

Audiodatei

Finanzrauschen Folge 26: DORA – Schutzschild gegen digitale Bedrohungen

Transkript

00:00 Ares Abasi

Willkommen zurück bei Finanzrauschen, dem Podcast für Banker von heute. In unserer letzten Folge beschäftigen wir uns mit dem Thema Proportionalität. Wie bereits angekündigt, sprechen wir heute über Dora, also Digital Operational Resilience Act, mit Rebecca Hartmann vom Genoverband.

Finanzrauschen, der Podcast für Banker. Mit Expertinnen und Experten klären wir die wichtigsten Themen rund um Regulatorik. Immer topaktuell und hochrelevant, mit Tipps für ihren Arbeitsalltag.

Hi Rebecca, Schön dich digital zu sehen. Wo sitzt du denn gerade?

00:35 Rebecca Hartmann

Ja, Ares, ich sitze im schönen Magdeburg. Zwar haben wir ein bisschen zugezogene Wolken, aber ansonsten ist alles hier ganz heiter.

00:00:43 Ares Abasi

Sehr schön, Rebecca. Du bist Abteilungsleiterin für das Kompetenzteam IT beim Genoverband und wie du mir mal erzählt hattest, obwohl du keine wirkliche IT-Erfahrung hattest, oder?

00:55 Rebecca Hartmann

Genau. Also das kam auch ehrlicherweise durch Zufall. Ich hole dich mal ganz kurz ab, wie ich da überhaupt hingekommen bin, wo ich jetzt sitze. Ich bin schon seit 2008 in der kompletten Volksbankenwelt unterwegs.

Das heißt, meine Beginne sind auch in der Volksbank gestartet. Und ja, mein Herz habe ich eigentlich ganz am Anfang mal an den Kreditbereich verloren. Das heißt, diese ganzen Marktfolge-Tätigkeiten waren das, was mir Spaß gemacht hat. Und irgendwann habe ich gedacht, ich gehe den nächsten Schritt und habe die Prüfungsassistenten-Laufbahn beim Genoverband begonnen und habe dort eine klassische Verbandsprüferausbildung gemacht.

Und mein Kollege kam dann irgendwann auf mich zu und hat gesagt: „Ja Rebecca, hast du nicht Lust in den IT-Bereich zu kommen?“ Da hab ich gedacht, ich und IT? Ich hatte gar keine Ahnung. Ich wusste, IT konnte ich schreiben, aber was hat das zu bedeuten? Aber ich habe mir die Frage gestellt, ist denn IT so ein Thema für die Zukunft? Und ich glaube, da kannst du mir zustimmen, IT beschäftigt halt jeden. Dann habe ich gedacht, weißt du was: „Tu das.“ Und bin 2017 in den IT-Spezialistenbereich bei uns gewechselt. Mittlerweile, mit 35 Jahren, bin ich Abteilungsleiterin von unserem Team, mit fast 80 People bei mir und wir gehen die ganzen Themen im Bereich IT in der Beratung, in der Prüfung etc. zusammen an.

02:19 Ares Abasi

Und wenn man dein Lächeln so sieht, bereust du es scheinbar auch nicht, gewechselt zu haben.

02:25 Rebecca Hartmann

Nee, also ich sag mal so, ITler sind ein bisschen besonders und da fühle ich mich einfach wohl. Also sei

es in der Musik, sei es auch im Gaming-Bereich, weil ich da private Interessen habe, passt IT komplett und auch die Mannschaft und mein Team. Ja ich liebe es wirklich und wenn man sagen kann, dass man seine Arbeit liebt, hat man ziemlich viel richtig gemacht.

02:44 Ares Abasi

Und das sieht man dir finde ich auch an. Stichwort Dora: Rebecca, kannst du uns kurz erklären, was du mit Dora zu tun hast, was Dora überhaupt bedeutet und warum das für Banken überhaupt so wichtig ist?

