00:00:02  
*Speaker 1:* So can you introduce yourself?

00:00:03  
*Speaker 2:* Yes. My name is Siamak. Uh, I'm working in a niche in the, um, the security department, actually, in the section of the security. My focus, uh, assignment and jobs is, uh, mostly on, um, analyze and pronunciations. Yeah, in general, cyber security and stuff like that. So. Yeah.

00:00:27  
*Speaker 1:* Yeah.

00:00:28  
*Speaker 2:* So you're talking. Yeah.

00:00:30  
*Speaker 1:* So how does CMT ensure the security and integrity of hospital I.T. infrastructure against evolving cyber threats?

00:00:40  
*Speaker 2:* Well, we have many security staff behind the wall. Actually, we like the company, actually. Of course, there's a firewall you can call, like a big wall against a wall, big wall or the public side. So to protect the enemies, you know, like all the ties coming in from other countries could be anywhere. So. And beside that, of course, also the other guy sitting and using the brains and doing the manual stuff as well as, you know, so always and always new challenges and you have to protect the company and region because we're doing the most important stuff in region. The most is the protection, the protecting the hospitals. That means the all the people actually could be you and me or your family or families actually could be laying down the operation table and doing some operation by doctor. So so our job is important to make sure that this operation goes well and no cost to people's lives and stuff like that. So so make sure that keep the company safe and yeah, everything is well.

00:01:45  
*Speaker 1:* What are the biggest cyber cyber security challenges facing Danish hospitals and how does seem to make it mitigate these risks?

00:01:54  
*Speaker 2:* Yeah, of course this is no secret. Everybody knows right now we are in different situations. situation. So the that we call a cyber war between Europe and other opposite sides like Russia, for example, and China, and they're all interested to get information and try to attack somehow, you know, by some cyber attack, you know, doing and hospitals, of course, one of the those things even you don't think that they will do that because of the cost of life and stuff. But still, we are in a war right now in this middle of the war. So, so still, we have to think about this very carefully. And what's important in this subject so protected as much as we can. So, so this yeah very important area. And I that's why everyday I work here is make me happy because we want to try to do make differences here to make the society and hospitals place and keep safe you know.

00:02:49  
*Speaker 1:* So how does CMT help to secure the information such as CPR numbers to help to protect the patients.

00:03:00  
*Speaker 2:* Well, of course, uh, as you know, that the paranormal is, uh, is a secure ID security in Denmark, so it's a very important idea. And, uh, it's a personal. So it's important to keep that secret and private. So especially Regine, we are working for the government. We are states in all. So we own all the animals somehow by the patients, you know? So it's our responsibility, uh, to do this, uh, keep it safe. And by doing any kind of, uh, could be some by doing some secure systems and locking down that, that, you know, leaking out, of course, by doing like, for example, any just the simple stuff, installing antivirus agents on your computers, personal computers do this, uh, for example, user rights very tied to not personal. Not everybody has any rights or admin rights to do this stuff, you know, so to somehow maybe by mistake. Not that I'm telling that like that. They do, but it could be by mistake or compromised by from the outside anyhow, you know, somehow. So. So our job is to protect this by this place software. We have actually and manual jobs and to keep them safe and not leaking out. So anyway, so it's a very important subject actually.

00:04:18  
*Speaker 1:* So what security challenges arise when integrating new digital solutions into hospital IT systems and how can they be addressed?

00:04:29  
*Speaker 2:* Uh, what do you mean exactly? If you put it out, you know, like an explorer.

00:04:35  
*Speaker 1:* So since, uh, basically region is not using its newest technology. Mhm.

00:04:41  
*Speaker 2:* Us you mean American technology or what? What technology.

00:04:45  
*Speaker 1:* Was that, medical technology.

00:04:46  
*Speaker 2:* Or medical technology? Yes. Yeah. And how would.

00:04:49  
*Speaker 1:* That how the integration of new digital solutions such as, for example, transfers from Nnamdi to mitigate the effect. Affected this kind of like cyber warfare. Where is it a more attacks, more threats?

