00:00:00  
*Speaker 1:* And then he's able to transcribe afterwards. Yeah. Okay, cool.

00:00:04  
*Speaker 2:* Can you please introduce yourself?

00:00:06  
*Speaker 1:* Yes. Um, my name is Daniel Wilkin. I'm a security specialist here at the Operational security in CMT and region. Region? Yeah. And I guess you would translate that to the to the capital region. Yeah. Yeah. Cool.

00:00:26  
*Speaker 2:* Yeah.

00:00:27  
*Speaker 1:* Any more or.

00:00:29  
*Speaker 2:* Uh, no. Uh, so how does CMT ensure the security and integrity of hospital IT infrastructure against evolving cyber threats?

00:00:39  
*Speaker 1:* Ah, well, that is the big question. Um, well, the problem with this cybersecurity field is that in a lot of ways, we are always behind because we can make this whole secure infrastructure and we can, um, you know, prepare as good as possible. But it's only when, when the very good hackers or evil minded people, they find a new way to actually attack or hurt infrastructure. Then we learn how to mitigate those threats, right? So we can do a lot of work on on building barriers and robustness and, um, creating multiple layers. So if they actually get through one layer, we have five more. And that's the whole kind of idea about it. Um, but but it is it is difficult to always ensure that that is, that it is secure. And especially with the development in AI technology, people find new, incredible, brilliant ways to manipulate and use AI for evil purposes. Um, so that's that's something that we are we're working fast to, to kind of secure this whole AI and keep us up to date and examine how, how can we actually defend And on on AI weapons, so to speak, if that makes sense. Yeah.

00:02:07  
*Speaker 2:* So what are the biggest cybersecurity challenges facing Danish hospitals, and how does your team mitigate these risks?

00:02:16  
*Speaker 1:* Um. Well, the biggest challenges we're facing, I'm not actually sure because we have a lot of, um, most attacks are the DDoS attacks. That's what we experienced mostly as what the the general people at different firms or companies experienced the most. And that's the same for us, but they are quite easy to mitigate if you have the right structure. And I think the biggest challenge is the the new unknown threats we see with AI technology. And the more destabilized, this international kind of cooperation between the world's nations becomes, the the more incentives are for other countries, such as Russia, to to try and hurt countries like Denmark further. And so I think the biggest challenge is that they are known for now with with AI technology and yeah and value chain is and that's also a big not a big problem. But that's that's where we have to be, you know, double check and be extra careful. Uh yeah. And what does it do? Um, well, we try to make as many of these, uh, risk based analysis analysis as possible to try and get into the mind of how if we were, if we wanted to attack the region, the capital, how would we do it or how which possible entries could we could we see? Um, and then we of course mitigate and remove and secure and defend. Um, and then we work very well with with other regions. We work with the European Union, with the Danish Ministry of Defense, and with many other entities, so we can secure this kind of multiple perspective on cybersecurity. Yeah.

00:04:21  
*Speaker 2:* Does seem to consider the risks of quantum computing.

00:04:27  
*Speaker 1:* Hmm. I guess we do. But we're not there yet, and we're kind of waiting for the quantum computer to actually be created and be, you know, functioning. Um, I guess it was was it the the CEO of Nvidia a couple of weeks ago who spoke out and said it will take 10 to 15 years before we're there? But of course, that is a that's a big topic. And when it becomes relevant we will work with that. But right now it's it's a too complicated technology for for evil minded or hacker hackers or Some other people to actually utilize quantum computers. Well, for now, a day will come, but we're not there yet.

00:05:12  
*Speaker 2:* How does digitalization in hospitals impact data security, particularly regarding the sensitive patient information such as CPR numbers?

00:05:22  
*Speaker 1:* Well, we are becoming. And if I don't, you know, completely answer the question. Just ask me again. Um, yeah. Well, um, digitalization at the hospitals, we are becoming more and more digitalized, and almost every machine we have are connected to the internet or in some ways, even fridges and light bulbs and whatnot. Um, but I say we have we have some procedures, we have some kind of, uh, standard procedures and a lot of optimizations that secure that, you know, person sensitive data like CPR numbers are very secure and often what is actually done in hospitals or different laboratories is that we connect something called an EDR number with the person's data. So you can't actually access the CPI number. You have to go through different kind of, um, methods to get the data. And it's all of the data's of course, encrypted. Right. Um, but we there have been in the past leaks of CPI numbers, and I can't say that it won't happen again in the future, but we're doing everything we can to, to make these secure procedures and. Yeah, and make sure that it's quite difficult for either for a person from the outside getting in and getting the data or from our colleagues making a human mistake. Uh, there are many layers of procedures that should. Yeah, you should make sure that that does not happen.

