KRIMINOLOGISCHES
FORSCHUNGSINSTITUT
NIEDERSACHSEN E.V.

Forschungsbericht Nr. 155

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

IT-Sicherheit
IN DER WIRTSCHAFT

Cyberangriffe gegen Unternehmen in Deutschland

Ergebnisse einer qualitativen Interviewstudie mit Experten

Zusatzförderung durch: pwc VHV STIFTUNG

Anja Stiller, Lukas Boll, Saskia Kretschmer, Gina Rosa Wollinger, Arne Dreißigacker

2020

FORSCHUNGSBERICHT Nr. 155

Cyberangriffe gegen Unternehmen in Deutschland

Ergebnisse einer qualitativen Interviewstudie mit Experten

Anja Stiller, Lukas Boll, Saskia Kretschmer, Gina Rosa Wollinger, Arne Dreißigacker

2020

Diese Publikation wurde vom Kriminologischen Forschungsinstitut Niedersachsen e. V. innerhalb des Projektes „Cyberangriffe gegen Unternehmen“ und im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie (BMWi) erstellt und ist unter https://kfn.de/publikationen/kfn-forschungsberichte/ eingestellt.

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

Projektlaufzeit: Dez. 2017 – Nov. 2020

Initiative „IT-Sicherheit in der Wirtschaft“

Die Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie will vor allem kleine und mittelständische Unternehmen beim sicheren Einsatz von IKT-Systemen unterstützen. Gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung soll eine Grundlage dafür geschaffen werden, um die Bewusstseinsbildung in der digitalen Wirtschaft beim Thema IT-Sicherheit im Mittelstand zu stärken. Unternehmen sollen durch konkrete Unterstützungsmaßnahmen dazu befähigt werden, ihre IT-Sicherheit zu verbessern. Weitere Informationen zur Initiative und ihren Angeboten sind unter www.it-sicherheit-in-der-wirtschaft.de abrufbar.

Druck: DruckTeam Druckgesellschaft mbH, Hannover.

© Kriminologisches Forschungsinstitut Niedersachsen e.V., 2020
Lützerodestraße 9, 30161 Hannover
Tel. +49 (0)511 34836-0, Fax: +49 (0)511 34836-10
E-Mail: kfn@kfn.de, Internet: www.kfn.de

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

IT-Sicherheit IN DER WIRTSCHAFT

aufgrund eines Beschlusses des Deutschen Bundestages

Zusatzförderung durch:

pwc

VHV STIFTUNG

Printed in Germany
Alle Rechte vorbehalten.

INHALT

ZUSAMMENFASSUNG

Das Projekt „Cyberangriffe gegen Unternehmen“ wird im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ vom Bundesministerium für Wirtschaft und Energie gefördert. Eine Zusatzförderung erfolgt durch die Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers sowie die VHV-Stiftung.

Nach der Aufarbeitung des Forschungsstands wurde die Befragung von Experten insbesondere aus Bundes- und Landesbehörden, die sich beruflich explizit mit Cyberangriffen auf Unternehmen beschäftigen, als zweites Arbeitspaket innerhalb des modular aufgebauten Projektes durchgeführt und bildet die Grundlage für diesen Bericht. Ziel dieser Befragung 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. Darüber hinaus diente sie als Ausgangspunkt für die Konzeption des Fragebogens für die deutschlandweite Unternehmensbefragung.[1]

Zwischen Februar und Mai 2018 wurden insgesamt sieben qualitative, leitfadengestützte Interviews mit Vertretern von staatlichen Behörden, vor allem der Strafverfolgung, durchgeführt. Die Auswahl der InterviewteilnehmerInnen erfolgte bewusst (*purposive sampling*; Schreier, 2010) nach den Kriterien Standort, arbeitsbezogene inhaltliche Schwerpunktsetzung sowie Art der Behörde und Position. Der Fokus der Behörden lag überwiegend auf Cyberkriminalität gegen Unternehmen und auf Internetkriminalität im Allgemeinen. Neben der Strafverfolgung lag der Arbeitsschwerpunkt der Experten zum Teil auch auf der Prävention und/oder der Aufklärung.

Übergeordnete Fragestellungen des eingesetzten Interviewleitfadens richteten sich einerseits auf die Risikofaktoren von Unternehmen in Hinblick auf Cyberangriffe und den Einsatz von IT-Sicherheitsmaßnahmen, um sich davor zu schützen. Andererseits standen die Erkenntnisse über die Zielrichtungen und Vorgehensweisen der TäterInnen sowie Möglichkeiten und Probleme von Prävention und Strafverfolgung im Fokus. Die Auswertung der Interviews orientierte sich an der qualitativen (zusammenfassenden) Inhaltsanalyse nach Mayring (2010). Hierbei wurden zunächst deduktiv – auf Basis des Interviewleitfadens – Kategorien gebildet. In einem

[1] Die Ergebnisse der Unternehmensbefragung finden sich bei Dreißigacker, Skarczinski und Wollinger (2020).

weiteren Schritt wurden die einzelnen Interviewsequenzen diesen Kategorien zugeordnet, anschließend paraphrasiert und generalisiert (induktive Bildung von Subkategorien). Im Folgenden werden die zentralen Ergebnisse dieser Auswertung, d.h. die inhaltlichen Kernaussagen der befragten Experten, thematische gegliedert und kurz zusammengefasst dargestellt. Anschließend wird auf offen gebliebene Fragen hingewiesen und Ansatzpunkte für die Optimierung der Strafverfolgung sowie für die Präventionsarbeit skizziert.

Risikofaktoren

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

TäterInnen

- Nach Einschätzung der Experten verlagern sich klassische Delikte wie Betrug und Erpressung zunehmend in den digitalen Raum.
- In Hinblick auf die TäterInnen wird ein breites Spektrum wahrgenommen, das von EinzeltäterInnen und gemeinschaftlich und arbeitsteilig vorgehenden TäterInnen ohne Beziehung zu den betroffenen Unternehmen über TäterInnen 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.

Abgeleitete Handlungsempfehlungen

- Die Bekanntheit der Zentralen Ansprechstellen Cybercrime (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 MitarbeiterInnen sowie die eigene Aus- und Weiterbildung innerhalb der Fachhochschulen für Polizei und öffentlichen Verwaltung diskutiert werden.

1 EINLEITUNG

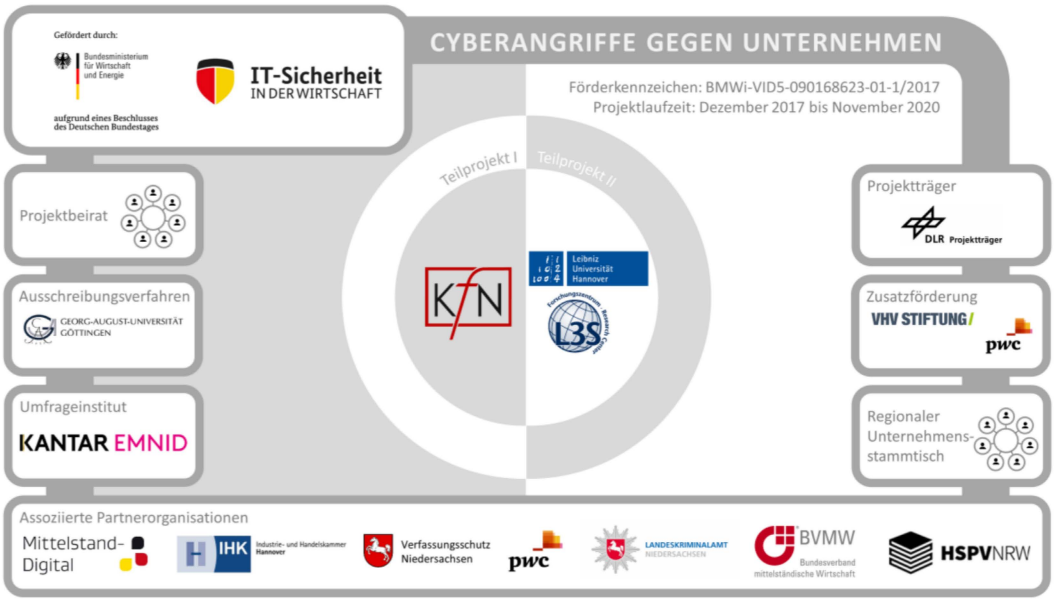
Mit der zunehmenden Digitalisierung der Gesellschaft spielt auch die Kriminalität im virtuellen Raum eine stetig wachsende Rolle. Nicht nur in der medialen Berichterstattung wurde dem Phänomen Cybercrime in den letzten Jahren steigende Aufmerksamkeit zuteil, auch Forscherinnen und Forscher sowie Behörden und Ämter befassen sich damit, was sich in zahlreichen Studien zu dem Thema (siehe u.a. Bitkom e.V., 2017; GDV, 2018; Hillebrand, Niederprüm, Schäfer, Thiele & Henseler-Ungar, 2017; KPMG, 2017) und der Einrichtung von speziellen Stellen bei Strafverfolgungsbehörden (z.B. CCCC, CuIKD, EC3, QRF, ZAC, ZCB, ZIT) sowie Kooperations- und Schutzeinrichtungen verschiedener Landes- und Bundesämter (z.B. CAZ, CERT-Bund, G4C, NCAZ, Zitis) widerspiegelt. Dabei werden nicht nur Privatpersonen Opfer von Cyberangriffen. Auch Unternehmen, deren Betriebsabläufe durch Angriffe auf die IT-Struktur zum Teil erheblich gestört werden können, stehen im Fokus. Die Polizeiliche Kriminalstatistik (PKS) verzeichnete im Jahr 2018 insgesamt 87.106 Fälle von Cyberangriffen im engeren Sinne[2] (BKA, 2019), wobei hier Privatpersonen und Unternehmen inkludiert sind. Der Schaden von Cyberangriffen gegen Unternehmen wird auf jährlich über 50 Milliarden Euro geschätzt (Bitkom e.V., 2017). Hillebrand et al. (2017) wiesen in diesem Zusammenhang darauf hin, dass es vor allem kleinen und mittlere Unternehmen (KMU) an adäquaten Schutzmaßnahmen fehlt. Der zunehmende Digitalisierungsgrad der Unternehmen sowie eine mangelnde Sensibilisierung gegenüber Cyberangriffen resultieren in einer immer größer werdenden Angriffsfläche, da in vielen KMU das Thema IT-Sicherheit nur eine untergeordnete Rolle spielt (Hillebrand et al., 2017). Es werden nicht immer essenzielle Schutzmaßnahmen ergriffen oder es sind noch veraltete Systeme im Einsatz (Hillebrand et al., 2017). Dabei sind reibungslos laufende IT-Systeme ein zentraler Bestandteil für viele Betriebsabläufe (GDV, 2019). Allerdings ist die Lage im Feld durch das rapide Aufkommen neuer Angriffsformen wie Ransomware oder CEO-Fraud sehr unübersichtlich (GDV, 2019); so müssen kontinuierlich neue Trends aufgearbeitet werden, auch von Strafverfolgungsbehörden.

Vor diesem Hintergrund hat sich das Kriminologische Forschungsinstitut Niedersachsen e.V. (KFN) zusammen mit dem Forschungszentrum L3S der Leibniz Universität Hannover dazu

2 Cybercrime im engeren Sinne umfasst laut der Definition des BKA „[…] die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten“ BKA (2017, S. 2).

entschlossen, eine breit angelegte Untersuchung durchzuführen, die differenziertes Wissen zum Thema Cyberangriffe liefern soll.

