00:00:00  
*Speaker 1:* Sure.

00:00:00  
*Speaker 2:* Yeah. So basically I'm just writing like my bachelor thesis about the cyber security and therefore like, I want to know more about the cyber security of solutions as well. So basically how we defend the cyber attacks and how you investigate it. And if we can kind of like monitor the threats by ourself as well, not only do it, but like also like locally if possible. So basically like what is the procedure to kind of like monitor this threat.

00:00:31  
*Speaker 1:* So today you guys have different systems that are being monitored by the same solution. We use this solution for you guys which is this defender for endpoint solution. It's Microsoft's own antivirus and endpoint detection and response software. It's what is installed by default on most windows systems. So you guys use, uh, Azure, right. For your cloud. You use Active Directory for your local system and then for hosting your, uh, what you call virtual machines. You know, where, where, where you guys deliver all your services and so on. You also use this in Azure. Um, the way that your, I guess, incident response is set up today is that you guys have us as your support. You, as I understand you guys don't have us as mixer or security operations center only. This means that in case of an alert or something like this, it has to have a certain level of high severity for it to reach our security center today. Uh, it depends on the agreement that you have. But, you know, these incidents that we get in are from different severity levels, right? Urgent, high, medium, low, so on. Um, and the way that it works today is that we have a not designated, uh, security team who kind of works as a temporary, what would you call it, incident response team for you guys. And if they see something, they move it to my team. But because you guys don't have this specific, uh, we call it an MDR managed, uh, advanced threat detection solution today. It's what we would call ad hoc cybersecurity. So we let the security systems that we have developed and implemented for you guys using our EMS, um, enterprise mobility and security solution. This is the solution that drives your Intune the way that we secure your client devices, your own laptop, so on. Um, and then we also monitor your Azure activity. Right. You're like today, most hacker attacks are not, uh, brute force attacks. It's not like where they sit. I mean, these happens, and I see them quite often, but most attempts are either by phishing, spoofing or using, you know, human error to get by our systems. So we set up as many forms of, you know, authentication protection for you guys, um, like this. And then if it was to bypass, and a lot of activity is performed by a user, suddenly we will be informed by this. And then, um, and then, you know, these alerts will be given to me or like one of my team like this. Uh, but you also asked if you guys could potentially do this yourself.

00:03:15  
*Speaker 2:* Yeah.

00:03:18  
*Speaker 1:* Yes. Um, if you want, uh, one second, I can log into your guys's solution, and you could get, like, I guess, a hands on solution of the way that from point A to point B, uh, you could monitor it so you guys get, like, uh, what would you call it? Uh, um. Shark solutions. One second. We have a couple of different clients that have to find the right one. Um, boop boop boop boop boom. Just so you can get a gist of what we look at on the day to day, because you have your domain controller and different systems. Yeah. Um, I don't know. Do you have any administrative rights to your guys's environment today?

00:03:58  
*Speaker 2:* I'm not sure. Honestly.

00:04:01  
*Speaker 1:* You haven't ever been given, like some kind of task to do, like system administration or something like this?

00:04:09  
*Speaker 2:* No, not really, but I'm also like, interested in, like creating the log reports. So for example. Yes. Yeah. Like my personal experience is that like my PC, it kind of reacts sometimes like weird. And I would like to monitor it like somehow, like, you know, like to kind of like control whether it's maybe like, I know wires populated or something. Mhm.

00:04:32  
*Speaker 1:* Okay. So when you say one second you seems a little strange. Let me just jump into the system when you say you see like weird traffic or something like this. Um, you get, you get is it. And you, you suspect this to be virus or something that slows you down, or some kind of behavior that seems weird. Or.

00:04:56  
*Speaker 2:* Yeah, for example, like my PC rebooted for like 2:04 weeks, like five times. Maybe it just suddenly goes black and reboots. So.

00:05:10  
*Speaker 1:* Okay, out of nowhere, just like no indicator of like, okay, now we're gonna do this action.

00:05:15  
*Speaker 2:* So basically, like I've been working with power BI and like it suddenly just like reboots. So it's kind of weird.

00:05:23  
*Speaker 1:* The whole machine reboots.

00:05:25  
*Speaker 2:* Yeah. So like, the whole machine goes black and, like. Yeah, I was losing, like, I was losing my, like, I was like, tasks a lot like my progress. Because, like, I haven't had time, like to save up the version. And I was like.

00:05:44  
*Speaker 1:* Damn it. Yeah. Of course that's. Yeah, that's hella annoying. Yes. Um, okay. Let me see. I seem to be having some problems with your password manager. Let me just try something different here. Um, um. But. Yeah. So. So is it more for your own? Kind of like local system, or is it for the whole entire. Kind of like, uh, Azure infrastructure, like your, your guys's IT infrastructure that you, you are interested in in this cybersecurity aspect?

00:06:18  
*Speaker 2:* Honestly, I would I would just say covers in general. So like just for you to explain, for example, like what it will be like the first kind of get a like first rate of the response on the cyber attack or like what kind of like cyber attacks we usually like come across and like, what is the kind of most popular cyber attack on the like small businesses like ours and like how to like best way to recover from it for sure.

00:06:45  
*Speaker 1:* Okay. So it's kind of like from what we would expect to see the most and then how we would recover from it, or how we would kind of, I guess, react in this situation. Is that it?

00:06:57  
*Speaker 2:* Yeah.

