00:00:00  
*Speaker 1:* Of course.

00:00:03  
*Speaker 2:* Yeah. So no worries. So, if you don't mind. Can you please tell me about yourself? So I read a little bit about you on LinkedIn, but I'm not sure.

00:00:17  
*Speaker 1:* Yeah, sure. Um, my name is Arnell. I work here at Houston at CMC. IMT. Uh, so the center for IT and tech technology. Medical technology. So I'm not usually saying the name of the workplace in English, but, uh, but yeah, I can. Yeah, but anyways, I'm working here with a team, uh, in, in a team where we detect and respond to, um, to incidents that may occur on our endpoints. And by endpoints, I mean my, our servers and our, uh, workstations, these, uh, client computers that people are using for normal work to work day to day basis. And essentially I'm working in the security platform. We get real time alerts. We have monitoring on all of our systems, uh, to observe whether or not something, uh, suspicious is going on in the machines and servers. And based on that, um, uh, conduct and deduct. Uh, the best solution or response to a given situation. Um, I we are approximately maybe like ten, you know, a team. Um, we are more in total, but we have another team who is looking at at the more the, um, how should I say the, uh, the proactive side of it while we are at the, uh, we detect and we respond. Well, they, um, the other team is conducting, um, mitigations or, like I should say, strategies. So, uh, we don't have to go into the, uh, response part, the detection part, but to make sure that the perimeter is more safe. Um, but, yeah, so we around ten in our team, and, uh, usually we, uh, uh, we look through a lot of data, uh, logs, uh, to determine, determine, um, at the scope of a given, uh, incident or case. And based on that, we use some procedures that are, um, very, uh, I should say well known or well established within incident response, uh, where we, um. Yeah. Well, we identify, um, a particular issue. We then scope the issue of the scope of engagement by looking into, um, uh, something called indicators of compromise. Um, and based on that, we kind of like, figure out the, the scope of a given incident and try to contain the incident. Uh, so. So if an incident is arising that we kind of, like, try to stop it there and not let it just spread out to, say, other computers and whatnot. Um, so yeah, there's a whole lot of process. So that's what we're working with here. Um, yeah. That's the basic something, I guess. Yeah.

00:03:22  
*Speaker 2:* So how does this EMT ensures the security and integrity of hospital I.T infrastructures? So as far as I know from your profile that you work with Azure based solutions. So can you comment about that? So how secure are the systems.

