Interviewer: I'm writing my bachelor thesis about cybersecurity solutions, focusing on how we defend against cyber attacks, investigate them, and monitor threats. I'm particularly interested in understanding the procedures for monitoring threats both remotely and locally if possible.

Expert: Today your organization uses different systems that are monitored by the same solution. We use Microsoft Defender for Endpoint, which is Microsoft's own antivirus and endpoint detection and response software installed by default on most Windows systems.

Expert: Your organization uses Azure for cloud services, Active Directory for your local systems, and Azure for hosting virtual machines where you deliver your services. Your incident response setup includes our support, though you don't have us as your dedicated security operations center. This means alerts need to reach a certain severity level before they reach our security center.

Incidents we receive come with different severity classifications: urgent, high, medium, and low. Currently, we have a team that functions as a temporary incident response team for your organization. If they identify concerns, they escalate them to my specialized team.

Since you don't have a specific Managed Detection and Response (MDR) solution, your cybersecurity approach is what we call "ad hoc." We implement security systems through our Enterprise Mobility and Security (EMS) solution, which drives your Intune setup to secure client devices like your laptops. We also monitor your Azure activity.

Expert: Most hacker attacks today aren't brute force attacks, though those do happen. The majority of attempts come through phishing, spoofing, or exploiting human error to bypass our systems. We establish multiple layers of authentication protection for your organization. If these protections are bypassed and unusual activity occurs, we receive alerts that my team addresses.

Interviewer: Could you explain what the first response to a cyber attack typically looks like? What kinds of cyber attacks do small businesses like ours usually face, and what's the best way to recover from them?

Expert: So you want to know what types of attacks we most commonly see, how we would recover from them, and how we would react in those situations?

Interviewer: Yes, exactly.

Expert: For smaller companies like yours, hackers use various attack patterns. The main point of entry nowadays is user credential theft or authentication theft—breaching systems by using existing accounts. While you might see DDoS attacks and automated breaches in movies, these are more difficult against Azure infrastructure managed by Microsoft.

The majority of attacks you would face involve breaches of user credentials. While compromising a standard user account creates problems like GDPR issues or exposure of sensitive data, the real concern is privilege escalation. This is where hackers move from having a

normal user account to escalating their access rights, potentially reaching root level or global admin rights—accounts that can do anything from deleting systems to accessing all resources.

Expert: There are countless ways hackers attempt to escalate privileges, making it nearly impossible to guarantee complete protection. However, we implement systems to limit these risks. We can detect when random users suddenly gain administrative rights or when users who haven't performed certain activities before start doing so.

We use various AI tools including Microsoft's own Copilot and Microsoft Threat Intelligence. The latter is a cloud database that continuously scrapes information about cyber attacks in real time. This helps us identify new attack types common for companies with your size and IT infrastructure, allowing us to recognize unusual user behavior as potential indicators of compromise.

About 95-99% of attacks are automated brute-forcing attempts. For example, if one of your users accidentally inputs their company credentials on a website and their username gets scraped, hacker groups may bombard that account with sign-in attempts. This is where our defensive measures like conditional access policies come into play—requiring multi-factor authentication when logging in from new devices.

Expert: Hackers have become increasingly sophisticated. They now create fake Microsoft multi-factor authentication websites that use API calls to contact Microsoft's actual authentication service. When a user visits these convincing fake sites—which look identical to Microsoft login pages except for different URLs—they enter their credentials and complete the multi-factor authentication process. The hackers then capture the authentication token for later use, bypassing your security.

Even though multi-factor authentication remains the best defense for users, it's not foolproof. We've seen many people fall victim to these sophisticated phishing attempts.

Expert: For your organization, we implement Intune security that manages all your devices and user security. This creates multiple authentication layers. Many companies also implement geofencing, which restricts access based on geographical location determined by IP addresses. While this can be spoofed using VPNs, our goal is to create enough hurdles that attackers give up and move on to easier targets.

Even large companies like Maersk, Lego, and government agencies get breached despite strong security. Our main objective is making attacks as difficult as possible. Hackers typically use automated attacks, and when faced with multiple security layers requiring manual intervention, they often abandon the attempt and look for less secure companies.

