Interviewer: What are the biggest cybersecurity challenges currently faced by Denmark?

Researcher: The biggest challenge is ransomware. This is particularly important because small and medium enterprises (SMEs) in Denmark are being hit by different types of ransomware attacks, and most cybersecurity incidents fall into this category.

Another challenge relates to the changing global political landscape. We're relying too much on tools from other countries, which makes us vulnerable. We need to become more independent in our cybersecurity infrastructure.

Interviewer: You mentioned the political situation influences Denmark's cybersecurity. Can you specify how exactly, for example, how it changed three years ago when the war in Europe broke out?

Researcher: Yes, of course. We're relying on IT infrastructure and cybersecurity solutions from other countries. If we imagine that a provider stops supporting us, we wouldn't be able to get updates for antivirus or security solutions. This would put our entire public infrastructure at risk.

There are also challenges with state actors. For example, what if powerful states decide to leverage their influence over companies like Microsoft? In the past, we had good trust and relationships with these companies, but everything has changed now, particularly with the situations involving China and Russia.

This means we need to rely more on EU-based solutions because we can better control them and maintain good relationships as a European country. This applies to everything, including military capabilities. The world is changing, and we need to adapt.

Interviewer: How do you think organizations in Denmark approach cybersecurity compared to other countries?

Researcher: There are two approaches. Some organizations focus primarily on compliance—fulfilling rules and requirements such as implementing intrusion detection systems or connecting to specific networks. However, after meeting these compliance standards, many organizations don't effectively use the solutions they've implemented.

This happens because maintaining these systems is expensive in terms of human resources. Many security devices and solutions generate false positives—alerts that indicate something is wrong when it isn't—about 90-99% of the time. Organizations invest just enough to meet requirements by purchasing specific solutions, but then return to normal operations without fully utilizing these systems.

This is a significant challenge that we're trying to address in current projects.

Interviewer: What role does the Danish government play in protecting national cybersecurity?

Researcher: We're seeing progress. For example, there are grants specifically for cybersecurity projects that target collaboration between universities, researchers, and industry. Aalborg University recently announced new labs, with cybersecurity being considered a priority.

The government is investing, but we need more investment in solutions for Danish companies, especially SMEs with fewer than 50 employees. These cybersecurity solutions are often too expensive for smaller companies that may not yet be profitable. Denmark has many such SMEs that should be targets for support.

The government has been particularly focused on securing the healthcare sector, working to develop a more secure healthcare infrastructure. Municipal governments are also responding to changes and equipping themselves with security solutions, which is encouraging.

Interviewer: How effective are Denmark's cybersecurity regulations, such as the Network and Information Systems Directive, in protecting critical infrastructure?

Researcher: I'm not an expert in regulations, but as far as I know, Denmark has well-defined regulations. However, as I mentioned earlier, companies meet these regulations initially, but the challenge is monitoring ongoing compliance. Maintaining proper security is extremely expensive.

Interviewer: How would you describe the current status of the healthcare sector? Is it secure enough, or are there areas that need additional protection?

Researcher: In healthcare, they've started implementing cybersecurity solutions, including network security solutions like MDR (Managed Detection and Response). Some companies are providing comprehensive protection across the healthcare sector.

The main issue in healthcare is the use of legacy systems. These older systems remain in place because developing new ones is expensive. These systems were often developed by different companies and developers over the years, as healthcare has a long history of digitization going back 20-30 years. Because these legacy systems still work and would be expensive to replace, organizations keep them.

Recently, there have been efforts to improve security in healthcare systems. The main threats to healthcare are ransomware attacks, which encrypt valuable data, and data breaches.

Interviewer: What do you think is the main target when attackers want to attack the healthcare system?

Researcher: The most interesting target is the communication between patients and healthcare providers. We recently had a case where a phone number was blocked due to communication issues with mobile operators, causing chaos.