Abbildung 1 Projektbeteiligte



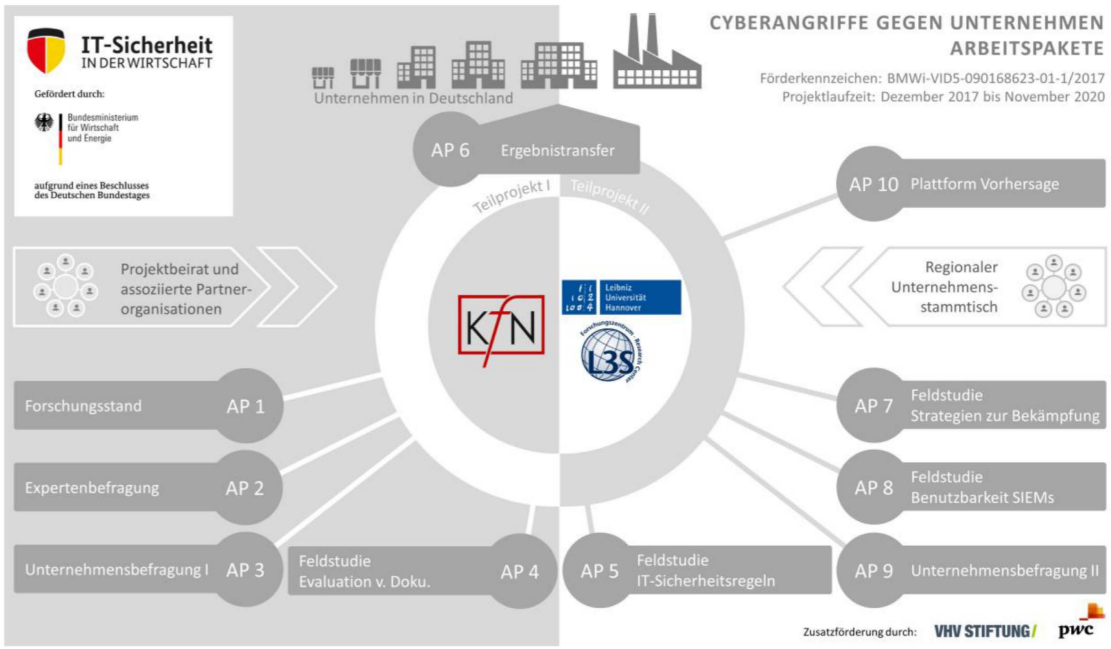
Das Projekt „Cyberangriffe gegen Unternehmen“ wird im Rahmen der Initiative IT-Sicherheit in der Wirtschaft des Bundesministeriums für Wirtschaft und Energie gefördert, erhält eine zusätzliche Förderung durch die VHV-Stiftung sowie von PricewaterhouseCoopers Wirtschaftsprüfungsgesellschaft mbH und wird durch einen beratenden Projektbeirat[3] unterstützt (Abbildung 1).[4] Es ist Modular aufgebaut und nutzt für die Beantwortung der jeweiligen Forschungsfragen unterschiedliche Erhebungsmethoden (Abbildung 2). Bisher wurden Interviews mit IT-Verantwortlichen in Unternehmen sowie mit Experten aus Bundes- und Landesbehörden (v.a. Strafverfolgungsbehörden) sowie der Versicherungswirtschaft durchgeführt, gefolgt von Feldstudien mit IT-Beschäftigten in Unternehmen zu den Themen „Evaluation von Dokumentation im Kontext kleiner und mittlerer Unternehmen“ und „IT-Sicherheitsregeln im Arbeitsalltag“

3 Darin sind neben den Förderern des Projektes der Bundesverband mittelständischer Wirtschaft, Mittelstand-Digital, die Industrie- und Handelskammer Hannover, das Landeskriminalamt Niedersachsen, 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-Sicherheits-Unternehmen CIPHRON vertreten.

4 Weitere Informationen zum Gesamtprojekt und allen Beteiligten finden sich unter https://cybercrime-forschung.de.

sowie einer Befragung von 5.000 Unternehmen in Deutschland mit besonderem Fokus auf kleinen und mittleren Unternehmen.[5] Die Laufzeit des Projektes ist auf drei Jahre von Dezember 2017 bis November 2020 angelegt.

Abbildung 2 Arbeitspakete



Die Grundlage für diesen Bericht stellen die Ergebnisse des Arbeitspakets 2 dar. Diese beruhen auf sieben qualitativen Interviews mit Vertretern von Bundes- und Landesbehörden (v.a. Strafverfolgungsbehörden) zum Thema Cyberangriffe gegen deutsche Unternehmen, die vom KFN durchgeführt wurden. Die Ergebnisse der qualitativen Experteninterviews gingen im Sinne eines sequenziellen Mixed-Method-Designs in die quantitative Unternehmensbefragung (AP 3) ein, insofern insbesondere Fragen zur Verbreitung von Cyberangriffen und deren Folgen sowie zu möglichen Risiko- und Schutzmaßnahmen aufgegriffen wurden.

Ergänzend zu den Erkenntnissen für die quantitative Unternehmensbefragung wurde zum anderen angestrebt, einen differenzierten Einblick hinsichtlich der Lage und der Entwicklungen von Cyberangriffen gegen Unternehmen aus der Perspektive von Strafverfolgungsbehörden zu erhalten und Schwierigkeiten bei der Ermittlungsarbeit in diesem Deliktsbereich herauszuarbeiten.

5 Die Ergebnisse der Unternehmensbefragung finden sich bei Dreißigacker et al. (2020).

2 FORSCHUNGSSTAND

Erkenntnisse zum Phänomen Cybercrime basieren einerseits auf polizeilich angezeigten oder zur Kenntnis gelangten Fällen, die in die Polizeiliche Kriminalstatistik (PKS) eingehen, dem sogenannten Hellfeld, und andererseits auf wissenschaftlichen Befragungen zu erlebten aber nicht immer angezeigten Vorfällen, dem sogenannten Dunkelfeld.

Polizeiliche Erkenntnisse zum Phänomen Cybercrime beziehen sich schwerpunktmäßig auf Hellfelddaten, die in der PKS jährlich veröffentlicht werden und die in das ebenfalls jährlich erscheinende Bundeslagebild Cybercrime des Bundeskriminalamts (BKA) eingehen. Gemäß der PKS für das Jahr 2018 hat die Polizei die Ermittlungen in 87.106 Fällen von Cybercrimedelikten im engeren Sinne (vorläufig) abgeschlossen und an die Staatsanwaltschaft übergeben (siehe Tabelle 1). Dies macht einen Anteil von 1,6 % bezogen auf alle Straftaten aus, die 2018 von der Polizei bearbeitet wurden. Bezogen auf Cybercrimedelikte konnte 2018 weiterhin in fast 40 % der Fälle eine tatverdächtigte Person ermittelt werden (BKA, 2019). Insgesamt ist 2017 ein finanzieller Schaden von 71,4 Millionen Euro entstanden (BKA, 2018), für 2018 liegen dazu bisher noch keine Zahlen vor.

Tabelle 1 Entwicklung von Cybercrime i.e.S. in der PKS[6]

	2014	2015	2016	2017	2018
Straftaten insgesamt	6.082.064	6.330.649	6.372.526	5.761.984	5.555.520
Cybercrime im engeren Sinne	49.925	45.793	82.649	85.960	87.106
Anteil an Straftaten insg.:	0,80%	0,70%	1,30%	1,50%	1,60%
Anteil der Fälle, in denen eine Tatverdächtige Person ermittelt werden konnte	29,40%	32,80%	38,70%	40,30%	38,90%
Finanzieller Schaden	35,9 Mio.	40,5 Mio.	50,9 Mio.	71,4 Mio.	-

Damit stieg der Anteil von als „Cybercrime im engeren Sinne“ erfassten Straftaten in der PKS von 2014 auf 2018 um 57 %. Dies lässt sich jedoch vor allem auf eine Veränderung der Erfassungsmodalitäten in der PKS zurückführen, indem verschiedene Betrugsdelikte, die zuvor nicht

6 BKA (2015), (2016), (2017), (2018), (2019).

Cybercrime zugeordnet wurden, seit Januar 2016 dazu gezählt werden:[7] Während im Jahr 2015 45.793 Straftaten als Cybercrime im engeren Sinn deklariert wurden, waren es im Jahr 2016 82.649 Taten. Doch auch in den Folgejahren lassen sich sowohl von 2016 auf 2017 (+4,0 %) als auch von 2017 auf 2018 (+1,3 %) steigende Tendenzen erkennen.

Insgesamt sind bei der Interpretation der Daten gemäß der PKS jedoch einige Einschränkungen bezüglich der Aussagekraft zu beachten. So werden in der Statistik nur Fälle erfasst, die angezeigt oder der Polizei selbst zur Kenntnis gelangt sind. Das Anzeigeverhalten ist im Bereich Cybercrime allerdings sehr zurückhaltend, wie verschiedene Dunkelfeldstudien zeigen (siehe u.a. Bitkom e.V., 2017; Bollhöfer & Jäger, 2018). Problematisch ist in diesem Deliktsbereich zusätzlich, dass nicht alle Opfer bemerken, dass sie von Cyberangriffen (z.B. von Spyware-Angriffen) betroffen sind.[8] Insofern kann davon ausgegangen werden, dass das Hellfeld nur einen relativ kleinen Teil der tatsächlichen Taten darstellt. Darüber hinaus obliegt die Schadenshöhe der Selbsteinschätzung der Betroffenen bei der Anzeigeerstattung, teilweise bleiben Angaben zum Schaden komplett aus. In diesem Fall wird ein „symbolischer Schaden von einem Euro“ (BKA, 2018, S. 30) berechnet. Ferner erlaubt die PKS bzw. das Bundeslagebild Cybercrime keine Differenzierung nach Merkmalen der Opfer (Unternehmen / Privatnutzer). Es bleibt demnach unklar, wie viele Unternehmen betroffen waren und um was für Unternehmen es sich dabei handelte. Insbesondere der letzte Aspekt wird jedoch in Dunkelfelduntersuchungen adressiert.

2.1 Prävalenzen

Das Bundesinstitut für Sicherheit in der Informationstechnik (BSI) führte in den Jahren 2018 und 2019 sogenannte Cyber-Sicherheits-Umfragen durch. Die Zielgruppe der Befragungen waren Behörden und Unternehmen, wobei der Betrachtungszeitraum die Jahre 2016, 2017 und 2018 umfasst. Die Befragung aus dem Jahr 2019 bezog sich dabei auf Ereignisse aus dem Jahr 2018. Neben etwa 500 größeren (ab 500 Beschäftigten) konnten 2018 und 2019 jeweils etwa 500 kleinere Organisationen (unter 250 Beschäftigte) erreicht werden. Einschränkend ist jedoch zu sagen, dass sich 14 % (2018) bzw. 11 % (2019) der befragten Organisationen selbst dem

7 Neun Delikte zählen insgesamt darunter: Sonstiger Computerbetrug, Vorbereitungshandlungen, betrügerisches Erlangen von Kfz, weitere Arten des Kreditbetruges, Betrug mittels rechtswidrig erlangter Daten von Zahlungskarten, Betrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel, Leistungskreditbetrug, Abrechnungsbetrug im Gesundheitswesen, Überweisungsbetrug - vgl. BKA (2017).

8 Straftaten, die nicht angezeigt und auch nicht in Dunkelfeldbefragungen genannt werden, z.B., weil sie vom Opfer selbst nicht bemerkt wurden, werden als doppeltes oder absolutes Dunkelfeld bezeichnet.

öffentlichen Dienst zuordnen. 70 % aller Befragten gaben an, 2016 oder 2017 Opfer eines Cyberangriffs gewesen zu sein. Für das Jahr 2018 lag dieser Anteil bei 33 %, wobei größere Unternehmen eher Angriffe verzeichneten (43 %). Dabei war die Hälfte der entdeckten Angriffe erfolgreich, sodass sich z.B. Täter und Täterinnen Zutritt zu internen IT-Systemen verschaffen konnten (BSI, 2018, 2019). Hierbei handelt es sich jedoch um keine repräsentative Befragung, deren Ergebnisse verallgemeinert werden können, da die Befragung auf einer willkürlichen Stichprobe basiert, bei der die Auswahl der teilnehmenden Organisationen im Ermessen der durchführenden Organisation oder der Unternehmen selbst (Selbstrekrutierung) lag. Zusätzlich schränken auch die kaum kontrollierbare Möglichkeit der Mehrfachteilnahme sowie der Anteil an Organisationen aus dem öffentlichen Dienst die Aussagekraft der Ergebnisse zur Betroffenheit von KMU ein.

In einer deutschlandweit repräsentativen Studie vom Bitkom e.V. (2017), die sich mit den Risiken der Digitalisierung im Wirtschaftsschutz befasste, wurden Führungskräfte aus 1.069 Unternehmen ab zehn Beschäftigten befragt. Die Repräsentativität der Ergebnisse wurde durch eine disproportional geschichtete Zufallsstichprobe und einer Gewichtung nach Branchen und Unternehmensgrößen gewährleistet. 53 % der befragten Unternehmen gaben an, dass ihr Unternehmen in den Jahren 2015 oder 2016 von Datendiebstahl, Industriespionage oder Sabotage betroffen waren, wobei weitere 26 % eine Betroffenheit vermuteten. Größere Unternehmen waren dabei häufiger betroffen als kleinere Unternehmen (60 % bei über 500 Mitarbeitern vs. 52 % bei 10-99 Mitarbeitern; vgl. Bitkom e.V., 2017).

