Integration eines Managed Cyber Defense Centers in die IT-Architektur eines Rechenzentrenbetreibers

Masterarbeit

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

vorgelegt von

Name: Göhner Vorname: Bastian Alexander

[redacted] [redacted] [redacted] [redacted]

Prüfer: Prof. Dr. rer. nat. Michael H. Breitner

Ort, den* Hannover, den 27.09.2019

*(Datum der Beendigung der Arbeit)

Inhaltsverzeichnis

1 Einleitung

Sicherheitsvorfälle in der Informationssicherheit und Netzwerkkommunikation gehören zu den weltweit größten Geschäftsrisiken.[1] Auch in Deutschland steht die Gefahr durch Cyberattacken im Fokus des Risikomanagements von Unternehmen. So sind deutschlandweit über 800 Millionen Schadprogramme im Umlauf und pro Tag tauchen 390.000 neue Varianten eines solchen Programmes auf.[2] Angriffsziele von Cyberattacken sind dabei vor allem Unternehmen im Bereich der Informationstechnik (IT).[3] Neben Unternehmen, können auch IT-Systeme privater Haushalte, Behörden und nicht staatlicher Organisationen betroffen sein. Die IT-Sicherheitslücken sowie die Angriffsklassen variieren dabei sehr stark voneinander. So traten ab 2017 verstärkt neue Versionen der Ransomwares WannaCry, Bad Rabbit und Petya auf. Auch Schwachstellen, die sich nicht durch Patches oder Updates beheben lassen, betreffen weltweit IT-Systeme. So wurden Hardware-Sicherheitslücken der Hersteller von Mikroprozessoren Intel Corp., AMD Corp. und ARM Ltd. Anfang 2018 unter den Namen Spectre und Meltdown bekannt und betrafen fast alle Mikroprozessoren auf dem Markt.[4] Auch können durch die sich ausweitende digitale Vernetzung und Cloud-Nutzung stetig mehr Geräte über das Internet erreicht werden, wodurch sich der potenzielle Angriffsvektor massiv erhöht. Eine Gefahr hierbei können Distributed Denial of Service Attacken sein, bei denen Internet of Things-Geräte fremdgesteuert und zu sogenannten Bot-Netzen zusammengeschlossen werden können.

Durch die zunehmende Professionalisierung der Angreifer und dem Anstieg von komplexen Sicherheitslücken in Hardware und Software nimmt die Bedeutung von unterschiedlichen Methoden und Technologien zur (Netzwerk-) Absicherung zu. Da ein vollständiges Erreichen von IT-Sicherheit in der Praxis nicht möglich ist, haben Maßnahmen in der IT-Sicherheit häufig das Ziel, Risiken zu reduzieren und Aufwände für den Angreifer zu erhöhen. So werden im Umgang mit IT-Systemen oft eine Vielzahl von Sensoren und Überwachungsmöglichkeiten eingesetzt, um Sicherheitsvorfälle frühzeitig und präzise zu erkennen.[5] Diese Detektion ist eine wichtige Voraussetzung für die Reaktion auf IT Sicherheitsvorfälle.

Eine Möglichkeit zur Überwachung von Netzwerkkommunikation ist der Aufbau eines Cyber Defense Centers (CDC). Die Motivation dieser Arbeit besteht darin, einen Proof of Concept für die Integration eines CDC bei dem Rechenzentrenbetreiber OEDIV KG durchzuführen. Durch ein CDC soll insbesondere die Informationssicherheit der

[1] Vgl. Allianz SE (Hrsg.) (2019).
[2] Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2018), S. 50.
[3] Vgl. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (2018), S. 10-11.
[4] Vgl. Eckert, C. (2018), S. 83.
[5] Vgl. Eckert, C. (2018), S. 1.

Rechenzentren-Services gewährleisten werden, da als Rechenzentrenbetreiber die Verfügbarkeit der Systeme und die Vertraulichkeit sowie Integrität der Daten(übertragung) höchste Priorität hat.

