Johner Institut

IT-Sicherheit: Erwartungen der Benannte Stellen

Mit Christian Rosenzweig, Prof. Dr. Christian Johner

Transkript

00:00:05 Sprecher 1

Medical Device Insights, ein Podcast des Jona Instituts für Medizinprodukteherstellen, Behörden und benannte Stellen.

00:00:18 Sprecher 2

Manchmal fordern benannte Stellen Dinge schneller ein, wie wir das selber gedacht haben und ein trauriges Beispiel dafür ist das Thema IT-Sicherheit.

00:00:27 Sprecher 2

Und in diesem Podcast wollen wir berichten,

00:00:30 Sprecher 2

Was wir beobachtet haben, was da zurzeit passiert, was benannte Stellen von den Herstellern einfordern, was wir empfehlen, was die Hersteller machen sollten, um letztlich Probleme zu vermeiden und ja, auch die Kosten, die damit typischerweise einhergehen und die Verzögerung bei den ganzen Zulassungsverfahren.

00:00:47 Sprecher 2

Und wen kompetenter könnte ich da einladen als meinen Kollegen, den Christian Rosenzweig, der Christian vielleicht doch 23 Worte zu sich sagt, damit die Hörer dich gut einordnen können.

00:00:57 Sprecher 3

Jawoll, hallo Christian.

00:00:58 Sprecher 3

Mein Name ist Christian Rosenzweig.

00:01:00 Sprecher 3

Ich bin seit 4 Jahren Berater am Jona Institut und betreue Medizinprodukteherstellen hauptsächlich zu den Themen Risikomanagement und I.

00:01:08 Sprecher 3

T.

00:01:08 Sprecher 3

Security.

00:01:08 Sprecher 2

Ja, das heißt, du bist genau unser richtiger Ansprechpartner.

00:01:11 Sprecher 2

Also, wir müssen zugeben, dass wir die Situation bis vor kurzem ein bisschen anders eingeschätzt hatten.

00:01:18 Sprecher 2

Ja, wir hatten nämlich ‚ne These, was benannte Stellen da konkret einfordern.

00:01:22 Sprecher 2

Das war Christian, wenn du das vielleicht ganz kurz noch mal wiederholen

00:01:26 Sprecher 2

würdest, bevor wir dann zur Realität kommen, was dachten wir, was benannte Stellen besonders einfordern?

00:01:31 Sprecher 3

Ja genau, wenn man sich mit dem Thema I.

00:01:33 Sprecher 3

T.

00:01:33 Sprecher 3

Sicherheit beschäftigt, dann wird man feststellen, dass das ein riesen Gebiet ist mit vielen, vielen Aktivitäten, mit vielen Konzepten, die da ‚ne Rolle spielen.

00:01:42 Sprecher 3

Und wir hatten eigentlich gedacht, dass sowohl die benannten Stellen mit ihren entsprechenden Auditoren als auch die Medizinproduktehersteller sich in dieses Themenfeld erstmal einarbeiten müssen.

00:01:50 Sprecher 3

Die M.

00:01:51 Sprecher 3

D.

00:01:51 Sprecher 3

R.

00:01:51 Sprecher 3

hat ja relativ schnell das Themengebiet eingeklagt.

00:01:55 Sprecher 3

Und die Leute mussten eben entsprechend nachziehen mit ihrer eigenen Qualifikation.

00:02:01 Sprecher 3

Ich habe dann mal mit einer benannten Stelle gesprochen und habe gefragt, was erwartet ihr da eigentlich am Anfang von den Herstellern?

00:02:07 Sprecher 3

Die können ja nicht von heute auf morgen alles implementieren.

00:02:10 Sprecher 3

Und dann haben die gesagt, uns sind zwei Punkte wichtig.

00:02:14 Sprecher 3

Das eine ist die Qualifikation des Personals und das andere ist, dass am Ende des Entwicklungsprozesses ein Penetration Test gemacht wird, um sozusagen nachzuweisen, dass das Produkt auch wirklich

00:02:24 Sprecher 3

ausreichend I.

