IM INTERVIEW: INÉS ATUG, TIMO KOB

„Google ist mein Gegner von morgen“

Die Spezialisten von Hisolutions über die Cybersicherheit deutscher Banken und die Risiken von Cloud-Auslagerungen für ihre Daten und ihre Strategie

Sicherheitslücken, offene Flanken im Datenschutz, unzureichende Prüfberichte und auch strategische Fallstricke: Wenn Banken Daten und Aktivitäten in die Cloud auslagern, lauert eine ganze Reihe an Risiken, wie Inés Atug, Senior Expert, und Timo Kob, Vorstand des IT-Managementhauses Hisolutions, im Interview der Börsen-Zeitung erläutern.

Börsen-Zeitung, 5.9.2020

■ **Herr Prof. Kob, vor drei Jahren bescheinigten Sie den deutschen Banken Nachholbedarf in Sachen Cyber-Security, auch wenn diese, wie Sie sagten, im Vergleich zu anderen Branchen gar nicht so schlecht dastünden. Gilt dies immer noch?**

Kob: Ich würde nicht sagen, dass dies falsch ist, wenngleich die übrigen Branchen inzwischen erfreulicherweise aufgeholt haben. Die Frage ist aber, inwieweit die unter enormem Kostendruck stehenden Finanzdienstleister neue Gefährdungen abfedern können.

■ **Wie sehen diese aus, Frau Atug?**

Atug: Phishing-Angriffe etwa werden immer präziser und nutzen auch neue Techniken: Es geht nicht mehr nur darum, Passwörter abzugreifen. Angreifer betreiben parallel Social Engineering per Telefon und versuchen in der kurzen Zeitspanne, in welcher die dabei gewonnenen Zugangsdaten dann gültig sind, Zugriff zu erhalten. Gerade bei Fintechs bin ich etwas skeptisch, was deren Absicherung angeht.

■ **Weil diese nicht so viele Mittel haben, um in ihre Sicherheit zu investieren?**

Atug: Das ist ein Punkt. Ein zweiter: Es fehlt der Druck von außen. Die Regulierung ist nicht hundertprozentig.

■ **Weil die BaFin im Falle der Fintechs, die keine Vollbanklizenz besitzen, den Daumen nicht draufhat?**

Atug: Genau.

■ **Die Aufsicht gibt Banken noch immer durchwachsene Noten. Bei der BaFin heißt es, nach Noten wären die besten Banken bei 3. Es seien aber auch vielen Fünfen dabei. Wo sind die Schwächen?**

Kob: Die BaFin hat ihr Hauptaugenmerk in letzter Zeit gar nicht auf den klassischen Betrug gelegt, sondern auf die Verfügbarkeit der IT und die Frage, wie schwierig es ist, eine Bank aus dem Geschäft zu nehmen. Da gab es jede Menge Mängelfeststellungen und massiven Druck auf die Institute, die das Thema Verfügbarkeit unterpriorisiert und dann in der Cloud vielleicht auch die einfache Lösung gesucht haben, nach dem Motto: Jetzt ist es in der Cloud, da kann nichts mehr passieren. Die Verfügbarkeit aber ist ja auch gesellschaftlich relevanter: Wenn die Deutsche Bank wegen einer Ransomware ein paar Millionen auf den Tisch legt, kann mir das als Kunde des Instituts egal sein. Wenn aber ein Angriff von nicht befreundeten Staaten in diesem nicht ausgesprochenen Kalten Krieg, den wir nun einmal haben, auf den Bankensektor stattfindet oder dort einfach nur das Vertrauen erschüttert, dann ist der Staat deutlich stärker betroffen. Da haben die Banken ihre Schutzmaßnahmen auch verbessert. Die Note 3 würde bei den besseren Häusern wahrscheinlich auch ich als angemessen ansehen, weil das Thema halt wahnsinnig komplex ist.