00:03:42  
*Speaker 1:* Well, um, yes. Uh, on my profile I have a, I have some Azure certified certifications and some experience within that though that is not my, um, current role. We have another team dedicated to the cloud part. And in terms of that cloud security, if you talk about that, we have that other team was trying to talk about, um, they are responsible for something called Prisma Cloud, which is like a solution where it kind of how should I say, um, uh, monitors, uh, policy violations in cloud incidents. So while we have a cloud department with their own tenant, we are providing solutions in which, where, um, applications, whether developed, uh, get scanned, um, through throughout the whole developing lifecycle, uh, with a shift left kind of strategy where, um, code is being scanned, uh, for vulnerabilities before they get into production. And this is all an automated process, which we have, uh, as a cloud solutions for that, um, cloud posture management. It's a system I believe it's called. If I'm not mistaken. Um, but yeah. So in that department, we have that. Um, so what was the question? How secure we are or how do we. Yeah. So we try our best, obviously. Um, we have, um, many, many I can't really comment on how many specific like endpoints we have, but we have in the many of thousands. And, um, thus we try our best to, to find all active, um, endpoints or hosts that are on the internet. And we deploy, um, our agent, uh, so this agent allows us to get the, the monitoring in real time on all of our, um, endpoints that are on the internet. And with this, we can deploy prevention policies, um, of, uh, search behavior. And we define rules and can manage what is allowed and not allowed on a system to, uh, to do um, with that said, uh, so yeah, we ensure that all of our assets have, um, a agent on them so we can actually see what's going on. We create our own custom alerts and rules based on the threat landscape and what is going on in the world. We are in the health care sector, so it is classified as critical infrastructure. And this these kind of branches of, uh, of businesses like, uh, where a lot of threat actors or bad actors are looking to target either due to. Yeah, it's due to money. Let's be honest here, a lot of them is like motivation and based on money, but sometimes it's also based on something political. Maybe we're not in good terms with, say, Russia or China. Um, so we are also alerted from that. So there's a lot of prevention we're doing in terms of also of the suppliers that we have. So, uh, it's no, um, it's no secret that we are very skeptic from everything that is rushing or China related, uh, due to the geopolitical atmosphere and also from, based on like our own, um, I should say, experience with say, uh, the Chinese, um, developed, uh, I, uh, just like OpenAI, you have a deep seek, uh, from China. And, uh, we have actually as one of the, one of the first companies in Denmark, actually went ahead and blocked this usage of this app because it was discovered that, um, data was being sent to China. And the way that it works in China very briefly is that if you have a business operating there, then the Chinese, um, I should say, um, government have a, um, a right to see all the data that they have in this company if you want to be protected by the government. So and we are afraid of that because, you know, especially in the health care, we're working with people who are PhD students who do research and all this. Uh, if these essentially, uh, business secrets are getting in the hands of our competitors, then that would be not good. So, um, we're very cautious in what software is being used, systems and suppliers, in terms of that part of security. And as I said, we, um, we try best to deploy these, uh, agents, uh, XDR agents is called extended uh, detection and response agents, uh, which essentially, uh, it's called extended because it collects both logs from our firewalls, the system behavior, the user context. So their behavior and whether or not it goes against the baseline of the the user in question. And with all this information, um, uh, we take them collectively and holistically, look into, uh, whether or not there's something actually going on that is malicious or if it's a false positive. So it's also a lot about figuring out the environment of the organization. And we are a big organization with a lot of the people who are doing custom code and stuff like that due to automation, um, that doctors might use some automation to for their file structures and such, uh, which sometimes comes out as being like, oh, something malicious happening because there's an automated program doing this, but then we clear it up as case by case basis. And with that, with the, uh, with learning the organization better and our infrastructure better, uh, we're able to fine tune our security products. So in our portal, we'll get we will reduce the number of false positives over time. Yes. And we obviously try best to, um, to deploy the latest, uh, updates for all of our systems, though. Um, it is um, we do also have to acknowledge the the fact here is that, uh, we work in health care, meaning there are a lot of scanners out there in the hospitals that might only work with a certain, uh, I should say, operating system that is considered legacy. And for those we have other mitigations when it comes to the access to these machines and the reason why we just don't go ahead and say, hey, let's just, uh, you know, uh, get a new server or whatever. Uh, for this specific case, uh, it's a question about money. It costs a lot of money, and sometimes it's very critical machines or applicators being used. Uh, that can mean the cost of life and death, which is why, you know, sometimes going with best practices, what we strive for. But realistically, practically speaking, um, security is a much more about processes and people. Right. And in the health care, our primary concern is obviously, uh, life. Right. So, um, but we are trying our very best to get everything shifted to the latest, um, uh, at least updates. And if that's not possible, we do other mitigation strategies to ensure that we make everything as safe as possible. Yeah.

00:11:22  
*Speaker 2:* So what are the biggest cyber security threats facing Danish hospitals, and how does CMT make it mitigate those risks?

00:11:32  
*Speaker 1:* The biggest risk that we have experienced or sorry can you say so.

00:11:38  
*Speaker 2:* So basically which kind of like cybersecurity risks have you experienced and what are the biggest threats like for the Danish hospitals in general?