00:06:58  
*Speaker 1:* Cool, cool. Okay. Yeah. For sure. Um, well, for you guys, for a smaller size, um, what would you say companies like you, there are different avenues of attack patterns that you can use. So one of them, as we briefly discussed, the main culprit or the main point of entry that these hackers use nowadays for companies of any size is user credential theft or authentication theft, meaning breach or lock in using an already existing account. Right? It's not like, you know, sometimes you would see in the movies this does happen, right? But where they would breach a system by doing a lot of like, uh, DDoS attacks or doing like breaches using scripts and automated services. This does happen a lot, but on the Azure side, Astrocyte because it's managed by Microsoft. Underlying security itself, it's really difficult to do. Um, so the majority of attacks that you guys would see would be breaches of your, um, like, user credentials, right? This could be a standard user account and so on. Um, but as you may know, and, uh, and as is the case, the real issue is not if they get access to one user. There are, of course, some problems there already in the form of um, in the form of like GDPR issues, or if the user has some specific like sensitive data on their given computer or account. Right. That's one thing. But in the grand scheme of things, that's not so important for a company, right? That's easy to recover from. But what we are most terrified of in these situations is what we call privileged escalation, right? It's where you go from having a normal user account, like maybe your account if I was just a normal administrative user in your company with no admin rights and so on. How can I, as a hacker, use this normal user account to escalate my access rights to maybe even all the way up to what we call root level or global admin rights? Write an admin account that can do anything, write delete systems, use system, so on, and that those are the kind of attacks that we see the most. They try to breach any account possible. Uh, this can be on premises. It could be your Active Directory, it could be your entry ID and so on. But then how is it possible for them to escalate accounts, right. Like gain more credentials. They there are so many different ways to do this. It's, uh, it's it's it's really almost impossible to guarantee every single escalation is not possible. But this is what we try to limit with these systems we set up at your guys's place. This group, for example, be some random users suddenly gaining and administrative right. It could, for example, be a user who has not committed a certain amount of activities before. Start to do it. This is a way that we can indicate it here. Now we use different AI tools. Microsoft's own Copilot, which is kind of like, I guess, a chatbot built into Microsoft. Uh, there is this extension of this called the Threat Intelligence, Microsoft Threat Intelligence, which is an AI tool, a giant, giant cloud database that scrapes all information about cyber attacks basically nonstop in real time to give us information about it. So if some new type of attack happens and it's something that's common in this type of what would you call it company size, that you have this specific kind of an what would you call it? Uh, IT infrastructure that you guys run when you see certain trends or user behavior, suddenly it could be an indicator of compromise. We we, as we call it, right? They have gained entry, but 90, I would say five, 99% of the time. Really all the attacks are these automated kind of brute forcing attempts on account. So let's say one of your guys's users by accident, you know, just human error inputs their data into like maybe their company data into some website or something. And this information, like the username gets scraped. And now, you know, these hacker groups has access to this. So they just try to bombard this account with, you know, user to sign in attempts. This is where, for example, the defense that we have for you guys, um, conditional access policies, which is the policies that protect your guys's users. Meaning let's say you log in from a new device for the first time, you will have to ensure that you can multifactor authenticate right to use two factor authentication by Mitre today. Right? You either use finger fingerprint on your already trusted two factor authentication device. Um, and then on top of that, of course you need your, uh, password. But one thing that we have seen is that these hackers have now been become so sophisticated that they set up these fake, uh, Microsoft multi-factor authentication websites where they use these API calls, which are these, um, maybe you know them from programming, but it's basically a way to contact a different service so that they make this fake website that contacts, uh, Microsoft's authenticator like multifactor authentication service to use it. But what happens is, let's say I was a victim of this attack. I go into a website, it looks like Microsoft. The only difference is the URL is different, but it's exactly 1 to 1 of what you would see when you log into like outlook and be asked to sign in. You lock in, you type in all your username and password, and then on top of that, it even asks you to use a multi-factor authentication to lock in. Um, and because, you know, you're just a normal user and you expect everything is fine, you go and you accept this lock in. Yeah. What they do is that they then take the token, this multi-factor authentication token, and then they save it for themselves so that they can reuse or kind of spoof your own two factor on multi-factor authentication when they try to breach your account. So even today there's multi-factor authentication, which is of course, it's even as a cyber security specialist, it's the best. Like it's the in general, it's the best type of defense you can use as a user, because it makes it a lot more difficult for anyone to breach your account. But it doesn't mean that it's not possible. And we have seen it many times, time and time again, that people fall for these things. Um, so this is just like one example of what I guess we would see a lot with you guys. So in regards to general cybersecurity, we have this, um, again, as I mentioned, this Intune baseline or this Intune security that manages all your devices, right, for your user devices, but it also manages the security for your users. This is separate. So let's say you log in on your phone to try to access some company resources. You'll be met with a layer of security like authenticate. This way. Make sure you're at the right location if this is set up. Now, a lot of companies, you know, because of this Russia situation, China situation, they set up, um, geofencing, as we call it, where we look at geographical location depending on IP addresses and so on. Uh, which again makes an extra level, of course, if you use VPN from another country to Denmark, you can spoof this, but that's again, we try to put up as many hurdles as possible. So you guys become such a troublesome victim that they just give up. That's that's a lot of a lot of the time. That's what we put up. Like things are so difficult for them that of course if they wanted to like we've heard this many times, big companies like mask, Lego, um, confuse the American government and stuff like these who are really, really secure. They still get breached. Right. So our, our main goal is just to make it as difficult as possible to breach anything. Because in general, even though you guys are a small company, of course you're a you're a prime target for these things. But these hackers usually send these attacks out automatically. So when there are so many hurdles that they have to do manual attacks and things like this, it is so difficult that usually they don't value to to attack you and just try to find another company who doesn't have this security, if that makes sense. So it's all about putting putting up hurdles. Um, yeah. And today, the the way the monitoring works, we lock your defender servers, like, your server locks into the same solution that we do with your client devices. This is how we generally do it. So if we also see what we saw like an example I could come up with two weeks ago, we had a large Danish company contact us because one of their um mail servers, exchange servers on premises have been breached or they have started seeing some very, very peculiar activity. Um, what had happened was and this could be an example for you guys with like, your Active Directory, um, someone or some other consultancy firm had been doing some maintenance on a server, like, let's say this happen to your guys's domain controller. There had been just some normal service agreement, right? I had to patch the system or something, and we add something new, which is like, you guys run Novation, for example, right. Uh, ERP and registry and or you have a file server. Sometimes you need a new integration to these services. And when you need a new integration, it means that you usually open up for a port, you know, for network access, so you can connect. And sometimes when these things happen, things don't get closed the right way. So this, um, other client, they had an open port basically where some hacker found out that this port was open and they started blasting requests in, and they actually got access to some accounts this way. So what we had to do was we had to troubleshoot, find out, okay, where are we getting these requests from? What port. How is this possible? Was it a human mistake or was it a actual breach? Um, because most of the time it's really just what they call vulnerability. Um, abuse. Right? They find a hole and then they use it. It's quite rare that they actually try to, uh, brute force breach, make a hole in your guys. The solution? Because it's very difficult to do in general. Um, so that's one of those. Uh, another just another example of it. But these attack types are endless, and you wouldn't believe the kind of things that we see, like the attempts that they make sometimes. Um, one could, for example, be not only, you know, these ransomware attacks, malware attacks where they lock down systems. Um, but what