Johner Institute

IT Security: Expectations of Notified Bodies

With Christian Rosenzweig, Prof. Dr. Christian Johner

Transcript

00:00:05 Speaker 1

Medical Device Insights, a podcast by the Jona Institute for medical device manufacturers, authorities and notified bodies.

00:00:18 Speaker 2

Sometimes notified bodies demand things more quickly, as we ourselves thought, and a sad example of this is the topic of IT security.

00:00:27 Speaker 2

And in this podcast we want to report,

00:00:30 Speaker 2

What we have observed, what is currently happening, what notified bodies are demanding from manufacturers, what we recommend, what manufacturers should do to ultimately avoid problems and yes, also the costs that are typically associated with this and the delay in all the approval procedures.

00:00:47 Speaker 2

And who more competent could I invite than my colleague, Christian Rosenzweig, who might say 23 words to Christian so that the listeners can classify you well.

00:00:57 Speaker 3

Yes, hello Christian.

00:00:58 Speaker 3

My name is Christian Rosenzweig.

00:01:00 Speaker 3

I have been a consultant at the Jona Institute for 4 years and advise medical device manufacturers mainly on the topics of risk management and risk management.

00:01:08 Speaker 3

T.

00:01:08 Speaker 3

Security.

00:01:08 Speaker 2

Yes, that means you are exactly the right person to contact.

00:01:11 Speaker 2

So, we have to admit that until recently we had assessed the situation a bit differently.

00:01:18 Speaker 2

Yes, we had a thesis about what notified bodies were specifically demanding.

00:01:22 Speaker 2

That was Christian, if you might repeat that again very briefly

00:01:26 Speaker 2

Before we come to reality, what did we think notified bodies in particular demand?

00:01:31 Speaker 3

Yes, exactly, if you deal with the topic I.

00:01:33 Speaker 3

T.

00:01:33 Speaker 3

Security, then you will find that this is a huge area with many, many activities, with many concepts that play a role.

00:01:42 Speaker 3

And we had actually thought that both the notified bodies with their respective auditors and the medical device manufacturers would first have to familiarize themselves with this topic.

00:01:50 Speaker 3

The M.

00:01:51 Speaker 3

D.

00:01:51 Speaker 3

R.

00:01:51 Speaker 3

has sued the subject area relatively quickly.

00:01:55 Speaker 3

And people had to follow suit accordingly with their own qualifications.

00:02:01 Speaker 3

I then spoke to a notified body and asked, what do you actually expect from the manufacturers at the beginning?

00:02:07 Speaker 3

They can't implement everything overnight.

00:02:10 Speaker 3

And then they said that two points were important to us.

00:02:14 Speaker 3

One is the qualification of the staff and the other is that a penetration test is carried out at the end of the development process to prove, so to speak, that the product really does

00:02:24 Speaker 3

Ausreichend I.

00:02:25 Speaker 3

T.

00:02:25 Speaker 3

and these are the framework conditions at the beginning and at the end of the development process, so to speak, they must be there in any case.

00:02:32 Speaker 3

And I've always passed that on to my manufacturers, to my customers, and then over time I saw that it's different after all.

00:02:39 Speaker 2

Yes, we have to talk about what is now being demanded.

00:02:43 Speaker 2

Maybe another question about this regulatory framework, because you can't demand anything there now.

00:02:49 Speaker 2

If we go through it very briefly, what do we have in terms of important

00:02:52 Speaker 2

regulatory requirements that manufacturers should be aware of and also comply with.

00:02:58 Speaker 3

Yes, that's exactly where the next problem comes from.

00:03:00 Speaker 3

The M.D.R.

00:03:01 Speaker 3

calls in Appendix 1 that information security must be taken into account in the product life cycle and does not elaborate much further.

00:03:10 Speaker 3

So you have to look for a source that is at least as authoritative as the M.D.R.

00:03:14 Speaker 3

and that's where the M.D.C.G.