Das CDC soll gemeinsam mit dem Partnerunternehmen 8com GmbH als Managed Service betrieben werden. Das Ziel dieser Arbeit ist es daher, zu prüfen, wie sich ein CDC in die IT-Architektur eines Rechenzentrenbetreibers integrieren lässt. Hieraus lässt sich die folgende Forschungsfrage ableiten:

Wie lässt sich ein Managed Cyber Defense Center

in die IT-Architektur eines Rechenzentrenbetreibers

integrieren?

Das Vorgehen, um die Forschungsfrage zu beantworten, ist in Abbildung 1 dargestellt. Im folgenden zweiten Kapitel werden die theoretischen Grundlagen des Themas behandelt. Hierbei werden zunächst relevante Begriffe und Theorien der Informationssicherheit definiert bzw. erläutert. Des Weiteren wird anhand einer Literaturanalyse in die Thematik CDC und Security Information and Event Management (SIEM)-Technologie eingeführt.

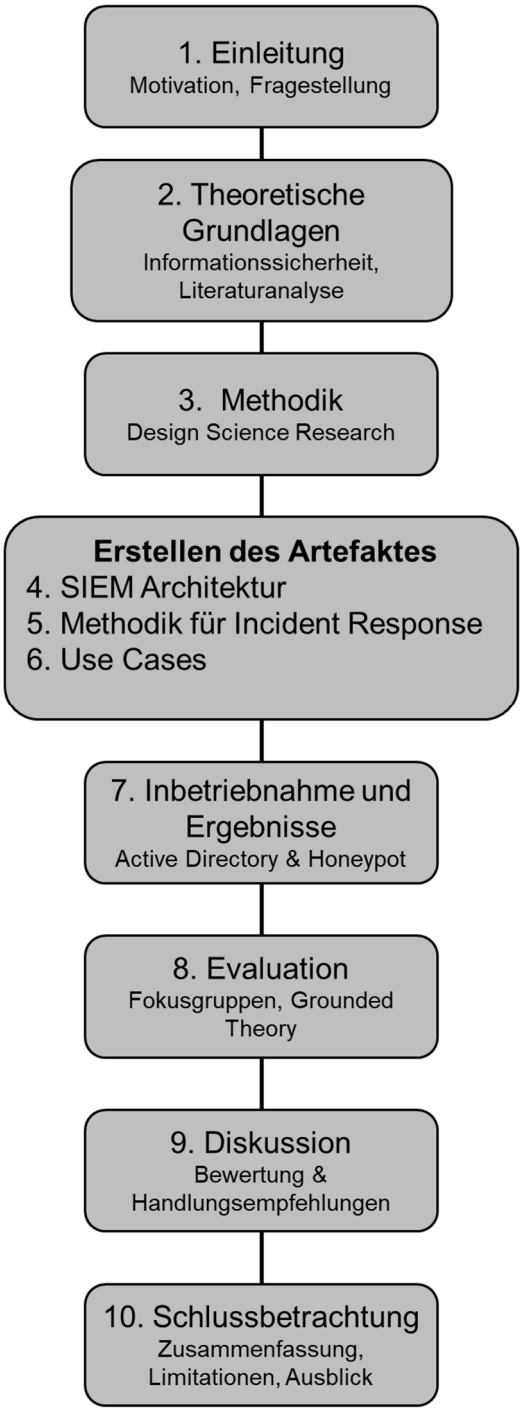

Abbildung 1: Struktur und Vorgehen. Quelle: Eigene Darstellung.