00:02:25 Sprecher 3

T.

00:02:25 Sprecher 3

sicher ist und das sind sozusagen die Rahmenbedingungen am Anfang und am Ende des Entwicklungsprozesses, die müssen auf jeden Fall da sein.

00:02:32 Sprecher 3

Und das habe ich auch immer so meinen Herstellern weitergegeben, meinen Kunden und dann habe ich eben im Lauf der Zeit gesehen, dass es doch anders ist.

00:02:39 Sprecher 2

Ja, da müssen wir gleich drüber sprechen, was jetzt eingefordert wird.

00:02:43 Sprecher 2

Vielleicht noch so ,ne Frage zu diesem regulatorischen Rahmen, weil man kann jetzt ja nicht irgendwas da fordern.

00:02:49 Sprecher 2

Wenn wir mal ganz kurz durchgehen, was haben wir so an wichtigen

00:02:52 Sprecher 2

regulatorischen Vorgaben, die Hersteller kennen und auch einhalten sollten.

00:02:58 Sprecher 3

Ja, genau da kommt auch das nächste Problem her.

00:03:00 Sprecher 3

Die M.D.R.

00:03:01 Sprecher 3

fordert im Anhang 1, dass Informationssicherheit eben berücksichtigt werden muss im Produktlebenszyklus und führt das Ganze aber nicht sehr viel weiter aus.

00:03:10 Sprecher 3

Also muss man nach einer Quelle suchen, die mindestens genauso verbindlich ist wie die M.D.R.

00:03:14 Sprecher 3

und da bietet sich das M.D.C.G.

00:03:16 Sprecher 3

Guidance Dokument an, das zumindest eine Interpretation der M.D.R.

00:03:19 Sprecher 3

liefert.

00:03:20 Sprecher 3

Jetzt hat dieses Guidance-Dokument sehr viel zum Thema IT-Sicherheit gesagt.

00:03:24 Sprecher 3

Das ist das MDCG 2019/16, aber leider Gottes auf sehr abstrakte Art und Weise und das hat den Herstellern oft nicht weitergeholfen.

00:03:32 Sprecher 3

Und dann haben sie sich eben auf die Suche gemacht und haben sehr, sehr viele verschiedene Dokumente gefunden, die man als Stand der Technik betrachten kann.

00:03:40 Sprecher 3

Und das hat die Problematik noch verschärft, weil eben dann keiner genau wusste, was ist jetzt eigentlich Stand der Technik, wie kann ich das selbst für mich definieren.

00:03:46 Sprecher 2

Absolut, und das war ja genau auch der Auslöser, dass wir gesagt haben, wir brechen das mal runter bis in wirklich binär entscheidbare Checkpunkte.

00:03:55 Sprecher 2

Und so ist ja genau die I.T.

00:03:56 Sprecher 2

Sicherheitsleitfahrten entstanden, den die benannten Stellen dann auch mehr oder weniger direkt übernommen haben.

00:04:02 Sprecher 2

Also, das heißt, da haben wir mal so ein sozusagen als verbindlichen Teil haben wir die M.D.R.

00:04:07 Sprecher 2

als nicht ganz so hilfreiche Interpretation des M.D.C.G.

00:04:12 Sprecher 2

Dokument und

00:04:13 Sprecher 2

zusätzlich eben dann den Leitfaden, der sehr konkret und sehr spezifisch ist.

00:04:18 Sprecher 2

Ja, jetzt haben wir quasi diesen Rahmen und wenn man jetzt mal reinschaut, was wird jetzt tatsächlich abgefragt, was sind da deine Erfahrungen?

00:04:25 Sprecher 3

Ja, das will ich an einem Beispiel mal klar machen, da hat neulich ein Hersteller mich angefragt, weil er in einem Audit mit einer benannten Stelle in Probleme gekommen ist.

00:04:33 Sprecher 3

Er hatte also Abweichungen bei der I.T.

00:04:36 Sprecher 3

Sicherheit und zwar war das ein aktives Medizinprodukt, das im O.P.

