Fernzugriff aus dem Ausland

Wenn die Wartung zur Spionagefalle wird

Der Beizug von Dritten für die Erbringung von IT-Dienstleistungen wird jedes Jahr wichtiger und ist kaum mehr wegzudenken. Im Zeitalter der hybriden IT-Infrastrukturen sind, oft ergänzend zur nach wie vor grossen Zahl von internen IT-Applikationen («on premise»), nun zunehmend die Cloud-Applikationen auf dem Vormarsch.

Christian Laux und Claudio Fuchs

Anders als im Cloud-Umfeld ist der Fernzugriff auf on premise-Applikationen sehr wenig geregelt. Unter-nehmen tun gut daran, genau diese Lücke zu schliessen. In der Schweiz denkt man zuerst an Spitäler mit Patientendaten oder an Banken mit Kundendaten. Die Frage geht am Ende aber alle Unternehmen etwas an.

Beispiel 1: Ein Spital

Wenn Sie sich als Patient einem Arzt zuwenden, gehen Sie automatisch und zu Recht davon aus, dass er Ihre Krankenakte streng vertraulich behandelt und nicht gegenüber Dritten offenbart. Im Zuge der Digitalisierung hängt die Krankenakte nun nicht mehr physisch bei ihm in einem Aktenschrank, sondern ist digital gespeichert. Der Arzt darf Ihre Geheimnisse an seine Hilfspersonen weitergeben. Hilfsperson ist, wer den Arzt erlaubterweise in seiner Tätigkeit unterstützt. Dieser Vorgang ist rechtlich gesprochen keine Offenbarung. Folglich müssen Sie als Patient nicht über den Beizug der Hilfsperson informiert werden.

In der Praxis ist es aber so, dass ein Klinikinformationssystem, ein Radiologiesystem oder ein Laborsystem nicht allein durch das Spital gewartet werden und sich IT-Dienstleister, möglicherweise sogar aus dem Ausland, via Fernzugriff einloggen. Dabei sind oftmals – insbesondere in der Datenbank – alle Informationen der Patienten offen zugänglich. Die Frage ist nun: Wo «beginnt» das Spital, und wo «hört es auf»? Zur Umschreibung kann man den Begriff «Perimeter» verwenden. Der Begriff bezeichnet die äussere Abgrenzung der Organisationseinheit (hier: des Spitals), die es zu organisieren gilt. Es geht also um die Frage, wo der Perimeter des Spitals endet (Abb. 1).

Das Schweizer Strafgesetzbuch, Datenschutzgesetz oder Medizinalberufgesetz verbieten per se nicht, dass Hilfspersonen beigezogen werden. Der Beizug von Hilfspersonen resultiert somit nicht in einer Offenbarung gegenüber Dritten, auch wenn sie Klartextzugriff auf geschützte Informationen erhalten. Konsequent weitergedacht würde dies bedeuten, dass der Arzt den Kreis der Hilfspersonen theoretisch unbegrenzt ausdehnen könnte.

Der absolut entscheidende Punkt ist die Kontrolle. Es braucht Kontrolle über die «verlängerte Werkbank». Das Spital muss alle Hilfspersonen so einbinden, als wären sie Mitarbeitende (Bindung an Weisungen, etc.) und nicht Externe. Fehlt es an Kontrolle, führt der unbeschränkte Beizug von Hilfspersonen womöglich zu einer verbotenen Offenbarung.

Beispiel 2: Eine Bank

In einem Rechtsgutachten (Nutzung von Cloud-Angeboten durch Banken: Zur Zulässigkeit nach Art. 47 BankG)* wurde die Frage erläutert, ob eine Bank den personellen und physischen Perimeter soweit erweitern kann, dass Bankkundendaten in der Cloud oder von einem ausländischen IT-Dienstleister einge-sehen werden können. Das Fazit des Rechtsgutachtens bejaht dies, denn das seit 1934 geltende Bankengesetz wurde 1970 dahingehend ergänzt, um sich gegen «ausländische Spionage» zu schützen. In letzter Zeit ist einiges gegangen und seit 2017 übermittelt die Schweiz ja auch detaillierte Informationen über Bankkonten regelmässig ins Ausland.