00:05:04  
*Speaker 2:* Well, uh, it's not a big difference between the media and the media is not that important. But of course, there is a, um, there is a, uh, argument for that because of course, anyhow, when it is, any time the new system comes and take over, the whole system is always, uh, some vulnerability. Of course, you have to think about it. Also, you have to make sure that this is made down as well. So again, we do the same procedure even more actually, uh, with the military comes down. So to try to integrate this within the medical and digital and still using it of course. And again, not beside that also AI technologies coming in of course, also that uh, our responsibility is to make sure that all this transmission and integration, all this, uh, being in secure way to do, you know, so so that's for sure. Yeah. It's very important actually. Primary important that we're working with them, especially in the security department. We are working a lot also with the information security department that is in the GDPR and ISO in all the more compliance department. So we do a lot, uh, to work together because, uh, somehow it's connected together anyway. So because it's when you're talking about the CPI number and all the stuff, so it's all based on compliance also. So we need to make sure to protect this stuff, you know, by writing and by installing implementing system and stuff like that. So yeah.

00:06:29  
*Speaker 1:* So what are the key considerations when ensuring the compliance with GDPR and other data protection regulations in the hospital digitalization efforts?

00:06:40  
*Speaker 2:* The main key is like first of all, of course, if you have something in some integration, let's see. This is some application implemented, some medical equipment or something. Where this implementation comes from is if a third party, for example, if there is any other country or whatever it is. So we need to protect for, for example, from the compliance part, like, uh, all this paperwork is all in place. That's to be handled often in Danish. We call it like an agreement between two partners. So that means that when you transferring some data or making sure that you secret for us, or make sure that this is private and you have to treat it nice and, uh, like a good behavior, you know, so not like they get out. Otherwise they're going to be responsible if somehow, you know, so of course illegal. So this is one of the keys as well. And they can buy this like from the technical part of like of course also making sure that this CPR or whatever it is in between the integration is not uh, making sure that they are secure. It is not only internally existing. So there's no way to come out to public, you know, parts, that's for sure. Yeah.

00:07:42  
*Speaker 1:* How does EMT collaborate with national and international cyber security agencies to protect hospital infrastructure against cyber threats?

00:07:51  
*Speaker 2:* Yeah. In Denmark we have this, uh, the call, uh, this is data security Decentral security information. This is actually for the whole regions. Their job is actually cooperate with all us, all the regions in Denmark. Like for example, Copenhagen could be a Jutland. No no, no, all of them. So their job is like a corporate. All of us in this way to inform us is any attacks or intrusion, whatever it could be, could be like dangerous for religion. So there will be all eyes on with this all. They call it like suck, suck, suck. You know, if you understand this, the security of operation center and analyze center. So they actually implement this only for regions. And as well we have a locally as well. And by this way. So we always be informed if there is any. And for attacks or or try to be in or smelling something like that. So we can be like prepared and do something about it. So all agencies and we of course also in the region. I can say also we also have a contract with some third party agencies as well to help us with like a if anything happens, you know, in, in, in compared to attacks and stuff. So we could get help and take care of the actions and also do something about it. So yes.

00:09:16  
*Speaker 1:* So what role does identity and access management play in securing the hospital IT environments, and what is the best practices for ensuring the strong security controls?

00:09:29  
*Speaker 2:* Okay. Um that is important actually subject uh, identity and access, you know, of course, uh, I can see from the region side, like, of course, in this part we do to isolate this, of course, between within the only region, of course. So. And then how you protect it. You said the question was, or.

00:09:51  
*Speaker 1:* So what is the best practice for ensuring strong security controls.

00:09:55  
*Speaker 2:* The best practice could be like for example, again, making sure that the compliance part is on the place. Of course, in the case, if something happened and then the technical part will be like within, like making sure to all the digital equipment and PC or whatever is involved with this, uh, situation to handling the, uh, security access ID authentication. So there as well, the isolated and especially specific plans, violence, we call it that they exist only there. So they're not getting out anyway. So so this is very important by doing for example, uh, this violent like logging and to check it out all the time by doing alarm stuff like that if something pop up or, uh, not, you know, some unique stuff, you know, so we can. Okay. What does that happen? You know, so this way some has to do always on, um, on the case and you know what's going on, you know, so to make sure that these are stable. And also.