02:56 Rebecca Hartmann

Na klar. Also ich sag mal, Dora ist mir das erste Mal 2022 begegnet. Da gab es eine Veranstaltung von der BaFin, wo Dora mal fallen gelassen worden ist. Das waren unsere ganz ersten Berührungspunkte. Dora wurde ins Leben gerufen von der EU, um den Banken in ihrer digitalen Betriebsstabilität zu helfen. Das bedeutet, dass Banken resilienter werden gegenüber diesen Cyber-Bedrohungen, gegenüber Cyberangriffen. Und die EU-Verordnung soll einfach die Banken dabei unterstützen, sich in diesen Bereichen besser aufzustellen. Da die EU-Verordnung (Dora) jetzt auch mittlerweile die BAIT für unsere Volks- und Raiffeisenbanken umgesetzt hat, sind wir natürlich auch der erste Ansprechpartner in dem Bereich mit der IT-Regulatorik, uns auch mit den ganzen Dora-Bereichen auseinanderzusetzen. Also wie gesagt, im Rahmen Prüfungen sind wir mit am Start, im Rahmen operativer Unterstützung, Beratung oder auch als Dozentin war ich gestern erst unterwegs und habe mit dem Aufsichtsrat darüber gesprochen.

03:58 Ares Abasi

Klingt erstmal nach einer Herausforderung. Wenn man dich aber so lächelnd sieht, hat man das Gefühl, Dora kann doch gar nicht so schlimm sein, oder?

04:07 Rebecca Hartmann

Ja, das wurde mir gestern auch gesagt: „Frau Hartmann, Sie sind ja immer so fröhlich bei der ganzen Sache!“ Da habe ich gesagt: „Ja, was wäre die Alternative? Dass ich den Kopf in den Sand stecke?“ Das wäre irgendwie nicht ganz so gut und das würde allen Beteiligten nicht weiterhelfen.

Also von daher, ich finde Dora ist halt so ein Schreckensgespenst und es ist natürlich schwere Kost im Sinne von der IT-Regulatorik, weil wir dort

wirklich sehr viele Anforderungen haben. Du musst dir vorstellen, das sind über 1400 Anforderungen, die da bei den Banken bestehen und es ist natürlich sehr aufwendig, das erstmal zu lesen, zu verstehen. Aber es ist machbar, weil es auch in einem Regelprozess dargestellt ist. Das heißt, es ist gar nicht so schwer, wie sich die meisten vorstellen. Man muss sich halt einfach damit auseinandersetzen und beschäftigen.

04:54 Ares Abasi

Ja, ich denke, viele Banken sehen Dora als sehr überwältigend an. Was sind denn die häufigsten Ängste oder Missverständnisse, die du beobachtest?

05:02 Rebecca Hartmann

Was immer kommt, ist: „Warum müssen wir das denn jetzt überhaupt machen? Warum kommt denn das überhaupt? Wir sind gar nicht betroffen.“ Ehrlicherweise stellt sich dieses „Warum“ nie bei mir in der ganzen Frage.

05:15 Ares Abasi

Aber betroffen ist ja eigentlich jeder, oder?

05:17 Rebecca Hartmann

Ja, natürlich. Weil IT ist überall, und dass man von einem Cyberangriff betroffen wird. Es kann auch jeder Bank passieren, also da muss nur eine kleine Spam-Mail aus Versehen im Ordner landen und ein Mitarbeiter muss drauf klicken, dann kann die ganze Bank lahmgelegt werden. Von daher: betroffen ist leider jeder und sollte sich damit auch auseinandersetzen. In der Vergangenheit war dieses ganze Thema leider auch immer sehr unter der Hand. So ist das gelaufen und von daher kommt jetzt die IT mehr in den Fokus. Das finde ich persönlich auch sehr gut, weil dadurch das Verständnis mehr geschaffen wird, dass man da auch Thematiken einfach angehen muss.

05:55 Ares Abasi

Die Umsetzungsfrist ist ja bereits abgelaufen, das hast du ja gerade auch schon so halb erwähnt. Wie kritisch ist denn die Lage wirklich für Banken, die noch nicht soweit sind?