Basierend auf dem Grundlagenteil wird das in dieser Arbeit verwendete Forschungsdesign „Design Science Research“ in Kapitel 3 vorgestellt und in diesem Zusammenhang die Entwicklung eines Artefakts beschrieben. Der Hauptteil dieser Arbeit besteht in dem Aufbau eines CDC für den Testbetrieb (das Artefakt). In diesem Rahmen sollen u.a. die Identifizierung und Anbindung der Logquellen vollzogen sowie der Ist-Zustand des Unternehmens und die Besonderheiten des Netzwerkverbundes erfasst werden, um spezielle Anforderungen an das Artefakt zu schlussfolgern. Zur Infrastruktur des CDC, also dem Artefakt, gehören weiterhin die Architektur für ein

SIEM, welche in Kapitel 4 erarbeitet wird. Ferner wird im Zuge des Artefaktes in Kapitel 5 eine Methodik für die Incident Response entwickelt sowie in Kapitel 6 Use Cases für ein CDC formuliert. Die Überführung des Artefaktes in den Produktivbetrieb soll in Kapitel 7 dargestellt werden. Für die Datenevaluation und Theoriebildung wird die Methodologie der Grounded Theory verwendet. Für die Datenevaluation werden ferner Transkriptionen von zwei durchgeführten Fokusgruppen verwendet. Das Vorgehen nach der Grounded Theory Methodologie und die konkrete Anwendung wird in Kapitel 8 gezeigt. Die Ergebnisse dieser Arbeit werden in Kapitel 9 diskutiert und dienen als Grundlage für einen Proof of Concept (PoC). Das letzte Kapitel fasst die Ergebnisse dieser Arbeit zusammen und gibt einen Ausblick auf weitere Vorgehens- und Forschungsmöglichkeiten.

2 Theoretische Grundlagen

2.1 Informationstechnik und -sicherheit

Ein Cyber Defense Center befasst sich mit der Sicherheit von informationstechnischen Systemen im Rahmen der Datenverarbeitung. In diesem Zusammenhang sollen deshalb zunächst die Begriffe Daten, Informationen, IT-System und Informationssicherheit definiert werden.

Daten und Informationen

Häufig werden die Begriffe Daten und Informationen synonym verwendet. Im Folgenden soll deshalb auf den Aspekt der Differenzierung zwischen Daten und Informationen eingegangen werden.

Daten gelten als entscheidender Rohstoff für die Zukunft. Sie liegen immateriell vor und sind nach Mertens (2017) „maschinell verarbeitbare Zeichen […], die Objekte und Objektbeziehungen der Realwelt durch ihre Merkmale beschreiben und damit repräsentieren.“[6] Damit unterscheiden sich Daten von anderen Rohstoffen, die in der Regel organischen oder anorganischen Ursprungs sind. Mertens definiert weiterhin Kriterien, nach denen Daten beschrieben werden können. So können Daten, wie in Tabelle 1 dargestellt, nach Datentyp (numerisch, alphabetisch, alphanumerisch), Erscheinungsform (akustisch, bildlich, schriftlich), Formatierung (strukturiert, semistrukturiert, unstrukturiert), Rang im Verarbeitungsprozess (Eingabe-, Ausgabedaten) oder ihrem Verwendungszweck (Stamm-, Bewegungs-, Vormerksdaten) klassifiziert werden.[7]

[6] Mertens, P. / Bodendorf, F. / König, W. et al. (2017), S. 36.
[7] Vgl. Mertens, P. / Bodendorf, F. / König, W. et al. (2017), S. 36-37.

angeraten. Hierbei zeigte sich, dass dies durch eine Vorselektion der Logdateien sichergestellt werden kann. Außerdem konnten so die Datenmenge reduziert und nur die für die Verarbeitung notwendigen Daten betrachtet werden (Datensparsamkeit). Da auch eine automatische Klassifizierung der Events stattfindet und Daten wie IP-Adresse, Computername und der Nutzername verarbeitet werden, ist für die Zukunft eine Risikofolgenabschätzung nach Art. 35 der DSGVO zu empfehlen. Hierbei wird das Risiko einer Datenverarbeitung im Sinne des Datenschutzes bewertet und ggf. die Datenverarbeitung untersagt bzw. unter Änderungen gestattet.