00:10:56  
*Speaker 1:* So how is the ransom ransomware threats evolving in the health care sector, and what preventive strategies are most effective for Danish hospitals?

00:11:06  
*Speaker 2:* Yeah, as you know, ransomware is actually, uh, one big role is, uh, doing all worldwide, right, actually, especially now in the hospital world. And for example, you can see that in England, NHS, for example, they've been hit by ransomware several times in back in US and Germany, you know, so but in Denmark we are lucky we haven't been hit on that much, you know, so especially the hospital I mean in this area. So protecting the yeah we know we are worried about that actually. And by protecting of course again to implement all this uh, protection we got uh, for example, all the product you can get, you know, it could be anything, could be Cisco product, could be pilots or whatever. I'm not saying which one we're running, of course, but by running this to protect the company's assets, you know, a lot of getting out in case of ransomware attacks. And also because besides that, we do a lot of actually also awareness for the employees. We know that also all this stuff is 8,090% is coming from internal from the companies workers, you know, by mistake or whatever, clicking some mails and not wanted, you know, and the attack is having good to do this stuff. You know after all you compare to 510 years ago. Right now it's so difficult to make a difference. Which one is right is not so. So that's why actually one of the important we do a lot of, uh, um, awareness in the, in the company region by doing the email and the screens, making videos myself. Actually my colleague actually be doing once a while videos in different kind of, uh, uh, subjects. So to tell people, okay, you have to be careful what to do and what to do. And also and of course all this implementation we have on the systems all around, you know, in the hospitals and offices, you know, so this way we try to protect of course, you never be 100%, but do the best we can, you know.

00:13:03  
*Speaker 1:* So what are the biggest threats cyber threats for Danish hospitals right now?

00:13:12  
*Speaker 2:* The biggest risk is like, yeah, attacking the hospital's equipment could be like, could be some like all the equipment, for example, not supporting the news, the security stuff, you know, so supporting. So that could be one of the scary part of course. Yeah it could be that. But anyway trying to do that on plan it again. You have to take care and you have to. Yeah it takes time. You know also because we're talking like lots of equipments around there. Also like talking like a couple of hundred thousand equipment from the small and the biggest one, you know. So and to take care of that of course already this plant and And then getting in on a process, you know, so to to gather this otherwise to fade them out by the new stuff, you know, and of course also yeah, we need to also convince the bosses, directors, the people responsible for the budget and stuff like that to make sure that we have some legacy systems we have to get them out of and get them off and try to invest and make still a lot of some of them a lot of money, you know. But if there is no money, they use an alternative, like to isolate them as well. So in this house, somehow they can continue working with this equipment and treating the patients and still secure enough, you know.

00:14:28  
*Speaker 1:* So so what will be the first step of, uh, reacting on the cyber attack on the medical equipment.

00:14:39  
*Speaker 2:* The first step for.

00:14:41  
*Speaker 1:* Yeah, what will be the first recovery step?

00:14:44  
*Speaker 2:* Recovery is the yeah, the recovery step. The first thing is you have to isolate this right away. If you have any suspicion of any equipment you think that might be infected by an attack or something? The first thing you do is isolated from the network as well, because then it's not going around. Spread it out, you know. So. So that's the first thing. And then you take it out of course. And to analyze the forensic, make forensic and then what exactly happened. Try to find out where it comes from, stuff like that. So that's a big work that we have to do now.

00:15:15  
*Speaker 1:* So what the worst outcome of the cyber attack on the hospital.