Eine im Rahmen des Projekts Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa (WISKOS) durchgeführte repräsentative Dunkelfeldstudie der Max-Planck-Gesellschaft untersuchte ebenfalls Aspekte von Cyberkriminalität in KMU (Bollhöfer & Jäger, 2018). Dabei bildeten 583 Unternehmen zwischen einem und 249 Beschäftigten aus einer systematischen Zufallsauswahl der Hoppenstedt-Firmendatenbank die Datengrundlage. Geschäftsführerinnen und Geschäftsführer bzw. Leitungsfunktionen der Informationstechnik wurden dazu postalisch oder online befragt. 44 % dieser Unternehmen gaben an, in den letzten fünf Jahren von einem „Illegalen Abfluss von Wissen, Informationen und/oder Daten“ betroffen gewesen zu sein oder zumindest konkrete Verdachtsfälle diesbezüglich zu haben (Bollhöfer & Jäger, 2018, S. 31).

Zwei Forsa-Umfragen im Auftrag des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) wendeten sich an jeweils 300 „Entscheider“ deutscher KMU[9] (GDV, 2018, S. 3, 2019, S. 2). Zum Auswahlverfahren bzw. der Stichprobenziehung sowie der Erhebungsmethode werden keine Angaben gemacht. Sowohl 2018 als auch 2019 gaben etwa ein Drittel der befragten Unternehmen an, jemals von Cyberangriffen betroffen gewesen zu sein. Dabei traten etwa 75 % dieser Angriffe in den letzten zwei Jahren vor dem Befragungszeitpunkt (Frühjahr 18/19) auf (GDV, 2018, 2019).

Weiterhin führte das Umfrageinstitut Kantar Emnid 2017 im Auftrag der Wirtschaftsprüfungsgesellschaft KPMG computergestützte telefonische Interviews (CATI) mit 504 Unternehmen durch. Befragt wurden dabei vor allem Leiterinnen und Leiter „der Internen Revision, […] des Rechnungswesens, […] der Rechtsabteilung sowie Geschäftsführer und Vorstände" (KPMG, 2017, S. 54). Angaben zu Unternehmensgrößen werden in der Studie nicht gemacht. 38 % der befragten Unternehmen gaben an, zwischen 2015 und 2017 von Angriffen betroffen gewesen zu sein (KPMG, 2017).

In einer weiteren repräsentativen Untersuchung vom Wissenschaftlichen Institut für Infrastruktur und Kommunikationsdienste (wik) gaben 80 % der befragten Chief Executive Officer (CEO) bzw. Chief Information Security Officer (CISO) von 1.508 kleinen und mittleren Unternehmen (1-499 Beschäftigte) an, 2017 Erfahrungen mit IT-Sicherheitsproblemen gemacht zu haben (vgl. Hillebrand et al., 2017). Die Repräsentativität der Umfrage wurde durch eine disproportional geschichtete Stichprobe gewährleistet, gewichtet wurde nach der Unternehmensgröße (vgl. Hillebrand et al., 2017). Etwa 50 % der kleineren Unternehmen (bis 49 Beschäftigte) gaben an, bereits Cyberangriffe „festgestellt zu haben“. Bei den größten Unternehmen (bis 10.000 Beschäftigte) lag dieser Anteil bei 90 % (Hillebrand et al., 2017, S. 27).

Es zeigt sich, dass Dunkelfeldstudien bezüglich der Angriffsprävalenzen untereinander schwer zu vergleichen sind. Gründe dafür sind, dass ihnen unterschiedliche Zielgruppen, Erhebungsmethoden, Operationalisierungen und Definitionen von „Cyberangriffen“ zugrunde liegen. Schon die Anzahl der Beschäftigten, die für den Begriff „kleines oder mittelständisches Unternehmen“ stehen, unterscheiden sich. Darüber hinaus sind nur wenige der vorgestellten Studien als deutschlandweit repräsentativ für die Grundgesamtheit der Unternehmen bzw. für KMU in Deutschland zu bewerten.

9 In den forsa-Umfragen wird keine Definition des Begriffs „Kleines oder Mittelständisches Unternehmen“ vorgenommen.

2.2 Angriffsarten und Schaden

Bezüglich spezieller Angriffsarten auf kleine und mittlere Unternehmen zeigen vorliegende Studien kein eindeutiges Bild. So stellen die BSI-Studien heraus, dass Angriffe auf Unternehmen und Behörden am häufigsten über Malware-Angriffe (57 % bzw. 53 %) durchgeführt werden, wobei Denial of Service (DDoS)-Attacken als zweithäufigste Angriffsmethode (18 %) genannt werden (BSI, 2018, 2019). Dies wird durch die wik-Studie bestätigt, bei der über 50 % der Befragten von Malware-Angriffen und etwa 25 % von DDoS-Angriffen berichteten (Hillebrand et al., 2017). In der Bitkom-Studie wurden neben 38% digitaler Vorfälle (digitales Social Engineering, digitale Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen, Ausspähen von digitaler Kommunikation) 62% analoge Vorfälle berichtet (v.a. Diebstahl, analoges Social Engineering, Sabotagen; Bitkom e.V., 2017, S. 3).
Der Abfluss von sensiblen Daten wird zumeist über das Öffnen von böswilligen Emails erreicht (vgl. Bollhöfer & Jäger, 2018; GDV, 2018, 2019). Laut der KPMG-Studie haben außerdem „Systembeschädigungen und Computersabotage“ (KPMG, 2017, S. 15) stark zugenommen: Während in den Befragungswellen 2013 und 2015 jeweils 13 % der Befragten diese Angriffsart als Einfallstor angaben, verdreifachte sich dieser Wert 2017 fast (36 %). Darüber hinaus gab etwa ein Drittel der Befragten an, dass im Befragungszeitraum Daten ausgespäht oder abgefangen wurden, etwa 25 % der Unternehmen wurden von Ransomware angegriffen. Außerdem gaben etwa zwei Drittel der von Angriffen betroffenen Unternehmen an, dass unzureichend geschulte Mitarbeiter und Mitarbeiterinnen ein zentraler Risikofaktor für Cyberangriffe seien. Das verstärkte Auftreten neuartiger Angriffe (z.B. Ransomware, CEO-Fraud) fordert den Beschäftigen ein erhöhtes Maß an Sensibilität für das Thema IT-Sicherheit ab. Häufig wird hier von Angreifenden die „Schwachstelle Mensch“ ausgenutzt, um Zugriff zu IT-Systemen oder vertraulichen Daten zu erhalten (vgl. KPMG, 2017).

Auch der in Studien angegebene finanzielle Gesamtschaden für ein Unternehmen aufgrund eines Cyberangriffs variiert stark. So werden zum einen nationale Gesamtschäden von etwa 55 Mrd. EUR pro Jahr angegeben (Bitkom e.V., (2017). Zum anderen werden Schadenssummen zwischen 15.000 EUR und 120.000 EUR pro Angriff genannt, wobei größere Unternehmen Schadensfälle von bis zu einer Millionen Euro pro Angriff feststellten (vgl. KPMG, 2017). Da monetäre Schäden durch Cyberangriffe aufgrund verschiedener Faktoren (direkt abgeflossene Schadenssummen sowie Folgekosten; Forensik, Ermittlung, Systemwiederherstellung etc.) schwer zu beziffern sind, wird in einigen Studien anstelle des finanziellen Schadens die Dauer von Betriebsausfällen erfragt (Bollhöfer & Jäger, 2018; BSI, 2019; GDV, 2018; Hillebrand et

al., 2017). Hierbei lassen sich ebenfalls größere Diskrepanzen feststellen, was nicht zuletzt an der unterschiedlichen Operationalisierung des Begriffs „Betriebsausfall“ liegt. So zeigen sich zum einen Einschränkungen im Betriebsablauf zwischen zwei Tagen und einer Woche (18 %) beziehungsweise keine schwerwiegenden Folgen oder lediglich kurzfristige Ausfälle (Bollhöfer & Jäger, 2018). Die wik-Studie hingegen berichtet von Betriebs- und Produktionsausfällen in etwa 30 % der betroffenen Unternehmen sowie gestörten Geschäftsprozessen zwischen vier Stunden und mehr als einer Woche bei der Hälfte der Betroffenen (Hillebrand et al., 2017, S. 47). Der GDV (2018) wiederum stellte fest, dass 40 % der Angriffe die KMU so schwer trafen, dass der Betrieb daraufhin (teilweise) eingestellt werden musste. Die schwerwiegendsten Folgen von Cyberangriffen wurden vom (vgl. BSI, 2019) berichtet: 87 % der befragten Organisationen stellten Betriebsausfälle oder -Störungen sowie monetäre Kosten (65 %) und Reputationsschäden (22 %) fest.

2.3 Anzeigeverhalten und Prävention

Auch wenn hohe Schadenssummen berichtet werden, wenden sich dennoch nur etwa 30 % der betroffenen Unternehmen an staatliche Stellen wie Polizei, Staatsanwaltschaft oder Verfassungsschutz (Bollhöfer und Jäger, 2018; Bitkom e.V., 2017). Interne Maßnahmen oder die Zuhilfenahme externer Beratungsangebote überwiegen mit 47 % (Bollhöfer & Jäger, 2018) bzw. 80 % (Bitkom e.V., 2017). Begründet wird dies mit der Angst vor Imageschäden oder sonstigen negativen Konsequenzen (Bitkom e.V., 2017). Weiterhin zeigen verschiedene Untersuchungen, dass unterschiedliche Maßnahmen zum Schutz vor Cyberangriffen implementiert werden. So berichtet das BSI (2019), dass etwa 42 % der Befragten Zwei-Faktor-Authentifizierungen einsetzen, wobei hier nur ein marginaler Unterschied zwischen kleineren (bis 499 Beschäftigte) und größeren Unternehmen besteht. Ein zentrales Management für die Sicherheit mobiler Endgeräte bzw. die Nutzung von IT-Security-Policies werden dagegen eher in größeren als in kleineren Unternehmen eingesetzt (72 % vs. 39 % bzw. 75 % vs. 51 %; vgl. BSI, 2019). Weitere Untersuchungen machen deutlich, dass in KMU zumeist zwar Firewalls und Antivirensoftware eingesetzt werden (ca. 85%, vgl. Hillebrand et al., 2017), das Anlegen regelmäßiger (verschlüsselter) Backups (68%; GDV, 2019) oder die Nutzung von VPN-Software hingegen seltener erfolgen (29% der kleineren Unternehmen; Hillebrand et al., 2017).

Zwar ist mit der zunehmenden Verbreitung digitaler Medien auch die Sensibilisierung kleiner und mittlerer Unternehmen in Deutschland bezüglich der Cybercrimerisiken in den letzten Jahren gewachsen (Hillebrand et al., 2017), dennoch werden in verschiedenen Untersuchungen

Verbesserungspotentiale bei der IT-Sicherheit von Unternehmen deutlich. So werden beispielsweise Intrusion-Detection-Systeme oder Penetrationstests, mit denen der Sicherheitsgrad in Unternehmen erheblich gesteigert werden kann, von weniger als 20 % der Unternehmen eingesetzt (vgl. Bitkom e.V., 2017). Hillebrand et al. (2017) konnten zudem zeigen, dass das Thema IT-Sicherheit im Unternehmen bei etwa einem Drittel der Befragten keine hohe Bedeutung hat. Auch führten nur 20 % der kleinen und 48 % der großen KMU jemals systematische IT-Sicherheitsanalysen durch (Hillebrand et al., 2017). Zudem wird eine Diskrepanz zwischen dem Bewusstsein der Notwendigkeit und der Durchführung von Sensibilisierungsmaßnahmen deutlich: Weitaus mehr Unternehmen halten beispielsweise regelmäßige Mitarbeiterschulungen für sinnvoll, als dass sie tatsächlich durchgeführt werden (Hillebrand et al., 2017). In diesem Zusammenhang haben Untersuchungen gezeigt, dass nur etwa die Hälfte aller von ihnen befragten Unternehmen Mitarbeiterschulungen bezüglich IT-Sicherheit durchführten (Bitkom e.V., 2017; Bollhöfer & Jäger, 2018). Auf der Basis von Experteninterviews (u.a. mit Vertretern aus Anbieterunternehmen, Verbänden, Handwerkskammern) schlussfolgern Hillebrand et al. (2017) diesbezüglich, dass vor allem eine fehlende Awareness unter Beschäftigten sowie die unzureichende Bekanntheit von Informationsangeboten bzgl. IT-Sicherheitsmaßnahmen maßgebliche Risiken für die IT-Sicherheit in Unternehmen darstellen.

