Interviewer: Can you introduce yourself?

Expert: Yes. My name is “Expert”. I work in the security department. My focus and job responsibilities are mostly on analysis and cybersecurity in general.

Interviewer: How does “COMPANY A” ensure the security and integrity of hospital IT infrastructure against evolving cyber threats?

Expert: We have many security measures in place. First, there's a firewall - like a big wall between us and the public side to protect against threats coming in from other countries. Besides that, we have security staff using their expertise and doing manual work as well.

We constantly face new challenges in protecting the company and the region because we're handling very important work - protecting hospitals. This means we're protecting systems that support operations where people - including you, me, our families - might be on an operating table receiving medical care. Our job is critical to ensure operations go smoothly without endangering people's lives. We work to keep the company safe and ensure everything runs well.

Interviewer: What are the biggest cybersecurity challenges facing Danish hospitals and how does “COMPANY A” mitigate these risks?

Expert: This is no secret. Currently, we're in the middle of a cyber war between Europe and opposing sides like Russia and China. These actors are interested in obtaining information and launching cyber attacks. Hospitals are targets even though you might think they wouldn't attack healthcare due to the potential loss of life. Nevertheless, we're in the middle of this war, so we must think very carefully about protection.

This is an important area, and that's why I'm happy to work here every day - we're trying to make a difference in keeping society and hospitals safe.

Interviewer: How does “COMPANY A” help to secure information such as CPR numbers to protect patients?

Expert: As you know, the personal number (CPR) is an important security ID in Denmark. It's personal information that must be kept private. Especially in our region where we work for the government, we're responsible for protecting this data.

We implement various security measures like secure systems that prevent data leakage. We use simple but effective approaches such as installing antivirus agents on computers and implementing strict user rights policies. Not everybody has administrative rights that could accidentally compromise security. Our job is to protect this information using specialized software and manual monitoring to prevent leaks.

Interviewer: What security challenges arise when integrating new digital solutions into hospital IT systems and how can they be addressed?

Expert: Any time a new system is implemented, there are vulnerabilities during the transition period. We follow the same security procedures - even more stringently - when new medical technology is implemented. With AI technologies also being introduced, our responsibility is to ensure that all these integrations happen securely.

This is a primary focus in the security department. We work closely with the information security department that handles GDPR and ISO compliance. There's significant collaboration because when we're talking about protecting CPR numbers and other sensitive data, it's all connected to compliance. We need to ensure protection through proper documentation, system implementation, and ongoing monitoring.

Interviewer: What are the key considerations when ensuring compliance with GDPR and other data protection regulations in hospital digitalization efforts?

Expert: The main consideration is understanding where implementations come from, especially with third-party systems. From the compliance perspective, we need to ensure all paperwork is in place - what we call in Danish an agreement between partners. This means when transferring data, we ensure it remains secure and private. Partners must handle it appropriately, otherwise they become legally responsible.

From the technical side, we ensure that CPR numbers and other sensitive data in integrations are secured and cannot be accessed publicly. It's about ensuring data remains within protected environments.

Interviewer: How does “COMPANY A” collaborate with national and international cybersecurity agencies to protect hospital infrastructure against cyber threats?

Expert: In Denmark, we have the Center for Cybersecurity that works with all regions across Denmark - Copenhagen, Jutland, and others. Their job is to coordinate information about attacks, intrusions, or any potential dangers to the regions. They operate what we call Security Operation Centers and Analysis Centers implemented specifically for the regions.

We also have local security operations. This way, we're always informed about potential attacks or suspicious activity so we can be prepared and respond appropriately. Additionally, in our region, we have contracts with third-party agencies to assist if an attack occurs, helping us take action and mitigate impacts.

Interviewer: What role does identity and access management play in securing hospital IT environments, and what are the best practices for ensuring strong security controls?

Expert: That's an important subject. For identity and access, we isolate systems within the region. Best practices include ensuring compliance measures are in place in case something happens.

On the technical side, we ensure all digital equipment, PCs, and other devices involved with security access, ID authentication are properly configured. We create isolated environments with

specific security protocols that don't expose sensitive information. We implement logging systems and alarms that alert us to unusual activities, allowing us to monitor situations continuously and maintain stability.

Interviewer: How are ransomware threats evolving in the healthcare sector, and what preventive strategies are most effective for Danish hospitals?