00:15:20  
*Speaker 2:* The worst of come, of course, is because we're talking about the life, you know, on the patients. That's the worst case you're thinking about. I mean, of course there's other cases as well. The data leak, you know, the personal stuff. But again, this is not the worst, but the worst case is ongoing. Like you have a patient on the table, uh, middle of the operation, something goes wrong with the digital stuff. And then customer life, you know? So that's the worst case scenario we can think, you know, it could be happen in the hospital region, of course. So that's why we always think the worst, uh, on the top of what can happen. That's why it's important case for us. So do what we can, you know best we can to and also convey some people if we see something, you know, and, um, sports and there is no there is a legacy system somewhere somehow. So we have to, of course, responsibility to tell the people. And that's one of the works that we do to, to, to, to attack, to detect these, uh, vulnerabilities and um, and uh, contacting, uh, responsible people that we call for better here and then so and then to try to tell them, okay, you have an honorable system. This system is very important. You have to fix it and right away as soon as possible, especially so. So this is our responsibility as well. So yeah.

00:16:38  
*Speaker 1:* How does CMT balance the need for accessibility and usability with strong cybersecurity measures in hospital I.T systems.

00:16:49  
*Speaker 2:* So how we do, how we try to call you when developing in this accessibility what the users, what we do to do. Of course, one of the things I mentioned before, like awareness, is to be careful how to or to use the computer and how do we be careful about the mails. And when you get the mail, if you space call this number, you're not sure about it, send it as a service, this department or security department to double check. That's what we do. Sometimes we get emails. Actually, when you use this on secure actually the good about it now they're getting better and better. So because we're doing all this awareness you know so I I'm happy that people they do even sometime could be right and good one anyway. So it's okay. This is good. No problem. And again because they're so good now it's difficult sometimes difficult difficult to to detect. Actually this is a real attack or not. So yeah. And again you try to tell people the truth. Also we are in a situation right now. We have to be careful and I think there are enough people they know. I worry about this also, of course, and especially these people working in the hospital at the front side. You know, there's, uh, nurses and doctors and stuff. I know they have a busy day normally. And sometimes there could be, um, when we come with more security, you know, they get pissed and angry, you know, say, okay, well, somebody scared about. So I understand the situation. They just want to save some people, you know? Anyway, so. But again, at the end, when the thing is over, they understand why we're doing this because we're doing to secure the job anyway. So that's why no one to try to, uh, destroy their work, you know? So, so.

00:18:30  
*Speaker 1:* So basically, what will happen if, for example, a doctor will get some ransomware, let's say malware on his PC? What will be the first step?

00:18:44  
*Speaker 2:* The first time we can actually, uh, we can see it under our system. We have a complex system here, the regime completely. So every time we put the agent on the early computers or the computers. So if in case this, uh, doctors or nurses computer get affected by some of this, it will be alarmed right away. We can see it on the system and then we do we can block it right away. We block it. That means you disconnect it totally from network. Everything. No internet, nothing. So that would be like a stupid PC with nothing, you know? So. So that's why we try and then do. The only solution is that if you have a time, of course you can check it out to play and to reference. What is it from what doesn't matter now. It's from everywhere anyway. So that's what you do. You just put the fresh image on it and then that's it. That's what we do. So it's make it easy. It's like our doctors up and running again. You can run new fresh without the malware or nothing.

00:19:39  
*Speaker 1:* How does the communication between the hospitals is being managed? How how it's managed to secure the data that is this transferring.

00:19:48  
*Speaker 2:* Between the hospitals. We have a good communication. That means we have all these departments. They have, of course, they have some boss, some leaders to take care of the department. Of course, all communication going by the email, we have the teams if we have any other compilation. But in case also we have to think about it. Also let us see if these attacks happen as there is no power or no mobile phone or no telecommunication. We have the old fashioned style like you take it out and all this. We practice in actually all the time. So yeah to do in case this happen, you know. So um, that's why we do so to make sure that everybody knows what to do. You know, the same like a firefighter, you have a practice and sometimes you're making alarms and you have to run on the stairs, leave everything you got, go there and do what to do. You know, everybody has a position the same we do once a while, you know? So to make practice in case attack happen, we simulate it like a real attack. And everybody knows what to do in case this happened. So. Yeah. Yeah.

