00:00:00  
*Speaker 1:* Can you introduce yourself?

00:00:01  
*Speaker 2:* Yeah, my name is Michael. Um, I'm 32 years old. I have been working for it for. 8 to 10 years. Uh, both as a supporter and, uh, consultant. Well, in Denmark and in Poland. Uh, and for the last three years, I think I work with the security. Um, where I've been working with CMX solutions. Uh, if you know what it is. So CM is a way you put a lot of locks inside and you use make some use cases where you can search for things you want to know. It's like, who has been locked in here, who has been getting, uh, admin rights to not have and like that. And yeah, now I'm here.

00:00:53  
*Speaker 1:* How long have you been working at TMT?

00:00:55  
*Speaker 2:* One year and eight months.

00:00:58  
*Speaker 1:* It's just it's just a question of the record. Yeah. So how does CMT ensure the security and integrity of hospital infrastructure against evolving cyber threats?

00:01:10  
*Speaker 2:* We are doing a lot with firewalls and making sure that we only zoom up for things that need to be open for the internet. And the other things we do is to have antivirus, uh, endpoints and all know knowing said I have said to have endpoints on the device. We know that it's there. We know that something we don't have. But in the cortex, as we use antivirus, we have, uh, like also a platform where we can see incidents and alerts. So this is the where we see and try to find out if there's something having under. Yeah.

00:01:50  
*Speaker 1:* So what are the biggest cybersecurity challenge facing Danish hospitals and how does CMT mitigate these risks?

00:01:58  
*Speaker 2:* I would say one of the biggest things is that money, because you have a lot of old, uh, medical equipment that's running on Windows 7 and like that. And to buy something new, if there's something new you can buy, it will cost so much money you don't have. But there is. The way they try to to make it safe is with antivirus and we have a VPN. It's a secure network where we put some of the when we know we put the windows you and Windows 8 machine there because then we'd be more, uh, secure. I hope mine is okay.

00:02:41  
*Speaker 1:* Oh, yeah. It's fine. Yeah. So what security challenges arise when integrating new digital solutions into the hospital IT systems, and how can they be addressed? Since you mentioned there's a lot of old medical equipment, how is these Digitalization techniques can affect.

00:03:03  
*Speaker 2:* Things. The biggest issue is that when you have old equipment, you don't get any updates for them. More, uh, Windows Update or what else they're going to be. And also with antivirus, you have a not the newest version, but you maybe have a live version you could put on or something. And I think that's one of the biggest issue because you try to make it safe. But again, it will never be safe. I don't know, I hope it's will answer the question.

00:03:36  
*Speaker 1:* So basically, during the past five years, there's been a huge digital digitalization progress in Denmark, including the change from the namely the timidity. Can you comment something about that? How did it affect the health care sector that.

00:03:54  
*Speaker 2:* Um, I don't know. Uh, I have not had any things with media and media and do in the hospital. Um, but I think one of the things is, um, better when it is now you have, uh, on the app on your mobile. I know we also had the anonymity on the mobile, but with MDT, you need to scan the QR code. I think also it's in, uh, in company, it needs to do that. And of course of that it is more secure because you don't just send and say click. It's okay. Okay.

00:04:33  
*Speaker 1:* So how does digitalization in hospitals impact data security, particularly regarding the sensitive patient information such as CPR numbers?

00:04:50  
*Speaker 2:* It's a good question. Um. Yeah. You can say one of the things maybe. I'm not sure I will answer the question, but when you have a lot of more, uh, details system and you have the, um, the CPI number or something like that, uh, if you take in the old time when we have it in paper, um, maybe it will be easier to get it. But you can also saying that when we get more and more details, new system, we look more into the how safe is the system? Instead of just saying that, we just buy it because notes some time ago when you just buy the system, maybe did, sometime they don't think about to make it. Uh, what does it say to this? Um, encrypted. Encrypted. Yeah. So because of that, I will say it's kind of sometime more secure. But again, you also know there's a lot of coming out there that's not thinking somewhat about its see security in the end when they make supper.

00:06:01  
*Speaker 1:* So, for example, I work at the Chip and we collaborate with various hospitals across Denmark. How can CMT ensure that we are doing the integrity of the data correctly?