Expert: Two weeks ago, a large Danish company contacted us because they noticed unusual activity on their Exchange server. We discovered that during routine maintenance, a consultant had opened a network port for integration purposes but failed to close it properly. Hackers discovered this vulnerability and exploited it to gain access to accounts.

Our response involved troubleshooting to identify the source of requests, determining which port was compromised, and assessing whether it was human error or a deliberate breach. Most attacks exploit vulnerabilities rather than attempting to create new holes in your security, as the latter is much more difficult.

Expert: Another concerning scenario involves hackers who gain admin access and try to maintain it for extended periods. They understand that companies like yours have backup solutions for recovery. If something breaks down, you can roll back to an earlier state—perhaps one week or one month back—removing everything installed during that period.

Sophisticated attackers might create multiple admin accounts so that if we close one, they still have others. They monitor your backup retention period—let's say one month—and maintain access for longer than that period. This means that even if we restore from backup, they still have access to your systems. This is why we continuously monitor Azure activity and user behavior for unusual actions.

Expert: If you notice something suspicious on your computer, you should follow your incident response plan. This means:

1. Stop all activity immediately
2. Shut down the computer
3. Contact your manager, who will then contact our security department

When we receive such reports, we investigate the logs from your machine through Defender for Endpoint. We assess:

- What type of attack is occurring
- Whether similar activity exists on other systems
- How to isolate the affected device to prevent spread

We determine whether the machine can be cleaned or needs to be completely wiped. Sometimes we encounter false positives—the system flags normal user behavior as suspicious.

Expert: If attackers gain access to your Active Directory or Entra ID (the cloud version), they could cause devastating damage—potentially wiping every machine in your environment using automated scripts, encrypting data, or causing irreversible harm.

In such cases, we immediately lock down the system. Every Azure instance has a special access method that Microsoft support and partners can use. This allows us to cut off everyone's access, including the hackers, while we investigate and remediate. We examine logs to determine when the activity started and whether it predates your backup retention period.

If we can block their accounts and remove access, we'll do so. If necessary, we'll restore from backup in an isolated environment, verify the absence of malicious activity, and then transition your organization to this clean environment.

Expert: Hackers often employ persistence techniques based on the MITRE ATT&CK framework, which catalogs adversarial tactics and techniques. They create child processes and backdoors that are difficult to detect, sometimes embedding them within Microsoft services. This makes it challenging to guarantee complete removal of all malicious elements.

While thorough analysis is possible, it's time-consuming. That's why we often opt for the backup restoration process—it's quicker and more effective, allowing you to resume operations faster. The priority is getting your business back to productivity, because if you can't work, you can't pay the cybersecurity bill either.

Interviewer: So since we're working with Data Lake and cloud computing, as far as I am familiar with it, how do we secure that? How do we ensure no one breaches the data and that it's secure enough?

Expert: It depends. You have both on-premises file servers and SharePoint online in the cloud. On the cloud side, everything is protected by underlying Microsoft services.

Looking at security historically, we used to have local data storage in server rooms. That's already a security concern - if someone physically enters your server room with a USB stick, they can take your data disks and run.

With SharePoint, every site you have includes data replication, so if something goes down, you still have access. But from a security standpoint, you should primarily focus on access rights.

Layer 1: Access Control

The most common attack types involve login breaches. If someone gains access to your account and you have sensitive data, that's already a breach. Microsoft uses conditional access technology in the cloud, meaning users need to fulfill certain conditions to log in. You've already done this verification to join this call, but if you were to use a personal phone or a different device, you would need to go through verification again.

Layer 2: Access Management

After someone has access, how do we ensure it's the right person? This involves monitoring access rights and roles, reviewing activity logs, and tracking how people are treating the data.

Layer 3: Compliance

How do we ensure compliance with regulatory standards? For example, there's a major European data compliance framework that Danish and European companies must follow. This includes data ethics and preventing data leakage.

