Johner Institut

IT-Strafrecht

Mit RAin Diana Nadeborn, Prof. Dr. Christian Johner

Transkript

00:00:05 Sprecher 1

Medical Device Insights.

00:00:08 Sprecher 1

Ein Podcast des Jona-Instituts für Medizinprodukte-Hersteller, Behörden und benannte Stellen.

00:00:21 Sprecher 2

In diesem Podcast war das Thema IT-Security schon einige Male Thema.

00:00:26 Sprecher 2

wenig überraschend, nachdem beispielsweise die M.D.R.

00:00:29 Sprecher 2

und die I.V.D.R.

00:00:30 Sprecher 2

genau diese I.T.

00:00:31 Sprecher 2

Security von Produkten mit einfordern und wie Sie wissen, die F.D.A.

00:00:35 Sprecher 2

natürlich genau in gleicher Weise.

00:00:36 Sprecher 2

Die I.T.

00:00:38 Sprecher 2

Security wird auch heute das Thema sein, allerdings unter einem bisschen anderen Blickwinkel.

00:00:42 Sprecher 2

Diesmal schauen wir uns nicht an, was I.T.

00:00:45 Sprecher 2

Security mäßig passieren kann im Hinsicht auf Angriff auf Produkte, sondern heute schauen wir uns das mal an, Angriffe auf die Organisationen.

00:00:54 Sprecher 2

Das heißt also, der Gegenstand oder das bedrohte Objekt ist jetzt nicht ‚n Medizinprodukt mit irgendwelchen Folgen für beispielsweise Patienten, sondern das bedrohte Objekt ist jetzt die Organisation selber und das kann beispielsweise eben ein Medizinproduktehersteller sein, aber auch andere Organisationsformen.

00:01:10 Sprecher 2

Und weil das so ein spannendes Thema ist und ein Anspruch so ist, hab ich auch jemand dazu gezogen, nämlich die Frau Rechtsanwältin Nadeborn, die sich genau auf dieses Thema

00:01:22 Sprecher 2

spezialisiert hat und mit der ich heute drüber sprechen will, ja was kann denn da passieren, wie muss ich mich als Organisation verhalten in diesen Fällen.

00:01:30 Sprecher 2

Denn man ist nicht nur das Opfer, sondern man ist auch leicht jemand, der dann aus rechtlicher Sicht noch zusätzliche Fehler begeht und da ist man in gewisser Weise doppelt geschädigt und das muss nicht sein und genau wie man sowas verweidet, das soll heute

00:01:42 Sprecher 2

Thema sein.

00:01:43 Sprecher 2

Ja, Frau Nadeborn, seien Sie ganz herzlich willkommen.

00:01:45 Sprecher 2

Wenn Sie vielleicht mit einer kurzen Vorstellung von sich beginnen würden, ja, was auch das, was Sie so tun, damit man einen Einblick von so einer Rechtsanwältin bekommt, dann glaub ich, dann hätten wir einen super Start.

00:01:56 Sprecher 3

Vielen Dank, Nadeborn mein Name.

00:01:58 Sprecher 3

Ich bin seit 12 Jahren Rechtsanwältin im Wirtschaftsstrafrecht und Partnerin der Kanzlei Zambi Kakis.

00:02:05 Sprecher 3

die einen Schwerpunkt im Medizinstrafrecht hat und mich hinzugezogen hat für den weiteren Schwerpunkt IT-Strafrecht.

00:02:13 Sprecher 3

Das mache ich seit vielen Jahren, IT-Strafrecht und zwar auf beiden Seiten, also sowohl Beschuldigte in Strafverfahren zu vertreten, als auch jetzt mit der Kanzlei Zambi Kakis vor allen Dingen Unternehmen zu beraten, wenn sie Betroffene von Straftaten geworden sind, nicht nur im Strafverfahren, sondern auch

im behördlichen Verfahren.

00:02:31 Sprecher 3

da ist es nämlich dann so, da kommt es dann von allen Seiten und wir bündeln das und koordinieren das.

