Cyberangriffe gegen Unternehmen

Projektabschlussbericht

Förderkennzeichen

BMWi-VID5-090168623-01-1/2017

Projektlaufzeit

01.12.2017 bis 30.11.2020 (verlängert bis 31.03.2021)

Projektpartner

Kriminologisches Forschungsinstitut Niedersachsen e.V. (KFN)

Leibniz Universität Hannover – Forschungszentrum L3S

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Zusatzgefördert durch:

VHV STIFTUNG

pwc

IT-Sicherheit IN DER WIRTSCHAFT

Cyberangriffe gegen Unternehmen

Projektabschlussbericht: BMWi-VID5-090168623-01-1/2017

Projektpartner:

Kriminologisches Forschungsinstitut Niedersachsen e.V. (KFN)
Ansprechpartner: Dipl.-Soz. Arne Dreißigacker

Leibniz Universität Hannover – Forschungszentrum L3S
Ansprechpartner: Prof. Dr. Sascha Fahl

Initiative „IT-Sicherheit in der Wirtschaft“

Das Projekt „Cyberangriffe gegen Unternehmen“ ist Teil der Initiative „IT-Sicherheit in der Wirtschaft“ im Förderschwerpunkt Mittelstand-Digital.

Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand 4.0-Kompetenzzentren, der Initiative „IT-Sicherheit in der Wirtschaft“ und Digital Jetzt umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.mittelstand-digital.de und www.it-sicherheit-in-der-wirtschaft.de.

ISBN: 978-3-948647-13-1

Autor*innen:

Arne Dreißigacker, Sascha Fahl, Nicolas Huaman, Bennet von Skarczinski, Christian Stransky, Gina Rosa Wollinger

Hannover, September 2021

Inhalt

1 Kurzdarstellung 7

1.1 Aufgabenstellung 7

1.2 Voraussetzungen 7

1.2.1 Kriminologisches Forschungsinstitut Niedersachsen e.V. (KFN) 8

1.2.2 Forschungszentrum L3S 8

1.3 Planung und Ablauf des Vorhabens 9

1.4 Forschungsstand 12

1.5 Zusammenarbeit mit anderen Stellen 15

2 Eingehende Darstellung 17

2.1 Durchgeführte Arbeiten, angestrebte und erreichte Ziele 17

2.1.1 Aufarbeitung Forschungsstand (AP 1: KFN) 17

2.1.2 Expert*inneninterviews (AP 2: KFN) 19

2.1.3 Unternehmensbefragung I (AP 3: KFN) 22

2.1.4 Feldstudie: Evaluation von Dokumentation im Kontext KMU (AP 4: L3S) 25

2.1.5 Feldstudie: IT-Sicherheitsregeln im Arbeitsalltag (AP 5: L3S) 26

2.1.6 Ergebnistransfer (AP 6: KFN/ L3S) 28

2.1.7 Feldstudie: Strategien zur Bekämpfung von Cybercrime (AP 7: L3S) 34

2.1.8 Feldstudie: Benutzbarkeit SIEMs (AP 8: L3S) 36

2.1.9 Unternehmensbefragung II (AP 9: KFN) 38

2.1.10 Vorhersage-Plattform (AP 10: L3S) 42

2.2 Wichtige Positionen des zahlenmäßigen Nachweises 42

2.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit 43

2.4 Nutzen und Verwertbarkeit der Ergebnisse 44

2.5 Fortschritt bei anderen Stellen 47

2.6 Erfolgte und geplante Veröffentlichungen der Ergebnisse 48

3 Anhang: Kurzzusammenfassung der Fachbeiträge 49

3.1 Verbreitung von Cyberkriminalität gegen Unternehmen in Deutschland 50

3.2 Im Visier: Repräsentative Studie zur Cyberkriminalität in deutschen Unternehmen 51

3.3 A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises 52

3.4 Understanding the adoption of cyber insurance for residual risks – An empirical large-scale survey on organizational factors of the demand side 53

3.5 Towards enhancing the information base on direct costs of cyber-attacks on organizations: Implications from literature and a large-scale survey 54
3.6 Cybercrime in Small and Medium-sized Enterprises 55
3.7 Cyberangriffe gegen Unternehmen: Erste Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland 56
Tabellen **57**
Abbildungen **57**
Literatur **58**

1 Kurzdarstellung

In diesem Abschnitt werden die Aufgabenstellung und die Voraussetzungen des Projektes "Cyberangriffe gegen Unternehmen" dargestellt, dessen Planung und Ablauf erläutert, der Forschungsstand zusammengefasst und die Zusammenarbeit mit anderen Stellen beschrieben.

1.1 Aufgabenstellung

Während in Deutschland in den letzten Jahren in vielen Kriminalitätsbereichen sinkende Fallzahlen zu verzeichnen sind, gehören Cybercrime-Delikte nach wie vor zu einem wachsenden Phänomen. Insbesondere Unternehmen stehen dabei im Fokus von Cyberkriminellen. Betroffene Unternehmen erleben zum Teil enorme finanzielle oder wettbewerbliche Nachteile als Folge. Anders als große Unternehmen mangelt es dabei kleinen und mittlere Unternehmen (KMU) auf der einen Seite oftmals am Bewusstsein für mögliche Gefahren durch Cyberangriffe und auf der anderen Seite an Möglichkeiten, IT-Sicherheit effektiv im Unternehmen zu implementieren.

Für die gesamte Wirtschaft Deutschlands muss es angesichts dieser Ausgangssituation ein zentrales Anliegen sein, auf die Bedrohungslage durch Cybercrime angemessen zu reagieren und sich mit dem Thema der IT-Sicherheit gezielter auseinanderzusetzen. Dies kann besonders gut gelingen, wenn die Unternehmen anhand aktueller und sorgfältig erarbeiteter Informationen erkennen können, auf welche Weise die Cyberangriffe erfolgen und wie man sich gegen sie effektiv schützen kann. Eine notwendige Voraussetzung dafür bilden empirische Erkenntnisse zur aktuellen Lage der IT-Sicherheit in Bezug auf Cyberangriffe in Deutschland und ein differenziertes Bild über die verschiedenen Angriffsarten und deren Verbreitung. Das Projekt "Cyberangriffe gegen Unternehmen" hatte zur Aufgabe, diese empirische fundierte Grundlage zu schaffen, Handlungsempfehlungen für KMU zu entwickeln und die wissenschaftlichen Erkenntnisse in die Praxis zu transferieren, um neben der Verbesserung der "Awareness" ein Beitrag zur Verbesserung der IT-Sicherheit von kleinen und mittelständischen Unternehmen (KMU) zu leisten.

1.2 Voraussetzungen

Anknüpfungspunkt für das Vorhaben war eine vom Bundesministerium für Wirtschaft und Energie (BMWi) bei der WIK-Consult in Auftrag gegebene Repräsentativerhebung im deutschen Mittelstand. Diese hat ergeben, dass für kleine und mittlere Unternehmen auf dem Gebiet Cybersicherheit sehr viel Handlungsbedarf besteht (BMWi 2012). Aber auch für größere Unternehmen und andere Bereiche der Wirtschaft, wie der Finanzbranche, haben verschiedene Studien der Jahre 2015 und 2016 gezeigt, dass im Verlauf von zwei Jahren 40- bis 50 % der Unternehmen von Cybercrime im Sinne von Wirtschaftsspionage, Sabotage oder Datendiebstahl betroffen waren (Bitkom 2015; KPMG 2015; PwC/Universität Halle 2016). Zwar zeigte sich auch, dass technische Instrumente, die Unternehmen im Hinblick auf IT-Sicherheit schützen sollen, vielfach vorhanden sind, verschiedene Informationsplattformen für Unternehmen auf die Gefahren von Cybercrime aufmerksam machen und Hilfestellungen bieten und zudem

vielfältige Möglichkeiten bestehen, sich durch IT-Dienstleister einschlägiges Know-how einzukaufen. Dennoch wiesen bisherige Erhebungen darauf hin, dass viele Unternehmen nicht bzw. nicht ausreichend geschützt sind, um Cyberangriffe erfolgreich abzuwehren. Dies traf vor allem auf kleine und mittelständische Unternehmen zu, die aufgrund ihrer Größe sowie aufgrund der ihnen zur Verfügung stehenden finanziellen Mittel nicht ohne weiteres in IT-Sicherheit investieren können. Daher wurde eine Förderausschreibung des BMWi und der Initiative "IT-Sicherheit in der Wirtschaft" auf die nachhaltige Verbesserung der IT-Sicherheit insbesondere von kleinen und mittelständischen Unternehmen ausgerichtet und in diesem Rahmen das Konsortium, bestehend aus dem Kriminologischen Forschungsinstitut Niedersachsen e.V. (KFN) und dem Forschungszentrum L3S, mit dem hier beschriebene Projekt "Cyberangriffe gegen Unternehmen" gefördert. Eine Zusatzförderung erfolgte durch die Wirtschaftsprüfungsgesellschaft und Unternehmensberatung PricewaterhouseCoopers (PwC)[1] sowie durch die VHV-Stiftung.[2]

1.2.1 Kriminologisches Forschungsinstitut Niedersachsen e.V. (KFN)

Das KFN ist eines der führenden kriminologischen Forschungsinstitute Deutschlands, das unabhängig und interdisziplinär grundlagen- und praxisorientierte kriminologische Forschung betreibt und fördert. Es arbeitet im Rahmen eines Kooperationsvertrages eng mit der Universität Göttingen zusammen und verfügt über breite Erfahrungen mit der multiperspektivischen Untersuchung von Ursachen, Entwicklung, Formen und Folgen abweichenden Verhaltens sowie der Institutionen der Sozialkontrolle. Ein zentrales Anliegen ist dabei immer auch die Vermittlung von Forschungsergebnissen in die Praxis und in die Öffentlichkeit. Bei der Erforschung der Cyberkriminalität in Deutschland nimmt das KFN eine Vorreiterstellung ein. Zu den Vorarbeiten in diesem Feld zählen verschiedene Untersuchungen zu den Phänomenen von Cyberkriminalität im weiteren und im engeren Sinne, deren Verbreitung die Folge für die Opfer. Dazu gehören Straftaten, die mittels Informationstechnik begangen werden, z.B. Cyberstalking, Cybergrooming und Cybermobbing,[3] und Straftaten, die sich vor allem gegen IT-Systeme oder deren Daten richten, z.B. Ransomware-, Spyware- oder Viren-Angriffe.[4]

1.2.2 Forschungszentrum L3S

Das Forschungszentrum L3S ist eine gemeinsame interdisziplinäre Einrichtung der Leibniz Universität Hannover und der Technischen Universität Braunschweig, die sich auf grundlagen- und anwendungsorientierte Forschung in den Bereichen Künstliche Intelligenz, Sicherheit, und Vernetzte Systeme konzentriert. Als eines von zwei deutschen BDVA Innovation Spaces und

[1] In dem hier beschriebenen Vorhaben stellt PwC einen wirtschaftswissenschaftlichen Mitarbeiter den kompletten Projektzeitraum in beratender Funktion zur Verfügung. Dieser hat vor allem die (betriebs-)wirtschaftlichen Aspekte untersucht, z.B. in Form von Kosten- und Nutzenanalysen und Risikoberechnungen.

[2] Die Förderung der VHV-Stiftung bezieht sich auf die Finanzierung eines Mitarbeiters für den gesamten Projektzeitraum. Dieser Mitarbeiter aus der Informatik hat vor allem eine Internetplattform zur Risikoprognose für Unternehmen realisiert.

[3] Bergmann/Baier 2016, 2018; Baier et al. 2016; Bergmann et al. 2016; Bergmann 2018

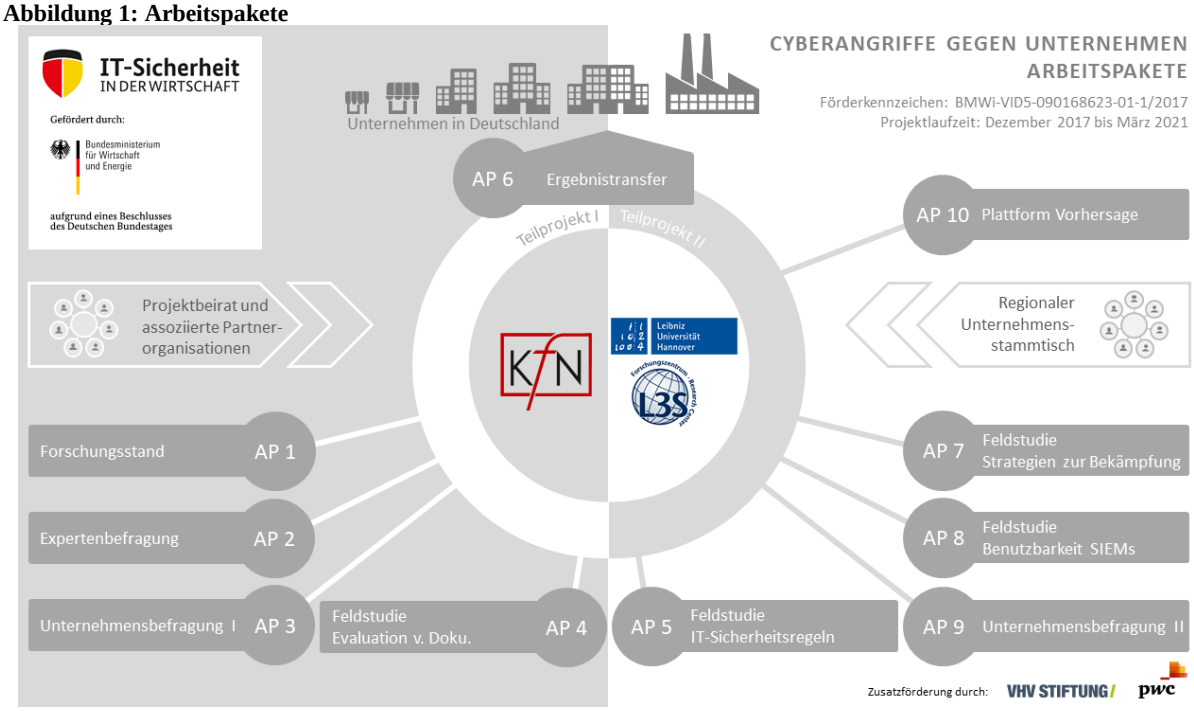
[4] Bergmann et al. 2018; Dreißigacker/Riesner 2018

als IDSA-Kompetenzzentrum unterstützt das L3S die Aktivitäten der Big Data Value Association und der International Dataspaces Association und erarbeitet regelmäßig Empfehlungen und Strategien für Wirtschaft, Politik, und Gesellschaft.

1.3 Planung und Ablauf des Vorhabens

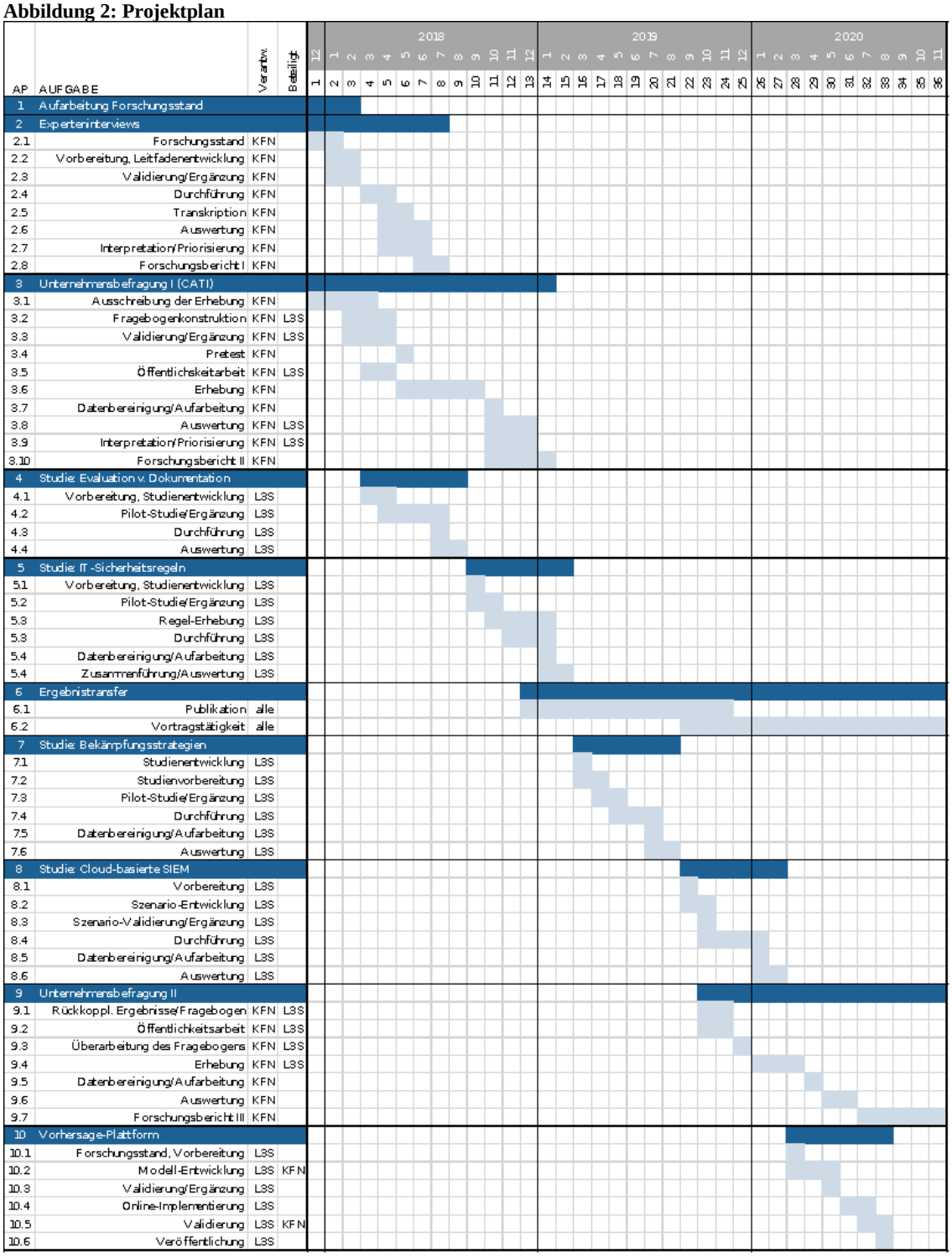
Für die Durchführung des Projektes war eine Laufzeit von 36 Monaten (Dez. 2017 bis Nov. 2020) vorgesehen. In Abbildung 1 sind die zehn Arbeitspakete (AP) dargestellt.

Abbildung 1: Arbeitspakete



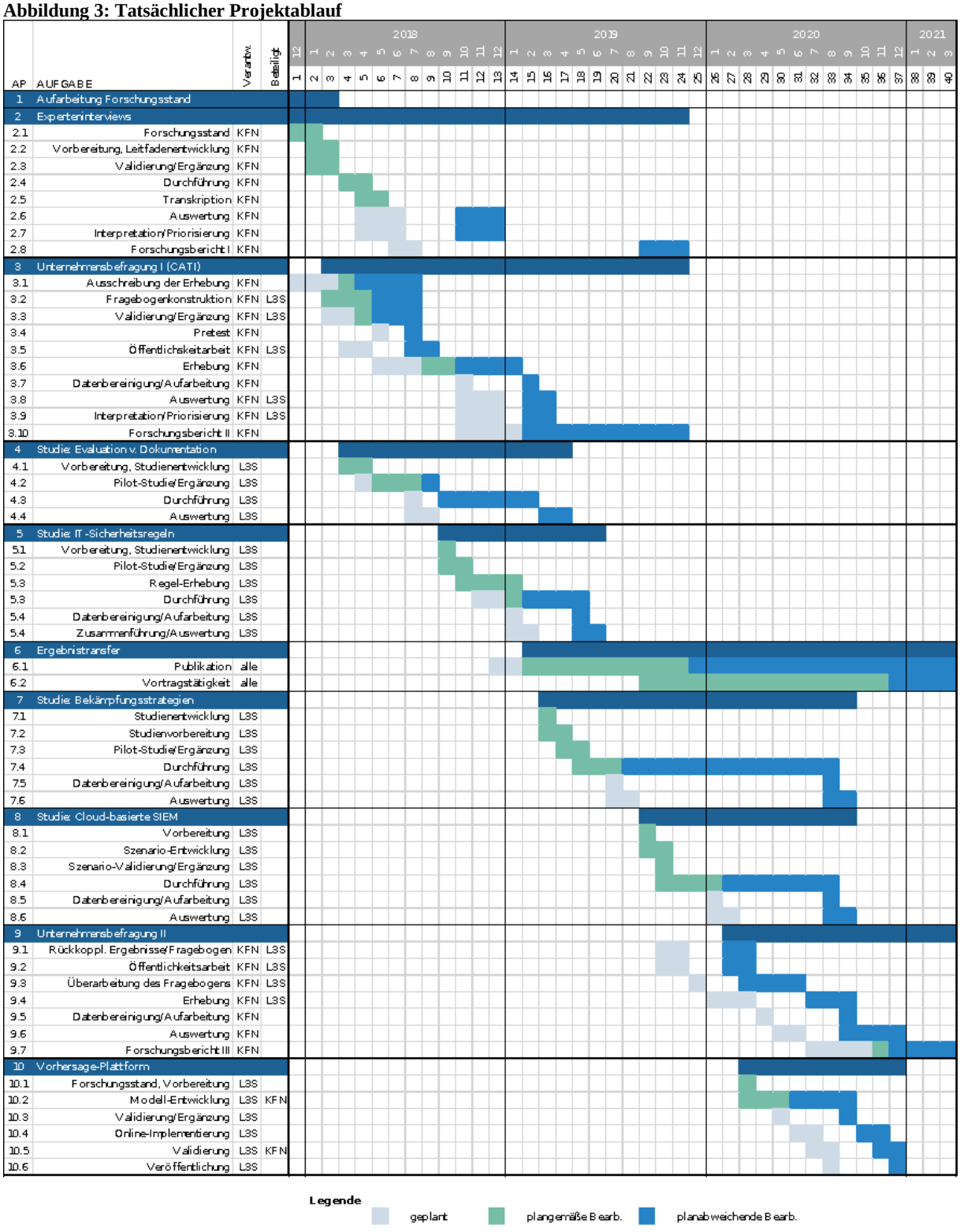
Die Aufarbeitung des Forschungsstandes (AP 1) und eine Expertenbefragung (AP 2) bildeten die Grundlage für die Unternehmensbefragung mit zwei Messzeitpunkten (AP 3 und 9) und die Feldstudien "Evaluation von Dokumentation im Kontext von KMUs" (AP 4), "IT-Sicherheitsregeln im Arbeitsalltag" (AP 5), "Strategien zur Bekämpfung von Cybercrime" (AP 7) und "Benutzbarkeit von Cloud-basierten SIEMs" (AP 8). Alle innerhalb des Projektes gewonnenen Erkenntnisse wurden für den Ergebnistransfer (AP 6) aufbereitet und in Form von Berichten, Factsheets und Vorträgen vermittelt. Die im Rahmen der Unternehmensbefragung erhobenen Daten bildeten die Grundlage für das in AP 10 entwickelte Risikoprognose-Tool CARE (Cyber Attack Risk Estimation) für KMU. Der geplante Ablauf ist in Abbildung 2 dargestellt.