00:07:03  
*Speaker 2:* So how is the ransomware threats evolving in the health care sector, and what preventive strategies are most effective for Danish hospitals?

00:07:12  
*Speaker 1:* All right. So the so the problem with ransomware for the hackers is that it's it's more difficult to actually, um, carry out so to speak. Um it does attack. Can you make quite simply and quite cheap but a ransomware attack. It's it requires more um, can you say more intelligent piece of equipment and codes and. Yeah. So, so you have to be very good to actually execute these kind of or successfully get these kind of ransomware into our systems. And the, the second that if per se that we were to be attacked by a ransomware, the second that it opens up on the first computer or server, that machine would automatically be isolated, so it cannot spread to other machines. And then we just, you know, delete the whole and back it up. Sorry for my language, but the whole backup and restore procedures is actually what kind of protects us against that. So if by some miracle, someone should be good enough to get through and actually, you know, spread some kind of ransomware, we would just, you know, delete the whole thing and then get the backup and build it again. It's going to take some time, but it's it's a matter of days or weeks. And then we'll be up and running again. Um, because we are not or I cannot say that for sure, but my guess would be that if we were to be attacked by ransomware, we would not engage with the hackers or pay you the ransom or whatever. That's that's not an option. We just. Yeah.

00:08:49  
*Speaker 2:* How about with technology? With medical technology?

00:08:53  
*Speaker 1:* With medical? Well, the most or almost all medical technology runs on an application or a operation or the AOS, a, um, operative operative system we get, you call it. Um, I'm not sure that's the right word, but it runs on some kind of application or software or. Yeah. And we also we could just restore some of those. It depends on the kind of ransomware. But but that's why we have the whole backup and recovery system. Um, because we lock and backup everything. Um, so, so if let's, let's say a mirror scanner or something, uh, we could just, you know, we could put theory, delete the, the whole system, the whole application, the whole thing, and install it or back it up again with the same data and then just keep going.

00:09:53  
*Speaker 2:* What about the risk for the patient?

00:09:58  
*Speaker 1:* There would be some disturbance in the I don't know what's called an English accent. In Danish we call it drift. You know, the whole day to day kind of managing of the systems. There would be some delays in patients. In handling patients and making procedures and operations and all this. But I actually have no idea how big the impact would be. But I guess that, well, it depends on how many people are on a waiting list for using these kind of machines. Right? Because it would take us maybe a few days, maybe a few weeks to get them up and running again. So it would hopefully be the most crucial. Um, but then you can just relocate them to another hospital or maybe another region where there are five different regions in Denmark. Um, so if if the whole capital region is, yeah, is offline, then we will just send them down to the to the one at Zeeland, um, a couple of hours in car down south and then they should have, you know, nice and operating. Yeah.

00:11:06  
*Speaker 2:* So basically the regions are independent from one another.

00:11:09  
*Speaker 1:* We collaborate and we kind of spar with each other. Uh, and if you can call it that. But we do collaborate a lot, uh, and kind of reflect on how we do cyber security, but we are independent.

00:11:24  
*Speaker 2:* So what security challenges arise when integrating new digital solutions into the hospitals IT systems, and how can they be addressed? For example, a couple of years ago people were using the NMT. Yeah, but now people are using method.

00:11:38  
*Speaker 1:* Yeah. Yeah. But the whole point of, of going from uh, media to, to media is that media is way more secure. Um, but of course, anytime we introduce a new kind of technology or digitalization, it's going to take some time for people to get used to it. Uh, the biggest problem overall with cybersecurity are never the programs or the codes or the applications. It's people because people are sometimes sloppy or have or too busy to, you know, remember all the details or remember to doing all the small security stuff. Um, I don't know if it's answered the question, but it's when we will introduce new, uh, new technologies. We always try to build them as close as something that is familiar with the way of working, uh, for the people. So. Yeah. So we don't create this whole new kind of idea, this what I would call a critical juncture in a way. Yeah. Where you shake up the whole procedure or familiarity with how you work.

