VATTENFALL

Vattenfall's views on Cybersecurity and Digital Policy

Introduction

Cybersecurity is a dynamic topic. Technological advances increase and policy development follows in lockstep. In addition, activity from malicious actors in the security domain further emphasise the importance of cybersecurity in the energy sector. For instance, consultancy *Cybersecurity Ventures* predicts that the costs for *ransomware* attacks will be around $265 billion (USD) annually by 2031[1]. Given the interdependencies and criticality of electricity supply to the economy and society, adequate security is vital. This applies to many aspects in the cyber domain, ranging from smart meters used by households, to complex systems used to control wind parks. Vattenfall considers cybersecurity a priority with corresponding cybersecurity standards. Indeed, as a vertically integrated utility, we recognise the need for a broad, holistic perspective to address the interdependencies efficiently in the electricity sector.

This paper outlines Vattenfall's commitment to cybersecurity and the company's perspective on policy design to support it.

Harmonisation of Regulatory Frameworks

The current regulatory frameworks for cybersecurity are diverse, and Vattenfall supports harmonisation to ensure a level playing field and exchange of best-practices. These help streamline implementation and foster collaboration and exchanges of best practices once implemented. The inclusion of ISO-standards in legislation is a good example of harmonisation of policy, that allows for both increased coordination between companies and national authorities and standardisation of security impact assessments.

However, Vattenfall advocates that care must be taken to ensure balanced regulation, avoiding excessive reporting obligations that could become a safety risk in themselves, due to the additional data being processed. Furthermore, compliance costs related to network codes any new administrative layers and reporting obligations should be minimised. This could be done by tasking a single agency with cybersecurity oversight.

Inclusiveness in policy-making

Vattenfall believes that all parties affected by regulation should be consulted during the drafting process. It is vital that all impacted parties have their voice heard in this complex and important matter, to ensure the quality of the regulatory framework and achieve a speedy implementation of policy.

[1] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

- Vattenfall is unwavering in its commitment to cybersecurity, and we understand the importance of a holistic approach to safeguard the electricity sector. We advocate for harmonized regulatory frameworks to enhance collaboration and share best practices
- We emphasize the importance of balanced regulation, avoiding excessive reporting obligations that could pose safety risks. We also aim to minimize compliance costs associated with new administrative layers..
- To do so, Inclusiveness in policy-making is crucial, ensuring that all affected parties have a say in shaping the regulatory framework. Vattenfall prioritizes cybersecurity and standards, recognizing the interconnectedness of the electricity sector's components. We will continue to improve cybersecurity measures to ensure the resilience of the energy system.

Vattenfall is a European energy company with approximately 19,000 employees. For more than 100 years we have electrified industries, supplied energy to people's homes and modernised our way of living through innovation and cooperation. Our goal is to make fossil-free living possible within one generation. Everything we do and the decisions we take shall lead to this goal. This is the basis of Vattenfall's strategy, and we advocate for a regulatory environment that makes this transition possible – in the energy sector and beyond in transport, industry etc

Contact : tim.koch@vattenfall.com
EU transparency ID number 12955024114-93