Atug: Vielfach ist die IT über Jahre gewachsen. Banken operieren häufig noch mit Großrechnern, die sie wegen ihrer Geschwindigkeit schätzen, die aber teuer sind. Unter Kostendruck sind diese Mainframes dann natürlich die ersten Systeme, die sie ablösen möchten, ohne aber auf die Performance verzichten zu müssen. Da ist natürlich der Blick Richtung Cloud, wo ich mir Ressourcen holen kann, so, wie ich sie brauche, durchaus verständlich. Was aber häufig vergessen wird: Wenn ich alte Infrastruktur und neue Cloud-Strukturen zusammenbringe, muss ich auch die Prozesse anpassen. Gegebenenfalls kommt die alte Infrastruktur dabei gar nicht hinterher. Zum Beispiel, wenn die alte IT in Intervallen von sechs Monaten Updates erhalten hat, dies in der Cloud aber fortlaufend stattfindet.

■ **Ist das ein Sicherheitsproblem?**

Atug: Ja. Wenn ich einen sicheren Dienst mit einer unsicheren Anwendung kommunizieren lasse, kann dies den sicheren Dienst gefährden.

Kob: Das war auch in der Diskussion über eine Fusion von Deutscher Bank und Commerzbank einer der entscheidenden Knackpunkte: dass man die IT nicht zusammenbekommen hat, weil sie nicht kompatibel und so unheimlich komplex ist – von seit den siebziger Jahren in Betrieb befindlichen Systemen, die ich einfach nicht loswerde, bis hin zu modernen Welten, weil ich allein mit Mainframes natürlich keine modernen Vertriebswege, wie die Fintechs sie mir aufzwingen, ermöglichen kann. Das sind 50 Jahre Wildwuchs. Und der ist schwierig zu schützen. Da erscheint die Cloud als naheliegende Antwort. Aber eine Bank holt sich damit andere Risiken herein.

■ **Welche?**

Atug: Es hört sich so einfach an, wenn jemand sagt, er geht in die Cloud. Banken stellen sich häufig ein simples Lift-and-Shift vor. Dass sie eine alte Anwendung in diese virtuelle Maschine packen, und in der Cloud wird das dann schon laufen. Ich sichere die Cloud aber auch anders ab. Das heißt, gegebenenfalls wurden bei der Entwicklung dieser Anwendung Annahmen getroffen über die Sicherheit dieser Umgebung, in der die Anwendung betrieben wird, und diese Sicherheitsmaßnahmen sind in der Cloud gar nicht vorhanden.

■ **Nehmen mit dem vermehrten Gang von Banken in die Cloud deren IT-Risiken zu?**

Kob: Das würde ich so allgemein nicht sagen, aber: Die Anforderungen ändern sich. Manche Sachen werden leichter, andere müssen anders gedacht werden. Die Gefahr ist nur, dass Banken allein den Vorteil sehen, dass es einfacher wird – das hat ja auch den Aspekt, dass die Anwendungen weit weg sind, Hauptsache, nicht bei ihnen, sondern bei anderen, die dann dafür zuständig sind. Und dass sie das, was sie zugleich nicht an Änderungen eingekauft haben, wieder nicht berücksichtigt haben: dass sich also die Fehler fortsetzen, die schon zuvor gemacht haben. So greifen die sehr tradierten Modelle, welche Banken in der Entwicklung fahren, einfach nicht mehr. Das sind ganz andere Denkwelten. Da haben Banken auch gar nicht die richtigen Leute dafür. Und im momentanen Arbeitsmarkt ist eine Bank für einen jungen Informatiker, der frisch von der Uni kommt, jetzt auch nicht der attraktivste Arbeitgeber. Das heißt, die Leute in den Banken müssen sich da einarbeiten und sagen sich bei bestimmten Dingen auch: Na ja, ich mache das schon irgendwie passend. Und das wird manchmal zum Problem.

Atug: Was mache ich zum Beispiel bei einem Sicherheitsvorfall? Es ist ja nicht so, dass eine Bank dann beim Cloud-Anbieter einfach einmal reingehen und sagen könnte: Jetzt gebt mir mal die Festplatten, auf denen ich meine Daten gespeichert habe, ich müsste da eine forensische Analyse durchführen. Das geht leider nicht, weil sich eine Bank etwa eine Public Cloud mit vielen anderen Kunden teilt. Und die wollen ja nicht, dass diese Festplatte dann an jemand Fremden herausgegeben wird. Die großen Cloud-Anbieter sind da in der Regel auch nicht so kooperativ.