00:03:16 Speaker 3

guidance document that at least provides an interpretation of the M.D.R.

00:03:19 Speaker 3

delivers.

00:03:20 Speaker 3

Now this guidance document has said a lot about IT security.

00:03:24 Speaker 3

That's the MDCG 2019/16, but unfortunately in a very abstract way and that often didn't help the manufacturers.

00:03:32 Speaker 3

And then they went on a search and found many, many different documents that can be considered state of the art.

00:03:40 Speaker 3

And that exacerbated the problem, because then no one knew exactly what the state of the art was, how I could define it for myself.

00:03:46 Speaker 2

Absolutely, and that was exactly the trigger that we said, we'll break it down to really binary-decidable checkpoints.

00:03:55 Speaker 2

And that's exactly how I.T.

00:03:56 Speaker 2

Safety guides were created, which the notified bodies then took over more or less directly.

00:04:02 Speaker 2

So, that means, we have a kind of binding part, so to speak, we have the M.D.R.

00:04:07 Speaker 2

as a not quite so helpful interpretation of the M.D.C.G.

00:04:12 Speaker 2

Document and

00:04:13 Speaker 2

in addition, the guideline, which is very concrete and very specific.

00:04:18 Speaker 2

Yes, now we have this framework, so to speak, and if you take a look now, what is actually being asked now, what are your experiences?

00:04:25 Speaker 3

Yes, I want to make that clear with an example, a manufacturer recently asked me because he got into problems in an audit with a notified body.

00:04:33 Speaker 3

So he had deviations in the I.T.

00:04:36 Speaker 3

Safety and that was an active medical device that was listed in the O.P.

00:04:39 Speaker 3

environment and he only had a U.S.B.

00:04:42 Speaker 3

interface, so it was a

00:04:43 Speaker 3

not a networked medical device, but simply a USB data interface.

00:04:48 Speaker 3

And he has argued that he does not need any IT security activities because he is only vulnerable to a limited extent.

00:04:56 Speaker 3

You just need physical access to this product.

00:04:58 Speaker 3

And that was his strategy, i.e. a risk-based approach.

00:05:01 Speaker 3

He also formulated it against the MDCG as a CAP analysis, i.e. against the MDCG document 2019/16 as a CAP analysis.

00:05:09 Speaker 3

and said that we don't need the activities listed there because we only have a USB interface and then the notified body said, no, that's not enough for us.

00:05:17 Speaker 3

Literally, she said that this is not an acceptable approach and then the manufacturer said, what do you have in mind instead and the notified body is not allowed to advise in such a case.

00:05:26 Speaker 3

That is, they have stuck to their statement that they simply do not accept it.

00:05:30 Speaker 3

Then the manufacturer tried to create other gap analyses against FDA guidance documents, for example, but it didn't work either

00:05:38 Speaker 3

And then he finally came to me and we looked together at how we could formulate the state of the art first and then looked at the standard to be harmonized, IEC 81001-5-1.

00:05:51 Speaker 3

This is precisely the one that the EU Commission has envisaged for harmonisation under the MDR.

00:05:56 Speaker 3

And then we said, we'll take them now and take the most important points out of them and try to map them, retrospectively, so to speak, the development process according to this standard

00:06:06 Speaker 3

to carry out and document.

00:06:08 Speaker 3

That's what we did.

00:06:09 Speaker 3

The notified body then said, great, that's the approach we would have imagined.

00:06:14 Speaker 3

And with that, we already knew that we were on the right track.

00:06:17 Speaker 3

But what happened then, and I think this is just as exciting, was that they weren't satisfied with that, but then went deeper in a further review step, brought in a technical expert themselves, who then took an even deeper look at the existing documentation that we had created after 81001.51.

00:06:36 Speaker 3

and in the process, they picked out things, such as that the system was provided with a password via user authentication, but the manufacturer did not implement anything that meant an expiration period of the password or that this would be sued by the user.