Abbildung 2: Projektplan



In Abbildung 3 ist der tatsächliche Projektablauf zu erkennen. Das Projekt wurde insbesondere aufgrund der negativen Auswirkungen der Corona-Krise auf die Teilnahmebereitschaft in Hinblick auf die Unternehmensbefragung II (AP 9) und die Feldstudien (AP 7 und 8) kostenneutral um vier Monate bis März 2021 verlängert.

Abbildung 3: Tatsächlicher Projektablauf



Neben diesen verlängerten Durchführungszeiten, kam es zu weiteren zeitlichen Verschiebungen innerhalb des Projektes. Dafür können folgende Gründe mit Bezug auf die betroffenen Arbeitspakete angeführt werden: Personalwechsel innerhalb des Projektes (AP 2), länger dauernde Vorbereitungszeit für das Ausschreibungsverfahren und damit verbundene Verzögerung der CATI-Befragung (AP 3), länger dauernde Durchführung, Datenbereitstellung und Auswertung

der Befragung (AP 3), sowie langwierige Teilnehmer*innenrekrutierung bei den Feldstudien (AP 4 und 5) infolge des Wegfalls der geplanten Incentivierung. Mit Ausnahme der Unternehmensbefragung II (AP 9), konnten dennoch alle Ziele in der geplanten Projektlaufzeit (bis Nov. 2020) realisiert werden. Neben der genannten Laufzeitverlängerung, die eine erforderliche Erhöhung des Rücklaufs der Unternehmensbefragung II möglich machte, wurde dazu für die Feldstudien (AP 7 und 8) eine methodische Anpassung (Remote-Durchführung) vorgenommen. Damit entfiel die Notwendigkeit von Vor-Ort-Terminen bei den Unternehmen, was sich positiv auf die Teilnahmebereitschaft ausgewirkt hat und die Durchführung beschleunigte.

1.4 Forschungsstand

Das Bundeskriminalamt (BKA) erfasste in seinem Jahresbericht 2014 zur Cyberkriminalität insgesamt 49.925 in Deutschland begangene Straftaten (BKA 2014: 4). Im Hinblick auf die zukünftige Entwicklung der Cyberkriminalität gelangt das BKA zu einer alarmierenden Risikobeurteilung: „Die zunehmende Vernetzung, die Abhängigkeit vernetzter, sich selbst steuernder Produktionsprozesse und Logistikketten von der Verfügbarkeit der Netze und die Problematik der Trennung/Abschottung dieser Netze zum Internet, stellen dabei eine große Herausforderung dar. […] Eine Schädigung der IT-Infrastruktur von Unternehmen kann mittlerweile nicht mehr nur zur Störung der Kommunikation führen, sondern vielmehr auch zum kompletten Produktionsstillstand, was enorme Verluste für Unternehmen nach sich ziehen würde. Insbesondere die Gefahr der digitalen Erpressung von Unternehmen steigt dadurch“ (BKA 2014: 13).

Diese vom BKA vorgetragene Einschätzung beruht primär auf den von ihm erfassten, angezeigten Fällen von Cyberkriminalität. Hinzu kommt das Dunkelfeld der nicht bekannt gewordenen Fälle. Hierzu wurden in den letzten vier Jahren verschiedene Studien vorgelegt. Die erste hatte das BMWI bei der WIK Consult in Auftrag gegeben und im Jahr 2012 veröffentlicht. Im Rahmen der Untersuchung wurden 955 KMU-Unternehmen zur IT-Sicherheit befragt. 2012 folgte eine zweite Erhebungswelle mit 922 Unternehmen, mit der das Ziel verfolgt wurde, die Erkenntnisse aus der ersten Studie weiter zu vertiefen. 62 Prozent der hieran beteiligten Firmen hatten bereits an der ersten Befragung mitgewirkt. Die WIK Consult konzentrierte sich weitgehend darauf, die verschiedenen Maßnahmen zu erfragen, die bei den Firmen die IT-Sicherheit gewährleisten sollten. Cyberangriffe wurden nur in sehr groben Kategorien erfasst und schlossen zudem auch Spam-Mails mit ein. Außerdem wurde nicht untersucht, ob die von kriminellen Cyberangriffen betroffenen Unternehmen die Polizei eingeschaltet haben und welche Erfahrungen sie hiermit gegebenenfalls sammeln konnten. Als wichtiger Befund der zweiten Erhebungswelle wurde hervorgehoben, dass die Unternehmen trotz des von ihnen berichteten Anstiegs der IT-Sicherheitsrisiken und der daraus erwachsenden Schäden nur selten ausreichende Gegenmaßnahmen ergriffen hätten.

Ein Jahr nach der WIK-Studie führte die Industrie- und Handelskammer Nord innerhalb der norddeutschen Bundesländer eine schriftliche Online-Befragung von 713 Unternehmen durch (IHK-Nord 2013). 33 Prozent der mitwirkenden Firmen gaben an, innerhalb eines Jahres mindestens einen Cyberangriff erlebt zu haben. Die große Mehrheit von ihnen hatte sich diesbezüglich nicht an die Polizei gewandt. Einen entsprechenden Befund erbrachte auch eine von

Bitkom in Auftrag gegebenen Studie (Bitkom 2015). Sie zeigte, dass nur jedes fünfte der 1.074 befragten Unternehmen nach einem Cyberangriff staatliche Stellen informiert hatte (Bitkom 2015: 24). Dabei war die Hälfte der befragten Unternehmen innerhalb der letzten zwei Jahre von Wirtschaftsspionage, Sabotage oder Datendiebstahl betroffen. Die höchsten Viktimisierungsraten ergaben sich für die Industrie und das Finanzwesen. Ansonsten aber blieb offen, welche Einflussfaktoren das Risiko solcher Angriffe erhöhen oder reduzieren.

Die „e-Crime-Studie" der KPMG erhebt alle zwei Jahre Informationen zum Phänomen Internetkriminalität gegenüber Unternehmen (KPMG 2015). Dabei wurden in der aktuellen Studie von 2015 505 Unternehmen aus unterschiedlichen Branchen und mit verschiedenen Umsatzgrößen befragt. Im Ergebnis zeigte sich, dass 40% der befragten Unternehmen innerhalb von zwei Jahren von Cyberangriffen betroffen waren, wobei dies besonders häufig auf Finanzdienstleister zutraf. Die Hälfte der Unternehmen gab an, sich „(…) durch ehemalige Arbeitnehmer beziehungsweise Insider bedroht (…)" zu fühlen (KPMG 2015: 17). Ebenso kommen auch andere Untersuchungen zu dem Ergebnis, dass es sich bei einem hohen Anteil der Täter/-innen um (ehemalige) Mitarbeiter/-innen handelt (Bitkom 2015: 20; in Bezug auf Datendiebstahl siehe Rantala 2008: 2; Smith et al. 2003: 7).

Eine weitere Studie zum Thema Cybercrime gegen Unternehmen haben PwC und die Universität Halle (PwC, Universität Halle 2016) im Jahr 2016 vorgelegt. Auf der Basis einer telefonisch durchgeführten Fragebogenerhebung mit 720 Unternehmen mit mindestens 500 Mitarbeitern registrierten die Autoren im Vergleich zu der 2013 entsprechend durchgeführten Befragung einen deutlichen Anstieg der IT-Angriffe. Im Hinblick auf das Ausspähen und Abfangen sicherheitsrelevanter Daten und den Diebstahl von Kunden- und Unternehmensdaten sei sogar eine Verdoppelung festzustellen, wenn man auch die im Rahmen der Untersuchung erfassten Verdachtsfälle berücksichtigt (ebd.: 20). Insgesamt betrachtet wurden nach dieser Studie im Verlauf von zwei Jahren 34 Prozent der befragten Unternehmen Opfer von Cybercrime. Weitere fünf Prozent berichteten zudem von entsprechenden Verdachtsfällen. Am häufigsten genannt wurden der Computerbetrug, die Manipulation von Konto- und Finanzdaten sowie das Ausspähen und Abfangen von Daten (z. B. Passwörter). Nach Angabe der befragten Firmen ist ihnen im Durchschnitt aus derartigen Cyberangriffen ein Schaden von 337.000 Euro entstanden. Der im Vergleich dazu niedrige Medianwert von 30.000 Euro zeigt allerdings, dass einer kleinen Anzahl von extrem hohen Schadensfällen mehrheitlich solche gegenüberstehen, die vergleichsweise gering ausfallen. Beachtung verdient ferner der Befund, dass die durchschnittliche Schadenshöhe umso höher liegt, je größer die Unternehmen sind. Bei solchen mit mehr als 10.000 Mitarbeitern liegt der durchschnittliche Schadensbetrag bei 4,4 Millionen Euro. Er beträgt dagegen „nur" 150.000 Euro für Unternehmen, die weltweit zwischen 500 und 999 Personen beschäftigen.

Im Vergleich zu diesen durchweg in Deutschland durchgeführten Studien zeigen Forschungsberichte aus den USA deutlich höhere Viktimisierungsraten. Dies hängt möglicherweise damit zusammen, dass dort die Digitalisierung der Wirtschaft weiter fortgeschritten ist. In die größte derartige Untersuchung konnte Rantala (2008) 8.000 Unternehmen einbeziehen. Sie erbrachte, dass bereits innerhalb von nur 12 Monaten vor der Datenerhebung 60 Prozent der Befragten mindestens einen Cyberangriff erlebt hatten. Auch hier fällt die Anzeigequote mit 15 Prozent

sehr niedrig aus. Der häufigste Grund für eine Nichtanzeige war, dass diese als aussichtslos eingeschätzt wurde (Rantala 2008).

Bei Einbeziehung internationaler Studien fällt ferner auf, dass die Unternehmen den Anteil der Organisierten Kriminalität (OK) sehr hoch einschätzen. Laut dem United Nations Office on Drugs and Crime (UNODC, 2016) sind über 80 Prozent der Cyberangriffe organisiert und werden strukturiert und zielorientiert durchgeführt. Eine entsprechende Einschätzung haben bei der von PwC und der Universität Halle 2015 durchgeführten Befragung nur 30 Prozent der Unternehmen abgegeben (PwC/Universität Halle 2016: 27). Die vom Bundesamt für Sicherheit in der Informationstechnologie (BSI) gegründete Allianz für Cyber-Sicherheit benennt allerdings auf der Basis einer Umfrage des Jahres 2015 die Organisierte Kriminalität für die kommenden Jahre als die Angreifer*innengruppe mit dem höchsten Bedrohungspotenzial: „Der bestehende Markt, auf dem die Schwachstellen, Angriffsmethoden oder die Durchführung von Cyberangriffen offeriert werden, sorgt dafür, dass die Gefährdungslage unübersichtlicher wird. So bieten Organisationen ihre Fähigkeiten und Leistungen auch anderen interessierten Kreisen im Rahmen von Auftragsarbeiten an („Cybercrime-as-a-Service“). Damit werden hochwertige Angriffe auch für Organisationen und Staaten verfügbar, die diese Expertise bisher nicht eigenständig bzw. aufgrund mangelnder Fähigkeiten grundsätzlich nicht ausbauen können“ (BSI 2015: 36). Angesichts dieser Entwicklungen gelangen auch die Autoren des von PwC und der Universität Halle vorgelegten Forschungsberichtes zu der Einschätzung, dass aufgrund der fortschreitenden Digitalisierung von Gesellschaft und Wirtschaft auch die OK in Deutschland ihre Aktivitäten vermehrt in die digitale Welt verlagern wird (2016: 27).

Insgesamt betrachtet zeigt der Überblick insbesondere zu den in Deutschland durchgeführten Studien, dass sie sich ganz überwiegend darauf beschränkt haben, Cybercrime deskriptiv zu erfassen. Dargestellt werden die Häufigkeit und Vorgehensweise von Cyberangriffen, teilweise auch die dadurch entstandenen Schäden sowie Risikoeinschätzungen der beteiligten Firmen. Es mangelt jedoch an systematischen Analysen zum Zusammenhang der verschiedenen Einflussfaktoren und an einer breit angelegten Differenzierung nach Unternehmenstypen. So wurde bisher nicht untersucht, in welchem Ausmaß bestimmter Verhaltensweisen von Unternehmen und spezifische Unternehmensmerkmale mit einer stärkeren Anfälligkeit von Cyberangriffen in Verbindung stehen.

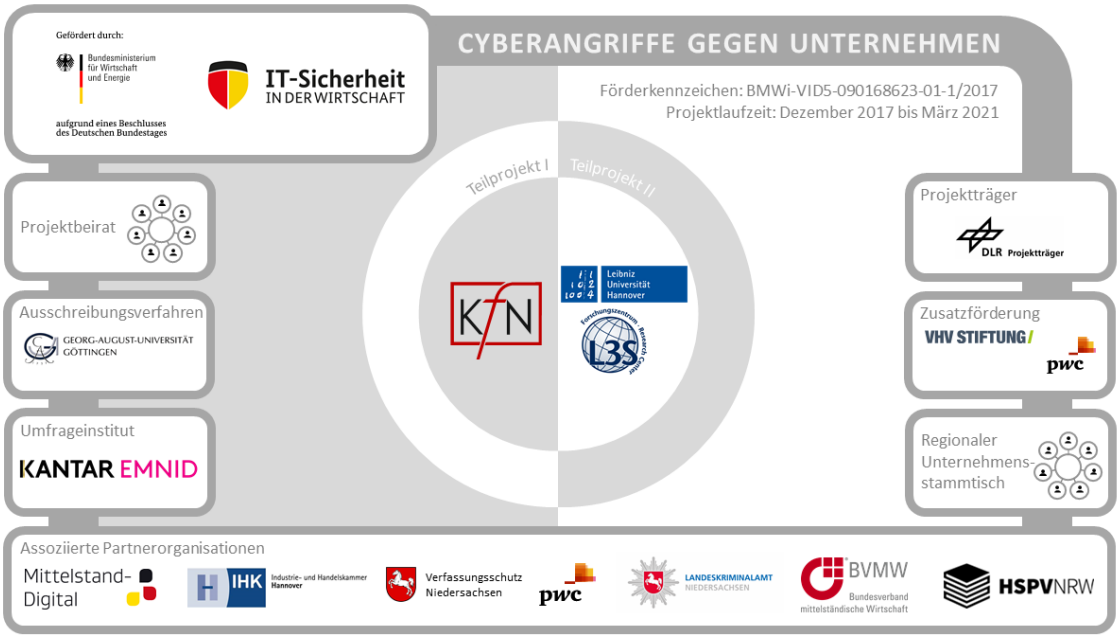
Eine wichtige Frage ist deshalb zu wenig geklärt worden: Was unterscheidet Unternehmen mit geringer Cybercrime-Belastung von solchen, die hier erhebliche Schäden erlitten haben? Nur wenn derartige Analysen durchgeführt werden, eröffnet sich die Möglichkeit, bestimmte Verhaltensweisen als „Risikoverhalten“ zu erkennen und darauf gestützt Vorschläge für eine effektive Prävention zu erarbeiten. Ein Hauptgrund ist hierfür, dass alle bisher in Deutschland durchgeführten Studien jeweils nur eine relativ geringe Zahl von Unternehmen befragen konnten. Dies hatte zur Folge, dass differenzierte Analysen zum Zusammenhang von Cyberangriffen und den von den Unternehmen eingerichteten Abwehrmaßnahmen nur ansatzweise oder gar nicht realisiert werden konnten. Hinzu kommt, dass die Studien durchweg einen wichtigen Aspekt vernachlässigt haben: Die Kooperation mit den Landeskriminalämtern bzw. den Verfassungsschutzbehörden. Die Frage, ob es sich für die von Cyberkriminalität betroffenen Unternehmen lohnt, mit den Sicherheitsbehörden zusammen zu arbeiten, konnte deshalb bisher nicht geklärt werden. Entsprechendes gilt für die Frage, in welchem Ausmaß die betroffenen Firmen

Schadenersatz von Versicherungen erhalten konnten und wie sie generell gegen Cyberkriminalität versichert sind.

1.5 Zusammenarbeit mit anderen Stellen

Innerhalb des Vorhabens wurde das Konsortium von mehreren assoziierten Partnern begleitet und unterstützt (Abbildung 4). Neben dem BMWi und dem DLR-Projektträger standen Vertreter*innen der folgenden Organisationen innerhalb eines dreimal tagenden Projektbeirats beratend zur Verfügung und leisteten wichtige Unterstützung beim Wissenstransfer: der Bundesverband mittelständischer Wirtschaft, Mittelstand-Digital, die Industrie- und Handelskammer Hannover, das Landeskriminalamt Niedersachsen (LKA NI), der Verfassungsschutz Niedersachsen, der Lehrstuhl für Unternehmensrechnung und Wirtschaftsinformatik der Universität Osnabrück, der Lehrstuhl für Kriminologie und Soziologie der Hochschule für Polizei und öffentliche Verwaltung NRW in Köln, die VHV Versicherung und das IT-Sicherheitsunternehmen CIPHRON.

Abbildung 4: Projektbeteiligte



Neben dem Projektbeirat wurde von PwC Hannover ein Unternehmensstammtisch etabliert und elf Mal ausgerichtet, um in den Austausch mit Unternehmen innerhalb der Region Hannover zu treten. Diese Veranstaltungen hatten Workshop-Charakter, bei denen sowohl aktuelle Vorkommnisse bei den teilnehmenden Unternehmen als auch verschiedene Inputvorträge eine Diskussionsgrundlage schufen und wichtige Impulse für das Forschungsvorhaben lieferten:

- Christian Pursche (LKA NI): Die Arbeit der Zentralen Ansprechstelle Cybercrime (ZAC) für die Wirtschaft
- Jörg Peine-Paulsen (Verfassungsschutz): Aktuelle Bedrohungslage aus Sicht des Wirtschaftsschutzes

- Sascha Fahl (L3S): Vorstellung des Forschungszentrums L3S
- Fabian Scherschel (Heise-online): Cybercrime – Aktuelle Entwicklungen
- Joachim Mohs (PwC): Klassische Fallgruben der Informationssicherheit – Erfahrungen aus langjähriger Prüfung und Beratung
- Nial Moore (PwC): Game of Threats – Cyber Security-Simulation für Manager

Zusammen mit den Vertretern der teilnehmenden Unternehmen wurden z.B. spezifische Aspekte von Cyberangriffen besprochen, Zugangswege zu Unternehmen im Rahmen der Feldstudien, die dabei eigesetzte Virtualisierungsinfrastruktur (AP 7 und 8), die Fragebogen für die beiden Unternehmensbefragungen (AP 3 und 9) sowie das Risikoprognosetool (AP 10) diskutiert und getestet. So konnten sowohl die Erhebungsinstrumente als auch die Projektergebnisse hinsichtlich ihrer Darstellung und Verständlichkeit insbesondere für die Zielgruppe der kleinen und mittleren Unternehmen verbessert werden. Daneben wurden die Teilnehmenden bei der Interpretation und Einordnung der Forschungsergebnisse eingebunden und lieferten immer wieder wichtige Einblicke in den Arbeitsalltag von IT-Abteilungen in Unternehmen.

Das Ausschreibungsverfahren für die im Projekt geplante Unternehmensbefragung I (siehe unten) wurde von der Georg-August-Universität Göttingen durchgeführt und der Auftrag zur Durchführung der CATI-Befragung an das Umfrageinstitut Kantar Emnid (heute: Kantar Public) vergeben.

2 Eingehende Darstellung

2.1 Durchgeführte Arbeiten, angestrebte und erreichte Ziele

Alle durchgeführten Projektarbeiten sowie die angestrebten und erreichten Ziele werden im Folgenden nach den im Projektantrag definierten Arbeitspaketen im Detail vorgestellt.

2.1.1 Aufarbeitung Forschungsstand (AP 1: KFN)

Ziele des Arbeitspaketes umfassen das Zusammenführen und Auswerten von akademischen Arbeiten und Projekten mit Relevanz zu Cybercrime. Die zusammengeführten und systematisierten Ergebnisse ermöglichen es, den derzeitigen Stand der relevanten Forschung zu bestimmen und erlauben so eine gezieltere Ausrichtung von Fragestellungen. Zusätzlich ermöglicht der Überblick über bereits durchgeführte Arbeiten, dass bereits bestehenden Erkenntnissen in die Projektgrundlage mit eingebracht, und alternative, noch unbeantwortete Fragestellungen aufgezeigt werden können.

Insgesamt wurden 320 Titel in einem Literaturverwaltungsprogramm systematisch erfasst, innerhalb von 82 Gruppen kategorisiert sowie mit 1.055 Wissenselementen (Kommentaren, Schlagwörtern etc.) angereichert. Die gesichtete Literatur kann in vier Kategorien gegliedert und beschrieben werden.[5]

Graue Literatur:
Ein Großteil der bestehenden Literatur zum Thema „Cyberangriffe gegen Unternehmen“ kann dem Bereich der grauen Literatur zugeordnet werden. Hier handelt es sich häufig um Berichte, Reports oder Studien von IT-Sicherheitsanbietern, Beratungshäusern oder Versicherungsunternehmen etc. Diese Beiträge beschreiben das Phänomen oft rein deskriptiv und wenden i.d.R. keine wissenschaftlichen Forschungsmethoden oder Gütekriterien an bzw. nennen solche nicht. Oftmals handelt es sich dabei um nicht repräsentative Stichproben, da häufig der eigene Kundenstamm oder eine bestimmte Zielgruppe befragt wird. In dieser Kategorie präsentierte Ergebnisse weichen teilweise stark voneinander ab oder widersprechen sich sogar. Gründe dafür könnten die bereits erwähnte fehlende Repräsentativität aber auch eigene Auswertungsspielräume bzw. Interessen sein, um die Ergebnisse z.B. für Marketing-Zwecke einzusetzen.

Staatliche und internationale Organisationen sowie Verbände:
Zu Titeln in dieser Kategorie gehören Veröffentlichungen von Polizei- und Regierungsbehörden sowie Non-Profit-Organisationen (z.B. BKA, BSI, Europol, Weltbank, Bitkom, EU-Kommission, OECD etc.). Auch diese Titel beschreiben das Phänomen oft rein deskriptiv. Je nach Autor/in haben die Veröffentlichungen unterschiedliche Zielsetzungen. So informieren Polizeibehörden eher über offizielle Statistiken, die lediglich das Hellfeld abbilden. Große internationale Organisationen zielen oft auf die Standardisierung bzw. Systematisierung des Phänomens ab, um einheitliche Frameworks, Kriterienwerke und Strategien entwickeln zu können.

