00:00:00  
*Speaker 1:* So, uh, what are the biggest cybersecurity challenges currently faced by Denmark?

00:00:10  
*Speaker 2:* Um. So the biggest are ransomware. You know, ransomware. Um, yeah. Transformers. And yeah, I think this is the biggest one. And also there are another challenge is with the changes in the political changes in the world. So we are relying too much on tools from different countries, from other countries. And that's makes us a bit, um, facing some challenges maybe. So we need to be more independent. Yeah, but ransomware are super Very important. And. Yeah. And we need to consider that because SMEs in Denmark are being hit by different ransomware, the ransomware and different ransomware. So and most of the cases are of this type.

00:01:23  
*Speaker 1:* So you mentioned the political situation influences the Denmark cybersecurity. Can you specify how exactly, for example, it changed three years ago when the war in Europe broke out?

00:01:39  
*Speaker 2:* Yes. Yes of course. So the thing is that we are relying on cybersecurity and let's say IT infrastructure, right? So just if we imagine that we pay a stop supporting us, okay. For example, we can't get updates from antivirus or antivirus or security solutions. Okay, so our public infrastructure, our let's say everything here in Denmark will be at risk, right? And there are some challenges. For example, sometimes there are. Some state actors okay. What if those big states they want to do something okay. For example, they want to use their power to push Microsoft or those companies to do something. Okay. Nobody knows okay. So that's why we need to be worried. But in the past we used to have like a very good trust and relationship and connection with those companies. But now everything is being changed okay. And so the things with China and on Russia. So it means that we need to be on the tools and the solutions. We need to rely more on the EU based solutions because we can control them. We have a good relationship and, you know, as a country in Europe, right? But that's true for everything, right? For military, for everything. So the world is changing and we know that.

00:03:28  
*Speaker 1:* So how do you think that organizations in Denmark approach to cyber security compared to other countries?

00:03:38  
*Speaker 2:* Okay, that's a good question. So there are two things. There are some that say if they want to do, let's say to be secure of or if they want to be security, um, let's say how to it's about compliance, right? So it means that there are some rules that they want to fulfill. For example, they need to have an intrusion detection system. They need to have to be connected to this. They need to have a solution. But how they use the solution after getting the compliance the standard or something like that, after meeting them, it seems that they just go. And then they meet the requirements and at some point they don't use it. Okay. Because it's expensive in the matter of human resources. And so we know that many of these devices or solutions, they raise false positive. Right. False positive means that okay, something is wrong, but it is not right. And 99% or I don't know, 90% of the time that's the case 99%. And so it means that they must invest in just going and to meet some requirements. And the requirements says that you need to buy something. You need to have that solution. That's security approaches solutions. And then when they meet that they just it's getting normal for them. Okay. Just reverting back to the the thing before this is this is a very challenge. And um, and this this is so true, I guess because recently we have been working on some project, and we hope we can address this challenge in the future. Project.

00:05:46  
*Speaker 1:* What role does the Danish government play in protecting national cyber security?

00:05:53  
*Speaker 2:* I think it's They are presently. They have, uh, we are seeing some progress because for example, the in the projects in that are targeting collaboration between the universities, researchers and the industry, we can see that there are some grants defined specific to cybersecurity. And of course, the universities are just acting. For example, uh, Auburn University recently has announced with some labs and then they are considering cyber security as a factor and as a a priority, let's say. So the government is considering this. But again, uh, we need to invest more on the solutions. And Danish companies. I know that there are some Danish companies bringing some solutions on the table, Let's see how we need to equip these companies and SMEs and everything. Because sometimes these cybersecurity solutions are expensive, especially for SMEs that they have, I don't know, like 50 employees less than 50. Right. Because it's super expensive for them. They need to just some of them, they don't have money. They haven't arrived to the stages that they can make income okay. They have income. So yeah. And and I know that in Denmark we have many, many of those companies SMEs okay. So they should be targets. And of course the common and these uh, I know that the government has been, let's say covering the healthcare sector and they're, they're thinking of it to have like more secure infrastructure Share in the health care that I know of. They are doing great job now because this is the main concern. And in the Commons, the Commons are also reacting to the changes. They are just being equipped with security solutions. That's very nice.

00:08:13  
*Speaker 1:* How effective are Denmark cybersecurity regulations such as the network and information systems, the directive and protecting critical infrastructures.