00:02:36 Sprecher 2

Das heißt, sie würden eher die Gehackten vertreten, jetzt aktuell, als die die Blackhead Hacker sozusagen, kann man das so sagen.

00:02:46 Sprecher 3

Genau, also ich komme aus dem Bereich der Individualverteidigung, also die Verkäufer auf Darknet Plattformen, die Administratoren, die eben die Daten mitgenommen haben und verkauft haben.

00:02:58 Sprecher 3

Das

00:02:58 Sprecher 3

sozusagen bei meinem meine ursprüngliche Klientel und nun dieses Wissen, auch diese Auseinandersetzung mit der Staatsanwaltschaft, mit Gericht, dieses Wissen bringe ich jetzt mit, um es andersrum auf Seite der Unternehmen einzusetzen.

00:03:11 Sprecher 3

Denn es ist so, im Bereich Cybercrime gibt es ja viel mehr Geschädigte als Täter.

00:03:17 Sprecher 3

Geschädigte sagt ja auch das L.

00:03:19 Sprecher 3

K.

00:03:20 Sprecher 3

A.

00:03:20 Sprecher 3

in seiner Lagebewertung, es ist nicht mehr die Frage ob, sondern nur noch wann.

00:03:24 Sprecher 3

kann ein Unternehmen Opfer von Straftaten wie DDoS-Attacken, ja, wenn die Unternehmenswebseite überlastet wird, werden von den berühmten Ransomware-Angriffen, wenn die Unternehmens-I.T.

00:03:36 Sprecher 3

verschlüsselt wird, wenn die Daten verschlüsselt werden und Lösegeldforderungen kommen oder auch vom C.E.O.

00:03:42 Sprecher 3

Fraud sehr häufig eben betrügerische E-Mails an die Buchhaltung und dann werden neue Kontonum-

mern mitgeteilt, an die das Geld überwiesen werden soll.

00:03:54 Sprecher 3

dann hätte man das Geld ja gerne auch wieder zurück und muss sich auch damit auseinandersetzen, stehen da strukturelle Probleme dahinter, die es vielleicht zu beheben gilt, um das nicht noch mal geschehen zu lassen?

00:04:06 Sprecher 2

Jetzt haben Sie schon ‚n bisschen angedeutet, also wenn man Opfer von so einer Attacke ist und ich habe jetzt schon gehört, das kann jetzt von Ihnen oder außen kommen, vielleicht haben Sie uns nachher noch ‚n paar mehr Beispiele dazu, dann ist man natürlich offensichtlich das Opfer, man ist auch jemand, der

00:04:24 Sprecher 2

möglicherweise auch selber Gegenstand einer Ermittlung werden kann, weil man vielleicht nicht alles getan hat, um die genau das zu verhindern.

00:04:33 Sprecher 2

Könnten Sie uns vielleicht deshalb noch mal ganz kurz ‚n paar Beispiele geben, 3 haben Sie, glaube ich, schon genannt gehabt und dann auf was muss man jetzt aufpassen oder auf was hätte man vielleicht vorher schon aufpassen müssen?

00:04:43 Sprecher 2

Also in welchen Bereichen bewegt man sich in die Rechtsnichtkonformität mit rein?

00:04:49 Sprecher 3

Genau, also wir sind jetzt im Bereich Angriffe von außen, die wird das Unternehmen bemerken, also beim Ransomware-Angriff, wenn kein Zugriff mehr möglich ist, weil die Daten verschlüsselt sind und die Täter ja dann eben mit den Lösegeldforderungen auf das Unternehmen zugehen, das wird einem nicht entgehen beim C.

00:05:04 Sprecher 3

E.

00:05:05 Sprecher 3

O.

00:05:06 Sprecher 3

Fraud, diese Überweisung an ja eben nicht mehr den Lieferanten, den Vertragspartner, sondern eben auf Täterkonten, die das natürlich dann auch schon umgewandelt haben in Kryptowährungen.

00:05:15 Sprecher 3

Ja, da ist eben die Frage, wie

00:05:17 Sprecher 3

wie schnell kann die Bank noch reagieren, wie schnell fällt das auf in der Buchhaltung, dass die Überweisung an das falsche Ziel gegangen ist.