we have seen before is, let's say we see someone access an account and they actually get access to an admin account. Um, they will try to maintain their level of access rights as long as possible because now hackers know, like your guys, um, at Shark Solutions, you have what we, you know, we have what we call a recovery service or a backup solution, meaning that if something breaks down, we can just recover by running these backup solutions. Meaning depending on how long you guys have, you could have one month backup, you could have two a year more. Uh, so you could just decide, let's say you get a virus attack all the way in and we can save it. We just make a rollback, right? So we go like a week back in time, and you, you remove everything that had been installed, you know, from these seven days, and then you go like this, um, this is what's one of the, the greatest strength to have. This is why backups are so important. Because as you may have heard, like, sometimes the hackers just go so far that people like me and my team, we can't do anything. It's just too late. If encryption and so on, it's not even worth the time. But hackers know this. So what they do now, if they're very, very advanced, is that they go in and they start to try to make separate admin accounts so that if we close one, they have another one, and then they will try to monitor and figure out how long your guys's backup is. Let's say hypothetically, it's one month. Then they would get access today, and then they would do their best to maintain this access level for over one month until your guys's backup is not usable anymore. And then every time we would try to back up one month, they would still have access to the system, you know, because of our one month. Um, so these are these things just become more and more. That's why with these system, we monitor Azure activity. We monitor user activity. Let's say that you were to delete an excessive amount of SharePoint data or something that you have never done before. There would be an alert about this and it would be informed like this. So I guess that's kind of just one a couple of examples of how these things happen. Um, and then if you want to get kind of how we do the escalation, usually what happens is let's say you, for example, you see something that's very suspicious or something starts running on your computer. You guys have what we call it, an escaped plane. It's a it's an IT. Or would you call it incident response plan, meaning that you as an employee should be able to kind of assess, okay, this is out of the ordinary. I need to contact someone instead of, you know, you start kind of trying to do things on your own because 99% of the time, if you start trying to do something on your own without being informed, you make things worse, you know, because that's what the hackers want. So immediately when these things happen, the, uh, the employees, like the victim, is supposed to just put their hands up, stop touching the system, and then immediately shut the computer down and then contact your manager, who will then contact our security department. Like this. If it does not get caught by the system, and because most of the time, almost all the time. That's why these systems are so good. They take all these attacks that happen, but just once, sometimes they do get by, you know? Otherwise there wouldn't be people like me or other people who sit and do cybersecurity. They do get by these systems. Then they reach out to us, we do an investigation. We go look at the logs that have been taken from your machine up to this defender for endpoint solution that we have in the cloud. I have access to it on my system. If you have an account, you can also look at it at your on your computer. Then we will, um investigate. Okay. What has been seen on this machine. What kind of attack is this? Has it been um, it have we seen similar activity or this kind of behavior on other systems? Because really, that's what we're most interested in. We would rather just, uh, remove one machine than having your whole entire company have to go, you know, in lockdown. So immediately. It's all about isolating this device and then seeing if there's anything similar. Has it had any connectivity to like, let's say your machine or some server of yours with an open connection? And do we have to make some investigation here? If not, it's all about seeing how big the damages on this computer. How far did they come? Is it salvageable? Is it able? Is it possible for us to do a complete deep clean on this machine and save it so the user can get it back? Or are we really? Do we really need to wipe the whole machine, uh, reset everything? Um, and then of course, this is the dream scenario. If it's not something serious, a lot of times in cybersecurity we get what is called false positives, where the system because, you know, it's very, very strict. They will just find things that look suspect or like look like suspect behavior. But in reality it's something natural. Um, so we see these often works like, oh, this looks really bad, but in reality it's normal user behavior. But if it's actually a malicious attack or something, this is where we again isolate and if needed, let's say they gain access to your servers or God forbid, your Active Directory because your Active Directory is basically a way for you to communicate to every single machine connected to your guys's system or domain. So if I gain access to your Active Directory or your entry ID, write the cloud version the same. Where we manage all your users and your devices, you can do some serious damage. I can wipe every single. Like let's say I was the hacker and I got access to this account. I could delete every single machine in your environment. I could make serious, serious harm. Like it? Like irreversible damage. If I got this. And you can do it very, very fast. Because these guys have scripts who automatically just, like, lock every machine or put a certain level of encryption and so on. So it's to a certain extent it's a double edged sword. But of course, you like, um, companies like you and every company nowadays, they have these systems for a reason, you know, so we can manage your devices. But again, this is where they want to gain access to because one thing is you gain access to one computer that's only one victim. But if you can gain access to the main system, you can gain access to every single one of your. As I can see right now, 52 licensed users and thereby stop all access that you can do. Meaning you can work, you can produce, um, you can lock machines, they can gain access to all your files and thereby delete and remove. Um, if this worst was to happen immediately we close the system. And this is not a very well known thing, but in every single Azure instance. Right. Every single, uh, Microsoft cloud environment, there is a secret, we would call it a secret, but there's a unique port of entry that Microsoft's own support department and us as Microsoft partners can access, meaning that when we lock this whole system down, everyone inside, including the hackers, lose access. Um, then we can use this backdoor to gain access to your system and then see where are we? Is it so bad that we have to do a, you know, uh, backup recovery or is and can we kind of again, what we usually do is that we investigate the logs and see when did this activity start? Because if it is before, you know, your data, uh, data recovery length. Right. Data. Um, uh, would you call it backup length? Then there's some other things we have to do. But if it's not, we'd simply do a recovery. Uh, in a separate solution to monitor. Okay, now that we do this backup. And again, this is only worst case scenario. If there so far, we can't do any, um, you know, if we can block their account, remove their access, so on. We do this recovery in a different setup where they can get access, but we then do an investigation. In this isolated instance of, you know, this backup to show and prove that there is no hacker attacks or malicious activity in this instance. And then following this, we will then basically push you guys into this new version, uh, again removing all kind of hacker activity and so on. Uh, like this. But generally speaking, with these things happen, uh, most of the time we always do a backup because these hackers use what again is called this persistence or exfiltration. It's basically a hacker attack type. Um, or uh, like, I don't know if you're if you're, um, what you call familiar with this Mitra. Mitra attack patterns or. Mitra. Um, case. I can show you if you or not, but it's basically this, um, this mythical attack. You use it for its attack reporting like adversarial tactics, techniques, all these different types that attackers use, right? It goes everything from standard brute forcing. It can be, uh, user escalation. It can be, uh, reconnaissance, credential theft, things like this. Right. Standard things like these. They are known when they get access to create what is called child processes. So that let's say that we go and remove everything and we expect everything is gone. Now there's normal user behavior. Everything is fine. They still have this backdoor that they created, which most of the time is very difficult to find because they created like this. Sometimes what they do is that they kind of create them Inside Microsoft services, so it's even harder to find. I'm making it. I wouldn't say impossible, but close to impossible to give. You guys. Let's say you write a shared solution. Uh, you have this attack and then you ask us after, can we guarantee that now that we use this system, that there's nothing left? We need to do exceptionally thorough analysis to be able to give you this response. Uh, most of the time, this takes a long time. So if the backup process is, is is possible, we choose this instead because, as you know, the most important for you guys is just get back into production, be able to work. Because if you can't work, you can't pay the cyber security bill anyway. So that's what's most important. Being quick and effective and making sure that, let's say something happens, you have this, um, what you called it backup strategy plan.