■ **Noch nicht konkret geklärt scheint ja auch, wie die Banken ihren aufsichtlichen Prüfpflichten bei den Cloud-Anbietern nachkommen können. Man arbeite mit den Cloud-Anbietern an einem akzeptablen Modus, hieß es bei der Bundesbank zuletzt. Ist das für eine Aufsicht ein valider Ansatz?**

Kob: Ich glaube, pragmatisch gesprochen wird es gar keinen anderen Weg geben.

■ **Müssten Aufseher nicht ganz anders an dieses Thema herangehen?**

Kob: Ich kann nachvollziehen, dass sich die Aufsicht der Cloud gegenüber öffnet. Das Konzept hat schon Vorteile, und die Cloud-Anbieter sind auch reifer geworden. Aber man muss nun auch bestimmte Regularien neu durchdenken. So forderte das Bundesamt für Sicherheit in der Informationstechnik (BSI) anfangs, Banken müssten exakt sagen können, welche Daten über welchen Server laufen und wo diese liegen. Das geht in der Cloud aber nicht. Also muss das BSI Sicherheit neu definieren. Ich würde aber auch nicht sagen, dass das BSI dies alles erst bis zum Ende durchdacht haben muss, bis wir dies den Banken ermöglichen. Das wäre wirtschaftlich einfach ein zu großer Wettbewerbsnachteil gegenüber den US-amerikanischen Instituten und den Fintechs.

■ **Das bedeutet: Mut zur aufsichtlichen Lücke.**

Kob: Mut, Regeln auch noch einmal nachträglich zu ändern.

Atug: Banken müssen jetzt daher überlegen, wie sie mit den Cloud-Anbietern entsprechende Zusatzvereinbarungen treffen können, um ihren Prüfpflichten nachzukommen. Der eine oder andere Cloud-Anbieter lässt sich diese Prüfmöglichkeit vergolden. Andere dagegen haben ein Interesse daran, dass die Banken ihre Cloud vermehrt nutzen.

■ **Google zum Beispiel.**

Atug: Zum Beispiel. Da die Cloud-Anbieter häufig aus den USA kommen, haben Banken nicht nur regulatorisch wegen der Bankenaufsicht, sondern auch auf Grund des Datenschutzes einiges zu prüfen. Meines Erachtens reicht das, was die Cloud-Betreiber derzeit von sich aus an Prüfberichten anbieten, nicht aus, um den Prüfanforderungen der Regulatoren nachzukommen. In den Prüfungen finden ja nur Stichproben statt. Für die Banken muss aber sichergestellt sein, dass das, was geprüft wurde, auch ihre Aktivitäten betrifft, dass zum Beispiel auch das Rechenzentrum in Frankfurt geprüft worden ist, in dem die Daten der Bank gespeichert werden. Da ist regulatorisch noch Raum für Verbesserungen. Auch für die Prüfer ist das schwierig: Die Cloud-Assets sind zwar da, solange eine Bank sie braucht, danach aber sind sie weg, und damit kann man sie nicht ein Jahr später identifizieren und anschauen.

Kob: Das ist jetzt nicht die riesige Prüflücke. Aber es ist weniger scharf, als es in der alten Welt war.

■ **Wie lässt sich dann sicherzustellen, dass die Banken ihre Prüfrechte tatsächlich durchsetzen können?**

Atug: Man schließt sich bei den Prüfungen zusammen.

■ **In Form von Pooled Audits.**

Atug: Ja, genau. Das ist ein Weg, den die Cloud-Anbieter mitgehen. Kann man das im Verbund der jeweiligen Bank organisieren, ist das auch eine Möglichkeit, mit den Cloud-Anbietern eher verhandeln zu können.