00:06:52 Speaker 3

And then the notified body argued that a password that does not have an expiration date is just as bad as no password at all and they do not accept that.

00:07:01 Speaker 3

And this actually shows that

00:07:03 Speaker 3

the notified bodies go deep into the fact that they not only have the general IT security life cycle process shown, but that they then also go into the content of the individual subject areas and question them.

00:07:15 Speaker 3

And this is a quality that we know from 62304, for example from the software life cycle process or from the risk management process according to ISO 14971.

00:07:24 Speaker 3

But I would not have expected that this detailed examination of the

00:07:30 Speaker 3

granularity.

00:07:31 Speaker 2

This is really surprising.

00:07:33 Speaker 2

On the one hand, of course, you can be happy if you approach it with competence, but on the other hand, of course, you always have to ask, is this still risk-based?

00:07:41 Speaker 2

So you said, we're talking about the USB interface here, i.e. the interface where you already sit directly on the device and the topic of password expiration is now not quite so simple that you can say that they always have to expire, because if you know how it works in the hospital.

00:07:58 Speaker 2

then it only increases the risk that they will write the password somewhere and thus reduce IT security afterwards.

00:08:04 Speaker 2

O.K., but that's the way things are now.

00:08:06 Speaker 2

So the competence is high, the level of detail obviously too.

00:08:12 Speaker 2

We can argue about how much risk management or risk-oriented this approach is.

00:08:17 Speaker 2

What would you recommend to the manufacturers now?

00:08:20 Speaker 2

So, what should they do now to avoid such unpleasant discussions as much as possible or at least shorten them?

00:08:28 Speaker 3

The path has actually already been specified by another notified body, which has written in a deviation report from another manufacturer, you don't have an I.

00:08:36 Speaker 3

T.

00:08:36 Speaker 3

Security documentation, what we would have expected at least would be the following and then they listed everything they would expect minimum and that is kindly exactly what we can now take as a guideline.

00:08:49 Speaker 3

And the good news is,

00:08:51 Speaker 3

This approach by the notified body, which it would have expected, is congruent with the IEC 8100151, namely exactly the standard that is due for harmonization under the MDR for IT security.

00:09:01 Speaker 3

In other words, how can the manufacturer prepare now by taking exactly this standard, reading through it, interpreting it and then implementing it accordingly in the quality management system and living by it.

00:09:12 Speaker 3

Perhaps one more point that is important: If I integrate this into my quality management system at time X and from now on I don't put any development into the products at the moment, then the question is: Do I have to work through my previous products that are already on the market after this process and maintain the technical documentation, so to speak?

00:09:31 Speaker 3

We know this under the term legacy devices, that you don't have products on the market under a standard, but now you have to meet this standard.

00:09:39 Speaker 3

And the 81151 also says very clearly how to deal with the case.

00:09:43 Speaker 3

There is an Appendix F that describes that the product has to be redeveloped.

00:09:49 Speaker 3

You have to name this software in the conversion, which also brings this software in the conversion to the level that is actually required or expected according to 81151.

00:09:59 Speaker 3

And the whole thing must also be provided with a risk assessment, which is supposed to prove that in the meantime, while this product is being redeveloped,

00:10:08 Speaker 3

can stay in the market with the product.

00:10:10 Speaker 2

Wow, of course these are extreme hurdles that are being set up.

00:10:13 Speaker 2

To a certain extent, one can certainly understand this, because many things are very, very rudimentary and stepmotherly regarding the I.

00:10:19 Speaker 2

T.

00:10:19 Speaker 2

security has been done so far.

00:10:21 Speaker 2

So in this respect, it is understandable that one takes a closer look at it.

00:10:25 Speaker 2

But right now, especially with the examples you have just mentioned, yes, one writes that to go very far.

00:10:29 Speaker 2

So that can shut down an entire company if you drill it through to the end.