00:08:26  
*Speaker 2:* Can you say that again?

00:08:28  
*Speaker 1:* So how are the Denmark cybersecurity regulations such as the network and information systems are efficient?

00:08:40  
*Speaker 2:* Okay, I'm not very into the regulation because that's another expertise. But as far as I know we do have some very well defined regulation. But as I said mentioned earlier, the companies meet those regulations and but it depends on how we monitor them to just keep meeting those regulations, you know. And because today it's super expensive to be like secure to stay secure.

00:09:18  
*Speaker 1:* How would you describe the current status of the health care sector? Is it secure enough, or are there any areas that you kind of can outline to kind of protect more?

00:09:32  
*Speaker 2:* I think in the health care, as I said. So they have started to just have some cybersecurity solutions, network security solutions. We call them MDR. And there are some companies doing it to to have like an umbrella over the whole health care sector. But the main issue in the health care is that sometimes they use legacy systems. So legacy system means that they are owned because it's expensive to develop new systems. Okay. From the ERP, from different systems that they use. And sometimes the systems are or have been developed by different companies, different developers. Okay. And because healthcare has a very long history of digitization or digitalization. Right. So it started from, I don't know, 20 or 30 years ago. Okay. But they have like many, many of those systems. And because they work and they are expensive, sometimes they're keeping it. They just work because they work. And so I think this is a very challenge there. But recently they have started to do, um, this, um, security security in the health care system. But the main threats towards the health care system is ransomware, because they used to just go, they just go and encrypt the data and they know that there is valuable data there. And of course, data breach is super important.

00:11:24  
*Speaker 1:* What do you think is the main target when the attacker wants to attack the healthcare system?

00:11:32  
*Speaker 2:* Okay. That's a good question. Mhm. When they want to attack the healthcare system. I think mainly uh mainly the, the most interesting part is the Communication between the patients and the healthcare. I think we used. We had a case that was not about an attack, but I think it was last week or the week before the last week. So the the phone number was blocked. Okay. Due to some communication issues like the, the operators, mobile operators and there were many people just it was super chaotic. Okay. But just imagine that. Yeah there is an attack and then they can just maybe we call it like interruption attack or DDoS attack or DDoS attack. Okay, denial of service. And then it means that we can just make the service out of reach of the legitimate or normal users. Just imagine what happens. That's that the impact will be huge. Okay. To the health. To the everyone. just thinks about the website. It could be about an Indian market. Everything is online. Okay, then you go just to a doctor, just getting something. Yeah a medicine. It's online and then you go to the pharmacy. So just imagine that system does work. You can't you can't get the medicine okay. And then yeah, it will be super chaotic. So the availability of services, especially the services that are in reach, will be able to be embraced by the patients to book or maybe to book a test or doctors or especially for the emergency cases. 1813 I guess that, yeah, that was the the phone number that was blocked. Yeah.

00:13:49  
*Speaker 1:* Do you know if it was a cyber attack and who was responsible for it.

00:13:54  
*Speaker 2:* I think that wasn't. I don't think that was a cyber attack because that was a network issue. Okay. At that time. Because sometimes it happens. And these systems are super complex just because they're like parallel lines. Okay. So managing them sometimes and then sometimes these operators, for example TDC or these operators, they try to update something operating and it messed up the things. But that shows the weaknesses. Right. That shows that the weakness is parts to us.

00:14:34  
*Speaker 1:* So what are the main cyber threats targeting the Danish companies and public institutions?

00:14:43  
*Speaker 2:* Okay. The main targets for the moment. I think again, it's ransomware. Because two weeks ago I had a guest from a company, a very consultancy companies, and that was my question from them. So because they were they used to do they are doing digital forensics means that the company just reached out to them. And then you have they go and just look at the the incidents. Right. So the thing was that the most thing, the most thing that has been reported by Danish companies is ransomware. And I think it's a killer ransomware. It's a specific ransomware that has like a very good spread and actually very bad. But yeah, I mean, yeah, this is, uh, it's a very sophisticated one. So most of the Danish companies have been hit with that one. And the fishing is super, uh, let's say popular among the apt groups because they start with the fishing. Right? Just sending you a link and then downloading some ransomware and other stuff. This is super critical these days.

