Cybersecurity im Energiesektor: Kritische Erfolgsfaktoren, Zukunftstrends und Handlungsempfehlungen

Masterarbeit

zur Erlangung des akademischen Grades „Master of Science (M. Sc.)“ im Studiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Münch Vorname: Jannik

[redacted]

Betreuerin: M. Sc. Jana Gerlach

Prüfer: Prof. Dr. Michael H. Breitner

Hannover, den 31.08.2022

Inhaltsverzeichnis

1. Einleitung

Im Hinblick auf die Cybersecurity des Energiesektors gab es am 23. Dezember 2015 einen populären Zwischenfall, der sich in der Ukraine ereignet hatte. An diesem Tag wurde die Stromversorgung in einem Teil des Landes für mehrere Stunden unterbrochen. Viele ukrainische Städte waren entweder vollständig oder teilweise von besagtem Ausfall betroffen. Schätzungen zufolge waren insgesamt 700.000 Ukrainer[2] von der Stromversorgung abgekoppelt. Gleichzeitig konnten die Betroffenen den verantwortlichen Energieversorgern, aufgrund einer Nichtverfügbarkeit der Unternehmenstelefondienste, keine Meldung darüber machen. Viele IT-Sicherheitsexperten und -Institutionen, unteranderem auch das Bundesamt für Sicherheit in der Informationstechnik (BSI), sind sich inzwischen sicher, dass ein gezielter Cyberangriff für diese Ereignisse verantwortlich war (vgl. Strathmann 2016; Tanriverdi 2016).

Inzwischen ist die Thematik Cybersecurity für lebenswichtige Infrastrukturen, wie es der Energiesektor zweifelsohne ist, stärker in den Fokus des öffentlichen Interesses und der Politik gerückt. Dieses lässt sich durch ein Statement des US-amerikanischen Präsidenten Joe Biden untermauern: „*I am committed to strengthening our cybersecurity by hardening our critical infrastructure against cyberattacks, disrupting ransomware networks, working to establish and promote clear rules of the road for all nations in cyberspace, and making clear we will hold accountable those that threaten our security*“ (The White House 2021). Auch in Deutschland hat sich 2021 der ehemalige Bundesminister des Innern und für Heimat Horst Seehofer zu dieser Thematik geäußert: „*Cybersicherheit ist kein notwendiges Übel, sondern Voraussetzung dafür, dass die Digitalisierung gelingt*“ (BMI 2021).

Der zuvor geschilderte Cybervorfall im Ausland und die beiden Zitate offenbaren gemeinschaftlich die Problematik, dass der Energiesektor ein potentiell attraktives Angriffsziel für beispielsweise politisch und/oder finanziell motivierte Cyberkriminelle darstellt und in Zukunft möglicherweise auch deutsche Energieunternehmen verstärkter in den Fokus von Hackergruppen rücken könnten. Dementsprechend ist es wichtig, dass sich der deutsche Energiesektor ganzheitlich mit dieser Thematik beschäftigt, damit ein Vorfall wie in der Ukraine 2015 für Deutschland vermieden werden kann.

Die Motivation dieser Thesis besteht darin, dass durch adäquate Forschungsarbeit ein hilfreicher Beitrag zur Unterstützung der Cybersecurity von deutschen Energieunternehmen erarbeitet wird. Hierzu sollen kritische Erfolgsfaktoren, die zum

[2] Aus Gründen der besseren Lesbarkeit wird in dieser Masterarbeit das generische Maskulinum benutzt. Dabei sind alle Geschlechteridentitäten als mitgemeint anzusehen.

Gelingen der Cybersecurity im Energiesektor beitragen können, mithilfe von Literatur und qualitativer Forschung erarbeitet werden. Weiterhin ist ein qualitativer Blick in die Zukunft zur Herausstellung von Trends, bedingt durch die hohe Aktualität bzw. Wandlungsgeschwindigkeit der Thematik unabdinglich. Letztlich sollen auf Grundlage der gesammelten Erkenntnisse breitgefächerte Handlungsempfehlungen ausgesprochen werden.