We need to secure not only against external threats but also ensure our own users don't accidentally leak data. This happens frequently.

One approach is using Data Loss Prevention (DLP) policies built into the cloud. These systems automatically scan files before you try to send them. For example, if you download something from SharePoint and try to email it, automatic data labeling algorithms check every file. If it contains CPR numbers or sensitive data and you're sending it to someone from a different domain or to many people, it will be automatically blocked.

The system either sends it for admin review or to our security team for verification: "Are you sure you want to send CPR numbers to 500 people in a newsletter?"

We also monitor access rights. For example: Why does the handyman have access to our economic system? This probably shouldn't be happening.

A common threat is when people leave companies, especially if there's bad blood. We've seen cases where departing employees insert USB drives and take company data. In our Security Operations Center, we have specific rules for monitoring when people leave companies.

We track if a person suddenly starts leaking data, moving data, mass-deleting data, or using USB sticks, which is generally against company policy. Some companies only allow company-owned USB sticks, and we can implement technical solutions that block unauthorized USB devices and alert security teams.

Even taking screenshots can be monitored, though it's more difficult. Generally, every activity on SharePoint is monitored and logged.

File servers present different security challenges because they're more traditional systems. We care more about whether outdated protocols are being used to access these systems and what policies are in place. File servers can be more like the "Wild West" with greater freedom. With on-premises systems, you have complete control but also complete responsibility.

Interviewer: How secure is the communication between internal users and outside users, for example when we communicate with customers?

Expert: For general communication like Teams or Outlook messages, there's strong protection. It's nearly impossible to escalate privileges unless someone sends you a malicious link.

For data sharing, we have those Data Loss Prevention policies I mentioned. There are also prerequisites for accepting invitations and external help.

A common scenario in Azure is external collaboration. Best practice is to create a separate file directory, completely isolated from your main systems, extract only the data the external person needs, and give them access only to that isolated instance. It's bad practice to give external people access to your systems, as not everything might be perfectly secured internally.

In Azure, we distinguish between internal and external users. By default, external accounts have fewer options for escalation. You could technically invite my private account into your Azure environment and give me global administrator rights, but company policies make this difficult.

We have monitoring capabilities where I would get an alert if many guest accounts suddenly received admin rights.

Interviewer: Since we have Data Lake and share a lot of information, with many people working on the same things - for example, when we pull Power BI reports, edit them, and push them back - how secure is this process?

Expert: Everything you download and re-upload from your company computer is generally trusted. We follow a Zero Trust architecture, meaning we don't trust anything outside the company until verified, but internal systems are generally trusted.

Since Power BI and Data Lakes fall under the same umbrella as SharePoint, if sensitive data is contained inside them and you try to share it inappropriately, the system should block it. There are ways to bypass this, but it's about making it difficult for people to make mistakes.

When you share a Power BI document externally, the company also places responsibility on the user. Even with underlying security protocols, if you try hard enough, you can bypass them. You need to consider who you're sharing with and whether you're authorized to share particular data.

Sometimes in a rush, things happen. We regularly review sharing permissions and analyze access settings. Often we find that if a URL is placed in a browser, the document can be accessed without authentication if security boundaries aren't properly set up. This means one mistake could compromise a Power BI report or grant unwanted access.

Interviewer: What effect would it have if “Company X” (consulting company) was under a cyber attack?

Expert: If someone breached my computer, they would need additional biometrics to access your sessions and password managers. Theoretically, the worst that could happen is they gain access to data on my computer.

We have automatic isolation protocols. If a breach is detected, the affected computer immediately loses all internet access, all connected sessions are terminated, and the computer gets wiped. This is annoying for us but secures your data.

We use enterprise-level password managers with extremely high security levels. Even if they breached my computer without the system detecting it, there are many hurdles to accessing that data.

From a security standpoint, we operate under strict protocols. We actually have our own external Security Operations Center. They handle our security to ensure objective decision-making without emotional bias.

This is important because if they breach us, they breach you as well. As Denmark's leading Microsoft partner, we have compliance standards we must maintain with Microsoft and regulatory entities.