3 ZIEL DER INTERVIEWSTUDIE

Das existierende, vermutlich sehr große (doppelte) Dunkelfeld sowie die Herangehensweisen der vereinzelten zumeist quantitativen Untersuchungen erschweren es, das Phänomen Cyberangriffe gegen Unternehmen zu verstehen. Auch ist die Sicht von Strafverfolgungsbehörden auf Cyberangriffe gegen Unternehmen bisher kaum Gegenstand der Forschung in Deutschland gewesen, weder quantitativ noch qualitativ. Dabei sind gerade die speziellen Einheiten der Bundes- und Landesbehörden die Akteure, die täglich mit Cyberangriffen zu tun haben. Sie tragen mit IT-Sicherheitsexpertinnen und -experten dazu bei, Angriffe aufzuklären und die Prävalenzen einzudämmen. Sie haben empirisch wertvolle Erfahrungswerte, zum Beispiel hinsichtlich der Täterinnen und Täter sowie Opfer, Risiko- und Schutzmaßnahmen sowie wirksamer Präventionsansätze. Darüber hinaus ermöglicht ihre Arbeit einen Einblick in interne Strukturen von Unternehmen, die in Unternehmensbefragungen gegebenenfalls unentdeckt bleiben würden.

Diese Erfahrungswerte werden in der vorliegenden Interviewstudie des KFN genutzt; zum einen als Grundlage für die Entwicklung einer deutschlandweiten quantitativen Befragung von Unternehmen zu ihren Erfahrungen mit Cybercrime. Ergänzend zu den Erkenntnissen für die quantitative Unternehmensbefragung wurde zum anderen angestrebt, einen differenzierten Einblick hinsichtlich der Lage und der Entwicklungen von Cybercrime gegen Unternehmen aus der Perspektive von Strafverfolgungsbehörden zu erhalten. Fokussiert wurde dabei die Einschätzung der Lage aus Sicht der Strafverfolgungsbehörden hinsichtlich allgemeiner Trends und Entwicklungen sowie hinsichtlich Täterinnen und Täter. Die Sicht der Experten auf allgemeine Trends und Entwicklungen im Bereich „Cyberangriffe auf Unternehmen“ kann darüber hinaus dazu beitragen, Unklarheiten und Unterschiede der quantitativen Studien zu erklären und zu ergänzen. Der Fokus auf die Täterinnen und Täter wurde gelegt, da in Unternehmensbefragungen oft nur Vermutungen zur Täterschaft erhoben werden können. In Strafverfolgungsbehörden existieren möglicherweise differenziertere Erkenntnisse darüber, welche Tätermerkmale entscheidend sind und wie sich Tätergruppen organisieren. Die systematische Aufarbeitung dieser Erkenntnisse kann dazu beitragen, die Strafverfolgung zu unterstützen. Ein weiterer Schwerpunkt war die Expertise der Befragten bezüglich Risiko- und Schutzmaßnahmen. Diese kann einerseits Auskunft darüber geben, wie die Aufstellung deutscher Unternehmen bezüglich IT-Sicherheit aus behördlicher Sicht eingeschätzt wird und andererseits einen

Einblick in weitere technische Risikofaktoren gewähren, die es Angreifern und Angreiferinnen ermöglichen, Zugriff zu internen IT-Strukturen zu erlangen. In diesem Zusammenhang war es zudem von Interesse, mit welchen Stärken und Herausforderungen sich die Behörden derzeit bei der Strafverfolgung konfrontiert sehen und welche Verbesserungsmöglichkeiten bestehen. Auch wurde fokussiert, welche kriminalpräventiven Aspekte aus behördlicher Sicht gewinnbringend erscheinen. In vorangegangenen Darstellungen wurde weiterhin deutlich, dass Betroffene Fälle von Cybercrime eher selten anzeigen (Bitkom e.V., 2017; Bollhöfer & Jäger, 2018). Die Repräsentativbefragung vom Bitkom e.V. (2017) zeigt, dass vor allem die Angst vor Imageproblemen der Grund dafür ist. Doch die Sicht der Strafverfolger, warum sich mehr als zwei Drittel aller Unternehmen nicht dafür entscheiden sie zu kontaktieren, wurde bisher nicht erforscht. Das gleiche gilt für die Möglichkeiten und Herausforderungen der Strafverfolgung von Cybercrimedelikten. Auch die Einschätzung verschiedener Cyber-Kriminalpräventionsmaßnahmen aus Sicht deutscher Strafverfolger und Strafverfolgerinnen wird in diesem Forschungsbericht aufgearbeitet.

Übergeordnet können diese Erkenntnisse Aufschluss darüber geben, welche Möglichkeiten und Herausforderungen derzeit in Hinblick auf Cyberangriffe gegen deutsche Unternehmen existieren. Daraus können wiederum Handlungsempfehlungen für politische Akteure aber auch Behörden und Unternehmen abgeleitet werden.

4 METHODE

Im Folgenden wird sich insgesamt mit dem methodischen Vorgehen beschäftigt. Dafür wird zum einen näher auf die Rekrutierung der Interviewteilnehmer eingegangen. Zum anderen wird die Auswertungsmethode erläutert, wobei dies systematisch entlang übergeordneter ausgewählter Kategorien erfolgt.

4.1 Erhebung

Zwischen Februar und Mai 2018 wurden insgesamt sieben qualitative, leitfadengestützte Interviews mit Vertretern von staatlichen Behörden, vor allem der Strafverfolgung, durchgeführt. Der Interviewleitfaden ist dem Anhang A zu entnehmen. Bei den Interviews handelte es sich um Experten- bzw. Expertinneninterviews, die einem explorativen Zweck dienten und „zur Strukturierung und Präzisierung des Forschungsfeldes und des weiteren Forschungsprozesses [sowie] zur Hypothesengenerierung“ beitragen sollten (Wassermann, 2015, S. 53). Als ExpertInnen wurden Personen verstanden, „die sich – ausgehend von einem spezifischen Praxis- oder Erfahrungswissen, das sich auf einen klar begrenzbaren Problemkreis bezieht – die Möglichkeit geschaffen haben, mit ihren Deutungen das konkrete Handlungsfeld sinnhaft und handlungsleitend für Andere zu strukturieren.“ (Bogner, Littig & Menz, 2014, S. 13). Die Besonderheit dieses ExpertInnenwissens liegt demnach neben einer vergleichsweise hohen „Reflexivität, Kohärenz oder Gewissheit […] insbesondere darin, dass dieses Wissen in besonderer Weise praxiswirksam und damit orientierungs- und handlungsleitend für andere Akteure wird“ (ebd., S. 14). Im Zusammenhang mit Cybercrime gegen Unternehmen kamen daher Personen als ExpertInnen in Betracht, die über ein entsprechendes Spezialwissen und Erfahrungen in diesem Bereich verfügen.

So erfolgte die Auswahl der InterviewteilnehmerInnen bewusst (zum *purposive sampling* siehe Schreier, 2010) nach den Kriterien Standort, arbeitsbezogene inhaltliche Schwerpunktsetzung sowie Art der Behörde und Position. Es wurde darauf geachtet, ein möglichst breites Spektrum von ExpertInnen in diesem Feld auszuwählen und sie durch gezielte persönliche Telefonate für die Interviewstudie zu gewinnen. Alle ausgewählten Akteure stimmten einem Interview zu.

Übergeordnete Fragestellungen der leitfadengestützten Interviews waren neben beruflichem Hintergrund der Interviewperson und einigen allgemeinen Angaben zur Behörde einerseits Zielrichtung und Vorgehensweise der Cyberkriminalität sowie die IT-Sicherheitsstrukturen der Unternehmen, die es den Angreifern erleichtern oder erschweren, den angestrebten Erfolg zu erreichen. Andererseits standen Möglichkeiten und Strategien von Prävention und Strafverfolgung im Fokus. Die Interviews wurden mittels Tonband aufgezeichnet und anschließend vollständig mit dem Transkriptionsprogramm „f4“ verschriftlicht. Die Interviews dauerten im Durchschnitt 88 Minuten und reichten von 52 bis 133 Minuten. Zwei der sieben Interviews wurden mit jeweils zwei Interviewteilnehmern geführt, die anderen fünf Interviews mit jeweils einer Person.

4.2 Auswertung

Bei der Auswertung der Interviews wurde sich an der qualitativen (zusammenfassenden) Inhaltsanalyse nach Mayring orientiert; eine Methode, die es ermöglicht, qualitative Daten systematisch zu analysieren (Mayring, 2010). Hierbei wurden zunächst deduktiv auf Basis des Interviewleitfadens Kategorien gebildet. Anhand eines Kodierschemas erfolgte die Kategorisierung dann durch zwei unabhängige BeurteilerInnen mit MAXQDA (Version 2018). Jedes Interview wurde dabei separat analysiert, wobei ein einzelnes Interview-Segment mindestens einen Satz bis maximal einen Absatz umfassen musste, um einer Kategorie zugeordnet werden zu können. Weiterhin war es möglich, dass einige Interviewaussagen in unterschiedliche Kategorien passten. Im Anschluss an den ersten Kategorisierungs-Prozess wurde Cohen’s Kappa mit MAXQDA berechnet, um die Übereinstimmung zwischen den beiden BeurteilerInnen zu bestimmen (Interrater-Übereinstimmung). Gemäß Viera und Garrett (2005) gelten κ-Werte von .01 bis .02 als etwas übereinstimmend, κ-Werte von .21 bis .4 als ausreichend übereinstimmend, κ-Werte von .41 bis .6 als moderat übereinstimmend, κ-Werte von .61 bis .8 als beachtlich übereinstimmend sowie κ-Werte von .81 bis .99 als nahezu perfekt übereinstimmend.

In einem weiteren Schritt wurden die einzelnen Interviewsequenzen im Rahmen der qualitativen Inhaltsanalyse paraphrasiert und generalisiert. Dabei wurden von einer Beurteilerin induktiv Subcodes generiert, wodurch ähnliche Aussagen zusammengefasst werden konnten. Diese Subcodes wurden von einem zweiten unabhängigen Beurteiler zusammen mit einem Kodierschema als Grundlage genutzt, um jede einzelne Interview-Sequenz zuordnen zu können. Im Anschluss an diesen zweiten Prozess wurde Cohen’s Kappa mit SPSS (Version 19) berechnet, um die Übereinstimmung zwischen den beiden BeurteilerInnen zu bestimmen.

Für die folgende Darstellung wurde sich auf eine Auswahl der im Interviewleitfaden enthaltenen Kategorien beschränkt. Dabei wurden sich für solche Kategorien entschieden, die, wie vorangegangen aufgezeigt, aktuelle Forschungslücken schließen (siehe Anhang 2 – Codesystem).

4.2.1 Trends/Entwicklungen und Täter/Täterinnen (allgemein)

Tabelle 2 zeigt das Kodierschema für die Kategorien „Trends und Entwicklungen“ sowie „Täter/Täterinnen“. Die Interrater-Übereinstimmung kann als ausreichend (κ = .299) bzw. moderat (κ = .409) übereinstimmend bewertet werden. Jede nicht übereinstimmende Aussage wurde im Anschluss an die Überprüfung der Übereinstimmung diskutiert bis eine Einigung erzielt wurde.

Tabelle 2 Kodierschema (Kategorien Trends/Entwicklungen und Täter/Täterinnen)

Kategorie	Beschreibung
Trends/Entwicklungen	allgemeine Aussagen (unspezifisch, z.B. nicht bezogen auf Angriffsart), Bewertung/Einschätzung, Bewertung der PKS, andere Studien, Versicherung
Täter bzw. Täterinnen	Bezeichnung, Beschreibung (Charakteristika), Besonderheiten

Tabelle 3 zeigt das Kodierschema für die generierten Subcodes. Die Interrater-Übereinstimmung war hier moderat (Trends/Entwicklungen = κ = .507) bzw. substanziell (Täter/Täterinnen = κ = .657). Jede nicht übereinstimmende Aussage wurde im Anschluss an die Überprüfung der Übereinstimmung diskutiert bis eine Einigung erzielt wurde.