00:11:47  
*Speaker 1:* Yeah. Uh, well, um, the thing is, um, uh, through our multiple reports of these annual reports that are coming out in terms of the threat Intel out in the big cyber space, uh, social engineering, um, is a technique that is predominantly, like the most used vector used by these, uh, threat actors externally, which consists of the good old phishing emails, whatever SMS phishing, which is acid, the primary, um, vector that is being used by these bad actors, uh, in terms of initial access to get into a system. Now, um, it's not something that we are getting targeted by, but we have, uh, also email solutions to filter out these kind of a of emails. So we don't have a big problem with it, though it's still very commonly used because it's very easy to automate, uh, but to just uh, uh, mass distribute, uh, uh, what's it called? A if a legitimately looking mail, especially if you make an AI today with the use of AI and generative AI. Uh, it's much easier now for the adversary to be able to make an AI that, say, go into as you did, go into LinkedIn, find information of a person. What do they like? What do they post, what do they talk about? And then in that essence, make a craft a better looking fish email, uh, hopefully to get someone to click on their on their links. Um, so that's a very common, uh, that we're seeing. Um, but the most are tremendous. I will say in terms of organization, that's something I've personally experienced, but I know we've had a ransomware, uh, incident before I started working here back in 2000. 17, I believe by 18. Not sure. And, um, these are very destructive because essentially just renders, uh, the effect systems useless by encrypting all data on the computer, uh, making them. Yeah, just use useless and, uh, and a lot of the times is demanding for you to pay a ransom, given the name of the ransomware. Uh, in terms of money, uh, obviously this is not something no one should or a victim should, you know, comply to do, uh, which is why for ransomware, it's very destructive. Uh, which the only real mitigation for these kind of, uh, extortion techniques is, uh, a recovery. So having a good backup plan, um, the corresponding to these systems criticality and and and how important it is. How much risk appetite do you have for a given system? Um, and how fast can you recover? So all these things also take into consideration in the, in our tactical, uh, plan of defense against these kind of attacks. Um, yeah. But but yeah, I recall there was something in 2017, 18. The ones that I've experienced is something that is much less detrimental. It was, uh, DDoS attacks against our website. It's probably going to be available in the news, by the way, this one I'm talking about, um, where our website, regulation h.dk, uh, got down. I don't recall how long I think it was an hour or something like that, if I'm not mistaken, which was committed by a, uh, it was said to be a Ukrainian based. um, how should I say, uh, hacker group. But it's also suspected that was Russian bad actors who were. Yeah, essentially proxying their IP. So it looked like it was another group because, yeah, we don't, at least from what I know geopolitically, don't have any issues with Ukraine. And I think it's the opposite. And, uh, yeah. And this particular group, it was called No Name. Uh, No Name, No Name zero 57 uh, 5057, I believe. Um, who at the time also conducted these does denial of service attacks, uh, against both the Copenhagen um, airport website, our website. Reagan who dot Dick and something called cold traffic. Uh, which is like those people who regulate from my knowledge. Uh, the, uh, the laws regarding, you know, um, safety on the cars and like, ah, yeah, driving laws and all these kind of things. Um, and nothing major happened, really, is just an overflow of influx of, um, what we call the incoming requests for this or a web service that are, of course, exposed online. And they take them down because they overload the website and, uh, yeah, but we got up real quickly and it's like a, like a little hit to the, to the head, nothing major because it's nothing critical. That is, you know, it's annoying, but nothing major. But what was really interesting by looking at this was the time frame of which had happened. It happened, I think, in the course, I believe it was 3 or 4 days. Uh, all these websites, these three websites, at least the big ones were targeted by the same group who took responsibility. And even though it was major, uh, or hit some services that were major. It is interesting to know that they targeted specifically the airport website, the health care website, and the yeah, the traffic thing website, all of which you can if you want to, uh, could, could categorize as being like critical infrastructure. So that was pretty interesting to see. But that said nothing. That was so, uh, major in terms of any disruptions, disruption at the hospitals. Yes.

00:18:02  
*Speaker 2:* So since we're touching the topic of Russia and Ukraine, how would you comment? The amount of cyber attacks that started happening happened before the war started?

00:18:17  
*Speaker 1:* Well, um, from what I know, we have always, uh, we have an internal, like list of IP, um, like countries where banning, um, uh, from entry to our systems. Though this is a medication, it's not, um, fault proof like. Like it is a good thing to do. But, you know, given how IP addresses work and VPNs and all this, um, it's easy for an adversary to disguise their traffic as coming or originating from somewhere else, but it does help at least clean up. Um, the amount of script kiddies that we call them, uh, that, uh, use automated tools that are just, you know, online available and just, you know, try to hit us. And most all of them are just getting blocked immediately by the geo blocking policies that we have in place. Uh, I believe actually, I don't really recall the exact number, but just, you know, by making these geo blocking, um, what's it called? Uh, yeah. Geo blocking by countries, uh, it actually reduced the amount of network scanning and attacks network based attacks from these countries by 70% or something like that. So it did a very big impact by, uh, switching this in the outer perimeter of a security defense system, which is our firewall, obviously. So, uh, so, yeah. Um, so you can kind of like, look at our security in the whole as being like a defensive. It's called defense in depth, uh, strategy, where we, uh, apply, uh, different layers of security. So from the firewall perspective, if you get an entry there, then, you know, you have the whole, um, what systems can actually interact with each other, the segmentation of network, how what which networks can communicate with each other? Um, uh, the device of a user, the and the actual fact that we have a client on these computers. So if there is a path of entry in some kind of a way a capacity, we have As they deploy these agents that will be able to detect the tool force. So there's yeah multiple layers in that sense. Mhm.

