Johner Institut

Zusammenspiel von Risikomanagement und IT-Security

Mit Christian Rosenzweig, Prof. Dr. Christian Johner

Transkript

00:00:05 Sprecher 1

Medical Device Insights, ein Podcast des Johner Instituts für Medizinprodukthersteller, Behörden und benannte Stellen.

00:00:20 Sprecher 2

Möglicherweise haben Sie auch von dem Vorfall neulich gehört, wo ein Arztpraxishersteller ja versehentlich wahrscheinlich Millionen an Patientendaten nicht richtig geschützt hatte und das ist offensichtlich ein

00:00:32 Sprecher 2

Problem mit der Vertraulichkeit der Daten, mit dem Datenschutz.

00:00:36 Sprecher 2

Jetzt sind wir aber gerade hier auch am Institut.

00:00:39 Sprecher 2

Unterstützen wir viele Hersteller, die eben Medizinprodukte herstellen und da haben solche Probleme mit der I.T.

00:00:45 Sprecher 2

Sicherheit ja oft auch noch mal direkte Auswirkungen auch auf die Patientensicherheit.

00:00:48 Sprecher 2

Und da geht es nicht nur um den Datenschutz.

00:00:51 Sprecher 2

Und so wollte ich heute mit dem Christian Rosenzweig beleuchten, wie I.T.

00:00:56 Sprecher 2

Sicherheit, wie Risikomanagement miteinander zusammenspielen, was wir da an Vorschriften haben, aber auch vielleicht ein paar

00:01:02 Sprecher 2

Best Practices, die Ihnen wiederum helfen, nicht die gleichen Fehler zu machen.

00:01:07 Sprecher 2

Ja, und wie schon angekündigt, ist mit mir heute der Christian Rosenzweig, der am besten noch ein paar Worte über sich sagt.

00:01:13 Sprecher 2

Dann können Sie ihn auch ein bisschen besser einschätzen, falls Sie ihn noch nicht kennen sollten.

00:01:17 Sprecher 3

Ja, hallo, mein Name ist Christian Rosenzweig.

00:01:19 Sprecher 3

Ich bin 50 Jahre alt, hab 3 wundervolle Kinder, hab in den 90er Jahren Krankenpflege gelernt.

00:01:25 Sprecher 3

Anschließend Medizintechnik studiert und viele Jahre in der Industrie gearbeitet als Entwicklungsingenieur für Medizinprodukte.

00:01:32 Sprecher 3

Hab dann gewechselt ins Qualitätsmanagement, bin auch Qualitätsmanagementbeauftragter gewesen und bin schließlich vor dreieinhalb Jahren zum Jona Institut gekommen als Berater für Medizinprodukte und betreue da die Schwerpunkte Risikomanagement und I.T.

00:01:45 Sprecher 3

Sicherheit.

00:01:46 Sprecher 2

Ja, da sind wir auch alle glücklich, sehr glücklich, einmal dass du da bist und zum anderen, dass du genau dich um diese Schwerpunkte auch mit kümmerst und unter anderem eben auch das Seminar ja zu beiden Themen mit anbietest.

00:01:58 Sprecher 2

Ja, schauen wir mal vielleicht ein bisschen rein.

00:02:00 Sprecher 2

Also, was sind so

00:02:01 Sprecher 2

Typische Schwierigkeiten, mit denen jetzt die Hersteller im Bereich Risikomanagement, I.T.

00:02:07 Sprecher 2

Sicherheit immer wieder kämpfen.

00:02:08 Sprecher 2

Was sind ja auch Dinge, die die benannten Stellen, die die Behörden regelmäßig bei denen kritisieren?

00:02:14 Sprecher 2

Man könnte halt sagen, ja, was für Probleme gibt es eigentlich da in dem Kontext?

00:02:18 Sprecher 3

Ja, das sind ganz viele.

00:02:19 Sprecher 3

Da muss man erstmal anfangen mit der Fragestellung, was sind denn überhaupt die regulatorischen Anforderungen, die ich erfüllen muss als Hersteller?

00:02:25 Sprecher 3

Und da tun sich die Hersteller teilweise schwer.

00:02:27 Sprecher 3

Beim Risikomanagement ist es noch relativ einfach, da ist die harmonisierte Norm ISO 14971 schon seit vielen Jahren der Goldstandard.

