Schwachstellen und Angriffsketten in der Wertschöpfungskette der Fleischproduktion

Eine Analyse an exemplarischen IT-Infrastrukturen

Manfred Hofmeier[1] und Ulrike Lechner[2]

Abstract: Im Rahmen des Deutsch-Österreichischen Forschungsprojekts NutriSafe (Sicherheit in der Lebensmittelproduktion und -logistik durch die Distributed-Ledger-Technologie) wurde eine Analyse zur Identifikation von relevanten Schwachstellen und Angriffsketten in Wertschöpfungsketten von Lebensmitteln durchgeführt. Die vorliegende Arbeit beschreibt die Analyse der IT-Infrastrukturen von fiktiven, aber der Realität nachempfundenen Akteuren der Wertschöpfungskette, basierend auf einem der Szenarien des NutriSafe-Projekts. Ergebnisse sind Beziehungen von Gefährdungen zu IT-Infrastrukturen und Modelle von Angriffsketten in Form von Attack Trees.

Keywords: Lebensmittelsicherheit, Cybersicherheit, Schwachstellen, Attack Trees

1 Einleitung

Im durch das Bundesministerium für Bildung und Forschung (BMBF) und das österreichische Bundesministerium für Verkehr, Innovation und Technik (BMVIT) geförderten Forschungsprojekt NutriSafe (Sicherheit in der Lebensmittelproduktion und -logistik durch die Distributed-Ledger-Technologie) forschen Universitäten, Unternehmen und Behörden daran, die Lebensmittelproduktion sowie deren Logistik unter Nutzung von Distributed-Ledger-Technologie (DLT) sicherer zu machen [Re19][Nu19].

In der Auswertung des Bundesamts für Sicherheit in der Informationstechnik (BSI) über die Häufigkeit von Cybervorfällen in Kritischen Infrastrukturen für das Jahr 2018 ist der Sektor Ernährung derjenige mit den wenigsten IT-Sicherheitsmeldungen [Bu18]. Das zur Meldung verpflichtende IT-Sicherheitsgesetz [Ge15] betrifft Unternehmen, die mehr als 434 500 Tonnen bzw. mehr als 350 Mio. Liter im Jahr produzieren oder verarbeiten [Bu16]. Der Sektor Ernährung ist jedoch von kleinen und mittleren Betrieben sowie Verfahren der kontinuierlichen Belieferung geprägt [Pl05]. Die Idee von NutriSafe soll vor allem die KMUs in Lebensmittelproduktion und -logistik ansprechen. Wenig ist über diesen Sektor aus Sicht der IT-Sicherheit bekannt.

[1] Universität der Bundeswehr München, Fakultät für Informatik, Institut für Schutz und Zuverlässigkeit, Werner-Heisenberg-Weg 39, 85577 Neubiberg, manfred.hofmeier@unibw.de
[2] Universität der Bundeswehr München, Fakultät für Informatik, Institut für Schutz und Zuverlässigkeit, Werner-Heisenberg-Weg 39, 85577 Neubiberg, ulrike.lechner@unibw.de

doi:10.18420/sicherheit2020_05

Im Rahmen von NutriSafe wurde eine Analyse zur Identifikation von Schwachstellen und Angriffsketten durchgeführt. Der Analyse liegen dabei zwei Szenarien [Wi19] und die dazugehörigen IT-Infrastrukturen [Ho19] zugrunde, die mittels Desk Research und Experteninterviews erstellt wurden. Das vorliegende Papier beschreibt die an die Szenarioentwicklung anknüpfende Analyse der Schwachstellen und Angriffsvektoren.

2 Vorgehensweise

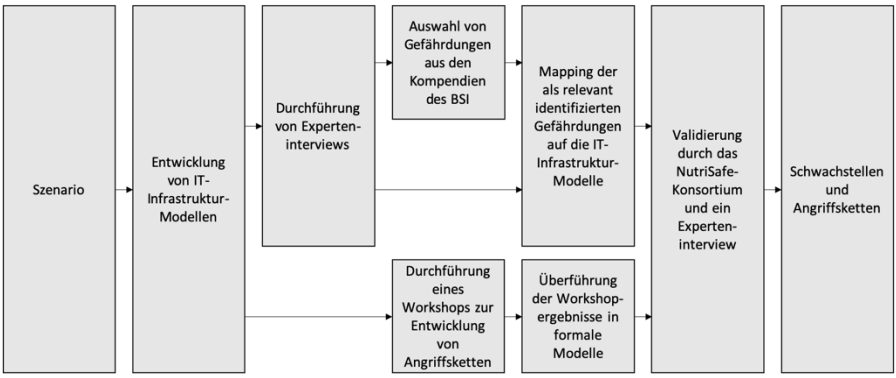

Abb. 1 Vorgehensweise der Schwachstellenanalyse im Projekt NutriSafe

Auf Basis des im Projekt NutriSafe entwickelten Szenarios wurden die IT-Infrastrukturen mittels Desk Research und informeller Notation modelliert [SW06] und im Anschluss durch die Experten im Projektkonsortium validiert (mehr zur Zusammensetzung des Konsortiums in [Nu19]). Diese Infrastrukturmodelle stellen die Grundlage der anschließenden Analyse dar.