00:04:39 Sprecher 3

Umfeld eingesetzt wird und er hatte nur eine U.S.B.

00:04:42 Sprecher 3

Schnittstelle, es war also ein

00:04:43 Sprecher 3

nicht vernetztes Medizinprodukt, sondern einfach nur eine USB-Datenschnittstelle.

00:04:48 Sprecher 3

Und er hat argumentiert, dass er dann keine Aktivitäten zur IT-Sicherheit braucht, weil er eben nur limitiert angreifbar ist.

00:04:56 Sprecher 3

Man braucht eben physischen Zugriff auf dieses Produkt.

00:04:58 Sprecher 3

Und das war seine Strategie, also ein risikobasiertes Vorgehen.

00:05:01 Sprecher 3

Er hat es auch gegen die MDCG als GAP-Analyse, also gegen das MDCG-Dokument 2019/16 als GAP-Analyse formuliert.

00:05:09 Sprecher 3

und hat gesagt, wir brauchen eben die dort aufgezählten Aktivitäten nicht, weil wir nur eine USB-Schnittstelle haben und dann hat die benannte Stelle gesagt, nein, das reicht uns nicht.

00:05:17 Sprecher 3

Wortwörtlich hat sie gesagt, das ist kein akzeptabler Approach und dann hat der Hersteller gesagt, was stellt ihr euch denn stattdessen vor und die benannte Stelle darf aber in so einem Fall nicht beraten.

00:05:26 Sprecher 3

Das heißt, sie sind auf ihrem Statement stehen geblieben, dass sie es eben einfach nicht akzeptieren.

00:05:30 Sprecher 3

Dann hat der Hersteller versucht, noch andere Gap-Analysen zu kreieren gegen FDA-Guidance-Dokumente beispielsweise, hat auch nicht funktioniert

00:05:38 Sprecher 3

Und dann ist er letztendlich zu mir gekommen und wir haben dann gemeinsam geschaut, wie könnten wir den Stand der Technik erst mal formulieren und haben dann die zu harmonisierende Norm, die IEC 81001-5-1 angeschaut.

00:05:51 Sprecher 3

Das ist eben die, die die EU-Kommission zur Harmonisierung unter der MDR vorgesehen hat.

00:05:56 Sprecher 3

Und dann haben wir gesagt, wir nehmen die jetzt und nehmen die wichtigsten Punkte da draus und versuchen, die abzubilden, nachträglich, also sozusagen den Entwicklungsprozess nach dieser Norm

00:06:06 Sprecher 3

durchzuführen und zu dokumentieren.

00:06:08 Sprecher 3

Das haben wir dann gemacht.

00:06:09 Sprecher 3

Daraufhin hat die benannte Stelle gesagt, prima, das ist jetzt der Approach, den wir uns vorgestellt hätten.

00:06:14 Sprecher 3

Und damit wussten wir schon mal, jetzt sind wir auf dem richtigen Pfad.

00:06:17 Sprecher 3

Was dann aber passiert ist, und das ist, glaube ich, ebenso spannend, die haben sich nicht damit zufrieden gegeben, sondern die sind dann in einem weiteren Review-Schritt tiefer reingegangen, haben einen Fachexperten sich selbst dazu geholt, der dann die vorhandene Dokumentation, die wir nach der 81001.51 erstellt hatten, noch tiefer angeschaut.

00:06:36 Sprecher 3

und dabei haben sie dann Sachen rausgepickt, wie zum Beispiel, dass das System über eine Benutzer-

authentifizierung per Passwort versehen war, aber der Hersteller hat nichts implementiert, was eine Ablauffrist des Passworts bedeutet oder dass das eingeklagt wird vom Anwender.

00:06:52 Sprecher 3

Und dann hat die benannte Stelle argumentiert, nicht mit einem Ablaufdatum versehenes Passwort ist genauso schlecht wie gar kein Passwort und das lassen sie nicht gelten.