Wissenschaftliche Literatur:

[5] Eine tabellarische Darstellung der für AP 3 und 9 relevanten Studien (Stand März 2020) findet sich im Forschungsbericht zur Unternehmensbefragung I bei Dreißigacker et al. (2020: 183ff.).

Die wissenschaftliche Literatur in diesem Phänomenbereich wächst seit einigen Jahren stark an. Unterscheiden lassen sich hier u.a. Veröffentlichungen mit reinem IT-Fokus gegenüber Titeln, die ebenfalls menschliche und organisatorische Aspekte einbeziehen. Zuletzt genannte Veröffentlichungen zeigen vermehrt, dass sehr häufig der Faktor Mensch für Sicherheitsrisiken und Zwischenfälle verantwortlich ist. Ein starker Fokus der wissenschaftlichen Literatur im Bereich Cyberangriffe liegt u.a. auf der Betrachtung Cybercrime in Verbindung mit Privatpersonen sowie Privacy und vernachlässigt daher tendenziell die Unternehmensperspektive.

Aktuelle Presse und Berichterstattung:
Ein geringerer Anteil der erfassten Literatur entstammt der Kategorie aktuelle Presse und Berichterstattung. Hier werden aktuelle Geschehnisse und Ereignisse verfolgt, die ggf. mit in das Forschungsprojekt einfließen. Wissenschaftlich wertvolle Hintergründe, Theorien und Hypothesen spielen hier eine untergeordnete Rolle.

Der so erarbeitete Forschungsstand wurde in einem projektinternen Workshop von L3S und KFN einen Tag lang besprochen. Dabei wurde v.a. diskutiert, welche Ableitungen für weitere Erhebungen des Vorhabens hieraus gezogen werden. Der Stand der Arbeitsergebnisse des AP 1 kann folgendermaßen zusammengefasst werden (Auswahl):

Begriffsdefinitionen:
Eine wesentliche Erkenntnis und zugleich eine Herausforderung bei der Erarbeitung des Forschungsstandes ist das Fehlen einheitlicher und anerkannter Begriffe und Definitionen sowohl im nationalen als auch im internationalen Kontext. So sind Begriffe beispielsweise doppelt belegt oder gleiche Sachverhalte werden in verschiedenen Veröffentlichungen unterschiedlich bezeichnet. Dies erschwert zum einen die Vergleichbarkeit bisheriger Forschungen, zum anderen sensibilisiert es aber auch das Projektteam im Verlauf der weiteren Projektkommunikation und insbesondere in der Transferphase auf eine einheitliche und weitestgehend akzeptierte Sprechweise zu achten. Vor dem Hintergrund dieser Erkenntnisse wurden Begriffsdefinition durch das Projektteam erarbeitet und für eine Berücksichtigung während der weiteren Forschungsarbeiten abgelegt.

Systematisierung von Cyberangriffen:
Neben den Begriffsdefinitionen wurde aus den Erkenntnissen des Forschungsstandes ein System zur Kategorisierung von Cyberangriffen erarbeitet. Diese Systematisierung berücksichtigt die verschiedenen Dimensionen eines Angriffes und bietet daneben weitere Vorzüge. Sie unterstützt die qualitative Auswertung der Experteninterviews und hilft den Fragebogen zur Unternehmensbefragung sinnvoll und weitestgehend ganzheitlich zu gestalten.

Ausgewählte Erkenntnisse und Hypothesen:
Wie bereits skizziert, ist das durch die Erarbeitung des Forschungsstandes entstandene Bild auf das Phänomen „Cyberangriffe gegen Unternehmen“ keineswegs homogen. Veröffentlichungen von unterschiedlichen Akteuren in verschiedenen Regionen, mit teilweise konträren Zielsetzungen, Methoden und Datenbasen führen mitunter zu uneinheitlichen, teilweise sogar widersprüchlichen Aussagen. In einem Punkt sind sich jedoch viele Veröffentlichungen einig: Cyberangriffe auf Unternehmen sind ein stark wachsendes sowie wirtschaftlich, gesellschaftlich und politisch zunehmendes Spannungsfeld, welches weiterer Untersuchung und der Erarbeitung solider Lösungen bedarf. Im Folgenden wird eine Auswahl zentraler Erkenntnisse und Hypothesen aufgeführt:

- Eine Verlagerung von analogen Straftaten in die digitale Welt ist beobachtbar
- Cybercrime weist ein sehr hohes Dunkelfeld auf
- Wichtige Aussagen bestehender Studien werden auf Basis mitunter geringer oder nicht repräsentativer Stichprobengrößen begründet
- Es fehlen geeignete Methoden um die Kosten eines Cyberangriffes in einem angemessenen Verhältnis von Aufwand und Nutzen zu ermitteln. Die Spanne der Schäden einzelner Unternehmen variiert sehr stark und geht kaum auf etwaige Unternehmensmerkmale ein
- Es fehlt an einer soliden Datenbasis für Unternehmen entstandene Kosten durch Cyberangriffe
- Unternehmen kennen ihre schützenswerten Daten nur unzureichend
- Risiko- bzw. Schutzfaktoren für bzw. gegen eine Viktimisierung von Unternehmen durch Cyberangriffe wurden bislang wenig systematisch erforscht. Es gibt jedoch Hinweise, dass Unternehmen unterschiedlich stark von Cyberangriffen betroffen sind. Unterschiede wurden beispielsweise in folgenden Bereichen festgestellt: Branche, Region, (De-)Zentralität, Marktführer, Unternehmensgröße etc.
- Täter mit Insiderwissen sind ein bislang unterschätztes Risiko. Hier fallen sehr oft sehr hohe Schäden bei Unternehmen an
- Cybercrime-Risikoeinschätzungen fallen für die Allgemeinheit schwerwiegender aus, als für das eigene Unternehmen. Dies kann u.a. auf falsche Selbsteinschätzungen oder eine übertriebene mediale Präsenz des Themas zurückzuführen sein
- Hypothese, dass die Anzahl der Angriffe nicht zwangsläufig steigt, sondern Angriffe häufiger erkannt werden. Dies wäre eine positive Entwicklung
- Hypothese, dass weniger die Technik, sondern häufig Menschen ein IT-Sicherheitsrisiko darstellen

Die Erkenntnisse der Aufbereitung des Forschungsstandes, z.B. aktuelle Trends und Entwicklungen, flossen u.a. in die Entwicklung der Experteninterview-Leitfäden (AP 2) und in den Entwurf des Fragebogens zur Unternehmensbefragung I (AP 3) ein.

*2.1.2 Expert*inneninterviews (AP 2: KFN)*

Ziel der Expert*inneninterviews war es, die Sicht der Akteure der Praxis in Bezug auf das Phänomen Cyberangriffe auf Unternehmen zu erfassen und in diesem Sinn gesichertes Expertenwissen zu gewinnen. Dabei handelt es sich um zwei Arten von Expert*innen: Zum einen sollen Akteure staatlicher Behörden sowie der Privatwirtschaft mit besonderem Fokus auf die Versicherungswirtschaft, die allgemein mit der Bekämpfung von Internetkriminalität beschäftigt sind, befragt werden. Diese Expert*innenbefragungen waren auf die Probleme der Strafverfolgung, die Kooperation mit betroffenen Unternehmen, deren IT-Sicherheit und Präventionsmöglichkeiten gerichtet.

Zum anderen sollen Expert*innen befragt werden, die konkret in der IT-(Sicherheits-)Abteilungen von Unternehmen aktiv sind. Diese zielten insbesondere auf die IT-Sicherheit der Unternehmen sowie auf die vorhandenen Kenntnisse und Handlungsabläufe bei einem Sicherheitsvorfall. Diese von L3S geführten Interviews mit IT-Spezialist*innen erfolgten telefonisch. Die Ergebnisse wurden zusätzlich zur Konzeption der Feldstudien (AP 4, 5, 7 und 8) genutzt.

Für die IT-Interviews des L3S mit KMUs wurde ein entsprechend zugeschnittener Leitfaden entwickelt, pilotiert und neun Interviews durchgeführt. Dabei handelte es sich um Gespräche mit den für IT zuständigen Abteilungen in KMUs sowie externer Dienstleister auf die wir hingewiesen wurden. Unter den neun geführten Interviews befanden sich drei externe Dienstleister und sowohl zu ihrem eigenen Stand der IT als auch zu denen der Kunden und der allgemeinen Kundschaft befragt, sodass detaillierte Informationen zu zwölf KMUs erhoben werden konnten. Die Interviews wurden vollständig transkribiert, anonymisiert und in einem "open coding" Ansatz mit 2 Wissenschaftlern ausgewertet.

Als erste Erkenntnisse der Interviews sind Begrifflichkeiten wie Phishing und Kreditkartenmissbrauch in die Systematisierung des Begriffes Cybercrime aus AP1 eingeflossen. Weiterhin werden die Interviews analysiert in Bezug auf:

- Fragestellungen und Unklarheiten zur IT-Sicherheit
- Relevanz und Bedeutung von IT(-Sicherheit) in Unternehmen
- Bekanntheit von Cybercrime-arten
- Verbreitung von Standards und Zertifizierungen im Kontext von Cybersicherheit
- Verbreitung konkreter technischer Sicherheitsmaßnahmen
- Relevanz und Umgang mit Kundendaten
- Erfassung und Erkennung von Cybercrime Vorfällen
- Notfallpläne und Verhalten bei einem Cybercrime-Vorfall

Diese qualitativen Ergebnisse wurden genutzt, um den Interview-Leitfaden für die Unternehmensbefragung I entsprechend anzupassen, fehlende Kategorien oder Unterkategorien für die IT-Sicherheit zu ergänzen, eine für KMUs verständliche Wortwahl zu finden und weitere Herausforderungen für die Arbeitspakete (AP 4, 5, 7 & 8) des Projektes zu identifizieren.

Für die vom KFN vor Ort durchgeführten Experteninterviews mit relevanten Behörden und Versicherern wurden entsprechend zugeschnittene Leitfäden entwickelt und insgesamt neun Interviews geführt. Dabei handelt es sich um Gespräche mit Experten der Zentralen Ansprechstellen Cybercrime (ZAC) der Landeskriminalämter Nordrhein-Westfalen, Sachsen, Niedersachsen und Bayern sowie dem Verfassungsschutz Niedersachsen, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und den Versicherungsunternehmen HDI und VHV sowie der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) der Generalstaatsanwaltschaft Frankfurt a.M.

Nach der Transkription und Anonymisierung wurde mit Hilfe der Software MAXQDA ein Kategoriensystem erstellt und Intercoderreliabilität überprüft. Aufgrund des Wechsels der Projektleitung und den zeitgleich anstehenden Vorbereitungsarbeiten für die Unternehmensbefragung I (AP 3) wurde die Auswertung nicht wie geplant zwischen April und Juni, sondern zwischen Oktober und Dezember 2018 durchgeführt. Die zentralen Ergebnissen, die detailliert in einem KFN-Forschungsbericht dokumentiert wurden,[6] werden im Folgenden noch einmal zusammengefasst:

- **Risikofaktoren:** Die IT-Sicherheit erhält in vielen Unternehmen vor dem Hintergrund der zunehmenden Digitalisierung noch nicht die notwendige Aufmerksamkeit, um auf

[6] Stiller et al. 2020.

bestehende Risiken wie Cyberkriminalität angemessen zu reagieren. Fehlende Awareness gilt demnach aus Sicht der Experten als zentraler Risikofaktor. Innovative und rentable Geschäftsideen oder Daten machen Unternehmen für potentielle Angreifer*innen zusätzlich attraktiv und steigern das Viktimisierungsrisiko. Insbesondere kleinere Unternehmen sind nach Expertensicht durch fehlende Ressourcen bezüglich IT-Sicherheit in der Regel schlechter aufgestellt als größere und entsprechend leichter anzugreifen.

- **Sicherheitsmaßnahmen:** Relativ verbreitet sind aus Expertensicht „klassische" direkte Sicherheitsmaßnahmen, die eher kurzfristig und kostengünstig ausgelegt sind (bspw. aktuelle Antivirensoftware, Firewalls, verschlüsselte Datensicherungen). Vergleichsweise selten werden Maßnahmen zur Steigerung der Resilienz wahrgenommen, die eher langfristig ausgelegt und ressourcenintensiv sind (bspw. IT-Sicherheitsbeauftragte, Incident-Response-Teams, regelmäßige Penetrationstests).
- **Probleme der Strafverfolgung:** Die Experten schätzen das Dunkelfeld im Bereich der Cyberkriminalität als sehr groß ein. Dies resultiere aus unentdeckten Angriffen, unzureichender Erfassung von Angriffen aus dem Ausland sowie aus einer geringen Anzeigequote. Als Gründe für die geringe Anzeigebereitschaft werden u.a. Befürchtungen eines Imageschadens sowie befürchtete Beeinträchtigungen des Betriebs durch die Ermittlungsarbeit gesehen. Die Zentralen Ansprechstellen Cybercrime für die Wirtschaft (ZAC) sind noch nicht überall bekannt und Anzeigen erfolgen von den Unternehmen häufig zu zögerlich, um einen aussichtsreichen Ermittlungsansatz zu finden. Die Dynamik des Feldes (u.a. Möglichkeiten der Anonymisierung, Vielzahl der Angriffsvektoren) führt zu einem stetigen Anpassungszwang der Behörden (Aktualität der Ermittlungsmethoden, Zuständigkeiten) und setzt den bestehenden rechtlichen Mitteln Grenzen. Die Rekrutierung qualifizierten Personals mit IT-Kompetenzen stellt die Behörden vor Probleme, da sie insbesondere in Hinblick auf die Bezahlung kaum mit der Wirtschaft konkurrieren können. Hinzu kommt eine damit zusammenhängende hohe Personalfluktuation in diesem Bereich.
- **Täter*innen:** Nach Einschätzung der Experten verlagern sich klassische Delikte wie Betrug und Erpressung zunehmend in den digitalen Raum. In Hinblick auf die Täter*innen wird ein breites Spektrum wahrgenommen, das von Einzeltäter*innen und gemeinschaftlich und arbeitsteilig vorgehenden Täter*innen ohne Beziehung zu den betroffenen Unternehmen über Täter*innen konkurrierender Unternehmen oder (ehemalige) Beschäftigte bis hin zu Nachrichtendiensten anderer Staaten reicht. Die Tatmotivation ist entsprechend sehr unterschiedlich (z.B. ideologisch, monetär, persönlich).
- **Offene Fragen/Forschungsbedarf:** Vor dem Hintergrund des mutmaßlich sehr großen Dunkelfeldes, besteht ein großer Forschungsbedarf hinsichtlich der Verbreitung von Cyberangriffen und verschiedener Angriffsarten innerhalb eines Jahres. Über das Ausmaß und die Art der Folgen von Cyberangriffen für betroffene Unternehmen besteht große Unklarheit. Darüber hinaus ist offen, welche weiteren Faktoren, das Risiko eines Cyberangriffs entscheidend beeinflussen (Wie können sich insbesondere kleine und mittlere Unternehmen mit geringeren Ressourcen schützen?). Die Präventionsarbeit der Behörden fokussiert vor allem kleine und mittlere Unternehmen. Hier besteht Unklarheit darüber, wie erfolgreich diese Unternehmen bisher erreicht wurden und wie bekannt vor allem die Zentralen Ansprechstellen Cybercrime (ZAC) sind.

Diese Ergebnisse flossen ebenfalls in die Konzeption des Fragebogens für die Unternehmensbefragung (AP 3 und 9) ein. Daneben wurden von diesen Ergebnissen folgende **Handlungsempfehlungen** in Hinblick auf die Arbeit der Strafverfolgungsbehörden abgeleitet:

- Die Bekanntheit der zentralen Ansprechstellen (ZAC) und deren Möglichkeiten sollte sowohl unter den kleinen und mittleren Unternehmen als auch in anderen Polizeidienststellen z.B. über Informationskampagnen gesteigert werden. Dies dürfte sich förderlich auf die Ermittlungsarbeit und die Anzeigebereitschaft auswirken.
- Um Befürchtungen hinsichtlich der Beeinträchtigung des Betriebsablaufs oder mangelndem Vertrauen in die Strafverfolgungsbehörden (vgl. auch Bollhöfer & Jäger, 2018) entgegenzuwirken, sollten Unternehmen stärker über die Vorgehensweisen, die Möglichkeiten und Grenzen der polizeilichen Ermittlung bspw. im Rahmen von Awareness-Schulungen und Beratungsangeboten aufgeklärt werden.
- Die Geeignetheit technischer und rechtlicher Mittel der Strafverfolgung ist in Hinblick auf eine wahrgenommene Deliktverschiebung in den digitalen Raum zu überprüfen und ggf. anzupassen. Vor dem Hintergrund eines permanenten Wandels potentieller Angriffsvektoren und Angriffsarten sollte sowohl die Überprüfung der technischen und rechtlichen Mittel der Strafverfolgung als auch der Aus- und Weiterbildungen der Mitarbeiter*innen regelmäßig erfolgen.
- Zur Verbesserung der Gewinnung und Bindung qualifizierten Personals mit IT-Kompetenz könnten Kooperationsmöglichkeiten mit Hochschulen, die Verbeamtung bisher angestellter Mitarbeiter*innen sowie die eigene Aus- und Weiterbildung innerhalb der Fachhochschulen für Polizei und öffentliche Verwaltung diskutiert werden.

2.1.3 Unternehmensbefragung I (AP 3: KFN)

Das Ziel der Unternehmensbefragung war es, differenzierte Informationen über das Ausmaß der Cyberangriffe, die den Unternehmen offenkundig geworden sind, zu erlangen und die Reaktionen (Anzeigeverhalten, Hinzuziehen von IT-Sicherheitsdienstleistern etc.) zu erheben. Ferner sollte analysiert werden, welche Faktoren das Risiko eines erfolgreichen Angriffs erhöhen und welche Schutzfaktoren bestehen. Bezüglich der Reaktion auf Angriffe war von Interesse, welche Erfahrungen mit der Polizei gemacht wurden und welche Gründe dafür vorliegen, sich nicht an die Polizei zu wenden. Hieraus sollten auch Ableitungen dafür gewonnen werden, wie eine Strafverfolgung gestaltet sein muss, damit Unternehmen sie vermehrt nutzen. Weiter war von Interesse, wie hoch die IT-Sicherheit der Unternehmen ist und inwiefern sie gegen Cyberangriffe versichert sind. Ferner sollte die Erhebung von spezifischen Unternehmensmerkmalen helfen, sinnvolle Differenzierungen zwischen Unternehmen treffen zu können.

Nach Ausschreibung und Vergabe der CATI-Erhebung an das Umfrageinstitut Kantar Emnid wurde die Befragung zwischen August 2018 und Januar 2019 mit plangemäß 5.000 Unternehmen ab zehn Beschäftigten auf Basis einer geschichteten Zufallsstichprobe durchgeführt. Nach Fertigstellung eines umfangreichen Forschungsberichtes[7] und der Erarbeitung einer Kurzfassung[8] für den Ergebnistransfer wurden beide Berichte gemeinsam im März 2020 unterstützt

[7] Dreißigacker et al. (2020).

[8] Kriminologisches Forschungsinstitut Niedersachsen (2020).

durch Pressearbeit (siehe AP 6) veröffentlicht. Zu den zentralen Ergebnissen der Unternehmensbefragung I zählen folgende Punkte:

- **Betroffenheit:** Über alle Angriffsarten hinweg waren etwa zwei Fünftel der Unternehmen ab 10 Beschäftigten in den letzten zwölf Monaten (immer bezogen auf die Zeit vor der Befragung) von mindestens einem Cyberangriff betroffen, auf den in irgendeiner Weise aktiv reagiert werden musste (41 %). Automatisiert abgewehrte Angriffe, z.B. Spam-E-Mails durch eine Firewall, sind hier nicht enthalten. Unterschieden nach Angriffsarten zeigt sich, dass vergleichsweise viele Unternehmen in den letzten zwölf Monaten von Phishing (22 %) und Schadsoftware-Angriffen (Ransomware: 13 %, Spyware: 11 % und sonstige Schadsoftware: 21 %) betroffen waren, gefolgt von CEO-Fraud (8 %), (D)DoS (6 %), Defacing und manuellem Hacking (jeweils 3 %). Im Unternehmensgrößenvergleich fallen relativ große Unterschiede bezüglich Ransomware, Phishing und besonders beim CEO-Fraud auf. Große Unternehmen sind von diesen Angriffsarten anteilig deutlich häufiger betroffen als kleine Unternehmen. Neben einer höheren Präsenz im Internet und einer umfangreicheren IT-Infrastruktur wirkt sich wahrscheinlich auch die mit der Unternehmensgröße zunehmende Anonymität unter den Beschäftigten aus. Weitere signifikante Unterschiede hinsichtlich der Betroffenheit der Unternehmen zeigen sich zwischen verschiedenen Branchen bzw. Wirtschaftszweigen. Unternehmen der Daseinsvorsorge waren z.B. seltener betroffen (31,1 %) als Unternehmen der übrigen Branchen (42,3 %) und scheinen demzufolge tendenziell besser geschützt zu sein oder entgegen der Erwartung weniger angegriffen zu werden.
- **Risikofaktoren:** Große Unternehmen (ab 500 Beschäftigte) mussten zwar anteilig deutlich häufiger auf Cyberangriffe in den letzten zwölf Monaten reagieren (58 %) als kleine Unternehmen (10-49 Beschäftigte: 39 %). Dieser Unterschied relativiert sich jedoch, wenn zusätzlich weitere Unternehmensmerkmale in den Blick genommen werden. Die Betroffenheitsraten innerhalb der Gruppen kleiner und mittlerer Unternehmen sind zum Teil sehr viel höher, wenn sie z.B. mehrere Standorte in Deutschland, mindestens einen zusätzlichen Standort im Ausland haben oder Güter bzw. Dienstleitungen exportieren. Bei Unternehmen, die über besondere Produkte, Herstellungsverfahren etc. oder eine besondere Reputation/ Kundenkreise verfügen, ist der Anteil der Betroffenen ebenfalls deutlich größer als bei den übrigen Unternehmen.
- **Folgen der schwerwiegendsten Cyberangriffe:** Für die Beantwortung weiterer Detailfragen sollten die befragten Unternehmen den schwerwiegendsten Angriff der letzten zwölf Monate auswählen. Bei 70 % der betroffenen Unternehmen entstanden direkte Kosten infolge dieses schwerwiegendsten Angriffes, wobei dieser Anteil bei kleinen Unternehmen (10-49 Beschäftigte: 72 %) etwas höher lag als bei den großen (ab 500 Beschäftigte: 65 %). Bei kleineren Unternehmen entstanden vergleichsweise häufig Kosten durch externe Beratung und die Wiederherstellung und Wiederbeschaffung, da sie in der Regel weniger eigene IT- oder sogar IT-Sicherheitsabteilungen haben und daher häufiger Dritte zu Rate ziehen mussten. Neben den genannten Kostenpositionen wurden insgesamt am häufigsten Kosten für Sofortmaßnahmen zur Abwehr und Aufklärung angeführt (40 %). Von Kosten durch Schadensersatz/ Strafen (1 %) und abgeflossene Gelder (2 %) wurde hingegen relativ selten berichtet. Die Höhe der direkten Gesamtkosten konnten bei 31 % der Unternehmen, bei denen Kosten entstanden sind,

aufgrund fehlender Angaben nicht berechnet werden. Bezogen auf die übrigen Fälle reichten die direkten Gesamtkosten bis zu 2 Mio. Euro, lagen im Durchschnitt bei rund 16.900 Euro und im Median bei 1.000 Euro. Auch wenn die direkten Kosten im Durchschnitt bzw. im Median erst einmal relativ gering erscheinen, darf nicht vergessen werden, dass sich diese auf jeweils einen Cyberangriff im letzten Jahr beziehen und auch versuchte Angriffe mitumfasst sind, die vereitelt werden konnten. In Hinblick auf die höheren Werte der angegebenen Gesamtkosten können „erfolgreiche" Cyberangriffe gerade für kleine und mittlere Unternehmen ein bestandsgefährdendes Ausmaß annehmen. Hinzu kommt, dass mögliche indirekte Kosten, wie z.B. Umsatzverluste aufgrund von Imageschäden oder erfolgreicher Produktspionage, die noch Monate nach dem Cyberangriff anfallen können, hier unberücksichtigt bleiben.