00:20:34  
*Speaker 2:* So how does CMT balance the need for accessibility and usability with a strong cybersecurity measures in hospital IT systems.

00:20:46  
*Speaker 1:* Yeah it's a it's a it's an ongoing process by talking to the people who actually use these systems. Um I should say these systems we have an internal flow um, in which there is a we, we have an internal flow that, um, where people from, say, hospitals can create something called a demand. And the mat essentially is a when you have a wish for a program or another system or, or you want to buy a new, I don't know, uh, router or anything, it goes through this demand process in which we have a, another department which qualifies the information that are given to these demands, and where they will go through a security check by us, and a compliance check by the compliance people. Whether or not to say, uh, you know, GDPR is, uh, being, uh, upheld. While we look at the technical specs, is it securely like, does it, does it have an end of support or anything this system or whatever they want, is there an alternative? Do we already have something existing that can be used instead of this new system or anything. It might be. So that's how we qualify the demands of wishes from the hospitals to evaluate whether or not they're secure or if we have anything that that can be used instead. So yeah, and all of this is obviously audited. So we can have, um, a cmdb or a configuration management system, a database, uh, to essentially make sure that everything is being documented, audited so we can retrace back and see what was done, why was something denied, what was something accepted and who did it, and etc.. Yeah.

00:22:29  
*Speaker 2:* So how does CMT collaborate with national and international cybersecurity agencies to protect hospital infrastructure against the cyber threats?

00:22:41  
*Speaker 1:* Yeah. Well, um, I can say that we, um, we obviously have our own security vendors, uh, in which they themselves have these events going on to their customers where we all like, you know, hear the latest about the news of this security and security around the world, and also some new updates for the systems to always be updated on what's going on. Um, we do also have a thread sharing, um, platform in which, um, different regions, especially in Denmark, um, like we, we're in region. Um, uh, I like to say the capital region of, uh. Yeah. Then you have the other regions in Denmark where we have this, um, uh, thread sharing platform where if one of the regions experienced something that is an actual threat, they can submit. I mean, we do submit our findings and report them into this platform so everyone can be, uh, yeah, be acknowledged about what's going on, especially if it's something we can see that has been targeted against us, because then if it's targeted against us and our hospitals most likely will be, uh, on other hospitals as well. So this is how we kind of communicate, uh, to all the other IT professionals. Um, yeah. And we also have a lot of threat, uh, Intel that we are getting from numerous, um, uh, government. Government. Um, uh, what's it called? Um, organizations that delve into the security research. Who have their own security researchers. And we have our own as well. Uh, from our security vendor, uh, which are people who are, like, constantly like looking into what's going on and update as they go with a new vulnerability or something to new tactics or techniques that are being used by actors in the world. So in this way, it's a very community kind of based knowledge sharing. Uh, what we do, uh, in terms of collaboration.

00:24:53  
*Speaker 2:* Okay. So what are the key considerations when ensuring compliance with the GDPR and other data protection regulations in data in hospital digitalization effort?

