Vorsicht vor Handshake-Deals

Zukunftsträchtige Innovationen kommen oft von kleinen Zulieferern – und bei diesen müssen die Lieferantenrisiken anders angepasst werden.

Von Matthias Niklowitz

Egal wie gross sie sind – die coolen Hersteller von mobilen Lösungen und von Versicherungs-Apps sind um Faktoren kleiner als ihre wichtigsten Kunden, die grossen und teilweise schwerfälligen Versicherungsgesellschaften. Ein Ungleichgewicht gibt es auch beim Wissen: Die kleinen Hersteller wissen alles über Kundenvorlieben und Benutzerführung. Aber ihre Expertise zu den komplexen Geschäfts- und IT-Prozessen einer Versicherung hält sich in Grenzen.

Ebenso ungleich verteilt sind bestimmte Risiken: Ein Versicherer, der eine coole Lösung eines kleinen Herstellers kauft, erwirbt damit gleichermassen ein Bündel von Risiken mit: Wer kümmert sich um die Wartung und Weiterentwicklung einer App, wenn der Hersteller entweder untergegangen oder von einem Konkurrenten geschluckt worden ist? Eine ähnliche Problematik ergibt sich, wenn man einige wichtige Geschäftsprozesse ausgelagert hat. Dann genügt es, wenn der Cloud-Provider oder der Software-as-a-Service-Partner ins Straucheln gerät, um das eigene Geschäft lahmzulegen. Ähnliches gilt übrigens auch für den Betrieb von Call-Centern. Natürlich gibt es in den Verträgen entsprechende Passagen – aber selbst eine finanzielle Regelung mit Ausgleichszahlungen nützt wenig, wenn die Firma selber nicht mehr existiert und es nichts mehr zu holen gibt.

83 %

der 2016 in den USA verschwundenen **Datensätze** betreffen Kranken- und Unfallversicherungen.

Gemäss Umfragen von Accenture und Capgemini sind sich viele Versicherungen nicht bewusst, wo und dass viele Risiken bei den Lieferanten stecken. Die Priorisierung des Operational Risk Managements der vergangenen Jahre habe bei vielen Versicherungen fälschlicherweise dazu geführt, dass diese fast automatisch annehmen, dass ihre Partnerfirmen und Lieferanten die gleichen Prioritäten gleich gut abgearbeitet haben.

Daten und Ruf weg

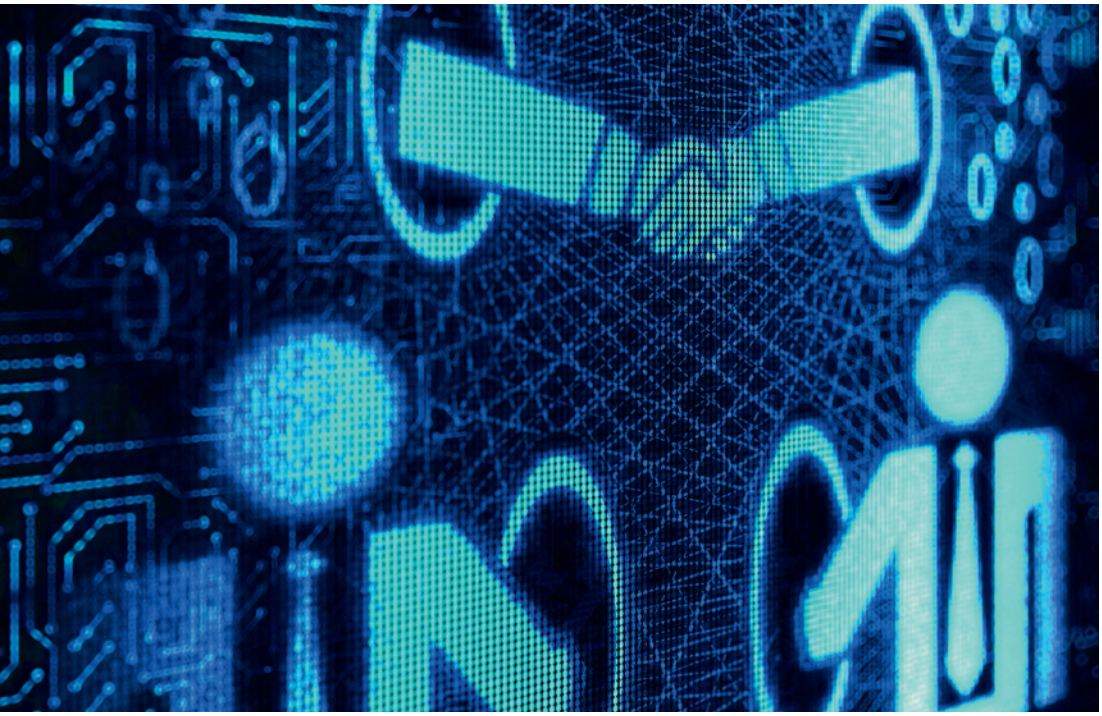
Lieferantenrisiken sind eigentlich kein neues Phänomen: Jede Versicherung, die ihr Rechenzentrum auslagert, kommt ins Schleudern, wenn der Betreiber des Rechenzentrums beispielsweise bei der IT-Sicherheit schlampt und die Kundendaten durch eine Hacker-Attacke abhanden kommen. Rasch wird dann aus einem Technologie-Risiko ein Reputationsproblem, bei dem selbst Zahlungen wenig nützen, weil zuvor ein teurer und mühsam aufgebauter guter Ruf beschädigt worden ist.