Expert: Ransomware is playing a major role worldwide, especially in the hospital sector. For example, in England, NHS has been hit by ransomware several times, as have healthcare systems in the US and Germany. In Denmark, we've been fortunate not to be significantly affected, especially in hospitals.

For protection, we implement various security products - I won't specify which ones we use - to protect company assets against ransomware attacks. We also focus heavily on awareness training for employees, recognizing that 80-90% of attacks come from internal sources when employees mistakenly click on malicious emails. Compared to 5-10 years ago, it's now much more difficult to differentiate between legitimate and malicious communications.

We conduct extensive awareness campaigns within the region using emails, screen notifications, and videos covering different security topics. We explain to people what to be careful about while implementing protective systems throughout hospitals and offices. While we can never be 100% secure, we do the best we can.

Interviewer: What are the biggest cyber threats for Danish hospitals right now?

Expert: One of the biggest risks is attacks targeting hospital equipment, especially older systems that don't support newer security features. Addressing this requires careful planning because we're talking about hundreds of thousands of pieces of equipment, from small to large.

We have plans to either update vulnerable systems or phase them out with newer equipment. This requires convincing directors and budget managers that we need to replace legacy systems, which can be expensive. When funding isn't available, we use alternative approaches like isolating vulnerable systems so they can continue functioning securely while still treating patients.

Interviewer: What would be the first recovery step when reacting to a cyber attack on medical equipment?

Expert: The first step is immediate isolation. If you suspect any equipment might be infected by an attack, you isolate it from the network immediately to prevent the threat from spreading. Then you remove it for forensic analysis to determine exactly what happened and where the attack originated. This is substantial work that we must do.

Interviewer: What's the worst possible outcome of a cyber attack on a hospital?

Expert: The worst outcome is definitely loss of patient life. While data leaks of personal information are serious, the worst-case scenario is having a patient on an operating table when something goes wrong with the digital systems, potentially causing loss of life. That's why we always prepare for the worst possible scenario.

It's our responsibility to detect vulnerabilities and contact those responsible when we find legacy systems or other issues that need immediate attention. We prioritize patient safety above all.

Interviewer: How does “COMPANY A” balance the need for accessibility and usability with strong cybersecurity measures in hospital IT systems?

Expert: One approach is awareness training - teaching users to be careful with computers and emails. We encourage them to forward suspicious emails to the service or security department for verification. I'm pleased that people are doing this, even when sometimes the emails turn out to be legitimate. Modern attacks are becoming so sophisticated that it's increasingly difficult to distinguish real threats.

We try to communicate honestly about the current threat situation. Most hospital staff understand, especially those working on the front lines like nurses and doctors. Sometimes they get frustrated with additional security measures because they're busy saving lives. But ultimately, they understand we're implementing these measures to secure their work, not to hinder it.

Interviewer: What would happen if a doctor's PC became infected with ransomware or malware?

Expert: We have a comprehensive monitoring system across the region with agents installed on all computers. If a doctor's or nurse's computer is infected, we receive an immediate alert. We can then block the machine right away, disconnecting it completely from the network - no internet, nothing. It essentially becomes a standalone PC with no connectivity.

If time permits, we may investigate the source of the infection, but what matters most is getting the doctor operational again. We install a fresh system image, and they're back up and running without the malware.

Interviewer: How is communication between hospitals managed to secure data transfers?

Expert: We have good communication structures with department leaders coordinating across hospitals. Communications typically happen through email and Teams. We also prepare for scenarios where attacks might disable power, mobile phones, or telecommunications by practicing old-fashioned communication methods.

We conduct regular drills, similar to fire drills, where we simulate attacks and ensure everyone knows their role and responsibilities. Everyone has assigned positions during an incident, and we practice to ensure preparedness in case of a real attack.

Interviewer: Do quantum computers pose a threat to hospitals?

Expert: Quantum computing poses threats to everything, including hospital systems. With current encryption, a quantum computer could decrypt protected information in seconds. However, there are also solutions being developed to address this.

Like ChatGPT and other AI tools, quantum computing can be misused to develop malware instead of beneficial applications. It all depends on how the technology is used.

Interviewer: ”COMPANY A” recommended blocking Grammarly and GPT on computers. At Chip, we were forbidden from using AI assistants. What's the reason for this?