00:25:08  
*Speaker 1:* Yeah. Well, this is obviously that my, uh, department specifically, but we do have tools in which we, um, configure policies that will detect, um, certain data patterns, uh, that can be considered, say, CPI or Social security numbers. Denmark. So, um, but obviously, uh, straight out of the box, I will say that, um, it's something that is continuously like being developed because as I said, like in technology, there's a lot of false positives where some data, uh, patterns can look like other things. So maybe a Danish, uh, CPR number will look like that of a Taiwanese, uh, license plate or something. And then you have these a lot of these false positives. So, um, it's an ongoing process. And we have tools that will detect, um, uh, emails being sent, uh, for example, if they're being sent by external to externally out of the company, if it has matches of certain conditions that we prescribe, Uh, we are able to see that and actually then confront the people who have sent these things and, and hear, uh, what they've done or why they've done or even go ahead and block them. But, um, these are all pillars we do have. I can't obviously go into specifically how we do it. Uh, but we are looking for data patterns, and we do tested regularly. Regularly. They're regular. Yeah. You know, and, um, based on this, we, uh, can make internal cases in which another department will see whether or not it is a question of reporting into something called data signal. I don't know if the English, um, the it's in Denmark. We have a regulation where if you have a data leakage, leakage, you have to report within 72 hours to data to signal. And, uh, this is something another department, not us, Uh, uh, have, uh, have the responsibility to do it to ensure it will be done if we are having a data leakage. Um, and yeah, in terms of the protection of the actual information, uh, we do data patterns. And based on that, we can figure out whether or not there is an actual some exfiltration of data going somewhere. And we have internal, um, I should have say, um, private, uh, folders that are specifically designed to either self delete or, uh, specific folders that are restricted to people who, uh, in a, in a need to know basis, but not in a nice no basis need to access patient journals and, and, and those kind of things in terms of if they have like a working related, um, cause to why they're doing what they're doing. Yes.

00:28:11  
*Speaker 2:* So you mentioned the CPI numbers. So how does digitalization in hospitals impact data security, particularly regarding sensitive patient information such as CPI numbers?

00:28:27  
*Speaker 1:* Um, yeah. Well, the systems that are, um, working with, uh, patient data or something that is sensitive are usually, uh, very restricted to certain accounts or computers or networks. So it's all depending on what the actual need is for the, um, the application in question. So, and where the data actually is going to be resided. So sometimes if it's very sensitive data, there is no solution that is secure, say from a network point of view. Then sometimes it's a matter of like having data being preserved on a local disk or something. That is not when you're not able to intercept or any of that kind of means if there isn't any solution to do this. We do also, however, uh, have um, uh, doctors or researchers who need to collaborate outside of Denmark with other uh, uh, hospitals or universities. And for this, we do have, uh, a solution where data can be sent, whatever data can be sent, um, in a secure manner, um, where the recipients of, uh, of this email will, uh, have, um, uh, let's say a temporary access to, um, uh, yeah, a package, if you will, is called, uh, to retrieve the data they need and the conditions in terms of, uh, the data criticality of it, if the if it's severe data, then we have to comply with having a I don't know what the English word is, but data be allow time, which essentially is, uh, agreement behind the sender and the, um, the recipient where the center is the data responsible, I guess, and the ones who are kind of processing this data have another set of contractual agreements that are getting that that they have in place before sending the actual data. Right? So you can just send it out to anywhere. Yeah. So you have to have a written contract, um, uh, that aligns these things, uh, in order to be able to first off utilize our platforms to send data and secondly, who you send it to. So, yeah, I hope that answered your question.

00:30:54  
*Speaker 2:* So how do you think that the general general cyber warfare affected the cybersecurity of hospitals? So how does the health care system is affected by the cyber warfare.

00:31:13  
*Speaker 1:* Well, um, I think it's, uh, it goes beyond saying that, uh, given the fact that we are in this critical infrastructure environment as if you want to conduct cyber warfare, one way to go about it, if you have no morality whatsoever, is obviously to go to and destroy systems where we have life dependent machines, uh, attached to patients. And it's it would be a real well, obviously there's a lot of crime around, around the world. And, you know, with the recent happenings around the news, we see it's not to go political, but international, uh, lobbying. Um, you know, I say violated all the time. So depending on who is the perpetrator, it feels like it's getting a more desensitized like approach to it. When people say, oh, you look at I'm not going to name countries, but I guess you know what I mean. Um, when you see these major countries are committing these, these war crimes and there's essentially just a kind of a silence to it, it kind of does give an impression that people are getting more. And I talk politically right now, getting more desensitized to it, when in actuality, um, just as much as it is a war crime to bomb hospitals or whatnot or target hospitals, um, targeting these systems is the same equivalent of. Yeah, just killing meaning? Meaning with meaninglessly innocent people. Right. So it's definitely something that is very important and very concerning. Uh, but it's yeah, it's unfortunately something that. Yeah, uh, if it's used as cyber war crime, it's, uh, it's very hard to deal with. Um. Yeah. Yeah. I don't know if that was an answer, but, uh, but, yeah, uh, it's definitely something that we are taking very seriously, especially given the political climate of asset, uh, violations of. Yeah, normal standard procedures of war, I guess. Uh, uh, yeah. Sorry not to get it all political.