00:20:50  
*Speaker 1:* Does quantum computers possess the strength for the hospitals?

00:20:55  
*Speaker 2:* Is there a quantum computer for everything? Actually, yeah, because the hospital is not the hospital only. We'll be talking about the, uh, the systems running in the hospitals, like on the companies, the application and stuff like that. That's why, for example, I could talk about the corruption in corruption and certificates and stuff like that. So if it does come up right now, we have the running, even though you're running the strongest encryption on the computers with the quantum computer, you can just decrypt the log in few seconds. You know, I mean, it's uh, that's Google basically. That's one of the. Yeah, I would say not benefits of this. Um, but again, there is a solution as well for that. So, so you can do something. There are of course there is threat for everything. Yeah. Quantum computer as well. It can be misused you know like the same like we have this chatbot I, you know, there can be also be used for dealing with malware and stuff instead of doing the good stuff, you know? So again, how to use it. Uh that's important.

00:21:58  
*Speaker 1:* So CMT recommended blocking the Grammarly and the GPT on, uh, on the computers. And for example, I work at Chip and we were forbidden to use, like, all the AI assistants. What what is what is what is the reason for it?

00:22:18  
*Speaker 2:* Yeah, we have, uh, policy in and region. Actually, there is no policy for blocking the chatbot. The real one, I mean, the American one. But we have a policy writing that you have to use it by responsibility, of course, and you have to have access. It's not just dealing, uh, sharing information, but upload the stuff, you know that. But all the other Chinese, uh, eyes and stuff like that, we block with the policy. We don't want to use this in our a company. So. And actually right now we're in process to also block anything. Any other right now is a deep sic of course is one of the biggest one now. But there are so many others as well. So try to make some policy and make plan process for to block as well as it was also maybe be thinking about like maybe just block everything else. Only watch this this one actually you need it. So it's much easier actually. So so of course this is important for us especially in the hospital area segment. So in dealing with the patient, all the stuff, sensitive stuff, sensitive information is important for us. Not everybody not them telling, not everybody they're doing the purpose. But anyway some mistake or whatever they don't know how to do, handle and deal with this stuff, you know, by mistake. Maybe it could be like uploading all the information is too late. You know, we don't want that, you know, even in America. So you have to be careful, cautious with this.

00:23:35  
*Speaker 1:* Would you consider the cyber attack on a hospital as cyber crime or cyber terrorism?

00:23:42  
*Speaker 2:* You mean the cyber attack? The hospital? Yeah. Yeah. Good question. I could be both. Because the crime. Yeah. It's a crime to attack in the hospital. You know, it's about the life and terrorism as well. Because behind the terrorism is always crime is the same. Actually, I would say so. I would say both of them actually either terrorism or. And also and there is another one as well. Espionage. Spying. You know. So that's for gathering the information. That's a different one of course. But those two could be like at the end, uh, will cost a life for those to be talking like terrorism and crime anyway. So, so I would say, yeah, both of them is, uh, is not good for the region, for hospitals.

00:24:26  
*Speaker 1:* Do you think that the political situation in the world affects the cyber warfare on the hospitals?

00:24:35  
*Speaker 2:* Politician infiltration?

00:24:36  
*Speaker 1:* Yeah.

00:24:37  
*Speaker 2:* Yeah, I would, because anytime you want political go out and say something wrong or whatever to that will do. We can see example of Ukraine and Russia. Anytime one political person goes from doesn't matter which country goes saying something to upset the Russian. But I think this is a free world, you have to say, of course, but but somehow will affect it anyway because they just listen. Yeah, okay. You say that I will do something, they don't care because these people, they don't care about the consequences. What's going to happen at the end for these people, you know. So they are they don't care the heating they can save in Ukraine and they just put him in the missiles, the damage in the hospitals physically, actually, they know this is going to hit this. But so for cyber attack, for them it's just like nothing anyway. So so that's for sure. Yeah this is on human you know. So I would say in this world I will say if you hitting the hospital is inhuman actually, because you know that at the end it's going to cost the people, you know, people life. So this is a yeah, I think maybe from the start was a little bit easy on it. They were a little bit they know it is. But it's getting worse and worse of course. Unfortunately, it wasn't that much actually worse. But later on, like the last couple of years actually, we tried to see more attacks coming, you know, cyber attacks against the hospital. Not only them, like every other country as well, you know. So they do. So they don't care.