00:10:34 Speaker 2

How can you help ensure that

00:10:37 Speaker 2

As a company, you can achieve IT security on the one hand, but you can‘t shut down the entire company and stop all the innovations that we also want.

00:10:45 Speaker 2

So we must not forget what the patients do and not just create documentation for well-known bodies.

00:10:51 Speaker 2

So, what would be your offers of support that you?

00:10:54 Speaker 2

to us.

00:10:55 Speaker 3

So you can clearly see what the expectations of the notified bodies are.

00:10:58 Speaker 3

I have just described it.

00:11:00 Speaker 3

And you can't get around it.

00:11:01 Speaker 3

That means it doesn't help to whine and discuss now, but you have to implement it.

00:11:05 Speaker 3

And that means that the first thing you have to do is deal with what the 8100151 actually demands of me?

00:11:11 Speaker 3

And for that I have to understand this norm.

00:11:13 Speaker 3

It takes time to read up on it, because these are very specific terms.

00:11:17 Speaker 3

You have to understand what threat modeling is, what is hidden behind it, what is

00:11:22 Speaker 3

Defense in Depth, what kind of concept is it and if you want to work on all this, then you need a lot of time in the company.

00:11:29 Speaker 3

You can save yourself this time, for example, by booking a seminar with us.

00:11:34 Speaker 3

I tried to really work through the whole topic, the whole 81151 including the whole background on IT security, in 2 days in a compressed way, I invested a lot of time in it and the manufacturers can now benefit from this, they can use it directly and

00:11:49 Speaker 3

to get their staff up to speed during the two days.

00:11:53 Speaker 3

This is the starting point, so to speak, to first qualify people, to enable them to implement the topic of IT security in their own company and then it is a matter of adapting the quality management system accordingly.

00:12:04 Speaker 3

We help, for example, with templates that we provide or through workshops in which we implement the adaptation of these templates to your own company.

00:12:12 Speaker 3

Then we also help operationally in day-to-day business, for example, when such threat modeling is done, which is a method to systematically

00:12:19 Speaker 3

To analyze IT security risks, you need a certain amount of experience to do that.

00:12:24 Speaker 3

And that's where we really help with hands-on workshops to moderate or carry out these risk analyses or, in case of doubt, to implement them in commissioned work, so that in the end a file can be created quickly.

00:12:37 Speaker 3

What is also very relevant is that at the end of the development process, certain I.

00:12:42 Speaker 3

T.

00:12:42 Speaker 3

Security tests can be done.

00:12:44 Speaker 3

As Jona Institute, we support this with vulnerability scanning or penetration tests.

00:12:49 Speaker 3

We also have appropriately qualified staff for this and these are roughly the individual activities with which we offer assistance.

00:12:56 Speaker 2

That's good and I can report, so especially if you now address the topic of penetration tests, we never had a case where we didn't come across serious gaps, although we all

00:13:06 Speaker 2

manufacturers were firmly convinced that this had not happened to him, but the probability seems to be very high to encounter gaps and I also found the stack that you just called us good, in the seminar to create the understanding and then with our help, also hands-on help, so we don't just advise, but rolled up my sleeves, then just smoothing out all these things and that always had something to do with processes, that always has something to do with documentation, but it has

00:13:31 Speaker 2

explicitly something to do with the products, because we don't want to have better documentation afterwards, but better products.

00:13:37 Speaker 2

Mr. Christian, 1000 thanks for this overview, because this was really an insight into what is happening right now and this is all information that is otherwise not accessible.

00:13:48 Speaker 2

So, I think hopefully everyone has understood the warning.

00:13:51 Speaker 2

You look very closely at what is happening in area I.

00:13:54 Speaker 2

T.

00:13:55 Speaker 2

Safety happens, but no one is alone.

00:13:57 Speaker 2

Christian, thank you very much.

00:13:59 Speaker 2

With pleasure, thank you.