Die Kompendien des BSI, speziell der Bereich „IND.1“ des IT-Grundschutz-Kompendiums [Bu19] und das ICS-Security-Kompendium [Bu13], wurden hinsichtlich Gefährdungen ausgewertet und Experteninterviews mit der Bundesvereinigung der Deutschen Ernährungsindustrie (BVE) und dem CERT@VDE wurden im Juli/August 2019 durchgeführt. Der Fokus auf die industriellen Steuersysteme und die Auswahl relevanter Gefährdungen aus den Kompendien fußt u.a. auf den Interviewergebnissen. Dabei stellte sich heraus, dass es eine große Schnittmenge von Gefährdungen in den Kompendien mit in den Interviews genannten Gefährdungen gibt. Die ausgewählten Gefährdungen wurden dann mit den Infrastrukturmodellen abgeglichen, um Schwachstellen zu identifizieren. Parallel dazu fand im August 2019 ein projektinterner Workshop zur Entwicklung von Angriffsketten statt. Im Workshop wurde zunächst eine kurze Einführung in eine einfache Form der Notation mit Attack Trees [Sc99] gegeben, gefolgt durch die kreative Entwicklung von Angriffsketten und Aufzeichnung mittels Attack Trees durch die einzelnen Teilnehmer. Im Anschluss an die kreative Phase folgte eine Gruppendiskussion, in der die einzelnen Angriffsketten in Bezug auf Plausibilität und

Realismus diskutiert und ggfs. verfeinert wurden. Im Nachgang wurden die Angriffsketten entsprechend bereinigt, in formale Modelle (Attack Trees [Sc99]) überführt und durch die Workshopteilnehmer einem Review unterzogen. Zuletzt wurden sowohl die identifizierten Schwachstellen als auch die entwickelten Angriffsketten in einem Interview mit einem IT-Sicherheitsexperten validiert.

3 Ergebnisse

3.1 Informationen aus den Interviews

Das gemeinnützige CERT@VDE des Verbands der Elektrotechnik Elektronik Informationstechnik e.V. (VDE) unterstützt Unternehmen bei IT-Sicherheitsvorfällen im Bereich der industriellen Automatisierungstechnik. Die Bundesvereinigung der Deutschen Ernährungsindustrie (BVE) ist ein Interessensverband der Unternehmen und Fachverbände und verantwortlich für den branchenspezifischen Sicherheitsstandard für die Ernährungsindustrie (B3S Ernährungsindustrie). Im Rahmen der Schwachstellenanalyse wurden mit beiden Organisationen telefonische Interviews durchgeführt. Wesentliche Ergebnisse beziehen sich auf die Relevanz des Themas:

- Es gibt IT-Sicherheitsvorfälle in Lebensmittelproduktion und -logistik, darunter öffentlich bekannt gewordene Beispiele von Ransomware-Vorfällen bei Logistikern. Dabei kann davon ausgegangen werden, dass derartige Vorfälle erst dann öffentlich bekannt gegeben werden, wenn sie bereits an die Öffentlichkeit gedrungen sind.
- Es ist mit der vollen Bandbreite an Angreifertypen mit unterschiedlichen Motiven zu rechnen. Neben Erpressung gibt es vor allem zwei Motive für potentielle Angreifer: Sabotage und (Industrie-)Spionage. So kann man davon ausgehen, dass der Typ des Cyberterroristen sich primär auf die industriellen Steuersysteme (ICS) fokussieren würde, um die Verfügbarkeit und Integrität der Waren anzugreifen. Dabei wäre mit einem komplexen Angriff zu rechnen, bei dem eine Vielfalt an unterschiedlichen Angriffsvektoren, wie etwa (Spear-)Phishing, zum Einsatz kommt. Bei kriminellen Akteuren steht – neben Erpressung mittels Ransomware – eher die Ausleitung von Daten zum Zweck der Industriespionage im Vordergrund. Es ist dabei aber nicht auszuschließen, dass staatliche Akteure eine solche Datenausleitung in Auftrag geben, da für staatliche Akteure oft ein Interesse an strategischen Planungen von fremdstaatlichen Konzernen besteht, besonders wenn es dabei um Planungen zum Erschließen von Ressourcen (z.B. Wasser) geht. Besonders hohe Motivation ist vermutlich bei sog. Hacktivisten vorhanden, beispielsweise in Bezug auf Großunternehmen, die wegen ihrer Beanspruchung von kritischen Ressourcen unter Kritik stehen. Aber auch in Bezug auf die Fleischindustrie ist mit Motivation zu rechnen. Innentäter stellen wie in anderen Branchen ein besonderes Risiko dar, da sie besonderen Zugriff auf Informationen und Systeme haben.