00:33:27  
*Speaker 2:* But but actually, like, I wanted to ask you, like, some of the, like, kind of like political questions related to, like, as a general politics and like, how cyberwarfare is affected in general. So since the US wants to buy Greenland, for example, there is a conflict between Denmark and the US. So how would you comment on these kind of situations?

00:33:50  
*Speaker 1:* Okay. Well, uh, I can't speak to much of what we're doing doing. But, um, I can't say that we are looking closely into Uh, how America and what Trump is talking about, uh, these certain times, especially when you talk about the buying of Greenland, where Trump obviously has said explicitly that he does not, um, exclude the use of military power, uh, um, in order to get Greenland. And due to these comments, we obviously have uh, also we also looking into seeing how we should act in terms of the products we use today. It's actually also been noted when, uh, I think it was a week ago, an article like I said, actually, if you want to later on through mail, but it's an article about how, uh, Trump has this is like, from what I'm remembering. So you gotta check out that article and then send it to you. But essentially a wake up call for companies who utilize cloud platforms like Microsoft, Google, uh, IBM, um, Amazon and stuff like this. Like these American big tech companies that every organization in Denmark or in Europe essentially use these platforms, which is many, uh, should have an exit plan ready because Trump has, uh, fired multiple people from the Department of Justice who ensure that these contractual obligations between USA and Europe, when it comes to data privacy and security should be upheld. Uh, Trump has essentially like fired these people. Um, which questions, uh, if America is going to do the same as China, it just, you know, uh, get, uh, get the American nose into our stuff. Um, which is very concerning, which is why in this article is outlining that European European total should have an exit plan to use some European based cloud, cloud, um, platforms. So it's something we consider. Uh, we looked at Musk as well. He has, um, also been in the political atmosphere, uh, and, uh, in terms of his eye, uh, that he is also working on this x eye or something like that. We are also looking into because I believe it's not like, uh, published yet, but we are also looking into possibly just blocking that as well. Um, I can't we haven't made that decision yet, but it's something we have internally discussed due to this, these talks about potentially making an ally like Denmark their enemy. So it's definitely something we are taking seriously. Um, because it's very weird. It's a weird political climate where, you know, supposed friends or allies can essentially just threaten each other. Um, based on what? Well, one can only guess. But when it's America, it's definitely not about natural resources, right? It's not. Uh. Um. But, uh. Yeah. So I hope I can answer your question. Yeah, but you got gone.

00:37:10  
*Speaker 2:* Yeah. So basically, you mentioned about the medical equipment and people dying as part of the, like, cybercrime. So can you can you explain this? So basically, I know that like we have the medical equipment that is controlled by the machines. So how can they be penetrated and how can they be like innovated like.

00:37:33  
*Speaker 1:* Yeah. Um, well there's a lot of different, uh, tactics and techniques that can be employed, but, uh, for, for any kind of attack to, to, to have any, uh, effect, you obviously need to have access to, to a machine or any machine, really. Uh, because, uh, Again. I'm not in the Department of network. Uh, I'm in here, but, um, there's, uh, a lot of kind of ways you can get into a system, either by, as we discussed earlier, about phishing emails, getting in someone to click on something so they get the credentials to give an account. This account, say, had a oh no, a user. It can also be a user who's just like, uh, not that not saying smart, dumb or something, but I know that careful and maybe places say note uh, to text file on the computer, name passwords or whatever to then get access to other systems or or other things that can just make a bad actor if they have initial access, uh, to, to to move laterally into the network. Now, the way to mitigate this, obviously, of course, is to employ, um, un like important services, uh, things like multi-factor authentication, uh, in which where solely knowing the password of a given user account doesn't give you access without other factors being, uh, put into play, whether that be your fingerprint or something that involves your phone. So it also dives into something you have rather than what you just know. So um, but so yeah, so so it can happen in many different ways. Uh, but, uh, the common thing is getting access somehow into a network which already by itself should be difficult enough and make it so difficult. So, so it's possible. Um, but obviously if you are inside the network, you're going to try to attack or try to target the most exploitable or the easiest exploitable systems, which can be critical systems, uh, that are deployed, uh, in real life. Um, but as I said, we have mitigations for it. But it's definitely when an attacker is inside. They want to be there, do as much damage, or get so much information as they can in the shortest amount of time. So anything that you added layer of complexity complexity to it, say with the MFA, for example, it discourages the attacker of continues to try to get further if you deployed these complex layers of security. So it's about essentially USD attacker have the capability of of something that the adversary has the capability of something. But then you make it so difficult or expensive for the attacker to just not do it. Yeah. Um, but yeah. So there's many different ways to get into the system. But if you do, you're going to try to see what is the easiest exploitable thing I can do and go, Uh, through that. Yeah.