00:07:01 Sprecher 3

Und daran sieht man eigentlich, dass

00:07:03 Sprecher 3

die benannten Stellen schon tief reingehen, dass die sich nicht nur den generellen IT-Security-Lebenszyklus-Prozess zeigen lassen, sondern dass die dann auch inhaltlich in die einzelnen Themengebiete reingehen und die hinterfragen.

00:07:15 Sprecher 3

Und das ist eine Qualität, die kennen wir aus der 62304, zum Beispiel aus dem Software-Lebenszyklus-Prozess oder aus dem Risikomanagement-Prozess nach ISO 14971.

00:07:24 Sprecher 3

Aber ich hätte nicht erwartet, dass jetzt schon in der ersten Welle der MDR-Audits diese Detailprüfung der

00:07:30 Sprecher 3

Granularität stattfindet.

00:07:31 Sprecher 2

Das ist wirklich überraschend.

00:07:33 Sprecher 2

Auf der einen Seite kann man natürlich froh sein, wenn da mal mit Kompetenz rangegangen wird, aber auf der anderen Seite muss man natürlich immer fragen, ist das jetzt noch risk-based?

00:07:41 Sprecher 2

Also du hast ja gesagt, wir sprechen hier von der USB-Schnittstelle, also von der Schnittstelle, wo man da ja schon direkt mit auf dem Gerät mit drauf sitzt und das Thema Ablauf von Passwörtern ist ja mittlerweile auch nicht ganz so einfach, dass man sagen kann, die müssen immer ablaufen, weil wenn man gerade weiß, wie es im Krankenhaus funktioniert.

00:07:58 Sprecher 2

dann steigert das höchstens die Gefahr, dass die das Passwort irgendwo draufschreiben und damit die IT-Sicherheit nachher verringern.

00:08:04 Sprecher 2

O.K., aber so sind jetzt die Dinge.

00:08:06 Sprecher 2

Also die Kompetenz ist hoch, der Detaillevel offensichtlich auch.

00:08:12 Sprecher 2

Wie sehr Risikomanagement oder risikoorientiert dieser Ansatz ist, darüber können wir streiten.

00:08:17 Sprecher 2

Was würdest du jetzt den Herstellern konkret empfehlen?

00:08:20 Sprecher 2

Also, was sollen sie jetzt tun, um solch leidlichen Diskussionen möglichst zu vermeiden oder zumindest abzukürzen?

00:08:28 Sprecher 3

Der Weg wurde eigentlich schon von einer anderen benannten Stelle vorgegeben, die hat nämlich in einen Abweichungsbericht eines anderen Herstellers reingeschrieben, ihr habt ja gar keine I.

00:08:36 Sprecher 3

T.

00:08:36 Sprecher 3

Security Dokumentation, was wir mindestens erwartet hätten, wäre folgendes und dann haben sie alles aufgezählt, was sie Minimum erwarten würden und das ist freundlicherweise genau das, was wir jetzt als Handlungsleitfaden nehmen können.

00:08:49 Sprecher 3

Und die gute Nachricht ist,

00:08:51 Sprecher 3

Diese Vorgehensweise der benannten Stelle, die sie erwartet hätte, ist deckungsgleich mit der IEC 8100151, nämlich genau die Norm, die zur Harmonisierung unter der MDR ansteht für IT-Security.

00:09:01 Sprecher 3

Das heißt, wie kann sich der Hersteller jetzt vorbereiten, indem er genau diese Norm nimmt, sie durchliest, interpretiert und dann entsprechend im Qualitätsmanagementsystem implementiert und danach lebt.

00:09:12 Sprecher 3

Vielleicht noch ein Punkt, der wichtig ist: Wenn ich das jetzt zum Zeitpunkt X in mein Qualitätsmanagementsystem integriere und von jetzt an im Moment keine Entwicklung in die Produkte stecke, dann ist die Frage: Muss ich denn meine bisherigen Produkte, die schon im Markt sind, auch nach diesem Prozess durcharbeiten und die technische Dokumentation sozusagen nachpflegen?