- Insgesamt ist die Prozessautomatisierung ein elementares Rückgrat der Lebensmittelwertschöpfungskette und daher ein besonders schützenswertes Angriffsziel. Dabei ist zu beachten, dass dabei vor allem Zulieferer oder Dienstleister des eigentlich anvisierten Unternehmens (z.B. Anlagenbauer oder Subunternehmer; teils kleine Ingenieurbüros) eine Schwachstelle darstellen. Wichtig für die Sicherheit ist eine Betrachtung der Herstellungskette und Teilbestandteile von eingesetzten Produkten (z.B. Produktionsanlagen). Weitere Themen sind die sichere Ausgestaltung der Fernwartung von Produktionsanlagen sowie Zutritts- und Zugriffsbeschränkungen, wobei auch physische Barrieren eine große Rolle spielen.

Aufgrund der Interviewergebnisse wurde bei der Auswertung der Kompendien der Schwerpunkt auf Produktion und industrielle Steuersysteme (ICS) gelegt.

3.2 Gefährdungen und Schwachstellen

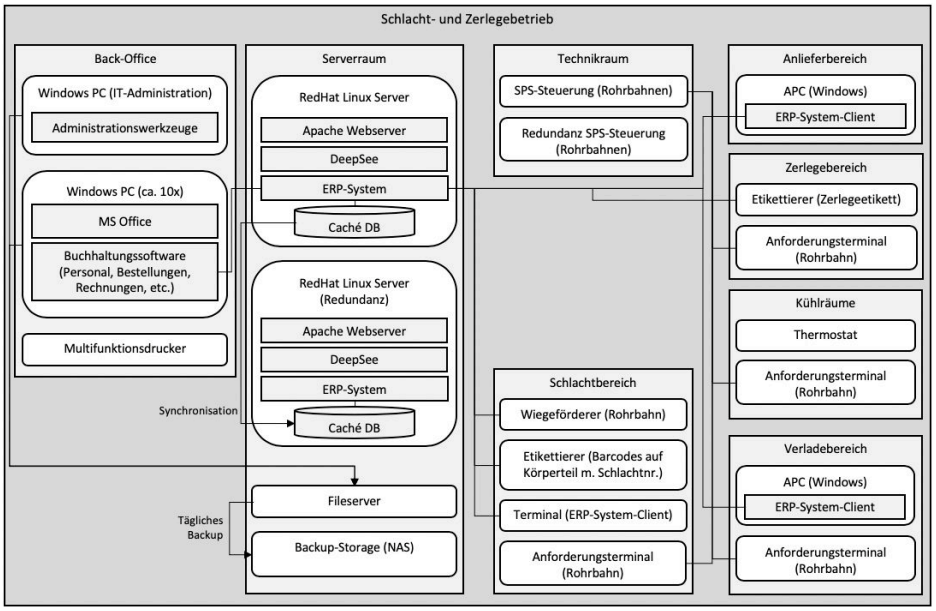

Abb. 2 Beispielhafte IT-Infrastruktur eines Schlacht- und Zerlegebetriebes [Ho19]

Im Folgenden werden die Bezüge der Gefährdungen zu den IT-Infrastrukturen zweier Akteure der Wertschöpfungskette für Kochschinken – Schlacht- und Zerlegebetrieb und Fleischproduktion/Metzgerei – beschrieben. Das Mapping wurde unter Zuhilfenahme von Literatur [Bu13][Bu18][Bu19][Dä18][DC19][Eu19][Fo16][Pl05][Ur13][Wy19], Interviews sowie der Expertise im Projektkonsortium (Zusammensetzung des Konsortiums in [Nu19]) durchgeführt.