- **Anzeigeverhalten:** Bezogen auf den schwerwiegendsten Cyberangriff der letzten zwölf Monate gaben lediglich 12 % der Unternehmen an, diesen polizeilich angezeigt zu haben. Zu den am häufigsten angezeigten Angriffsarten zählen CEO-Fraud (25 %), Spyware (20 %) und manuelles Hacking (19 %). Große Unternehmen (ab 500 Beschäftigte) erstatteten mit 22 % häufiger Anzeige als kleine Unternehmen (10-49 Beschäftigte) mit 11 %. Bemerkenswert ist, dass über ein Fünftel der kleineren Unternehmen als Nichtanzeigegrund angab, gar nicht zu wissen, an wen man sich dafür zu wenden habe. Dies weist auf einen Informationsbedarf hin und bietet einen Ansatzpunkt zur Erhöhung der Anzeigequote. Der häufigste Nichtanzeigegrund ist allerdings die fehlende Aussicht auf einen Ermittlungserfolg (72 %). Befürchtungen von Imageschäden (3 %), Arbeitsbehinderungen (11 %) oder von behördlicher Einsicht in vertrauliche Daten (5 %) spielen demgegenüber nur eine kleinere Rolle.
- **Schutzfaktoren:** Viele der erfragten technischen IT-Sicherheitsmaßnahmen – z.B. regelmäßige Backups und deren physisch getrennte Aufbewahrung, aktuelle Antivirensoftware, regelmäßige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches sowie der Schutz der IT-Systeme mit einer Firewall – wurden von fast allen Unternehmen eingesetzt. Trotzdem waren viele dieser Unternehmen im letzten Jahr von mindestens einem Cyberangriff betroffen. Dieser Umstand weist darauf hin, dass die Wirkung technischer Maßnahmen mit weiteren Faktoren zusammenhängt. Neben der Qualität, dem Reifegrad sowie der sachgemäßen Konfiguration und Wartung der technischen Maßnahmen dürften dazu ebenso die Frage des Designs, der Nutzbarkeit und der Einbindung in organisatorische Abläufe und Prozesse zählen. Organisatorische IT-Sicherheitsmaßnahmen waren im Vergleich zu den technischen weniger weit verbreitet, standen aber fast alle im Zusammenhang mit der Betroffenheit von Cyberangriffen. Insbesondere Unternehmen, die ihre Richtlinien zur IT-Sicherheit und zum Notfallmanagement regelmäßig überprüfen und Verstöße gegebenenfalls ahnden, waren signifikant seltener in den letzten zwölf Monaten von Cyberangriffen betroffen als Unternehmen, die dies nicht taten. Es kommt also nicht nur darauf an, entsprechende Richtlinien und IT-Sicherheitsmaßnahmen einzuführen, sondern diese auch innerhalb des Unternehmens ‚zu leben'. Nicht vergessen werden darf, dass solche Richtlinien technische Maßnahmen voraussetzen, die sich in den Arbeitsalltag der Beschäftigten gut integrieren lassen sollten. Schriftlich fixierte Richtlinien zum Notfallmanagement, die Zertifizierung der IT-Sicherheit sowie regelmäßige Risiko- und Schwachstellenanalysen stehen ebenfalls im Zusammenhang mit niedrigeren Betroffenheitsraten. Schulungen zur IT-

Sicherheit für Beschäftigte weisen bei mittleren Unternehmen einen Zusammenhang mit einer niedrigeren Betroffenheit aus, während dies bei Mindestanforderungen für Passwörter vor allem bei den kleinen Unternehmen der Fall ist.

Der eingesetzte Fragebogen sowie die Ergebnisse der ersten Unternehmensbefragung wurden in Hinblick auf die Folgebefragung (AP 9) reflektiert und zur Konzeption des Online-Fragebogens genutzt. Darüber hinaus bildeten die Daten die Grundlage für die Vorhersageplattform (AP 10).

2.1.4 Feldstudie: Evaluation von Dokumentation im Kontext KMU (AP 4: L3S)

In diesem Arbeitspaket sollten Feldstudien mit ausgewählten Unternehmen, die an der Datenerhebung im Rahmen des Projekts teilnehmen, vor Ort durchgeführt werden. Ziel war es, zu untersuchen, wie eine gute und einfache Nutzbarmachung von ausgewählten Dokumentationen zur sicheren Konfiguration von IT-Systemen auch für kleinere und Kleinstunternehmen beiträgt. Die sichere Konfiguration von IT-Systemen ist als grundlegende Verteidigungslinie gegen Cybercrime zu verstehen. Die ausgewählten Dokumentationen sollten daher für möglichst viele Nutzer verfügbar und verständlich sein, so dass bei der Konfiguration von IT-Systemen ein möglichst hohes Maß an Sicherheit erreicht werden kann. Ziel dieses Arbeitspaketes war es zum einen die Qualität der aktuellen Dokumentationen im Hinblick auf Aktualität, Verständlichkeit und Effektivität zu ermitteln. Zum anderen sollten basierend auf diesen Erkenntnissen, mögliche Verbesserungsvorschläge ausgearbeitet und zur Verfügung gestellt werden, um zukünftige Dokumente zu verbessern. Zielgruppe waren vor allem kleinere und Kleinstunternehmen, die häufig keine dedizierten Mitarbeiter*innen für IT-Sicherheit haben, aber trotzdem ein möglichst großes Maß an IT-Sicherheit in ihrem Unternehmen umsetzen möchten.

Diese Studie wurde aufgrund von Rekrutierungsproblemen verlängert und die Anzahl der Teilnehmer in Rücksprache mit dem DLR-PT von 20 auf 15 reduziert. Das Tool wurde auf dem 2. Projektbeiratstreffen (20.03.2019) explizit vorgestellt und ermöglichte unter anderem eine Bearbeitung der Studie online oder unterwegs, um weniger eng an Arbeitszeiträume oder Termine gebunden zu sein und so die Rekrutierung und Teilnahme zu erleichtern. Bei der Vorstellung wurde jedoch entschieden, dass zunächst weiter auf Veranstaltungen und bei Vorträgen des Projekts rekrutiert werden soll, um so interessierte Firmen direkter ansprechen zu können. Außerdem wurde über die Newsletter der IHK und HannoverIT Einladungen zur Teilnahme an den Studien versendet.

Die Feldstudie konnte mithilfe dieser Maßnahmen abgeschlossen werden, als Evaluation wurden die beliebtesten Ressourcen für Cybersecurity von Seiten der Teilnehmenden KMUs ermittelt:

- **Allgemein Ressourcen:** Unabhängig von Größe und Sicherheitsverständnis werden folgende Plattformen (geordnet nach Häufigkeit der Nennung) verwendet, um Informationen zu Betrieb und ggf. Sicherheitslücken zu erhalten:
    - Google oder andere Suchmaschinen
    - IT-Journalismus, also Quellen wie Heise.de & Golem
    - Blogs, meist von Privatpersonen betriebene Blogs zu Setup und Wartung bestimmter Software

  - Interne Dokumentationen der Firmen
  - BSI Sicherheitskatalog
  - In wenigen Fällen IT-Notfallkarte des BSI an den Arbeitsplätzen

  Anmerkung: Speziell Blogs und Google Suche bestätigten sich hierbei in den späteren aufgabenbasierten Feldstudien als am häufigsten konsultierte Quellen für konkrete sicherheitsrelevante Aufgabenstellungen.

- **Ressourcen für professionelle IT-Abteilungen:** In den IT-Abteilungen von Bankendienstleistern und anderen Unternehmen mit großem Kundenstamm oder erhöhten Sicherheitsanforderungen zeigte sich neben der Schulung von Personal vor allem die Beobachtung, Einschätzung und Auswertung angekündigter CVEs, z.B. in der offiziellen Dankenbank (https://cve.mitre.org/cve/search_cve_list.html) oder auch über Ticker und Mailinglisten für Komponenten der verwendeten Infrastruktur. Aufgrund des hohen technischen Grades der Informationen in CVEs (Angabe der Datei und des exakten technischen Vorgehens für die Ausnutzung einer Sicherheitslücke) lässt sich hiermit sehr genaue Vorsorge und Umgang mit Sicherheitslücken betreiben, die aber auch ein hohes technisches Knowhow über die gesamte zu schützende Infrastruktur benötigt, was für kleine und mittlere Unternehmen vermutlich untauglich ist. Eine Eigenbeteiligung an den Mailinglisten zur grundlegenden Klärung von Unverständlichkeiten ist bei den meisten Mailinglisten generell unerwünscht und ein tieferes Verständnis der betroffenen Software wird vorausgesetzt.
- **Ressourcen für kleinere IT-Abteilungen:** Die am häufigsten genutzte Quelle von kleineren IT-Abteilungen in Unternehmen waren tatsächlich Interne Dokumentationen und die Google Suche. Hier wurde auch das “Hörensagen” von Kollegen aus anderen Bereichen als Quelle genannt, die für eine zuverlässige Betreuung der IT-Sicherheit aber untauglich ist.

Aus den qualitativen Informationen der Feldstudie konnte bei einigen Teilnehmern, speziell in kleineren IT-Abteilungen, auf ein niedriges Bewusstsein bezüglich Cyberangriffen geschlossen werden. Während der Ansatz über die direkten CVE Ankündigungen die genaueste, schnellste und am besten angepasste Bearbeitung von Sicherheitslücken ermöglicht, ist der benötigte Aufwand und das benötigte Level an Schulung für kleinere IT-Abteilungen tendenziell zu hoch. Hinzu kommt, dass kaum Unterstützung bei deren Bearbeitung geboten wird. Da ein Ziel unserer Vorhersageplattform (AP10) die Sensibilisierung und Schulung weniger professioneller Abteilungen in kleinen und mittleren Unternehmen ist, haben wir Quellen, die über CVEs direkt arbeiten und keine Unterstützung wie z.B. das BSI oder Journalistische Portale bieten, nicht in Betracht gezogen.

2.1.5 Feldstudie: IT-Sicherheitsregeln im Arbeitsalltag (AP 5: L3S)

Grundlegende Regelungen zur Verteidigung gegen Cybercrime sind wirkungslos, wenn sie im Arbeitsalltag nicht umgesetzt werde. Die möglichen Gründe für Abweichungen reichen von geänderten Anforderungen bis hin zu einfacher Ignoranz. Dieses Arbeitspaket umfasst einen Vergleich von sicherheitsrelevanten Arbeitsschritte mit den vorherrschenden, unternehmensinternen Regelungen. Hierbei ist insbesondere die Diskrepanz zwischen vorgegebenen Regelungen und den tatsächlichen Arbeitsabläufen im Alltag von Interesse. Ziele des Arbeitspaketes sind die Identifizierung von missachteten sicherheitsrelevanten Regelungen, die Feststellung

von möglichen Gründen für diese Abweichungen (Ausnahmen) und das Erarbeiten von Verbesserungsvorschlägen mit dem endgültigen Ziel, die IT-Sicherheit zu verbessern.

Die in AP 5 geführten Interviews erfolgten telefonisch und teilweise vor Ort. Mithilfe der in AP 4 erwähnten methodischen Anpassungen wurden hier weitere Interviews im Laufe des Jahres 2019 durchgeführt und das AP abgeschlossen. Die Interviews wurden nach Durchführung anonymisiert und transkribiert, bevor sie von zwei Wissenschaftler*innen durch einen an "thematic analysis" orientierten Ansatz qualitativ ausgewertet wurden.

Folgende Tendenzen und Schwierigkeiten haben wir in den Interviews festgestellt:

- **IT-Sicherheit Zuständigkeit:** Nur ein Unternehmen gab in unseren Interviews an, eine eigene Abteilung für IT-Sicherheit zu haben. Drei gaben an, dass sie externe Dienstleister zur Unterstützung zumindest teilweise mit einbeziehen.
- **Prozess-Zertifizierungen & Schulungen:** 70 % der Unternehmen aus unserem Sample an KMUs gaben an, keine Prozesse wie ITIL einzusetzen. Die verbleibenden 30 % setzten allerdings auch nur die notwendigen Abläufe nach Absprache mit dem Datenschutzbeauftragten, z.B. "orientiert an ITIL" oder "orientiert an den Anforderungen der GDPR/DSGVO", um. Hier ist klarer Nachbesserungsbedarf für KMUs zu erkennen, da Schulungen und von Mitarbeiter*innen umgesetzte Ablaufprozesse wichtig sind, um "Social Engineering"-Angriffe wie Phishing abzuwehren, die laut unserer Unternehmensumfragen (AP 3 und 9) eine hohe Prävalenz mit steigender Tendenz haben.
- **Backups:** Während beim Themenfeld Backups keine Ausnahmen oder ähnliches angegeben wurden, haben fünf Unternehmen zumindest Probleme und Anpassungen mit der Zeit gemeldet. Meist waren dabei Backuplösungen und Server zeitweise nicht erreichbar oder automatische Backups wurden nicht durchgeführt. Drei dieser Unternehmen setzen daher auf zwei kombinierte Backuplösungen anstelle von nur einem Anbieter. Ein weiteres Unternehmen gab an, zwar keine Probleme gehabt zu haben, aber auch regelmäßig zu prüfen, ob Backups planmäßig ablaufen und die Wiedereinstellung funktionieren würde. Zusammengefasst zeigten sich zwar solche kontrollierten Ansätze zur Verhinderung von Datenverlusten, die allerdings gleichzeitig auch auf Probleme beim Managen der Backups hinweisen.
- **Passwort Policies & andere Sicherheitsmaßnahmen:** Ein zentrales Ergebnis ist, dass in allen teilnehmenden Unternehmen Ausnahmen für Sicherheitsmaßnahmen aller Kategorien (außer Kommunikation) relativ selten waren und wenn, dann wurden diese meist gut begründet. Am häufigsten wurden Passwortrichtlinien genannt, die aufgrund von Mitarbeiter*innenbeschwerden für die ganze Firma geändert, dann aber konsequent durchgezogen wurden. Hier scheint der Trend von komplexen Policies mit mehreren Zeichenkategorien zu langen aber beliebigen Passwörtern zu gehen, was mit aktuellen Empfehlungen des BSI übereinstimmt.[9] Allerdings gab es auch ein Unternehmen im Sample, das nur vier Zeichen für ihre Passwörter verlangte und nur ein Unternehmen gab an, auf Passwort Manager für sichere Passwörter innerhalb des gesamten Unterneh-

[9] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

mens zu setzen. Außerhalb solcher generellen Anpassungen waren gemeldete Sicherheitsmaßnahmen und Ausnahmen sinnvoll implementiert und besprochen, z.B. die konsequente Verweigerung von Remote Zugriff auf Firmennetzwerke außer bei abgesprochenen Außeneinsätzen. Hier wurde dann für die Ausnahmen zum Beispiel auch sichere Lösungen wie VPNs oder SSH-tunnel implementiert, um die Ausnahmen sicher umzusetzen.

- **Kommunikationstools:** Generell wurden bei den Kommunikationslösungen von KMUs wenig Probleme genannt. E-Mail war in allen KMUs ein wichtiges Kommunikationstool, nur drei setzten dabei auf zusätzliche Schutzmaßnahmen wie S/MIME und PGP/GPG. Zusätzlich kamen in zwei Unternehmen interne Chatlösungen wie Mattermost zum Einsatz. Zwei weitere KMUs gaben ebenfalls an, dass in ihren Firmen WhatsApp zum Einsatz kommen würde. Zudem gaben zwei weitere Unternehmen an, dass ihnen bekannt sei, dass Mitarbeiter*innen auch entgegen den Anweisungen WhatsApp nutzen würden, dies aber geduldet sei oder auf Kundenwunsch geschehe. Dies ist aus Sicht der DSGVO bedenklich, da hierbei Metadaten von Kunden mit Facebook geteilt werden, auch wenn der Inhalt der Kommunikation selbst verschlüsselt ist.

Die Ergebnisse von AP 5 flossen hauptsächlich ins Design und die detaillierten Fragen zu Sicherheitsmaßnahmen der Unternehmensbefragung 2 (AP 9) ein. Allerdings zeigt sich hier in den gemeldeten Erfahrungen zu Kommunikationstools, dass vor allem Mitarbeiter*innenschulungen notwendig sind, um die sinnvolle Einhaltung von Sicherheitsvorgaben in Unternehmen umzusetzen. Dies wurde auch in der Vorhersageplattform (AP 10) in der Priorisierung von Schulungen berücksichtigt.

2.1.6 Ergebnistransfer (AP 6: KFN/ L3S)

Ziel dieses Arbeitspakets war es, die Ergebnisse der vorherigen Arbeitspakete in die Praxis zu transformieren. Dies bedeutet, dass Unternehmen über die Häufigkeit von Cyberangriffen und die Angriffsarten informiert werden sollen. Des Weiteren sollen sie jedoch auch über effektive Präventionsmaßnahmen und Unterstützungsmöglichkeiten aufgeklärt werden.

Für den Ergebnistransfer werden unterschiedliche Plattformen genutzt. Zum einen sollten kleinere Publikationen in Form von Flyern und Broschüren entstehen. Zum anderen wurden Vorträge und Workshops auf diversen Veranstaltungen gehalten. Ferner wurden verschiedene Online-Plattformen für den Transfer genutzt. Neben der Sensibilisierung für den Problembereich stand auch das Aufzeigen praxisgerechter Handlungsanleitungen im Fokus.

In Tabelle 1 finden sich alle Transferaktivitäten im Laufe des Projektes, bei denen das Projekt im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ sowie die Forschungsergebnisse vorgestellt wurden.

Tabelle 1: Projektbezogene Transferaktivitäten

Art	Details	Datum
Vortrag	Wollinger, Gina Rosa; Fahl, Sascha (2018): Cyberangriffe gegen Unternehmen. Hannover Messe, 23.04.2018, Hannover.	23.04.2018
Vortrag	Fahl, Sascha; Wollinger, Gina Rosa (2018): Cyberangriffe gegen Unternehmen. CEBIT, 12.06.2018, Hannover	12.06.2018
Projekt-Webseite	https://cybercrime-forschung.de	01.08.2018
Presseinterview	Berger, Michael B. (06.08.2018): Internetkriminalität nimmt rasant zu. Hannoversche Allgemeine Zeitung (HAZ). Abrufbar unter: http://www.haz.de/Nachrichten/Der-Norden/LKA-NIedersachsen-beobachtet-rasanten-Anstieg-der-Cyberkriminalitaet (zuletzt geprüft am 11.10.2018).	03.08.2018
Presseinterview	Neuthinger, Eva (14.09.2018): Erste Schritte zur Cybersicherheit. Handelsjournal (HDJ), 9/2018, S. 48.	09.08.2018
Vortrag	Wollinger, Gina Rosa; Dreißigacker, Arne (2018): Kriminologische Perspektiven auf das Phänomen Cybercrime. Internet Security Days (ISD), 20.09.2018, Brühl.	20.09.2018
Vortrag	Dreißigacker, Arne; Skarczinski, Bennet von (2018): Forschungsprojekt: Cyberangriffe gegen Unternehmen. Mittelstand-Digital Regionalkonferenz. Arbeitsgruppe IT-Sicherheit. Berlin, 08.11.2018.	08.11.2018
Vortrag	Dreißigacker, Arne (2018): Cybercrime im Hell- und Dunkelfeld. November der Wissenschaften. Kriminologisches Forschungsinstitut Niedersachsen e. V., Hannover, 08.11.2018.	08.11.2018
Vortrag	Wollinger, Gina (2018): Cyberangriffe gegen Unternehmen. November der Wissenschaft. Kriminologisches Forschungsinstitut e. V., Hannover, 08.11.2018.	08.11.2018
Vortrag	Wollinger, Gina Rosa; Stiller, Anja; von Skarczinski, Bennet; Dreißigacker, Arne: „Cybercrime gegen Unternehmen“ aus Sicht der Strafverfolgung. 24. Deutscher Präventionstag (DPT), 20.-21.05.2019, Berlin.	20.05.2019
Vortrag	Wollinger, Gina Rosa; Dreißigacker, Arne (2019): Empirische Befunde zum Phänomen Cyberangriffe gegen Unternehmen: Wie reagieren die Polizei und Unternehmen? Symposium des Instituts für Polizei- und Kriminalwissenschaften der FHöV NRW zum Thema „Cybercrime - Herausforderungen und Gegenstrategien für die öffentliche Verwaltung und Unternehmen“, 28.05.2019, Gelsenkirchen.	28.05.2019
Unternehmens-stammtisch	Dreißigacker, Arne; Skarczinski, Bennet von: Erste Ergebnisse der Unternehmensbefragung	28.06.2019
Vortrag	Skarczinski, Bennet von; Dreißigacker, Arne (2019): Unternehmen als Ziel von Cyberangriffen. Erste Ergebnisse einer Unternehmensbefragung. Vortrag auf der Tagung des Norddeutschen Kriminologischen Gesprächskreises (Nordkrim), Hannover	30.08.2019
Vortrag	Dreißigacker, Arne; Skarczinski, Bennet von; Wollinger, Gina Rosa (2019): Cyberangriffe gegen Unternehmen. Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland. Vortrag auf der 16. Wissenschaftlichen Tagung der Kriminologischen Gesellschaft (KrimG), Wien.	06.09.2019