00:05:25 Sprecher 3

Auch die D.

00:05:25 Sprecher 3

DOS-Attacke wird man schnell bemerken, weil der Online-Shop oder die Online-Präsenz nicht mehr zugänglich ist für die Kunden, mit denen man ja in Kontakt sein möchte.

00:05:37 Sprecher 3

Also das Bemerken, wenn der Schaden schon eingetreten ist, ist unmittelbar.

00:05:42 Sprecher 3

Dem gehen natürlich Straftaten voraus von Seiten der Hacker, die

00:05:46 Sprecher 3

dann unbemerkt waren.

00:05:48 Sprecher 3

Um das besser zu verhindern, ist insgesamt I.T.

00:05:52 Sprecher 3

Compliance Maßnahmen ein Aufstellen von technisch organisatorischen Maßnahmen, die wie sie auch im B.S.I.

00:05:59 Sprecher 3

Gesetz vorgesehen sind, wie sie auch in der Datenschutzgrundverordnung vorgesehen sind, die die Zugriffe von außen möglichst minimieren oder dass man es eben schneller bemerkt.

00:06:08 Sprecher 2

Sie haben uns jetzt schön geschildert gehabt, quasi welche Form der Angriffe haben wir von außen, weitere Beispiele genannt, haben auch

00:06:15 Sprecher 2

Gesetze genannt, also B.S.I.

00:06:17 Sprecher 2

Gesetz, Datenschutzgrundverordnung als ‚n weiteres Beispiel.

00:06:20 Sprecher 2

Wenn wir jetzt mal den Fokus lenken auf die Angriffe von Ihnen, hätten Sie uns da auch Beispiele dafür und vielleicht auch noch weiterführen, gleich die Frage, haben wir dann andere Gesetze, die wir hier anstatt oder zusätzlich zu beachten hätten?

00:06:35 Sprecher 3

Ja, tatsächlich in meiner anwaltlichen Praxis spielen die Angriffe von innen durch den Innentäter eine besonders große Rolle, denn hier ist es ja so,

00:06:43 Sprecher 3

dass das geschädigte Unternehmen und der Täter sich kennen, so dass die das Strafverfahren sich gegen eine identifizierte Person, die sich auch im Inland befindet und ohne weiteres greifbar ist, richtet.

00:06:54 Sprecher 3

Und diese Angriffe der Innentäter ist eine Person, ein kann ein Angestellter sein, ein externer Dienstleister, der ursprünglich eine Zugriffsberechtigung erteilt bekommen hat vom Unternehmen für spezifische dienstliche Zwecke, diese dann aber missbraucht die Zugriffsberechtigung, also das technische

00:07:12 Sprecher 3

Können ausnutzt und über das rechtliche Dürfen hinausgeht.

00:07:16 Sprecher 3

Natürlich ist das in den Dienstverträgen, in den Arbeitsverträgen ausgeschlossen, die Daten eben zu kopieren und dann entweder also zu monetarisieren, indem man sie an die Konkurrenz verkauft, die man schon kennt, selber das Konkurrenzunternehmen aufbaut, damit viele Dinge, die Menschen sich da einfallen lassen können, wie man mit den Unternehmensdaten zu Geld kommt.

00:07:39 Sprecher 2

Welche Gesetze werdet ihr

00:07:41 Sprecher 2

zu beachten, die auf der einen Seite die geschädigten Unternehmen befolgen müssen und was wären die Gesetze, die gegen die diese internen Straftäter, sag ich schon, also die internen Akteure verstoßen hätten?

00:07:54 Sprecher 2

Also, es ist quasi ,ne Doppelfrage.

00:07:56 Sprecher 2

Also, auf was müssen die Unternehmen achten, damit sie da jetzt nicht selber noch mal, obwohl sie ja Opfer geworden sind, gegen weitere Gesetze verstoßen?

00:08:04 Sprecher 2

Also, welche sind da zu beachten und was sind die Gesetze, gegen die offensichtlich diese Innentäter verstoßen haben?

