Interviewer: Can you introduce yourself?

Expert: My name is “Expert”. I have been working in IT for 8 to 10 years, both as a supporter and consultant in Denmark and in Poland. For the last three years, I've been working with security, specifically with SIEM solutions. SIEM is a way you collect logs and create use cases where you can search for things you want to monitor - like who has gained unauthorized admin rights or accessed restricted areas.

Interviewer: How long have you been working at “COMPANY A”?

Expert: One year and eight months.

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

Expert: We do a lot with firewalls, making sure that we only open connections that need to be accessible from the internet. We also use antivirus endpoints on devices. In our platform, Cortex, we can see incidents and alerts, which helps us monitor and detect potential security issues.

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

Expert: One of the biggest challenges is budget constraints. We have a lot of old medical equipment running on outdated systems like Windows 7. Purchasing new equipment is very expensive, and sometimes new alternatives aren't even available. To mitigate risks, we use antivirus protection and have a secure VPN network where we place vulnerable machines like those running Windows 7 or 8 to make them more secure.

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

Expert: The biggest issue with old equipment is that they no longer receive updates - whether Windows updates or other security patches. Even with antivirus, you might not be able to run the newest version but perhaps a lighter version. That's one of the biggest issues - you try to make these systems safe, but they'll never be completely secure.

Interviewer: During the past five years, there's been huge digitalization progress in Denmark, including the change from NemID to MitID. How did it affect the healthcare sector?

Expert: I haven't worked directly with MitID in hospitals, but I think one improvement is having the app on your mobile device. With MitID, you need to scan a QR code, which is more secure because you don't just click a button to approve.

Interviewer: How does digitalization in hospitals impact data security, particularly regarding sensitive patient information such as CPR numbers?

Expert: That's a good question. If you compare to the old days when records were on paper, perhaps it was easier to access information physically. But with newer digital systems, we look more carefully at system security before implementation rather than just purchasing without consideration. We're now more likely to ensure systems are encrypted. So in some ways, digitalization has made things more secure. However, there are still many vendors that don't prioritize security when developing software.

Interviewer: I work at “COMPANY B”, and we collaborate with various hospitals across Denmark. How can “COMPANY A” ensure that we're maintaining the integrity of the data correctly?

Expert: I know a little about “COMPANY B”. Do you use the SDN network? SDN stands for "Sundhedens Data Netværk" (Health Data Network) - it's a network connecting all hospitals that has been upgraded for better security. I think Chip might be using this network, which would help ensure security, though I'm not certain.

Interviewer: Can you detect in emails if we inadvertently include CPR numbers or sensitive patient data?

Expert: I know “Person X” is working with that. I haven't seen the system personally, but I know he can monitor if CPR numbers have been sent from Office 365.

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

Expert: When agencies issue recommendations or alerts, we typically implement them. For example, TikTok has been banned from all our computers and mobile devices. We've also banned some AI applications from China. We work with an organization called "Mist" (name uncertain) for hospital cybersecurity, and they advise on blocking access from certain countries. I believe we've blocked 39 out of 40 recommended countries.

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: For asset management, when you have access management programs properly documented in our ICSM system, it's easier to handle software vulnerabilities. You can quickly identify which systems have vulnerable software and ensure updates are applied, or in the case of OT (Operational Technology) systems, you can block specific vulnerabilities.

I'm still learning about IT security - I completed my security certification in 2021, and in my previous job, I was part-time internal IT responsible while focusing on security.

Interviewer: Our systems currently use passwords and usernames. How can hospitals improve this?

Expert: We're implementing multi-factor authentication, sometimes using a key on your phone. Some systems also use ID cards for login on mobile computers, combined with a PIN or password. Not all systems support multi-factor authentication, but it's also about user awareness - teaching people not to click suspicious email links. Security is as much about human behavior as technology.

Interviewer: Does “COMPANY A” provide this kind of training?

Expert: I don't know.

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

Expert: Ransomware has been a significant issue for hospitals in other countries. I believe there was a ransomware attack on a Danish hospital last year, or perhaps it was another company whose software the hospital uses. One strategy we use is monitoring what's being installed to detect malware. We could improve by restricting what users can download. Currently, we have different security layers where some users can install software and others cannot.

Interviewer: Chip, as a medical organization, has banned the usage of GPT, Grammarly, and different AI helpers. Can you comment on this? What is your statement about AI and the threat to cybersecurity?

Expert: I believe Grammarly has been blocked at our organization too. One of the biggest issues with AI is that there are so many different platforms - some good, some not. I've heard that people can find ways around AI restrictions by rephrasing questions. This is still a new area, and the best approach is probably to evaluate which AI tools are acceptable and which should be blocked, based on recommendations from security agencies.

Interviewer: Does “COMPANY A” consider quantum computers a threat to cybersecurity?

Expert: I don't know specifically, but I think all companies are considering this threat, which is why there's so much emphasis on multi-factor authentication. We know it's easier to crack passwords with advanced computing, so we require certain password complexity standards. But even with a quantum computer, an attacker would still need access to password files. By blocking hacking tools and implementing multi-factor authentication, we're taking steps to mitigate these future risks.

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

Expert: Good question. One approach is hiring project leaders to phase out outdated systems like Windows 7 or Server 2008, which improves security. However, hospitals often have legacy systems that can't be easily replaced. In these cases, we need to apply for special exemptions to maintain these systems without updates.

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

Expert: We should involve IT security architects more in the procurement process to evaluate new systems before purchase. We also need more funding to replace outdated equipment.