Die IT-Infrastruktur des Schlacht- und Zerlegebetriebes (Abb. 2) gliedert sich im Groben in die Bereiche Back-Office, Serverraum und Produktionsbereich. Der Produktionsbereich wiederum ist gegliedert in die verschiedenen physischen Bereiche Anlieferbereich, Schlachtbereich, Zerlegebereich, Kühlräume, Verladebereich und den Technikraum, der die SPS-Steuerung für die Rohrbahnen enthält, mit der die Fleischhaken für den Transport von Tierhälften gesteuert werden. Einige Bereiche in der Produktion enthalten Anforderungsterminals für diese Rohrbahn. Rohrbahn und ERP-System bilden die zwei wichtigsten Bestandteile der technischen Infrastruktur in diesem Betrieb. Das ERP-System und der Produktionsbereich sind durch Netzwerksegmentation vom Back-Office getrennt.

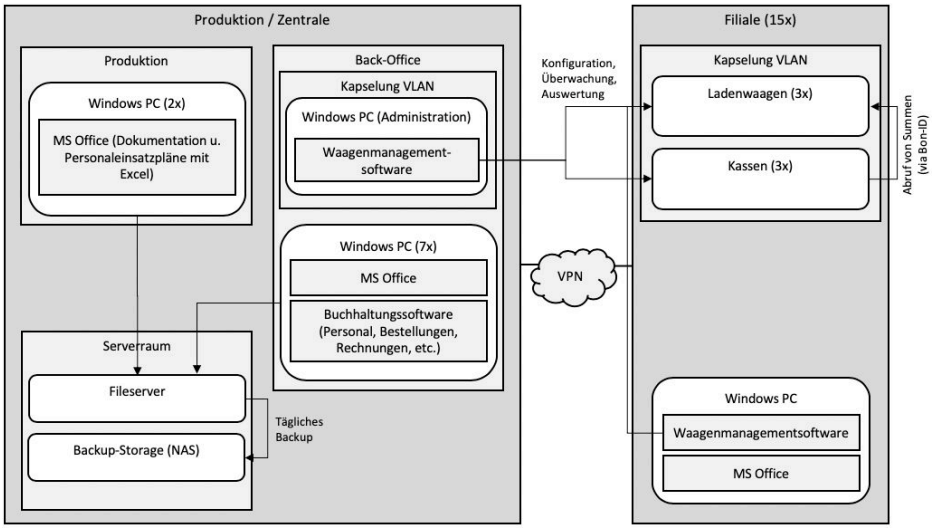

Abb. 3 Beispielhafte IT-Infrastruktur für Fleischproduktion / Metzgerei [Ho19]

Die IT-Infrastruktur der Fleischproduktion im Kochschinken-Szenario von NutriSafe (Abb. 3) gliedert sich im Wesentlichen in die Zentrale mit Produktion und Back-Office und in die 15 Filialen, verbunden durch ein Virtual Private Network (VPN). Elementarer Bestandteil sind die Ladenwaagen und Kassen, die zentral über eine entsprechende Software verwaltet werden (z.B. Einstellen von Produkten und Preisen, Auswerten von Verkäufen). Die Waagen und Kassen sind dabei in ein eigenes VLAN gekapselt. Die Produktion geschieht zwar maschinell (z.B. Kutter), jedoch sind diese in der Regel nicht vernetzt, warum diese auch nicht in der IT-Infrastruktur abgebildet sind. Lediglich die Dokumentation wird IT-gestützt durchgeführt. Dazu wird parallel zum laufenden Betrieb auf Papier dokumentiert und im Nachgang werden die Daten in MS Excel überführt.