06:04 Rebecca Hartmann

Ja, da müssen wir, glaube ich, ein bisschen sondieren. Also 17.1. ist in dem Sinne abgelaufen, da hilft nichts mehr. Alles, was jetzt nicht umgesetzt ist, ist eine

Beanstandung. Und das ist eine Feststellung, die dort getroffen wird, auch im Rahmen der Prüfung. Aber nichtsdestotrotz haben die meisten Banken ja schon eine solide Grundlagenbasis geschaffen. Das heißt, so schriftlich fixierte Ordnungen, die umzusetzen, das heißt Arbeitsanweisung, Richtlinien, da habe ich von der Vielzahl der Banken eine Rückmeldung, dass sie das bereits gemacht haben. Jetzt geht es auch darum, diese ganzen Themen, die sie vielleicht im Vorfeld schon mal betrachtet haben, auch wirklich umzusetzen und in die Praxis zu nehmen. Weil ich denke, wir müssen jetzt alle auch erstmal mit der kompletten DORA-Verordnung leben, sie mit Leben füllen, damit es dann auch wirklich als Mehrwert verstanden wird und ein Mehrwert für die gesamte Landschaft schaffen kann.

06:57 Ares Abasi

Ich mag ja immer Praxisbeispiele. Kannst du denn eins nennen und einfach mal so step by step aufzeigen, was man machen kann, was ein Unternehmen tun kann, um Dora einzuführen.

07:08 Rebecca Hartmann

Vielleicht hole ich dich da einfach mal ab, wie wir es gemacht haben, weil wir auch in vielen Themen mit den Banken zusammen unterwegs waren. Da haben wir wirklich erstmal geprüft, OK, was ist denn überhaupt in Dora enthalten? Was gibt es denn da für Anforderungen? Das ist der erste Step: Lesen. Man kann viel lesen, damit man es erstmal versteht und dann bei sich in der Bank zu prüfen, was habe ich denn überhaupt schon? Weil ganz viele Themen, die in der Dora auch drin sind, wie zum Beispiel das Change Management, also wie man Veränderungen in der IT dokumentiert, gibt es schon. Da muss man nur ein wenig nachschärfen, vielleicht dann auch in den Begrifflichkeiten und prüfen, wie wir es dann dementsprechend umsetzen können. Also ganz konkret in die Verordnung reinzugehen, sich einzelne kleine Maßnahmenpakete zu gestalten und sich dann entsprechende Fristen zu setzen. Aber es hilft halt nichts, wie gesagt, den Kopf in den Sand zu stecken, sondern step by step vorzugehen und vielleicht auch für sich in der Bank zu prüfen, was sind denn jetzt die größten Pain Points, die ich habe. Weil die meisten Banken wissen, wo es in ihrer IT Probleme gibt und die kann man jetzt auch mit Dora gut lösen und dann auch angehen, weil da ein gutes Vorgehen auch mit erläutert wird.

08:20 Ares Abasi

Es geht ja wahrscheinlich auch ganz einfach, wenn du jetzt zum Beispiel mal nach vorne schaust und sagst, wie könnte man eine abgespeckte Variante vielleicht durchführen, um das Ganze sehr schnell und sehr einfach handhabbarer zu machen?

08:33 Rebecca Hartmann

Ja, ich sag mal so: Handhabbarer wird es mit Dora in den meisten Fällen werden, weil auch Dora diesen Proportionalitätsgrundsatz hat. Da hattet ihr auch schon drüber gesprochen. Und hier geht es auch darum, risikobasiert zu gucken, was für IT-Risiken habe ich in meiner Bank? Hier aus der Praxis heraus gesprochen: Die Banken haben auch erstmal geprüft, mit welchen IT-Dienstleistern arbeiten wir überhaupt zusammen und brauchen wir die überhaupt? Weil wir hatten Institute, da waren über 300-400 IT-Dienstleister mit aktiv gewesen und davon haben wir auch erstmal eine Vielzahl von IT-Dienstleistern die Verträge aufgekündigt, weil sie gar nicht mehr relevant waren.

09:12 Ares Abasi

Wie sieht denn eine ideale Zusammenarbeit zwischen Bank und IT-Dienstleister aus?