00:40:54  
*Speaker 2:* So what future trends do you foresee in hospital cybersecurity, and how should that infrastructure evolve to address emerging threats?

00:41:07  
*Speaker 1:* Well, I think with the rise of AI that, um, cybersecurity as a whole, whole, we need to employ more, much more automation. Um, so, so ensure that with the amounts of attacks that can be automated today, that we have a corresponding response to it. And this can be done by not looking like at one specific, uh, say hacker tool or whatever, but looking holistically at the techniques that are being used, uh, because there could be many, many, many exploits that are being created every single day. But the techniques in which how they operate usually is the same. Usually there's only like one of four, I believe a year that is being developed which are considering new techniques. I can also link you that um, it was 1 or 4, I'm not sure, but I'll send you the article so you can, uh, fact check. Um, but uh, but yeah. So, uh, automation, uh, to combat this, this AI, the usage of AI in terms of attacks. And I think another threat we have to be, uh, cautious of is the, um, advancements in, uh, deepfake, if, you know, uh, so essentially having AIS that recreate AI videos, uh, using a particular person's face or mimicking or cloning their voice, uh, I myself personally have tried to clone my own voice using a recording of my phone. I recorded, I think, 30s of my voice, and it sounded like just like me over one sample. And to make that clone very good. You need at least 15 samples. I gave it one and it sounded a lot like me. So I made myself say some stupid, stupid stuff like, oh, I'm kidnapped or something, right? So, uh, where I'm thinking like, well, in the future, if you can both make video, um, and voice, um, and tell it like in, um, if you can tell the difference between an AI generated video call, like right now on streams, and even with an AI with the capability of, like, responding back to what you're saying in real time, then that poses an issue when you think about the implications of gaining information. And if you got information to the, then you have the information to get further into the network and etc.. So I think definitely more automation b b we should look at how AI videos are generated. Is there is there any, uh, patterns that we can, uh, or analysis we can do or tools we can use to identify these AI videos? Uh, because they're just going to get more and more sophisticated over time, and especially that and also phishing emails. Uh, even though it sounds like it's ridiculous that we still had this issue in 2025. But, yeah, uh, the more sophisticated all these kind of techniques are, the less indistinguishable they are from reality. And thus that can turn an issue. So yeah. And also we also must remember also the fact that depending on where you are at the hospital, sometimes you're in a very a lot of stress at work, like say the emergency department EMT um, if you get a phone call from your boss of some sort mimicking his voice or whatnot, you might not. Hackers might also utilize the fact that you're pressured at the moment or something like this, uh, in order to. Yeah. Just get some information or money or whatever it might be, uh, based on the people that are targeting. So, yeah, being more cautious about your your working environment, your. We have these identity cards where we go in and, you know, uh, you know, try not to, like, be a good person and just hold the door for us, for anyone, you know, make sure that they scan themselves or at least have the cards visible. All these things are very, like, logical for some. But, you know, we are humans and, you know, uh, sometimes it's raining. Oh, yeah. Of course. Just go and be a good human being. But in actuality, when it comes to physical security, this is not something we either allow or endorse. But practically speaking, uh, we I have seen it, you know, so. Or if I know someone, you know, something different, but you get what I mean. So, yeah, be being more cautious of AI and how it's going to be used and and yeah more automation essentially. There's also something we're working towards and are working currently at with. Yeah.

00:45:53  
*Speaker 2:* So what are the roles. Do identity and access management play in security hostile IT environments. And how does Azure support these security measures. So you mentioned we have this access card with like pictures and everything.