Gefährdung	Relevanz für die IT-Infrastruktur Schlacht- und Zerlegebetrieb	Relevanz für die IT-Infrastruktur Fleischproduktion
Organisatorische Gefährdungen (basierend auf dem ICS-Security-Kompendium [Bu13])		
Unzureichende Regelungen zur IT-Security	Es sind nur rudimentäre Regelungen vorhanden, die nur bei der Anstellung neuer Mitarbeiter kommuniziert werden	Es sind nur rudimentäre Regelungen vorhanden, die nur bei der Anstellung neuer Mitarbeiter kommuniziert werden
Unzureichende Dokumentation	Es ist zwar eine Dokumentation der Systeme im segmentierten Netz vorhanden, aber deren genaue Konfiguration sowie die Office-Computer und deren Konfiguration sind i.d.R. nicht dokumentiert	Es ist zwar eine Dokumentation der Waagen und Kassen im segmentierten Netz vorhanden, aber die Office-Computer und deren Konfiguration sind i.d.R. nicht dokumentiert
Unvollständige Absicherung der Fernwartungszugänge	Die Fernwartung der Rohrbahn sowie der Server und PCs ist nicht auf bestimmte, spezifisch freigegebene Zeiträume beschränkt	
Fehlende Überwachung der unterstützenden Infrastruktur	Es gibt keine Überwachung innerhalb des Netzwerks (z.B. keine netzwerkbasierten Intrusion-Detection-Systeme)	Es gibt keine Überwachung innerhalb des Netzwerks (z.B. keine netzwerkbasierten Intrusion-Detection-Systeme)
Mangelnde Awareness		Aufgrund der primär manuellen Tätigkeit spielt IT-Sicherheit für die meisten Mitarbeiter keine große Rolle; Das Personal in der Buchhaltung ist ein wenig sensibilisiert, bringt aber nur rudimentäre IT-Kompetenzen mit
Menschliche Fehlhandlungen (basierend auf dem ICS-Security-Kompendium [Bu13])		
Unzureichende Absicherung oder zu weitreichende Vernetzung	Alle Produktionsanalagen (ERP-Server und Clients, Rohrbahn) befinden sich im selben VLAN	
Unzureichende Validierung von Eingaben und Ausgaben	Dokumentation von Wareneingang, Warenausgang und Verarbeitung erfolgt händisch mit Excel	
Weitere Gefährdungen (basierend auf Interviews und IND.1 IT-Grundschutz [Bu19])		
Unzureichender Zugangsschutz		Es gibt keine reglementierten Zutrittsbeschränkungen für Mitarbeiter
Unzureichender Zugriffsschutz		Der PC für das Waagenmana–gement ist mit einem generischen Account mit leicht zu merkendem Passwort gesichert
Unzureichende Redundanzen (z.B. Single Points of Failure)	Für die SPS-Steuerung ist zwar eine Redundanz vorhanden, aber im selben Raum; Für das ERP-Serversystem ist zwar eine Redundanz vorhanden, aber im selben Raum	Alle wichtigen Daten liegen auf einem Fileserver ohne Redundanz (nur Backup vorhanden); Einige Produktionsanlagen sind aufgrund des hohen Kaufpreises nur einmal vorhanden

Tab. 1 Mapping der Gefährdungen auf die IT-Infrastrukturen (Auszug)

In Bezug auf die Infrastruktur des Schlacht- und Zerlegebetriebes ergeben sich folgende Schwachstellen: Sowohl die SPS-Steuerung als auch da ERP-System haben zwar Redundanzen, jedoch befinden sich diese jeweils im selben Raum. So ist zwar Ausfallsicherheit gegenüber den meisten einfachen Defekten oder Angriffen gegeben, jedoch wären bei physischen Bedrohungen wie Brand oder Wassereinbruch beide Einheiten betroffen. Bei dem ERP-System, welches das Herz in Bezug auf die Daten darstellt und u.a. für die innerbetriebliche Rückverfolgbarkeit von Fleisch wichtig ist, würde auf Dokumentation in Papierform zurückgegriffen werden, wodurch die Produktivität stark verringert werden würde. Bei einem Ausfall der Rohrbahn würde der Transport von Tieren und Tierhälften manuell erfolgen, wodurch ebenfalls die Produktivität stark eingeschränkt würde. Zudem gibt es in der Infrastruktur in diesem Szenario kein versioniertes Backup für das ERP-System. So ist zwar eine Redundanz gegeben, aber Schutz vor Datenmanipulation und dafür notwendige Rollback-Option bestehen so nicht.

Bei der Fleischproduktion/Metzgerei bestehen neben geringer Awareness für IT-Sicherheit, bedingt durch die primär manuelle und analog maschinelle Technik, vor Allem Schwachstellen wie mangelhaft gesicherte Zugänge zu den einzelnen Computern, darunter die Computer für das Waagen- und Kassenmanagement. Zusätzlich fehlen physische Zutrittsregelungen und -beschränkungen innerhalb der Produktionsanlagen und der Filialen. Aufgrund der Natur der Betriebe ist das aber unvermeidlich, wodurch ein grundlegendes Vertrauen in die Mitarbeiter und eine entsprechende Sorgfalt bei der Anstellung neuer Mitarbeiter nötig sind.

Die Schwachstellen geben zwar einen Überblick über Problembereiche, für sich genommen geben sie aber nur eine grobe Sicht auf die IT-Sicherheit. Daher wurden auch mögliche Angriffspfade mit Täterprofilen und Intentionen modelliert, um exemplarisch zu beleuchten, welche Vorfälle bzw. Angriffe existieren können, um besonders kritische und problematische Punkte sowie Ziele von Angreifern sichtbar zu machen.

