Risiko oder Isolation – das Modell Rosenthal

Know-how Das Modell Rosenthal berechnet, wie gross das Risiko der Datenherausgabe ist, wenn Unternehmen und Behörden in der Cloud eines US-Anbieters arbeiten. Der Erfinder erklärt den Hintergrund seines Modells und äussert sich zur kursierenden Kritik an der Methode.

Von Matthias Wintsch

Ein Name, um den man in der Schweiz kaum herumkommt, wenn es um Datenschutzthemen geht, ist David Rosenthal. Der Jurist und Partner bei der Wirtschaftskanzlei Vischer macht regelmässig von sich reden, unter anderem, weil er seine klaren und teils polarisierenden Positionen zu Datenschutzthemen gerne öffentlichkeitswirksam bekanntgibt. Seinen Hintergrund hat Rosenthal in der Informatik und im Journalismus. Bereits in den 90er-Jahren war er als freischaffender Software-Entwickler und Tech-Journalist tätig, seit Anfang der 2000er-Jahre beschäftigt er sich als Jurist hauptberuflich mit Digitalthemen und ist seit 2020 Partner bei Vischer.

Rechtmässige Überwachung

2022 hat es der Datenschutzspezialist besonders mit einer Arbeit in die Medien geschafft: dem Modell Rosenthal, einer Methode zur Risikobeurteilung zum Thema Lawful Access. Der Lawful Access – frei übersetzt der «rechtmässige Zugriff» – beschreibt den Vorgang, dass eine (hier ausländische) Behörde ihr lokales Recht benutzt, um einen Provider in ihrem Land zur Herausgabe von Kundendaten zu zwingen. Das kann auch dann funktionieren, wenn er die Daten auf einem Server im Ausland gespeichert hat – beispielsweise in einer Microsoft-365-Instanz, die in den Schweizer Datenzentren von Microsoft untergebracht ist. In den USA ist eine Form des Lawful Access in einem Gesetz namens CLOUD Act geregelt, das für viele Spezialisten zum roten Tuch geworden ist. Wenn es um den Einsatz von Cloud-Lösungen mit US-Wurzeln geht, dient der CLOUD Act besonders Schweizer Cloud-Providern des Öfteren auch als Verkaufsargument: Denn wenn aus den USA nicht auf die Daten zugegriffen werden kann, kann sie auch die Behörde dort nicht herausverlangen.

Das Modell Rosenthal ist eine Methode zur Berechnung der Eintrittswahrscheinlichkeit eines solchen Zugriffs und als Excel-Tool im Open-Source-Modell zur freien Nutzung verfügbar. Entwickelt wurde es 2019 im Auftrag einer Schweizer Bank. Der breiten Öffentlichkeit bekannt wurde es aber vor allem, weil es im Rahmen der Microsoft-365-Evaluierung beim Kanton Zürich 2022 zum Einsatz kam. In diesem Fall ergab das Modell Rosenthal, dass die Wahrscheinlichkeit eines Zugriffs via Lawful Access aus den USA auf die Geschäftsdaten des Kantons über fünf Jahre hinweg 0,74 Prozent beträgt. Das war für den Kanton tief genug – der Einsatz wurde bewilligt, was wiederum bei bestimmten Datenschützern sauer aufgestossen ist. Die Kritiker argumentieren, dass sich ein solches Risiko nicht einfach mit einem Modell wegkalkulieren lasse und dass die berechneten Wahrscheinlichkeiten aus der Luft gegriffen seien bis hin zur Meinung, dass die Methode schlicht überflüssig ist, weil das Risiko sowieso null sein müsse. Wir haben David Rosenthal in den Vischer-Büros in Zürich getroffen, um das Modell unter die Lupe zu nehmen und der Kritik auf den Grund zu gehen.