Tabelle 3 Kodierschema (Subcodes zu Trends/Entwicklungen und Täter/Täterinnen)

Code	Beschreibung
Trends/Entwicklungen	
Täter/Täterinnen	Allgemeines zum Vorgehen der TäterInnen, zu den Zielen der TäterInnen, zu der Zusammensetzung TäterInnentyp; wenn es nicht einem passenden Subcode zugeordnet werden kann (keine Aussage über Trend/ Fläche/ Verlagerung)
Täter/Täterinnen_Angriffstrends	Art des Angriffes, Vorgehen, Cyber-Phänomen, Strategien seitens der AngreiferInnen, Anpassungsprozesse an technische Gegebenheiten, Potentiale, Zukunftsszenarien über Angriffe
Täter/Täterinnen_Angriffsfläche	Dimension/ Ausmaß/ potenzielle Zugänge im Allgemeinen gesteigert, Wachstum eines potenziellen TäterInnenkreises oder potenzieller Angriffsziele - z.B. durch Digitalisierung/ technische Innovationen/ Zugang/ Vernetzung, Potenziale hinsichtlich der Angriffsausmaße, generelles Wachstum von Cybercrime
Täter/Täterinnen_Verlagerung	bereits bekannte Straftaten verlagern sich in die Online-Welt; keine neuen Phänomene, sondern bekannte Delikte finden einen neuen Kanal im Cybercrime
Betroffene	Allgemeines zur Aufstellung der Betroffenen; wenn es nicht einem passenden Subcode zugeordnet werden kann (keine Aussage, welchen Akteur es genau betrifft/ betrifft alle Akteure im gleichem Maße)

Code	Beschreibung
Betroffene_Angebot	Schutzmaßnahmen/ Angebote/ Vorgehen/ Entwicklungen/ Potenziale auf Seite der Anbieter (z.B. Versicherer, Behörden, Dienstleister, Externe)
Betroffene_Nachfrage	Schutzmaßnahmen/ Aufstellung/ Vorgehen/ Entwicklungen/ Stand/ Potenziale auf Seite der Betroffenen (Unternehmen)
(unzureichende) Datenerfassung	(fehlende oder nicht ausreichende) Datenerfassung zum Thema Cybercrime/ Cybersicherheit, (fehlende oder unzureichende) Datengrundlage zur Erfassung des Phänomens, Dunkelfeld, Möglichkeiten der Datenerfassung; das „Wie“ im Gegensatz zu dem Code „aktuelle Studien“
aktuelle Studien	Datengrundlage auf derer die Einschätzung der Behörden erfolgt, Darstellung des Feldes in Zahlen, Beurteilung der Datengrundlage aktueller Studien; konkrete Zahlen im Gegensatz zum Code „(unzureichende) Datenerfassung“
Täter/Täterinnen	
allgemein	allgemeine Aussagen zu TäterInnen oder zum Täter- bzw. Täterinnenfeld oder zu potenziellen Täter/Täterinnen, Aussagen über deren Professionalität, Zugänge; wenn nicht spezifisch auf bestimmten Täter- bzw. Täterinnentyp bezogen
Einzeltäter/-täterinnen	Täter bzw. Täterinnen agieren hauptsächlich allein (z.B. Script-Kiddies, Mitarbeiter) oder bieten ihre Fähigkeiten als Dienstleistungen an (geschäftliche Basis ohne Gruppenidentität/ gemeinsames Ziel
Gruppen	Täter bzw. Täterinnen agieren in Gruppen; ihr Vorgehen ist dabei gekennzeichnet von Organisation; zumeist zielt der Angriff dabei auf Ertrag ab; es sind mehrere Personen beteiligt; teilweise arbeitsteilig (Aufgabenteilung je nach Kompetenzfeld/ ergänzend); es wird impliziert, dass eine Gruppendynamik vorherrscht; hierzu gehört auch das Verhalten innerhalb der Gruppe (Kommunikation etc.)
staatlich	Angriffe gehen von Nachrichtendiensten oder Behörden aus; Staatliche Akteure, die angreifen oder Daten abgreifen/ ausspionieren
Wettbewerber	Angriffe gehen von Wettbewerbern (konkurrierenden Unternehmen) aus; zumeist wettbewerbsschädigend; Datenklau von Firmengeheimnissen; als Akteur wird nur allgemein das „Unternehmen“ oder der „Wettbewerber“ genannt
Strafverfolgung	Umgang der Behörden mit Täterschaft im Hinblick auf Strafverfolgung/ Unwissen der Behörden, wer genau Täter oder Täterin ist; Verhaltensweisen der Täter bzw. Täterinnen/ der Betroffenen/ der Behörden, die zu einer erfolgreichen/ erfolglosen Strafverfolgung führen können
Angriffsart	allgemeine Aussagen zu verschiedenen Angriffsarten/ Vorgehensweisen; wenn nicht spezifisch auf bestimmten Täter- bzw. Täterinnentyp bezogen
Soziodemografie	allgemeine Aussagen zu soziodemografischen Merkmalen der Täterin bzw. des Täters (Alter, Geschlecht, Herkunft) / Zusammensetzung von Täter bzw. Täterinnen; wenn nicht spezifisch auf bestimmten Täter- bzw. Täterinnentyp bezogen
Motive	allgemeine Aussagen zu Zielen/Motiven der Täterin bzw. des Täters (politisch, idealistisch, wirtschaftlich); wenn nicht spezifisch auf bestimmten Tätertyp bezogen

4.2.2 Risikofaktoren, Schutzmaßnahmen und Kontaktaufnahme mit Behörden (bezogen auf Unternehmen)

Tabelle 4 (S. 29) zeigt das Kodierschema für die Kategorien „Risikofaktoren“, „Schutzmaßnahmen“ sowie „Kontaktaufnahme mit Behörden“ bezogen auf Unternehmen. Die Interrater-

Übereinstimmung reichte von etwas (Schutzmaßnahmen = κ = .195) bis ausreichend übereinstimmend (Risikofaktoren = κ = .283, Kontaktaufnahme mit Behörden = κ = .310). Jede nicht übereinstimmende Aussage wurde im Anschluss an die Überprüfung der Übereinstimmung diskutiert bis eine Einigung erzielt wurde.

Tabelle 4 Kodierschema (Kategorien Risikofaktoren, Schutzmaßnahmen und Kontaktaufnahme mit Behörden)

Kategorie	Beschreibung
Risikofaktoren	konkrete Bezeichnung, intern (Unternehmen, Beschäftigte), extern, Charakteristika
Schutzmaßnahmen	Bezeichnung, Organisation/Struktur des Unternehmens
Kontaktaufnahme mit Behörden	Allgemeines zur Kontaktaufnahme, Verlauf des Erstkontaktes, keine Kontaktaufnahme, Intention, Bekanntheit von Behörden in Zusammenhang mit Kontaktaufnahme, mögliche Zeitpunkte, Konsequenzen (bei Anzeige), Beratungsinhalte, Hilfestellung

Tabelle 5 zeigt das Kodierschema für die generierten Subcodes. Die Interrater-Übereinstimmung war hier moderat (Risikofaktoren = κ = .421, Schutzmaßnahmen = κ = .598, Kontaktaufnahme = κ = .503). Jede nicht übereinstimmende Aussage wurde im Anschluss an die Überprüfung der Übereinstimmung diskutiert bis eine Einigung erzielt wurde.

Tabelle 5 Kodierschema (Subcodes zu Risikofaktoren, Schutzmaßnahmen und Kontaktaufnahme mit Behörden)

Code	Beschreibung
Risikofaktoren	
fehlende Sensibilisierung	Risikofaktoren, die durch fehlendes technisches Wissen auf Seiten der Unternehmen entstehen oder durch fehlende Sensibilisierung der Beschäftigten; unbewusstes Risiko und dadurch fehlende Ausstattung/ schlechte Aufstellung
Nachlässigkeit	Rückständigkeit, wie z.B. durch alte Systeme und fehlende Annahme von Innovationen/ neuer Software/ keine Inanspruchnahme professioneller Services; im Gegensatz zum Code „fehlende Sensibilisierung“ ist das Risiko bewusst, wird aber aus Kosten- oder Trägheitsgründen vernachlässigt
Digitalisierung	Risikofaktoren, die durch die voranschreitende Digitalisierung und der damit einhergehenden Vernetzung entstehen, direkte Zugänge in das Netzwerk, fehlende, aber auch zu hohe Komplexität, Anwendungsbezüge durch Digitalisierung (wie im Falle von Cyberwar)
(fehlende) Standards	Risikofaktoren, die durch (fehlende) Standards (Vorschriften, technische Ausstattung*) entstehen; Notfallmaßnahmen im Falle eines Angriffs/ Dokumentation über etwaige Schritte/ standardisierte Verfahren im Bereich Cybersicherheit
	*zur Abgrenzung zum Code „Sensibilisierung“ und „Nachlässigkeit“: kein Hinweis darauf, dass Risikobewusstsein vorhanden oder nicht vorhanden ist, genereller Umstand ohne kommunizierte Absicht seitens der Unternehmen

Code	Beschreibung
kleine Unternehmen	mangelnde Ausstattung/ mangelnde Ressourcen zur Aufrüstung als Umstand speziell in kleinen Unternehmen – daher vermehrt das Ziel von Angriffen
große Unternehmen	große Angriffsfläche/ viel Umsatz/ schlechte Aufstellung in der IT-Sicherheit als Umstand (speziell in größeren Unternehmen)
Unternehmensspezifische Merkmale	Unternehmensmerkmale oder -eigenschaften, die das Risiko eines Angriffs auf das Unternehmen erhöhen, wie z.B. innovative/ lukrative Firmengeheimnisse, Nutzung bestimmter Software oder Betriebssystemen;
	unabhängig von der Firmengröße
Schutzmaßnahmen	
Diskrepanz zwischen kleinen und großen Unternehmen	verschiedene Aufstellungen hinsichtlich der Sicherheitsstandards, die zumeist der Größe eines Unternehmens geschuldet sind; Differenzierung zwischen kleinen und großen Unternehmen/ alten und jungen Unternehmen
direkter Schutz	klassische Maßnahmen zur Verhinderung von Attacken/ Angriffen/ Eindringen, die noch vor dem eigentlichen Angriff greifen; Kontrollmaßnahmen zur Einsehbarkeit von Datentransfer und Nutzung; Maßnahmen, die nicht zum direkten Schutz vor Angriffen eingeleitet werden, aber dennoch Angriffe verhindern können oder schneller erkennen lassen
Resilienz	langfristige Maßnahmen, die die Resilienz eines Unternehmens im Falle eines Angriffs erhöhen; langfristige Maßnahmen, die während oder nach einem Angriff greifen
Rolle weiterer Akteure	Rolle staatlicher Akteure oder Versicherungen im Hinblick auf Schutz vor Cyberkriminalität, Wirkung auf Unternehmen durch Vorgaben/ Aufklärung etc.
Kontaktaufnahme mit Behörden	
Art der Kontaktaufnahme	Fälle, in denen die Unternehmen die Leistungen der Behörden in Anspruch nehmen; konkret: wie der Kontakt erfolgt/ welche Behörden kontaktiert werden, worüber der Kontakt erfolgt (Externe)
Bekanntheit	Ausbleiben von Kontaktaufnahme durch fehlende Bekanntheit; Aussagen über die generelle Bekanntheit (oder fehlende Bekanntheit) der Behörden
Vorbehalte	Vorbehalte und Verweigerung von Anzeigen der Angriffe seitens der Unternehmen aufgrund von Gerüchten/ Mythen/ Erfahrungen/ Vorbehalte gegenüber den Behörden. Typische Fälle/ Gründe
sich anschließende Leistungen	Aussagen zum Ermittlungserfolg/ Vorgehen/ Leistungsspektrum der Behörden. Umgang mit bestimmten Fallarten. Beratung/ Broschüren/ Vorträge/ Empfehlungen. Generelle Aussagen über die Zusammenarbeit mit den Unternehmen. Empfehlungen seitens der Behörden zum Verhalten der Unternehmen/ der Betroffenen

4.2.3 Strafverfolgung und Kriminalprävention (Perspektive Behörden)

Tabelle 6 (S. 31) zeigt das Kodierschema für die Kategorien „Strafverfolgung“ und „Kriminalprävention“ aus der Perspektive der Behörden. Die Interrater-Übereinstimmung kann als ausreichend übereinstimmend (Kriminalprävention = κ = .294, Strafverfolgung: Stärken = κ =

.237) bzw. als moderat (Strafverfolgung: Probleme/Herausforderungen = κ = .429, Strafverfolgung: Optimierungsvorschläge = κ = .443) bewertet werden. Jede nicht übereinstimmende Aussage wurde im Anschluss an die Überprüfung der Übereinstimmung diskutiert bis eine Einigung erzielt wurde.