09:18 Rebecca Hartmann

Ganz viel Kommunikation und offene Kommunikation. Das heißt, wir haben auch in der Dora das sogenannte IKT-Drittparteirisikomanagement, wo wir die Verträge mit den Dienstleistern abstimmen müssen. Hier ist einfach eine gute Zusammenarbeit mit den Dienstleistern entscheidend. Das heißt, als Bank stellt man die Anforderung, bekommt auch die Antworten der IT-Dienstleister, dass die IT-Dienstleister auf der anderen Seite dann auch Verständnis für die Umsetzung haben in den Banken, den Banken die benötigten Informationen zur Verfügung stellen, wie zum Beispiel, ob sie ISO-zertifiziert sind, ob sie Sicherheitsmaßnahmen umgesetzt haben und dass da einfach die Zusammenarbeit noch verschärft und verstärkt wird. Da haben wir in Teilbereichen noch ganz große Kommunikationsbarrieren, wo vielleicht auch die Bank sich falsch ausdrückt und der IT-Dienstleister gar nicht weiß, was er antworten soll. Da fungieren wir an der ein oder anderen Stelle auch so ein bisschen als Übersetzer, würde ich sagen.

10:17 Ares Abasi

Das heißt also, so eine Art toxische Beziehung und du

als beste Freundin rätst deiner Freundin dazu, Schluss zu machen und sich einen Neuen zu suchen, oder?

10:26 Rebecca Hartmann

Ja so kannst du es verstehen. Oder wir gucken mal, wie wir in eine Paartherapie reingehen können, um daran zu arbeiten, dass es dann besser funktioniert. Genau, ein sehr gutes Beispiel, Ares.

10:37 Ares Abasi

Wenn du mal in die Glaskugel schaust, wie wird sich die IT-Landschaft der Volksbanken und Raiffeisenbanken durch Dora in fünf Jahren verändert haben? Idealerweise.

10:48 Rebecca Hartmann

Idealerweise, Wünsche darf man ja äußern, glaube ich, dass sich mit Dora die IT-Dienstleister so ein bisschen zentralisieren. Das bedeutet, dass wir nicht mehr die Vielzahl von IT-Dienstleistern haben, sondern die Banken sich eher auf bestimmte IT-Dienstleister berufen und zentralisieren werden, weil sie schon merken, dass sich die Anforderungen erhöht haben und es nur noch gewisse IT-Dienstleister gibt, die das dann auch umsetzen können. Und zum anderen, dass wir dann zukünftig natürlich auch für diese ganzen Cyberangriffe und Bedrohungen besser gewappnet sind, weil die Kommunikation mit der Bank und den IT-Dienstleistern verbessert wird und dann auch bewusst ist, was man tut, wie man es tut und was da vielleicht auch für Schwachstellen sind. Also das hoffe ich, dass das zukünftig so erfolgt.

11:38 Ares Abasi

Das ist ja eigentlich schon eine perfekte Einleitung für den Schluss. Wenn du jetzt mal in dich gehst und sagst, welchen Motivationsspruch könntest du einer Bank auf den Weg geben, um Dora anzupacken?

11:50 Rebecca Hartmann

Macht es einfach, findet keine Ausreden und habt auf jeden Fall keine Angst davor, weil es sind ganz viele Begrifflichkeiten drin, die vielleicht am Anfang sehr abschreckend wirken. Aber tut es, geht in die Umsetzung und versucht euer Bestes an der Stelle zu machen. Die andere Alternative ist, zu ignorieren. Das wird auf Dauer nicht funktionieren und da werden dann gegebenenfalls auch Sanktionen auf die Banken zukommen. Also von daher, macht es so, wie es in eurem Ermessen und in euren Möglichkeiten da ist.

12:26 Ares Abasi

Mhm, da kriegt man doch direkt Lust, Dora umzusetzen. Und falls man Fragen haben sollte, darf man dich sicherlich auch kontaktieren?

12:34 Rebecca Hartmann

Natürlich, jederzeit. Also gestern war ich bei einer Veranstaltung, da hat mich auch schon jemand Dora Hartmann genannt. Also von daher, vielleicht muss ich auch noch meinen Namen umbenennen, aber Rebecca Hartmann genügt. Da können Sie mich sehr gerne erreichen.

12:49 Ares Abasi

Super, vielen Dank, liebe Rebecca. Ich wollte gerade schon Dora sagen. Nächstes Mal wird es um das Thema Barrierefreiheit gehen. Vielen Dank fürs Zuschalten, vielen Dank Rebecca für deine Zeit und bis zum nächsten Mal.