00:02:34 Sprecher 3

Beim IT-Sicherheitsthema sieht es ein bisschen anders aus, da gibt es nämlich noch nicht diesen Goldstandard für Medizinprodukte.

00:02:41 Sprecher 3

Da ist der Hersteller dann meistens mit einer Masse an regulatorischen Anforderungen konfrontiert, die mehr oder weniger verbindlich sind.

00:02:48 Sprecher 3

Es gibt da jede Menge Guidance-Dokumente,

00:02:51 Sprecher 3

Frameworks, Normen und in dieser Masse muss er sich dann irgendwie navigieren und zurechtfinden und eigentlich bleibt für ihn immer das Gefühl, er hat irgendwas unberücksichtigt gelassen und scheitert dann an der Umsetzung, weil es einfach zu viel ist.

00:03:04 Sprecher 3

Die nächste Problematik ist, dass diese regulatorischen Anforderungen dann natürlich auch umgesetzt werden müssen.

00:03:10 Sprecher 3

Das heißt, man muss sie interpretieren und verstehen, wie man sie in die eigene Praxis, ins eigene Unternehmen überträgt.

00:03:15 Sprecher 3

Bei der 14971 ist es so, dass die mittlerweile sehr prägnant

00:03:19 Sprecher 3

Die einzelnen Anforderungen formuliert, aber trotzdem bietet sie auch Interpretationsspielraum und da tun sich halt Hersteller auch schwer, das dann entsprechend umzusetzen.

00:03:28 Sprecher 3

Da hilft es immer, erfahrene Kollegen an der Seite zu haben, die so ein bisschen Best-Practice-Erfahrung haben.

00:03:34 Sprecher 2

Also, ich hab jetzt so 2 Punkte gehört.

00:03:36 Sprecher 2

Der erste Typ für Schwierigkeiten ist, man weiß gar nicht, was regulatorisch gefordert ist und die zweite, wenn man es weiß, weiß man nicht, wie man es umsetzen soll.

00:03:42 Sprecher 2

Ganz genau, schauen wir vielleicht da in beide Themen noch mal mit ein.

00:03:45 Sprecher 2

Also, die fährt 271 zum Risikomanagement, die hast du bereits genannt und ich denk, dass die IVDR und MDR auch ein Risikomanagementsystem ja sogar verlangt.

00:03:54 Sprecher 2

Das tauchte, glaub ich, schon im Artikel 10 mit auf.

00:03:56 Sprecher 2

Ich glaub, das ist hindenklich bekannt.

00:03:57 Sprecher 2

Wenn wir jetzt vielleicht noch mal in den Bereich IT-Sicherheit reingehen, was haben wir da an

00:04:02 Sprecher 2

Vorgaben, was man da an Normen, was sollte ein Hersteller da auf dem Zettel haben?

00:04:07 Sprecher 3

Ja, das fängt schon mal an mit der Forderung in der M.

00:04:10 Sprecher 3

D.

00:04:10 Sprecher 3

R.

00:04:10 Sprecher 3

selbst beziehungsweise I.

00:04:11 Sprecher 3

V.

00:04:11 Sprecher 3

D.

00:04:11 Sprecher 3

R.

00:04:12 Sprecher 3

Da heißt es jetzt eben in Anhang 1 bei den grundlegenden Sicherheits und Leistungsanforderungen, dass das Thema I.

00:04:16 Sprecher 3

T.

00:04:16 Sprecher 3

Sicherheit eben auch berücksichtigt werden muss.

00:04:19 Sprecher 3

Punkt.

00:04:19 Sprecher 3

Und das ist für viele Hersteller jetzt zwar ‚n Einstiegspunkt, ‚n Triggerpunkt, aber das gibt natürlich nicht viel Substanz her.

00:04:26 Sprecher 3

Die nächste Ebene ist dann das M.D.C.G.

00:04:29 Sprecher 3

Guidance Dokument 2019 strich 16 Revision 1.

00:04:34 Sprecher 3

Das beschreibt jetzt schon ein bisschen mehr spezifischer, was da drunter zu verstehen ist unter I.T.

00:04:39 Sprecher 3

Sicherheit, aber ehrlich gesagt, bleibt es auch noch sehr unspezifisch und sehr an der Oberfläche, aber es hat schon Präferenzen auf verschiedene Normen oder andere Guidance Dokumente, über die man sich dann immer tiefer ins Thema reingraben kann.