Komplexität greifbar machen

Schon zu Beginn des Gesprächs bestätigt Rosenthal, dass das ganze Thema für die meisten Personen eigentlich nicht fassbar und zu komplex ist. «Und das trifft auch auf manche Behördenvertreter zu», wie er anfügt. 2019 hat er von der bereits erwähnten Bank daher den Auftrag erhalten zu ermitteln, welches Bündel an Massnahmen gegen den ausländischen Behördenzugriff beim Gang in die Cloud genügt, damit ihr keine Verletzung des Bankgeheimnisses vorgeworfen werden kann. «Wir Juristen arbeiten mit Worten und Memoranden, aber damit konnte ich diese Aufgabe nicht befriedigend lösen – es war eine Gleichung mit zu vielen Komponenten, also habe ich es mit Zahlen probiert und das funktionierte sehr gut», wie er erklärt. «Wenn jemand nur das Ergebnis von aussen aus der Distanz ansieht, ohne die Methodik und die rechtlichen Überlegungen dahinter zu verstehen, wird ihm das suspekt vorkommen, das kann ich verstehen.»

Das Excel-Tool zur Methode Rosenthal ist als Fragebogen konzipiert, der das Problem in kleine Teile aufteilt und sie einzeln beurteilen lässt. Beispielsweise wird abgefragt, wie viele Fälle es schätzungsweise jährlich gibt, in denen eine ausländische Behörde versuchen wird, auf dem Rechtsweg an relevante Daten zu gelangen. Oder mit welcher Chance der Provider an die Daten seines Kunden unverschlüsselt gelangen könnte (was z.B. oft 80% bis 100% sein wird). Der Beurteiler macht sich dazu Gedanken, schaut etwa Erfahrungswerte oder Rechtsprechung dazu an und gibt an, wie zuversichtlich er ist, dass eine bestimmte Massnahme wirksam ist. Alles zusammen ergibt die statistische Gesamtwahrscheinlichkeit eines Lawful Access über eine bestimmte Periode – das sind die erwähnten 0,74 Prozent innerhalb von fünf Jahren beim Kanton Zürich.

Sein Modell hat ungeachtet der jüngsten Kritik Erfolg: Es wurde bereits von etlichen Unternehmen und Behörden zur Eva-

luierung von Cloud-Lösungen aus den USA genutzt, seine Mitbewerber setzen es ein, der Weltverband der Datenschutzspezialisten bietet es an, die Bundeskanzlei bezeichnete es in ihrem Cloud-Gutachten als «Gute Praxis» und die Staatsanwaltschaft Basel-Stadt bestätigte die Eignung einer solchen Berechnung.

Der Umstand, dass er das Modell kostenlos zugänglich machte, lässt vermuten, dass hier versteckte Interessensbindungen zu den grossen Cloud-Providern bestehen. Rosenthal winkt ab: «Ich stehe in den Cloud-Projekten jeweils auf deren Gegenseite, habe etwa die heute in der Schweiz von Banken, Spitälern und Behörden benutzten Spezialbedingungen mit Microsoft ausgehandelt», antwortet er. «Ich will, dass wir in der Schweiz gute Standards haben, ich löse gerne Probleme, die bisher niemand gelöst hat, und wer mich kennt weiss, dass ich Know-how ausgiebig teile.» Und er räumt ein, dass ihn die breite Unterstützung persönlich antreibe weiterzumachen. «Ich bewirke gerne etwas», sagt er, «Datenschutz muss praktikabel sein, damit er zum Ziel führt, und ich bin überzeugt, das ist möglich.»

Kann die Schweizer Cloud mithalten?

Nun sagen gewisse Datenschutzbehörden, dass jedes noch so kleine Risiko eines Lawful Access eines zu viel und eine risikobasierte Analyse daher von vornherein nicht angebracht ist. «Datenschutz war schon immer risikobasiert», entgegnet Rosenthal. «Es gibt kein Null-Risiko im Leben». Darauf hätten die Fundamentalisten unter den Datenschützern, wie er sie nennt, keine vernünftige Antwort, weil der Null-Risiko-Ansatz nicht umsetzbar sei. «Auch die EU-Datenschützer vertreten den Null-Risiko-Ansatz und wollen so erzwingen, dass Daten aus Europa in Europa bleiben müssen. Damit machen sie sich unglaubwürdig und schaden der Sache.»