00:46:10  
*Speaker 1:* Yeah yeah yeah. Well in terms of if I can't speak too much about Azure because I don't work personally in it, but I do know that we do is not everyone who has access to Azure. And if you have access to Azure, it's um, on the administrators of our cloud incident, that administrator who has rights to certain, um, column subscriptions or certain, um, resource groups in which resources are deployed. And now I don't work with Azure, but, um, it's essentially on the responsibility of whoever owns that resource group to ensure that access management, um, access management is done like correct writes and management is done correctly. Um, so I can't speak on that. Uh, but I, I would like to think that it is something that is being like looked at very heavily. Just like yesterday, I went to this, um, from our security vendor. They had an event going through the, uh, the rest of the future and stuff like this. And they actually reported that almost 99% of all cloud accounts are overprivileged. Uh, which is a great stat, right? 99. Uh, now, I haven't obviously gone in and saw the research. They just said it. Um, but I'd like to believe it. Why not? Because it's very abstract. You know, when you're in the cloud and, you know, it's. Yeah, I'm not going to comment on that. But my point is, uh, but having, uh, having a good overview of who has access to what is something that is heavily encouraged. And we said our system, whenever you want a change on a given user, you have to go through this. Now this is a change process called so it's different demand. But uh, and then through these changes is documented what is changed from a user perspective. Um, but obviously this is a process, that process that is internal and is being enforced. Um, however, uh, I can't say that all the many thousands of workers we have around, uh, are doing that. I mean, it is something that we have in our policies and something we are encouraging people to do. Yeah, but, you know, that's the amount we can do. And obviously we have alert notifications on When users are getting say, um, I'm becoming a part of a much higher, uh, privileged group. All of a sudden this goes into user behavior, which is given from the user context of the XDR agent we have on our computers. So, um, yeah, I don't know if that was an answer. Uh, but yeah, um, the access management, uh, obviously it's a system depending dependent on who owns the resources or who is responsible, should I say, have the resources. And that differs from systems to system. But we do have with all of the solutions that we have in here internally. Uh, certain people who are, uh, described in our cmdb as being the responsible technical people who will have direct contact to our vendors if something should occur, a new configuration, a new update or whatever. We have people who have the responsibility of tackling this and is based on these people. Um, that should ensure the identity and access management of their respective system. Uh, yeah.

00:49:52  
*Speaker 2:* Interesting. So, like, how would you comment about the identity theft? So we spoke about the AI and we spoke about the. Double on authentication. Yeah. So how to improve it.

00:50:12  
*Speaker 1:* Um, yeah. Um, um, well starters at least, um, obviously it would be nice to say, you know, deployment everywhere. Uh, because then, you know, don't solely rely on a single, uh, factor, uh, with password and username, which can be known by anyone but employ something that is personal or something physical that you have your phone. But the reality is, some systems might not even support that. Some do, some don't. And depending on the system and its criticality and and all this, these factors, um, uh, is being deployed accordingly. Um, yeah. So, uh, I don't know, uh, uh, for the physical aspect, obviously it awareness campaign that is being done by our I guess you can say information security department here. Uh, they put out campaigns of, uh, on a wallpaper, for example. They do campaigns of ensuring that people remember to say, do something very easy, like locking your screen, you know, don't leave your computer like that. Don't leave your cards here, you know, because they can be copied and everything. Right? It's all so, um, so awareness, I guess, is an answer. Um, and, uh, yeah. And so most critical systems, uh, try to employ other factors than just solely username and password. Yeah, that's what I would like. That's what I guess would be the best option to do. Yeah. Uh, because in a perfect scenario with multi-factor authentication, uh, you have something, you know, so your password and username, uh, something you have your phone and something you are, which would then be maybe a biometric, uh, fingerprints or something like that. Um, so these factors would make it very, very difficult, uh, to, to bypass, in fact, I believe and you can do your own research on this. I believe a such a, um, such a bypass would be in the realms of 2 or $3 dollars to do. Which is just the thing to say. Like nothing is secure, but like nothing is by itself 1% secure. But it's about making it so secure that is too expensive for anyone's, or something that is very infeasible for a hacker to do, and to do that to the most important systems that that is obviously the recommendation to go with. Yeah.

00:53:01  
*Speaker 2:* Yeah. I don't have any more questions, honestly.

00:53:06  
*Speaker 1:* Okay, cool. I will, uh, give you the article on first of the techniques, I believe. I if I find out, uh, the amount of techniques that have been deployed, uh, each year. And I will also give you the thing about the cloud exit plan, uh, recommendations for Europe, um, due to, uh, Trump and his latest, uh.