Tabelle 6 Kodierschema (Kategorien Strafverfolgung und Kriminalprävention)

Kategorie	Beschreibung
Strafverfolgung: Stärken	Besonderheiten der Behörde, spezifische Ausbildungen/Lehrgänge, Kompetenzen der Behörde, Erfolge der Behörde (in der Ermittlungsarbeit und daneben), Alternativen der Strafverfolgung, Vor-/Nachteile der Behörde (z.B. Ausstattung)
Strafverfolgung: Probleme/Herausforderungen	Grenzen, Verunsicherung, (gesetzliche) Schwierigkeiten, Probleme bei der Anzeigenerstattung, innerhalb der Behörde (personell, materiell)
Strafverfolgung: Optimierungsvorschläge	innerhalb der Behörde (personell, materiell)
Kriminalprävention	Angebote der Behörde, Prioritäten, Zufriedenheit von Unternehmen, allgemeine Schutzmaßnahmen

Tabelle 7 zeigt das Kodierschema für die generierten Subcodes. Die Interrater-Übereinstimmung war hier moderat (Kriminalprävention = κ = .454, Stärken = κ = .529) bzw. substanziell (Probleme/Herausforderungen = κ = .647, Optimierungsvorschläge = κ = .716). Jede nicht übereinstimmende Aussage wurde im Anschluss an die Überprüfung der Übereinstimmung diskutiert bis eine Einigung erzielt wurde.

Tabelle 7 Kodierschema (Subcodes zu Strafverfolgung und Kriminalprävention)

Code	Beschreibung
Strafverfolgung: Stärken	
zentralisiert	Behörden werden als Kompetenzzentrum beschrieben; viele verschiedene Fähigkeiten/ Möglichkeiten/ Themen, die sich in der Beratungsstelle bündeln; Fokus liegt auf der Rolle als zentraler Ansprechpartner/ Single point of contact
Fokus auf Geschädigten	im Vergleich zur Polizei divergierendes Vorgehen; Umgang mit dem Geschädigten hinsichtlich der Strafverfolgung; Fokus auf den Interessen des Geschädigten hinsichtlich der Strafverfolgung
breite Aufstellung: allgemein	allgemeine Aufstellung, sofern es keinem weiteren Sub-Subcode zugeordnet werden kann
breite Aufstellung: Kooperationen	Kooperationen und Vernetzung mit anderen Akteuren (Ländern, Behörden, Unternehmen usw.)/ Zusammenarbeit
breite Aufstellung: Technik	Aussagen zur technischen Aufstellung der Behörden. Dabei steht das „Wie“ im Fokus

Code	Beschreibung
breite Aufstellung: personell	Aussagen zur personellen Aufstellung der Behörden. Aussagen über Qualität/ Expertise/ Fachwissen, Umfang, Zulauf der Beschäftigten
breite Aufstellung: Schwerpunkt	Sondereinheiten und Schwerpunktsetzung auf einzelne Teilbereiche sowie anlassunabhängige Recherchen/ Strafverfolgungen
Strafverfolgung: Probleme und Herausforderungen	
deliktimmanent	Problematiken und Schwierigkeiten, die sich aus dem Feld ergeben, wie z.B. Anonymität des Täters, Zeitmangel bei der Ermittlung, Angriffe aus dem Ausland, die generelle Felddynamik (Erneuerungen, Weiterentwicklung); Fokus auf Täterseite/ Deliktart (ergeben sich nicht aus dem Verhalten der Behörden)
Datenbasis	unzureichende Datenbasis zu Cyberangriffen, wie auch fehlende Anzeigen seitens der Unternehmen (unzureichendes Anzeigeverhalten), dadurch fehlende Einsicht in das Feld/ großes Dunkelfeld
Konkurrenzfähigkeit	Konkurrenzfähigkeit im Hinblick auf den Arbeitsmarkt; Akquise von Fachpersonal/ spezialisierten Fachkräften und Halten dieser Arbeitskräfte durch Anreize, wie Geld oder Verbeamtung; expliziter Vergleich zur Privatwirtschaft im Hinblick auf Fachpersonal (Im Vergleich zur Kategorie „Ressourcen“ steht das Expertenwissen/ Qualität/ Ausbildung der Beschäftigten im Fokus)
Ermittlungsmethoden	unzureichendes „Werkzeug“ zur Ermittlung der Täter; fehlende Passung der Methoden zur erfolgreichen Ermittlung/ beschränkte Möglichkeiten zur Strafverfolgung
Erwartungen an die Behörden	falsche Wahrnehmung oder nichtzutreffende Erwartungen an die Behörden hinsichtlich der Zusammenarbeit mit Unternehmen; Vorbehalte/ Mythen/ Ängste der Unternehmen
Ressourcen	generelle Aufstellung im Hinblick auf die Kapazitäten zur Fallbearbeitung (personell, Standorte etc.) (im Vergleich zur „Konkurrenzfähigkeit“ geht es hier um die Quantität der Aufstellung)
Zuständigkeiten	Kooperationen und Verantwortungen: Grenzen/ Überlappungen/ Zusammenarbeit mit anderen Behörden; geteilte Verantwortlichkeiten/ unterschiedliche Zielsetzungen, die zu Schwierigkeiten führen
Sanktionierung	Kritik an der Ahndung: generell am Verfahren/ Vorgang oder an der Härte der Strafe/ den Umgang mit den Tätern bzw. Täterinnen/ Rechte
Strafverfolgung: Optimierungsvorschläge	
Spezialisten	Herausbilden von Expertenwissen durch Maßnahmen, Akquirierung etc.
Strafverfolgung	Wie komme ich zum Täter/zur Täterin? (Strafverfolgung bis zum Punkt an dem ein Täter/eine Täterin identifiziert werden konnte); staatliche Vorgaben/ Standards/ Verfahrensweisen zur Vereinheitlichung & Transparenz

Code	Beschreibung
Sanktionen	Was mache ich dann mit dem Täter? (Täter ist bekannt und wird sanktioniert); Strafverfahren/ explizite Erwähnung von möglichen Gesetzen zur Vereinfachung/ Optimierung im Hinblick auf Cybercrime/ Cybersicherheit/ Haftungsregelungen
Schutz	(gesetzliche/ rechtliche) Maßnahmen zum Schutz von Daten vor einem Angriff
Kriminalprävention	
durch Medien	Unternehmen werden sensibilisiert durch die mediale Aufmerksamkeit/ Fokussierung auf Angriffe oder Maßnahmen
durch Behörden: allgemein	Behörden gehen aktiv auf die Unternehmen zu und sensibilisieren die Unternehmen im Hinblick auf Cybersicherheit/ bieten Leistungen an/ steigern ihren Bekanntheitsgrad
durch Behörden: Öffentlichkeitsarbeit	alle allgemeinen Tätigkeiten, die für die Öffentlichkeit bestimmt sind durch z.B. Vorträge/ Broschüren etc. (aktiv von den Behörden angeboten)
durch Behörden: Test/Übungen	Tests oder Übungen wie auch Seminar, die seitens der Behörden angeboten werden
durch Behörden: Awareness	allgemeine Aussagen über die notwendige oder vorhandene Steigerung der Sensibilität/ Awareness für die Thematik (eher allgemein, im Gegensatz zum Subcode „Öffentlichkeitsarbeit“ keine konkrete Benennung wie Awareness geschaffen wird; eher Empfehlungscharakter)
durch Behörden: Zielgruppengeleitet	Aussagen, die die Eingrenzung einer/ Ausrichtung auf eine bestimmte Zielgruppe anzeigen
durch Behörden: Bewertung von Unternehmen	Rückmeldung und Feedback seitens der Unternehmen zum Angebot der Behörden/ Aussagen darüber, wie das Angebot der Behörden angenommen oder wahrgenommen wird/ Kritik oder Optimierungsvorschläge, die seitens der Unternehmen geäußert werden oder an die Behörden herangetragen werden, Bewertung der Leistung/ des Angebots
spezifische Präventionsmaßnahmen	konkret von den Behörden genannte Maßnahmen oder Vorgehensweisen, die präventiv gegen Cyberattacken wirken, wie z.B. Firewalls/ Backups etc.

5 ERGEBNISSE

In diesem Kapitel wird zunächst die Stichprobe beschrieben. Anschließend werden die wesentlichen Ergebnisse der qualitativen Inhaltsanalyse mit Hilfe beispielhafter Interview-Aussagen zu den oben ausgewählten Kategorien dargestellt und in einem weiteren Schritt inhaltlich zusammengefasst.

5.1 Beschreibung der Stichprobe

Die wesentlichen Merkmale der Interviewteilnehmer sind in Tabelle 8 zusammengefasst.

Tabelle 8 Wesentliche Merkmale der Interviewteilnehmer

Person					Institution	
Int. Nr.	**Geschl.**	**Position**	**Arbeitsschwerpunkt**	**Beschäftigungsdauer** (in Jahren)	**Zielgruppe**	**Schwerpunkt**
1	m	Dezernatsleiter	Koordinierung, Strafverfolgung	?	Unternehmen	Strafverfolgung
2	m	Kriminalbeamter	Prävention, Kontaktaufnahme zu Unternehmen, technische Unterstützung	4	Unternehmen	Strafverfolgung
3	m	Fachbereichsleiter	Aufklärung Cyberangriffe	39	Unternehmen	Aufklärung, Prävention, Sensibilisierung
4	m	Leiter	Abwehr, Prävention, Technik, Observation	7	Unternehmen	Aufklärung, Prävention, Strafverfolgung
5	m	Stellv. Sachgebietsleiter	Auswertung und Gremienarbeit, Ansprechpartner für Unternehmen	2	Unternehmen	Strafverfolgung
6	m (B1)	Leiter	Qualitätsmanagement, Neuorientierung und Umstrukturierung der eigenen Behörde, Networking	?	Internetkriminalität allgemein	Strafverfolgung
	m (B2)	Strafermittler	Strafermittlung, Weiterbildung von Justiz und Polizei, Kooperation mit Wirtschaft	?	Internetkriminalität allgemein	Strafverfolgung
7	m (B1)	Sachgebietsleiter	Administration, Vernetzung mit anderen Strafverfolgungsbehörden	3	Unternehmen	Strafverfolgung
	m (B2)	Kriminalbeamter	Prävention, Sensibilisierung & Netzwerken mit Wirtschaftsunternehmen; Kooperation mit Hochschulen	7	Unternehmen	Strafverfolgung

Alle Interviewteilnehmer waren männlich und zwischen zwei und 39 Jahren in staatlichen Behörden beschäftigt. Die Position und der Schwerpunkt der Arbeit können der Tabelle 8 (S. 35) entnommen werden. Die Zielgruppe der Behörden war überwiegend Unternehmen oder Internetkriminalität im Allgemeinen. Bei zwei Behörden spielten Unternehmen eine eher untergeordnete Rolle. Der Schwerpunkt der Behörden war vor allem die Strafverfolgung; vereinzelt lag der Fokus auch auf Prävention und/oder Aufklärung.

5.2 Wesentliche Ergebnisse aus den qualitativen Interviews

Die Ergebnisse werden entlang der oben ausgewählten, für die Darstellung des Phänomens relevanten Kategorien abgebildet. Einige Interviewaussagen können in unterschiedlichen Subcodes (allerdings nicht einer Kategorie) vorkommen, da einzelne Aussagen aus verschiedener Perspektive betrachtet werden können. Hinsichtlich der fokussierten Kategorien wurden insgesamt 60 Subcodes generiert.