Vortrag	Dreißigacker, Arne; Skarczinski, Bennet von (2019): Initiative IT-Sicherheit in der Wirtschaft - Projekt „Cyberangriffe gegen Unternehmen“. Vortrag auf der it-sa 2019, Nürnberg.	10.10.2019
Vortrag	Skarczinski, Bennet von; Dreißigacker, Arne (2019): Cyberangriffe gegen Unternehmen. Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland. Wirtschaftsschutztagung. Verfassungsschutz Niedersachsen. Hannover.	04.11.2019
Vortrag	Fahl, Sascha; Dreißigacker, Arne (2020): Cyberangriffe gegen Unternehmen: Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland. Vortrag auf dem IT-Security-Nachmittag der Hochschule Hannover.	13.01.2020
Vortrag	Dreißigacker, Arne (2020): Cybercrime - Ergebnisse aus der Forschung. Vortrag im Rahmen der Tagung Polizeiarbeit 3.0: Staatliche Sicherheitsorgane im digitalen Wandel. Essel.	02.03.2020
Vortrag	Dreißigacker, Arne (2020): Cyberangriffe gegen Unternehmen: Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland. Vortrag auf der Sitzung der Fokusgruppe Cybersicherheit von Hannover IT.	09.03.2020
Presseinterview	Reuning, Arndt (16.03.2020): Studie: Cyberangriffe auf deutsche Unternehmen – Interview Arne Dreißigacker, KFN. Deutschlandfunk (DLF): Forschung aktuell (16:48 Uhr). Abrufbar unter: https://srv.deutschlandradio.de/themes/dradio/script/aod/index.html?audioMode=2&audioID=4&audio=817010 (zuletzt geprüft am 02.04.2020).	10.03.2020
Presseinterview	Elisabeth Schmidt (17.03.2020): Studie zu Cybercrime. Viele Unternehmen sind nicht gut gerüstet. ZDFheute. Abrufbar unter: https://www.zdf.de/nachrichten/wirtschaft/cybercrime-unternehmen-schutzmassnahmen-100.html (zuletzt geprüft am 02.04.2020).	13.03.2020
Meldung auf KFN-Webseite	KFN (16.03.2020): Neuer Forschungsbericht veröffentlicht: Cyberangriffe gegen Unternehmen in Deutschland. Abrufbar unter: https://kfn.de/blog/2020/03/neuer-forschungsbericht-veroeffentlicht-cyberangriffe-gegen-unternehmen-in-deutschland/ (zuletzt geprüft am 02.04.2020).	16.03.2020
Meldung auf der Projekt-Webseite	Forschungsbericht veröffentlicht: Cyberangriffe gegen Unternehmen in Deutschland. Abrufbar unter: https://cybercrime-forschung.de/news/forschungsbericht/	16.03.2020
DPA-Meldung	DPA (16.03.2020): Umfrage: Gut 40 Prozent deutscher Unternehmen erleben Cyberangriffe. Laut dem Kriminologischen Forschungsinstitut Niedersachsen erstatten gerade kleinere Firmen wenige Anzeigen nach Angriffen. Abrufbar z.B. unter: https://www.heise.de/newsticker/meldung/Umfrage-Gut-40-Prozent-deutscher-Unternehmen-erleben-Cyberangriffe-4683167.html (zuletzt geprüft am 02.04.2020)	16.03.2020
Meldung Newsletter IHK-Hannover	Hillmer, Sabine (16.03.2020): Cyberangriffe: Deutschlandweite Befragung von 5000 Unternehmen erschienen. Abrufbar unter: https://www.hannover.ihk.de/ihk-themen/sicherheit/digitale-sicherheit/hinweise-tipps-leitfaeden/befragung-zu-cyberangriffen.html (zuletzt geprüft am 02.04.2020)	16.03.2020
Meldung auf PwC-Webseite	Mohs, Joachim (16.03.2020): Cyberangriffe gegen Unternehmen. Befragung des Kriminologischen Forschungsinstitut Niedersachsen (KFN) zum Thema Cyberangriffe. Abrufbar unter: https://www.pwc.de/de/im-fokus/cyber-security/cyberangriffe-gegen-unternehmen.html (zuletzt geprüft am 02.04.2020).	16.03.2020

E-Mail an Befragungsteilnehmer*innen	Dankes-E-Mail mit Forschungs- und Kurzbericht der Unternehmensbefragung an die 5.000 teilnehmenden Unternehmen in Deutschland	16.03.2020
Meldung auf ZDF-Webseite	Schmitd, Elisabeth (17.03.2020): Studie zu Cybercrime. Viele Unternehmen sind nicht gut gerüstet. Abrufbar unter: https://www.zdf.de/nachrichten/wirtschaft/cybercrime-unternehmen-schutzmassnahmen-100.html (zuletzt geprüft am 09.07.2021)	17.03.2020
Presseinterview	Michael B. Berger (23.03.2020): IT-Angriffe: Nur wenige werden angezeigt. Neue KFN-Studie zu Cyberattacken: Unsicherheit unter Unternehmen ist groß. Hannoversche Allgemeine Zeitung (HAZ). Abrufbar unter https://www.zdf.de/nachrichten/wirtschaft/cybercrime-unternehmen-schutzmassnahmen-100.html (zuletzt geprüft am 02.04.2020).	20.03.2020
Vortrag	Wollinger, Gina Rosa; Dreißigacker, Arne (2020): Cyberangriffe gegen Unternehmen: Erste Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland. Vortrag auf der secIT 2020, Hannover.	25.03.2020
Vortrag	Dreißigacker, Arne (2020): Cyberangriffe gegen Unternehmen: Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland. Vortrag auf der Tagung des Arbeitskreises "IT-Security" der Digitalagentur Niedersachsen. Hannover (online).	11.05.2020
Vortrag	Skarczinski, Bennet von (2020): Cyberangriffe gegen Unternehmen - aktuelle Studie des KFN. Vortrag auf der Tagung des Unternehmerverbände Niedersachsen e.V. (UVN) zum Thema: "AUF DEN PUNKT. Wirtschaft? Sicher! - analog und digital. Hannover (online).	08.06.2020
Vortrag	Skarczinski, Bennet von (2020): Cyberangriffe gegen Unternehmen - aktuelle Studie des KFN. Vortrag auf der 21. Sitzung des BSI Expertenkreises Cyber-Sicherheit im Rahmen der Allianz für Cyber-Sicherheit. Bonn (online)	17.06.2020
Vortrag	Dreißigacker, Arne; Skarczinski, Bennet von; Wollinger, Gina Rosa (2020): Cyberangriffe gegen Unternehmen. Vortrag auf dem 25. Deutschen Präventionstag, Kassel (online).	28.09.2020
Meldung	Hanser Verlag (Hrsg.) (2020): Unternehmen im Visier von Cyberangriffen. QZ - Qualität und Zuverlässigkeit: Die Zeitschrift für Qualitätsmanagement und Qualitätssicherung 65 (11/2020), S. 8.	02.11.2020
Meldung auf PwC-Webseite	Moore, Nial; Skarczinski, Bennet v. (2020): Cyberangriffe auf Medienhäuser: mangelndes Risikobewusstsein. Abrufbar unter: https://www.pwc.de/de/technologie-medien-und-telekommunikation/german-entertainment-and-media-outlook-2020-2024/cyberangriffe-auf-medienhaeuser-mangelndes-risikobewusstsein.html (zuletzt geprüft am 09.07.2021)	18.11.2020
Meldung in PwC-Broschüre	Moore, Nial; Skarczinski, Bennet v. (2020): Cyberangriffe auf Medienhäuser: mangelndes Risikobewusstsein. In: PwC (Hrsg.): German Entertainment and Media Outlook 2020-2024. Fakte, Prognosen und Trends für 13 Segmente der Entertainment- und Medienbranche in Deutschland. S. 23.	18.11.2020
Unternehmensstammtisch	Skarczinski, Bennet von; Dreißigacker, Arne; Fahl, Sascha (2021): Cyberangriffe gegen Unternehmen. (online).	19.02.2021
Vortrag	Dreißigacker, Arne; Wollinger, Gina Rosa (2021): Cybercrime – Ergebnisse aus der Forschung. DHPol, Münster (online).	11.03.2021

Unternehmens-stammtisch	Skarczinski, Bennet von; Dreißigacker, Arne; Huaman, Nicolas; Fahl, Sascha (2021): Cyberangriffe gegen Unternehmen. (online).	19.03.2021
Vortrag	Wollinger, Gina Rosa; Dreißigacker, Arne (2021): Cybercrime gegen Unternehmen. Befunde zum Ausmaß und Ableitungen für die Polizeiarbeit. Online-Tagung „Polizei-Informatik 2021“ (online).	20.04.2021
Vortrag	Dreißigacker, Arne; Wollinger, Gina Rosa; Skarczinski, Bennet von. (2021): Cybercrime gegen Unternehmen. Presentation on Demand auf dem 26. Deutschen Präventionstag (DPT), Köln (online).	10.05.2021
Vortrag	Wollinger, Gina Rosa; Dreißigacker, Arne (2021): Wie gut schützen sich Unternehmen vor Cybercrime und welche Ableitungen ergeben sich für die polizeiliche Prävention? Vortrag auf der Veranstaltung „Prävention von Cybercrime“, Polizei NRW (online).	27.05.2021
Vortrag	Dreißigacker, Arne; Wollinger, Gina Rosa (2021): Cyberangriffe gegen Unternehmen. Vortrag auf der Veranstaltung „Forum KI 2021“, Kriminalistisches Institut des Bundeskriminalamtes (online)	16.06.2021
Vortrag	Fahl, Sascha (2021): Buisnesstalk Cyberrisiken. Sparkasse Hannover (online)	16.06.2021
Vortrag	Dreißigacker, Arne (2021): Prävention und Reaktion bei Cyber-Spionage. Vortrag auf der Veranstaltung „Münchner Cyber Dialog“, Cyber Akademie (online).	17.06.2021
Vortrag	Huaman, Nicolas (2021): A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises, USENIX Security 2021 (online)	11.08.2021
Presseinterview	Kuhn, Johannes (05.07.2021): Hacker-Angriff über IT-Dienstleister trifft zahlreiche Unternehmen. Deutschlandfunk. Abrufbar unter https://ondemand-mp3.dradio.de/file/dradio/2021/07/05/hacker_angriff_ueber_it_dienstleister_trifft_zahlreiche_dlf_20210705_1310_8f56a992.mp3 (zuletzt geprüft am 07.07.2021).	05.07.2021
Interview	Jahn, Joachim (2021): Vom Enkeltrick zum Abrechnungsbetrug. Interview mit Tillmann Bartsch und Arne Dreißigacker. NJW-aktuell 37/2021, S. 12-13	20.08.2021
Meldung auf KFN-Webseite	KFN (13.09.2021): Neuer Forschungsbericht veröffentlicht: Cyberangriffe gegen Unternehmen in Deutschland. Abrufbar unter: https://kfn.de/blog/2021/09/neuer-forschungsbericht-veroeffentlicht-cyberangriffe-gegen-unternehmen-in-deutschland-2/ (zuletzt geprüft am 14.09.2021).	13.09.2021
DPA-Meldung	DPA (13.09.2021): Corona-Pandemie erhöht das Risiko von Cyberangriffen. Abrufbar z.B. unter https://www.faz.net/agenturmeldungen/dpa/corona-pandemie-erhoeht-das-risiko-von-cyberangriffen-17534320.html (zuletzt geprüft am 14.09.2021).	13.09.2021
Meldung Heise-online	Beer, Kristina (13.09.2021): Unternehmensbefragung: Corona trägt zum Risiko von Cyberangriffen bei. Abrufbar unter https://www.heise.de/news/Unternehmensbefragung-Corona-traegt-zum-Risiko-von-Cyberangriffen-bei-6190084.html (zuletzt geprüft am 14.09.2021).	13.09.2021
Meldung Deutschlandfunk	Stratenschulte, Julian (13.09.2021): Corona-Pandemie. Cyberangriffe durch Arbeit im Homeoffice. Abrufbar unter https://www.deutschlandfunk.de/corona-pandemie-cyberangriffe-durch-arbeit-im-home-office.2850.de.html	13.09.2021

Presseinterview	Sarnow, Simone (13.09.2021): Homeoffice erhöht Risiko von Cyberangriffen auf Unternehmen. SWR3 Radio	13.09.2021
Meldung Newsletter IHK Hannover	Hillmer, Sabine (14.09.2021): Unternehmensbefragung: Risiko von Cyberangriffen steigt. Abrufbar unter: https://www.hannover.ihk.de/ihk-themen/sicherheit/digitale-sicherheit/hinweise-tipps-leitfaeden/risikocyberangriffesteigt.html (zuletzt geprüft am 14.09.2021).	14.09.2021

Die Ergebnisse des Projektes, die bei den Vortragstätigkeiten und der Öffentlichkeitsarbeit vorgestellt und genutzt wurden, sind in Tabelle 2 aufgeführt. Dazu zählt insbesondere auch die über Projektwebseite zur Verfügung gestellte Vorhersageplattform CARE (Cyber Attack Risk Estimation). Diese bietet insbesondere kleinen und mittleren Unternehmen neben einer individuellen Risikoeinschätzung in Bezug auf die Gefährdung durch unterschiedliche Cyberangriffe auch entsprechende Handlungsempfehlungen zur Reduzierung der größten Risiken. Die Plattform wurde zudem in den Sec-O-Mat der Transferstelle IT-Sicherheit im Mittelstand (TISiM) eingebunden und damit deren Bekanntheit erhöht.

Tabelle 2: Projektbezogene Ergebnisse

Art	Autoren/ Beteiligte	Bezeichnung/Titel	Einreichung/ Durchführung
Forschungsstand (AP 1)	KFN	Überblick/Klassifikation verfügbarer Studien zum Thema Cyberangriffe gegen Unternehmen	15.03.2018 (intern)
Workshop (AP 1 u. 3)	KFN/L3S	Ableitungen aus dem Forschungsstand für die Unternehmensbefragung	15.03.2018 (intern)
Factsheet (AP 2)	KFN	Cyberangriffe gegen Unternehmen. Anzeigen.	02.07.2019
Factsheet (AP 3)	KFN	Cyberangriffe gegen Unternehmen. Befragung.	20.08.2019
Factsheet (AP 4)	L3S	Cyberangriffe gegen Unternehmen. Messaging-Apps.	01.10.2019
Workshop (AP 3 u. 10)	KFN/L3S	Tiefergehende Auswertung der Befragungsdaten für das Prognosemodell	14.06.2019 (intern)
Forschungsbericht (AP 3)	Dreißigacker et al.	Cyberangriffe gegen Unternehmen. Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019.	08.11.2019
Forschungsbericht (AP 2)	Stiller et al.	Cyberangriffe gegen Unternehmen. Ergebnisse einer qualitativen Interviewstudie mit Experten.	02.12.2019
Workshop (AP 9)	KFN/L3S	Überarbeitung des Fragebogens zur zweiten Unternehmensbefragung	07.02.2020 (intern)
Kurzbericht (AP 3)	KFN	Cyberangriffe gegen Unternehmen. Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland 2018/19. Kurzbericht.	14.02.2020
Forschungsbericht (AP 3)	Dreißigacker et al.	Cyber-attacks against companies in Germany. Results of a representative company survey 2018/2019.	25.08.2020

Prognoseplattform CARE (AP 10)	L3S	CARE (Cyber Attack Risk Estimation) für KMU. https://www.cybercrime-forschung.de/care	15.12.2020
Forschungsbericht (AP 9)	Dreißigacker et al.	Cyberangriffe gegen Unternehmen. Ergebnisse einer Folgebefragung 2020.	01.07.2021
Poster	Dreißigacker	Cyberangriffe gegen Unternehmen. Poster für das Symposium des LKA-Niedersachsen zum Thema „Zwei Welten? Wissenschaftliche Erkenntnisse in polizeilicher Strategie und Praxis“	06/2018
Fachbeitrag	Dreißigacker/ Wollinger	Verbreitung von Cyberkriminalität gegen Unternehmen in Deutschland. In: Wollinger/Schulze (Hg.): Handbuch Cybersecurity für die öffentliche Verwaltung. Wiesbaden: Kommunal- und Schul-Verlag, S. 89–109.	02/2020
Fachbeitrag	Dreißigacker et al.	Im Visier: Repräsentative Studie zur Cyberkriminalität in deutschen Unternehmen. iX – Magazin für professionelle Informationstechnik (6/2020), S. 78-81.	03/2020
Fachbeitrag	Huaman et al.	A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises. In: Proceedings of the 30th USENIX Security Symposium, USENIX Security ’21.	02/2021
Fachbeitrag	Skarczinski et al.	Understanding the adoption of cyber insurance for residual risks – An empirical large-scale survey on organizational factors of the demand side. In: European Conference on Information Systems (ECIS 2021), Research Papers, 72.	03/2021
Fachbeitrag	Skarczinski et al.	Towards enhancing the information base on direct costs of cyber-attacks on organizations: Implications from literature and a large-scale survey. Journal of Cybersecurity	03/2021
Poster	Huaman et al.	Cybercrime in Small and Medium-sized Enterprises. SOUPS 2021 Posters.	05/2021
Fachbeitrag	Dreißigacker et al.	Cyberangriffe gegen Unternehmen: Erste Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland. DOI: 10.25365/phaidra.175.	01/2020

2.1.7 Feldstudie: Strategien zur Bekämpfung von Cybercrime (AP 7: L3S)

In diesem Arbeitspaket wurden qualitative Feldstudien mit ausgewählten Unternehmen, die an der Datenerhebung im Rahmen des Projekts teilnehmen. Im Rahmen der Feldstudie stand die Frage im Mittelpunkt, mit welchen Strategien im Hinblick auf Sicherheitsanalysen und IT-Forensik das IT-Personal arbeitet, um Cyberangriffe aufzuspüren und welche Gegenmaßnahmen ergriffen werden. Dazu wurden Cyberangriffe auf IT-Systeme simuliert und entsprechende IT-forensische Spuren auf diesen Systemen hinterlassen. Hierzu gehören unter anderem ein Datenbankangriff (SQL-Injection), ein DDoS Angriff auf die Infrastruktur und ein Defacing auf der Website des Servers. Teilnehmer*innen untersuchen diese Maschine mithilfe einer Beschreibung der vorgefallenen Angriffe. Genutzt wird dieselbe Virtualisierungsinfrastruktur wie

bei AP 4. Die Strategie des Teilnehmers zum Umgang mit Cyberangriffen wurde festgehalten und für die Auswahl der Quellen der Vorhersageplattform genutzt. Zur Durchführungen der Studien waren Veranstaltungen vor Ort geplant. Da sich die Rekrutierung auch hier als sehr schwierig erwies und aufgrund der Corona-Situation zusätzlich beeinträchtigt wurde, wurde hier schließlich nach Rücksprache mit dem DLR vollständig auf eine Online-Studie mittels der Virtualisierungsplattform umgestellt. Aufgrund der COVID-19 Pandemie in 2020 wurde die Feldstudie online mittels des in AP4 vorgestellten Tools durchgeführt. Darüber hatten die Teilnehmer*innen Zugriff auf einen virtuellen Server eines fiktiven Unternehmens. Über Spuren in Logs und im Filesystem konnte auf einen "Internal Attacker" geschlossen werden, also auf eine/n Mitarbeiter*in, der bzw. die das im Studienszenario vorgestellte Unternehmen vor kurzem verlassen hat und nun seine Zugriffsrechte missbraucht, um dem Unternehmen zu schaden.

Die Studiendurchführungen wurden aufgezeichnet und dann transkribiert, anonymisiert und durch zwei Forschende nach dem "open coding" Ansatz qualitativ auf Ansätze zum Umgang mit den eingebauten Angriffen gecodet. Hier eine Zusammenfassung unserer Ergebnisse:

- **Sozialer oder Kommunikativer Ansatz:** Alle Teilnehmer*innen meldeten die Kommunikation oder soziale Komponente als wichtige Grundlage zum Lösen des Angriffs, auch bevor klarer wurde, dass es sich hierbei um einen unternehmensinternen Angreifer handelt. Alle Teilnehmer*innen haben im Laufe der Studie Teile dieser Informationen erfragt, die von den Interviewer*innen/ Betreuer*innen bereitgestellt wurden. Dazu gehörten Fragen zum generellen Zustand des Netzwerkes, dem vermuteten Angriffszeitpunkt, sowie den Mitarbeiter*innen zum Zeitpunkt des Angriffs. Weitergehend haben einige Teilnehmer*innen nach der Auswertung des Authentifizierungsprotokolls eine Rücksprache mit den auf den betroffenen Servern im vermuteten Zeitraum des Angriffs angemeldeten Mitarbeiter*innen gehalten. Weiterhin gaben Teilnehmende an, eine Absprache mit dem Datenschutzbeauftragten, externen Dienstleistern und Firmenleitung zum weiteren Vorgehen durchzuführen.
- **Zentrale Authentifizierung:** Ein in unserem fiktiven Unternehmen und teilweise in den teilnehmenden Unternehmen selbst fehlender aber dennoch oft vorgeschlagener Ansatz ist die zentrale Authentifizierung z.B. über Active Directory, LDAP oder Shibboleth. Damit können alle Nutzer*innen und Zugänge über ein zentrales System verwaltet werden. Dies würde speziell in unserem Szenario ermöglichen, sowohl die Zugänge der internen Angreifer*innen zum Zeitpunkt des Austritts aus dem Unternehmen zu sperren, als auch Daten darüber zentral zu sammeln, welche/r Nutzer*innen wann und wo auf Unternehmensressourcen zugegriffen hat. Dies würde die Analyse und Nachverfolgung von Angriffen allgemein erleichtern.
- **Dokumentation & Bezeugung:** Die Teilnehmenden gaben weiterhin an, in Fällen solcher Cyberangriffe auf jeden Fall jeden Schritt auf dem System zu dokumentieren und idealerweise eine zweite Person zur Bezeugung der Situation hinzuzuziehen. Dies soll auch später im Falle einer Anzeige des Angriffs und zur Erfüllung der Meldepflicht zur rechtlichen Absicherung genutzt werden.

Abgesehen von der zentralen Authentifizierung, die fast als eine Sicherheitsmaßnahme gesehen werden kann, war zusammenfassend vor allem die Vorbereitung auf eine Rücksprache durch öffentliche Stellen sowie die gesehene Notwendigkeit, nach einem Sicherheitsvorfall so schnell

wie möglich eine rechtlich haltbare Beweissammlung durchzuführen, erkennbar. Um das Sicherheitsproblem selbst zu beheben wurde häufig das Neuaufsetzen des Systems oder die Einbindung von zentraler Authentifizierung zur Absicherung gegen den in unserem Szenario vorgestellten internen Angriff vorgeschlagen.

Dies lässt darauf schließen, dass es wichtig ist, öffentliche Stellen mit Beratungsfunktion für genau diese Punkte zu stärken und deren Bekanntheit für Unternehmen zu erhöhen. Unsere Vorhersageplattform (AP10) priorisiert dahingehend z.B. die Ratgeber des BSI.