00:25:59  
*Speaker 1:* So what future trends do you foresee in the hospital cybersecurity. And how should that infrastructure evolve to address emerging threats?

00:26:08  
*Speaker 2:* Again.

00:26:10  
*Speaker 1:* What future trends do you foresee in hospital cybersecurity and how should I.T. infrastructure evolve to address emerging threats?

00:26:20  
*Speaker 2:* Okay. Yeah, do be strong. And I said this is not the easy way to do but thinking. And I'm telling you, as soon as the attack is getting better, of course we try to get better to protect the assets and the other side again, they try to be even better to. That's what is important for us to be ahead, like a 2 or 3 step ahead before them, but it takes time. But now I think people are worried about it. So now they try to be actually actually good progress on this. Try to educate the people in cybersecurity and and tell them how to actually actually demo one of the now in the last couple of years, three years, one on the national hackers team we have in Denmark. So they try to intend to find in order to see who's winning. We win number one. Actually, in Denmark we are very good minds and young people for try to, you know, in cybersecurity and in this area. So it's good stuff. So I think we should develop all this knowledge and in this area to to get better and better, you know. So unfortunately we have working with dealing with some people like China and Russia for example, this state works, uh, hackers, you know, they're working for us there. So they just been, uh, pushed down. So they're the only two, the only thing they do from morning and evening, or maybe in 24 hours, they just try to behind the computer and try to hack. So getting better and better, you know. So that's why they do the hackers that will do. Normally they can use three months, six months, one year just for research to do something. And that's what they do. They have time. They have a lot of people to do. So it's important for us to catch this and be ahead to the front, you know. So this is a way only way only unfortunately.

00:27:59  
*Speaker 1:* What would be the optimal way to protect hospitals for now?

00:28:04  
*Speaker 2:* Optimal way. The only optimal way is like, uh, protecting. Unfortunately not because we can't even you cannot just close the down all hospitals. Unfortunately, that's the problem, you know, so we have to give them some free, uh, space as well, you know, do the job, because if you try to just lock it down, everything is going to be, uh, uh, make their work actually difficult and stuff like that. So we have to be balance, you know, making balance at the same time, making secure and not disturbing. There are works and and working in security as well, you know. So so this is a big difficult balance here, but that's what we try to do, you know. So so everybody's happy you know. Yeah.

00:28:48  
*Speaker 1:* Can you maybe give an example from your career of the cyber attack on the hospitals and like what was the outcome?

00:28:56  
*Speaker 2:* I can tell, for example, example, just not a few years back, actually, uh, he was officially on the internet anyway. So it was like it was a ransomware attack, they call it. Uh, I wasn't here, but it was. Janos actually was working here. You know him, actually. So. And he told me that actually there was a time in ransomware at that time, but that was not the war that time anyway, because in Russia. But it was like talking 6 or 7 years ago back or something. So. So the outcome was, you know, uh, fortunately it was good, actually not that bad. So it was on a few systems and they fixed it right away to so it was not a problem. But again, at that time it was a different time. Uh, we didn't have any tight security at that time. So now we are totally tight. So and this is you can read about it in any way, this instance, we can search about it, you know.

00:29:43  
*Speaker 1:* What was it, uh, Victoria Hospital.