Abgeleitet aus dieser Problematik lassen sich drei explizite Forschungsfragen formulieren, die im Verlauf dieser Masterarbeit beantwortet werden:

(1) Was sind kritische Erfolgsfaktoren (KEFs) von Cybersecurity im Energiesektor?
(2) Welche Zukunftstrends lassen sich hinsichtlich der Cybersecurity im Energiesektor beobachten?
(3) Welche Handlungsempfehlungen können bezüglich Cybersecurity im Energiesektor ausgesprochen werden?

Zur systematischen Aufarbeitung der drei Forschungsfragen wurde diese Masterarbeit in acht Hauptkapitel unterteilt. Anknüpfend an das erste einleitende Kapitel wird im nächsten Schritt auf Theoretische Grundlagen, welche der Schaffung eines Verständnisfundaments dienen, eingegangen. Hierbei wird auf die Themenkomplexe Cybersecurity, Cyberangriff, KEF und kritische Infrastrukturen (KRITIS) eingegangen. Zuzüglich werden weitere Kurzdefinitionen gegeben. Das dritte Kapitel beschäftigt sich mit dem Design Science Research (DSR) nach Hevner, in welchen die gesamte Thesis eingebettet wurde. Im vierten Kapitel wird in vier Teilabschnitten ein systematischer Literaturrückblick anhand zweier wissenschaftlicher Artikel von Webster und Watson gegeben. Das fünfte Kapitel widmet sich der Thematik der Experteninterviews und thematisiert die Gestaltung dieser, der Expertensuche, der Durchführung des Transkriptionsprozesses und erklärt die Vorgehensweise der qualitativen Inhaltsanalyse (QIA) nach Mayring. Im sechsten Hauptkapitel wird zunächst die relevante Literatur bzgl. allgemeiner KEFs von Cybersecurity ausgewertet. Im Anschluss daran werden die gesamten Inhalte der elf Experteninterviews mithilfe der QIA ausgewertet. Letztlich wird im dritten Teilabschnitt des sechsten Kapitels eine Ergebnistabelle von auf den Energiesektor angepassten KEFs geliefert. Im vorletzten Kapitel werden die gesamten erarbeiteten Ergebnisse kritisch diskutiert und die Forschungsfragen umfassend beantwortet. Zum Abschluss der Thesis wird ein Fazit gegeben.

Herstellern verschiedenste Siegel für die jeweiligen Produkte geben, die ein gewisses Sicherheitsniveau garantieren. Die kleineren und technisch unerfahrenen Energieunternehmen würden von dieser Transparenz und dem Garantieversprechen enorm profitieren. Die abschließende Handlungsempfehlung ist, dass die KEFs dieser Thesis praktische Anwendung bei den Energieunternehmen finden sollten. Weiterhin sollten künftige Forschungspapiere aufbauend auf dieser Arbeit weiterführende Untersuchungen forcieren. Die Welt der Cybersecurity und die des Energiesektors drehen sich kontinuierlich weiter und auch die Erforschung auf diesem Gebiet muss stetig sowie bedarfsorientiert stattfinden.

