Interviewer: Can you please introduce yourself?

Expert: My name is “Expert”. I'm a security specialist here at Operational Security in “COMPANY A” for the capital region.

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

Expert: That's the big question. The challenge with cybersecurity is that we're often playing catch-up. We can build secure infrastructure and prepare as thoroughly as possible, but it's only when skilled hackers or malicious actors find new attack vectors that we learn how to mitigate those specific threats.

Our approach involves building barriers and robustness, creating multiple defensive layers. If attackers breach one layer, we have several more protecting our systems. This multilayered strategy is fundamental to our security posture.

It's difficult to guarantee absolute security, especially with the rapid development of AI technology. People are constantly finding innovative ways to use AI for malicious purposes. We're working quickly to secure our systems against AI-based threats and examining how we can defend against what could be described as "AI weapons."

Interviewer: What are the biggest cybersecurity challenges facing Danish hospitals, and how does your team mitigate these risks?

Expert: While DDoS attacks are the most common threats we face—similar to what other organizations experience—these are relatively easy to mitigate with the right infrastructure. I believe the biggest challenges are the emerging, unknown threats associated with AI technology.

As international cooperation becomes more destabilized, countries like Russia have greater incentives to target nations like Denmark. These evolving AI-based threats and supply chain vulnerabilities require extra vigilance.

To address these risks, we conduct extensive risk-based analyses, trying to anticipate potential attack vectors by thinking like adversaries: "If we wanted to attack the capital region, how would we do it?" Based on these analyses, we implement appropriate mitigations and defenses.

We also collaborate extensively with other regions, the European Union, the Danish Ministry of Defense, and various entities to ensure we maintain multiple perspectives on cybersecurity.

Interviewer: Does “COMPANY A” consider the risks of quantum computing?

Expert: We're aware of quantum computing risks, but this technology isn't yet a practical threat. The CEO of NVIDIA recently suggested it might take 10-15 years before quantum computers become functional at scale. When quantum computing becomes relevant to security, we'll certainly address it, but currently, it's too complex for malicious actors to utilize effectively.

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

Expert: Our hospitals are becoming increasingly digitalized, with almost every device—from medical equipment to fridges and even light bulbs—connected to the internet. We have standard procedures and optimizations to ensure sensitive personal data like CPR numbers remain secure.

One key approach is connecting an EDR number to a person's data, making direct access to CPR numbers more difficult. All data is encrypted, and multiple security layers exist to prevent unauthorized access.

While there have been past leaks of CPR numbers, and I can't guarantee it won't happen again, we implement comprehensive security procedures to make it difficult for external actors to breach our systems or for colleagues to make human errors. Our multiple procedural layers help minimize these risks.

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

Expert: Ransomware presents challenges for attackers because executing these attacks requires more sophisticated equipment and code than simpler attacks. To be successful, attackers need considerable skill to infiltrate our systems.

If ransomware were to infiltrate our network, the affected machine would automatically be isolated to prevent spread. Our primary defense is our backup and recovery system—we would delete the affected systems, restore from backups, and rebuild. While this might take days or weeks, it's an effective strategy.

I believe we wouldn't engage with hackers or pay ransoms—that's not an option for us.

Interviewer: What about risks to medical technology?

Expert: Most medical technology runs on applications or operating systems that we can restore if compromised. Regardless of the type of ransomware, our backup and recovery systems protect these critical systems. For example, if an MRI scanner were affected, we could remove the infected system, reinstall from backups, and continue operations.

Interviewer: What about the risk for patients?

Expert: There would be some operational disruption and delays in patient care, procedures, and operations. The impact would depend on how many patients are waiting to use the affected systems. Recovery might take a few days or weeks, but we would prioritize critical cases.

We could also relocate patients to other hospitals or regions if necessary. Denmark has five different healthcare regions, so if the capital region were offline, we could send patients to facilities in Zealand, a couple of hours south by car.

Interviewer: So the regions are independent from one another?

Expert: We collaborate extensively and share cybersecurity insights, but operationally, we are independent.

Interviewer: What security challenges arise when integrating new digital solutions into hospital IT systems, and how can they be addressed? For example, a couple of years ago people were using NMT, but now people are using MedNet.

Expert: The transition from MedIA to MedNet was specifically to improve security. Whenever we introduce new technology, there's an adjustment period. The biggest security challenges are rarely with the programs or applications themselves—they're with people. Users can be sloppy, too busy to remember security details, or neglect security procedures.

When introducing new technologies, we try to design them with familiar workflows so users don't face a complete paradigm shift. This reduces the likelihood of security errors during transition periods.

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

Expert: We're implementing privileged access management (PAM) to ensure the right people have the right access to the right programs—and nothing more. This involves considerable manual work to verify that each individual has access only to the systems and documents necessary for their daily work.

We segment access so doctors and nurses in hospitals can only access specific systems they need. If they require access to additional resources, they must contact our service desk and apply for permission to access other documents, folders, programs, or applications.

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

Expert: We work closely with the Center for Cybersecurity in Denmark (CFCS), which operates under the Ministry of Defense. They are cybersecurity experts who analyze external threats to Denmark and different sectors. Whenever new threats emerge, they alert us and help prepare appropriate mitigations.

We also collaborate extensively with the European Union's agency called ENISA, which is their primary cybersecurity department. They produce many reports and sector-specific recommendations for ensuring cybersecurity. We stay current with their guidance and work with them to implement the latest security approaches.

Additionally, we coordinate with other regions and security entities, but our primary collaborations are with CFCS and the European Union.

Interviewer: Do you consider cyber attacks on the healthcare system as terrorism?

Expert: It depends on the motive. If the purpose is simply to disrupt our operations, I'm not sure I'd call it terrorism. If an attack were conducted by a state actor like the Russian government, it would be considered cyber warfare—essentially a declaration of war.

The threat of what we call "cyberterrorism" is actually quite low. Traditionally, terrorism requires a religious, ideological, or political purpose. Attacks intended merely to harm or destabilize Denmark wouldn't necessarily qualify as terrorism—they would be classified as cyber warfare.

The threat of cyber warfare is significant, and the general threat of cyber attacks is extremely high, largely due to the destabilized international situation with ongoing conflicts involving Russia and tensions with China.

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

Expert: We're working with the Center for Cybersecurity and the European Union to stay as current as possible on emerging attack methodologies, then rapidly developing mitigations for these threats.I anticipate that working with and countering artificial intelligence will dominate our focus in the coming years. We're already integrating AI features into our firewall systems to better detect and mitigate AI-based threats. However, AI is evolving extremely rapidly, making it challenging for anyone to keep pace. Artificial intelligence represents one of our biggest security concerns, so we're focusing on understanding what's possible and developing strategies to block, mitigate, or prevent malicious AI applications.