Datenschutz im Dialog

Ein Interview mit Maximilian Groth

Die gemeinsame Verarbeitung und Analyse von Kundendaten zwischen Unternehmen bietet enorme Chancen, einzigartige Wettbewerbsvorteile zu schaffen. Allerdings gestaltet sich die Datenteilung für die meisten Unternehmen aufgrund der Gefahr eines Kontrollverlustes oder einer Verletzung des Datenschutzgesetzes meist schwierig. Das Zürcher Start-up und Gewinner der «Cyber Start-up Challenge 21» bietet mit seinen sog. «Data Clean Rooms» die Chance, diesen Zielkonflikt zu lösen. Seine Plattform erlaubt es Unternehmen, sensitive Daten zu teilen und kollaborativ auszuwerten. Da diese Daten im gesamten Prozess konstant verschlüsselt sind, erfüllt Decentriq sogar die Datensicherheitsstandards von Behörden wie der Schweizer Armee. In unserem Interview mit CEO und Mitgründer Maximilian Groth sprechen wir darüber, weshalb Datenschutz und Datenauswertung kein Widerspruch sein muss und wieso Unternehmen proaktiver auf das Thema Datenschutz eingehen sollten.

Das Interview führt Mauro Gotsch, Doktorand am Institut für Marketing und Customer Insight der Universität St. Gallen (IMC-HSG)

Decentriq wirbt auf seiner Website mit dem Slogan «Sensitive data is your competitive advantage». Brauchen Unternehmen wirklich immer mehr sensible Daten, um kompetitiv zu bleiben?

Ja. Denn gerade die sensitiven Daten sind meist sowohl wertbringend als auch weniger genutzt in vielen Unternehmen. So sind beispielsweise Banken in einem Nachteil, wenn sie ihre sensiblen Daten nicht nutzen können, während beispielsweise Amazon dies tut.

Es sind aber nicht nur die Banken oder besonders regulierte Unternehmen, welche im Nachteil sind. Ich glaube, gerade in unseren Breitengraden wird der exponentielle Nutzen von solchen Daten oft noch unterschätzt. Früher, während der ersten Industrialisierung, konnten Unternehmen ihre Ressourcen meist nur linear skalieren. Man investierte in eine neue Fabrik und hat somit vielleicht die Produktion verdoppelt. Diesen Gewinn konnte man dann wieder in eine neue Anlage reinvestieren, und so weiter. Doch heutzutage, mit Daten als zentraler Unternehmensressource, hat das Ganze einen exponentiellen Charakter. Ab einem gewissen Reifegrad in einem datenintensiven Geschäftsfeld kann dich deine Konkurrenz heutzutage kaum noch einholen.

Diesen exponentiellen Nutzen demonstriert Amazon ja deutlich – zusammen mit dem erhöhten Risiko, das mit der Konzentration von vielen Daten in einem Unternehmen einhergeht. Stichwort: Data-Leaks, Hackerangriffe, Verletzung der Privatsphäre von Kunden, etc. Wäre es da nicht angebracht zu sagen, dass die meisten Unternehmen lieber die Finger von sensiblen Daten lassen sollen?

Pauschal ist dies natürlich schwierig zu sagen, aber tendenziell hätte ich gesagt: Nein, ich glaube eher das Gegenteil. Versteh' mich bitte nicht falsch, ich finde diese Leaks furchtbar, aber ich glaube, wir sollten nicht vergessen, dass unsere Datenökonomie auch noch relativ jung ist. Autofahren wurde auch nicht sicherer, indem man weniger gefahren ist – es brauchte fast 60 Jahre an Unfällen und Fehlern in der kommerziellen Nutzung, bis der Airbag und der Sicherheitsgurt zum Standard wurden. Ähnliches gilt für die Datenverarbeitung: Wir müssen aus den Fehlern lernen, die wir beobachten. Aber ich glaube zu versuchen, einfach gar keine Fehler zu machen, heisst, keinen Fortschritt zu machen. Und ich glaube, das ist extremst gefährlich.