3.3 Angriffsketten

In einem Workshop unter Verwendung von Kreativtechniken wurden Angriffsketten für diese Infrastruktur mittels Attack Trees [Sc99] entwickelt, anschließend auf Plausibilität und Realitätsnähe diskutiert, entsprechend angepasst und dann bereinigt ausmodelliert. Insgesamt wurden auf diese Weise fünf verschiedene Attack Trees zu den IT-Infrastrukturen der NutriSafe-Szenarien entwickelt, die verschiedene Angriffsstrategien unterschiedlicher Angreifertypen beschreiben. Nachfolgend werden exemplarisch zwei Beispiele für Attack Trees zu den oben beschriebenen IT-Infrastrukturen dargestellt.

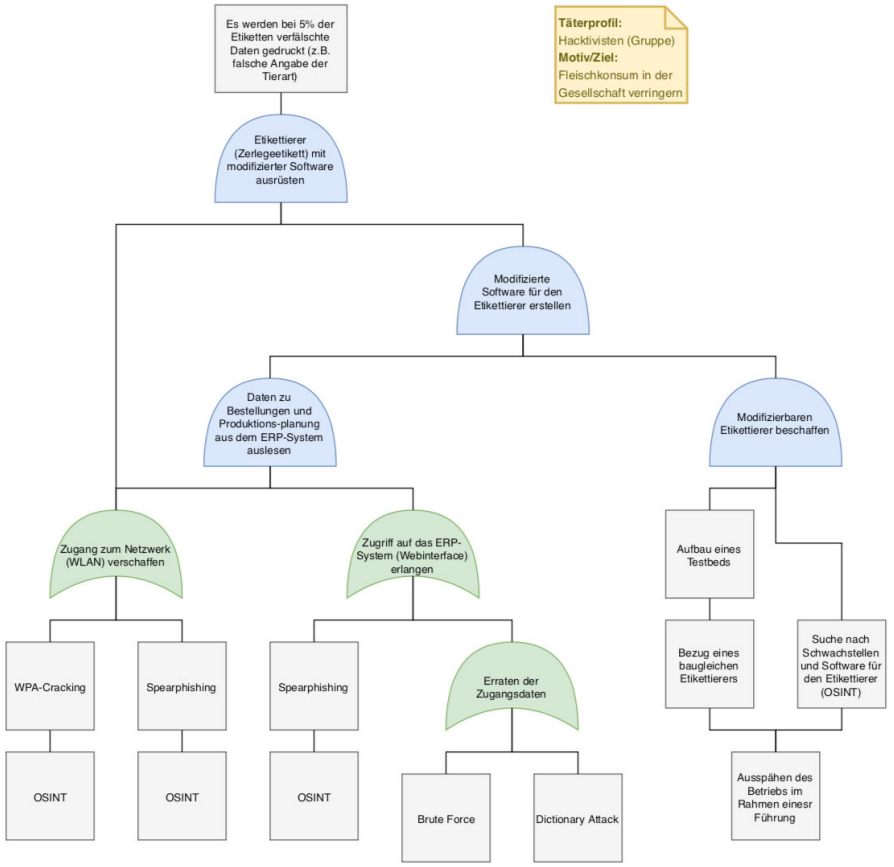

Abb. 4 Attack Tree für einen Hacktivistenangriff auf einen Schlacht- und Zerlegebetrieb

Der Attack Tree in Abb. 4 beschreibt einen komplexen (fiktiven) Angriff durch eine Hacktivistengruppe, die durch gezielte Fehletikettierung der Produkte das Vertrauen in Fleischprodukte verringern möchte. Der Angriff soll so gestaltet sein, dass nur ein kleiner Prozentsatz der Etiketten verfälscht wird, so dass die Fehletikettierung möglichst nicht auffällt und diese Produkte in den Handel geraten. Der Angriff erfordert dabei viel Aufwand und physischen Zugang zum Betrieb.

Ein weiterer Attack Tree (Abb. 5) beschreibt einen klassischen Angriff durch einen Innentäter in einer Metzgereifiliale. Hierbei möchte ein Auszubildender, der in Streit mit dem Filialleiter ist und erwartet, gekündigt zu werden, der Filiale schaden. Das Motiv ist dabei Rache und Ziel des Angriffs ist ein Defacement der Kassenzettel. Da es sich um einen Innentäter handelt, ist der Zugang zu den entsprechenden Räumen und Systemen relativ leicht zu erlangen.

