ausreichen, die Daten zu rekonstruieren. Unter der Voraussetzung, dass die Dienste nicht regelwidrig kooperieren und nicht fusionieren, liesse sich durch die verteilte Speicherung die Sicherheit erhöhen. Die Algorithmen dazu sind vorhanden und im Bereich von Festplatten in Form von RAID-Anordnungen schon lange in Gebrauch[15]. In der Praxis spielen solche Konstruktionen aber zurzeit kaum eine Rolle.

Bei verarbeitenden Diensten sind Lösungen für Cloud-übliche Anwendungen über *abgesicherte Mehrparteienberechnungen (Secure Multi Party Computation)* noch sehr weit entfernt.

So bleibt zurzeit nur, den Transfer von Daten mit langem Schutzbedarf in die Cloud sehr gut zu überlegen.

Fazit

Bei Cloud-Speicherdiensten lassen sich Daten so verschlüsseln, dass der Cloud-Anbieter keinen Einblick nehmen kann. Die Techniken dazu sind einfach umzusetzen, Programmbibliotheken sind vorhanden. Eine verstärkte Nachfrage der Nutzer nach solchen Lösungen könnte hier einen deutlichen Fortschritt erzeugen.

Bei verarbeitenden Cloud-Diensten ist eine durchgängige Verschlüsselung zurzeit nicht möglich, insbesondere lassen sich Office-Anwendungen nicht so betreiben, dass die Daten durchgängig vor einer Einblicknahme geschützt sind.

Die Kryptografie stellt mit der homomorphen Verschlüsselung ein Verfahren bereit, das prinzipiell in der Lage ist, beliebige Berechnungen auf verschlüsselten Daten durchzuführen, das aber noch Jahre von einem Einsatz in gängigen Cloud-Applikationen entfernt ist.

Auf der Hardwareseite hat Intel mit SGX eine interessante Technologie entwickelt, bei der Operationen im Innern des Prozessors auf Klartexten durchgeführt werden, die Klartexte aber niemals unverschlüsselt den geschützten Speicher des Prozessors verlassen. Zurzeit gibt es relevante Angriffe auf die noch recht neue Technologie. Sie hat ausserdem das Problem, dass sehr komplexe Programme, die viele Programmbibliotheken einbinden und viele Aufrufe in das Betriebssystem machen, zumindest vorläufig nicht umsetzbar sind. Es bleibt aber spannend, diese Technologie zu beobachten.

Allen Verschlüsselungslösungen ist gemein, dass die Schutzkraft kryptografischer Algorithmen im Laufe der Zeit nachlässt. Schon bei einem Schutzzeitraum, der sieben Jahre übersteigt, lässt sich nicht mehr garantieren, dass er aufrechterhalten werden kann. Vor einem Transfer von Daten in die Cloud sollte der Cloud-Kunde analysieren, wie sensibel die Daten sind und wie lange der Schutz aufrechterhalten werden muss.

Beim Schutzziel der Verfügbarkeit ist zu bedenken, dass die Verfügbarkeit auch durch behördliche Vorgaben aus dem Rechtsraum des Cloud-Anbieters beeinflusst werden kann.

Neben dem Schutzziel der Vertraulichkeit, das im Fokus dieses Beitrags steht, gibt es noch weitere Schutzziele, die ein Cloud-Anbieter erfüllen sollte. Dazu gehört insbesondere das Schutzziel der Verfügbarkeit. Hierbei ist zu bedenken, dass die Verfügbarkeit auch durch behördliche Vorgaben aus dem Rechtsraum des Cloud-Anbieters beeinflusst werden kann. ■

Fussnoten

1 Siehe dazu <https://azure.microsoft.com/en-us/blog/introducing-azure-confidential-computing/>.
2 Borgmann/Hahn/Herfert/Kunz/Richter/Viebeg/Vowé (2012), 12.
3 Vgl. die Übersicht unter <https://cloudarchitectmusings.com/2018/03/09/data-encryption-in-the-cloud-part-4-aws-azure-and-google-cloud/>.
4 Siehe dazu die über <https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-azure-encryption> und die in den verlinkten Dokumentationen bereitgestellten Informationen.
5 Dies geschieht unter Verwendung eines symmetrischen Verschlüsselungssystems, z.B. AES.
6 Dazu wird häufig ein Hardware-Security-Modul (HSM) verwendet, das den Schlüssel vor physischen und softwarebasierten Angriffen schützt.
7 Dies ist der Regelfall für die verarbeitenden Cloud-Dienste und dadurch bedingt, dass Methoden einer geschützten Verarbeitung technisch noch nicht für komplexe Cloud-Dienste geeignet sind, siehe dazu unten zum Thema «Schutz während der Verarbeitung».
8 Odun-Ayo/Misra/Omoregbe/Onibere/Bulama/Damasevičius (2017), 103.
9 Oracle (2010), 10. Vgl. ferner <https://www.hrcloud.com/blog/how-hr-cloud-secures-your-data>.
10 Siehe zu Intel SGX die Dokumentation von Costan/Devadas (2016).
11 Vgl. Kraft/Weber/Marx/Stöwer/Grosse-Onnebrink/Larbig/Oberle (2015), 23; Kogos/Filippova/Epishkina (2017), 466. Vgl. ferner die Einschätzung des Kryptografen Bruce Schneier, der sogar bezweifelt, dass homomorphe Verschlüsselung jemals für eine breite Anwendung praktikabel wird (<https://www.schneier.com/blog/archives/2019/07/google_releases_1.html>).
12 Bundesamt für Sicherheit in der Informationstechnik (2019), 16.
13 Bundesarchivgesetz, § 11 Abs. 3.
14 Männer 81,7 Jahre, Frauen 85,4 Jahre. Quelle: <https://www.bfs.admin.ch/bfs/de/home/statistiken/bevoelkerung/geburten-todesfaelle/lebenserwartung.html>.
15 Siehe dazu Patterson/Gibson/Katz (1988).

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement **digma** (4 Hefte des laufenden Jahrgangs) à **CHF 178.00**
(Versandkosten: Schweiz inklusive)

Name Vorname

Firma

E-Mail

Strasse/Nr.

PLZ Ort

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8001 Zürich
Telefon +41 44 200 29 29
Telefax +41 44 200 29 28
E-Mail: zeitschriften@schulthess.com
Homepage: www.schulthess.com

Schulthess §