00:16:12  
*Speaker 1:* So what are the biggest challenges in deploying the AI based security solutions in Denmarks industries?

00:16:21  
*Speaker 2:* Okay, so when it comes to AI based security solutions, um, there are two things. Actually, we don't have a very good AI based security solutions so far because the cyber security industry, the security field is super complex because it acts or its its interact with the users. The behavior of the users are different. Okay. So sometimes these cybersecurity companies, they use AI as a buzzword like just AI based solution. But in let's say behind the scenes is something similar to Manuel. Okay. Or maybe there are some scripts doing some automatic thing, but that's not intelligent. Okay. I think we are still far from those fully autonomous. We call it autonomous. Autonomous means that they can do something by themselves. Just detecting something and acting. Okay. And just, just maybe interpreting and acting. This is something that we call autonomous. And we are studying this here. But no companies so far can say that I have a very intelligent Security solutions. But as Denmark is in front line of digitalization, I believe that if there will be one in the future, I think they will have them. Like the Danish companies, they will have them. Because the good thing about Denmark or Danish industry then me or even Danes is that they easily embrace new technologies. Okay. That's why Denmark is very good at digitalization, right? So this is not apart from that. So if there is so good solutions, it will be in the market quickly in all companies in Denmark. And it's cheap. And if it is cheap it's not expensive.

00:18:39  
*Speaker 1:* So are Danish organizations adopting the adversarial machine learning defenses to protect the AI models from the cyber attacks.

00:18:50  
*Speaker 2:* Okay, that's a very good question. So in the adversarial machine learning, I think the company is they don't know what it is, right? Because when it comes to adverts, because the companies still are fighting against the traditional systems. Right. To embrace AI first. But their understanding of adversarial machine learning is not enough. Or if they don't know what it is at all. The reason is the reason that they need to maybe know more about it. There are many other companies, like AI based companies, that they just bring some solutions on the table. Okay. But nobody studies that. How robust Are those solutions, right? And then these companies, including Danish companies, they go and buy some solutions. For example, there is something and h r I don't know solution. They use AI for just doing something right. So filtering out the the parts, the applicants and blah blah blah. But they never study okay. So how for example it can be bypassed. Right. And then then they have no clue how the system is being trained. Okay. And training a model is super challenging. And we know that it requires a huge amount of GPUs or some good models. So it means money. It requires good talents, human resources, AI talents that are real. Okay, so it means money again. It requires lots of data and they require time. But sometimes these companies, they offer solutions. They just for example, in one month they bring up a solution. So that means that they haven't collected enough data or good data. They haven't trained the model enough. They haven't tested these models. So I think Danish companies still don't know about this as a threat because there are there are many other things. Okay. Apart from this, they need to understand before this because they are still fighting with the companies to understand the importance of cybersecurity. Okay. And then we can just discuss about this adversarial machine learning.

00:21:42  
*Speaker 1:* So how do you assess that the Danish business is prepared against the cyber threats such as ransomware and phishing?

00:21:53  
*Speaker 2:* I think actually this is not based on a study, but this is based on a feeling. I think we are not ready and we are not equipped, well-equipped, and we need to because still, um, cyber security, especially these cases, some threats, some common threads. Sometimes we think that this is for our next door. It's not for us. It's not threatening us. Okay. Until we get into that okay. And it's late. So I think, uh, yeah, we need to invest on this one again, the awareness of these companies and we are doing our best here as well, just to inviting people. Many people, especially the young people, the young generation, I think they do have a better understanding and they they feel it better. But the maybe the older generation, they think that's yeah, it's not the time to put money on that. Yeah.

00:23:10  
*Speaker 1:* So how is AI being integrated into the Denmark cybersecurity defense strategies?