00:29:08  
*Speaker 2:* Yeah.

00:29:09  
*Speaker 1:* So since we're working with Data Lake and the cloud computing, as far as I am familiar with it. So how do we secure that? No one breaches the data and that it's secure enough.

00:29:24  
*Speaker 2:* So it depends. So we you guys have both on premises file servers and then you also use SharePoint online on the cloud. Um, so on the cloud side, um, everything is what would you call it. It is protected by underlying Microsoft services. Everything is hosted behind. So first point of contact right. We have local data storage houses as it was in the old days, right where they would have it in the in the basement. They would have their servers. If you have it like this, that's already a security concern, right? You have data laying here. If someone goes into your basement, goes with a USB stick, you can pull it all out, take the data disk and run on top of this. So there are different levels of it. When you have it, let's say SharePoint, every SharePoint site that you guys have has data replication. So if something goes down, you have access to it. But from a security standpoint, what you would primarily focus on is access rights to them. Because again, most common attack types is lock in breaches. And if someone gains access to your account and you have sensitive data that's already been breached, then so what people would do again is set up this, um, technology that Microsoft uses a lot in the cloud called conditional accesses, meaning that you as a user need to fulfill a certain amount of conditions for you to be able to log in. So now you have already fulfilled this. That's why you can call me here. But if you were to, let's say use a personal phone or something, a different device, you would have to go through the same verification again. So this is already one level of security. Number two is your management level. So after you have gotten your access, how do I ensure that it's the right person who has this access. Right. So this could be monitoring what kind of access rights and roles that you guys have. It could be keeping up with, uh, activity logs and so on. Okay. Now that I, you know, these people have access, are they actually treating the data like they're supposed to? And then the last bit is more of a compliance standpoint. It is. How do I make sure that I, I comply with regulatory standards. It could be this new thing that is everywhere in Europe. This needs to I don't know if you've heard about it, but it's, it's it's basically like a giant European, um, data compliance thing that a lot of Danish companies and European companies have to, um, have a reasonable level of data security and data understanding. So this could be, for example, data ethics. Like how do I ensure that the data that I have is good? And then number two is ensuring that data leakage doesn't happen, because one thing is that we secure that other people can come in, but we also need to secure that our own users don't leak data by accident. And this happens very, very often. One of these ways, um, is by using what is called a DLP, a data loss prevention policy. This is something built in the cloud, meaning that let's say you download something or you try to share some data from SharePoint. There are these automatic data labeling algorithms or systems that basically go into every single file that you have before you try to send it in outlook or something, depending. Again, this all depends on the way that the company has set this up. But in general it should be like this. Then let's say that you have a document with some CPR numbers or some sensitive data in the moment that this reaches your outlook and you try to send it to someone from a different domain, it could be a private account, it could be just a different company. Or you send it to a bunch of people who of course is not supposed to have this data. This will automatically be blocked. And then it either will be sent to revision at the admin like of your company, or at our security team, where you do like a verification. Hey, uh, Julie, are you sure you want to be sending CPR numbers to 500 people in, like, uh, in a newsletter? Is this a good idea? Yes. No. Um, and then you also go and monitor. Okay. Why does every single person in my company, even the secretary or like, the what would you call it, maybe the the the handyman. Why does he have access to our economic system? Like what's going this is probably not supposed to be like this. How do we make sure that this doesn't happen? Um, because one thing that has happened quite often and we've seen a trend in recent years is that, for example, when people get fired, you know, and there's bad blood between the company and the employee. Sometimes we see people go and pull USB sticks into the machine and take a bunch of company data or do things like this. So most of the time when we get someone like, this is what we do in our secure SOC. Um, let's say you were a security operations center. Um, client we have a specific set of rules for when people leave companies. So that would monitor your data the way that it's being like this user has access to different data. Okay. If if this person if both he, for example, starts leaking all kinds of data are like moving data, deleting mass amounts of data using USB sticks because in general this is bad ethics or bad. Um, but usually it's against company policy to use USB pens. Um, Shark. Um, you guys have, like, one way of doing it. Other companies have none. Um, some companies use these policies where it's like, you can only use company owned USB spin sticks. And as we as we both know, when you get told something, you might still do another thing. But when you use these policies, you can also take knowledge like from a, from a technical standpoint, implement it so that it will be straight up blocked on your machine. When you input a USB pin or you try to move data. And then we are alerted so everyone knows. So there are many ways because even even something like taking a screenshot of data or doing things like this can also be monitored, but it's more difficult. Um, but in general, every single activity, type or activity that's being committed, uh, for example, on SharePoint is being monitored and the data is being, um, locked like this. Um, file servers are a different story because it's a bit more old school, and this is where we actually care more about, like, uh, are we using, uh, outdated protocols to gain access to our systems? Uh, the users who connect to these system, what policies are we using? Because it's a little more, um, what would you call it? Let loose the Wild West, in theory, with these, uh, old school system, because it's. You have so much freedom you still do in Microsoft Cloud, but you have some fundamentals, right? They still manage your infrastructure. They still manage the service that you run. But the one that you have access to, you can do whatever you want. So in theory, you could set up some very, very, extremely weak protocols where you could do a Google search and then you would have access. I see this all the time. I do these security analysts analysis, um, out at customers to kind of make an assessment of where they are. And sometimes you see some of the craziest things where, you know, they assume that everything is good. And then there's just like a back door that hasn't been looked at in ten years. And even if someone should, like, smell it in the air, their whole company would go, go down. So everything in the Microsoft cloud is more focused towards user user access and user mistakes. Access to data like this from and then on a server standpoint locally, for example, your file servers, it's much more important about like network security, right? How can I connect to these systems and so on. It's like this. Yeah.