00:04:50 Sprecher 3

Und ganz neu ist letztes Jahr eine Norm auf den Markt gekommen, die IEC 81001 strich 5 strich 1.

00:04:57 Sprecher 3

Die steht mittlerweile auch auf der Vorschlagsliste der E.U.

00:05:00 Sprecher 3

Kommission zur Harmonisierung und die wird sich hoffentlich zum Goldstandard in der Medizinprodukt-tewelt dann etablieren.

00:05:06 Sprecher 2

Könntest du uns da ganz kurz so ‚n paar Punkte nennen, die jetzt diese neue Norm mit adressiert, also dass man einfach mal zum Gefühl hat, was da gefordert wird?

00:05:14 Sprecher 3

Ja, das Schöne an

00:05:15 Sprecher 3

dieser Norm ist, dass sie sich so ein bisschen an der 62304, dem Software-Lebenszyklus, entlanghangelt.

00:05:21 Sprecher 3

Das heißt, die übernimmt quasi das gleiche Grundkonzept des Entwicklungsprozesses und klinkt sich da mit ihren Aktivitäten ein.

00:05:27 Sprecher 3

Und die sagt dann zum Beispiel, wenn du Anforderungsmanagement machst, dann berücksichtige bitte auch die Anforderungen an IT-Sicherheit und dabei auch die IT-Sicherheitsumgebung, in der dein Produkt eingebunden ist und jongliert da so ein bisschen mit den Anforderungen, die du ans Produkt selbst aufstellst oder eben an den Betreiber richtest.

00:05:44 Sprecher 3

Und

00:05:45 Sprecher 3

Das zusammen gibt dann eben dieses Sicherheitskonzept oder diese I.T.

00:05:48 Sprecher 3

Security Capabilities des Produktes und dann geht es eben weiter über die Architektur, wo ich dann eben auch bestimmte I.T.

00:05:55 Sprecher 3

sicherheitsrelevante Gesichtspunkte wie dieses Defense In Depth Modell berücksichtigen muss.

00:06:01 Sprecher 3

Über die Implementierung hin zu den Tests und bei den Tests gibt es jetzt eben auch einen Blumenstrauß an neuen Tests, die bisher so nicht bekannt waren oder so nicht üblich waren.

00:06:11 Sprecher 3

Penetration Test, Vulnerability Scanning.

00:06:14 Sprecher 3

Sind da zu nennen oder fast Testing, die kommen da jetzt eben noch neu dazu.

00:06:17 Sprecher 2

Also, neu im Sinne, dass es regulatorisch medizinproduktespezifisch gefordert wird, weil in der IT-Security-Zelle ist es jetzt nicht so neu.

00:06:25 Sprecher 2

Genau, aber eben neu, halt eben, dass es jetzt mal, dass man so konkret wird.

00:06:30 Sprecher 2

Also, was man jetzt schön hört, was du bereits berichtet hast, ist, dass die IT-Sicherheit eben nichts ist, was man reinprüft, sondern dass es über den kompletten Entwicklungs oder musst du sogar sagen, Produktlebenszyklus sind.

00:06:43 Sprecher 2

gelebt werden muss.

00:06:44 Sprecher 2

Also, dass wir in allen Phasen Aktivitäten haben, vielleicht kleine Werbung in eigener Sache.

00:06:48 Sprecher 2

Deswegen haben wir auch den I.T.

00:06:50 Sprecher 2

Security Guide, den wir ja gemeinsam geschrieben haben und den die benannten Stellen jetzt ja auch bei sich verwenden, genau nach diesen Phasen wiederum sortiert, um vielleicht auch noch mal ‚ne Stufe granularer oder prüfbarer zu werden, was diese Lebenszyklusaktivitäten mit angeht.

00:07:06 Sprecher 2

Also, ich glaub, das ist für Hersteller wirklich ‚n wichtige

00:07:09 Sprecher 2

Erkenntnis, das was du auch noch mal gerade gesagt hast, oder eine wichtige Sache, die es im Kopf behalten sollten: IT-Sicherheit beginnt mit der Beginn oder vor Beginn der Entwicklung und nicht erst, wenn das Produkt gebaut worden ist und man dann schaut, ja, ist das überhaupt sicher?

00:07:21 Sprecher 2

Jetzt waren wir schon sehr im Thema IT-Security mit drin.

00:07:25 Sprecher 2

Hättest du uns noch ein paar?