00:23:21  
*Speaker 2:* Okay. That's another good question again. Uh, so I think. The AI let's say industry will step into many other industries. Right. And cyber security is one of them. And the AI can play an important role, of course, in cybersecurity as well. But it shouldn't just send a signal that it can replace its defense solutions. So the output of this, for example, it can be used in radar systems okay, to detect but to recognize the same type of flying stuff in the sky. Or it can be just scanning under the sea. What is going on there. And so these are the things that we can. The topics or the fields that we can enter by using our AI. Again, the main problem with the AI is when it comes to cybersecurity is false positives. And the main issue here is that It's not clear what is. It's. What is inside of it? Okay. That's because when we talk about deep learning and these machine learning things, they are always like a black box, right? And when it comes to okay, they say yes, no or there is an alert, but we don't know how they come up with that. That's why we have explainable AI right. So we mean that okay. We need to have AI models. When they say something they can explain it that we can see that okay, this based on these facts they decide they come up with this label. So if there is an attack somewhere and the system says that okay, there is an attack there. So based on what? Based on the fact we need to say that. Right. So this is how I can help cyber security. But I think it's not about only Danish. It's about it's helping globally. Yeah, okay. Because we can't expect just to have a progress or maybe an advancement in the or enhancement in Danish defense only with AI because it can impact the whole, the global ecosystem and then one can benefit from it as well.

00:26:17  
*Speaker 1:* So how do you see that AI is being used in the offensive strategies?

00:26:26  
*Speaker 2:* Oh, that's a good question. Another good question. So we call it red teaming right. So we have blue teaming and red teaming. And that's very unfortunate that That's this generative AI is an AI's. They can easily be because they do have APIs. Okay. And then you can easily connect the system. And then just imagine that an insider. So insider means that there is somebody somebody that is inside the company who is not happy or who is who has some monetary, let's say, purposes. Okay. So they can just have their system and they can have it connected to APIs from Gen A's, and then just let the system run some commands or install some tools and then try to scan the other, other systems, okay. By themselves okay. And then they are watching. Or maybe if they need to access to something they can help assist the agent. They are agent. That is super scary with the insider's. If we have the insider's, this eye is super scary. Yeah.

00:27:59  
*Speaker 1:* How is Denmark contributing to research and AI driven cybersecurity?

00:28:07  
*Speaker 2:* I think recently Denmark is doing well, right, in this, uh, research on, let's say, the intersection of AI and cyber security. So and we can see that there is a shift in the the grants and everything like the funding. So it it means that there is a priority for them. And they see that this is an important field to invest in the field. And I think that that's a correct way of. But I think we need to have more, maybe involving more companies to invest in, maybe larger companies. I know that Novo Nordisk has some funding, but it's they're not addressing cybersecurity directly. Okay. But Austin or other big names, they could be just having some funds aside for this cybersecurity and AI.

00:29:15  
*Speaker 1:* What are the opportunities for a collaboration between academia, industry and government in Denmark to improve the cybersecurity?

00:29:26  
*Speaker 2:* Okay, I think academia can play a great role in increasing the awareness at first step. For example, we can have events we can have some, let's say, uh, festivals or something like that. Okay. To tell the people like to shout that this is important. Okay. And there must be some, let's say, facilities to do this. Okay. Like some budgets or something like that. And for example, some bonus to the employees of those companies. They can just attend these types of events. Okay. And then because I think there must be an organized way of, um, communicating recent and real time alerts, real time threats. Okay. We should be faster at communication. For example, if yesterday there has been an attack You know, in on the water sector. Okay. So it must be there must be a channel or something like that just to go to just spread the news maybe, I don't know, there must be a TV show on the TV too, or we are, I don't know, for 20 minutes or 30 minutes. Does this updating everyone okay about the things because that should goes into the culture okay. So the government should invest in this one and this this can be done by universities, not by other entities because university don't follow any monetary or any money. Right. Or this they're just doing it for non profit okay. And the other thing is that the industry is maybe there must be some projects That requires three partners one university, one industry, one partner and one government partner. And those could maybe be most projects. And again regulation because government is is not building a solution. They just regulate the solutions. Right. But they need to know how to regulate. Okay. And for knowing that they need to collaborate with industry or partners, maybe in a consortium or something. And the universities. Right. So they need to collaborate and agree on some metrics for just a regulation and to enable some Danish companies to be able to deliver some solutions to these SMEs, like Danish made solutions to these SMEs. So the government should also invest Just more because I know that there are many other startups, but the initial startups, they they reach to a certain point, but they are not able to grow more in their cybersecurity. But so they need to sell themselves like they could be acquired by other companies, and they can't extend their market to other countries in the EU. So there must be, let's say, targeting other countries as well. Maybe something or maybe in the in the Nordic region, the government. Nothing prevents us to have like a consortium between Denmark, Sweden and Norway is having to get together to have like a common solution for many of these challenges. Right.