00:37:33  
*Speaker 1:* So how about the communication between the like inside user and outside user for example like like how we communicate with customers. Like how secure it is.

00:37:44  
*Speaker 2:* Yeah. So it depends a bit. So general communication if we're talking just like a team's message outlook message. Um, in general there's a lot of protection. Uh, you it's it's near impossible to do any kind of escalation again, unless someone sent you a link through teams and then you communicate this way, right? But let's say it is about you leaking data or should be something like this. Then we have this data loss prevention policies first of all. Number two, there's a lot of prerequisites that you as a user have to go through, um, to, to kind of accept invitations, accept external help. Um, one thing that happens a lot specifically in Azure is, uh, external collaboration. Right? Someone needs access to something that you have when we do these things. The best practice and the way that the company policy is supposed to be and the way that it's supposed to be monitored, is you create a separate file, separate directory, completely different from what you guys usually use, and then you will extract the data that this external person needs. And then they have access to this isolated instance. Right. It's it's bad practice in general to just give access to people to your system. Right. Because first and foremost, everything might not be perfect inside. Right? And then you get someone else who's like, okay, this is, uh, this is this is good stuff. Let me just do whatever I can here. So you try as much as possible to, um, isolate and segment the different systems for external internal use. If you go into your Azure today, you have what we call internal. And then we have external users. So actually different user um types in Azure. You can also have this in your local system your Active Directory. And by default these uh external accounts have a lot less options of escalation. And it's kind of pre-built that they don't have a lot of access unless you as an admin give them because you could, uh, you could invite my private account into your, um, Azure's environment now, and you could give me global administrator. But of course we have company policies that make it very, very difficult to do so. And we have um, algorithms and again, monitoring capabilities where I would get, for example, an alert that said, okay, um, we are getting uh, like 30 different guest accounts and all of them are getting admin rights. What is going on here? Why is why is this happening? No one knows anything about it. Let's stop this immediately. Like this. Um, but general collaboration. If I are you referring to just like, communication, or is it like data sharing or the way that you work with others?

00:40:32  
*Speaker 1:* I would say it's both. Since we have like right now, like Data Lake, and we share a lot of the information together and like a lot of people are working on the like same stuff kind of. And for example, like when we pull like the power BI report, we have to pull it down, edit it and push it back. So how well it is like how secure it is, like not to bring the damage to the data.

00:40:57  
*Speaker 2:* So everything that you download and re-upload from your company computer is generally trusted. We go by this architecture type called Zero Trust. So everything outside of the company we don't trust at all until we get some kind of clarification. But internally, again because power BI and data lakes, they go under the same umbrella as SharePoint and so on, if sensitive data is contained inside of them, and you basically try to share it, it should block it, right? It should. But again, there are certain ways either there are certain ways to bypass this. Right. But again, it's all about making it as difficult for people to make mistakes as possible. So even this data that you do and I know let's say you do power BI external collaboration, you have to share this given um, power BI document to an external. And even though it's it's not always like the best way to think about it, But there's also a certain other. The company puts a certain level of responsibility on the user. So let's say you have an important power BI document. Now you are in charge of it. So we have these underlying security protocols and so on. But if you want to you can bypass them if you try hard enough. So that means that you also have to think about okay, maybe I should think about who I'm sharing these things with. And let me make sure or if I have any questions about, okay, what am I allowed to do? And am I supposed to do these things? You know, because sometimes things just go fast. I have to delivery this. This didn't save correctly. I don't I don't have time for this. Sometimes these things happen. And then we do like a review. I get notifications sometimes from, uh, SharePoint sites that my, uh, that, that our clients click on where you can see in the settings. We do like an analysis. Okay. If I just take this URL and put it in, can I actually access this without anything? And more often than not, it's actually like this if you don't, um, set up these security boundaries. Meaning that one mistake and this power BI report is gone. Uh, like, or all this access is already drawn out. So you have to make sure that, you know, when you give this right, you know, you have this sharing deal, uh, function where you can see, like, okay, everyone that has access to this are these people, and that's it. Uh, you don't go with this, like, thought after I can't. I actually trust this. Like, is this good? It is like, this is the way that you can give access out unless you just say everyone can read it or this is open for everyone. Yeah.