Die naheliegendste Lösung wäre in der Tat, einfach keine Daten in die Hände ausländischer Anbieter zu geben. Eine Schweizer Cloud mit Schweizer Lösungen zu haben, würde das Risiko eines Zugriffs ausländischer Behörden zwar nicht gänzlich aus der Welt schaffen – es kann sie auch in der Schweiz geben –, aber es wäre kleiner. «Natürlich», so Rosenthal, «und eine solche Lösung kann auch punkto Abhängigkeit vom Ausland Sinn machen, aber dann sollten wir dies beim Namen nennen und nicht so tun, als gebe es rechtlich keine andere Option.»

Nun wäre es vermessen zu sagen, dass die Schweiz keine kompetenten Cloud-Provider hat. Warum also nicht einfach auf eine Schweizer Lösung zurückgreifen? Rosenthal: «Meine Klienten und ihre IT-Profis sagen mir deutlich, dass man hierzulande nicht annähernd an das Niveau der US-Hyperscaler herankommt.» Das gelte sowohl betreffend Cybersicherheit als auch Funktionalität. «Wenn die Schweiz in diesen Bereichen nicht mithalten kann, ist auch dies ein Risiko, das mitbewertet werden und – mit dem Lawful Access – in eine Gesamtbeurteilung einfliessen muss.» Müssten sich seine Klienten zwischen höherem Schutz vor Hackern und höherem Schutz vor ausländischen Behörden entscheiden, sei die Wahl meist einfach. «Viele wären froh, das Risiko von Cyberangriffen wäre so gering wie jenes von Zugriffen ausländischer Behörden.»

Die Idee einer Schweizer Cloud mit Schweizer Softwarelösungen, die den Bedarf der Behörden und Unternehmen voll decken kann, weist er daher nicht kategorisch von der Hand, hält sie aber für unrealistisch. «Und nehmen wir an, dass sei doch realistisch: Welche anderen Risiken schaffen wir und sind wir bereit, den Preis zu bezahlen?» so Rosenthal. «Ich finde diese Diskussion ist wichtig und sie sollte geführt werden, da bin ich völlig emotionslos, aber sie ist eine politische oder geschäftliche und keine rechtliche. Das ist wie bei den Kampfjets, die auch aus dem Ausland kommen. Ich gehe aber auch davon aus, dass viele Anwendungen weiter auf reinen Schweizer Rechenzentren betrieben werden und in absehbarer Zeit nicht in eine ausländische Cloud wandern. Es wird also einen Mix geben.»

«Datenschutz war schon immer risikobasiert. Es gibt kein Null-Risiko im Leben.»

David Rosenthal, Jurist und Partner bei Vischer

Nach bestem Gewissen

Ebenfalls sieht sich Rosenthal dem Vorwurf ausgesetzt, dass die Methode das Ergebnis vorgeben würde und der Benutzer damit einfach das zu hören bekomme, was er möchte. Auch dem widerspricht er: Die Werte bestimme der Benutzer. «In Zürich kam das Gremium zu einem sehr tiefen Wert, aber ich hatte auch schon Fälle mit Werten über 20 Prozent, die dann als zu hoch bewertet wurden und daher Nachbesserungen bei den Schutzmassnahmen nötig wurden.»

Ausserdem seien die Schätzungen in der Regel konservativ, ergänzt Rosenthal: «Beim Kanton Zürich ist es etwa so, dass E-Mails mit Geschäftsfalldaten verschlüsselt werden und Microsoft den Schlüssel nicht hat – der Kanton geht damit viel weiter als andere.» Normalerweise wäre an dieser Stelle die Diskussion zu Ende und man würde von keinem relevanten Risiko mehr ausgehen. Hier aber sei aus reiner Vorsicht trotzdem eine Chance von 10 Prozent angenommen worden, dass Microsoft die Verschlüsselung knacken kann, obwohl sie Stand der Technik sei. «Mir scheint, die Zürcher Datenschützerin hat das Excel gar nicht wirklich geprüft, denn sonst würde sie nicht kritisieren, was der Kanton hier tut – nämlich genau das, was sie verlangt und sie selbst als genügend erachtet.»