00:07:27 Sprecher 2

Tipps, wie wir ja dieses Zusammenspiel zwischen IT-Security und Risikomanagement hinbekommen.

00:07:33 Sprecher 2

Also, du hast jetzt schön gezeigt, wie die IT-Sicherheit und der Software-Lebenszyklus-Prozess ineinander spielt.

00:07:38 Sprecher 2

Ja, wenn man sozusagen bei den Anforderungen oder bei der Architektur, da wer zum Beispiel ein Threat Modeling anwendet und nachher die Tests hat man dann halt die Sondertests wie Penetration Tests, aber wie?

00:07:47 Sprecher 2

spielt jetzt dieser IT-Security-Prozess und der Risikomanagement-Prozess zusammen?

00:07:52 Sprecher 2

Könntest du da noch ein paar Tipps geben?

00:07:54 Sprecher 3

Ja, das ist ein ganz wichtiges Thema, wo viele Hersteller auch auf die Nase fallen, möchte ich nicht sagen, aber zumindest ihre Probleme haben, weil in der IT-Security geht es immer um die Schutzziele Datenintegrität, Datenverfügbarkeit und Datenvertraulichkeit und beim Risikomanagement nach 14971 geht es eigentlich um das Schutzziel Patientenschaden oder Schaden am Menschen zu verhindern.

00:08:13 Sprecher 3

Und die beiden Themen jetzt übereinander zu legen, ist schwierig.

00:08:16 Sprecher 3

Zumindest bei den Bewertungskatalogen, da habe ich dann eben Schwierigkeiten zu sagen, der klassische Schaden am Menschenbewertungskatalog, da bringe ich jetzt die Datenschutzthematik noch mit rein und deswegen ist es sinnvoll, die beiden Bereiche aufzutrennen und zu sagen, ich habe einen Standalone-Risikomanagementprozess für die IT-Security und habe auf der anderen Seite das 14971 Konstrukt mit seiner eigenen Risikotabelle.

00:08:38 Sprecher 3

Und jetzt erstelle ich eben auf Seite der IT-Security eine Risikotabelle, entweder auf Basis des Thread Modeling, das du schon angesprochen hast.

00:08:46 Sprecher 3

oder über andere Methoden, wie dieses mehr FMEA-basierte Threat Risk Analysis Modell und die Risiken, die ich dabei finde, die übertrage ich eben in die Liste der IT-Security Risiken, mache da auch einen anderen Bewertungskatalog, wie zum Beispiel einen CVSS Score und definiere dann auch Maßnahmen und eine Risikoakzeptanz in dem Gebiet.

00:09:06 Sprecher 3

Und wenn ich damit fertig bin, dann übertrag ich die Erkenntnisse aus dieser Tabelle, so sie denn relevant sind, in die

00:09:14 Sprecher 3

Risikotabelle nach 14 971, weil dann kann ich nämlich weiter bis zum Schaden am Menschen durchdeklinieren und hab dann diese Risiken dort auch erfasst und bewertet und mit Maßnahmen versehen, falls die darüber hinausgehen über das, was ich in der I.

00:09:28 Sprecher 3

T.

00:09:29 Sprecher 3

Security schon als Maßnahmen festgelegt hab.

00:09:31 Sprecher 2

Ah, OK, also das sind jetzt vielleicht ein Gedanke und sozusagen noch eine ganz kurze Zusammenfassung von mir, ob ich alles richtig verstanden hab.

00:09:37 Sprecher 2

Also das erste, was du gesagt hast, ist passt auf, wir haben unterschiedliche Ziele oder wir können

00:09:42 Sprecher 2

gegebenenfalls unterschiedliche Ziele haben in der IT Security und im Risikomanagement, vielleicht sogar noch ein Beispiel dafür.

00:09:48 Sprecher 2

Es kann sein, dass wir mit einer Erhöhung der IT Security die Safety kompromittieren.

00:09:54 Sprecher 2

Wir hatten sogar so einen Fall schon mal gehabt, da haben die die Zugriffsrechte auf Patientendaten für Pflegekräfte reduziert und haben damit die Vertraulichkeit als einen Aspekt der IT Security hochgefahren.

00:10:06 Sprecher 2

Das Ergebnis war, die Pflegekräfte waren nicht mehr

00:10:10 Sprecher 2

In der Lage, Fehler in Medikationsverschreibungen zu finden und es ist auch wirklich was passiert.

00:10:14 Sprecher 2

Patient Safety ging runter.

