Unterschätztes *Problem*

Bei **Transaktionen** werden Unternehmen oft unbemerkt zu IT-Providern, mit neuen Haftungsfragen und Auswirkungen auf Versicherungslösungen.

ANNA LARA WEIGELT UND CARLOS CASIÁN

Support mit Haftungsfolge: Transaktionen machen Firmen zu IT-Dienstleistern.

FOTOS: SHUTTERSTOCK GETTY IMAGES

Traditionelle Unternehmen sind meist keine IT-Dienstleister oder Hosting-Provider. Durch die Digitalisierung und die zunehmenden Angebote an digitalen Services oder Produkten können sie jedoch unwissentlich zu solchen Anbietern werden. Dieses Szenario tritt oft bei Transaktionen ein, wenn Teile des Unternehmens oder Tochtergesellschaften verkauft werden und die IT-Infrastruktur temporär zur Verfügung gestellt wird. Daraus ergeben sich gewisse Implikationen.

Transaktionen sind generell komplex. Bei einem Verkauf mit fortbestehender IT-Bereitstellung entsteht ein hochkomplexes Zusammenspiel aus verschiedenen Rechtsgebieten, Haftungsregeln, Datenschutzvorgaben, Lizenzvereinbarungen und operativer Trennung, bei dem Unschärfen schnell zu nicht kalkulierten Risiken führen können.

Haftungsrisiken bei IT-Ausfällen

Typischerweise regelt ein Transition Service Agreement (TSA) die IT-Bereitstellung zwischen Käufer und Verkäufer. Darin festgelegt sind Leistungsbeschreibung, Service-Level-Agreements, Kosten, Haftungsgrenzen, Haftungsausschlüsse, Daten- und Sicherheitsanforderungen, Übergangs- und Exit-Vereinbarungen, Kündigungsmodalitäten sowie Eskalationsprozesse. Oft wird jedoch übersehen, dass der Verkäufer damit faktisch die Rolle eines professionellen IT-Dienstleisters übernimmt und neue Haftungsrisiken entstehen, die nicht geprüft oder korrekt adressiert wurden. Der Einwand, man stelle «nur» die eigenen Systeme und Dienstleistungen weiterhin zur Verfügung, die zuvor auch intern erbracht wurden, lässt sich so nicht halten.

Fällt das IT-System aus, etwa durch einen Cyberangriff, kann der Verkäufer seine im TSA zugesagte Leistung nicht mehr erbringen. Für den Käufer ist dies kein internes IT-Problem, sondern ein Leistungsversagen seines IT-Providers. Schadenersatzforderungen oder Vertragsstrafen können die Folge sein und den Verkäufer in seiner Rolle als IT-Dienstleister treffen.

Der Umgang mit diesem Risiko sollte früh im Transaktionsprozess erfolgen. Es empfiehlt sich eine saubere Risikobewertung und die Überprüfung der Versicherungsstruktur in einer interdisziplinären Runde mit Legal-, IT-, M&A-Spezialisten sowie dem Broker/Versicherungsberater. Andernfalls können Deckungslücken entstehen, die ein nicht einkalkuliertes, finanzielles Risiko für den Verkäufer darstellen. Besonders Cyber- und Haftpflichtversicherungen sollten geprüft werden, da es im Kontext von Cybervorfällen und IT-Dienstleistungen Abgrenzungsthematiken gibt, die adressiert werden müssen.

Deckungslücken im TSA-Szenario

Bei der Cyberversicherung, die generell die finanziellen Folgen eines Cyberangriffs auf das versicherte IT-System sowie Ansprüche Dritter wegen Datenschutz- und Vertraulichkeitsverletzungen deckt, ergeben sich mindestens zwei Herausforderungen. Erstens: Die Cyberversicherung des Verkäufers schützt das finanzielle Interesse des Versicherungsnehmers. Entsteht durch einen Cyberangriff ein Schaden bei der abgespaltenen Gesellschaft, stimmt diese Vermögenseinbusse nicht zwingend mit dem finanziellen Interesse des Verkäufers überein. Zweitens stellt sich aus Sicht einer allfälligen Cyberversicherung des Käufers die Frage, ob das vom Verkäufer bereitgestellte IT-System tatsächlich als versichertes IT-System gilt und mögliche Schäden darüber gedeckt sind. Dies ist entsprechend abzuklären.

Was passiert, wenn eine Pflichtverletzung des Verkäufers zu einem Schaden beim Käufer führt? Handelt es sich um einen reinen Vermögensschaden ohne Personen- oder Sachschaden, ist die Berufshaftpflichtversicherung zu prüfen. Diese wird jedoch vorwiegend von Unternehmen abgeschlossen, die Dienstleistungen anbieten. Viele Unternehmen in der Rolle eines temporären IT-Providers verfügen allerdings in der Regel nicht über eine spezifische Berufshaftpflichtversicherung. Falls doch, gilt es zu prüfen, ob sie im vorliegenden IT-Kontext greift, denn Einschränkungen hinsichtlich Cybervorfällen oder Ausschlüssen bei Technologieprodukten sind keine Seltenheit.

Viele Unternehmen verfügen nicht über eine spezifische Berufshaftpflichtversicherung.

Die Komplexität dieses vermeintlichen Nebenrisikos bei Transaktionen zeigt sich an mehreren Stellen: Erstens beim Erkennen, dass das Unternehmen zumindest temporär zu einem IT-Dienstleister wird. Zweitens bei der klaren Festlegung der Rechte und Pflichten im Rahmen eines TSA. Und drittens bei den Implikationen für den Versicherungsschutz und dem daraus resultierenden Handlungsbedarf.