Worin sehen Sie die Gefahr hauptsächlich?

Viele Unternehmen haben ja nicht ein rein digitales Geschäftsmodell wie z.B. Facebook. Das heisst, Digitalisierung ist für sie ein Zusatz, wie man sich als Unternehmen weiterentwickelt hat. Aber ihre Produkte hatten damit bisher verhältnismässig wenig zu tun. Datenspeicherung war zwar immer ein Teil des Geschäfts, aber diese war immer aufwendig und teuer. In St. Gallen steht die Stiftsbibliothek – so wie die Bücher dort aufbewahrt werden, haben bis vor Kurzem alle ihre Daten gesammelt und gespeichert:

> «Ab einem gewissen Reifegrad in einem datenintensiven Geschäftsfeld, kann dich deine Konkurrenz heutzutage kaum noch einholen.»

von Hand niedergeschrieben, gedruckt und archiviert. Doch Datenerhebung und Speicherung kostet ja mittlerweile fast nichts mehr und ist auch viel einfacher geworden. Dementsprechend versuchen nun auch KMUs, teilweise noch basierend auf ihrer alten Infrastruktur, den grössten Wert aus ihren Daten rauszuholen. Dieser Anspruch ist legitim, aber ohne vorher in die notwendigen Unternehmensressourcen zu investieren, ist dies, wie wenn man eine Tür aus dem 19. Jahrhundert an einem Tresor hätte; da zieht ein Einbrecher einmal etwas fester daran und schon ist er drin. Ich denke, das wird im Gespräch über Datenschutz oft vergessen: Big Tech sind vielleicht die grössten Nutzer, aber diese investieren dafür auch am meisten in Cyber-Security, Auswertungsprozesse und Abwehrsysteme. Vor Kurzem wurde eine grosse DDOS-Attacke auf Microsoft verübt und Microsoft hat berichtet, dass

Maximilian Groth,
Co-Founder & CEO
von Decentriq
www.decentriq.com

sie diese abfedern konnten. Es gibt, glaube ich, nicht viele Unternehmen, die dies geschafft hätten.[1]

Natürlich macht es Sinn, dass so grosse Ziele wie Microsoft eher angegriffen werden, doch in manchen kleineren Unternehmen wird gar nicht in Datenschutz und Cyber-Security investiert. Wir wissen das, weil es im Dark Web riesige Pools von aggregierten Datensätzen von all diesen kleineren Firmen gibt, die man dann für irgendeinen Zweck und ohne Kontrolle von aussen miteinander «matchen» könnte. Insgesamt könnte dies langfristig sogar gefährlicher für den Kunden oder die Unternehmen sein, als das, was Facebook gerade tut.

Damit wären wir bei dem Thema dieser Ausgabe: «Privacy as Strategy?» Die Frage ist: sollten das Marketing oder eben auch kleinere Unternehmen den Schutz der (digitalen) Privatsphäre von Kunden als zentrale strategische Mission verstehen?

Absolut. Kundenfokus ist essentiell und dies beinhaltet auch Datensicherheit und Datenschutz. Mir ist aber wichtig zu betonen, dass dies nicht bedeuten soll, dass wir aufhören sollten, Daten zu

> «Kundenfokus ist essenziell und dies beinhaltet auch Datensicherheit und Datenschutz.»

nutzen. Das Ziel ist, verantwortungsvoll mit diesen umzugehen. Dazu muss es für Unternehmen auch ein bisschen Freiraum geben, weil man sonst ja gar nichts mehr versuchen dürfte. Den Dialog, wie gross dieser Freiraum sein darf, führen wir momentan auf gesellschaftlicher Ebene. Wie bei der Industrialisierung ist dies aber ein Prozess – so hat man früher ja auch 14-Stunden-Arbeitsschichten gehabt, sieben Tage die Woche. Mittlerweile haben wir eine 40-Stunden-Woche. Darüber haben wir uns gesellschaftlich geeinigt – dasselbe gilt für den Datenschutz: Was ist gesund für einen Menschen?