2.1.8 Feldstudie: Benutzbarkeit SIEMs (AP 8: L3S)

In diesem Arbeitspaket sollten Laborstudien mit ausgewählten Unternehmen, die an der Datenerhebung im Rahmen des Projekts teilnehmen, im L3S-Labor durchgeführt werden. Im Rahmen der Laborstudie sollte die Benutzbarkeit der zwei bekanntesten Cloud-basierten SIEM Lösungen im Hinblick auf die Identifikation von Cybercrime-Angriffen untersucht werden. Dazu wurden Szenarien vorbereiten, in denen Studienteilnehmer*innen mit Hilfe der Cloud-basierten SIEM Lösungen simulierte, aber realitätsgetreue Cyberangriffe identifizieren sollten. Auf der Basis der Resultate sollten Benutzbarkeitsschwierigkeiten aktueller Systeme identifiziert und Verbesserungsvorschläge für zukünftige Cloud-basierte SIEM abgeleitet werden.

Für die Feldstudie wurden SIEMs ausgewählt, die sowohl OpenSource als auch in der eigenen Infrastruktur betreibbar sind. Bei diesen handelt es sich um Wazuh und ELK Stack SIEM. Ursprünglich sah der Studienplan hierfür Apache Metron an Stelle von ELK Stack vor. Das Produkt wurde allerdings seitens Apache eingestellt und musste daher ersetzt werden.

Gemäß Studienplan wählten die Teilnehmer*innen jeweils eines der SIEMs aus und sollten anschließend die Logs eines Servers mit mehreren Sicherheitsvorfällen in dem SIEM analysieren. Um die Benutzbarkeit der SIEMs zu untersuchen, wurden die Teilnehmer*innen gebeten, am Ende eine Umfrage zu beantworten. Hierbei wurde der NPM (Netpromoter) Score erfasst. Zudem wurden die Korrektheit bzw. der Effekt der den Teilnehmer*innen gegebenen Ratschläge in Bezug auf die IT-Sicherheit ausgewertet.

Die Durchführung der Studien war ursprünglich ebenfalls vor Ort geplant und wurde aus den gleichen Gründen wie bei AP 7 und nach Rücksprache mit dem DLR vollständig online durchgeführt.

Die Online Studie präsentierte hierbei die SIEMs WAZUH und ELK Stack SIEM. Beide waren mit Logs eines simulierten SSH Brute Force Angriffes gefüllt und die Teilnehmenden sollten die Interfaces gegeneinander abwägen, Einschätzungen zu der Sicherheitslücke und zu ergreifenden Maßnahmen abgeben sowie Details bezüglich ihrer eigenen Erfahrungen mit SIEMs teilen. Die Ergebnisse wurden wieder qualitativ mittels open coding der Antworten mit zwei Forschenden ausgewertet. Die Ergebnisse fassen wir im Folgenden kurz zusammen:

- **Wichtige Funktionen eines SIEM:** Die meisten Teilnehmer*innen gaben an, dass die Security Events Funktion von WAZUH, also das regelmäßige loggen auffälliger Ereignisse im Netzwerk und auf den überwachten Systemen die wichtigste Funktion sein. Diese ist sicherheitstechnisch tatsächlich sinnvoll, um die Vorbereitung von Angriffen auf die Firma zu bemerken und rechtzeitig agieren zu können, jedoch gaben die verbleibenden Teilnehmer an, Funktionen wie PCI DSS und die Übersicht über Vulnerabilities

zu bevorzugen, um Compliance mit Vorgaben wie dem BSI Grundschutz und die Sicherheit der Systeme überwachen zu können.
Die Teilnehmer*innen, die ELK Stack nutzten, haben hingegen sehr unterschiedliche Funktionen als wichtigste genannt. Die "Detections" Oberfläche hat sich als wichtigste Quelle herauskristallisiert, gefolgt von der generellen "Overview" oder "Cases" Oberfläche. Der Rest teilte sich auf die "Hosts", "Network" und "Timelines" Tabs auf.

- **Umgang mit Sicherheitsvorfällen:** Im Falle unseres Szenarios handelte es sich um einen SSH Brute Force Angriff. Für dieses Szenario haben sich die Teilnehmer*innen in WAZUH und ELK Stack SIEM vor allem angriffsspezifische Informationen und Unterstützung gewünscht, z.B., dass Angriffe vom selben Täter*in, d.h. derselben Source IP, zur leichteren Analyse in einem gewissen Zeitraum zu einem Angriff zusammengefasst werden. Mithilfe der von WAZUH und ELK Stack SIEM bereitgestellten Informationen würden die meisten Teilnehmer*innen die IP-range des Täters blocken und Security Hardening am Ziel vornehmen. Nur wenige haben angegeben, zu versuchen, nach dieser IP-Adresse zu fanden und in einem Fall wurde sogar eine Rücksprache mit der Marketing- oder Geschäftsabteilung vorgeschlagen, um abzuklären ob diese IP Range für Kund*innen wichtig ist und überhaupt geblockt werden kann. Es lässt sich erkennen, dass in unserem Szenario das SIEM weniger für Nachweise und Nachverfolgbarkeit von Cybercrime genutzt wird und mehr zur Verbesserung und Kontrolle der unternehmensinternen IT-Sicherheit.
- **Populäre SIEM:** In unserem Sampleset waren die populärsten SIEM tatsächlich IBM QRadar als proprietäre Lösung von IBM und das ELK Stack SIEM als Open Source SIEM. Daneben traten Wazuh, Splunk und Arcsight in unserem Datensatz als bekannte und genutzte SIEM auf. Die meisten Teilnehmer*innen in unserer Studie, die SIEMs in Unternehmen genutzt haben, gaben an, diese intern genutzt und überwacht zu haben. Nur wenige wussten von externen Dienstleister*innen, die SIEMs als Teil der Dienstleistung für das Unternehmen einsetzten. Dabei könnte es sich allerdings um ein Wahrnehmungsproblem handeln, da Mitarbeiter*innen eines Unternehmens nicht unbedingt das gesamte Angebot eines externen Dienstleisters kennen dürften und speziell SIEMs hier vermutlich auch nicht primär beworben werden.
- **Wahrnehmung von SIEMs:** Bei der Frage nach generellen Problemen und Eindrücken zu SIEMs wurde vor allem die niedrige Genauigkeit der SIEMs angeführt, verbunden mit einer hohen False Positive Rate und Anzeigeproblemen wie die in unserem Szenario genannte Menge an Einträgen für "einen" Brute-force Angriff. Diese erschweren das reagieren auf einen "echten" Angriff, da dieser erst aus den falschen Angriffen aussortiert und teilweise aus mehreren unterschiedlichen Alarmen zusammengesetzt werden muss. Positiv fanden die Teilnehmer*innen hingegen die Nachverfolgbarkeit und die einfache Verarbeitung im Vergleich zum manuellen Sammeln und Lesen von Serverlogs. Auch die hohe Anpassbarkeit an unternehmensspezifische Infrastruktur wurde bei einigen SIEMs wie dem ELK Stack positiv hervorgehoben.
- **Angriffsarten:** Die Teilnehmer*innen meldeten vor allem verschiedene Arten von BruteForce und DDoS Angriffen als häufige Angriffsarten, die von SIEMs deployed werde. Vereinzelt wurden auch Lücken in Webanwendungen gefunden sowie APT und Ransomware-Angriffe durch ein SIEM festgestellt und aufgehalten oder nachverfolgt.

2.1.9 Unternehmensbefragung II (AP 9: KFN)

Über die zweite Unternehmensbefragung sollte einerseits abgebildet werden, wie sich das Phänomen Cyberangriffe gegen Unternehmen innerhalb eines Jahres entwickelt hat. Dabei ist von Interesse, welche Unternehmen wiederholt viktimisiert wurden und durch welche Angriffsarten. Des Weiteren sollte in diesem Arbeitspaket gesondert geprüft werden, welche Unternehmen in IT-Sicherheit investiert haben, was sie dabei genau getan haben und was die ausschlaggebenden Gründe dafür waren. Ferner sollte erfragt werden, welche Probleme dabei auftraten und welcher weitere Unterstützungsbedarf existiert.

Die zweite Unternehmensbefragung richtete sich an alle Teilnehmer der CATI-Befragung, die ihr Einverständnis zur erneuten Teilnahme gegeben haben, und wurde mittels eines Online-Fragebogens durchgeführt. Für die Kontaktaufnahme hatten von 5.000 Unternehmen 3.429 (68,6 %) eine E-Mail-Adresse hinterlegten, die von Kantar Emnid gesammelt übergeben wurde.

Für die Online-Befragung wurde der Fragebogen der CATI-Befragung in Zusammenarbeit mit L3S überarbeitet und mit der Umfragesoftware Qualtrics programmiert. Die Veränderungen wurden auf der Projektbeiratssitzung am 28.02.2020 vorgestellt und diskutiert. Eine Diskussion im Rahmen des Regionalen Unternehmensstammtisches bei PwC in Hannover musst im Zusammenhang mit der Covid-19-Krise abgesagt werden. Aufgrund der Corona-Krise und der damit verbunden beeinträchtigten Erreichbarkeit und Teilnahmebereitschaft der Unternehmen wurde die Online-Befragung zeitlich weiter verschoben und zwischen Juli und September mit vier Erinnerungsschreiben per E-Mail durchgeführt. Der Fragebogen wurde auf die besondere Situation hin angepasst, insofern Fragen zur IT-Sicherheit in der Corona-Krise ergänzt wurden. Die Angaben von immerhin 687 Unternehmen konnten in die Auswertung einbezogen werden. Dies entspricht einer Teilnahmequote von 14,7 % auf Basis der bereinigten Bruttostichprobe.

Die Ergebnisse dieser Folgebefragung wurden ebenfalls in einem weiteren Forschungsbericht festgehalten.[10] Zu den zentralen Ergebnissen zählen folgende Punkte:

- **IT-Sicherheitsmaßnahmen:** Gemäß der Ergebnisse von Befragung I (2018/19) sind basale technische Maßnahmen wie der Schutz der IT-Systeme durch eine Firewall, regelmäßige Backups, aktuelle Antivirensoftware und regelmäßige Sicherheitsupdates und Patches in fast allen Unternehmen ab zehn Beschäftigten im Einsatz, wohingegen organisatorische Maßnahmen wie Richtlinien zur IT- und Informationssicherheit oder zum Notfallmanagement, IT-Sicherheitsschulungen, Zertifizierung der IT-Sicherheit, regelmäßige Risiko- und Schwachstellenanalysen sowie Übungen/ Simulationen zum Ausfall wichtiger IT-Systeme weniger weit verbreitet sind. Dieser Befund lässt sich mit den Ergebnissen von Befragung II (2020) bestätigen und weiter schärfen, insofern zusätzliche IT-Sicherheitsmaßnahmen und Einschätzungen zum Reifegrad und der Verbreitung innerhalb der Unternehmen erhoben wurden. Dabei zeigt sich einerseits eine weite Verbreitung dieser Basismaßnahmen, andererseits weist der Reifegrad der eingesetzten Maßnahmen eine große Varianz auf. Die Anteile der Unternehmen, die bereits die folgenden in Befragung II zusätzlich erhobene IT-Sicherheitsmaßnahmen einsetzen,

[10] Dreißigacker et al. (2021).

sind vergleichsweise klein: Zwei-Faktor-Authentifizierung (32,0 %), Security Information and Event Management (21,6 %), Security Operation Center (11,6 %), der Austausch von Bedrohungsdaten (21,2 %), Informationssicherheitsmanagementsysteme (15,2 %) und auf künstlicher Intelligenz basierte Maßnahmen (14,6 %). Dies dürfte darauf zurückzuführen sein, dass diese z.T. erst ab einer gewissen Unternehmensgröße sinnvoll sind und mehr personelle wie finanzielle Ressourcen voraussetzen. Immerhin etwa zwei Drittel der Unternehmen setzen Verschlüsselung von sensiblen Daten (65,2 %), Verschlüsselung von Kommunikation (60,4 %) und Netzwerksegmentierung (62,6 %) ein, wobei es insbesondere beim Thema Verschlüsselung ebenfalls große Varianz bezüglich des Reifegrades und der Verbreitung innerhalb der Unternehmen gibt. Während fast alle Unternehmen angeben, regelmäßige Backups durchzuführen (99,6 %) und den Reifegrad bzw. die Verbreitung im Unternehmen dabei meist eher hoch einschätzen, testen lediglich drei Viertel (77,4 %) die Datenwiederherstellung (Restoring). Hinzu kommt, dass diese Tests mit meist relativ geringem Reifegrad häufig nur einen Teil der Unternehmens-IT einbeziehen.

- **Corona-Situation:** Mit Beginn der Corona-Krise im ersten Quartal 2020 veränderte sich die Situation für die IT-Sicherheit in den Unternehmen schlagartig. Es wurden ad hoc Möglichkeiten für Homeoffice geschaffen, über zwei Drittel der Unternehmen (68,0 %) boten dies zum Zeitpunkt der Befragung ihren Beschäftigten an. Damit verbunden stieg auch der Anteil der Unternehmen, bei denen die Nutzung privater Soft-/ Hardware für dienstliche Zwecke möglich ist, auf knapp ein Drittel (30,8 %). In etwa jedem achten Unternehmen (12,7 %) hat sich nach Einschätzung der Unternehmensvertreter*innen die Corona-Krise insgesamt negativ auf die IT-Sicherheit ausgewirkt. Etwa ein Fünftel (20,1 %) traf zusätzliche IT-Sicherheitsmaßnahmen aufgrund der veränderten Situation. Dazu zählen insbesondere die Einrichtung und Absicherung weiterer VPN-Zugangsmöglichkeiten und die Anschaffung und Absicherung zusätzlicher Soft- und Hardware für die Arbeit im Homeoffice. Über die Hälfte der Unternehmen schätzte das Risiko eines schädigenden ungezielten Cyberangriffs in den nächsten zwölf Monaten als sehr/ eher hoch ein. Da das Treffen zusätzlicher IT-Sicherheitsmaßnahmen in einem statistisch signifikanten Zusammenhang mit der wirtschaftlichen Situation der Unternehmen steht, dürfte sich dieses Risiko insbesondere für krisenbedingt geschwächte Unternehmen auch objektiv erhöht haben.
- **Cyberangriffe:** Insgesamt gaben 59,6 % der Unternehmen an, dass sie in den zwölf Monaten vor der Befragung II (2020) auf mindestens einen (versuchten) Cyberangriff der erfragten Angriffsarten reagieren mussten. Im Vergleich mit den Ergebnissen der ersten Befragung ist dies ein deutlicher Anstieg, denn bezogen auf die zwölf Monate vor Befragung I (2018/19) waren nur 41,1 % aller befragten Unternehmen betroffen bzw. 50,2 % der Unternehmen, die dann auch an der zweiten Befragung teilgenommen haben. Dieser Anstieg der Gesamtprävalenzrate ist zumindest tendenziell in allen Beschäftigtengrößenklassen erkennbar. Ein Branchenvergleich war aufgrund der geringen Fallzahl nur sehr eingeschränkt möglich, weist aber darauf hin, dass die Entwicklung nicht in allen Branchen gleichermaßen stattgefunden zu haben scheint. Differenziert nach Angriffsarten ließ sich zeigen, dass insbesondere die signifikante Zunahme der Prävalenzraten von Phishing und von sonstiger Schadsoftware hinter dem Anstieg der

Gesamtprävalenzrate steht. Während auf diese Angriffsarten in allen Beschäftigtengrößenklassen häufiger reagiert werden musste, veränderten sich die Prävalenzraten anderer Angriffsarten kaum oder lediglich in einzelnen Beschäftigtengrößenklassen. So ist z.B. für größere Unternehmen ab 250 Beschäftigten erkennbar, dass die Belastung durch CEO-Fraud in der letzten Zeit zumindest tendenziell zugenommen hat, während sie in den übrigen Unternehmen stagnierte.

- **Schwerwiegendster Cyberangriff:** In Hinblick auf die Frage, wie die schwerwiegendsten Cyberangriffe entdeckt wurden, zeigte sich, dass die Mehrzahl der berichteten Angriffe (88,7 %) durch Beschäftigte in den Unternehmen entdeckt wurden, meist im Rahmen von regulären Sicherheitsmaßnahmen oder Kontrollen (64,7 %). Ein Anteil von 15,5 % gab hingegen an, dass der berichtete Angriff erst durch den Eintritt negativer Auswirkungen erkannt wurde und bei weiteren 11,5 % spielte der Zufall eine entscheidende Rolle. Dies verweist auf Schwierigkeiten bzw. Verbesserungspotentiale bei der rechtzeitigen Erkennung von Cyberangriffen im Rahmen von geregelten Abläufen. Gefragt nach technischen Maßnahmen, die in erster Linie an der Entdeckung beteiligt waren, gaben zwei Fünftel an, auf den Angriff durch die eingesetzte Antivirensoftware (40,0 %) aufmerksam geworden zu sein, weitere 17,5 % erkannten den Angriff mit Hilfe einer Firewall. Bei immerhin knapp ein Drittel (31,2 %) war keine technische Maßnahme beteiligt. Erneut zeigte sich, dass die Spannbreite der Kosten, die durch die berichteten schwerwiegendsten Cyberangriffe der vergangenen zwölf Monate verursacht wurden, sehr groß ist (20 EUR bis 3,8 Mio. EUR), die Kosten mehrheitlich aber relativ gering ausfielen (Durchschnitt: 7.890 EUR, Median: 500 EUR). Dies wird auch durch die von den Unternehmensvertreter*innen vorgenommene Einschätzung der entstandenen materiellen und nicht-materiellen Schäden gestützt. Insgesamt betrachtet war der Schaden lediglich bei 1,6 % mittelfristig/ deutlich spürbar. Lediglich ein Unternehmen berichtete von einem langfristigen/ hohen nicht-materiellen Schaden. Die Antwortoption „Bestandsgefährdend“ wurde von keinem der teilnehmenden Unternehmen gewählt. Auch wenn die meisten Unternehmen auf Cyberangriffe reagieren müssen, scheinen Vorfälle mit sehr schwerwiegenden kostenintensiven Folgen demnach seltene Ausnahmen zu bleiben.
- **Anzeigeverhalten:** Das Anzeigeverhalten ist weiterhin als gering zu beschreiben. Lediglich 8,5 % der Unternehmen, die Angaben zum schwerwiegendsten Cyberangriff der letzten zwölf Monate machten, zeigten diesen auch an. Diese Quote liegt tendenziell sogar unter der aus Befragung I (11,9 %). Erneut ist zu erkennen, dass große Unternehmen (ab 500 Besch.) häufiger anzeigen als kleinere sowie dass es Unterschiede zwischen den Angriffsarten gibt, wobei Phishing selten und CEO-Fraud oder Spyware-Angriffe vergleichsweise häufig angezeigt werden. Dabei spielt allerdings auch das Tatstadium eine Rolle. Cyberangriffe, die aus Sicht der Unternehmen zumindest teilweise erfolgreich waren, wurden häufiger angezeigt (25,6 %) als Angriffe, die als „nicht erfolgreich“ eingestuft wurden (5,7 %). Zu dem mit 82,1 % am häufigsten angegebenen Nichtanzeigegrund zählt dementsprechend die Antwortkategorie „Weil kein oder nur geringer Schaden entstanden ist“. Ein weiterhin sehr häufiger Grund dafür ist die fehlende Aussicht auf einen Ermittlungserfolg (52,8 %) und die Unsicherheit, an wen man sich für eine Anzeige genau wenden muss (17,1 %). Letzteres wurde insbesondere von

kleinen Unternehmen (10-49 Besch.) angegeben, bei denen weiterhin ein Informationsdefizit zu bestehen scheint.

- **Schutzmaßnahmen:** Etliche der erfragten IT-Sicherheitsmaßnahmen stehen (ohne Kontrolle der Beschäftigtengrößenklasse) positiv im Zusammenhang mit der Betroffenheit von Cyberangriffen, d.h. mit dem Erleben mindestens eines Cyberangriffs in den letzten zwölf Monaten, auf den reagiert werden musste. Dazu zählen insbesondere schriftliche Richtlinien zur Informations- bzw. IT-Sicherheit, Risiko- und Schwachstellenanalysen (auch Pentest), Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme, aktive Überwachung der Verfügbarkeit und zeitnahe Installation von Sicherheitsupdates, Netzwerksegmentierung, Austausch von Bedrohungsdaten (z.B. Threat Intelligence Dienste) sowie die Auslagerung der IT-Security an externe Dienstleister. Dies wurde nach weiteren Gruppenvergleichen so interpretiert, dass mit diesen Maßnahmen die Aufmerksamkeit bzw. die Fähigkeiten zur Detektion von Cyberangriffen steigen. Denn wenn diese Maßnahmen in Zusammenhang mit dem Erleben eines als (teilweise) erfolgreich bewerteten Cyberangriffs gesetzt werden, ändern sich fast durchgehend die Vorzeichen. Insbesondere schriftliche Richtlinien zur Informations- bzw. IT-Sicherheit, Risiko- und Schwachstellenanalysen (auch Penetrationtesting), Verschlüsselung von sensiblen Daten und die Auslagerung der IT-Security an externe Dienstleister stehen mit einer geringeren Wahrscheinlichkeit in Zusammenhang, einen Cyberangriff zu erleben, der das Versuchsstadium überschreitet. Demgemäß zeigte sich, dass Unternehmen mit besonderen Produkten, Herstellungsverfahren oder Dienstleistungen bzw. mit besonderer Reputation oder Kundenkreis, die im Gegensatz zu anderen Unternehmen häufiger auf diese IT-Sicherheitsmaßnahmen setzen, auch häufiger (versuchte) Angriffe detektierten aber deutlich seltener einen (teilweise) erfolgreichen Cyberangriff erlebten. Dass der Mensch eine zentrale Rolle innerhalb der IT-Sicherheit der Unternehmen spielt, wird an drei Punkten besonders deutlich: Erstens handelt es sich beim Großteil der berichteten Cyberangriffe um Phishing-Angriffe, die auf eine Täuschung von IT-Anwender*innen z.B. zur Erlangung sensibler Informationen abzielen. Auf der anderen Seite wird, zweitens, die Mehrzahl der Angriffe von den Beschäftigten der Unternehmen entdeckt und das häufig auch ohne Beteiligung technischer Maßnahmen. Und drittens können viele technische und organisatorische IT-Sicherheitsmaßnahmen erst eine Wirkung entfalten, wenn diese (richtig) „genutzt“ werden: Insbesondere Richtlinien zur IT-Sicherheit müssen innerhalb der Unternehmen gelebt werden, mit Übungen und Simulationen lassen sich die Aufmerksamkeit und Reaktionsfähigkeit von Beschäftigten gegenüber Cyberangriffen steigern und sinnvolle technische Maßnahmen wie Verschlüsselungen müssen – ihre gute Nutzbarkeit vorausgesetzt – angewendet werden. Die Verschlüsselung von Kommunikation ist im Übrigen die einzige der erhobenen Maßnahmen, die sowohl negativ mit dem Erleben mindestens eines (versuchten) Angriffs als auch mit dem Erleben eines (teilweise) erfolgreichen Angriffs in Zusammenhang steht. Dies spricht mit aller Vorsicht dafür, dass eine derartige Verschlüsselung bereits Angriffsversuche unterbinden bzw. die Erfolgsaussichten für die Täter*innen verringern kann.

