IM INTERVIEW: TIMO KOB, HISOLUTIONS

„Da wird stark aufgeräumt“

Experte diagnostiziert „Hallo-wach-Effekt“ bei den Bankenaufsehern in Sachen Cybersecurity und warnt vor einer Wiederholung von Fehlern der Vergangenheit

Im Vergleich zu anderen Branchen stehen die deutschen Banken mit ihrer IT-Sicherheit im Grunde gar nicht einmal so schlecht da, wie der Cybersecurity-Experte Timo Kob meint. Das Problem: Die Bedrohungen haben deutlich zugenommen, die Täter sind professioneller geworden, die Schadenvolumina sind gestiegen, und Banken wie Aufseher haben Nachholbedarf.

Börsen-Zeitung, 17.1.2017

Herr Prof. Kob, die Bundesbank unternimmt eine Reihe von Sonderprüfungen der IT deutscher Banken. Steht es wirklich so schlimm um die Informationstechnik der deutschen Kreditwirtschaft?

Das ist eine Frage des Blickwinkels. Wenn man die deutsche Bankenlandschaft mit der Wirtschaft vergleicht, würde ich sagen: nein. Denn im Durchschnitt sind die Finanzdienstleister besser geschützt und vorbereitet als die meisten anderen Branchen, weil sie schon seit vielen Jahren über die Mindestanforderungen ans Risikomanagement der deutschen Aufsicht oder über den Baseler Ausschuss reguliert sind und daher schon viel früher entsprechende Anstrengungen auch in ihrer IT unternommen haben. Andererseits ist hundertprozentig natürlich niemand sicher, erst recht nicht, was die sich momentan immer stärker auftuenden Schwachstellen angeht. Und Banken sind natürlich ein besonders attraktives Opfer, denn in einer Bank kommt man direkt an Geld. Im Falle eines Maschinenbauers ist eine Monetarisierung der Beute da etwas schwieriger.

Deswegen haben sich Banken auch besser zu schützen.

Als attraktives Ziel muss man einfach mehr tun.

Für Außenstehende bleibt allerdings der Eindruck, dass sich die Störfälle, ob nun intern oder extern verursacht, häufen: Deutsche Bank und Commerzbank hatten in diesem Jahr Ausfälle in ihrem Online-Banking, die britische Tesco Bank wurde gehackt. Täuscht der Eindruck?

Zum einen hat sich die Sensibilität erhöht. Eine Nachricht, die vor ein paar Jahren vielleicht noch unter ferner liefen gelaufen wäre, erhält inzwischen eine höhere Aufmerksamkeit. Und auch die Banken haben eine andere Sicht: Früher haben sie sich als Opfer geschämt. Inzwischen

> *„Die Angriffe sind einfach gut orchestriert, mitunter auch mit Hilfe von Know-how, das von in der Bank sitzenden Tätern stammt. Da ist es einfach sehr schwer, sich zu verteidigen.“*

befinden sie sich damit ja in den besten Kreisen. Sie sind also eher bereit, einen Fall öffentlich zu machen. Früher gab es auch Vorfälle, die wurden aber vermehrt unter der Wasseroberfläche mit den betroffenen Kunden reguliert.

Gibt es jetzt mehr oder weniger Fälle?

Die Bedrohung hat definitiv zugenommen. Es sind mehr Täter geworden, und sie sind professioneller als früher. Diese Professionalität hat wiederum zwei Dimensionen: Sie zeigt sich einmal in besseren Angriffen und zugleich in jeweils höheren Schadenvolumina. Früher hat sich der einzelne Täter vielleicht mit – ich möchte jetzt nicht sagen: Peanuts …

Das wäre die Einheit von 25 Mill. Euro.

Früher war es vielleicht ein Viertel Peanuts. Jetzt geht es schon eher um mehrere Peanuts oder schon ein kleines Schälchen mit Erdnüssen. Die organisierte Kriminalität steigt stärker ein, und damit ist das Schadenvolumen pro Fall deutlich angestiegen.