Schlussendlich lässt sich feststellen, dass dem Bereich Cyber Abwehr durch ein CDC insgesamt ein unterstützender Effekt beikommt. Unternehmen der IT-Branche können durch ein CDC die steigenden Anforderungen besser organisieren sowie dynamischer auf Incidents reagieren. Zukünftige Risiken können reduziert werden, indem Prozesse für ein CDC entwickelt und etabliert werden. Die Relevanz für technische und organisatorische Maßnahmen zum Schutz vor Cyber Bedrohungen wird durch die zunehmende Professionalisierung der Angreifer und technische Innovationen auch zukünftig steigen. Vor diesem Hintergrund ist ein CDC deshalb ein effektives Mittel, um besseren Schutz der Informationssicherheit für ein Unternehmen zu generieren. Für den Anwendungsfall des in dieser Arbeit behandelten Unternehmen, ist der Erfolg des CDC letztlich erst nach einer vollständigen technischen Umsetzung und organisatorischen Einbettung abzusehen.

10 Schlussbetrachtung

10.1 Zusammenfassung

Ziel dieser Arbeit war es, ein Cyber Defense Center erfolgreich in die IT-Architektur eines Rechenzentrenbetreibers zu integrieren. Hierfür wurden zunächst die theoretischen Grundlagen der Informationssicherheit erläutert. Hinsichtlich der Schutzziele der Informationssicherheit zeigte sich hierbei, dass ein CDC dazu beitragen kann, die Schutzziele besser zu erfüllen. Aufbauend darauf wurde in einer Literaturanalyse nach Webster und Watson relevante Literatur zum Themenbereich CDC systematisch untersucht. In diesem Rahmen wurden hinsichtlich des CDC Konzepte, Strategien, SIEM-Technologie und das Log Management erläutert. Ferner konnten Forschungsschwerpunkte sowie -lücken identifiziert werden, aus der sich insbesondere Implikationen für die weitere Bearbeitung der Forschungsfrage ableiten ließen. Es konnte festgestellt werden, dass zu dem Thema CDC eine Vielzahl an Best Practice-Sammlungen und Frameworks existieren. Die genaue Erläuterung dieser Frameworks wäre jedoch nicht zielführend gewesen und hätte einen zu großen Teil dieser Arbeit eingenommen. Trotz dessen ist die Rolle von Frameworks ein zentrales Thema beim Aufbau eines CDC oder SIEM. Weiterhin konnte gezeigt werden, dass

speziell zu dem Thema Managed CDC wenig konkrete Best Practices existieren. Dies liegt daran, dass Unternehmen oft eigene CDC aufbauen, anstatt dies mit einem Partnerunternehmen zu tun. Auch beschränkt sich ein großer Teil der Literatur auf die Rollenverteilung des Teams innerhalb eines CDC oder den Umgang mit einem speziellen Tool, wie etwa eines SIEM.

Die Forschungsmethode des Design Science Research hat sich insofern als nützlich erwiesen, als dass ein deduktiver mit einem induktiven Forschungsansatz verknüpft werden konnte, um ein Artefakt in Form eines CDC zu erstellen. In der Ist-Erhebung des Unternehmensnetzwerkes konnten Erfahrungen dazu genutzt werden, um Verbesserungspotentiale für das CDC zu identifizieren, die sich für den späteren Produktivbetrieb bzw. die Anwendung des CDC nutzen lassen.

Ein Schwerpunkt dieser Arbeit lag in der Entwicklung einer Methodik für das Incident Response. Zu diesem Zweck wurden mit den Use Cases bzw. dem Incident Response Plan eigene Abläufe entwickelt. Anhand des Incident Response Plans bzw. Use Cases ließ sich ein kontrolliertes und standardisiertes Vorgehen für Incidents etablieren. Nach einer Einführung bzw. dem Go- Live konnten die Use Cases in der Praxis erprobt werden. Dabei zeigte sich u.a. das Potential eines CDC, sowohl als Frühwarnsystem als auch für den Umgang mit Incidents. Eine Aussage über den zukünftigen Erfolg des CDC ließ sich angesichts der noch fehlenden Einbindung von Kundensystemen jedoch schlussendlich noch nicht treffen.

