Cybersecurity im Energiesektor

Eine Studie der Frankfurt School und der 4C GROUP AG

München, November 2022

Management Summary

Struktureller Wandel in der OT

Besonders im KRITIS-Umfeld findet durch die immer weiter fortschreitende Konvergenz von IT- und OT-Systemen ein deutlicher struktureller Wandel statt. Der ständig steigende Bedarf an quantitativen Analysen aus dem Betrieb führt dazu, dass immer mehr neue Technologien wie Künstliche Intelligenz und Cloudcomputing im hochkomplexen OT-Umfeld Einzug halten. Auch das sog. Industrial Internet-of-Things (IIoT), in dem industrielle Steuerungsanlagen miteinander vernetzt werden, öffnet einen vorher nie dagewesenen Angriffsvektor für Cyberangriffe.

Forschungsdesign & Methodik

Der aktuelle Forschungsstand zu Cybersecurity Ansätzen im deutschen Energiesektor ist stark begrenzt. Aus diesem Grund wurden im Rahmen dieser Studie qualitative Interviews mit insgesamt 12 Fachexperten (z.B. Leiter Prozessdatentechnik) der 30 größten Stromnetzbetreiber aus dem Bereich Telekommunikationsinfrastruktur geführt. Die Interviews und die Antworten aus den Interviews wurden in Kooperation mit der Frankfurt School durchgeführt, kodiert, ausgewertet und in der vorliegenden Unterlage zusammengefasst.

Studienergebnisse

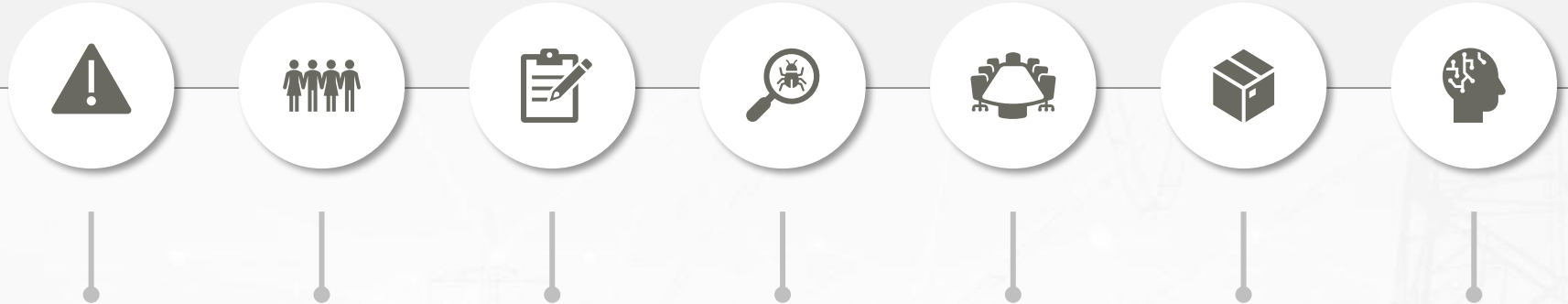
Mit Hilfe von sieben offenen Fragestellungen wurden im Rahmen der Studie praktische Ansätze im Bereich Cybersecurity diskutiert. Die Fragen beschäftigten sich mit der Anzahl und Intensität von Cyberangriffen, den Verantwortlichkeiten, Steuerungsmechanismen, der Informations-beschaffung, dem Bewusstsein des Top-Managements, Risiken in der Lieferkette sowie Zukunftstechnologien und Konzepten. Die wesentlichen Kerninhalte der Antworten haben wir für Sie analysiert und auf den folgenden Seiten dieser Unterlage zusammengefasst.

Bausteine für den Erfolg

Basierend auf den Erkenntnissen zu praktischen Ansätzen im Bereich Cybersecurity konnten vier wesentliche technische und organisatorische Bausteine für den Erfolg abgeleitet werden. Zu diesen zählt die Schärfung und Sicherung des Bewusstseins für Cybersecurity des Top-Managements, die enge Zusammenarbeit mit Lieferanten und Herstellern, die Etablierung eines zentralen OT-CERTs sowie abschließend die proaktive und kontinuierliche Weiterentwicklung aller Cybersecurity Maßnahmen

© 2022 | 4C GROUP AG

Übersicht der Interviewschwerpunkte



Relevanz Cyberattacken

Cybersecurity Rollenverteilung

Steuerungs-mechanismen

Überblick Cyberrisiken

Awareness Top-Management

Risiken der Lieferkette

Zukunfts-technologien

© 2022 | 4C GROUP AG

Technische & organisatorische Bausteine für den Erfolg

Schärfung und Sicherung des Bewusstseins des Top-Mgmts.