00:33:29  
*Speaker 1:* How do you implore on the right digital solutions such as method. Is there any risk that AI driven solutions can bridge the gap?

00:33:44  
*Speaker 2:* There is a big risk and need. Let's be. Everyone knows what if they don't work? It doesn't work. Yeah. So. And the risk is that I think it's not a solution. Um, I would say that's developed by government, by an official and the entity is by companies. It's by private sector. Okay. I think a company in France is doing some development is maintaining. So there is always a risk. But about the AI things. It depends on how we, um, let's say see that, for example, just if we have a malware on a mobile phone, okay, maybe they are able to open the browser and doing something and then just hit the button and just go to let's say Italy, and then just hit the those pin and just lock on. Okay. But I think you're not in that step because it involves multifactor authentication okay. And it's 2 or 3 sometimes actors okay. So you should go to the website. You should know the ID right. And then you hit the ID and then it goes through and just hit a QR code. And then there is a Pin code later. So these are the. So so far we have this multifactor. But again sometimes. Because in the older versions there used to be some SMS based authentication. Right. It's easy to bypass the SMS versions and authentication by taking over the I piece. Right. So it's easy. But in this one because it's internet based. But um, yeah, this is, this is the and I remember that in the we had a problem that we, we used to receive some notifications okay. When there was a request and by accident you could accept that notification. But now we need to add we don't have any notification. So I don't think for the moment I can really impacted. Okay. The only concern is interruption attacks and DDoS attacks against this. But nobody knows about the future.

00:36:48  
*Speaker 1:* What trends in cybercrime should Denmark be most concerned about in the coming years?

00:36:58  
*Speaker 2:* Okay. I think, um, threats against critical infrastructure, especially water system and energy grids, these are super, super important and they are building the whole society. Okay. Just based on this. So there has been some reports about the attacks on Florida water systems Guess what? Their systems just imagine that they can just change and manipulate the substances being added to this water treatment system. So that's threatening the lives, right? And the energy grid is also super important. Just imagine that the metro is out of energy, right out of power. So I think these two are super important for Denmark. The other thing is the health care system. We discussed that, but I think it has less priority than this critical infrastructure. And the other threats that I can imagine is. Yeah. And the issue with the, the C, the, the cables on the scene, that that's another issue that we need to cover. And the other thing that maybe is super important is the emergence of quantum computing that we need to be aware of. Just imagine that we I think maybe in the sea, under the sea they are doing something. Yeah. But just imagine they collect these data, huge amounts of data. Of course those are encrypted. They cannot open it. But after ten years they will open it. So they can just get access to many of the sensitive information. Yeah, probably. So this is another issue that we need to be concerned.

00:39:13  
*Speaker 1:* So you mentioned a lot the water infrastructure the energy infrastructure. Do you have any experience of fencing the attack or experience maybe witnessing one.

00:39:30  
*Speaker 2:* Not in Denmark as some cases in the US about these water systems. Okay, but not here in Denmark. But I know that recently there has been a report by the center for Cyber Security about the water system. So it's getting attractive by attracted by those apts or apts to impact. And this is because of the Danish style of water managing water system, because there are many villages, there are many of those. And they have like very community small communities, like for like just managing this, the water in that village. Okay. And sometimes they use like old style or system traditional systems. And this is challenging and I think they are addressing this 1 in 1 of the reports, but I haven't seen any anyhow because sometimes they don't publish it so we can't see them, so we can just see them on the news or something, or maybe even within our networks. But yeah.

00:40:52  
*Speaker 1:* So would you say that Denmark is very dependable on the resources or what will be the or, say, the emergency act in case the Denmark will not have access to the power?

00:41:08  
*Speaker 2:* Okay. I think we should have backups. Yes. And everyone should know that the what to do in this case. I can't remember if I have been Your pulse is knowledge. Before I haven't seen that on the TVs as well. So what to do if the mobile phones are off? Okay. There is like electricity outage, so I think I don't have any clue now. But again, if there is some some of these interruptions, there will be super chaotic. Let's imagine that when we go to like this traffic lights, if it doesn't work on an intersection, there will be a chaotic situation, right? Nobody knows where to go. Okay. So there must be some awareness in these fields. Yeah, but they don't have any now.

00:42:28  
*Speaker 1:* Yep.