00:09:31 Sprecher 3

Das kennen wir unter dem Begriff Legacy Devices, dass man eben schon Produkte nicht unter einer Norm im Markt hat, aber jetzt diese Norm erfüllen muss.

00:09:39 Sprecher 3

Und da sagt die 81151 auch ganz klar, wie man in dem Fall umgehen soll.

00:09:43 Sprecher 3

Da gibt es nämlich einen Anhang F, der beschreibt, dass man das Produkt nachentwickeln muss.

00:09:49 Sprecher 3

Man muss diese Software in der Umstellung nennen, die das auch, diese Software in der Umstellung auf den Stand bringen, der eigentlich nach 81151 erforderlich ist oder erwartet wird.

00:09:59 Sprecher 3

Und das Ganze muss man auch noch mit einer Risikobetrachtung versehen, die belegen soll, dass man in der Zwischenzeit, während man dieses Produkt eben nachentwickelt,

00:10:08 Sprecher 3

mit dem Produkt im Markt bleiben kann.

00:10:10 Sprecher 2

Boah, das sind natürlich extreme Hürden, die da aufgebaut werden.

00:10:13 Sprecher 2

Ein Stück weit kann man das sicher verstehen, weil doch vieles sehr, sehr rudimentär und stiefmütterlich bezüglich der I.

00:10:19 Sprecher 2

T.

00:10:19 Sprecher 2

Sicherheit bisher gemacht wurde.

00:10:21 Sprecher 2

Also insofern ist das nachvollziehbar, dass man da genauer drauf schaut.

00:10:25 Sprecher 2

Aber jetzt gerade bei den Beispielen, die du jetzt genannt hast, ja, schreibt man doch das sehr weit zu gehen.

00:10:29 Sprecher 2

Also das kann eine ganze Firma stilllegen, wenn man das jetzt da eher bis zum Ende durchexerziert.

00:10:34 Sprecher 2

Wie kannst du dabei helfen, dass

00:10:37 Sprecher 2

Man als Firma auf der einen Seite die IT-Sicherheit erreichen kann, aber jetzt nicht das ganze Unternehmen stilllegt und die ganzen Innovationen stoppt, die wir ja auch haben wollen.

00:10:45 Sprecher 2

Also dürfen wir nicht vergessen, was so die Patienten machen und nicht nur Dokumentationen für bekannte Stellen erstellen.

00:10:51 Sprecher 2

Also, was wären deine Unterstützungsangebote, die du?

00:10:54 Sprecher 2

uns geben kannst.

00:10:55 Sprecher 3

Also man sieht ja ganz klar, was die Erwartungshaltungen der benannten Stellen sind.

00:10:58 Sprecher 3

Ich habe es ja gerade dargestellt.

00:11:00 Sprecher 3

Und daran kommt man nicht vorbei.

00:11:01 Sprecher 3

Das heißt, es hilft jetzt nichts zu jammern und zu diskutieren, sondern man muss es umsetzen.

00:11:05 Sprecher 3

Und das heißt, man muss sich als erstes damit beschäftigen, was fordert die 8100151 von mir eigentlich?

00:11:11 Sprecher 3

Und dazu muss ich diese Norm verstehen.

00:11:13 Sprecher 3

Das dauert wieder, bis man sich da eingelesen hat, weil das eben ganz bestimmte Begrifflichkeiten auch sind.

00:11:17 Sprecher 3

Da muss man verstehen, was ist denn ein Threat-Modeling, was versteckt sich dahinter, was ist

00:11:22 Sprecher 3

Defense in Depth, was ist das für ein Konzept und wenn man das alles sich erarbeiten will, dann braucht man dafür viel Zeit im Unternehmen.

00:11:29 Sprecher 3

Das kann man sich ersparen, diese Zeit, indem man beispielsweise ein Seminar bei uns bucht.