Now imagine if there was an attack—perhaps an interruption attack or DDoS (Distributed Denial of Service) attack—that made services unavailable to legitimate users. The impact would be

enormous. Everything in healthcare is online: visiting doctors, getting prescriptions, going to the pharmacy. If that system doesn't work and you can't get medicine, it creates chaos. The availability of services, particularly for emergency cases like the 1813 hotline that was recently blocked, is critical.

Interviewer: Do you know if that incident was a cyber attack and who was responsible?

Researcher: I don't think it was a cyber attack. It was a network issue. These systems are complex with parallel networks, and sometimes when operators like TDC try to update something, it causes problems. But this incident exposed vulnerabilities in our systems.

Interviewer: What are the main cyber threats targeting Danish companies and public institutions?

Researcher: Currently, ransomware is the primary threat. Two weeks ago, I hosted guests from a consultancy company that performs digital forensics for companies dealing with incidents. They reported that ransomware is the most common issue reported by Danish companies.

I believe it's Akira ransomware, a specific and sophisticated variant that has spread widely among Danish companies. Phishing is also very popular among APT (Advanced Persistent Threat) groups. They typically start with phishing—sending links that download ransomware and other malware. This remains extremely critical.

Interviewer: What are the biggest challenges in deploying AI-based security solutions in Denmark's industries?

Researcher: There are two main challenges. First, we don't yet have very effective AI-based security solutions because the cybersecurity field is extremely complex, involving diverse user behaviors. Sometimes cybersecurity companies use AI as a buzzword, but behind the scenes, their solutions are similar to manual processes or simple automated scripts rather than truly intelligent systems.

We're still far from fully autonomous systems that can detect issues, interpret them, and act independently. We're studying this area, but no company can yet claim to have truly intelligent security solutions.

Denmark is at the forefront of digitalization, so I believe Danish companies will quickly adopt effective AI security solutions when they become available. Danes readily embrace new technologies, which is why Denmark excels at digitalization. If good, affordable solutions emerge, they'll be quickly adopted across Danish companies.

Interviewer: Are Danish organizations adopting adversarial machine learning defenses to protect AI models from cyber attacks?

Researcher: That's a very good question. Regarding adversarial machine learning, most companies don't understand what it is. They're still struggling with traditional systems before even considering AI adoption.

Many AI-based companies offer solutions, but nobody studies how robust these solutions are. Danish companies purchase these solutions—for example, AI-based HR applications for filtering applicants—without understanding how they might be bypassed or how the systems were trained.

Training an AI model is challenging and expensive. It requires significant GPU resources, AI talent, large amounts of data, and time. Sometimes companies offer solutions after just one month of development, which suggests they haven't collected enough quality data or properly trained and tested their models.

Danish companies don't yet recognize adversarial machine learning as a threat because they're still trying to understand the fundamental importance of cybersecurity.

Interviewer: How do you assess Danish businesses' preparedness against cyber threats such as ransomware and phishing?

Researcher: This isn't based on a formal study, but I feel we're not ready or well-equipped. We often think cybersecurity threats affect others, not us—until we're affected, and by then it's too late. We need to invest more in awareness, especially among companies.

We're doing our best here to educate people. The younger generation seems to have a better understanding and sensitivity to these issues, while the older generation might be more reluctant to invest in cybersecurity.

Interviewer: How is AI being integrated into Denmark's cybersecurity defense strategies?

Researcher: AI will enter many industries, including cybersecurity, where it can play an important role. However, we shouldn't assume it can completely replace existing defense solutions.

AI can be used in radar systems to detect flying objects or for scanning underwater environments. The main challenge with AI in cybersecurity is false positives and the "black box" nature of deep learning and machine learning—we often don't know how they reach their conclusions.

This is why we need explainable AI that can justify its decisions based on facts. If an AI system detects an attack, it should explain the basis for that detection. This approach can help cybersecurity globally, not just in Denmark. We can't expect to enhance Danish defenses with AI in isolation because it affects the global ecosystem.

Interviewer: How do you see AI being used in offensive strategies?