Mehr Hürden – tieferes Risiko

Ein wichtiger Faktor respektive eine weitere Hürde, die das Risiko massgeblich mindern können, sind laut David Rosenthal die vertraglichen Feinheiten, die mit den Providern ausgehandelt werden. Hier geht es etwa um die Frage, unter welchen Bedingungen ein Provider im Ausland gezwungen werden kann, Daten seiner Kunden herauszugeben. Denn, wie Rosenthal sagt, sei das zum Beispiel in den USA nicht bereits dann der Fall,

wenn der Provider es technisch schaffen kann, an die Daten heranzukommen. «Die Hürden sind für die Behörden höher, und das kann man durch vertragliche Vorkehrungen ausnutzen und so den technischen Schutz ergänzen.»

Hinzu kommt: Für die USA ist es dank Rechtshilfeabkommen mit der Schweiz in den allermeisten Fällen ohnehin viel einfacher, an Daten aus der Schweiz heranzukommen als über den US CLOUD Act. «Unsere Erhebung zeigte, dass dieser Weg in 95 Prozent der Fälle funktioniert; ich hatte den Wert zunächst tiefer geschätzt», so Rosenthal. Ausserdem schütze die Schweiz ihr Territorium auch digital recht gut, sagt der Jurist, viel besser als die EU: «Die Mitarbeiter von Microsoft würden sich strafbar machen, wenn sie einer US-Behörde ohne Einwilligung der Schweizer Behörden in der Schweiz gespeicherte Daten herausgeben», hält er fest. «Ich weiss aus eigener Erfahrung mit US-Behörden und US-Gerichten, dass diese die Schweizer Souveränität grundsätzlich respektieren.»

Diese rechtlichen Feinheiten in den Verträgen seien natürlich keine Garantie dafür, dass kein Lawful Access stattfinden könnte, betont Rosenthal. Aber es seien weitere Faktoren, die ein Eintreten unwahrscheinlich machen, besonders weil der Rechtshilfeweg ohnehin viel bequemer und schneller sei als der Weg über den CLOUD Act.

Das Modell Rosenthal basiert dabei auf der Annahme, dass alle diese technischen und rechtlichen Aspekte gegeben sein müssen, damit es zum Lawful Access kommt. «Ich habe dabei die Bedingungen in so kleine Teile aufgetrennt, dass sie sich wenigstens grob einschätzen lassen – und mehr braucht es nicht, um eine Grössenordnung zu erhalten», so Rosenthal. Er rechnet vor: Müssen vier Bedingungen erfüllt sein, damit es zum Schaden kommt, und ist die Chance bei jeder 50:50, so ist die rechnerische Wahrscheinlichkeit eines Schadens 6,25 Prozent. «Und je mehr Hürden wir einbauen, etwa mit dem Vertrag oder technischen Massnahmen, desto tiefer ist der Wert. Ich sage meinen Klienten nicht, wie hoch diese Wahrscheinlichkeiten sind, das schätzen sie selbst. Ich biete ihnen nur den Rahmen dazu.»

Zahlen aus der Kristallkugel?

Dass trotz konservativen Schätzungen solch tiefe Zahlen resultieren, kann stutzig machen. Auch kann der Eindruck entstehen, dass die Zahlen in der Risikoabschätzung aus der Luft gegriffen sind und keine wirkliche Basis haben. «Es ist richtig, dass es sich um Schätzungen handelt – niemand von uns hat eine Kristallkugel», räumt Rosenthal ein, «aber fast alle Entscheide, die wir im Leben, in der Politik und im Geschäft treffen, basieren auf Annahmen und Einschätzungen, und da sagt uns die Wissenschaft, dass es wichtig ist, hierfür ein strukturiertes Verfahren zu verwenden.» Genau dies biete seine Methode. «Zuvor beurteilten die Leute das Thema rein emotional». Ob die Zahlen aus der Luft gegriffen seien, könne jeder anhand der Begründungen selbst prüfen. Für einen Juristen gehöre es zum täglichen Brot, die Chance rechtlicher Argumente einzuschätzen, was aber meist völlig unstrukturiert geschehe.