00:29:46  
*Speaker 2:* Uh, I can't remember which hospital, but you can see from I think it was from 2016 or something else, but I can ask and he can confirm he knows exactly. Yeah. Actually, he knows I believe it could be one of them. Yeah. So that possible. But anyway, it was like a minor. Wasn't that crazy. So it was like fast and up and running. So imagine that now is even more stronger because we are tight in security. So that's not possible right now. Of course anything is possible. But again we haven't been hit. So that was the only time in actually I remember this. I heard about it. I wasn't there myself. But we can say another company has done but the hospital. Know what other mask. For example, one of the other example like they had down, you know, by ransomware. Anyway, they got big. They got about the economical, uh, financial problem for them, you know, So so they had to pay a lot of money and for them cost them a lot of money. They lose a lot of. So that's why that will happen. If you do you get hit by ransomware. But I think it was a start anyway. Uh, from the ransomware that time you want to start with. So the people didn't know what they wanted. So but now people there are still some people, the repair and stuff, you know. So anyway, I don't understand it. But they do they don't they don't see the serious about this and how big it is, you know. So.

00:31:12  
*Speaker 1:* So basically hospitals and like the region operates on the Microsoft based computers.

00:31:20  
*Speaker 2:* Not all. Yeah. Some of them. Yeah. Some of them. Yeah. So it could be different. I'll be talking like PCs. I could be uh, Microsoft and could be also Linux, for example. We have equipments. There are no either Microsoft or there could be some special, uh, homemade, uh, uh, firmware or application inside. Yeah. We do small little The devices, for example, for scanning is you cannot install a Microsoft relies on it, but the kernel could be something else some other. So you have to. That's what I'm telling you. So but basically yeah, the most part is we're talking like a PCs and server and stuff like that. It's Mac, Microsoft or or Linux, but mostly is Microsoft like 80%? Yeah.

00:32:01  
*Speaker 1:* Do you see any threads regarding the world, uh, situation targeting the Microsoft solutions and Microsoft apps?

00:32:11  
*Speaker 2:* Yeah, all the time, because I know the Microsoft they try they try to get better. But again, not enough. But always saying the Microsoft they should get better. But that's why they have guys like us for example. Also we can mention we can find someone about the old stuff like that. So record report to them and they need us as well. They know that even they tried to keep it tight anyway, the product. But again there are guys that want to sell the product. That's the way it is. But at the end when you end up in you and me and we have to use it, then, we find out the vulnerabilities later on, you know. So that's the problem. Always is you always, it seems always in these products anyway. So the thread is everyday always. And that's why they come in all the time patches and stuff. So to patch up you know. Yeah we talking uh we, we, we call that the Patch Tuesday because all the times the Microsofts come all the way every Tuesdays when you patch on windows. So imagine every week we have this. So how vulnerable they are you know so so yeah they are one have already running. Now next week is going to be new patches on your computer.

00:33:11  
*Speaker 1:* Yeah I didn't know about it.

00:33:13  
*Speaker 2:* Yeah it's crazy huh.

00:33:17  
*Speaker 1:* Is indeed. Yeah.

00:33:19  
*Speaker 2:* That's why we try to tell people and also restricting people to do not to install. They don't you don't give the people, uh, everybody to have the admin rights to just go and download and install everything on computer because then it makes it bigger, you know, so risky. So this is one of the other stuff, for example, to do protecting your assets and not necessarily to give everybody every rights and just giving them what they need. And that's it. You have to work with it anyway. So.

00:33:45  
*Speaker 1:* Yeah. So therefore there's not all the apps that you're allowed to install. Yes.

00:33:50  
*Speaker 2:* Exactly. Yeah. You have an app store on internally here we call it Software Shop. All the software we have been checking out. And since this is good enough to use and that's it. Behind that if they need something else. Except that if they're not existing, they have to make a system in the system demand we call so we can review and see okay, why do you need this? Is it good enough security enough is not at the end. We accept or not accept. So this is the process we're running. Yeah. So yeah, of course we keep it tight as possible. We don't give them rights to everybody. Just they can do anything they want. So, you know, this is the one of the reasons also we are secure also because this is a most companies have to do you know they don't do so.

00:34:31  
*Speaker 1:* So fair.

00:34:33  
*Speaker 2:* Enough. Yeah.

00:34:34  
*Speaker 1:* Yeah I don't have any more questions okay.