00:43:33  
*Speaker 1:* So what effect would it be like, for example, like a fellow mind will be like under a cyber attack.

00:43:39  
*Speaker 2:* If fellow mine was under cyber attack. Yeah. So we have specific um in fellow mind and in many of the, the consultancy firm world. We have a certain amount of, uh. Let me think. An example could be if someone breached my computer for them to have access to your guys's, um, sessions and access to these, uh, password managers and so on. Um, they would have to use extra biometrics. So the theoretically, the worst that could happen is that they gain access to the data that I have on my computer. If I was, you know, to make a mistake like this. Uh, but then immediately we have a high level of automatic isolation. So the second that something like this happens to the computer, like, even even the second, we had something similar happen, um, not with us, but but with, uh, someone that we give access to, like, we secure, um, the second that something like this happens, we have, like, a no, no, um, we have a strict, strict policy where the second we see something is just blocked, like you, you lose all internet access to the computer. Everything is gone. Um. And it makes it so that every session connected to it is gone. Uh, it also means that for us, it's actually a very annoying if something like this happens because, like, all our computers and stuff like this, if there's anything, they just get wiped and all the company data for everyone else is gone. So it's problematic for us, but it's secure for you guys. Um, we also have a high level of security on our, um, for example, we use these password managers. Um, it's like enterprise level things for you guys. Um, which has an extremely high level of security, meaning that for, again, if they were to breach my computer and this didn't get registered in this system, there are so many hurdles that they have to get through to get to this data, you know, before. Yeah. Yeah. They, they I guess security wise because we are we are they, they force us to be under a strict we have our own uh, actually External Security Operations Center because we could theoretically, um, drive ourselves like me and my team. Um, but we actually have another. Of course, I can name them, but we have another, um, security operation team externally who ordered all our security to make sure that if things like this happen, you know, we don't use human emotion and be like, ah, I don't have time for this right now. Then they just do it for us, you know? Um, of course there are some overlap, right? Because we are security specialists also. But they are what we would be to you guys actually. So yeah, I guess that's the way that, uh, but it's a very, very, very good question because in theory, if they got full access to this, then they have full access to you. Um, but there are so many levels of multi-factor authentication that I have to go through on a daily basis that they would be caught in it. And every time they would try to make a new one, even an example could be, uh, internally here, every single time someone tries to make a new authentication method or something, we get an alert on it. So every single little thing that's, you know, activity type, we also can monitor it. Um, yeah. I mean, from a security standpoint it's good, but sometimes it's annoying, I'll be honest. But it's just how it is, you know? So yeah, it'll be like this. Um, and just to, just to kind of clarify, I mentioned this in his talk, but us as a consultancy house and, and fellow mind is what we call a Microsoft, uh, partner. We're actually what would you call it, like Denmark's best Microsoft partner. We have a layer of compliance that we have to constantly give in to Microsoft and give in to, like, not the government, but these compliance entities to make sure that we constantly have our right security, uh, monitoring. Because again, if they if they breach us, they breach you. And it's the same, um, for us, even worse. So yeah.

00:47:44  
*Speaker 1:* It's like this.

00:47:46  
*Speaker 2:* Interestingly. So what is the biggest threat right now like for for us, for small companies, for big companies.

00:47:55  
*Speaker 1:* Well, yeah. Um, there are different concerns. Um, one of them is when you are, you guys are like what we call an SMP. So small to medium sized. Um, what they would focus on primarily with you would be either, um, for standard ransomware attacks. Right? They would lock you in and they would ask for your money, uh, or they would use what we have seen before where you have a certain amount of budget. Right. But if you use Microsoft Cloud, in theory, you have endless budget until they stop you. So what we actually see a lot of, uh, is attempts to breach not your users and stuff like this, but breach actually you breach users, but just to get access to your Azure environment, because in Azure, what they do is that they build up huge amounts of virtual machines in your Azure environment, right? Extremely quickly. And then they start Bitcoin mining using your guys's virtual machines and extracting it out. Because the payment for these virtual machines, they are like thousands of dollars, sometimes an hour. And they run multiple of them. Right. And then they just they they set these up in series like tens, maybe sometimes hundreds if possible. Right. If you don't have the right security, it's possible. But for example, with you, it's something we monitor a lot of course. Um, and then they would just start to bitcoin mine and all this cost right would be exceptional. We have seen actually uh, Danish companies and international companies go bankrupt because of this type of attack because, uh, not only does it affect them, but it also affects let's say fellow mine. Um, actually, because if you guys if this for example, virtual machine. Uh, we call it a virtual machine hijacking. They go in and they build up all these virtual machines to start running these. Um, Bitcoin mining. They can do this in minutes, by the way. Like they deploy a script and then suddenly you guys have, like, 50 different virtual machines, the most expensive you can have. And they're running these, uh, the bill is what we call pay as you go in cloud, which is what is so good about it. Right. It's a scalable solution. So you can you can just make a virtual machine really cool, really fun. But the downside of it is everyone else who has access can also do this. Um, so this is something that we monitor very heavily. If something happens, we monitor, um, this part of your company also, uh, specifically for chaque solution. Again, you're not part of our SOC, so I don't go super in detail with you. Usually it's other people. Uh, but, uh, it these would be user issues. So like, do you, do you go through security awareness training today.

00:50:41  
*Speaker 2:* Nope.

