ATTACKS ON THE INDUSTRIAL INTERNET OF THINGS – DEVELOPMENT OF A MULTI-LAYER TAXONOMY

Abstract

The Industrial Internet of Things (IIoT) provides new opportunities to improve process and production efficiency, which enable new business models. At the same time, the high degree of cross-linking and decentralization increases the complexity of IIoT systems and creates new vulnerabilities. Hence, organizations are not only vulnerable to conventional IT threats, but also to a multitude of new, IIoT-specific attacks. Yet, a literature-based and empirically evaluated understanding of attacks on the IIoT is still lacking. Against this backdrop, we develop a multi-layer taxonomy that helps researchers and practitioners to identify similarities and differences between attacks on the IIoT. Based on the latest literature and a sample of about 50 attacks, we deductively and inductively determine attack characteristics and dimensions. We demonstrate the usefulness and practical relevance of our taxonomy by applying it to a real-world incident affecting a German steel facility. By combining IT security, IIoT, and risk management to form an interdisciplinary approach, we contribute to the descriptive knowledge in these fields. Industry experts confirm that our taxonomy enables a detailed classification of attacks, which supports the identification, documentation, and communication of incidents within organizations and their value-creation networks. With this, our taxonomy provides a profound basis for the further development of IT security management and the derivation of mitigation measures.

Keywords: Industrial Internet of Things, Industry 4.0, IT Security, Attacks, Taxonomy.