Sind die Banken dafür gewappnet?

Na ja, wir reden vom Bankensektor ja nicht als eine prosperierende Branche. Der Kostendruck in den Instituten in den vergangenen Jahren ist auch an der IT nicht vorbeigegangen. Der Vorsprung, den die Branche vor zehn, 15 Jahren noch hatte, der ist ein bisschen aufgefressen worden, indem man gesagt hat, wir machen auch nicht mehr als nötig.

Warum?

Nach Beginn der Finanzkrise war klar zu beobachten, dass das Thema in den Hintergrund geraten ist. Das gilt im Übrigen auch für die Deutsche Bundesbank und für die BaFin, die auf das Thema dann einfach weniger Augenmerk gelegt haben. Und jetzt ist man auf beiden Seiten dabei, das etwas nachzuholen.

Zuletzt kamen von den Aufsehern ja beinahe dramatische Appelle an die Banken, ihre IT zu verbessern. Spricht daraus ein schlechtes Gewissen?

Sicherlich gibt es da einen gewissen Hallo-wach-Effekt und wohl auch das Gefühl, dass man früher darauf hätte achten sollen. Man hat es lange einfach unterschätzt. In vielen Fällen hat man auch eher nicht intentionale Probleme thematisiert, wenn es etwa ums Thema Verfügbarkeit ging – zum Beispiel einen Stromausfall. Man kennt das ja, dass Risikowahrnehmung und echtes Risiko deutlich auseinanderlaufen können. Das Thema Hacker war unsichtbar und konnotiert mit dem genialen Einzeltäter. Geniale Einzeltäter gibt es halt überschaubar viele. Und jetzt sieht man auf einmal: Man muss kein technisches Genie sein, sondern nur kriminelle Energie haben, und wenn dann noch kriminelles Talent hinzukommt … Die Angriffe sind einfach gut orchestriert, mitunter auch mit Hilfe von Know-how, das von in der Bank sitzenden Tätern stammt. Da ist es einfach sehr schwer, sich zu verteidigen. Das wäre es auch, wenn man perfekt vorbereitet wäre.

Wie stehen denn insgesamt kritische Infrastrukturen in Deutschland und deren Regulierung im europäischen Vergleich da?

Das kann man daran ablesen, dass die Vorbereitungen auf die EU-Richtlinie zur Netz- und Informationssicherheit (NIS) für andere Länder noch viel größere Probleme mit sich bringt als für deutsche Unternehmen. Die NIS ist die EU-Variante des deutschen IT-Sicherheitsgesetzes. Im Ausland hat man noch gar nichts an solchen nationalen Regelungen.

Hierzulande gibt es ja schon ein IT-Sicherheitsgesetz, im Ausland nicht.

Da gibt es auch kein Bundesamt für Sicherheit in der Informationstechnik. In dieser Hinsicht ist Deutschland schon wieder der Musterknabe in der EU. Dennoch muss die NIS gerade hierzulande mit einem wahnsinnigen Druck umgesetzt werden. Eigentlich läuft die Frist bis Mai 2018. Bis zur Bundestagswahl im September 2017 kann man aber damit nicht warten. Die erste Sitzung des neuen Kabinetts dürfte kaum vor November oder Dezember nächsten Jahres stattfinden, und da wird man sich auch nicht zuerst mit IT-Fragen beschäftigen wollen. Das heißt, die Zeit reicht nicht aus, um es nach der Wahl zu erledigen. Sprich: Das Ding wird jetzt durchgeprügelt. So hatten die Verbände gerade einmal eine Woche Zeit, um den Referentenentwurf zu kommentieren. Jetzt werden die Kommentare binnen zweier Wochen eingebaut, und Ende Januar schon kommt das Gesetz ins Kabinett. Viele sind baff, was da jetzt in der Umsetzung auf sie zukommt, denn viele hatten sich bisher noch nicht so richtig darum gekümmert, weil eben das IT-Sicherheitsgesetz und die EU-Datenschutzgrundverordnung im Vordergrund standen. Da behaupte noch einer, Politik funktioniere langsam.