00:50:43  
*Speaker 1:* Okay, so this is something where let's say you use something like cyber pilot or so safe. Maybe you've seen it in your in your private life. You get this like you have to do these mandatory modules or you know, you don't pass like learn about cyber security. We call this a cyber awareness campaign where throughout the year you get these modules that you as an employee have to do, or you get someone like me or one of my colleagues to go explain cyber security, like you and I have just had a discussion about things that you need to pay attention to. But now the rest of your 50 colleagues, they are kind of out of the loop, right? Yeah. Um, because again, we have done studies on this before, but about 90 plus percent, 85, 90 plus percent of all cyber attacks are from human error, something like this today. And because the underlying cyber security like for your servers, for your Azure cloud and so on is so strong. It is the point of entry that most of the time happens is through users. That's why cyber security is so extremely important now, like cybersecurity awareness. So that your users, when they go through, they're like, okay, this seems weird. I've heard about this being dangerous. Maybe I should think, but when you just go through and maybe the day that you got hired, okay, this is our IT company policy. Let me just skim through the pages and then let me go on on my day. We don't really know what you guys are allowed to do, and we're not really. You guys are maybe not well informed about. Well, this is if I see something like this, the alarm bells should start ringing, you know, because when you are in a company PC, you are a big, big, big target compared to on your private life in general. Right? Because we are way more interested in companies who have a lot of money than versus maybe students who are an issue or something like this, you know? Um, so for sure, um, cyber, cyber, um, cyber awareness, policy training and stuff. I think my colleague is talking with yours about setting this up. Otherwise, I strongly recommend that you maybe talk to your, uh, colleagues or whoever's in charge about this because it's very, very important to get, um, also from a compliance standpoint, if they want, you know, from their IT revision guys and so on, it's very important, not from just the security standpoint, but also from a compliance, because you you guys as users, you are you know, you are the you are the golden ticket for a hacker in reality, you know, so it's uh, it's like that. So I would be most scared from user activity and I would be most scared about not continuing the IT growth plan that you have. Because the number one way to get breached is not updating your systems and having old, uh, old systems where let's say. Yeah, you have like, these old. Yeah. You know, SMB versions or TLS, these very old versions where basically if you sit on your computer now and did like a ping to some other system, you have full access like this, that's the way to get in. But if you keep monitoring it, if you keep maintaining these baselines, educate you guys, as you know, employees and colleagues, that's the way to go for sure. Um, but yeah, user behavior is probably what I'd be most scared of for sure.

00:54:00  
*Speaker 2:* So I have a pretty like tricky question. So since we're like using the printer that is connected to our local network, can a hacker intercept the document sent to printer?

00:54:14  
*Speaker 1:* It could, they could. Um, I don't know how your guys's printers are set up, per se. Um, but do you use, like, printers or do you use, like, some other printer management software today?

00:54:30  
*Speaker 2:* I have no idea. Like, I just, like, I just press print and just print.

00:54:35  
*Speaker 1:* Okay.

00:54:36  
*Speaker 2:* Yeah. Like in word or PDF or something like this. It just prints. Okay. Because yes. Yes and no. It depends on the type of printer. But in general, a standard printer who just has normal connectivity to your WiFi most of the time are actually quite easy to reach until you unless you look into them. And most of the time, which is something that may be a little, uh, golden nugget that you can bring back, make sure that the default password on your printers are changed, because in general, this is not something people do. And that means that if I go out to your guys's environment right now, you could. So, okay, there are two answers. Number one, there's this.

00:55:19  
*Speaker 1:* Yeah.

00:55:20  
*Speaker 2:* Um, you gain access by using this default password like you probably seen it by yourself, but like these books or HP or something, you go and Google the what you call model number. You get the manual PDF and in there it sets the default password. So if you go find that you can get full access to the printer. That's why it's very important that you change these by default. Uh, in general. Um, because otherwise again, you could just use this knowledge right now and then you could log in to the printer. I've had full full access number two. There's also because today we've spoken a lot about cloud security, which is what we focus mainly about here. But there is also the old school network, uh, network traffic and hijacking. Right. So you're referring to this man in the middle attack, right where you send data this way. And then in the middle of the data stream, someone pops in and then sees what you have. Um, yes. This is possible on your network. It depends a bit on the way that the server is. Sorry, the printer is set up. Um, to be honest, I'm not sure. The way that you guys have set up printers is something that we would have to look into. Um, but let's say that you go into your company, um, network. And if you don't have the right kind of security on your local network, I, I'm pretty sure if I remember correctly, at Shark Solutions, you have an internal network and then you have a guest network, right? Um, and your internal network. Do you know if, let's say I just bring my random computer in and I take a, um, land cable, right, an Ethernet cable and put it into the side of my PC? Do you know if I would have access to your internet?

00:56:57  
*Speaker 1:* I'm not sure if we use a land cable. I think we use a password.

00:57:01  
*Speaker 2:* So you you use a Wi-Fi password for your internal network, and then you're in.

00:57:07  
*Speaker 1:* Yeah.

00:57:08  
*Speaker 2:* Could you use your own private, uh, phone to log in to this internal network? Also, if you had this password and username.

00:57:17  
*Speaker 1:* I'm not sure, but I hope I, I think so, yeah.

00:57:20  
*Speaker 2:* Okay, okay. Because, um, to not to get too technical, the network protocols that you use usually sleep are different from your internal and guest, because guest is the one that you just give to everyone, right? Usually it's not as secure because you as a company don't really like this has nothing to do with us. This is just for people who come and drink coffee and by by, you know, but for internal. Right. This is where your domain controller. Right. Your active directory, maybe even connections to again printer to your different services file servers.

00:57:51  
*Speaker 1:* Yeah.

00:57:52  
*Speaker 2:* This is where we actually care about it. Because usually the way that it's set up is that cloud right. The cloud has it's basically one big land local network for you guys for your users. Yeah. But now that we're talking about old school networking, you have to think about that. Microsoft is not just making sure that this is fine. This is your own network. Regardless if you use Cisco, HP, Jupiter or whatever, you use juniper. Um, you could, as you maybe have heard before, if it's an insecure, unsecure network, you can use these gadgets or tools right. These cybersecurity emitters. So like maybe you've seen them from your school or something. There are these nice little gadgets with antennas that you can put inside of your computer to gain access to a network, and then you can use something like Wireshark or some other, uh, network monitoring solutions. And then if you set it up right and the network is not configured correctly, you can see every single action, every single detail that someone does on a network. Right. So this means, for example, as you just mentioned, you said you hope that you can connect to your internal network with your phone.