■ **Big Tech war ja nun nicht immer bekannt für einen besonders skrupulösen Umgang mit Kundendaten. Würde es überhaupt bemerkt, wenn ein Cloud-Anbieter die Daten, die ihm eine Bank, entgegen der Vereinbarung spiegeln und andernorts weiterverarbeiten würde?**

Atug: Genau deshalb brauche ich die Audit-Rechte. Ich gehe davon aus, dass die Cloud-Anbieter ordentlich arbeiten und dies nicht machen würden. Aber ich glaube auch, dass es sehr schwer wäre, im Nachhinein nachzuprüfen, dass nicht unerlaubt Daten weiterverarbeitet wurden. Das Spiegeln gehört nun einmal auch zur Verfügbarkeit einer Cloud hinzu. Denn indem in anderen Rechenzentren Redundanzen vorgehalten werden, habe ich eine andere Verfügbarkeit, und wenn in dem einen Rechenzentrum etwas ausfällt, habe ich in dem anderen Rechenzentrum Kapazitäten. Eine Herausforderung geht von dem Urteil des EuGH aus, dem zufolge die zwischen der EU und den USA getroffene Absprache Privacy Shield nicht mehr ausreicht, um bei einem Transfer von Daten in die USA die europäischen Anforderungen an den Datenschutz zu erfüllen. Aus meiner Sicht haben die Richter in ihrem Urteil deutlich gemacht, dass Unternehmen schon selbst prüfen müssen, ob die Datenschutzgrundverordnung von ihren Geschäftspartnern in den USA wirklich eingehalten werden können. Und das ist auf Grund der Gesetzgebung in den USA hinsichtlich Spionage schon schwieriger. Auch sieht die amerikanische Gesetzgebung, zum Beispiel der Patriotic Act etwa vor, dass die Behörden, wenn sie einen Terrorangriff vermuten, keinen gerichtlichen Beschluss benötigen, um auf etwas zuzugreifen, und der Zugriff darf unter Umständen nicht an die Bank gemeldet werden.

■ **Ohne Restvertrauen geht es also nicht, oder?**

Atug: Das ist im Outsourcing generell der Fall. Bei Auslagerungen in die Cloud fällt es uns aber nochmals schwerer, denn es ist häufig ein anderes Land mit anderen Gesetzen. Zudem: Wenn ich in ein Rechenzentrum auslagere, dann habe ich dort Leute, mit denen ich reden kann, und Vertragsverhandlungen mache ich nicht mit dem Vertrieb, sondern mit dem Geschäftsführer. So etwas stärkt das Vertrauen. Bei den Cloud-Anbietern bekommt man ein vorgefertigtes Vertragspamphlet, und wenn ich Zusatzvereinbarungen treffen möchte, kann das schon sehr langwierig sein. Und in der Regel treffe ich dann auch nicht den Chef von Microsoft oder Amazon Web Services.

■ **Cloud-Anbieter argumentieren ja damit, dass auf Wunsch der Kunden Server in Europa zum Einsatz kommen und Kunden zudem ihre eigene Verschlüsselung mitbringen können, so dass sie, selbst wenn sie wollten, keinen Zugriff auf die Daten hätten. Ist das eine probate Lösung oder eher PR?**

Atug: Das ist schon viel PR. Denn Datenspeicherung ist das eine, Datenverarbeitung das andere. Es kann durchaus sein, dass die Daten in Deutschland gespeichert werden, verarbeitet werden sie aber unter Umständen in Irland, in den USA oder irgendwo auf der Welt, je nachdem, wo der Dienst, den ich gebucht habe, vorhanden ist. Wenn ich also eine Microsoft-Cloud nutze und in Frankfurt speichere, muss ich damit rechnen, dass Teile meiner Anmeldung etwa in Irland verarbeitet werden. Und wenn die Regulatorik sagt, es darf nur in Deutschland sein, wäre das zum Beispiel schon einmal ein Problem. Auch hier gibt es aber eine Lernkurve bei den Cloud-Anbietern. Eine Verschlüsselung wiederum können Banken tatsächlich auf sicherem Wege selbst generieren und diese in die Cloud übertragen. Rein theoretisch gedacht hat ein Administrator auch dann die Möglichkeit, darauf zuzugreifen. Dedizierte Module erhöhen die Sicherheit, sind aber teuer. Insgesamt sind die Cloud-Anbieter schon bemüht, mehr Sicherheit anzubieten.