10.2 Limitationen

Implikationen für die Bearbeitung der Fragestellung ergaben sich aus den dieser Arbeit unterliegenden Limitationen. In diesem Kapitel werden die identifizierten Begrenzungen erläutert.

Die Literaturanalyse nach Webster und Watson hat gezeigt, dass zu dem Themengebiet CDC eine Vielzahl an Best Practice-Sammlungen und Frameworks existieren, die vielfach heuristische Methoden zur Entwicklung von Use Cases erörtern. Aus Datenschutzgründen sowie Verarbeitungsverträgen mit Kunden, musste der Umfang der Implementierung des CDC und damit die Anwendung der Use Cases jedoch auf das Unternehmensnetzwerk der OEDIV KG beschränkt werden. Somit konnten die in der Literatur empfohlenen Best Practices nur teilweise Anwendung finden. Dabei konnten vor allem Use Cases, die in Shared Netzwerken (z.B. Firewall-Umgebungen) angewendet werden, noch nicht implementiert werden, da die Datenverarbeitung seitens dem Partnerunternehmen 8com GmbH nicht von den Kundenverträgen abgedeckt wurde.

Insgesamt ist diese Arbeit durch eine spezielle Sichtweise limitiert, da sie allein die relevanten Daten der OEDIV KG thematisiert. Da andere Unternehmen nach verschiedenartigen Frameworks oder Unternehmensarchitekturen aufgebaut sind, ist über eine generelle Übertragbarkeit der Ergebnisse keine gesicherte Aussage zu treffen. Zudem konnten nicht alle entwickelten Use Cases in der Praxis getestet werden, da der Grad der technischen Umsetzung zum Abschlussdatum dieser Arbeit noch nicht vollzogen wurde. Somit konnte keine Revision aller Use Cases stattfinden. Hierfür empfiehlt es sich, weitere Forschung zu Konzepten der Validierung von Use Cases zu betreiben.

10.3 Ausblick

Im Umfang der vorliegenden Arbeit wurden Möglichkeiten der Integration eines Cyber Defense Centers evaluiert. Als wichtiges Ergebnis kann die Umsetzung von zuvor definierten Use Cases und damit der Beginn der Einführung eines CDC genannt werden. Hiermit wurde die Basis für die nächsten Schritte gelegt wie die Implementierung auf Kunden-Systemen. Das weitere Vorgehen und dafür erforderliche Forschungsperspektiven werden im Folgenden vorgestellt.

Zunächst bietet der Erfahrungsgewinn aus der Anbindung des CDC an das Unternehmens-Netzwerk eine Grundlage für weitere Forschungsmöglichkeiten. Die Integration zeigte, dass Incidents nicht nur schneller erkannt, sondern auch besser analysiert werden konnten. Weiterhin wurde festgestellt, dass hierfür eine notwendige Anpassung der Parameter und Filter des CDC essenziell für den Erfolg ist. Dieses Optimierungsverfahren erfolgte nach dem „Trial and Error“- Prinzip. Eine systematische Validierung der darauf beruhenden Parameter-Einstellungen nach wissenschaftlichen Forschungsmethoden wäre wünschenswert, da sie weitere Optimierungspotentiale identifizieren kann.

Eine zusätzliche Optimierung der CDC Parameter ergibt sich durch das Sammeln von Erfahrungswerten in der praktischen Anwendung. Durch die Einarbeitung sowie Training und Gewöhnung der Mitarbeiter an die neuen Prozesse können weitere Verbesserungspotentiale (organisatorische sowie technische) identifiziert werden. Denkbar wären hierbei sowohl Evaluierungen des Zusammenspiels verschiedener Unternehmensbereiche und -ebenen als auch Möglichkeiten der Automatisierung in einem CDC.