00:59:02  
*Speaker 1:* I mean, like, I don't I'm not hoping like but but yeah, like.

00:59:06  
*Speaker 2:* I know for for your ease like it's easy for you. Right. But if you can that proves that there's potentially a security issue. Because the way that it's supposed to be is that you use what is called an 800 and 21X, it's this maybe you've heard about it, but it's this security protocol that gives your computer and your computer only company trusted machine the allowance or rights to actually gain access to your internal network. Right? Because this means that if I were some bad guy and I go to your network, I get this may be a pretty simple password from you or something or someone else, right? I just ask like, uh, you know, I need some quick internet access for this internal blah, blah, blah. Can you give it to me? Oh, yeah. Sure, sure. Here it is. You gain access to this system, I plop this into the side of my computer, and I start not only printer data, it's every single thing that you guys do on the network. That's why also, it's this is also, uh, pretty important to remember when you go to something like a, uh, airport or you go to McDonald's or something where you use one of these guest, uh, networks, it's almost always not allowed to use company devices on these networks Works because they are. Generally speaking, you can see this. You know, if you connect with your phone to a network, you can see like a little bit. Sometimes you see this thing called WPA two or something like this. It doesn't really matter, but it's like some security stuff. But if you see a network that has no password in it, nothing at all, sometimes these guest has it. Please do not connect to it with your, um, company devices because we have seen directors of large, large Danish companies do this and then their credentials get hijacked because they are on these, it gets seen very, very often. So yes, in theory it's it would be possible to take this data from your printer to your device. Yeah.

01:01:07  
*Speaker 1:* Oh my God.

01:01:09  
*Speaker 2:* Yeah. It's a scary world.

01:01:11  
*Speaker 1:* So very scary. But I would say is it like since we're like I would say like communicate between like different countries, is there like a risk even though, like we're using internal network, for example, like a lot of my colleagues are working from us. And since right now is the relationship between Denmark and us is not great. Does it put us into the risk?

01:01:35  
*Speaker 2:* It puts up everyone, not specifically you and risk. Um, from a technology technological standpoint, it could do a little bit because what we have started doing is actually in our geo fencing or our geo geo blocking, um, systems. We start actually, um, blocking access to USA. Now if, unless the company customers has a need to do so because now US is being used as like a proxy service to use hacker attacks. Right? So usually they use China, Russia, um, US now and sometimes other countries to, you know, send these attacks from. So from a strictly tech standpoint, it's not like Yes, there are always worries about it. Um, but all the primary Microsoft solutions and service are developed by us. You know, even though we have our own data warehouses in Europe, you know, Germany, Eastern Europe and stuff like this, they are still owned and managed by Microsoft. So and as long as that's a us, um, you know, own company and to be honest, like it's a, it's at this point it's like a governmental entity. Right. When they're this big, it's like a lot of people are very like, uh, worried, worried. And I am of course, also about it. But when it comes to like, you know, you use these internal policies, um, for example, you use VPNs, I assume, to different solutions. I know you use Cisco. That's very secure. It's it's what we call end to end, um, end to end encryption. And as long as your users use this, it's it's fine because again this becomes private network. But again, if they are on their own home network and you know when they are on different systems, for example, fellow mine, I'm pretty sure doesn't fly to us and then make the installations there. I'm not sure, but maybe you have some other. The second that we start splitting up, offices starts splitting up. Networking means that maybe your office is secure, but your your colleagues in the US are maybe not secure because they don't run the same level of security as you guys do. Um, so that's already like a security issue. And when we use, of course, there is the problem of delay of data and so on because it's big distances. But, um, whenever we talk to people outside our country, that's already a security risk. You know, it's that's just how it is. But in general, it shouldn't really give you any big problems as long as they use their VPN into your system. They kind of cut off all options of kind of screwing up our, our system, and then they just do it at their own home office. But again, a VPN system can also be hacked if it's installed and running when they get breached. So there are some serious, um, security concerns. And again, most importantly, if their network is not secure, as I just mentioned, it is pretty easy to breach someone like this. So that's of course something to keep in mind. Yeah.

01:04:48  
*Speaker 1:* Very interesting. I have right now a lot to talk about with less.

01:04:54  
*Speaker 2:* Yeah. Yeah, sure. For sure. Um, I'm sure some of these things that maybe he, he has not informed you or it's, it's implemented or maybe it's something that's underway. I if I'm not mistaken, it's something that you guys are new customer or something like this. Like you like for us, you're like, you're a new, uh, new and fellow mine, if I'm not mistaken. Yeah. So, um. Yeah. So. So that means that you're you're maybe you're still in the process of setting up a lot of these security measures that we have mentioned about today, because that's usually something that we do in fellow mind. Uh, like you really have to say no for us not to do it. You know, it's because it's, you know, as we mentioned, there are so many ways to, to, to, to get breached, but for sure bring this by him. Um, and if you have any questions more something arrives or some questions. It's good because as I can see right now, I think it looks okay. But again, I'm not like primary on you guys. So if there's something you just reach out most of the time they'll probably reach out to me anyway. But yeah.

01:05:55  
*Speaker 1:* But great. Sure. Yeah. Thank you so much.

01:05:58  
*Speaker 2:* No worries at all. If there's any questions or anything for your report, you can just reach, send me a mail and we'll figure it out.

01:06:04  
*Speaker 1:* Yeah. Great. Yep. Yeah. Thank you so much.

01:06:08  
*Speaker 2:* Cool. No problem. Yeah. Have a lovely day.

01:06:10  
*Speaker 1:* Yeah. Have a nice day too.

01:06:12  
*Speaker 2:* Thank you.

01:06:12  
*Speaker 1:* Bye bye. Bye bye.