Was kommt denn auf die Banken zu?

In der NIS tauchen zum Beispiel Vorgaben auf, die etwa nicht nur die klassischen Infrastruktursektoren wie Telekom, Versorger und Finanzen betreffen, sondern, was bisher häufig übersehen wurde, auch digitale Dienste wie Cloud-Anbieter, Suchmaschinen und, da wird es spannend auch in Sachen Fintech, Online-Marktplätze. Und ein Online-Marktplatz ist alles, wo ich Leistungen Dritter kaufe. Das könnte schon bei der Fondsgesellschaft beginnen.

Heißt das, dass ein Plattformbetreiber, der Fonds vertreibt, die Anforderungen der Richtlinie wird erfüllen müssen?

Das ist die Frage, die noch nicht bis zum Ende durchdefiniert ist. Klar ist aber, dass sich etwa von einem Marktplatzgedanken getragene Fintech-Modelle eben auch mit der NIS beschäftigen sollten.

Wenn Banken jetzt in ihre IT investieren wollen, wo sollen sie dann überhaupt anfangen?

Was auf jeden Fall nicht mehr reicht, ist zu denken: Ich stelle mir vorn eine Firewall hin, und hinten packe ich einen Virenscanner drauf. Das reicht vielleicht für den dummen Angreifer, aber nicht gegen einen hochmotivierten und erst recht nicht gegen einen hochmotivierten, klugen Angreifer.

Was muss also passieren?

Der erste Fehler hat gar nichts mit Technik zu tun, sondern mit dem Glauben, dass man außen in guter mittelalterlicher Tradition eine Burgmauer hochzieht, und innen braucht man die Tür dann nicht weiter abschließen. Das hat vielleicht im Mittelalter funktioniert, aber heute nicht mehr. Der Glaube, es gebe einen im Hause, der für IT-Sicherheit zuständig ist, und die anderen leben weiter auf einer Insel der Glückseligkeit, der funktioniert halt nicht. Jede Applikation, die ich habe, egal wo sie liegt und ob es dabei eine Schnittstelle zum Kunden nach außen gibt oder nicht, hat ein Angriffspotenzial, und dementsprechend muss ich in jeder Applikation vom ersten Tag an das Thema Sicherheit berücksichtigen.

Geschieht dies denn nicht?

Das Problem ist: Banken haben ganz viele Anwendungen, bei denen sie das eben nicht mitgedacht haben. Im besten Fall wurde nachträglich für die Sicherheit gesorgt, im schlimmsten Fall nicht. Das heißt, wenn ich jetzt in diese Anwendung hineingehe, weil ich sie schützen will, dann werde ich immer nur eine zweitklassige Sicherheit erreichen, weil sie eben nicht von Anfang an berücksichtigt worden ist.

Muss man sich das so vorstellen, dass es in jeder Bank noch einen Ozean früher entwickelter Anwendungen gibt, die noch nicht gesichert sind?

Wo jedenfalls das Thema IT-Security stiefmütterlich oder erst nachträglich berücksichtigt wurde, weil man sich darauf verlassen hat, dass man ja vor der bösen Außenwelt schon geschützt wird. Jetzt aber erlebt man, dass der Täter drinnen sitzt, dass die Angriffe so klug sind, dass sie alle Hürden überschreiten, dass man drinnen aber nicht darauf geachtet hat, ob es dort Indizien für einen Täter gibt. Das ist wie bei einer Alarmanlage. Man kann seine Außenhaut schützen, und man kann drinnen Bewegungsmelder einbauen. Wenn das eine nicht mehr greift, wirkt das andere. In den Banken muss man wegkommen vom Gedanken „Jemand schützt mich“ hin zum Gedanken „Jeder muss selbst seinen Beitrag dazu leisten“. Die Schweizer sagen immer: Wir haben keine Armee – wir sind eine Armee. So muss jede Fachabteilung einer Bank in der IT nicht ein notwendiges Übel sehen, sondern einen eigenen Beitrag leisten, sich zu schützen.