00:10:15 Sprecher 2

Das heißt, die können sogar im Extremfall im Widerspruch stehen.

00:10:19 Sprecher 2

Und in einer Norm, ich glaub, das ist die UL 2900 strich 2 strich 1 steht sogar so ein Konzept mit drin und die FDA hat es auch.

00:10:25 Sprecher 2

Breaking the Glass, also quasi wie so eine Art Feuermelder, wo man dann sagen kann, ich überschreibe jetzt alles, vergesst jetzt hier die die Vertraulichkeit.

00:10:33 Sprecher 2

Wir müssen hier jetzt um die Patientensicherheit kümmern.

00:10:35 Sprecher 2

Also, das ist, glaub ich, ein wichtiger Aspekt.

00:10:37 Sprecher 2

dann das Zweite, was du gesagt hast, war eigentlich, wie die beiden zusammen spielen.

00:10:42 Sprecher 2

Und wenn ich dich richtig verstanden hab, haben wir auf der einen Seite diesen I.T.

00:10:45 Sprecher 2

Security Prozess mit dem Ziel, I.T.

00:10:48 Sprecher 2

Sicherheitsrisiken zu identifizieren und die wiederum werden dann in den Risikomanagementprozess mit eingespielt.

00:10:55 Sprecher 2

Und da schaut man ja, was wäre dann so ein Risiko oder eine Kompromittierung, was würde die Bedeutung der I.T.

00:11:00 Sprecher 2

Sicherheit für die Patientensicherheit, kann man das so sagen?

00:11:03 Sprecher 3

Ganz genau, und es geht sogar noch einen Schritt weiter.

00:11:06 Sprecher 3

wenn man das M.D.C.G.

00:11:07 Sprecher 3

Dokument anschaut, dann sieht man auf der allerletzten Seite, dass da die beiden Prozesse gegenübergestellt sind, der I.T.

00:11:14 Sprecher 3

Security Risikomanagementprozess und der 14 971 Risikoprozess und dann sind da Pfeile dazwischen gemalt und das sind diese Bezüge, die man da hat.

00:11:21 Sprecher 3

Ich schaue eben nach, hat ein Risiko aus der I.T.

00:11:24 Sprecher 3

Security auch einen Bezug zum Schaden am Menschen, dann überführ ich das.

00:11:27 Sprecher 3

Aber es kann auch sein, dass eine Maßnahme im Bereich der I.T.

00:11:30 Sprecher 3

Security jetzt wieder eine

00:11:32 Sprecher 3

auslösende Risikoursache ist für 14 971 und umgekehrt kann auch eine Maßnahme im 14 971 Bereich

wieder ein I.

00:11:40 Sprecher 3

T.

00:11:40 Sprecher 3

Security Risiko bedingen.

00:11:41 Sprecher 3

Wenn ich zum Beispiel sag, ich hab das Problem, dass meine Medikationsdaten auch verschwinden können, weil die Festplatte zum Beispiel crasht, dann mach ich eben ein ein Backup in der Cloud, damit ich dieses Problem jetzt auf 14 971 Seite nicht mehr hab.

00:11:55 Sprecher 3

aber dadurch hab ich natürlich jetzt wieder ein Loch gerissen im Bereich Datenvertraulichkeit, weil in der Cloud liegen meine Patientendaten jetzt und dann muss ich dort wieder handhaben und diese, diese ständigen Zirkelbezüge oder diese ständigen Iterationsschritte, die muss ich eben im Entwicklungsprozess berücksichtigen.

00:12:11 Sprecher 2

Mhm, hast du noch weitere Tipps, die uns sozusagen gerade bei diesem komplexen Handling da helfen könnten, weiß ich, Richtung Automatisieren, Werkzeuge, Vorgehensmodelle?

00:12:21 Sprecher 3

Ja, das Wichtigste ist, ich hab

00:12:23 Sprecher 3

eine Schnittstelle in den Verantwortlichkeiten.

00:12:27 Sprecher 3

Ich habe meistens ein Team, das sich um die 1479 Risiken kümmert, der klassische Risikomanager ist da als Rolle benannt und auf der anderen Seite habe ich eben dieses Team der IT-Security-Experten und die müssen sich irgendwie miteinander entweder an einen Tisch setzen oder kommunizieren und müssen auch die entsprechenden Werkzeuge haben und was sich da eben etabliert hat ist, dass sie ihre getrennten Tabellen führen, aber die dann immer austauschen und das kann man natürlich toolgestützt machen

00:12:52 Sprecher 3

wobei mir bis jetzt noch kein Tool untergekommen ist, dass ich wirklich problemlos empfehlen könnte.