00:08:10 Sprecher 3

Genau, also die Innentäter, die internen Akteure, machen sich in verschiedener Weise strafbar.

00:08:16 Sprecher 3

Zum einen ist häufig das Geschäftsgeheimnisgesetz betroffen.

00:08:20 Sprecher 3

Der Verrat von Geschäftsgeheimnissen ist eine Straftat und in der Regel.

00:08:25 Sprecher 3

sind ja die wertvollen Daten eben Geschäftsgeheimnisse, die da eben monetarisiert werden sollen.

00:08:31 Sprecher 3

Dann zum anderen ist es auch ein Ausspähen von Daten, ne, das ist Paragraph 202 A.

00:08:37 Sprecher 3

StGB, ursprünglich konzipiert für den Außenangriff, aber nach aktueller B.G.H.

00:08:42 Sprecher 3

Rechtsprechung wohl auch auf die Innentäter anwendbar.

00:08:46 Sprecher 3

Je nachdem, wen man vertritt, würde man eben da die eine oder die andere Auffassung vertreten und immer auch im Boot ist Paragraph 42 Bundesdatenschutzgesetz, eben das

00:08:55 Sprecher 3

Das Unberechtigte, das unbefugte Verarbeiten von Daten, was ja an der Stelle auch stattfindet, ist strafbar.

00:09:01 Sprecher 3

Also, das ist ohne weiteres strafbar.

00:09:05 Sprecher 3

Das so ist ja auch dann die Strafanzeige.

00:09:08 Sprecher 3

Häufig geht das ja noch mit arbeitsrechtlichen Prozessen einher oder eben die Trennung vom Dienstleister.

00:09:14 Sprecher 3

das Auseinandergehen mit dem Geschäftsführer Gesellschafter sollte dieser die Zugriffsbefugnisse missbraucht haben.

00:09:20 Sprecher 3

Also das ist die eine Schiene: Strafrecht plus Gesellschaftsrecht plus Arbeitsrecht plus Vertragsrecht, Haftungsrecht und worauf Unternehmen dann eben achten müssen.

00:09:31 Sprecher 3

Es ist zugleich

00:09:32 Sprecher 3

nicht, weil es in der Regel ja auch personenbezogene Daten sind, eine Datenschutzverletzung eingetreten, wo sie Meldepflichten haben, leider in der schwierigen Rolle, das muss man prüfen, es muss nicht immer alles

00:09:45 Sprecher 3

gemeldet werden, da kann man vielleicht auch überlegen, in welchem Umfang.

00:09:50 Sprecher 3

Die Frage ist auch, ob man betroffene Dritte auch noch benachrichtigen muss, da gibt es auch Pflichten dazu und dann, ob eben die Datenschutzbehörde Überprüfungen einleitet, die eben bis zu, also natürlich muss man abstellen, das Defizit, aber auch bis zu Bußgeldern führen können und da ist eben ein guter Einwand, wer ein I.

00:10:09 Sprecher 3

T.

00:10:09 Sprecher 3

Compliance System vorher hatte, ist hoffentlich gar nicht erst betroffen, wer es zumindest dann einführt, das ist strafzumessungsmäßig

00:10:15 Sprecher 3

nicht zu berücksichtigen.

00:10:17 Sprecher 3

Das mildert auf jeden Fall die Sanktionen, weil dann hat das Unternehmen ja eingeleitet, was es ohnehin hätte einleiten sollen.

00:10:25 Sprecher 2

Mhm, jetzt haben Sie sehr schön geschildert, die beiden sozusagen Rechtsbereiche oder auch ja auch gemünzt auf die jeweiligen Akteure.

00:10:33 Sprecher 2

Können Sie uns mal so ‚n Strafmaß für beide Seiten zeigen?

00:10:37 Sprecher 2

Also, was droht einem, der so ‚n Geheimnisverrat begeht auf der einen Seite und was droht einem Unternehmen, das

00:10:44 Sprecher 2

Seinen Anforderungen nicht gerecht wird, beispielsweise zu melden.

00:10:48 Sprecher 3

Also da es sich bei den Innentätern, ja den Arbeitnehmern, Dienstleistern und so weiter.