Kob: Ich will noch eine andere, volkswirtschaftlich spannende Frage jenseits der Cybersicherheit ansprechen: Wer profitiert bei den Auslagerungen eigentlich auf der langen Strecke von wem? Google hat eine Banklizenz und will Girokonten herausgeben, Apple hat Apple Pay. Was also ist das Know-how, das Banken haben, das Google noch nicht hat? Es sind die Prozesse, wie solche Transaktionen ablaufen. Wenn ich diese aber genau in die Hände desjenigen gebe, der mein Konkurrent von morgen ist, dann gebe ich ihm in gewissem Sinne die Blaupause und zeige ihm, wo ich angreifbar bin. Das erleben wir schon bei Amazon, die plötzlich Batterien herstellen, weil sie festgestellt haben, dass diese sich sehr gut bei ihnen verkaufen.

Atug: Da geht es um Datensouveränität. Facebook und die anderen haben erkannt, dass Daten ein nicht vergänglicher Rohstoff sind, dass sie Daten sammeln, analysieren, damit arbeiten und auf diese Weise Geld verdienen können. Im Endeffekt geben Banken ihr Know-how, ihre Kunden-, aber auch ihre internen Daten einem Provider, der damit arbeiten kann.

Kob: Sie müssen ja nicht an die Kundendaten gehen und damit einen Bruch der Vertraulichkeit begehen. Aber im Rahmen der Arbeit muss natürlich offengelegt werden, wie eine Bank arbeitet. Denn wie soll sonst die Cloud funktionieren? Für die Banken geht es damit nicht nur darum, ihre Daten zu schützen, sondern eben auch, wie sie mit diesen umgehen. Das ist die geschäftspolitische Frage: Ist der Partner ein Freund oder kein Freund? Und ich habe manchmal noch den Eindruck, dass in Banken noch immer gedacht wird: Google, das ist doch diese Suchmaschine. Nein: Google ist mein Gegner von morgen, den ich damit entsprechend hochfahre. Manchmal aber haben sich die Verhältnisse inzwischen so gedreht, dass Banken gar keine Alternativen zum Outsourcing haben.

■ **Eine ernüchternde Bilanz: Die Datensicherheit ist nicht unbedingt gewährleistet, Prüfpflichten ein laufender Prozess, und hinzu kommt die Gefahr der strategischen Selbstentleibung. Da müssten Sie doch schreiend durch die Gegend laufen und Bankvorstände vor Auslagerungen in die Cloud warnen.**

Kob: Nein. In der Datensicherheit erkaufen sich die Banken Vorteile mit gewissen Nachteilen, aber ich würde nicht sagen, dass eine Bank in der Cloud unsicherer ist bezüglich des Themas Vertraulichkeit. Im Bereich der Verfügbarkeit haben Sie sogar gewisse Vorteile, dadurch bekomme ich auch Vorteile in der Flexibilität meiner Anwendungen und in der Sicherheit. Aber: Ich muss mir eben über die Schattenseiten bewusst sein. Wie es der frühere Telefónica-Deutschland-Chef Thorsten Dirks schon sagte: Wenn Sie einen Scheißprozess digitalisieren, dann haben Sie einen scheißdigitalen Prozess.

■ **Wie groß ist die Gefahr, dass einer der großen Cloud-Anbieter Opfer eines Hackerangriffs wird? Was gibt es schönere Ziele als ein Haus, in dem sich Daten von gleich mehreren Banken erbeuten lassen?**

Kob: Die großen Cloud-Anbieter haben die besten IT-Security-Abteilungen, die man auf dem Planeten findet. Ich glaube schon, dass sie so viel Abschreckungsmacht aufgebaut haben, dass der Weg für Angreifer schon sehr lang ist. Vor ein paar Jahren aber war das noch ganz anders.

■ **Brauchen Europas Banken einen europäischen Cloud-Anbieter?**

Kob: Wird das Projekt Gaia-X ein Erfolg, wäre es sicher etwas, was Banken nicht schlecht zu Gesicht stehen würde.

Atug: Ich fände es gut, wenn zumindest Teile der IT-Infrastruktur in Europa verbleiben würden. Leider haben wir das verschlafen. Die Amerikaner haben schon in den neunziger Jahren damit angefangen.

> *„Man wird in gewissen Punkten nicht mehr wettbewerbsfähig werden, aber vielleicht kommt man an den Punkt, an dem diese Nachteile nicht so schwer wiegen, dass man diesen Weg mit einem US-Anbieter gehen muss.“*

Kob: Man wird in gewissen Punkten nicht mehr wettbewerbsfähig werden, aber vielleicht kommt man an den Punkt, an dem diese Nachteile nicht so schwer wiegen, dass man diesen Weg mit einem US-Anbieter gehen muss.