Researcher: That's a good question about red teaming (offensive security). Unfortunately, generative AI systems with their APIs can be easily connected to other systems. Imagine an insider—someone within a company who is disgruntled or motivated by money—connecting systems to generative AI APIs and running commands or installing tools to scan other systems. The insider could watch and assist the AI agent when necessary. This scenario involving insiders and AI is particularly concerning.

Interviewer: How is Denmark contributing to research in AI-driven cybersecurity?

Researcher: Denmark is doing well in research at the intersection of AI and cybersecurity. We're seeing a shift in grants and funding, indicating that this field is a priority for investment. This is the right approach, but we need more involvement from companies, especially larger ones. While Novo Nordisk has some funding programs, they don't directly address cybersecurity. Other major companies like Ørsted could allocate funds specifically for cybersecurity and AI.

Interviewer: What opportunities exist for collaboration between academia, industry, and government in Denmark to improve cybersecurity?

Researcher: Academia can play a significant role in raising awareness through events, festivals, and other initiatives. We need budgets for these activities and incentives for company employees to attend.

We need an organized system for communicating real-time alerts and threats. If there's an attack on the water sector, for example, there should be a dedicated channel to spread this information, perhaps through a regular TV segment. Universities are ideal for this role because they operate as non-profit entities.

There should be more projects requiring three-way partnerships between universities, industry, and government. The government's role is regulation rather than building solutions, but they need to know how to regulate effectively. This requires collaboration with industry and academic partners in consortiums to establish metrics for regulation.

The government should also support Danish cybersecurity startups that reach a certain point but struggle to grow further. These companies are often acquired or unable to expand to other markets. We could form consortiums with other Nordic countries like Sweden and Norway to develop common solutions for these challenges.

Interviewer: How do you view digital solutions such as MitID? Is there any risk that AI-driven solutions can bridge the gap?

Researcher: There's definitely risk, especially since these solutions are developed by private sector companies, not government entities. A company in France is handling some development and maintenance of MitID.

Regarding AI, it depends on how we implement it. For example, malware on a mobile phone might open a browser and attempt to access an account, but multi-factor authentication provides

some protection. The process requires multiple steps: accessing the website, entering credentials, scanning a QR code, and entering a PIN.

In older versions with SMS-based authentication, it was easier to bypass security by taking over IP addresses. The current internet-based system is more secure. I remember there used to be an issue with notifications that could be accidentally accepted, but now notifications have been removed.

I don't think AI can significantly impact these systems currently. The main concerns are interruption attacks and DDoS attacks, but the future remains uncertain.

Interviewer: What trends in cybercrime should Denmark be most concerned about in the coming years?

Researcher: Threats against critical infrastructure, especially water systems and energy grids, are extremely important as they form the foundation of our society. There have been reports of attacks on water systems in Florida where attackers attempted to manipulate substances added to water treatment systems, threatening lives.

Energy grid security is equally important—imagine the metro losing power. These two areas should be top priorities for Denmark, even more so than healthcare.

Another concern is the security of underwater cables. The emergence of quantum computing is also worrying. Malicious actors might collect large amounts of encrypted data now that they can't access, but in ten years, quantum computing might allow them to decrypt this information and access sensitive data.

Interviewer: You mentioned water and energy infrastructure. Have you experienced or witnessed any attacks on these systems?

Researcher: Not in Denmark, but there have been cases in the US involving water systems. The Center for Cybersecurity in Denmark recently published a report about water systems becoming attractive targets for APT groups. This is particularly concerning because of Denmark's decentralized water management approach, with many small villages having their own community-based water management systems using traditional or older technology.

Interviewer: Would you say Denmark is very dependent on these resources? What would be the emergency response if Denmark lost access to power?

Researcher: We should have backup systems, and everyone should know what to do in such scenarios. I can't recall seeing any public information campaigns about what to do if mobile phones go down or during an electricity outage. I don't have any clear understanding of the procedures.

If these types of interruptions occur, the situation would be chaotic. Imagine traffic lights not working at intersections—nobody would know where to go. There needs to be more awareness in these areas, but I don't believe we have adequate preparation currently.