00:10:55 Sprecher 3

um Personen handelt, die in der Regel nicht vorbestraft sind, regulär im Berufsleben stehen, verheiratet mit Wohnsitz und allem, da bewegen wir uns im Bereich der Geldstrafen.

00:11:05 Sprecher 3

Also eine Freiheitsstrafe, obwohl das vorgesehen ist vom Strafrahmen und natürlich bei Wiederholungstätern dann auch zum Einsatz kommt, ist für den Ersttäter, um den es sich in der Regel handelt.

00:11:15 Sprecher 3

Also geht es um Geldstrafen.

00:11:17 Sprecher 3

Das sind aber auch noch Personen, die auch noch mit Abschreckung schon die Durchsuchung selbst, die Durchsuchung am Arbeitsplatz und zu Hause durchaus sich beeindrucken lassen.

00:11:26 Sprecher 3

Also sozusagen das scharfe Schwert der Untersuchungshaft, die aufrechterhalten bleibt bis zur Hauptverhandlung, ist in diesen Fällen gar nicht notwendig.

00:11:35 Sprecher 3

Also der Strafrahmen sicherlich überschaubar für die Täter, aber trotzdem abschreckend genug.

00:11:40 Sprecher 3

meines Erachtens, so dass dieses, was von politischer Seite immer gefordert wird, es müssten also mehr höhere Strafrahmen um die Täter da abzuschrecken.

00:11:51 Sprecher 3

Ich glaube, das ist, wäre jetzt rechtspolitisch, teile ich diese Auffassung nicht.

00:11:56 Sprecher 3

Was für die Unternehmen, wenn sie erstmal in dem behördlichen Verfahren sind und sich dann mit dem Datenschutzbeauftragten des Landes auseinandersetzen müssen, hat verschiedene Instrumentarien bis zum Bußgeld,

00:12:10 Sprecher 3

das liest man ja nun auch die ganze Zeit in der Berichterstattung, Bußgelder bis 4% des Unternehmens Umsatzes, wir bleiben sicherlich in der Regel drunter.

00:12:19 Sprecher 3

Also wir, ich kann Ihnen Beispiele jetzt sehen, aufsagen, wo es natürlich die Millionen Bußgelder gab, aber wenn man dann eben kooperiert mit der Behörde, das ist der Weg, den man dann wohl einschlagen muss in der Regel, da kommt man auf jeden Fall zu besseren Ergebnissen.

00:12:35 Sprecher 2

Sie haben jetzt schon angedeutet, auf was man alles achten sollte und das ist natürlich auch genau das,

00:12:40 Sprecher 2

bei dem sie unterstützen.

00:12:41 Sprecher 2

Ich versuch das mal zusammenzufassen, ob ich das alles hab, damit sie es ergänzen können.

00:12:45 Sprecher 2

Also, das sind einmal Fragestellungen, die sie helfen zu beantworten.

00:12:49 Sprecher 2

Wie gehe ich gegen diese Person vor, die mich geschädigt hat, insbesondere wenn es ‚ne Interne ist.

00:12:54 Sprecher 2

Das nächste ist, wie stell ich sicher, dass ich mich rechtskonform gegenüber den Behörden verhalte.

00:13:00 Sprecher 2

Also, die Entscheidung treffe, muss ich ja melden, muss ich nicht melden.

00:13:04 Sprecher 2

Ich glaub, das ist noch ,n Punkt, bei dem sie wahrscheinlich helfen können.

00:13:07 Sprecher 2

Dann hat hatten sie so anklingen lassen,

00:13:10 Sprecher 2

ja letztlich die Strategie, die man dann vielleicht auch in dem Verfahren einschlagen muss.

00:13:14 Sprecher 2

Sie hatten angedeutet, ja ,ne ,ne Bereitschaft, ,n I.

00:13:17 Sprecher 2

T.

00:13:17 Sprecher 2

Compliance System einzuführen, falls man das noch nicht hat.

00:13:20 Sprecher 2

Können Sie dann noch ,n bisschen mehr drüber berichten, was solche entscheidenden Fragestellungen sind, auf die man aufpassen sollte und bei denen Sie natürlich unterstützen können?