00:06:18  
*Speaker 2:* Um, again, I'm not I know a little bit about Chip, but one of the things I think's is that I will also maybe things. Do you use, uh, the S10 network? Um, you don't know?

00:06:34  
*Speaker 1:* I don't know, I'm just using the system.

00:06:36  
*Speaker 2:* Yeah. Okay. Yeah. There is, it's the network. It's, um, Sun Hills data network. Uh, it's a, um, network where it's connected to old hospital. Uh, and they upgraded to make it more secure. So I think. I don't know if Chip is, but I think everything's chip is also good this way. So because of that way, I will say it's make it is secure to do that. And again I'm not sure.

00:07:08  
*Speaker 1:* Can you detect in the emails if we for example right number or like enclose some sensitive patient data.

00:07:17  
*Speaker 2:* Uh I know, yeah I know, I know Janus is working with that. Oh.

00:07:23  
*Speaker 1:* So you can kind of see the threat and mitigate about it.

00:07:28  
*Speaker 2:* I have not seen the system, but I know that he can see if there's been what I know. What is that? Has been sent CPR number from office 365.

00:07:38  
*Speaker 1:* Okay. How does CMT collaborate with national and international cybersecurity agencies to protect hospital infrastructure against cyber threats?

00:07:49  
*Speaker 2:* Uh, I know we, uh, do it like that when, uh, What's it called, if that makes sense. Uh, when, uh. Yeah, when they ask, say something. We see this. You would need to think about that to do something about that. And no, we often do it because we take TikTok. It's been banned from all. You cannot do it. You use it on your computer or your mobile. Um, I also know that we have banned some AI from China, so we are doing that. Um, also we have, uh, I cannot remember the name, but there's something called missed. It's also something from the hospital to copyright for them. And they also said that is for country. Uh, think about to plot this country to access the region from outside. Inside. Yeah. And I know from the 40 country I think it's 39. We have blocked. So we are doing that.

00:08:51  
*Speaker 1:* Hmm. So what role does identity and access management play in securing hospitality environments, and what are the best practices for ensuring strong security controls?

00:09:04  
*Speaker 2:* Can I say it again?

00:09:06  
*Speaker 1:* Yes. So what role does identity and access management play in securing hostile IT environments? And what are the best practices for ensuring strong security controls?

00:09:18  
*Speaker 2:* Yeah. If you take asset management, one of the things that I will say is that when you have access management, uh, programs and talk made to it has been dog that's been a are some words I'm not good to saying. But when you have a lot of you know, what software or application you have on a computer's and has been you know, it is that and this has been documented in our, uh, ICM, uh, I CSM system. Um, you have easier to when you have a CD Reliability on a software when you know it's out there, it easier to to check in the s management system to see who has the software and to say, okay, you need to update it if possible or to if you have an OT license. You can also uh saying this all ability should be blocked on this.

00:10:17  
*Speaker 1:* Yeah.

00:10:19  
*Speaker 2:* And yeah.

00:10:20  
*Speaker 1:* Yeah.

00:10:20  
*Speaker 2:* Yeah. And about the other question with the efficiency, um, and also I'm also still learning a lot uh, with ISO security because it was in 21, I think I finished my PPA in that security, uh, and, and my last job, I was part time internal I.T responsible and all the time was ISO security. So it's still something for me. It's still. I need to learn.

00:10:51  
*Speaker 1:* Yeah. Of course. So basically our systems, they use the passwords and the username. How can hospital. I would say improving it.

00:11:02  
*Speaker 2:* Yeah I know we are doing it just like that. We uh multifactor uh, and sometimes it's a key you have on your phone. Uh, but I also know if somebody thinks to use their card to login, uh, on the mobile computers.

00:11:17  
*Speaker 1:* Really?

00:11:18  
*Speaker 2:* Yeah, I think some have. Oh, and they have a key, then password they need to test after I know that. Uh, I'm not sure anything to use it, but again, it depends on to saying multifactor where you can't. Not saying all system you can do it on. But again it's also much about how are you as a person do your things about what you're doing. When you see an email, do you just click on the link or uh, open it as a. So it's much more about, um, it's more about to also to make some good awareness companion to saying that. What do you do?

00:12:03  
*Speaker 1:* Does this EMT do this kind of trainings to.