Expert: In our region, we don't have a policy completely blocking the main AI chatbots, but we do have a policy requiring responsible use and ensuring users don't share sensitive information when uploading content. We do block Chinese AI tools and other less trusted systems.

We're currently in the process of considering blocking more AI tools, possibly allowing only approved systems that are needed. This is especially important in the hospital environment where we handle sensitive patient information. We're concerned about accidental uploads of sensitive information, even to American services. We need to be cautious with this data.

Interviewer: Would you consider a cyber attack on a hospital as cybercrime or cyber terrorism?

Expert: It could be both. Attacking a hospital is certainly a crime because it puts lives at risk. It's also terrorism because there's always crime behind terrorism. Another category is espionage - spying to gather information. But both terrorism and crime ultimately can cost lives, so neither is acceptable for hospitals and regional healthcare.

Interviewer: Do you think the political situation in the world affects cyber warfare against hospitals?

Expert: Absolutely. We can see examples with Ukraine and Russia - whenever a political figure says something that upsets Russia, there can be consequences. These actors don't care about the impact on people. In Ukraine, they knowingly target hospitals with missiles causing physical damage, so cyber attacks would mean nothing to them.

Attacking hospitals is inhuman because it costs people their lives. Unfortunately, the situation has worsened in recent years with more cyber attacks directed at hospitals worldwide. These attackers simply don't care about the consequences.

Interviewer: What future trends do you foresee in hospital cybersecurity, and how should IT infrastructure evolve to address emerging threats?

Expert: As attacks become more sophisticated, we must constantly improve our defenses. It's important to stay 2-3 steps ahead, though this takes time. People are now more concerned about cybersecurity, which has led to good progress in educating people and raising awareness.

Denmark has a national hackers team that competes internationally, and we've ranked number one. We have talented young minds in cybersecurity, which is encouraging. We need to continue developing this knowledge to improve our defenses.

Unfortunately, we're dealing with state-sponsored hackers from countries like China and Russia who work around the clock on hacking activities. They might spend months or even a year researching vulnerabilities. We need to anticipate these efforts and stay ahead - that's the only way.

Interviewer: What would be the optimal way to protect hospitals now?

Expert: The challenge is that we can't simply shut down hospitals completely. We need to find a balance between security and functionality. If we lock down everything too tightly, it makes healthcare work difficult. We need to maintain security without disrupting the critical work being done. It's a difficult balance, but that's what we strive for - ensuring everyone can work effectively while maintaining security.

Interviewer: Can you give an example from your career of a cyber attack on hospitals and its outcome?

Expert: There was a ransomware attack a few years ago - about 6-7 years back. Fortunately, the outcome wasn't too bad. It affected only a few systems, and they were fixed quickly. At that time, security wasn't as tight as it is now. You can find information about this incident online from around 2016.

Another example outside our region was a company that was hit by ransomware. They faced significant financial problems and had to pay a lot of money. That shows what can happen with a ransomware attack. Unfortunately, some people still don't understand the seriousness of these threats.

Interviewer: Do hospitals and the region operate primarily on Microsoft-based computers?

Expert: Not all systems are Microsoft-based. For PCs, it could be Microsoft or Linux. Some medical equipment has specialized firmware or applications. Small devices for scanning can't run Microsoft systems but use other specialized operating systems. Overall, about 80% of our PCs and servers run Microsoft, with the rest on Linux.

Interviewer: Do you see threats targeting Microsoft solutions and apps due to the global situation?

Expert: All the time. Microsoft is trying to improve, but it's never enough. They need security professionals like us to find and report vulnerabilities. They're focused on selling products, and often vulnerabilities are only discovered after deployment.

We call it "Patch Tuesday" because Microsoft releases security patches every Tuesday. This shows how vulnerable these systems are - every week there are new patches. That's why we

restrict users from having admin rights to download and install software freely. This reduces risk. We only give people the access rights they need to do their jobs.

Interviewer: So that's why not all apps are allowed to be installed?

Expert: Exactly. We have an internal app store called Software Shop with pre-approved software that we've vetted for security. If users need something that isn't available, they must submit a system demand that we review to determine if it's secure enough to approve. This process helps us maintain tight security by controlling what software is installed. Many companies don't do this, which is why we're more secure.

Interviewer: That's all the questions I have.