00:13:29 Sprecher 3

Wenn das Unternehmen sich unsicher ist oder die dafür zuständigen Compliance Officer oder die Geschäftsleitung insgesamt, wenn man es delegiert hat, dann eben an einen Bereichsleiter, dann eine Ersteinschätzung vorzunehmen, wie ist denn der Stand der I.

00:13:45 Sprecher 3

T.

00:13:45 Sprecher 3

Sicherheit und Datenschutz.

00:13:46 Sprecher 3

Ja, also schön ist natürlich, wenn das dieses Wissen schon vorhanden ist im Unternehmen, ansonsten ist eine Ersteinschätzung dazu sinnvoll, um dann zu schauen, welche technisch organisatorischen Maßnahmen könnten noch ergänzt werden.

00:13:59 Sprecher 3

bis zu einem, das kann man natürlich dann abgestuft machen, bis zu einem vollumfänglichen I.

00:14:04 Sprecher 3

T.

00:14:04 Sprecher 3

Compliance Management System natürlich, aber in der Regel, wenn wir immer rückblickend schauen, sind eigentlich häufig die Basisanforderung nicht erfüllt.

00:14:13 Sprecher 3

Also gibt es überhaupt einen Zugriffsberechtigungen, das Management im Unternehmen, ja, das nicht alle über die gleichen Accounts auf alle Daten zugreifen können.

00:14:25 Sprecher 3

natürlich, alle nicken da immer zu dem und stimmen einem zu.

00:14:29 Sprecher 3

Wenn ich meine Mandanten angucke, ist es aber nicht flächendeckend vorhanden.

00:14:32 Sprecher 3

Ist auch meine Beobachtung, auch zu sozusagen zu den Basisregeln gehört natürlich, gibt es einen Back-up, ja, was abgekoppelt ist von Internetzugängen auf das, was auch tatsächlich technisch wieder eingespielt werden kann.

00:14:47 Sprecher 3

eine Selbstverständlichkeit.

00:14:48 Sprecher 3

Natürlich, bei Ihnen ist das so, in unserem, in unserer Kanzlei ist das so, bei meinen Mandanten nicht immer und dann das führt aber zu ganz anderen Ausgangssituationen, wenn man den Ransomware-Angriff hat und die Daten verschlüsselt sind oder sozusagen dritte, jetzt meine letzte, sozusagen Basisregel, Zwei-Faktor-Authentifizierung, ja, für die sensibelsten Bereiche, ist das vorhanden oder nicht.

00:15:12 Sprecher 3

Schön wär es, ja, und wir sollten das alle haben,

00:15:15 Sprecher 3

sicherlich geht eine Ersteinschätzung darüber hinaus, aber schon diese Felder wären zu identifizieren und ne, also wenn man irgendwo anfängt, dann fängt man damit an.

00:15:24 Sprecher 3

Gibt es natürlich je nach Unternehmensgröße auch in einem viel weiter differenzierten System und dann, wenn man sich eben für die Außenangriffe vorbereiten möchte, ein also Notfallmanagement vorher besprechen, wie würde ein Krisenstab sich zusammensetzen, wie sind diese Personen erreichbar, ja,

00:15:43 Sprecher 3

wie kann ein Plan B aussehen, wenn man nicht auf alles zugreifen kann.

00:15:48 Sprecher 3

Das wäre im Idealfall vorher zu erledigen und wenn es aber geschehen ist, wenn eben das Kind in Brunnen gefallen ist, wenn leider die das Unternehmen bemerkt, dass schon etwas geschehen ist, dann sind eben diese Fragen, ne, die die die behördlichen Verfahren koordinieren, die Meldungen, die Benachrichtigungspflichten auch gegenüber der Versicherung letztendlich, die ja auch ein Interesse daran haben,

00:16:11 Sprecher 3

ein, also das Lagebild, ja, wie die betroffenen Unternehmen, von welcher Seite sie betroffen sind, wieder die Muster sind, um diese Informationen auch zu bekommen, kriegen sie auch viel Unterstützung von Seiten der Ermittlungsbehörden.