Mit der Formulierung von Use Cases ist ein standardisiertes Vorgehen für Incidents eingeführt worden. Die Entwicklung dieser Use Cases beruhen sowohl auf Empfehlungen aus der wissenschaftlichen Literatur („Best Practices“) als auch auf

Erfahrungs- und Erwartungswerte der Mitarbeiter des Unternehmens. Durch die Beratung des Partnerunternehmens 8com GmbH konnten weitere Use Cases identifiziert werden. Für die OEDIV KG haben sich damit praxisrelevante Use Cases ergeben, die u.a. eine Verbesserung der Incident Response nach sich ziehen konnten. Bei der Sichtung der wissenschaftlichen Literatur hat sich jedoch gezeigt, dass ein Mangel hinsichtlich der konzeptionellen Entwicklung von Use Cases für ein CDC besteht. Hierbei wäre ein Forschungsansatz, ein Modell für die Entwicklung von Use Cases zu erarbeiten, dass nicht (allein) auf heuristischen Methoden beruht.

Die Möglichkeiten der Datenanalyse sind durch die Einführung eines CDC gestiegen. Durch den tieferen Einblick in die Netzwerkkommunikation können weitere Informationen für die Weiterentwicklung von Produkten, Services und Organisationen gewonnen werden. Hierbei bietet ein CDC eine Vielzahl an Innovationsmöglichkeiten. Ein zu entwickelndes Verfahren, mit dem diese Informationen nutzbar gemacht werden, bietet einen Ansatz für weitere Forschung. Hierbei sollte darauf geachtet werden, welche Informationen Implikationen für die organisatorischen und welche für die technischen Aspekte des CDCs haben, um nicht nötige Informationen zu extrahieren. Auch für die Weiterentwicklung eines bestehenden CDC empfiehlt sich eine tiefergehende Untersuchung, um die digitalen Entwicklungen zu berücksichtigen.

Ein CDC bringt den Vorteil der zentralen Verarbeitung großer Mengen an Daten. Zugleich ist das Datenvolumen so hoch, dass eine manuelle Bearbeitung selbst von vorselektierten Incidents für ein mittelständiges Unternehmen nicht praktikabel ist. Bei einer Partnerschaftsgestaltung ist die Schwierigkeit darin bemessen, welches Unternehmen, welche Aufgabe innerhalb eines CDC übernimmt. Hier stellt sich die Frage, welches Unternehmen die größere Expertise, die geeigneteren Tools und Möglichkeiten hat, beispielsweise Incident Response Prozesse durchzuführen. Um die Effektivität eines partnerschaftlich betriebenen CDC im Vergleich zu einem selbstgeführten CDC zu bewerten, wäre weitere Forschung notwendig.

Da die Arbeit auf der IT-Architektur und dem Unternehmensumfeld der OEDIV KG basiert, ist weitere Forschung im Bereich von Use Cases für CDC-Umgebungen in unternehmensunspezifischer bzw. abstrakterer Form für eine breite Anwendbarkeit wünschenswert. Ein Transfer der Ergebnisse dieser Arbeit ist aufgrund ähnlicher Strukturen und Datenquellen insbesondere für IT-Unternehmen möglich.

Insgesamt konnte für das Unternehmen mit der vorliegenden Arbeit die Basis für weitere Entwicklungen im Bereich Cyber Defense Center gelegt werden. In einem Umfeld steigender Datenvolumen und immer professioneller agierenden Angreifer, überwiegen die Vorteile eines CDC immer mehr den Aufwand, den ein CDC mit sich

bringt. Nicht zuletzt stärkt ein CDC damit die Wettbewerbsfähigkeit im Kontext der sich schnell verändernden IT-Branche.