Atug: Es gibt ja auch in Europa einige Cloud-Anbieter. Die sind aber eher im Mittelstand angesiedelt. Und ob eine Bank darauf verzichten kann, in die Cloud zu gehen? Das stelle ich mir schwierig vor.

Kob: Um einen europäischen Cloud-Anbieter zu etablieren, muss aber auch die erforderliche Nachfrage da sein. Die Telekom hat ja, teilweise mit Microsoft, schon versucht, Angebote zu machen, und ein Treuhändermodell zugesichert, damit die Daten nicht nach Amerika gehen. Der Preis, der dafür zu zahlen war, war nicht in Euro, sondern, dass bestimmte Features nicht erhältlich waren oder eben später kamen. Das hat der Markt aber nicht angenommen. Der Dienst wurde eingestellt.

Atug: Aus der Industrie kam das Feedback: Wenn die Features nicht da sind, gehe ich halt doch in die normale Cloud. Das ist dann auch bei Microsoft angekommen.

Das Interview führte Bernd Neubacher.

ZUR PERSON

Sicherheitsleute

Fotos: Lotte Ostermann

Inés Atug Timo Kob

bn – Inés Atug ist Senior Expert, Timo Kob Vorstand und Gründer des Security- und IT-Management-Beratungshauses Hisolutions, das eigenen Angaben zufolge für 75 % der Top-20-Banken im deutschsprachigen Raum arbeitet. Atug arbeitet seit 2012 in der Informationssicherheit und befasst sich vor allem mit dem Themenfeld Secure Cloud-Computing und Kryptografie. Die Managerin, die an der Open University im britischen Milton Keynes ein Studium der Mathematik sowie an der Ruhr-Universität Bochum in Applied IT Security absolvierte, berät und begleitet Unternehmen bei der Einführung von Informationssicherheitsmanagement-Systemen und agiert als Prüferin Kritischer Infrastrukturen (Kritis). Sie ist Penetration Tester, zertifizierte Datenschutzbeauftragte und hält neben anderem die Zusatzqualifikation IT-Grundschutz-Praktiker des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Prof. Timo Kob ist seit 1992 national und international in der Beratung von Unternehmen, Behörden, Regierungen und supranationalen Institutionen in Fragen der IT und Cybersicherheit tätig. Zu diesen zählen das BSI, das österreichische Bundeskanzleramt, die OSZE sowie die europäische Agentur für Netzwerk- und Informationssicherheit (Enisa). Kob, Mitautor des BSI-Standards „Notfallmanagement“, lehrt als Professor an der FH Campus Wien und forscht in den Feldern Informationssicherheit, Cyberspionage sowie Wirtschaftsschutz.

(Börsen-Zeitung, 5.9.2020)

OUTSOURCING

Abflug in die Wolke

Börsen-Zeitung, 5.9.2020

bn – Deutschlands Finanzsektor zieht es in die Datenwolke. So hat allein Google binnen Jahresfrist die Deutsche Börse, die Deutsche Bank sowie Finanz Informatik Technologie Service, die Tochter des Sparkassen-IT-Dienstleisters, als Kunden akquiriert; die Commerzbank nutzte den Cloud-Anbieter schon zuvor. Während die Sparkassen neben Google deren Konkurrenten Amazon, IBM und Microsoft anbinden wollen, plant die Deutsche Bank im Zuge einer exklusiven Partnerschaft mit Google auch eine gemeinsame Produktentwicklung.

Auch unter Europas Großbanken greifen Auslagerungen in die Datenwolke um sich, wie die Bundesanstalt für Finanzdienstleistungsaufsicht feststellt. Die meisten Institute versuchten, Cloud-Technologie-Lösungen in ihre Systemlandschaft zu implementieren, hießt es im jüngsten Jahresbericht. Was Auslagerungen kritischer Prozessen in öffentliche Clouds angeht, hielten sich die Häuser angesichts von Cyberrisiken, Datenschutz- und Verschlüsselungsfragen indes „weiterhin deutlich zurück“.

(Börsen-Zeitung, 5.9.2020)