Exponiert sind auch und gerade Versicherungen und Krankenkassen: Hacker hatten sich in den vergangenen Jahren regelrecht auf diese Firmen spezialisiert, um Daten zu stehlen, mit denen sich neue bzw. falsche Identitäten aufbauen und Versicherungsleistungen beziehen lassen. Das US-Identity Theft Resource Center registrierte im laufenden Jahr (Stand Ende März) alleine für die USA insbesondere bei Kranken- und Unfallversicherungen 63 Vorfälle, bei denen 3,8 Millionen Datensätze abhanden gekommen waren. Das entspricht 83 Prozent aller verschwundenen Datensätze. Banken und selbst Industrie- und Handelsfirmen weisen aktuell weitaus weniger Probleme auf. Und laut einer Umfrage des Versicherungsbrokers Willis steigt die Summe der direkten und indirekten Schäden von Jahr zu Jahr überproportional an – weil immer gravierende Vorfälle erfolgen.

Längst haben sich auch die Regulatoren in aller Welt dieser Probleme angenommen. Die Finma nennt in ihren Prüflisten für die Risikoanalyse explizit die elektronische Infrastruktur und das Outsourcing als zu prüfende Punkte. Versicherungen dürfen demnach auch die Risiken, die via kleine App-Hersteller ins Haus kommen, nicht (mehr) auf die leichte Schulter nehmen.

Ergänzend haben sich auch die Wirtschaftsprüfer wie KPMG und Deloitte dem Problem angenommen. Deloitte schlägt vor, die Risiken weiter zu unterteilen und unterschiedliche Risiko-Klassen zu bilden. Einige Applikationen – wie mobile Apps – sind aus unterschiedlichen Gründen anders zu bewerten als ein CRM-System im Call-Center. Risiken manifestieren sich durch das Fehlen von Kontingenzplänen und sichtbar sind sie bei den Analysen, wenn festgestellt wird, dass wichtige Prozesse, die von einem bestimmten (kleinen) Unternehmen kontrolliert werden, auch die für das Funktionieren der ganzen Versicherung kritischen Prozesse sind.

BILD: ISTOCK



Vielen Versicherungen ist nicht bewusst, wo und dass viele Risiken bei den IT-Lieferanten stecken. Vorsicht ist vor allem bei Vereinbarungen per Handschlag geboten.