- Im Rahmen der Studie hat sich deutlich herausgestellt, dass ein **hohes Bewusstsein** des Top-Managements die Sicherstellung der Cyber-Resilienz erleichtert
- Durch die aktuellen geopolitischen Herausforderungen sind geeignete **Cybersecurity Abwehrmaßnahmen** und ein hohes Bewusstsein in der Unternehmensführung essentiell

- Machen Sie Ihrer Geschäftsführung (weiterhin) bewusst, welche **große strategische Relevanz** das Thema Cybersecurity besitzt
- Nur durch **regelmäßigen Kontakt** stellen Sie sicher, dass Ihr Top-Management die Notwendigkeit sieht, ausreichende Ressourcen zur **Aufrechterhaltung** und **Weiterentwicklung** der Cybersecurity Resilienz Ihres Unternehmens bereitzustellen

Reduzieren von Risiken in der Wertschöpfungskette

- Der **Einsatz von Lieferanten** in der Wertschöpfungskette innerhalb von kritischen Infrastrukturen bringt viele Chancen aber auch Risiken mit sich
- Eine **tiefe Integration** in die Wertschöpfungskette kann zu erheblichen **Cybersecurity Herausforderungen** führen, wenn der Lieferant oder deren Kommunikationswege kompromittiert werden

- Achten Sie auf ausreichende **Nachweise und Qualifikationen** im Bereich Cybersecurity (z.B. durch ein Self-Assessment) & halten Sie die **Abhängigkeiten zu Lieferanten** möglichst gering
- **Überprüfen** Sie regelmäßig die Cybersecurity Resilienz der Lieferanten durch **Audits,** erproben Sie **Krisenszenarien**, um bei Bedrohungslagen richtig agieren zu können und stellen Sie sicher, Kommunikationsstrecken jederzeit trennen zu können („**Red Button**“)

Etablierung eines zentralen OT-CERT

- Das OT-CERT stellt die **zentrale Instanz** zur Sammlung, Aggregierung und Klassifizierung aller Cybersecurity Informationen für die OT dar
- Durch das gegebene branchen- und produktionsspezifische Knowhow wird sichergestellt, dass unternehmensrelevante **Bedrohungslagen frühzeitig erkannt** & sachgerecht darauf reagiert werden kann

- Etablieren Sie in Ihrem Unternehmen die **Funktion des „OT-CERTs“** bzw. bauen Sie diese weiter aus, um auf eine **zentrale und zuverlässige Anlaufstelle** für produktionsrelevante Bedrohungslagen zurückgreifen zu können
- Setzen Sie bewusst auf **Fachexperten aus dem Bereich der Produktionsdaten- & Nachrichtentechnik**, um bestmöglich auf die Besonderheiten im Produktionsumfeld eingehen zu können

Proaktive Weiterentwicklung Cybersecurity Maßnahmen

- Trotz der hohen strategischen Relevanz ist Cybersecurity **ein technologienahe Disziplin**, die einem stetigen Wandel unterliegt und kontinuierlich weiterentwickelt und angepasst werden muss
- Nur durch das **proaktive Weiterentwickeln** der Cybersecurity Maßnahmen im Unternehmen kann sichergestellt werden, auch in Zukunft vor Cyberangriffen geschützt zu sein

- Durch die stetig steigenden Bedrohungslage müssen Sie sicherstellen, dass sich Ihre Cybersecurity Maßnahmen stets auf **dem aktuellen Stand der Technik** befinden
- Evaluieren Sie **regelmäßig aktuelle Technologien und Konzepte** wie z.B. NextGen Firewalls, Intrusion Detection Systeme, Zero Trust, um neue Angriffsvektoren zu minimieren

4C Handlungsempfehlung

© 2022 | 4C GROUP AG

Martin Stephany
Partner
martin.stephany@4cgroup.com
+49 173 346 58 29

Florian Zemler
Managing Consultant
florian.zemler@4cgroup.com
+49 173 346 58 43

Yannick Lang
Frankfurt School
yannick.lang@fs-students.de
+49 160 968 874 62

© 2022 | 4C GROUP AG

Impressum | 4C GROUP AG

Office München
Elsenheimerstraße 55a
80687 München

Office Frankfurt
Senckenberganlage 19
60325 Frankfurt

Office Berlin
Französische Straße 8
10117 Berlin

Office Düsseldorf
Sky Office, Kennedydamm 24
40221 Düsseldorf

4cgroup.com