Interviewer: What is the biggest threat right now for small to medium companies?

Expert: For small to medium-sized businesses like yours, primary concerns include standard ransomware attacks where they lock your systems and demand payment.

Another trend we're seeing is attackers targeting cloud resources. Since you use Microsoft Cloud with "pay as you go" pricing, attackers try to breach users to gain access to your Azure environment. They quickly build many high-powered virtual machines for cryptocurrency mining, extracting profits while generating enormous costs for you. These virtual machines can cost thousands of dollars per hour.

We've seen companies go bankrupt from these attacks. Attackers can deploy a script and suddenly create 50 expensive virtual machines in minutes. The scalability that makes cloud computing attractive also creates this risk. We monitor this aspect of your company very closely.

The most significant user-related risk is lack of security awareness. Do you currently receive security awareness training?

Interviewer: No.

Expert: This is something to consider. You could use platforms like Cyber Pilot or So Safe that provide mandatory security modules, or have someone like me explain cybersecurity concepts to employees.

Studies show that 85-90% of cyber attacks result from human error. The underlying security for servers and cloud is strong, so attackers target users as the entry point. That's why cybersecurity awareness is extremely important.

When you work on a company PC, you're a much bigger target than in your private life because companies have money, making them more attractive than individuals. I believe my colleague is discussing setting up security awareness training with your team, but I strongly recommend pursuing this from both security and compliance perspectives.

Users are the "golden ticket" for hackers. I would be most concerned about user activity and not continuing your IT growth plan. The number one way to get breached is not updating systems and running outdated protocols. If you maintain baseline security, keep systems updated, and educate employees, you'll be well-protected.

Interviewer: Since we're using printers connected to our local network, could a hacker intercept documents sent to the printer?

Expert: Yes, they could, depending on how your printers are set up. A standard printer with normal WiFi connectivity is quite easy to access unless properly secured.

An important tip: make sure the default passwords on your printers are changed. Often, people don't do this. If I went to your environment right now, I could potentially Google your printer

model number, find the manual PDF with the default password, and gain full access to the printer.

Beyond cloud security, there's also traditional network traffic concerns - what's called a "man-in-the-middle" attack where someone intercepts data in transit. This is possible on your network depending on your printer setup.

Let me ask you: Do you know if your company uses separate internal and guest networks?

Interviewer: I think we use a password for network access.

Expert: So you use a WiFi password for your internal network. Could you use your own personal phone to log into this internal network if you had the password?

Interviewer: I'm not sure, but I think so, yes.

Expert: This potentially indicates a security issue. Ideally, you should use 802.1X authentication protocol, which only allows company-trusted machines to access your internal network.

If someone gets your network password, they could connect their device and potentially monitor not just printer data but all network traffic. This is why you should never connect company devices to unsecured networks like those in airports or restaurants. We've seen directors of large Danish companies do this and have their credentials stolen.

Interviewer: Since we communicate between different countries and many colleagues work from the US, does this create additional risk given the current relationship between Denmark and the US?

Expert: It puts everyone at some risk, not specifically you. From a technical standpoint, we've actually started geo-blocking access to the US unless companies specifically need it, as the US is increasingly being used as a proxy for cyber attacks.

While there are concerns, Microsoft solutions and services are developed by US companies. As long as your colleagues use VPNs with end-to-end encryption to connect to your systems, it creates a private network tunnel that's relatively secure.

The real issue is that while your Danish office might be secure, your US colleagues might not have the same security level. Whenever we communicate outside our country, that's inherently a security risk. And if their home networks aren't secure, as we discussed earlier, they could be breached more easily.

Interviewer: Very interesting. I have a lot to discuss with our team now.

Expert: I'm sure some of these things are either already implemented or in progress. If I'm not mistaken, you're a relatively new customer with “Company X”, so you're probably still setting up

many of these security measures. Feel free to raise these points with your team, and if you have any questions, just reach out to me.

Interviewer: Thank you so much.

Expert: No worries at all. If you have any questions for your report, just send me an email and we'll figure it out.

Interviewer: Thank you. Have a nice day.