Entschärf hat sich das Problem bei den kleinen App-Herstellern insofern, dass es in der Schweiz mit Necetera, Ergon Informatik oder Namics eine Reihe von Firmen mit exzellentem Track Record gibt, die sichere Apps bauen können und die auch die erforderliche kritische Masse haben, die das David-und-Goliath-Problem abschwächt. Es gibt indes weitere Bereiche wie Analytics, Online-Werbe-Optimierung oder Risk Management, in denen sich kleine Anbieter mit vielversprechender Technologie tummeln – und bei diesen stellt sich die Risikofrage weiterhin. KPMG hat auch deshalb Richtlinien und Entscheidungshilfen mit den wichtigsten Eckpfeilern Risk Assessment, Drittparteien-Due-Diligence-Prüfung, dem Contracting und der anschliessenden regelmässigen Prüfung der Vertragsinhalte, der regulativen Umgebung und der sich verändernden Problemlage bei den Lieferanten entwickelt.

Auf die besonderen Bedingungen und Umstände für Versicherungsunternehmen weist das US-Beratungshaus TBI hin: Die Wahl einer Partnerfirma und das Contracting von IT-Projekten sowie von Outsourcing-Vorhaben sei der leichte Part des Ganzen. «Erst wenn der Vertrag unterzeichnet ist, zeigen sich die Herausforderungen», so die Experten. Es gebe bei der Analyse unzähliger Verträge eine Reihe von auffälligen Merkmalen, die mit erfolgreichen Beziehungen zu Lieferanten einhergehen: Es finden sehr regelmässige, atmosphärisch gute und inhaltlich befriedigende Gespräche zwischen den Beteiligten statt. Es werden dabei klare Erwartungshaltungen kommuniziert – nicht nur zu Verfügbarkeiten, sondern auch zum beteiligten Personal, Anpassungen bei der IT-Sicherheit, der An- oder Abwesenheit von Schlüsselpersonen und von Abgängen wichtiger Beteiligter. Schliesslich sind die wichtigsten Eckpunkte vertraglich fixiert worden – inklusive den Rollen und Verantwortlichkeiten.

Umgekehrt gibt es laut TBI auch einige Anzeichen, bei denen Vorsicht geboten ist: Dazu zählen Handshake-Vereinbarungen (insbesondere der CEOs der beteiligten Versicherungen und den Lieferanten), aufkommendes Unwohlsein mit der einmal vorgenommenen Auswahl des Lieferanten, wichtige Ab- oder Zugänge auf allen Seiten des Tisches, die Mischung von Rollen als Technologie-Lieferant für die Lösung eines bestimmten Problems mit strategischen Beratungs- und Begleitungselementen sowie fehlende bzw. nicht eingeplante Ressourcen, um sich um die Beziehung mit dem Lieferanten während der Vertragslaufzeit zu kümmern.

Reden, reden, reden

Natürlich schliessen auch regelmässige Gespräche Probleme nicht aus. TBI empfiehlt wiederkehrende, bei überaus wichtigen Beziehungen sogar wöchentliche oder zweiwöchentliche Meetings, bei denen gleich zu Beginn festgelegt wird, wer sich bis wann um die Lösung von offenen Fragen zu kümmern hat. Verpasste Fristen sollten gleich weiter nach oben eskaliert werden.

Inzwischen gibt es eine Reihe von Versicherungen, die spezielle Policen für den Umgang mit Lieferantenrisiken entwickelt haben. Risiken, die von den IT-Lieferanten und/oder den Herstellern von speziellen wichtigen Softwareprodukten wie Apps ausgehen, werden gewöhnlich durch die grossen Industrieversicherer abgedeckt. Ausser man kümmert sich gleich Inhouse um solche Risiken – was indes bei Kranken- und Unfallversicherungen in der Regel gar nicht und bei Rückversicherungen je nach Struktur nur mit Einschränkungen funktioniert. •

Inzwischen gibt es eine Reihe von Versicherungen, die spezielle Policen für den Umgang mit Lieferantenrisiken entwickelt haben.