Ob sich eine Einschätzung als falsch erweisen kann? «Ja, sicher, wie überall», räumt Rosenthal ein. «Das ist alles mit etlichen Unsicherheiten verbunden, auch Umstände ändern sich. Aber irgendwo müssen wir ansetzen und Entscheide treffen, und es gibt kein risikofreies Leben.» Beim Lawful Access evaluiere man die einzelnen Punkte über viele Stunden hinweg, weil das Thema für viele neu sei. «In anderen Bereichen, wie etwa der Informationssicherheit, werden Risiken viel gröber und rascher evaluiert und niemand hat damit ein Problem, weil wir uns es so gewohnt sind.»

An diesem Punkt ist man dazu hingerissen, die Frage nach dem Sinn oder Unsinn von Risikoabschätzungen aufzuwerfen. «Man kann sie und sollte sie stellen», räumt der Jurist ein. «Aber was ist die Alternative? Technologie bietet unheimlich viele Möglichkeiten, aber wir wollen trotzdem nicht aufs Geratewohl handeln.» Dass auch einer sauberen Risikobeurteilung eine gewisse Zufälligkeit innewohnt, streitet er nicht ab. «Aber sie bietet die Basis, sich methodisch mit einem Risiko und den Gegenmassnahmen auseinanderzusetzen und so bessere Entscheide zu treffen.» Er vertritt beim Risiko-Management einen schematisierten Ansatz, in dem die Fragestellungen in kleine Elemente aufgeteilt werden und so der Zufall am besten bekämpft wird. Und dass mehr Schutzmassnahmen – organisatorisch oder technologisch – zu einem tieferen Risiko führten, sei logisch und Sinn der Sache. «Meinen Kritikern sage ich: Sagt, wie man es besser machen soll. Bisher kam da nichts.»

Was KMU damit anfangen können

Die zwei Grundsatzfragen, die bleiben, sind zum einen, ob im Fall des Lawful Access das Risiko-Management als valabler Ansatz zum Einsatz kommen darf und zum anderen, ob Schweizer Unternehmen oder jedenfalls Behörden grundsätzlich auf den Einsatz von US-Cloud-Technologie verzichten sollten. Es ist so weit auch nachvollziehbar, wenn Rosenthal sagt, dass dieser Entscheid nicht bei ihm liege, sondern von den Unternehmen, den Behörden und der Politik beantwortet werden müsse.

Doch der Grossteil der Schweizer Unternehmenslandschaft – die KMU – hat weder die Mittel noch die Zeit, jeden einzelnen Einsatz der Cloud einer Risikoanalyse zu unterziehen. Hier rät Rosenthal den KMU, sich nicht auf das Risiko des ausländischen Behördenzugriffs zu versteifen und pragmatisch zu handeln. Denn: «Gerade bei Standard-Setups sind die Differenzen in der Beurteilung nicht gross.» Gut fände er es, wenn Berufs- oder Branchenverbände das Thema für ihre Mitglieder aufarbeiten und Hilfestellen anbieten könnten. So könnte definiert werden, welche Punkte man bei diesen Standard-Setups im Griff haben müsse. «Dann kann jedes KMU selbst entscheiden, ob es den Use Case so umsetzen und das Risiko übernehmen will. Selbst bei sensiblen Daten werden es die meisten für tragbar erachten, wenn gewisse Bedingungen erfüllt sind.» Seine Empfehlung: «Ich würde eine Pro-Contra-Liste machen und mich entscheiden. Meist geht es ja nicht einmal um die Frage ob Cloud, sondern welche Auswahl an Services, welches Paket an Schutzmassnahmen und welche Konfiguration.»

In der Praxis sei er mit seinen Klienten allerdings schon deutlich über die Fragestellung nach dem Lawful Access hinaus, wie er zum Schluss unseres Gesprächs erklärt. Zum Einsatz kommen weitere Tools, in denen das Lawful-Access-Risiko nur noch einer von Dutzenden Faktoren ist, die bei einer Cloud-Evaluierung berücksichtigt werden müssen. Andere, für ihn viel wichtigere Aspekte sind etwa die abgesprochenen Abhängigkeiten, die Komplexität der Konfiguration und Steuerung von Cloud-Setups und interne Massnahmen wie die Prüfung der Logs und Audit-Reports. Rosenthal: «Diese Themen machen mir mehr Sorgen, hier sollten wir die Kraft investieren.» ■