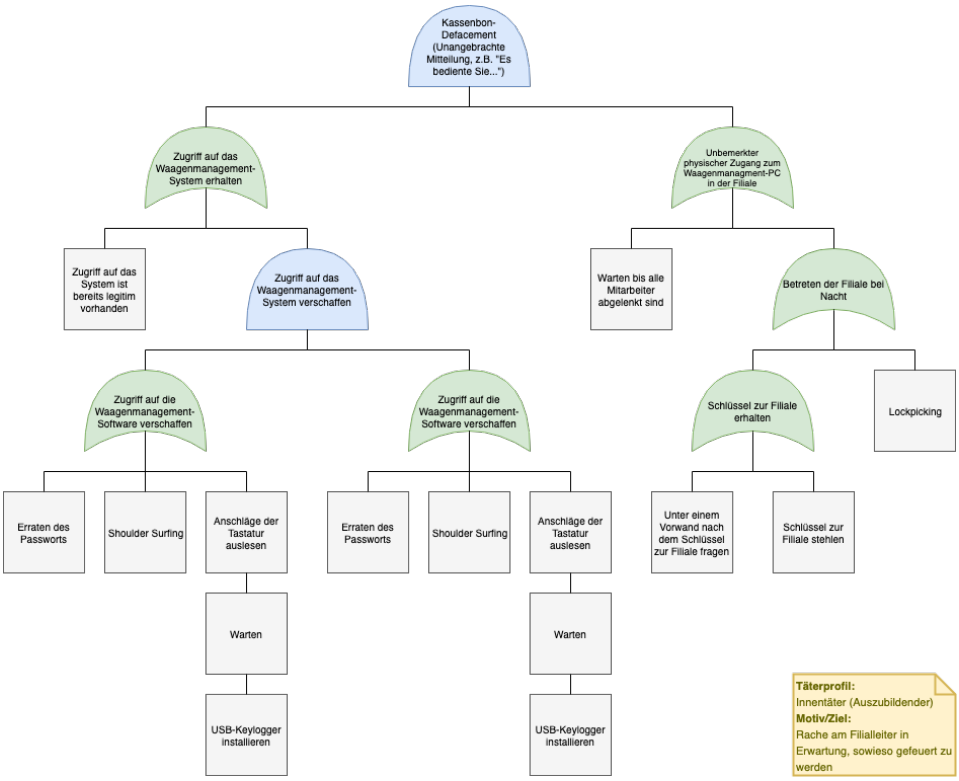

Abb. 5 Attack Tree für einen Angriff durch einen Innentäter in einer Metzgereifiliale

4 Limitationen und Diskussion

Diese Arbeit leistet einen Beitrag, die IT-Sicherheit bei kleinen und mittleren Unternehmen zu verstehen. Es gibt dazu wenige verwertbare Informationen und diese Information ist auch nicht leicht zu beschaffen. Wir verwenden hierzu drei Analyseperspektiven: Die Interviews mit Experten ergeben, dass mehr passiert als in der Öffentlichkeit bekannt ist, also dass das Thema der IT-Sicherheit relevant ist, und dass vor allem bei den industriellen Steuersystemen (ICS) Schwachstellen kritisch sind. Diese Systeme sind aus Sicherheitsperspektive für produzierende Betriebe und Kritische Infrastrukturen besonders schützenswert [RL18]. ICS-Schwachstellen werden sonst eher bei großen industriellen Betrieben thematisiert. Die Szenarioanalyse mit Hilfe der Kompendien des BSI zeigt die Vielfalt der Schwachstellen, selbst bei einem kleinen Betrieb in der Lebensmittelproduktion. Mit dem kreativen Ansatz lassen sich auch spezifische Bedrohungsszenarien für einen Betrieb und seine Kunden und damit die Gesellschaft aufzeigen. So konnten auch sektorenspezifische Angriffspunkte identifiziert

werden, wie etwa Etikettendrucker und Waagenmanagementsysteme. Der dreistufige Prozess über Interviews, Analyse der Referenzwerke und Kreativmethoden stellt dabei die Qualität der gewonnenen Daten sicher.

Die Analyse basiert auf Szenarien, die im Forschungsprojekt NutriSafe entwickelt wurden. Sie sind fiktiv aber realitätsnah und somit sind die Ergebnisse der Schwachstellenanalyse ebenfalls als realitätsnah einzuschätzen und wurden auch durch ein Interview mit einem IT-Sicherheitsexperten validiert. Da die Industriestruktur in der Fleischwirtschaft aber heterogen ist, sind die Ergebnisse nicht ohne weiteres auf die gesamte Branche verallgemeinerbar.