Was brauchen denn Banken, um für den Fall vorbereitet zu sein, dass Täter trotz der Vorkehrungen in ihre Systeme eingedrungen sind?

Zuallererst eine Angriffserkennung. Aktuell dauert es im Schnitt 180 Tage, bis ein Einbrecher entdeckt wird. Eine der wichtigsten Aufgaben ist es daher, diese Zeit zu verkürzen. Dann müssen Sie etwa Krisenstabsübungen aufsetzen. Sie dürfen Spuren nicht verwischen, müssen sich aber auch darüber bewusst sein, dass es in den meisten Fällen gar nicht darum geht, den Täter zu finden, sondern nur darum herauszufinden, wie er es gemacht hat und ob er wirklich wieder draußen ist, um noch in Zukunft sicher zu sein. Denn der Glaube, solche Fälle aufklären und den Täter ausfindig machen zu können, zerstäubt oft genug an der Realität, weil das bei guten Tätern oft einfach nicht mehr nachzuvollziehen ist.

Sind Ihnen denn überhaupt Fälle bekannt, in denen Täter dingfest gemacht wurden?

Das sind meistens die Fälle, in denen es um Innentäter geht, wo also eine große Gelegenheit auf eine geringe Kompetenz stößt. Wo es wirklich um größere Summen geht und denn auch höhere Hürden zu überwinden sind, ist es schwierig, und wenn man Täter findet, dann sind es meist nur dumme Hilfskräfte. An die Leute im Hintergrund kommt man auch dann meistens nicht heran.

Haben Sparkassen und Genossen, hinter denen jeweils große IT-Dienstleister stehen, bessere Chancen, Cyberattacken abzuwehren, als kleine Privatbanken?

Natürlich sind die Skaleneffekte einer großen Gruppe in diesem Zusammenhang schon eine Menge wert. Die Gefahrensituation sieht ja grundsätzlich für jede Bank erst einmal identisch aus. Das kleine Unternehmen mit einem geringeren IT-Etat hat daher nicht dieselben Möglichkeiten wie ein Großkonzern oder ein Bankenverbund. Da gilt in kleinen Banken manchmal immer noch das Sankt-Florians-Prinzip nach dem Motto „Ich bin ja so klein, es wird schon jemand anderen treffen“. Dafür aber haben kleinere Banken oft ein deutlich schärferes Profil mit entsprechend besser angepassten Prozessen als eine Universalbank. Dort ist die Prozess- und Anwendungslandschaft notgedrungen so komplex, dass sich in diesem Dschungel auch ganz andere Lücken auftun können. Deshalb kann ich Ihre Frage nur mit einem entschiedenen Berater-Jein beantworten.

Was leitet sich denn daraus für den Aufstieg der Fintechs ab, denen es allzu oft ja erst einmal darum geht, Minimum Viable Products zu entwickeln, also Produkte mit absoluten Mindestanforderungen? Ergeben sich da neue Dimensionen von Problemen für die IT-Sicherheit?

Ja, vor allem ist das Gefühl da, dass man alle Fehler wieder von vorn durchgeht. Das Versäumnis, IT-Sicherheit nicht von Anfang an zu denken, wiederholt sich scheinbar.

Woher kommt das?

Das ist natürlich dem amerikanischen Gedanken des Fast Fail geschuldet. Es ist ja tatsächlich nicht so, dass man durch die Compliance-Regeln, die einem auferlegt werden, noch besonders agil ist und ein besonders kreatives Umfeld haben kann. Das ist ja auch nicht das ursprüngliche Geschäftsmodell der Banken. Jetzt braucht man aber das Kreative, das Agile und die Einstellung, einfach einmal etwas ausprobieren zu können, und wenn es nicht funktioniert, landet es auf dem virtuellen Friedhof. Das Problem sind aber nicht die Ansätze, die scheitern, sondern diejenigen, die funktionieren. Denn sie sind schnell auf den Markt gebracht worden, um zu schauen, ob das Geschäftsmodell funktioniert, natürlich wieder ohne das erforderliche Sicherheitsdenken. Dann entsteht dieselbe Situation, die wir vorher hatten: Man muss im Nachhinein versuchen, die Sicherheit zu implementieren, was dann wieder zu den größten Problemen führt.