00:12:57 Sprecher 2

Was würdest du Menschen empfehlen, die da tiefer einsteigen wollen?

00:13:02 Sprecher 2

Also, ich würd mal vermutlich da vielleicht deine Kontaktdaten preisgeben.

00:13:06 Sprecher 2

Was können die noch machen, wenn die ja vielleicht auch produktspezifische Fragen haben oder noch tiefer in dieses Thema, ja, Nahtstelle Risikomanagement, I.

00:13:15 Sprecher 2

T.

00:13:15 Sprecher 2

Security, wenn die da noch tiefer einsteigen wollen.

00:13:17 Sprecher 3

Ja,

00:13:18 Sprecher 3

ein ganz guter Einstieg ist immer das Seminar sowohl für Risikomanagement als auch für I.

00:13:23 Sprecher 3

T.

00:13:23 Sprecher 3

Sicherheit, weil man da eben komprimiert in 2 Tagen noch mal alle Themen rund um dieses Konzept oder die Vorgehensweise erfährt und viele Hersteller haben da ‚n Aha-Erlebnis, weil sie eben sagen, ich hab das bis jetzt immer auf bestimmte Art und Weise bei mir umgesetzt, aber jetzt hab ich noch mal den vollen Blick auf das Thema bekommen und das hat mich jetzt noch mal weitergebracht.

00:13:44 Sprecher 3

Neben diesen Seminaren können wir dann auch Workshops als Format anbieten.

00:13:48 Sprecher 3

Dabei kann man interaktiv mit dem Hersteller zusammen seine Akten durchgehen, seine Vorgehensweisen besprechen, Fragen beantworten oder eben ganz neu Verfahren und Prozesse etablieren oder eben Akten erstellen, die dann auch konform bei der Zulassung verwendet werden können.

00:14:05 Sprecher 2

Auch F.D.L.

00:14:05 Sprecher 3

Ja, ganz genau.

00:14:07 Sprecher 3

da arbeiten wir auch international mit unseren entsprechenden Team zusammen, die auch in anderen Märkten etabliert sind und bei ID Security haben wir ganz neu im Programm das Thema Penetration Tests, das heißt wir bieten dann auch operative Unterstützung bei der Durchführung, das heißt die Durchführung im Auftrag des Herstellers von Penetration Tests oder Vulnerability Scanning als auch Risikoanalyse für sein Produkt und das ist jetzt eine Ergänzung unserer Dienstleistungen in der Art und Weise, dass wir jetzt eben vollen

00:14:37 Sprecher 3

umfangreichen Service bieten rund um I.

00:14:39 Sprecher 3

T.

00:14:39 Sprecher 2

Security.

00:14:40 Sprecher 2

Ja, und das hat den Herstellern, die da waren, glaube ich, auch immer ziemlich gut getan, weil wir haben noch nie nichts gefunden.

00:14:44 Sprecher 2

Also zum Teil waren das sogar katastrophale Fehler und müssen ja nicht noch jemand in der Tages-schau haben, wobei wir ja wieder am Anfang des Podcasts zurückgekehrt wären.

00:14:54 Sprecher 2

Ich glaub, so sind wir genau eingestiegen mit diesem einen Praxishersteller.

00:14:57 Sprecher 2

Also das wäre auf jeden Fall ,ne sehr gute Maßnahme, um da diese Löcher abzuklopfen.

00:15:02 Sprecher 2

Ja, also ich würd sagen, ich verlink das einfach, ist dann also sowohl

00:15:06 Sprecher 2

deine beiden Seminare Risikomanagement I.

00:15:08 Sprecher 2

T.

00:15:08 Sprecher 2

Security und auch die Hinweise zu unseren Penetration Testern.

00:15:13 Sprecher 2

Ich glaub, das ist ein umfangreiches, ein gutes Angebot.

00:15:15 Sprecher 2

Ja, du, da bleibt mir nur dir ganz, ganz herzlichen Dank zu sagen.

00:15:18 Sprecher 2

Hat super Spaß gemacht.

00:15:20 Sprecher 2

Ich hoffe, bis bald wieder.

00:15:21 Sprecher 3

Danke dir auch, Christian.