00:12:47  
*Speaker 2:* So how does UMT balance the need for accessibility and usability with strong cybersecurity measures in the hospital, IT systems with accessibility?

00:12:59  
*Speaker 1:* And what was the other usability? Um, well, we have a what we're working on is a lot of this, uh, what we call Pam privileged access management. Um, a lot of what we are doing now is making sure that the right people have the right access to the right programs, but that's it. So there's a lot of manual work making sure that I have the the rights and the needs and the access to the systems and the the documents and whatnot that I would need for my daily work. But I can I can't access any other stuff. Um, so it's a lot of kind of macro. Um. Yeah. Isolating or what you would call it. Um, because segmenting in Danish six. Segmenting it, I guess. Um, so making sure that the doctors and the nurses in the hospitals where they can only access specifically those systems, so they need to and none other stuff. Um, so they would have to kind of call us or the service desk or, um, And apply for access to any other documents and kind of maps, whatever it could be. Yeah, folders, programs, application systems and you name it.

00:14:21  
*Speaker 2:* So how does UMD collaborate with national and international cybersecurity agencies to protect hospital infrastructure against cyber threats?

00:14:30  
*Speaker 1:* Um, we have the center for Cybersecurity in Denmark, um, CFCs, which we call it. They are. They are kind of the wing under the Ministry of Defense. And then they are working. They have their own kind of entity within the the if the I would call it the intelligence defense, uh, agency, something like that. Um, so they are experts on cybersecurity and they kind of make analysis. A lot of the, the external threats that are towards Denmark and to watch different sectors. And um, so we collaborate a lot with them. So if at any time there is some kind of, um, new pop up in the whole picture of where the threat is, they will come and talk to us and, uh, kind of prepare us to, to do the right mitigations and look the right places. And then we collaborate a lot with the European Union. They have their agency called Enisa, uh, which is kind of their whole top department of cybersecurity, and they make a lot of reports and a lot of sector specific recommendations for how to ensure cyber security. So we, of course, are always up to date on where they are. And then we collaborate with them on how to kind of implement the the newest ways of doing cyber security. Um, and then of course, with the regions and the and, and other kind of, yeah, entities that do cyber security, but it's mostly the center for cyber Security and and the European Union.

00:16:17  
*Speaker 2:* So do you consider the cyber attack on the health care system as a terrorism?

00:16:23  
*Speaker 1:* Well, it depends on the motive. It really does depend on the motive, because if the whole purpose is to hurt us or kind of disturb our everyday work. Um. I'm not sure I would call that it is some kind of terrorism, but let's say it was a official Russian government doing these attacks. Then it's just cyber warfare. It's a declaration of war in some some kind. Generally, the threat of what we call cyberterrorism is actually quite low. And because often terrorism to be called terrorism should have either a religious purpose or a ideological political purpose. So the whole point of just hurting us, to hurt us or to to destabilise Denmark or something. That's. I would not call that motive enough for it to be terrorism. It would be cyber warfare instead. Uh, but the whole threat of cyber warfare is quite high. And the threat generally for cyber attacks is is extremely high. Um, but that's mostly due to the destabilized situation we have internationally with, with the Russian war going on and, and a lot of China. Yeah.

00:17:37  
*Speaker 2:* So what future trends do you foresee in hospital cybersecurity, and how should I.T. infrastructure evolve to address emerging threats?

00:17:46  
*Speaker 1:* Well, we are I have to say, yes. Cool. Um, I would say that what we do is that when we do cooperate with the center of the center for Cyber Security and, and the European Union is what we try to be as up to date as possible on how people are finding new ways to manipulate systems. um, and use systems to kind of hurt us. And then we run as fast as we can to to mitigate these kind of threats. Right. Uh, but I can foresee that, uh, working with and against what you could say AI, artificial intelligence is what we are in the next couple of years are going to be all about. And we are trying to integrate some new, new features in AI in our firewall systems, um, to better detect the use of AI and better mitigate. But AI is evolving extremely fast. Uh, so it's difficult for anyone actually to kind of keep up with it. But that's AI. That is one of the biggest threats. That's artificial intelligence. Um, so that's what we're kind of working towards, being up to date on what's possible and how to block it or mitigate it or avoid any use of it. Yeah. Cool. Yeah. It's that again.