Was ist zu tun?

In der IT reden Banken inzwischen von einer IT zweier Geschwindigkeiten: Auf der einen Seite die klassische, seriöse, aber etwas langsame IT, auf der anderen Seite schnelle Lösungen, um auf Anforderungen von Fachbereichen einzugehen. In diese Richtung müssen wir auch im Bereich Security gehen: einen Weg zu finden, einerseits die Sicherheit zu haben, dass ich langfristig wieder in die Compliance-Anforderungen eines großen Modells reinlaufen kann, ohne andererseits aber kreative Geschäftsmodelle schon am Anfang dadurch abzutöten, dass ich ihnen diesen ganzen Ballast an den Hals hänge. Und da stehen alle Banken eigentlich noch am Anfang bei der Aufgabe, diese Balance zu finden, also Sicherheit von Anfang an mitzudenken, ohne an Geschwindigkeit zu verlieren. Das ist die große Herausforderung. Und da habe ich so viele gute Lösungen noch nicht gesehen.

> *„Aktuell dauert es im Schnitt 180 Tage, bis ein Einbrecher entdeckt wird. Eine der wichtigsten Aufgaben ist es daher, diese Zeit zu verkürzen.“*

Haben die Aufseher dieses Problem denn auf dem Schirm?

Ich kenne noch keine konkreten Fälle, in denen Aufseher schon irgendetwas mit einem Fintech zu tun haben. Ich würde von den Gesprächen, die ich führe, und den Sonderprüfungen, die ich vor der Nase habe, sagen, dies ist ein Thema, auf das auch die Aufsicht noch kein großes Augenmerk gelegt hat.

Warum nicht?

Die haben so viele andere Baustellen zu bearbeiten. Und die Aufseher richten sich natürlich auch immer danach, wo gerade etwas passiert ist. Im Grunde fahren BaFin, Bundesbank und EZB da ein reaktives Geschäftsmodell. Deswegen glaube ich, dass die mit Fintechs verbundenen Risiken aktuell noch nicht so auf dem Radar stehen.

Bringen die Aufseher denn überhaupt das Know-how mit, die IT größerer Banken zu verstehen, wenn sie diese prüfen?

Man kann über die Jahre den Reifegrad der Prüfungen sehr schön verfolgen. Vor der Finanzkrise schmunzelten Banken noch ein wenig über das, was da geprüft wurde. Da wurden vor allem Häkchen gemacht, ohne dass die IT deshalb immer verstanden wurde. Bis zur Finanzkrise hat das funktioniert. Entsprechend haben die Banken das Thema locker genommen und sich gesagt, wir machen mal das, was sinnvoll ist, und für den Rest bauen wir Potemkinsche Dörfer – und das war immer noch mehr, als andere Branchen ta-

> *„Entsprechend haben die Banken das Thema locker genommen und sich gesagt, wir machen mal das, was sinnvoll ist, und für den Rest bauen wir Potemkin’sche Dörfer.“*

ten. Mit der Finanzkrise verschwand das Thema vom Radar, und jetzt steht es wieder auf der Agenda. Die Professionalität, die in den Prüfungsinstanzen inzwischen aber vorhanden ist, ist ganz erstaunlich. Das ist wirklich sehr gut.

Man hört ja tolle Sachen von Prüfungen. Da geht es mal um eine unabhängige Code Review, mal um Beanstandungen, es lägen nicht genügend Kilometer zwischen der Bank und deren Notfallzentrum. Wo wollen die Aufseher mit ihren Prüfungen hin? Wo ist das Konzept?