8. Fazit

Die Thematik Cybersecurity im Energiesektor wurde in dieser Thesis ausführlich aufgearbeitet, indem Literaturforschung sowie qualitative Forschung in Form von Experteninterviews betrieben wurde. Mithilfe der Literatur konnten elf initiale KEFs von Cybersecurity ausgearbeitet werden. Anknüpfend daran wurden durch elf Experteninterviews neue Eindrücke, die explizit für den Energiesektor Gültigkeit haben, gewonnen. Aufbauend auf den Erkenntnissen dieser beiden Auswertungen und der anschließenden Ergebniszusammenführung, sind 15 KEFs seitens Cybersecurity für den Energiesektor expliziert worden. Diese KEFs wurden in die drei Dimensionen ‚People', ‚Process' und ‚Technology' einsortiert. Zu der Kategorie ‚People' gehören die KEFs ‚Cybersecurity-Kultur', ‚Top Management Support', ‚Struktur', ‚Wissen & Awareness', ‚Dienste (intern/extern)', ‚Spezialisten (intern/extern)' und ‚Gesetzgeber'. Die ‚Prozessdimension' umfasst abschließend ‚Managementprozesse', ‚Entwicklungsprozesse', ‚Prüfprozesse & Dokumentation (intern/extern)' sowie ‚Austauschprozesse'. Die erforschten technologischen KEFs bzgl. Cybersecurity des Energiesektors sind ‚adäquate IT & OT', ‚Security Infrastruktur', ‚Security by Design' und ‚Automatisierung & Dezentralität'. Eine wichtige auszusprechende Handlungsempfehlung für Energieunternehmen besteht in der Umsetzung dieser 15 KEFs. Die relevantesten Zukunftstrends, die Gültigkeit für den Energiesektor haben sind die Digitalisierung, Dezentralisierung, Automatisierung, Cloudifizierung und Virtualisierung. Außerdem kommen in diesem Zuge die Strukturwandlungsaspekte, bedingt durch die Energiewende hinzu. Dementsprechend werden immer mehr (erneuerbare) Energiegewinnungsanlagen im Feld verteilt. Des Weiteren wird sich die Datenmenge die der Energiesektor verarbeiten muss erhöhen. Es ist jederzeit zu beachten, dass sich die Cyberkriminellen auf diese Veränderungen einstellen und versuchen werden über andere Einfallstore, wie z.B. über Fernwartungszugänge, Schäden hervorzurufen. Hieraus leitet sich die weitere essentielle Handlungsempfehlung ab, dass der Energiesektor permanent die Märkte, die eigene Lieferkette und die Cyberangriffsstrategien der Kriminellen beobachten

muss. Auch der Energiesektor ist einem ewigen Wettrüsten mit Cyberkriminellen ausgesetzt. Daher ist es anzuraten sich mit anderen Akteuren und den gesetzgebenden Instanzen in Form des BSI und der BNetzA auszutauschen. Außerdem müssen die Energieunternehmen in erster Linie proaktiv die Cybersecurity-Grundlagen umsetzen, bevor neuartige KI-Algorithmen installiert werden können. Hierzu gehören beispielsweise ein ISMS und ein BCMS, welche unter Zuhilfenahme von Standards und externen Fachleuten aufgebaut werden sollten. Die externen Spezialisten sind besonders für die vielen kleinen Energieunternehmen ein hochbrisanter Erfolgstreiber. Hinzu kommt, dass die Energieunternehmen im Zuge der angestrebten Automatisierungen, mehrfache Redundanzen bzgl. ihrer Informationsverbindungen aufbauen sollten. In Anbetracht dessen muss auch für Nachwuchskräfte im Bereich der Cybersecurity des Energiesektors gesorgt werden.

Zum Abschluss dieser Masterarbeit werden weitere auf diesen Ergebnissen aufbauende Forschungen empfohlen, um die sich stetig veränderbaren Aspekte von Cybersecurity im Energiesektor zu berücksichtigen und den Praktikern auch künftig Entscheidungshilfen geben zu können. Es muss alles darangesetzt werden, dass ein Vorkommnis wie in der Ukraine 2015 verhindert wird, sodass unser Alltagsleben keine weitreichenden Einschränkungen erfahren muss.

„*Im Moment gibt es immer noch mehr Stromausfälle, die durch Eichhörnchen verursacht werden als durch Hacker. Sollte auch weiterhin so bleiben*“ (B10, Anhang E.10). Die Hauptnachricht des Zitats, dass Hacker bzw. Cyberkriminelle bisher keine weitreichenden Schäden verursacht haben, sollte für alle Unternehmen des Energiesektors, zum jetzigen und zukünftigen Zeitpunkt, im Zentrum des Interesses stehen.