5.2.1 Trends/Entwicklungen und Täter/Täterinnen (allgemein)

Trends und Entwicklungen

Dieser Kategorie wurden insgesamt 128 Aussagen zugeordnet. Die Mehrheit der Interview-Aussagen bezog sich auf den Subcode „(unzureichende) Datenerfassung“ (n=29). Interviewteilnehmer 2 war zum Beispiel der Meinung, dass „(…) wir auch das Problem [haben], dass PKS-mäßig zum Beispiel Auslandsstraftaten noch unsauber erfasst wurden bislang.“ und Interviewteilnehmer 6 (B1), dass

> „es ist in der Tat richtig [ist], so was haben wir noch nie gehabt. Also großes Ausspähen irgendwelcher Daten aus Unternehmen, seien es wie gesagt Kundendaten, seien es Unternehmensdaten, Anzeigeverhalten gleich null oder Anzeigeaufkommen gleich null. Das ist, in diesem Bereich wissen wir nichts.“

Interviewteilnehmer 4 wies in diesem Zusammenhang auf Unternehmen als Fehlerquelle hin und ergänzte:

> „Also seriös wird das keiner sagen können. Ist genauso wie bei Schadenshöhen, die die irgendwo mal gemeldet werden, das kann keiner seriös, weil gar keiner das Dunkelfeld kennt. Es gibt genug Firmen, die es schön für sich behalten, und die es vielleicht auch noch gar nicht gemerkt haben.“

Weitere Trends bzw. Entwicklungen umfassten Angebote für Betroffene (n=20). Hier kamen vielfältig Versicherungen zur Sprache; so äußerte Interviewteilnehmer 2 beispielsweise:

> „Was so die Cybercrime-Versicherung angeht, die wollen natürlich Verkaufszahlen, die haben ne ganz andere Zielrichtung dahinter, die wollen ihre Versicherung verkaufen, haben aber wirklich gar keine Ahnung, was auf sie zukommt. Null. Und das geben die Versicherer eigentlich auch selber zu. Also die versuchen dann natürlich sich auf dem Markt zu stellen, versuchen irgendwas abzusichern, wo sie überhaupt gar keine richtigen Zahlen haben, mit denen sie arbeiten können, wo sie das Risiko selber für sich berechnen können. Ich glaube, das wird nen sehr spannendes Thema."

Aber auch hinsichtlich der Arbeit von Behörden habe sich bereits einiges getan:

> „Na ja gut, das ist ja allgemein bekannt, dass sich sämtliche Behörden jetzt mittlerweile des Themas angenommen haben, sei es das Bundeskriminalamt, sei es die Landeskriminalämter, mit den zentralen Ansprechstellen. Die Bundeswehr stellt eine eigene Waffengattung auf, die sie der Cybercrime-Bekämpfung, (…), also das hat sich mit Sicherheit verbessert, weil das Thema einfach präsenter ist und eben auch in der Politik angekommen ist, und dass man sich dessen bewusst ist, dass man sich des Themas annehmen muss." (Interview 5).

Zudem wiesen die Interviewteilnehmer auf die sich entwickelten/entwickelnden Angriffsflächen für Täter/Täterinnen hin (n=17). Hierzu äußerte Interviewteilnehmer 3 beispielsweise:

> „Und damit ist ja die Auswirkung, die die Cybercrime machen kann, also die Zugriffe, wo ich übers Internet hinkomme, dass die Angriffsoberfläche wird immer größer und größer und die Auswirkungen, die da ist, gravierender, ja. Also das ist definitiv eine Riesenherausforderung, die wir momentan haben, dass einfach die Auswirkungen schlimmer werden."

Auch sich entwickelte/entwickelnde Angriffstrends von Täter/Täterinnen spielten unter den Interviewteilnehmern eine Rolle (n=12); dabei wurden zum Teil steigende spezifische Angriffe thematisiert (z.B. CEO-Fraud, Business Email Compromise, Ransomware), es wurde sich aber auch allgemein dazu geäußert:

> „Also in den letzten Jahren ist mir eigentlich nichts sehr Neues aufgefallen, sondern ja es hieß mal anders, aber Web-Portal war anders, aber im Prinzip, das Grunddelikt ist eigentlich immer das Gleiche." (Interview 7, B2) oder „Und das wird mit Sicherheit in der Zukunft so weitergehen, dass es immer wieder neue Phänomene gibt, immer wieder neue Angriffsmuster und wir

gucken oh wieder was Neues. Vor die Lage werden wir sicherlich nicht kommen." (Interview 6, B2).

Ein weiterer Subcode im Rahmen der Kategorie „Trends und Entwicklungen" war neben der Erscheinung neuer Phänomene oder Angriffsarten auch die Verlagerung von Delikten in die digitale Welt (n=10). So äußerte beispielsweise Interviewteilnehmer 5:

„Vor allem, weil es ist ja nicht nur die die klassische Cybercrime-Attacke, sondern es sind ja die früheren Allerweltsdelikte Waffenhandel, Betäubungsmittelhandel, der auf der Straße stattgefunden hat, findet mittlerweile ja alles online statt."

Weiterhin wurden in dieser Kategorie allgemeine Aussagen zu „Betroffenen" gemacht (n=11): Interviewteilnehmer 4 war beispielsweise der Meinung, dass

„(…) wenn man sich dann für ne Versicherung entschieden hat, sage ich mal, wird man schon von den Versicherungen hingedrückt dafür, dass man einfach sicherer wird. Weil die haben ja keinen Bock zu zahlen."

Interviewteilnehmer 2 äußerte sich allgemein zum Datenschutz:

„Und wie schon gesagt, also ich glaube, dass ne Menge stattfindet, aber das fängt schon im Grunde genommen an bei Facebook, Amazon, Google und so, (…), was dort an Daten abfließt und miteinander vernetzt und verknüpft ist, ob das alles so in Sachen Datenschutz international richtig ist und rechtlich ist und selbst in den Ländern, wo diese Firmen angesiedelt sind, weiß ich nicht. Da wird es bestimmt auch noch den ein oder anderen Superskandal geben."

Der Subcode „Betroffene_Nachfrage" (n=11) bezog sich auf die Inanspruchnahme präventiver Maßnahmen seitens der Unternehmen. So äußerte Interviewteilnehmer 3 beispielsweise:

„Ich denke mir mal, also die Situation aus Seiten der Verschlüsselung sieht eigentlich ganz gut aus, ja. Also wenn sie es gibt, sie können ihre Daten gut schützen, wenn sie entsprechend investieren, ja. Ich glaube dann ist, Cybercrime wäre beherrschbar, wenn sie entsprechend Prävention betreiben."

Weiterhin wurden auch allgemeine Aussagen zu Entwicklungen bzw. Trends in Bezug auf „Täter bzw. Täterinnen" gemacht (n=9): Interviewteilnehmer 5 war beispielsweise der Meinung, dass

„die Veränderung ist dahingehend, dass jetzt nicht mehr nur ein enger Kreis der Nerds als Täter in Frage kommt, sondern die Täter ja aus allen Bereichen kommen.“, Interviewteilnehmer 3 ergänzt „Aber man könnte schon sagen, in der Regel finden sich schon Leute zusammen, wo die Harmonie, oder wo man sich aus dem gleichen Kulturkreis zum Beispiel. Aber das Bild ist viel zu unvollständig, um hier ne belastbare Aussage geben zu können.“

Ein weiterer Subcode im Rahmen der Kategorie „Trends und Entwicklungen“ war „aktuelle Studien“ (n=9). Hier wurden im Gegensatz zu den eher kritischen Äußerungen beim Subcode „(unzureichende) Datengrundlage“ aktuelle Studien dargestellt, so zum Beispiel Interviewteilnehmer 1:

„Also ich hatte ja schon ausgeführt, welche Phänomene jetzt aus unserer Sicht derzeit so ne größere Rolle spielen und ich kann jetzt auch nur auf die offiziellen Studien, die so vorliegen, verweisen, ne. Also wir haben jetzt für Bundesland B keine gesonderte Lage, ne.“

Täter bzw. Täterinnen

In dieser Kategorie befinden sich insgesamt 126 Aussagen. Die Aussagen der Interviewteilnehmer in dieser Kategorie wurden am häufigsten dem Subcode „Täter/Täterinnen_Gruppen“ zugeordnet (n = 24). Interviewteilnehmer 1 war zum Beispiel der Meinung, dass

„viele Cyberangriffe, die wir so feststellen, eingebettet sind in gewisse Täterstrukturen, in Gruppierungen, die eben sich lose zusammengeschlossen hat, um Straftaten zu begehen.“ oder Interviewteilnehmer 6 (B1), dass „bei CEO-Fraud würde ich allerdings auch davon ausgehen, dass es fast durchgängig Tätergruppierungen sind, das sind keine Einzeltäter. Dazu ist es viel zu komplex. Wir haben viel zu viele Informationen, das ist verteilt (…).“

Weiterhin wurden auch ganz allgemeine Aussagen zu Täter/Täterinnen gemacht (n = 17): Interviewteilnehmer 3 äußerte diesbezüglich beispielsweise:

„Und ich gehe davon aus, dass Cybercrime halt, wenn es um Geld geht, dass die halt auch wissen, wo sie investieren müssen und wo nicht, ja.“ Interviewteilnehmer 2 ergänzt: „ne, weil letztendlich hat ja jeder, der jetzt vielleicht ne kriminelle Vergangenheit von ein, zwei Jahren hat, der hat ja sein Wissen auch irgendwie erworben über die Zeit. Der ist ja nicht von null auf hundert dann gut geworden, hat sich zwei, drei Youtube-Tutorials angeguckt, sondern das muss man ja auch erstmal aufbauen.“

Ein weiterer Subcode im Rahmen der Kategorie „Täter/Täterinnen“ war „Strafverfolgung“ (n = 16). Hier ging es vor allem um den Umgang der Behörden mit der Täterschaft. So berichtete beispielsweise Interviewteilnehmer 6 (B1):

> „Aber es ist auch sehr stark und das ist der zweite Parameter natürlich, wer begeht welche Straftat. Es ist eine hochorganisierte professionelle Tätergruppierung und dann werden die Erfolgsaussichten relativ gering sein.“ oder Interviewteilnehmer 4 „Und wenn ich mich sozusagen zurückhalte, nur was weiß ich, ganz wenige Hacks mache, das ist ja dann das glaube ich auch, bin ich lange unentdeckt, ja. Wenn ich aber irgendwo meine Dienstleistungen anbiete, dass eine Firma das machen, dass das in Auftrag gegeben kann, ja, dann bin ich auch für die Strafverfolgung eventuell wieder greifbar.“

Der Subcode „Täter/Täterinnen_staatlich“ bezog sich auf Täter/Täterinnen aus Behörden oder Nachrichtendiensten (n = 14). Interviewteilnehmer 7 (B1) war beispielsweise der Meinung, dass

> „[gezielte Attacken, NotPetya] sind ja sehr komplexe Cyberattacken, die entweder von ja organisierten kriminellen Strukturen ausgehen, aber auch nicht allzu selten staatlich organisiert sind.“ oder Interviewteilnehmer 5 äußerte: „Dann haben wir natürlich aktuelles Beispiel Land 4, die staatlichen Nachrichtendienste, die da in diesem Bereich tätig sind.“

Auch wurden von den Interviewteilnehmern unterschiedliche Motive von Tätern bzw. Täterinnen angesprochen (n = 14). So war beispielsweise Interviewteilnehmer 2 der Meinung, dass

> „(…) es dann doch glaube ich eher die Leute [sind], die sich vielleicht das Wissen aus diesen Foren holen, ja, aber dann entweder alleine vorgehen, aus verschiedensten Gründen, entweder, weil sie was ausprobieren wollen, weil sie sich selber ausprobieren wollen oder manchmal vielleicht auch weil sie sich, ich sag mal wie so nen Robin Hood fühlen und irgendwo Daten klauen wollen, die sie dann veröffentlichen möchten.“

Interviewteilnehmer 5 fügte hinzu:

> „Oder, was auch sehr oft vorkommt sind, dass der Täter aus dem Kreis der eigenen Mitarbeiter stammt, sei es aus den unterschiedlichen Motivationsgründen, der ist bei der Beförderung übergangen worden, der hat keine Lohnerhöhung bekommen, hat ne Abmahnung bekommen und will demzufolge sich rächen.“

Interviewteilnehmer 6 (B1) sprach wiederum den finanziellen Aspekt an:

„(…) mit ner richtigen guten ja in Anführungszeichen Geschäftsidee geht es schon drum, möglichst viel Geld in kurzer Zeit zu machen und nicht nur zu zeigen, ich bin der tolle Cyberhecht und kann in Firmennetzwerke eindringen. Ich glaube, das ist, spielt heute eher ne untergeordnete Rolle."