Konzept ist an diesem Punkt ein schönes Wort. Die erste Absicht war sicher, bei den Banken mit dem aufzuräumen, was teilweise beim Thema Outsourcing passiert ist. Da geht es jetzt darum, dass Banken eine Gesamttransparenz und Gesamtverantwortung darstellen müssen. Das Thema spielt dabei tatsächlich in einer technisch und organisatorisch hochwertigen Liga. Das zieht sich bis zu Fragen wie „Wie bereitet ihr euch auf Krisen vor? Wie bindet ihr euren Outsourcing-Partner mit ein?“ Da ist die Prüftiefe etwa beim Thema der Verfügbarkeit schon auf sehr hohem Niveau. Und das ist auch das, was die Banken stresst, weil die lange damit nicht gerechnet haben, dass eine solche Anspruchshaltung dahintersteht. Und nach dem, was man aktuell hört, hat die Aufsicht mit dem Thema klassische Cybersecurity und Cyberkriminalität sicher nochmals eine Schippe draufgelegt.

Worum geht es in den Prüfungen außerdem?

Um das Thema Vertraulichkeit. Da dreht sich ein Großteil um Rollen und Rechte, also um den ausreichenden Schutz von Zugangsinformationen. Auch dort gibt es in den Häusern noch genügend zu tun, um Rollenkonzepte durchziehen zu können, die nicht nur technisch, sondern auch organisatorisch funktionieren. Da ist immer viel nach dem Motto „Hauptsache, es funktioniert“ aufgebaut worden, mit dem Selbstverständnis „Der Täter sitzt ja draußen, hier drinnen müssen wir ja arbeitsfähig bleiben“. Da wird stark aufgeräumt. Und der nächste Schub wird dann sicher die Frage sein: Wie ist die Qualität der Anwendung in der Architektur? Ist Sicherheit von Anfang an mitbedacht worden? Da kommen wir dann tatsächlich zum Thema der Code Reviews. Und danach könnte das nächste Thema dann Fintechs sein.

Das Interview führte
Bernd Neubacher.

ZUR PERSON

Bankenschützer

Timo Kob

bn – Seitdem die Aufsicht der Informationstechnik deutscher Banken verstärkt auf den Zahn fühlt, dürften dort die Dienste von Timo Kob noch etwas gefragter sein als zuvor. Das von ihm gegründete Sicherheitsberatungshaus Hisolutions arbeitet eigenen Angaben zufolge für 75% der Top-20-Banken, darunter auch solche, bei denen die Deutsche Bundesbank zu einer IT-Sonderprüfung erschienen ist.

Kob berät seit 1992 national und international branchenübergreifend Unternehmen, Behörden, Regierungen und supranationale Institutionen, unter ihnen das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundeskanzleramt Österreich, die OSZE und die europäische Agentur für Netzwerk- und Informationssicherheit (ENISA). Darüber hinaus war er maßgeblich an der Etablierung internationaler Standards für Informationssicherheit und Business Continuity beteiligt.

Kob forscht in den Feldern Informationssicherheit, Cyberspionage sowie Wirtschaftsschutz. Er ist Professor für Wirtschaftsschutz und Cybersecurity an der FH Campus Wien und fungiert dort seit 2012 als Forschungsfeldleiter für „Corporate Security & Information Security“. An der Frankfurt School of Finance & Management gestaltete er 2010 den Studiengang „Certified Security Manager“.

Kob ist stellvertretender Vorstandsvorsitzender des ASW Bundesverbandes (Allianz für Sicherheit in der Wirtschaft e.V.) und darüber hinaus Vorstandsmitglied des IT-Branchenverbandes Bitkom. Als parteiloser Experte saß er im vergangenen Jahr in der Programmkommission „Zukunft der Arbeit“ der CDU Deutschlands zur Ausgestaltung der Digitalen Agenda.

(Börsen-Zeitung, 17.1.2017)