Obwohl die Mitarbeitenden eines ausländischen IT-Dienstleisters strafrechtlich unter Umständen nicht belangt werden können, geht das Rechtsgutachten davon aus, dass die betreffenden Mitarbeitenden in die Risikosphäre der Bank eingebunden werden können, ohne dass eine Offenbarung gegenüber Dritten stattfindet (Abb. 2).

Die Bank erweitert den physischen und personellen Perimeter also dahingehend, dass das Rechencenter und die Mitarbeitenden des IT-Dienstleisters nicht mehr als Dritte angesehen werden können. Der entscheidende Punkt dabei ist, dass die Bank mittels technischer und organisatorischer Massnahmen die Kontrolle darüber behält. Damit darf eine Bank Applikationen in der Cloud verwenden oder auch ausländischen Mitarbeitenden Fernzugriff erlauben.

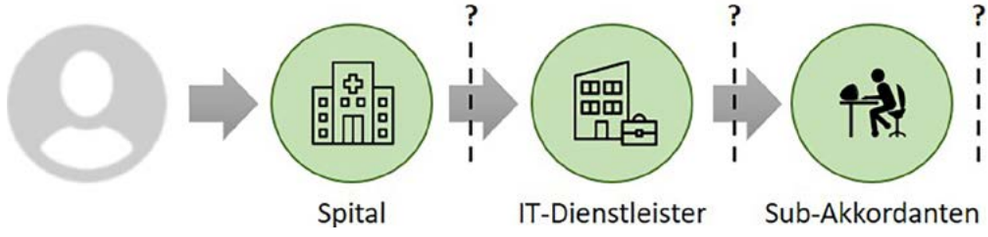

Abb. 1: Sachverhalt Outsourcing

Dr. iur. Christian Laux ist Rechtsanwalt bei Laux Lawyers AG. www.lauxlawyers.ch

Claudio Fuchs ist Managing Director Switzerland & Austria, IPG Group. www.ipg-group.com/de/

Alle anderen Branchen

Andere Branchen wie Handel oder Industrie unterliegen in der Schweiz nicht der gleichen Fülle von Gesetzgebungen, wie ein Spital oder eine Bank. Trotzdem gilt es die Daten zu schützen. Dabei muss es sich nicht um personenbezogene Daten handeln. Jedes Unternehmen hat Betriebsgeheimnisse, welche im Falle einer Offenbarung dem Unternehmen einen Schaden zufügen können. Dies kann ein Image-Schaden sein oder auch ein zukünftiger wirtschaftlicher Schaden aufgrund von Wirtschaftsspionage.

Diese Kontrolle der verlängerten Werkbank kann exakt gleich mit technischen und organisatorischen Massnahmen erfolgen, muss aber durch ein griffiges Vertragswerk unterstützt werden. Die in den Prozessen eingebunden Mitarbeitenden müssen über die Unternehmensgrenze von Dritten zu Beteiligten gemacht werden.

Was heisst nun Kontrolle?

Kontrolle muss ganzheitlich als stetiger Prozess verstanden werden. Zuerst muss man die Materie verstehen und dann müssen durch präventive Massnahmen die Risiken eines Datenverlusts reduziert werden. Weiter empfehlen wir durch Verbesserung der Nachvollziehbarkeit die Möglichkeiten von reaktiven Massnahmen zu erhöhen, um im Fall der Fälle Sanktionsmöglichkeiten ergreifen zu können. Beim

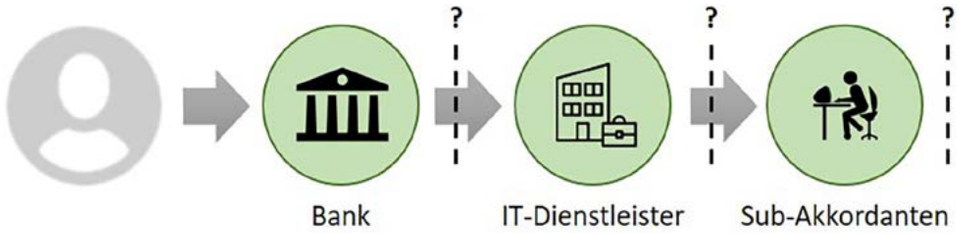

Abb. 2: Kontrollspanne einer Bank bei Beizug von Dritten

Thema Fernzugriff von IT-Dienstleistern, welche mit privilegierten Berechtigungen möglicherweise auf Ihre Daten zugreifen, empfiehlt es sich die folgenden organisatorischen und technischen Massnahmen anzuwenden:

- Schutzbedarfsanalyse über alle relevanten IT-Systeme durchführen
- Interne Weisungen für Zugang auf Daten (Access Management) aufsetzen
- Berechtigungs- und Rollenkonzepte für die exponierten IT-Systeme erstellen
- Die Verwaltung der Benutzer und Berechtigungen sauber regeln
- Benutzer von intern wie auch extern zur persönlichen Identifikation zwingen
- Passwörter privilegierter Accounts nach Gebrauch immer wechseln
- Die Session der Fernzugriffe und der Datentransfer protokollieren/aufzeichnen

Fernzugriffe, auch aus dem Ausland, auf kritische Daten sind rechtlich erlaubt. Die Risiken müssen allerdings gut kontrollierbar sein. Die Verantwortung liegt beim Unternehmen selbst. Zieht beispielsweise ein Spital Dritte in seine IT-Umgebung ein, behält das Spital die Verantwortung zum Schutz der Daten. Die Kontrolle muss jederzeit durch technische, organisatorische und vertragliche Massnahmen gewährleistet sein. ■

**https://www.lauxlawyers.ch/wp-content/uploads/2019/03/Cloud-und-Bankgeheimnis.pdf*

Accès à distance depuis l'étranger

D'année en année, le recours à des tiers pour la fourniture de services informatiques devient plus important et est devenu pratiquement incontournable. À l'ère des infrastructures informatiques hybrides, les applications cloud ont de plus en plus le vent en poupe, complétant souvent le nombre encore important d'applications informatiques internes (« on premise »). Cela a des conséquences sur la sécurité des informations qui doivent faire l'objet d'une protection particulière, notamment en cas d'accès pour télémaintenance depuis l'étranger. En effet, toute entreprise possède des secrets industriels dont la divulgation pourrait lui causer un préjudice. Il peut s'agir d'une atteinte à l'image ou d'un préjudice économique futur résultant d'espionnage industriel. Cela implique que l' « établi étendu » - ici, les prestataires de services informatiques - fasse l'objet d'un contrôle spécial. Cela peut passer par des mesures techniques et organisationnelles mais doit surtout s›appuyer sur un cadre contractuel clair. Les collaborateurs impliqués dans les processus doivent passer du statut de tiers à celui de participants, au-delà des limites de l'entreprise.

Le contrôle doit être considéré globalement comme un processus continu. Il faut tout d'abord comprendre le sujet, puis réduire les risques de perte de données par des mesures préventives. Les auteurs recommandent en plus d'augmenter les possibilités de mesures réactives en améliorant la traçabilité afin de pouvoir prendre des sanctions le cas échéant. En ce qui concerne l'accès à distance par des prestataires informatiques susceptibles d'accéder à vos données avec des autorisations privilégiées, les mesures organisationnelles et techniques suivantes sont recommandées :

- Procéder à une analyse des besoins de protection de tous les systèmes informatiques concernés
- Mettre en place des instructions internes pour l'accès aux données (gestion des accès)
- Établir des concepts d'autorisation et de rôle pour les systèmes informatiques exposés
- Gérer de manière claire les utilisateurs et les autorisations
- Obliger les utilisateurs, internes comme externes, à s'identifier personnellement
- Toujours changer les mots de passe des comptes privilégiés après leur utilisation
- Consigner et enregistrer les sessions d'accès à distance et de transfert de données

Les accès à distance, même depuis l'étranger, à des données critiques sont légalement autorisés. Les risques doivent toutefois être facilement contrôlables. La responsabilité incombe à l'entreprise elle-même.