00:16:25 Sprecher 3

Genau, und dann letztendlich eben, dann gibt es ein Strafverfahren, was wir dann auf der Seite eben der.

00:16:30 Sprecher 3

Strafanzeigeerstatter, vertreten der Geschädigten und teilweise kann es eben sein, wenn es Defizite offenbart hat auf Seiten der Geschäftsleitung, dass dort selber noch ein eigenes Ordnungswidrigkeitenverfahren oder Strafverfahren gegen die Geschäftsleitung, eben die Frage unterlassene Aufsichtsmaßnahmen, ja, wurde nicht genug getan im präventiven Bereich, da kümmern wir uns natürlich auch drum.

00:16:55 Sprecher 2

Wow, also ich fass ganz kurz zusammen, weil das so ,ne Menge, die Sie uns da geschildert haben.

00:16:59 Sprecher 2

Also der erste Bucket war alles, was eigentlich präventiv ist, unter anderem eben sicherstellen, dass die notwendigen Maßnahmen ergriffen sind.

00:17:07 Sprecher 2

Und Sie haben jetzt ja über sehr basale Maßnahmen gesprochen, aber dass die nicht immer erfüllt werden, da zeugen Ihre Mandanten offensichtlich eindeutig davon.

00:17:17 Sprecher 2

Das zweite, wo Sie dann unterstützen, das fand ich sehr spannend, war in ganz verschiedenen Bereichen, nämlich einmal Richtung Behörden,

00:17:24 Sprecher 2

also zu entscheiden, muss ich melden, wie muss ich melden, wie gehe ich da gut vor.

00:17:27 Sprecher 2

Dann, was neu dazu kommt im Bereich der Versicherung, weil da geht es wahrscheinlich dann ums meiste Geld, was man da bekommt oder eben dann halt ungünstigerweise nicht bekommt.

00:17:36 Sprecher 2

Dann das Dritte, vielleicht mit beidem verwoben, wie geht man jetzt vor, um sich technisch organisatorisch auf Stand zu bringen.

00:17:43 Sprecher 2

Und dann haben wir quasi noch mal so 2 juristische Stränge, nämlich einmal gegen die Personen, die geschädigt haben

00:17:51 Sprecher 2

und dann aber auch gegebenenfalls wird man auch verklagt, weil man irgendwelche Maßnahmen nicht ergriffen hat und auch da begleiten sie dabei.

00:17:59 Sprecher 2

Ja, das ist eine riesen Menge.

00:18:01 Sprecher 2

Ja, ich hoff, dass das Ihnen, unseren Zuhörern, einen Überblick darüber verschafft hat, auf was Sie achten sollten.

00:18:08 Sprecher 2

Ich glaub, präventiv ist immer besser, wie post mortem aktiv zu werden und bei welchen Aktivitäten eben Rechtsanwältinnen und Rechtsanwälte besonders hilfreich sind.

00:18:20 Sprecher 2

Also, ich hab hier viel gelernt, Frau Nadeborn.

00:18:23 Sprecher 2

Ganz herzlichen Dank, dass Sie uns da haben dran teilnehmen lassen.

00:18:26 Sprecher 2

Wenn Sie gestatten, werde ich auch Ihre Kontaktdaten mit in die Shownotes mit reinnehmen.

00:18:32 Sprecher 2

Dann können alle, die da Unterstützung brauchen, sich bei Frau Nadeborn direkt melden.

00:18:37 Sprecher 2

Ich denk, der Aufruf wird auf jeden Fall sein, machen Sie es präventiv, auch wenn Frau Nadeborn auch hinterher noch hilft.

00:18:44 Sprecher 2

Aber ich glaube, es wäre für alle Seiten etwas weniger Arbeit, das rechtzeitig zu tun.

00:18:48 Sprecher 2

bleibt mir nur, ganz herzlichen Dank zu sagen.

00:18:51 Sprecher 2

Frau Naderlem.

00:18:52 Sprecher 2

Bis bald.

00:18:53 Sprecher 3

Gerne, bis dann!