Was sollten oder können Unternehmen zu diesem Dialog beisteuern?

Ich finde das sehr schwierig. Wenn wir das im Sinne des St. Galler Management Modells anschauen, sind bei profitorientierten Unternehmen natürlich die Shareholder eine der zentralen Anspruchsgruppen. Für diese ist kommerziell erfolgreich zu sein natürlich wichtig, was zu einem gewissen Dilemma für diese Firmen führen kann. Nehmen wir Facebook als Beispiel. Facebook möchte natürlich Werbung verkaufen. Die Werbung können sie umso teurer verkaufen, wenn möglichst viele Leute möglichst lange auf der Plattform sind. Dadurch sind sie incentiviert, Inhalte zu zeigen, welche stark auf die Interessen und die Weltanschauung einzelner Nutzerinnen und Nutzer angepasst sind. Leider bedeutet das oft auch, dass ihnen die Inhalte gezeigt werden, welche sie wütend machen oder sonst emotional berühren – Stichwort «Fake News».

Für mich ist dies aber nicht wirklich ein Datenschutz- sondern mehr ein Menschenschutzproblem. Hier müsste man sich als Unternehmen die eigene Datenverarbeitung anschauen und sagen: «Hey, da sollten wir eine Informationsvalidierung durchführen.» Meiner Meinung nach haben Unternehmen bei der Überprüfung der Auswirkung ihrer Datennutzung dementsprechend eine gewisse Pflicht.

Das bedeutet aber nicht unbedingt, dass die Monetarisierung von erhobenen Daten per se schlecht ist. Man darf da nicht rein binär rangehen. Was ich persönlich viel schlimmer finde, ist, wenn man einfach nicht transparent über die eigenen Tätigkeiten ist, oder schlimmer, wenn Unfälle oder negative Praktiken vertuscht oder verschleiert werden. Als Beispiel: Ich rege mich jedes Mal auf bei den Webseiten, bei denen man irgendwie 50 Sachen anklicken und einen riesigen Text lesen muss, nur um Cookies auszuschalten. Gleichzeitig gibt es andere Webseiten, die einfach fragen: «Hey, ist es okay, wenn wir deine Daten auswerten, um die Website oder unseren Dienst so oder so besser zu machen? Ja oder Nein?». So fühle ich mich als Besucher der Website nicht bevormundet und der Nutzen ist für mich auch leichter erklärt. Sollte es dann zu einem Leak kommen, ist das immer noch schlecht – aber es kann passieren – und ich kann es verstehen. Auch in Basel, in der Chemieindustrie, passieren manchmal Unfälle. Das Schlimme ist, wenn man es

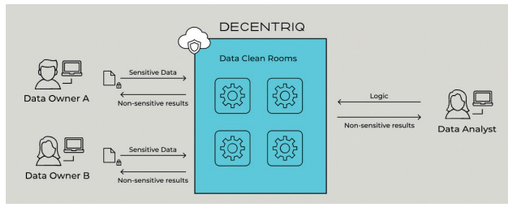


Abb.1: Decentriq Data Clean Rooms – how they work. Quelle: Decentriq.

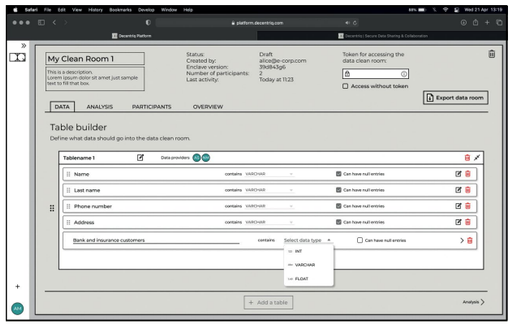


Abb. 2: Decentriq Platform 1 & 2. Quelle: Decentriq.

dann einfach versucht zu verschleiern, zu sagen «Ups, keine Sorge, nichts passiert.» Stattdessen sollten Unternehmen voll auf Transparenz setzen und anerkennen: «Hey, wir haben ein Problem, das kann passieren in unserer Industrie, wie können wir zukünftige Vorfälle vermeiden?»