Eine frühzeitige Analyse und gezielte Absicherung helfen somit Unternehmen, Haftungsrisiken im Transaktionsprozess zu erkennen und zu minimieren.

Anna Lara Weigelt, Fachspezialistin Special Risks, und Carlos Casián, Fachspezialist Special Risks, Kessler & Co AG

Chancen wie auch Missbrauch

Künstliche Intelligenz ermöglicht leistungsfähige Schutzmechanismen, aber senkt auch die Einstiegshürden für ausgefeiltere Cyberkriminalität.

NICOLAS FASOLO

KI am **Kicker**: Schnelle Angriffe treffen auf eine lernende Verteidigung.

Moderne Systeme der künstlichen Intelligenz sind in der Lage, enorme Datenmengen zu verarbeiten, Muster zu erkennen und Inhalte weitgehend automatisiert zu generieren. In der Cybersicherheit haben sich KI-basierte Verfahren insbesondere bei der Anomalieerkennung, der Verhaltensanalyse, dem Natural-Language-Processing sowie der automatisierten Entscheidungsunterstützung etabliert. Diese Fähigkeiten erlauben eine schnellere Bedrohungserkennung, vorausschauende Risikoanalysen und Reaktionen auf komplexe Angriffsszenarien in Echtzeit. Gleichzeitig können dieselben Modelle überzeugende Texte, Programmcodes oder – in bestimmten Kontexten – auch schädliche Artefakte erzeugen. Damit wird KI zu einem vielseitigen Werkzeug mit klarer Dual-Use-Problematik.

Schutz von Infrastrukturen

IT-Security-Fachleute nutzen KI zunehmend als Ergänzung klassischer Abwehrmechanismen. Machine-Learning-Modelle analysieren beispielsweise Netzwerkverkehr und erkennen Abweichungen vom Normalverhalten, häufig auch solche Bedrohungen, die signaturbasierte Systeme übersehen. KI-gestützte Tools unterstützen Security Operations Center (SOC), indem sie Alerts korrelieren, Vorfälle priorisieren und Fehlalarme reduzieren. Auch im Vulnerability-Management kommt KI zum Einsatz: Sie hilft bei der Analyse von Quellcodes und Systemkonfigurationen und identifiziert potenzielle Schwachstellen, bevor Angreifer diese ausnutzen können. Verantwortungsbewusst eingesetzt, erhöhen solche Technologien Skalierbarkeit, Effizienz und Resilienz komplexer digitaler Infrastrukturen.

Auch Cyberkriminelle setzen zunehmend auf KI, um Reichweite und Wirksamkeit ihrer Angriffe zu steigern. Incident-Response-Teams wie etwa von Yarix (Var Group) beobachten beispielsweise automatisierte Reconnaissance-Prozesse, die exponierte Dienste oder Fehlkonfigurationen in kurzer Zeit kartieren. Generative Modelle werden jedoch gleichzeitig von der Gegenseite genutzt, um täuschend echte Phishing-Nachrichten, Schadsoftware-Codes oder Social-Engineering-Skripte zielgerichtet zu erstellen. Darüber hinaus kann KI helfen, Sicherheitsmechanismen zu umgehen, etwa durch dynamische Modifikation von Schadcode oder durch das Imitieren legitimen Nutzerverhaltens. Diese Entwicklung senkt technische Einstiegshürden und ermöglicht auch weniger erfahrenen Akteuren zunehmend komplexe Angriffe. Umso mehr ist ein wachsames und schlagkräftiges Abwehrdispositiv notwendig.

Das Fundament sicherer KI

Ein höheres Sicherheitsniveau entsteht durch das Zusammenspiel von Technologie, Governance und Bewusstseinsbildung. Unternehmen sollten KI gezielt in ihre Verteidigungsstrategien integrieren, gleichzeitig jedoch menschliche Kontrolle und klare Verantwortlichkeiten sicherstellen. Regelmässige Risikoanalysen, Systemhärtung, Secure-by-Design-Entwicklung sowie belastbare Incident-Response-Konzepte bleiben zentrale Bausteine moderner IT-Security. Darüber hinaus tragen Schulung, ethische Leitlinien und regulatorische Rahmenbedingungen dazu bei, Missbrauch einzudämmen und verantwortungsvolle Innovation zu fördern, ohne technologischen Fortschritt auszubremsen.

Richtig eingesetzt, kann KI als analytischer Assistent bei sicherheitsrelevanten Aufgaben wertvolle Dienste leisten. Sie unterstützt etwa bei Threat-Modeling-Prozessen, erklärt komplexe Angriffstechniken oder hilft bei der Analyse von Log-Daten und Systemkonfigurationen. Voraussetzung für einen effektiven Einsatz sind klare Einsatzgrenzen, die Validierung von Ergebnissen sowie der sorgfältige Umgang mit sensiblen Daten. Wird KI als unterstützendes Werkzeug – und nicht als alleinige Autorität – verstanden, kann sie die Lagebeurteilung verbessern und fundierte Entscheidungen erleichtern. Wichtig bleibt jedoch: Sicherheitskritische Aufgaben sollten nicht unreflektiert an KI-Systeme delegiert werden. Richtig genutzt erweitert sie menschliche Fähigkeiten – sie ersetzt sie nicht.

Nicolas Fasolo, Incident Response Team Leader bei Var Group