00:11:34 Sprecher 3

Ich habe versucht, in 2 Tagen wirklich das ganze Thema, die ganze 81151 inklusive dem ganzen Hintergrund zur IT-Sicherheit komprimiert aufzuarbeiten, habe da viel Zeit rein investiert und davon können die Hersteller jetzt profitieren, die können das direkt nutzen und

00:11:49 Sprecher 3

um ihr Personal in den zwei Tagen auf den richtigen Stand zu bringen.

00:11:53 Sprecher 3

Das ist sozusagen der Startpunkt, um die Leute erstmal zu qualifizieren, zu enablen, dass sie in der Lage sind, Thema IT-Sicherheit im eigenen Unternehmen umzusetzen und dann geht es eben darum, das Qualitätsmanagementsystem entsprechend anzupassen.

00:12:04 Sprecher 3

Da helfen wir beispielsweise durch Vorlagen, die wir zur Verfügung stellen oder durch Workshops, in denen wir die Anpassung dieser Vorlagen ans eigene Unternehmen umsetzen.

00:12:12 Sprecher 3

Dann helfen wir auch operativ im Tagesgeschäft, wenn zum Beispiel so ein Threat Modeling gemacht wird, das ist eine Methode, um systematisch

00:12:19 Sprecher 3

IT-Security-Risiken zu analysieren, dann braucht man eine gewisse Erfahrung, um das zu machen.

00:12:24 Sprecher 3

Und da helfen wir dann wirklich mit Hands-on-Workshops, diese Risikoanalysen zu moderieren oder durchzuführen oder auch im Zweifelsfall in Auftragsarbeit umzusetzen, sodass dann am Ende eben schnell eine Akte entstehen kann.

00:12:37 Sprecher 3

Was auch noch ganz relevant ist, ist am Ende des Entwicklungsprozesses müssen ja bestimmte I.

00:12:42 Sprecher 3

T.

00:12:42 Sprecher 3

Security Tests gemacht werden.

00:12:44 Sprecher 3

Da unterstützen wir als Jona Institut durch Vulnerability Scanning oder Penetration Tests.

00:12:49 Sprecher 3

Da haben wir auch entsprechend qualifiziertes Personal dafür und das sind ganz grob mal die einzelnen Aktivitäten, mit denen wir Hilfestellung bieten.

00:12:56 Sprecher 2

Das ist gut und ich kann berichten, also gerade wenn du jetzt das Thema Penetration Tests ansprichst, wir hatten auch nie ‚n Fall, wo wir nicht auf gravierende Lücken gestoßen sind, obwohl wir alle

00:13:06 Sprecher 2

Hersteller ganz fest davon überzeugt waren, dass ihm das nicht passiert sei, aber die Wahrscheinlichkeit scheint sehr hoch zu sein, da auf Lücken zu treffen und ich fand auch den Stack, den du uns gerade gut genannt hast, im Seminar quasi mal das Verständnis schaffen und dann eben gern mit unserer Hilfe,

auch Hands-on-Hilfe, also wir tun ja nicht nur beraten, sondern bekrempelte Ärmel hoch, dann einfach diese ganzen Sachen glatt zu ziehen und das hatte immer was mit Prozessen zu tun, das hat immer was mit Dokumentation zu tun, aber es hat

00:13:31 Sprecher 2

explizit eben auch was mit den Produkten zu tun, weil wir wollen ja nachher nicht noch bessere Dokumentation haben, sondern bessere Produkte.

00:13:37 Sprecher 2

Herr Christian, 1000 Dank für diesen Überblick, weil das war jetzt wirklich ein Einblick in das, was gerade geschieht und das sind ja alles Informationen, die sonst so nicht zugänglich sind.

00:13:48 Sprecher 2

Also, ich glaube, die Warnung hat hoffentlich jeder verstanden.

00:13:51 Sprecher 2

Man schaut sehr genau drauf, was im Bereich I.

00:13:54 Sprecher 2

T.

00:13:55 Sprecher 2

Sicherheit passiert, aber keiner ist dabei alleine.

00:13:57 Sprecher 2

Christian, vielen herzlichen Dank.

00:13:59 Sprecher 2

Sehr gerne, danke.