Da braucht es dann eben die Investitionen in moderne Datenerhebungs- und Datenschutzstrukturen, die wir bereits angesprochen haben.

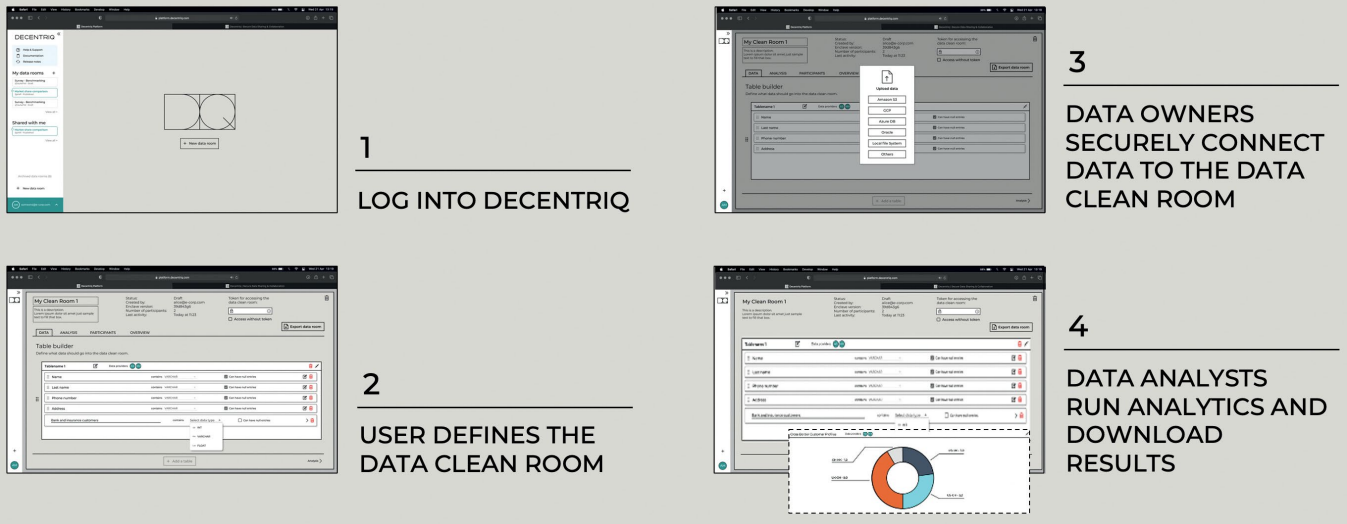
Wie sähe dann für Sie eine gute Investition aus? Was sind Projekte, vielleicht auch industrieweite Kollaborationen, in denen die Nutzung von Kundendaten sowohl bei Unternehmen als auch Kundinnen und Kunden zu einem Mehrwert führen würde?

Ein gutes Beispiel kommt für mich aus der Prävention von Cyber-Attacken. Diese geschehen in vielen Industrien ja wirklich ununterbrochen. Also die Großkonzerne weltweit werden 24/7 angegriffen. Das soll nicht zu dramatisch klingen – die meisten dieser Angriffe sind relativ ungefährlich – doch sie sind eine Konstante. Oft sind es einfache Algorithmen, die überprüfen, ob eine Tür offen ist. Tritt der Fall ein, hat diese Firma ein Problem. Aber dann gibt es natürlich auch ganz andere Kaliber von Angriffen. Meistens stecken da Hackergruppen dahinter und viele Firmen denken, dass sie keine Chance gegen diese organisierten Angriffe hätten. Doch dies ist etwas, da können sich Industrien gegenseitig helfen, indem sie Informationen zu diesen Angriffen miteinander teilen.