2.1.10 Vorhersage-Plattform (AP 10: L3S)

Im Rahmen des Projekts wurde eine große Anzahl von Unternehmen im Hinblick auf IT-Sicherheitsrelevante Aspekte, die einen Einfluss auf die Anfälligkeit für Cybercrime haben, untersucht. Um die resultierenden Ergebnisse für die Zielgruppe kleiner und mittlerer Unternehmen zur Verfügung zu stellen, wurde in diesem Arbeitspaket die Vorhersage-Plattform CARE (Cyber Attack Risk Estimation) entwickelt. Dazu wurden die Daten der Unternehmensbefragungen (AP 3, AP 9) für Regressionsanalysen durch das L3S verwendet. Diese webbasierte Plattform ist online für ein breites Publikum unter https://www.cybercrime-forschung.de/care verfügbar und erlaubt nach der Angabe einiger weniger Parameter eine Risikoeinschätzung für verschiedene Cyberangriffsarten. Zusätzlich präsentiert die Plattform mögliche Vorschläge zur Risikoverringerung.

Die Plattform wurde 2019 einmal als Papier-Prototyp im Rahme eines Projektbeiratstreffens besprochen. Hierbei wurde besonders Wert daraufgelegt, dass der Fragebogen nicht zu lang, d.h. wesentlich kürzer als der Fragebogen des ~20-minütigen Telefoninterviews, ausfällt und sich auf Fragen beschränkt, die ein Mitarbeiter des Unternehmens durch simple Nachfrage im Unternehmen ohne längere Bearbeitungszeit beantworten kann. Fragen wie das exakte Budget der IT-Sicherheit im Unternehmen und technische Details bei der Umsetzung von Sicherheitsmaßnahmen wurden also außen vorgelassen oder stark vereinfacht. In Form eines “vertikalen Prototypen”, d.h. mit grundlegender Funktionalität aller für die finale Darstellung der Website notwendigen Komponenten, wurde das Tool dann beim 3. Projektbeiratstreffen am 28.02.2020 als eine Webanwendung vorgestellt, einmal komplett vorgeführt und besprochen. Hier wurde dann vor allem die Darstellung der Ergebnisse diskutiert, um möglichst leicht verständliche aber sensibilisierende Informationen zu vermitteln. In Zusammenschau mit den Besprechungsergebnissen des Regionalen Unternehmensstammtisches kristallisierte sich die Darstellung über zwei Diagramme heraus: ein Spinnennetzdiagramm, mit dem die Gefährdung durch konkrete Angriffe und das Level der Gefährdung dargestellt wird, und ein Balkendiagramm, das bereits erfüllte und noch fehlende Sicherheitsmaßnahmen sowie deren Einfluss auf das Risiko von Cyberangriffen aufzeigt.

Unter diesen beiden Übersichtsdiagrammen werden dann konkrete Maßnahmen aufgeführt, geordnet nach dem Einfluss, den sie auf das Gesamtrisiko von Cyberangriffen in dem jeweiligen Unternehmen haben. Neben einer kurzen Beschreibung werden weiterführende Links zur sinnvollen Umsetzung der entsprechenden Maßnahmen in der Dokumentation des BSI und in journalistischen Quellen, wie z.B. heise.de, angezeigt. Dabei haben wir uns gegen die Empfehlung von Blogposts trotz ihrer Popularität entschieden, weil diese tendenziell nicht aktualisiert werden, wenn Empfehlungen sich ändern und daher meistens auf Dauer keine zuverlässige Quelle darstellen.

2.2 Wichtige Positionen des zahlenmäßigen Nachweises

Die Ausgaben für die Beauftragung einer CATI-Befragung von netto 5.000 Unternehmen ab zehn Beschäftigten in Deutschland (ca. 46 %) und die Ausgaben für Personal (ca. 45 %) stellten die größten Position im Projektvolumen dar. Das restliche Volumen war überwiegend für die Vergabe weiterer Aufträge (Beratung für Zugang zur Wirtschaft) vorgesehen. Diese Mittel konnte zu einem Teil für die Durchführung der CATI-Befragung umgewidmet werden, da die

Befragung brutto etwa 14 % über den dafür eingeworbenen Kosten lag, und auf den restlichen Teil verzichtet werden, da der Zugang zur Wirtschaft über die Netzwerke der Projektbeiratsmitglieder gesichert war. Weitere Einsparungen bei den Personalmitteln aufgrund eines Personalwechsels in der Projektlaufzeit und bei den Reisekosten aufgrund verringerter Reisetätigkeit im Zuge der Corona-Krise ermöglichten eine kostenneutrale Verlängerung des Projektes um vier Monate. Diese Verlängerung war angesichts von zeitlichen Verzögerungen in der Corona-Krise notwendig, um insbesondere die Aussagekraft der Ergebnisse der zweiten Unternehmensbefragung (AP 9) sicherzustellen und das Arbeitspaket abzuschließen.

2.3 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die Digitalisierung in der deutschen Wirtschaft nimmt weiter zu und hat zuletzt bedingt durch die Corona-Krise zusätzlich an Bedeutung gewonnen. Fast alle Unternehmen sehen die mit der Digitalisierung verbundenen Chancen. Unklarheit herrschte hingegen lange bei der Frage, wie groß die mit ihr verbundenen Risiken in Hinblick auf Cyberkriminalität für Unternehmen unterschiedlicher Größen und Branchen in Deutschland sind und wie sich diese innerhalb eines Jahres entwickeln. Dies wurde u.a. auch in den im Projekt geführten Expert*inneninterviews deutlich. Die Hellfelddaten der Polizeilichen Kriminalstatistik (PKS) weisen zwar seit einigen Jahren auf einen Anstieg der Fallzahlen im Bereich Cyberkriminalität hin, aber die Fragen zum Ausmaß und zur Entwicklung in Deutschland lassen sich mit ihnen aufgrund eines sehr großen Dunkelfeldes (bspw. aufgrund nicht angezeigter Fälle) nicht zuverlässig beantworten. Um diese Risiken bewerten und steuern zu können ist ein differenziertes Wissen zur Art, Häufigkeit und den Folgen von Cyberangriffen gegen Unternehmen sowie zu relevanten Risiko- und Schutzmaßnahmen nötig. Um dieses Wissen zu generieren und offene Fragen zum Risiko und zur IT-Sicherheit von Unternehmen zu klären, wurde das hier beschriebene Projekt durchgeführt. Neben verschiedenen Feldstudien und Expert*innenbefragungen wurden umfangreiche längsschnittliche Daten zum Thema Cyberangriffe gegen Unternehmen in Deutschland unabhängig und nach wissenschaftlichen Standards erhoben und ausgewertet. Mit einer großen repräsentativen Stichprobe von 5.000 Unternehmen ab zehn Beschäftigten wurden differenzierte Schlussfolgerungen hinsichtlich der Verbreitung von Cyberangriffen, des Anzeigeverhaltens und zur Entwicklung verschiedener Cyberangriffsarten möglich, die weit über Erkenntnisse anhand von Hellfelddaten wie der Polizeilichen Kriminalstatistik (PKS) hinausgehen. So konnte z.B. verdeutlicht werden, dass ein großer Teil dieser Unternehmen in den letzten zwölf Monaten von Cyberangriffen betroffen war, was sich aufgrund einer sehr niedrigen Anzeigequote nicht in den offiziellen Kriminalitätsstatistiken widerspiegelt. Daneben zeigte sich, dass die Spannbreite der durch Cyberangriffe verursachten Schäden sehr groß ist, wenngleich die entstandenen direkten Kosten mehrheitlich überschaubar blieben. Insbesondere organisatorische Maßnahmen, die den Faktor Mensch betreffen, scheinen bei der Prävention von Cyberangriffen einen Unterschied zu machen und sind demnach in Hinblick auf ihre Verbreitung vor allem bei kleinen und mittleren Unternehmen besonders zu fördern. Ebenfalls ließ sich zeigen, dass die Belastung durch Cyberangriffe (insbesondere Phishing und sonstige Schadsoftware-Angriffe) zwischen den Jahren 2018 und 2020 gestiegen ist, wobei Vorfälle mit sehr hohen oder sogar bestandsgefährdenden Schäden nach wie vor die Ausnahme sind. Da die Anzeigequote weiterhin sehr gering ausfiel, ist von einem größer gewordenen Dunkelfeld auszugehen. Die Befragung mittels

Web Survey in Befragung II machte es zudem möglich, die Komplexität der IT-Sicherheitsstruktur in den Unternehmen detaillierter zu erfassen und zu untersuchen. Dabei wurden trotz fast überall zum Einsatz kommender basaler technischer IT-Sicherheitsmaßnahmen z.T. große qualitative Unterschiede erkennbar, die in zukünftiger Forschung weiter in den Blick zu nehmen sind.

2.4 Nutzen und Verwertbarkeit der Ergebnisse

Ziel der Initiative „IT-Sicherheit in der Wirtschaft“ ist es, eine höhere IT-Sicherheit bei Unternehmen, insbesondere bei kleinen und mittleren Unternehmen, zu erreichen. Um zu diesem Vorhaben beizutragen, waren die Ziele des vorliegenden Projekts a) Erkenntnisse zur Phänomenologie Cyberangriffe gegen Unternehmen zu erlangen, um besser mit der Problematik umgehen zu können, b) Möglichkeiten der Unterstützung für kleinen und mittelständischen Unternehmen zu erfassen, um diese besser und gezielte ausbauen zu können, c) Handlungsempfehlungen für Unternehmen zu entwickeln, damit diese sich besser schützen können und d) gewonnene Erkenntnisse in die Praxis zu transferieren und dabei v.a. für das Problem zu sensibilisieren. Bezogen auf diese Ziele können die folgenden in den frei verfügbaren Forschungsberichten detailliert dokumentierten Ergebnisse genutzt und weiter verwertet werden:

a) Erkenntnisse zur Phänomenologie

   Erste Erkenntnisse konnten bereits durch die strukturierte Aufarbeitung des Forschungsstands sowie durch die Experteninterviews gewonnen werden und sind in die Konzeption des Fragebogens für die Befragung von 5.000 Unternehmen eingeflossen. Dazu zählt, dass das Phänomen Cyberangriffe gegen Unternehmen sehr dynamisch und vielseitig ist und eine große Bandbreite an verschiedenen Studien existiert, die sich schon in Hinblick auf das methodische Vorgehen und der jeweiligen Operationalisierung zum Teil stark unterscheiden. Daraus resultieren sehr unterschiedliche und teils widersprüchliche Angaben z.B. zur Verbreitung und zu den Folgen von Cyberangriffen. Ferner fallen aber auch viele offene Fragestellungen auf, die bisher nicht oder nur sehr selten adressiert wurden. Dazu zählen insbesondere differenzierte Auswirkungen einzelner Angriffsarten auf Technik, Prozesse, Organisation und Beschäftigte von Unternehmen, Art und Höhe entstehender Kosten infolge von Cyberangriffen und nicht zuletzt Risiko- und Schutzfaktoren, die sich auf die Betroffenheit von Cyberangriffen auswirken.

   Daher erfolgte eine transparent dokumentierte Ziehung einer geschichteten Zufallsstichprobe, die es unter Berücksichtigung gewisser Einschränkungen erlaubt, Rückschlüsse auf die Grundgesamtheit (Unternehmen in Deutschland mit mehr als zehn Beschäftigten) zu ziehen, die z.B. bei Willkürstichproben ausgeschlossen sind. Die vergleichsweise große Nettostichprobe von 5.000 Unternehmen macht es zudem möglich, Ergebnisse und Zusammenhänge differenzierter darzustellen als in vielen Studien mit kleinerem Stichprobenumfang. Daneben ermöglicht die Nutzung von WZ08-Klassen zur Zuordnung der Branchenzugehörigkeit der Unternehmen zum einen die Vergleichbarkeit mit anderen offiziellen Unternehmensstatistiken, als auch die internationale Anschlussfähigkeit der Ergebnisse für bestimmte Branchen. Des Weiteren wurden unterschiedliche strukturelle Unternehmensmerkmale sowie IT-Sicherheitsmaßnahmen in Zusammenhang mit der Betroffenheit von Cyberangriffen gesetzt und die herausgearbeiteten

möglichen Risiko- und Schutzfaktoren differenziert nach Beschäftigtengrößenklassen dargestellt. Von dem umfangreichen Forschungsbericht wurde anschließend für den Ergebnistransfer eine zielgruppengerecht aufbereitete Kurzversion erstellt, die zusammen mit zwei erarbeiteten Factsheets im Rahmen von Messen und Tagungen sowie auf der Webseite des Projektes zur Verfügung gestellt wurde.

b) Möglichkeiten der Unterstützung für kleinen und mittelständischen Unternehmen

Viele Unternehmen scheinen die Cyberangriffsrisiken zu unterschätzen, denn ein Anteil von 69 % geht von einem sehr oder eher geringen Risiko aus, in den nächsten zwölf Monaten von einem ungezielten Cyberangriff getroffen zu werden. Bezogen auf gezielte Angriffe liegt dieser Anteil bei erstaunlichen 93 %. Unternehmen, die in den letzten zwölf Monaten auf keinen Cyberangriff reagieren mussten, schätzten diese Risiken zudem noch deutlich geringer ein. Daher scheint es weiterhin sinnvoll zu sein, im Rahmen von Awareness-Kampagnen auf die bestehenden und sich verändernden Risiken hinzuweisen.

Hinzu kommt, dass lediglich 12 % der Unternehmen den schwerwiegendsten Cyberangriff der letzten zwölf Monate polizeilich anzeigten. Zwar erstatten größere Unternehmen (ab 500 Beschäftigte) mit 22 % häufiger Anzeige als kleine Unternehmen (10-49 Beschäftigte) mit 11 %, aber von der überwiegenden Mehrheit der Cyberangriffe erlangen die Strafverfolgungsbehörden demnach keine Kenntnis. Ein relativ häufig genannter Nichtanzeigegrund ist die Unsicherheit von Unternehmen, an wen genau sie sich für eine Anzeige wenden müssen. Diesbezüglich ist stärker auf die Zentralen Ansprechstellen Cybercrime (ZAC) für Wirtschaftsunternehmen der Polizei hinzuweisen und die Sinnhaftigkeit solcher Anzeigen zu vermitteln.

In Hinblick auf die bereits vorhandenen IT-Sicherheitsmaßnahmen zeigen die Ergebnisse der Befragung, dass so gut wie alle Unternehmen bereits grundlegende technische IT-Sicherheitsmaßnahmen einsetzen. Dazu gehören regelmäßige Backups und deren physisch getrennte Aufbewahrung, aktuelle Antivirensoftware, regelmäßige und zeitnahe Installation verfügbarer Sicherheitsupdates und Patches sowie eine Firewall. Der Anteil der Unternehmen mit diesen technischen Maßnahmen liegt in allen Unternehmensgrößenklassen jeweils über 90 %. Insbesondere kleine und mittlere Unternehmen sollten daher darin bestärkt und unterstützt werden, die vorhandenen technischen IT-Sicherheitsmaßnahmen regelmäßig zu überprüfen, zu warten, ggf. zu verbessern und sie stärker in organisatorische Abläufe und Prozesse der Unternehmen einzubinden.

Daneben sollte das Zusammenspiel von Mensch und Technik stärker in den Blick genommen werden. Denn gegenüber den technischen Maßnahmen sind organisatorischen IT-Sicherheitsmaßnahmen weniger weit verbreitet. Etwa ein Drittel der Unternehmen hat keine schriftlich fixierten Richtlinien zur IT-Sicherheit. Knapp die Hälfte der Unternehmen verfügt über keine schriftlich fixierten Richtlinien zum Notfallmanagement, führt keine regelmäßigen Risiko- und Schwachstellenanalysen und keine Schulungen zur IT-Sicherheit für Beschäftigte durch. Nur jeweils ein Viertel der Unternehmen hat eine zertifizierte IT-Sicherheit und führt Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme durch. Gleichzeitig weisen die Ergebnisse darauf hin, dass diese

organisatorischen Maßnahmen im Zusammenhang mit der Betroffenheit von Cyberangriffen stehen und somit einen wichtigen Baustein zur Abwehr von Cyberangriffen darstellen. Vor allem Unternehmen, die schriftlich fixierte Richtlinien einsetzen und darüber hinaus deren Einhaltung regelmäßig überprüfen und Verstöße ggf. ahnden, waren mit 35 % deutlich seltener betroffen als Unternehmen, die dies nicht taten (55 %). Schulungen zur IT-Sicherheit für Beschäftigte stehen vor allem bei mittleren Unternehmen (50 bis 499 Beschäftigte) im Zusammenhang mit einer niedrigeren Betroffenheitsrate. Während etwa die Hälfte der mittleren Unternehmen ohne solche Schulungen auf Cyberangriffe reagieren musste, lag der Anteil bei Unternehmen mit geschulten Beschäftigten rund zehn Prozentpunkte darunter.

c) Handlungsempfehlungen für Unternehmen

Das Ziel, Handlungsempfehlungen für Unternehmen zu erarbeiten, baut ebenfalls auf den Erkenntnissen der Unternehmensbefragung auf. Von diesen Ergebnissen ausgehend lassen sich insbesondere für kleine und mittlere Unternehmen mit verschiedenen risikosteigernden Merkmalen drei Schlussfolgerungen für die Verbesserung der IT-Sicherheit ziehen:

- IT-Sicherheit beginnt mit Risikobewusstsein: Unternehmen sollten sich ihrer Risikomerkmale und ihres Cyberangriffsrisikos bewusst sein. Gibt es z.B. bestimmte Unternehmensmerkmale, die für Angreifer interessant sein könnten bzw. die das Risiko eines Cyberangriffs erhöhen? Vor welchen Cyberangriffsarten ist das Unternehmen möglicherweise besonders bedroht? Welche Schutzgüter sind vor dem Hintergrund begrenzter Ressourcen besonders zu schützen und vor wem oder gegen was?
- Technik ist nicht gleich Technik: Unternehmen sollten regelmäßig den Bedarf, die Qualität, den Reifegrad, die Konfiguration und die Funktionsfähigkeit technischer IT-Maßnahmen überprüfen, ggf. verbessern und an veränderte Anforderungen anpassen. Ist z.B. die Frequenz der Datensicherung angemessen, funktioniert die Datenwiederherstellung und wieviel Zeit wird ggf. dafür benötigt? Ist der Firewall-Schutz, d.h. die Art der Paketfilterung, ausreichend und fachgerecht konfiguriert?
- Technik allein reicht nicht: Unternehmen sollten das Zusammenspiel von Mensch und Technik innerhalb der Organisation stärker in den Blick nehmen. Sind z.B. die technischen Maßnahmen mit Verhaltensregeln verbunden? Werden sie regelmäßig überprüft, kommuniziert und „richtige“ Verhaltensweisen gefördert oder hängen diese Regeln möglicherweise sogar mit problematischen Ausweichhandlungen zusammen, da sie sich z.B. nicht sinnvoll in den Arbeitsalltag der Beschäftigten integrieren lassen? Gibt es eine positive und konstruktive Fehlerkultur, die eine schnelle Fehlererkennung und -analyse erlaubt und so zur Verbesserung der IT-Sicherheit beiträgt?

d) Praxistransfer

Der Transfer der Ergebnisse in die Praxis wurde in der Transferphase realisiert. Diese wurde durch ein Transferkonzept vorbereitet. Alle wesentlichen Transferaktivitäten

sind in Tabelle 2 und Tabelle 3 aufgeführt. Neben den genannten Vortragstätigkeiten und der realisierten Webpräsenz ist die umfangreiche Öffentlichkeitsarbeit zur Veröffentlichung der Forschungsergebnisse zu erwähnen, die allerdings von der Covid-19-Krise überschattet wurde. Daneben wurde ein Kurzbericht für Verantwortliche und Entscheider*innen insbesondere kleiner und mittlerer Unternehmen erarbeitet und zusammen mit zwei Factsheets zur freien Verfügung gestellt. Der Kurzbericht wurde bereits an die 5.000 Unternehmen versendet, die an der Befragung teilgenommen haben. Der Artikel im iX-Magazin für professionelle Informationstechnik des Heise-Zeitschriften-Verlags mit einer Druckauflage von ca. 39.000 Exemplaren dürfte ebenfalls zur weiteren Verbreitung der zentralen Ergebnisse und zur Vergrößerung der Bekanntheit des Projektes und der Initiative „IT-Sicherheit in der Wirtschaft“ beigetragen haben. Darüber hinaus bietet die auf den Ergebnissen der Unternehmensbefragungen basierende Vorhersage-Plattform CARE eine einfache Möglichkeit individuelle Schwachpunkte bei der IT-Sicherheit zu erkennen und gezielte Hinweise für deren Beseitigung. Sowohl alle projektbezogenen Ergebnisberichte und Materialien als auch die Vorhersage-Plattform CARE stehen auf der Webseite des KFN:

https://kfn.de/forschungsprojekte/cyberangriffe-gegen-unternehmen/

und der Webseite des Projektes:

https://cybercrime-forschung.de

frei zur Verfügung. CARE wurde zudem in den Sec-O-Mat der TISiM aufgenommen und verlinkt, womit eine nachhaltige Verwertung auch nach Ende des Projektes gegeben ist.

Der strukturiert aufbereitete Forschungsstand und die umfänglich in Forschungsberichten dokumentierten Projektergebnisse leisten einen Beitrag zur weiteren Erforschung und zur Erhöhung der IT-Sicherheit von Unternehmen. Insbesondere die Ergebnisse der Unternehmensbefragungen ermöglichen eine nach Wirtschaftszweigen und Beschäftigtengrößenklassen differenzierte Lageeinschätzung und bieten Hinweise auf relevante Risiko- und Schutzfaktoren. Das auf den Daten der Unternehmensbefragungen basierende Risikoprognosetool CARE ist aller Voraussicht nach mindestens drei Jahre nach Projektende online und kann in dieser Zeit kostenfrei genutzt werden. Für diesen Zeitraum wird der Betrieb mit Sicherheitsupdates aber ohne inhaltliche Aktualisierungen sichergestellt.