Angriffe auf Betriebe in der Lebensmittelproduktion und -logistik sind nur selten dokumentiert. Vorfälle werden nur selten gemeldet oder veröffentlicht. Die Ergebnisse aus dieser Arbeit schließen diese Lücke. Solche Beispiele sind nicht nur interessant für Forschung und Lehre, sondern auch für die Praxis hilfreich zur Orientierung [Ve18].

5 Acknowledgements

Wir danken dem Bundesministerium für Bildung und Forschung (BMBF) für die Möglichkeit der Forschung im Rahmen des Projektes NutriSafe (FKZ 13N15070 bis 13N15076) sowie dem Sicherheitsforschungsförderprogramm KIRAS, finanziert vom Bundesministerium für Verkehr, Innovation und Technologie (Projektnummer: 867015).

Literaturverzeichnis

[Bu13] Bundesamt für Sicherheit in der Informationstechnik: ICS-Security-Kompendium. Bonn, 2013.

[Bu16] Bundesministerium des Innern: Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV). 2016.

[Bu18] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2018. Bonn, 2018.

[Bu19] Bundesamt für Sicherheit in der Informationstechnik: IND.1 Betriebs- und Steuerungstechnik. In: (Bundesamt für Sicherheit in der Informationstechnik): IT-Grundschutz-Kompendium. Bonn, 2019.

[Dä18] Dännart, S: IT-Sicherheit in der Molkerei: Familientradition und Hochverfügbarkeit. In (Lechner, U; Dännart, S; Rieb, A; Rudel, S): CASE|KRITIS - Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen. Berlin, 2918.

[DC19] DuHadway, S; Carnovale, S: Malicious Supply Chain Risk: A Literature Review and Future Directions. In: Revisiting Supply Chain Risk. 2019.

[Eu19] European Union Agency for Cybersecurity: ENISA Threat Landscape Report 2018 - 15 Top Cyberthreats and Trends. 2019.

[Fo16] Fontanazza, M: FBI Says Terrorists May Target Food Sector. In: FoodSafetyTech. https://foodsafetytech.com/news_article/fbi-says-terrorists-may-target-food-sector, zuletzt abgerufen am 09.01.2020. 2016.

[Ge15] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). In: Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31. 2015.

[Ho19] Hofmeier, M: Beispiele für IT-Infrastrukturen in den Wertschöpfungsketten der NutriSafe-Szenarien. https://nutrisafe.de/veroeffentlichungen. Neubiberg, 2019.

[Nu19] NutriSafe – Sicherheit in der Lebensmittelproduktion und -logistik durch die Distributed-Ledger-Technologie, https://nutrisafe.de, zuletzt abgerufen am 01.10.2019.

[Pl05] Platz, U: Vulnerabilität von Logistikstrukturen im Lebensmittelhandel. Landwirtschaftsverlag, Münster-Hiltrup, 2005.

[Re19] Reimers, T. et al.: Absicherung von Wertschöpfungsketten in der Lebensmittelproduktion und -logistik mittels Distributed-Ledger-Technologie – Das Forschungsdesign. In: Tagungsband zum 16. Deutschen IT-Sicherheitskongress. Bonn, 2019.

[RL18] Rudel, S; Lechner, U: IT-Sicherheit für Kritische Infrastrukturen – State of the Art. https://www.itskritis.de/state-of-the-art.html. Neubiberg, 2018.

[Sc99] Schneier, B: Attack Trees. 1999.

[SW06] Schubert, P.; Wölfle, R: The Experience Methodology for Writing IS Case Studies. In: Americas Conference on Information Systems (AMCIS). 2006.

[Ur13] Urciuoli, L; Männistö, T; Hintsa, J; Tamanna, K: Supply Chain Cyber Security – Potential Threats. In: Information & Security, Volume 29, Issue 1. 2013.

[Ve18] VeSiKi: Monitor 2.0 IT-Sicherheit Kritischer Infrastrukturen. https://itskritis.de/monitor. Neubiberg, 2018.

[Wi19] Wilhelmi, T: Kurzbeschreibung der NutriSafe-Szenarien Produktion und Logistik von Bio-Kochschinken und Weichkäse. https://nutrisafe.de/veroeffentlichungen. Neubiberg, 2019.

[Wy19] von Wyl, H: Metzger Wechsler und die Hacker. In: Compass Security. https://www.compass-security.com/fileadmin/Datein/News/2019/MOB_01_EPIC_LOW_RES_PDF-pages-4-6.pdf, zuletzt abgerufen am 09.01.2020. 2019.