Wenn zum Beispiel die Mauro AG gerade mit einem speziellen Algorithmus angegriffen wird, dann ist die Wahrscheinlichkeit sehr groß, dass auch die Max AG aus derselben Industrie entweder zeitgleich oder kurz später damit angegriffen wird. Aber jetzt hat die Mauro AG gewisse sensitive Informationen über diesen Angriff, die der Max AG helfen könnte, aber kann oder möchte diese nicht mit der Konkurrenz teilen. Das heisst, man braucht irgendeine Partei – ein sog. Orchestrator, der diesen Unternehmen eine Plattform zu Verfügung stellt, in denen diese Angriffsdaten verschlüsselt zwischen allen Parteien geteilt werden können. Alle Parteien können mit sämtlichen Daten arbeiten, aber niemand sieht das gesamte Datenset. Dieses Modell ist nichts Neues – ich hatte gelesen, dass das in Amerika schon lange gang und gäbe ist, weil natürlich amerikanische Firmen tendenziell noch mehr Attacken sehen und sich viele alleine dagegen nicht wehren können. Es sind solche Projekte, welche einen klaren Mehrwert für alle Teilnehmenden bieten, aber trotzdem aus fehlender Kenntnis oder Angst vor Kontrollverlust oft nicht durchgeführt werden.

[1] https://www.netzwoche.ch/news/2021-10-14/microsoft-meldet-bislang-groessten-ddos-angriff-auf-azure

Abb. 3: Run Collaboration in Minutes



Quelle: Decentriq.

Über Cyber-Security hinaus gibt es da natürlich noch weitere Zusammenarbeitsmöglichkeiten – z.B. das Teilen von Kundendaten zwischen Herstellern und Einzelhändlern, um eine einheitliche Kundenerfahrung zu schaffen. Voraussetzung ist natürlich, dass diese Unternehmen moderne Technologien einsetzen, um den Datenschutz und die Datensicherheit bestmöglich zu gewährleisten.

Vielleicht daran anschliessend und als letzte Frage: Würden Sie in dem Fall sagen, dass die steigenden Kundenbedürfnisse nach einer digitalen Privatsphäre vereinbar sind mit dem Bedürfnis vieler Unternehmen, auch sensible Daten für die Wertgenerierung zu nutzen?

Absolut. Für mich ist das keine binäre Geschichte. Es ist kein «Entweder-Oder» und ich finde diese Reduktion auch immer ein bisschen schade. Das Wichtigste ist, einen offenen Dialog zu führen – gesellschaftlich und mit den eigenen Kunden. Alles was extrem ist, scheitert irgendwann, dafür gibt es genügend Beispiele. Es kann einem nicht komplett egal sein, aber man kann sich vor diesen Entwicklungen auch nicht verstecken.

Wir können anerkennen, dass moderne Datenauswertung Gefahren mit sich bringen kann. Aber es gibt bereits heute wirklich viele Technologien, welche diese Gefahren mitigieren können. Ich betone mitigieren – nichts ist eine 100%ige Lösung. Aber die Firmen, welche sich diese Technologien angeeignet haben über die letzten Jahre, die haben neben der Expertise auch kulturell davon profitiert. Es ist extremst wichtig, im Unternehmen diese Datenschutz-Awareness zu schaffen. Die Technologien können Probleme mitigieren, aber die Mitarbeiterinnen und Mitarbeiter sind durch das Führen dieses Datenschutzdialoges auch viel offener und kreativer bei der Arbeit. Aus dem Nutzen von diesen neuen Technologien entstehen wiederum neue Instrumente, welche ein Unternehmen auf dem Markt besser aufstellen. Wir bei Decentriq haben das jetzt schon oft gehört von Firmen, die über die letzten Jahre in solche Projekte investiert haben. Plötzlich fragen andere Firmen in der Industrie, wie sie nachziehen können. Das ist natürlich erst mal ein Kompliment und Image-Boost für diese Firma – der Market-Leader zu sein. Doch viel wichtiger ist, dass diese Unternehmen jetzt einen zukunftsgerichteten Vorsprung haben, den sie weiter ausbauen können.

Das passt ja wunderbar als Schlusswort – danke Ihnen vielmals für Ihre Zeit und Ihre Antworten!