00:12:06  
*Speaker 2:* I don't know.

00:12:10  
*Speaker 1:* The horse. How are the ransomware threats evolving in the health care sector, and what preventive strategies are most effective for Danish hospitals?

00:12:22  
*Speaker 2:* I know in, uh, other country, ransomware has been a big issue. Uh, on hospital. Uh, also things that was last year in was it in once hospital? I think there was ransomware, I think or maybe it also it goes in another company that the users suffer from. Um, but one of the things is, uh, enterprises that also look at, uh, what is being installed is, is this the a malware or something like that we do here. Um. One of the things that we could be better to do here is not to think that you can download what you want. Uh, but I also know they have, um, different kind of security layers. Some can install, some cannot install software. So they are doing something.

00:13:18  
*Speaker 1:* So for example, uh, Chip, as a medical organization, they banned usage of GPT, Grammarly and the different AI helpers. Can you comment on this? What what is the same statement about the AI and the threat to cybersecurity.

00:13:38  
*Speaker 2:* If I remember. Uh, Grammarly. Grammarly has been blocked. I think I can remember, yeah. Um. I think it's one of the biggest issue with AI is that there are so many of them. And one of them, some of them is good and some are not good. But again, what I also have heard is that you can cheat it and saying if the person I don't know, you can try to ask another way and another way and you maybe will get the answer to the end. Um, but I think this is the. Yeah, it's a good question because because it's still very new. Can we see? Um, but I think the best way to do this is to, um, try to see which one is best and which ones you blocked out of, maybe from, uh, agency saying that. Do this and do that thing. Uh, but yeah, it's a I don't know.

00:14:41  
*Speaker 1:* Okay, so does GMT consider the quantum computers a threat to the cyber warfare?

00:14:50  
*Speaker 2:* I don't know, really. Uh, but again, I think we all thinks about it because, um, this is also the reason why we talk about so much about multifactor, because they you cannot use the computer because you have access security. Um, but we know it's more easier to fake a password. And the ways I would say it have done something is that you you need to have certain words in your password. Um. But I think all, all, uh, companies things about the trade, about quantum computers, because, you know, when they're more they vault that will have things that be more try to create a password. But the other way you can say is this, that if you have a quantum computer, you still need to have the file with the password. And if you try to, if you do more about to saying that hacking tools, if they're blocked, they'll be more difficult to get it. I know there's some people that use the same password from, uh, another side, uh, website so they can get the password there. But again, this factor you cannot come in. So with that way I was saying we are doing something long question and a long answer, but I hope it was okay.

00:16:25  
*Speaker 1:* It was. It was good. Yeah. How does CMT balance the need for accessibility and usability with strong cybersecurity measures in hospital I.T. system?

00:16:46  
*Speaker 2:* Very good question. I hope I get this answer right. Just saying that. Well. But one of the things they're trying to do is when you have an example, they are hiring project leader to saying that now you need to work with, try to get some of the old servers closed down like Windows 7 2008 server. And when you do that, you're trying to improve your security level. Um, but again, hospitals have a lot of old system, so sometimes it's not possible. But again, now you need to have a, um, I need to search to, to get um, I don't know, the version things. Um.

00:17:35  
*Speaker 1:* So.

00:17:36  
*Speaker 2:* Yeah. Uh. This this person. Yeah. Do you know what it is?

00:17:45  
*Speaker 1:* This person.

00:17:47  
*Speaker 2:* Know you need to search and I need you need to apply for to to for one year that you will not do anything to that. Oh okay. Yeah I cannot. Oh okay. Yeah yeah yeah. Yeah. For you to get to to 30 to 1:00.

00:18:04  
*Speaker 1:* Yeah I have a have still to.

00:18:07  
*Speaker 2:* Yeah.

00:18:07  
*Speaker 1:* Of course. Yeah. So what future trends do you foresee in hospital cybersecurity. And how should I.T. infrastructure evolve to address emerging threats.

00:18:17  
*Speaker 2:* Uh, could use, uh, more. Uh, um, when you try to buy a new system, set more, uh, get something from an IT security architect to look through and saying, yeah, this is not good. It's not good. This is one of the things. And the other thing is to try to get more money to change old equipment. I've said that was the. Yeah, yeah, yeah. What's that? Yeah. Okay.