2.5 Fortschritt bei anderen Stellen

Die Datenlage bezogen auf Unternehmen als Betroffene von Cyberangriffen ist nach wie vor als unzureichend und fragmentiert zu beschreiben. Neben den diversen kommerziellen Studien aus der IT-, Beratungs- und Versicherungswirtschaft, die aufgrund inhaltlicher Interessenskonflikte und z.T. methodischer Einschränkungen nicht immer als unproblematisch anzusehen sind, herrscht weiterhin ein Mangel an unabhängigen wissenschaftlichen Studien.[11] Für aktuelle

[11] Vgl. Lamprecht & Vladova (2020: 348). Eine ausführliche Darstellung des Forschungsstandes zum Thema Cyberangriffe gegen Unternehmen findet sich bei Dreißigacker et al. (2020a: 21ff.).

empirische Forschungsergebnisse außerhalb des Forschungsprojektes „Cyberangriffe gegen Unternehmen“ kann auf die Studie „Cyber Security Breaches Survey“ des Britischen Ministeriums für Digitales, Kultur, Medien und Sport[12] verwiesen werden, die sich mittels Repräsentativbefragung den Einschätzungen und Maßnahmen von Unternehmen gegen Cyber-Bedrohungen sowie den Kosten und Auswirkungen von Vorfällen widmet. Die Studie von Buil-Gil et al.[13] analysiert den Einfluss von Online-Verhalten und dem Vorhandensein von Sicherheitsmaßnahmen auf die Viktimisierung von Unternehmen in Großbritannien. Die Ergebnisse dieser beiden Studien sind aufgrund anders zusammengesetzter Stichproben nicht sinnvoll direkt mit den Ergebnissen der Unternehmensbefragungen in diesem Projekt zu vergleichen. Dennoch weisen auch sie z.B. darauf hin, dass die direkten Kosten infolge von Cyberangriffen sehr schief verteilt und mehrheitlich sehr gering sind und dass dem “Faktor Mensch” und organisatorischen Maßnahmen wie IT-Sicherheitsschulung der Beschäftigten gegenüber rein technischen Maßnahmen mehr Bedeutung beigemessen werden sollte.

2.6 Erfolgte und geplante Veröffentlichungen der Ergebnisse

Alle bereits veröffentlichten bzw. eingereichten Ergebnisse sind bereits in Tabelle 3 (siehe Abschnitt 2.1 AP 6) aufgeführt, dabei handelt es sich um vier KFN-Forschungsberichte (Nr. 152, 155, 158 und 162), einen zielgruppenspezifisch aufbereiteten Kurzbericht, drei Factsheets, zwei Sammelbandbeiträge sowie ein Poster und drei Beiträge für internationale Fachzeitschriften bzw. Tagungsberichte (siehe auch Anhang 1). Darüber hinaus befinden sich ein weiterer Sammelbandbeitrag zu den Ergebnissen der beiden Unternehmensbefragungen und drei weitere Fachzeitschriften-/Tagungsbeiträge zu den Kosten von Cyberangriffen in der Vorbereitung:

- Dreißigacker, A; Skarczinski, B.v.; Wollinger, G.R.: Unternehmen als Opfer von Cyberkriminalität. In: Rüdiger & Bayerl (Hrsg.): Cyberkriminologie. Band 2 [Arbeitstitel]. Springer
- Skarczinski, B.v.; Dreißigacker, A.; Teuteberg, F.: Towards enhancing the information base on direct costs of cyber-attacks on organizations: Implications from literature and a large-scale survey. Organizational Cybersecurity Journal (OCJ), eingereicht am 10.08.2021.
- Skarczinski, B.v.; Dreißigacker, A.; Teuteberg, F.: Exploring the Link between Security Measures and Direct Costs of Cyber-Attacks on Firms: An Analysis of Survey Data using PLS-PM. Internationale Tagung Wirtschaftsinformatik (WI), eingereicht am 31.08.2021.
- Skarczinski, B.v.; Raschke, M.: Modeling costs of cyber-attacks [Arbeitstitel]. Journal of Risk and Insurance.

[12] Department for Digital, Culture, Media & Sport (2021).
[13] Buil-Gil et al. (2021).

3 Anhang: Kurzzusammenfassung der Fachbeiträge

- Dreißigacker & Wollinger: Verbreitung von Cyberkriminalität gegen Unternehmen in Deutschland.
- Dreißigacker et al.: Im Visier: Repräsentative Studie zur Cyberkriminalität in deutschen Unternehmen.
- Huaman et al.: A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises.
- Skarczinski et al.: Understanding the adoption of cyber insurance for residual risks – An empirical large-scale survey on organizational factors of the demand side
- Skarczinski et al.: Towards enhancing the information base on direct costs of cyber-attacks on organizations: Implications from literature and a large-scale survey.
- Huaman et al.: A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises.
- Dreißigacker et al.: Cyberangriffe gegen Unternehmen: Erste Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland.

3.1 Verbreitung von Cyberkriminalität gegen Unternehmen in Deutschland

Autor*innen:

Dreißigacker, A.[1]; Wollinger, G.R.[2]

Institutionen:

[1] Kriminologisches Forschungsinstitut Niedersachsen e.V., Hannover

[2] Hochschule für Polizei und öffentliche Verwaltung Nordrhein-Westfalen, Köln

Sammelband:

Wollinger & Schulze (Hrsg.) (2020): Handbuch für Cybersecurity für die öffentliche Verwaltung, Wiesbaden: Kommunal- und Schul-Verlag

Abstrakt:

Der Beitrag thematisiert die Frage der Verbreitung von Cyberangriffen in Deutschland, d.h., in welcher Häufigkeit Straftaten aus dem genannten Bereich vorkommen und wer davon betroffen ist. Da es bislang an Untersuchungen mangelt, werden die Daten der Unternehmensbefragung des Projektes "Cyberangriffe gegen Unternehmen" herangezogen, um sich dem Ausmaß von Cyberkriminalität gegen die öffentliche Verwaltung in Deutschland anzunähern. Dies erscheint insofern ein geeigneter Weg zu sein, als dass Unternehmen gewisse organisationale Ähnlichkeiten mit Behörden aufweisen und Kommunen auch Träger öffentlicher Unternehmen der Daseinsvorsorge wie z.B. Versorgungs- und Verkehrsbetriebe sind. Auch wenn in der herangezogenen Studie Behörden bzw. Unternehmen der öffentlichen Verwaltung nicht im Mittelpunkt standen, legen die Ergebnisse nahe, dass diese ebenso durch Cyberangriffe gefährdet sind und weitere Forschung zu diesem speziellen Bereich notwendig ist, um ein differenzierteres Lagebild zu erhalten sowie spezifische Risiko- und Schutzfaktoren herauszustellen.

3.2 Im Visier: Repräsentative Studie zur Cyberkriminalität in deutschen Unternehmen

Autor*innen:

Dreißigacker, A.[1]; Skarczinski, B.v.[2]; Wollinger, G.R.[3]

Institutionen:

[1] Kriminologisches Forschungsinstitut Niedersachsen e.V., Hannover

[2] PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, Hannover

[3] Hochschule für Polizei und öffentliche Verwaltung Nordrhein-Westfalen, Köln

Journal:

iX – Magazin für professionelle Informationstechnik (6/2020)

Abstrakt:

Die Digitalisierung in der Gesellschaft bietet Unternehmen vielfältige Chancen und Möglichkeiten, birgt aber gleichzeitig auch Risiken z.B. in Form von Cyberkriminalität. Cyberangriffe und deren Auswirkungen stellen ein unternehmerisches Risiko dar, das sich aufgrund der fehlenden verlässlichen Datenbasis nur schwer einschätzen, bewerten und steuern lässt. Der Beitrag stellt ausgewählte Ergebnisse des im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie (BMWi) geförderten Projektes “Cyberangriffe gegen Unternehmen” vor. Auf Basis einer groß angelegten repräsentativen Befragung von 5.000 Unternehmen in Deutschland wird gezeigt, dass nicht alle Unternehmen gleichermaßen betroffen sind und auf mögliche Risiko- und Schutzfaktoren hingewiesen.

3.3 A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises

Autor*innen:

Huaman, N.[1]; Skarczinski, B.v.[2]; Stransky, C.[3]; Wermke, D.[3]; Acar, Y.[4]; Dreißigacker, A.[5]; Fahl, S.[1]

Institutionen:

[1] Leibniz-Universität Hannover, CISPA Helmholtz Center for Information Security

[2] PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, Hannover

[3] Leibniz-Universität Hannover

[4] Leibniz-Universität Hannover, Max-Planck-Institute for Security and Privacy

[5] Kriminologisches Forschungsinstitut Niedersachsen e.V., Hannover

Konferenz:

USENIX Security ’21

Abstrakt:

Cybercrime is on the rise. Attacks by hackers, organized crime and nation-state adversaries are an economic threat for companies world-wide. Small and medium-sized enterprises (SMEs) have increasingly become victims of cyberattacks in recent years. SMEs often lack the awareness and resources to deploy extensive information security measures. However, the health of SMEs is critical for society: For example, in Germany, 38.8% of all employees work in SMEs, which contributed 31.9% of the German annual gross domestic product in 2018. Many guidelines and recommendations encourage companies to invest more into their information security measures. However, there is a lack of understanding of the adoption of security measures in SMEs, their risk perception with regards to cybercrime and their experiences with cyberattacks. To address this gap in research, we performed 5,000 computer-assisted telephone-interviews (CATIs) with representatives of SMEs in Germany. We report on their experiences with cybercrime, management of information security and risk perception. We present and discuss empirical results of the adoption of both technical and organizational security measures and risk awareness in SMEs. We find that many technical security measures and basic awareness have been deployed in the majority of companies. We uncover differences in reporting cybercrime incidences for SMEs based on their industry sector, company size and security awareness. We conclude our work with a discussion of recommendations for future research, industry and policy makers.

3.4 Understanding the adoption of cyber insurance for residual risks – An empirical large-scale survey on organizational factors of the demand side

Autor*innen:

Skarczinski, B.v.[1]; Boll, L.[2]; Teuteberg, F.[3]

Institutionen:

[1] PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, Hannover

[2] Kriminologisches Forschungsinstitut Niedersachsen e.V., Hannover

[3] Universität Osnabrück

Journal:

ECIS 2021 Research Papers. 72.

Abstrakt:

This research paper analyzes technological, organizational, and environmental (TOE framework) adoption factors of cyber insurances (CI) by conducting a computer-assisted telephone interview study with 2,483 German firms. Considering our screening of related literature, this study, to our knowledge, is the first large-scale empirical study analyzing organizational adoption factors of CI on the demand side. We distinguish between firms that have or have not considered CI and those that have or have not adopted CI following considerations. Our regression results indicate that there are statistically significant factors on the consideration and adoption of CI across all TOE dimensions. Subsequently, we discuss the extent to which CI is perceived as an appropriate tool to manage information security and derive propositions for the education of firms and further research in academia.

3.5 Towards enhancing the information base on direct costs of cyber-attacks on organizations: Implications from literature and a large-scale survey

Autor*innen:

Skarczinski, B.v.[1]; Dreißigacker, A.[2]; Teuteberg, F.[3]

Institutionen:

[1] PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, Hannover

[2] Kriminologisches Forschungsinstitut Niedersachsen e.V., Hannover

[3] Universität Osnabrück

Journal:

Eingereicht bei: Organizational Cybersecurity Journal

Abstrakt:

Despite the global relevance of information security, cyber-attacks and their consequences have been relatively little researched. Especially the missing empirical basis of costs caused by cyber-attacks on an organizational level is stated in literature. At the same time, transparency about costs is urgently needed by managers, since also information security management (ISM) is subject to the principles of economic efficiency. In order to make well-informed decisions, managers are dependent on reliable data on costs and benefits of IS, which are often retrieved from external sources. To enhance the information base on direct costs of cyber-attacks we analyze existing literature and find it hardly meets our benchmark requirements. Due to the lack of reliable data, we conduct a large-scale computer assisted telephone interview survey with 5,000 German organizations and show costs as a consequence of crime as well as costs responding to crime directly assignable to the most severe attack within the last 12 months by eight attack types, six costs items, employee classes and industries. Our findings indicate the majority of organizations in Germany suffer no or little such costs, whereas a small part suffers high costs. However, organizations are not affected equally, since prevalence rates and costs by attack-types, employee class and other variables tend to vary. Moreover, we find indications that board members and IT-managers show partly different response behaviors. Based on existing literature, expert interviews and our empirical results we drafted an activity plan containing further research questions and action items for organizations, government/society and academia on how information on costs of cyber-attacks could be better collected and used.

3.6 Cybercrime in Small and Medium-sized Enterprises

Autor*innen:

Huaman, N.[1]; Krause, A.[3]; Skarczinski, B.v.[2]; Stransky, C.[3]; Wermke, D.[3]; Acar, Y.[4]; Dreißigacker, A.[5]; Fahl, S.[1]

Institutionen:

[1] Leibniz-Universität Hannover, CISPA Helmholtz Center for Information Security

[2] PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, Hannover

[3] Leibniz-Universität Hannover

[4] Leibniz-Universität Hannover, Max-Planck-Institute for Security and Privacy

[5] Kriminologisches Forschungsinstitut Niedersachsen e.V., Hannover

Postersession:

SOUPS 2021 Posters

Abstrakt:

Cybercrime is on the rise. Attacks by hackers, organized crime and nation-state adversaries are an economic threat for companies world-wide. Small and medium-sized enterprises (SMEs) have increasingly become victims of cyberattacks in recent years. SMEs often lack the awareness and resources to deploy extensive information security measures. However, the health of SMEs is critical for society: For example, in Germany, 38.8% of all employees work in SMEs, which contributed 31.9% of the German annual gross domestic product in 2018. Many guidelines and recommendations encourage companies to invest more into their information security measures. However, there is a lack of understanding of the adoption of security measures in SMEs, their risk perception with regards to cybercrime and their experiences with cyberattacks. To address this gap in research, we performed 5,000 computer-assisted telephone-interviews (CATIs) with representatives of SMEs in Germany. We report on their experiences with cybercrime, management of information security and risk perception. We present and discuss empirical results of the adoption of both technical and organizational security measures and risk awareness in SMEs. We find that many technical security measures and basic awareness have been deployed in the majority of companies. We uncover differences in reporting cybercrime incidences for SMEs based on their industry sector, company size and security awareness. We conclude our work with a discussion of recommendations for future research, industry and policy makers.

3.7 Cyberangriffe gegen Unternehmen: Erste Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland

Autor*innen:

Dreißigacker, A.[1]; Skarczinski, B.v.[2]; Wollinger, G.R.[3]

Institutionen:

[1] Kriminologisches Forschungsinstitut Niedersachsen e.V., Hannover

[2] PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, Hannover

[3] Hochschule für Polizei und öffentliche Verwaltung Nordrhein-Westfalen, Köln

Sammelband:

Grafl; Stempkowski; Beclin & Haider (Hrsg.): "Sag, wie hast du's mit der Kriminologie?". Die Kriminologie im Gespräch mit ihren Nachbardisziplinen. Mönchengladbach: Forum Verlag Godesberg (Neue Kriminologische Schriftenreihe, 118)

Abstrakt:

Nach einer kurzen Einführung in das Themenfeld Cybercrime mit den verschiedenen Delikts- und Phänomenbereichen stellt der Beitrag das methodische Vorgehen und erste Ergebnisse einer CATI-Befragung mit 5.000 Unternehmen ab 10 Beschäftigten in Deutschland zur Betroffenheit, zu den vorhandenen IT-Sicherheitsmaßnahmen sowie zu den Folgen der schwerwiegendsten Cyberangriffe vor. Zu den zentralen Befunden zählt, dass viele Unternehmen innerhalb eines Jahres von verschiedenen Cyberangriffsarten betroffen sind, obwohl insbesondere technischer Sicherheitsmaßnahmen vorhanden waren. Phishing und Schadsoftware-Angriffe zählen zu den am häufigsten erlebten Angriffsarten, werden aber nur relativ selten angezeigt, womit von einem sehr großen Dunkelfeld ausgegangen werden kann.

Tabellen

Tabelle 1: Projektbezogene Transferaktivitäten 29
Tabelle 2: Projektbezogene Ergebnisse 33

Abbildungen

Abbildung 1: Arbeitspakete 9
Abbildung 2: Projektplan 10
Abbildung 3: Tatsächlicher Projektablauf 11
Abbildung 4: Projektbeteiligte 15

Literatur

Baier, D., Krenz, M., & Bergmann, M. C. (2016). Verbreitung und Einflussfaktoren des Cyberbullyings: Ergebnisse einer Repräsentativbefragung in Niedersachsen. Zeitschrift für Soziologie der Erziehung und Sozialisation, 36(3), 227–245.

Bergmann, M.C. (2018). Prävalenzen und Prädiktoren von Cyberbullying im Schulformvergleich. Bildung und Erziehung (71) 1: 49-64.

Bergmann, M.C., & Baier, D. (2016). Erfahrungen von Jugendlichen mit Cybergrooming: Schülerbefragung – Jugenddelinquenz. Rechtspsychologie, 2(2), 172–189. doi:10.5771/2365-1083-2016-2-172

Bergmann, M.C.; Baier, D. (2018). Prevalence and Correlates of Cyberbullying Perpetration. Findings from a German Representative Student Survey. International Journal of Environmental Research and Public Health 15(2), 274. http://www.mdpi.com/1660-4601/15/2/274

Bergmann, M. C., Beckmann, L., Krieg, Y., Schepker, K., Baier, D., & Mößle, T. (2016). Cyberbullying, Cyberstalking und Cybergrooming – Gefahren der Nutzung neuer Medien. Eine Befragung an Katholischen Schulen in Nordrhein-Westfalen. Hannover: KFN.

Bergmann, M.C.; Dreißigacker, A.; Skarczinski, B.v. & Wollinger, G.R. (2018). Cyber-Dependent Crime Victimization: The Same Risk for Everyone? Cyberpsychology, Behavior, and Social Networking Vol. 21 (2), S. 84–90. DOI: 10.1089/cyber.2016.0727

Bitkom (Hrsg.) (2015): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter. Abrufbar unter: https://www.bitkom.org/Publikationen/2015/Studien/Studienbericht-Wirtschaftsschutz/150709-Studienbericht-Wirtschaftsschutz.pdf (geprüft am 1.2.2016).

BMWi (Hrsg.) (2012): IT-Sicherheitsniveau in kleinen und mittleren Unternehmen. Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie. Abrufbar unter: http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Redaktion/PDF/it-sicherheit-studie-publikation,property=pdf,bereich=itsicherheit,sprache=de,rwb=true.pdf (geprüft am 14.3.2016)

Bollhöfer, E. & Jäger, A. (2018). Wirtschaftsspionage und Konkurrenzausspähung. Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung. Freiburg i.Br.: Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V. Zugriff am 16.10.2019. Verfügbar unter https://wiskos.de/files/pdf4/M3_Komplett_Online_neu_doi.pdf

Buil-Gil, D., N. Lord & E. Barrett, 2021: The Dynamics of Business, Cybersecurity and Cyber-Victimization: Foregrounding the Internal Guardian in Prevention. Victims & Offenders 16: 286–315.

Bundeskriminalamt (Hrsg.) (2014): Cybercrime. Bundeslagebild 2014. Wiesbaden.

Department for Digital, Culture, Media & Sport (DCMS), 2021: Cyber Security Breaches Survey. London, UK.

Dreißigacker, A. & Riesner, L. (2018). Private Internetnutzung und Erfahrung mit computerbezogener Kriminalität. Ergebnisse der Dunkelfeldstudien des Landeskriminalamtes Schleswig-Holstein 2015 und 2017. (KFN-Forschungsberichte No. 139). Hannover: KFN.

Dreißigacker, A. & Wollinger, G.R. (2020): Verbreitung von Cyberkriminalität gegen Unternehmen in Deutschland. In: Gina Rosa Wollinger und Anna Schulze (Hg.): Handbuch Cybersecurity für die öffentliche Verwaltung. Wiesbaden: Kommunal- und Schul-Verlag (KSV Verwaltungspraxis), S. 89-109.

Dreißigacker, A., Skarczinski, B.v. & Wollinger, G.R. (2020a): Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019. (KFN-Forschungsberichte 152). Hannover: KFN.

Dreißigacker, A., Skarczinski, B.v. & Wollinger, G.R. (2020b): Im Visier: Repräsentative Studie zur Cyberkriminalität in deutschen Unternehmen. In: iX - Magazin für professionelle Informationstechnik (6), S. 78-81.

Dreißigacker, A., Skarczinski, B.v. & Wollinger, G.R. (2020c): Cyberangriffe gegen Unternehmen: Erste Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland. In: C. Grafl, M. Stempkowski, K. Beclin & I. Haider (Hg.): "Sag, wie hast du's mit der Kriminologie?". Die Kriminologie im Gespräch mit ihren Nachbardisziplinen. Mönchengladbach: Forum Verlag Godesberg (Neue Kriminologische Schriftenreihe, 118), S. 933-952.

Dreißigacker, A., Skarczinski, B.v. & Wollinger, G.R. (2021): Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer Folgebefragung 2020. (KFN-Forschungsberichte 162). Hannover: KFN.

Gewerkschaft der Polizei (Hrsg.) (2014): Cybercrime. Digitaler Angriff auf die Wirtschaft. Hamm.

Huaman, N., Skarczinski, B.v., Wermke, D., Stransky, C., Acar, Y., Dreißigacker, A. & Fahl, S. (2021): A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises. In: Proceedings of the 30th USENIX Security Symposium.

IHK-Nord (Hrsg.) (2013): Unternehmensbefragung zur Betroffenheit der norddeutschen Wirtschaft von Cybercrime. Abrufbar unter: http://www.hannover.ihk.de/fileadmin/data/Dokumente/Themen/Sicherheit/Studie_Cybercrime_Umfrageauswertung_10062013.pdf (geprüft am 1.2.2016).

KPMG (Hrsg.) (2015): e-Crime. Computerkriminalität in der deutschen Wirtschaft. Abrufbar unter: https://www.kpmg.com/DE/de/Documents/e-crime-studie-2015.pdf. (geprüft am 1.2.2016).

Kriminologisches Forschungsinstitut Niedersachsen e.V. (2020): Cyberangriffe gegen Unternehmen. Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland 2018/2019. Kurzbericht. Hannover: KFN.

Lamprecht, S. & G. Vladova, 2020: Cyber-Viktimisierung von Unternehmen. S. 345–371 in: T.-G. Rüdiger & P.S. Bayerl (Hrsg.), Cyberkriminologie. Wiesbaden: Springer Fachmedien Wiesbaden.

PwC, Martin-Luther-Universität Halle-Wittenberg (Hrsg.) 2016: Wirtschaftskriminalität in der analogen und der digitalen Wirtschaft. Abrufbar unter: http://www.pwc.de/de/risiko-management/assets/studie-wirtschaftskriminalitaet-2016.pdf (geprüft am 14.3.2016).

Rantala, R. R. (2008): Cybercrime against Business. Bureau of Justice Statistics, Special Report. Abrufbar unter: http://www.justiceacademy.org/iShare/Library-BJS/CyberCrimes.pdf (geprüft am 7.3.2016).

Smith, K. T.; Smith, L. M.; Smith J. L. (2011): Case Studies of Cybercrime and its Impact on Marketing Activity and Shareholder Value. In: Academy of Marketing Studies Journal.

Skarczinski, B.v., Boll, L. & Teuteberg, F. (2021): Understanding the adoption of cyber insurance for residual risks. An empirical large-scale survey on organizational factors of the demand side. In: ECIS 2021 Research Papers (72).

Stiller, A., L. Boll, S. Kretschmer, G.R. Wollinger & A. Dreißigacker, 2020: Cyberangriffe gegen Unternehmen in Deutschland: Ergebnisse einer qualitativen Interviewstudie mit Experten. KFN-Forschungsbericht 155. Hannover: KFN.

ISBN: 978-3-948647-13-1