Ergänzend zu Tätern bzw. Täterinnen in Gruppen sowie Täter bzw. Täterinnen aus Behörden oder Nachrichtendiensten wurden auch Einzeltäter thematisiert (n = 13). So äußerte beispielsweise Interviewteilnehmer 5:

„Wichtig sind halt die Hacker, diese technisch motivierten Personen mit entsprechendem technischen know how, die eben zum einen ihr Wissen für sich nutzen und zum anderen eben im Bereich Cybercrime as a Service ihr Wissen auch anbieten für nicht so kompetente Personen und dadurch noch mal Gewinne generieren."

Einige Interviewteilnehmer äußerten sich auch allgemein zu verschiedenen Angriffsarten (n = 11), wie beispielsweise in Interview 3:

„Bei Ransomware, wenn sie normalerweise breit verteilen und auf einmal der Aufwand für jemanden, der sich jetzt auf einmal gezielt anzugreifen, weil er vor nem Jahr gezahlt hat, nee." oder in Interview 7 (B2): „Man braucht im Prinzip beide Ebenen. Zum einen muss die IT-Abteilung natürlich wissen, was gerade so passiert, wo die Angriffsszenarien vielleicht sind, was unsere Täter dann irgendwo ausnutzen, weil das auch Sachen sind, die gar nicht immer so unbedingt offensichtlich sind."

Weiterhin wurden auch Angaben zur „Soziodemografie" der Täter bzw. Täterinnen gemacht (n = 9), wobei sich das auf das Alter, das Geschlecht, die Bildung, finanzielle Situation sowie die Nationalität bezog. So war beispielsweise Interviewteilnehmer 1 folgender Meinung:

„Der überwiegende Teil der Täter, die wir zu Gesicht bekommen, hat doch eher sozial schwaches Niveau. Da sehen die Wohnungen teilweise sehr schlecht aus, messihaft, das einzige, was dort von hoher Qualität ist, ist dann in der Regel der PC. Insofern ist das schon ne Auffälligkeit."

Der Subcode „Täter/Täterinnen_Wettbewerber" bezog sich auf Täter bzw. Täterinnen aus konkurrierenden Unternehmen (n = 8), was beispielsweise in Interview 3 deutlich wird:

„(…) wenn ich Konkurrenzspionage mir irgendwie angucke und dann den Konkurrenten lahmlege, also üblicherweise diese ganz normale Ransomware, wie wir sie seit paar Jahren haben,

das ist ja mittlerweile beim IT-Betrieb Standard. Da wird nen Rechner verschlüsselt, ich spiele das Backup zurück und gut ist, ja“.

5.2.2 Risikofaktoren, Schutzmaßnahmen und Kontaktaufnahme mit Behörden (bezogen auf Unternehmen)

Kontaktaufnahme mit Behörden

Dieser Kategorie wurden insgesamt 100 Aussagen zugeordnet, wobei sich die Mehrheit der Interview-Aussagen auf den Subcode „sich anschließende Leistungen“ bezog (n=37). Interviewteilnehmer 4 äußerte beispielsweise:

„Es können auch konkrete Fälle sein, dass einer sagt ‚Wir haben gemerkt, wir sind angegriffen worden, könnt Ihr mal kommen‘. Dann gucken wir uns das mal an, aber dann würde die Empfehlung weitergehen, dass wir über zum Beispiel Organisation B sagen, geht mal an die, da gibt es also Firmen, die möglicherweise euch helfen können, das Ganze wieder zu heilen, weil das machen wir nicht.“

Interviewteilnehmer 7 (B2) konkretisiert die Reaktion im Falle einer Erpressung:

„Aber die polizeiliche Grundsatzempfehlung sagt grundsätzlich auf keinen Fall zahlen. Das haben auch selbst unsere amerikanischen Kollegen mittlerweile verstanden, die haben auch am Anfang immer gesagt ‚Zahlen, dann ist die Sache erledigt‘. Mittlerweile haben auch die verstanden und empfehlen grundsätzlich keine Zahlung, um diese Spirale zu durchbrechen und vielleicht irgendwann mal Ransomware trocken zu legen, was natürlich utopisch ist, aber irgendeiner zahlt immer und solange wird es lukrativ.“

„Vorbehalte“ seitens der Unternehmen bei der Kontaktaufnahme mit Behörden konnten 24 Aussagen der Interviewteilnehmer entnommen werden. Ein Beispiel dafür wäre Interview 5:

„Na ja, wie gesagt, es bestehen diverse Vorbehalte gegen die Polizei in Form von, dass wir den Fall an die Presse weitergeben, oder dass wir die IT-Struktur des Unternehmens sicherstellen und demzufolge sind gewisse Vorbehalte eben da gegenüber einer Anzeigenerstattung bei der Polizei, aber grundsätzlich werden diese Vorbehalte weniger, auch weil eben die Angriffe auch mehr werden und die mediale Aufmerksamkeit größer wird und man eigentlich über die mediale Berichterstattung dann auch mitbekommt, dass die Vorbehalte nicht ganz begründet sind.“

Ein weiteres Beispiel wäre Interview 3:

> „Wissen Sie, das ist auch häufig also es wird immer so nen bisschen der Teufel an die Wand gemalt, dass die Firmen wollen dieses nicht und jenes nicht oder so etwas, ja. Ich denke mir mal, allgemein wenn die Firmen, also es gibt Firmen, die wenden sich nicht an uns, weil sie schlechte Erfahrungen gemacht haben mit Mitarbeitern (…)."

In Bezug auf die „Art der Kontaktaufnahme" konnten 20 Aussagen identifiziert werden. Interviewteilnehmer 1 äußerte beispielsweise:

> „Wir haben natürlich da drüber hinaus auch mehr Kontakte, wo eben einfach noch jemand fragt ‚Wie verhalte ich mich jetzt richtig? Wo muss ich ne Anzeige machen?', ne. Also nicht jeder Anruf hier ist gleich so nen Fall, wo wir ich sage mal das volle Programm fahren, sondern es ist eher so, dass man 10 Prozent der Anrufe hier der Kontaktaufnahmen zu uns am Ende zu nem ersten Angriff zum Beispiel vor Ort beim Unternehmen führen."

Interviewteilnehmer 2 führt dazu aus:

> „Aber mittlerweile spricht sich das immer mehr von Unternehmen zu Unternehmen weiter, ne dass man wirklich auch dann mitkriegt, oder dass wir die Emails reinbekommen, wir haben jetzt von dem und dem gehört oder ich habe von nem Bekannten oder wir haben gehört, dass Sie da und dann in dem Ort oder wir haben gelesen, dass das und das gewesen ist und wir haben gesucht nach einer solchen Sache im Internet und sind dann auf Sie gestoßen. Eigentlich kommen immer mehr die Unternehmen auf uns zu und fragen nach solchen Sachen."

Dem Subcode „Bekanntheit" wurden 19 Aussagen zugeordnet, wobei beispielsweise Interviewteilnehmer 4 berichtete, dass

> „(…) wenn dieser Name oder diese Marke Verfassungsschutz bekannt ist, gibt es die Propaganda über die Organisationen, Mund-zu-Mund-Propaganda und dann gibt's auch Anrufe, die dann wieder sagen ‚Mensch, ich hab hier so ne Fortbildungsveranstaltung', wir hatten das also neulich bei einem Radiosender ‚Wir möchten gerne mal unsere Mitarbeiter schulen.' (…)."

Interviewteilnehmer 6 (B2) äußerte hingegen:

> „(…) wir haben es versucht sowohl auf Ebene kleinerer Unternehmen, Unternehmensverbände, Organisationen den Kontakt zu suchen. Wir haben es auf der großen Bühne probiert in Stadt Z, wie heißt das noch mal? Veranstaltung 1 waren wir Speaker bei den großen Unternehmen und ich nenne jetzt einfach mal ein Beispiel, zum Beispiel die Firma H ist ja glaube ich ein ziemliches

großes Unternehmen in Deutschland, die wollten also unbedingt neben den ganzen kleinen Unternehmen auch, unseren Kontakt haben, haben diesen Kontakt für sich quasi unternehmensintern in den Abläufen hinterlegt für den Fall der Fälle. Das ist glaube ich das, was die Unternehmen gerne haben, dass sie so für den Fall der Fälle unsere Ansprechstellen kennen, aber es passiert nichts."

Risikofaktoren

In dieser Kategorie befinden sich insgesamt 99 Aussagen, die am häufigsten dem Subcode „Digitalisierung" zugeordnet wurden (n=31). Interviewteilnehmer 2 war beispielsweise der Meinung, dass „(...), die, die mehr vernetzt sind, sind natürlich mehr mehr betroffen, klar." Interviewteilnehmer 7 (B1) ergänzt diesbezüglich:

„Problem ist natürlich, die Digitalisierung nimmt darauf keine Rücksicht, die Entwicklungsschritte sind dermaßen schnell, wir bedrohen uns ja ständig gegenseitig mit neuen Techniken, die irgendwo verbaut werden, das muss alles irgendwo auch investiert werden und soll alles funktionieren. Bringen sie ner Kommune, die im Nothaushalt eben jetzt bei, sie muss aber noch E-Gouvernement machen und das muss alles sicher sein und sollen Geld für investieren in diese Bereiche, das ist genauso schwierig, als wenn sie in der Produktionsanlage die ne Getränkeabfüllanlage haben, in der Brauereiwesen, die vor 20 Jahren gebaut wurde mit Skala-Anschlüssen, und die heute vernetzt funktionieren soll, die Anschlüsse aber gar nicht sicher sind nach technischem Standard, wie wir es eigentlich definieren, weil die Anlage läuft immer noch 20 Jahre, weil die wird ja nicht einfach neu gebaut, nur weil wir jetzt IT haben. Und das ist halt ja auch die Schwierigkeit, dass die Produktionsmaschinen in der Wirtschaft deutlich länger leben als die IT, die Halbwertszeit eigentlich da ist."

„Fehlende Standards" als Risikofaktor konnte 18 Aussagen der Interviewteilnehmer entnommen werden. Ein Beispiel dafür wäre Interview 5:

„Dann oftmals wird keine Virenscanner verwendet oder keine Firewall oder es werden keine Backups erstellt oder wenn Backups erstellt werden, wird der, wenn es eine externe Festplatte ist, die bleibt am Netz hängen, was natürlich schlecht ist, wenn ich mir eine Ransomware einfange, die verschlüsselt nämlich das Backup dann gleich mit. Also das sind so die technischen Mängel, die oftmals bei Unternehmen vorherrschen." Ein weiteres Beispiel bietet Interview 1: „Ja ein Stichwort ist Sicherheitsmanagement, Risikomanagement. Das sind Faktoren, die bei sehr, sehr vielen von den Unternehmern, die wir begegnen, noch nicht angeschoben wurden."

Auch eine „fehlende Sensibilisierung" wurde von den Interviewteilnehmern als Risikofaktor benannt (n=15). So äußerte beispielsweise Interviewteilnehmer 3:

> „Ich meine, wenn ich meine vollautomatisierte Firma habe, bin ich stark digitalisiert, aber der Angriffsvektor läuft ja im Regelfall bei Cybercrime über die Person hinter der Tastatur, ne. Der muss auf die E-Mail draufklicken und der surft im Internet und fängt sich etwas ein. Ich will ja gar nicht sagen, dass er Schuld daran ist, aber meine, die Steuerung meiner Walzanlage oder was auch immer, die kann ich nicht direkt aus dem Internet angreifen, das funktioniert nicht. Ich brauche ja erstmal diesen Einstieg dort irgendwo rein."

Weiterhin wurden „kleine Unternehmen" aufgrund mangelnder Ressourcen als Risikofaktor identifiziert (n=14), wobei aber auch „große Unternehmen" als Risikofaktor genannt wurden, allerdings in einer deutlich geringeren Anzahl (n=2). Hinsichtlich „kleine Unternehmen" ist beispielsweise Interviewteilnehmer 1 der Meinung:

> „(…) dass die kleinen Unternehmen und im Bereich der Cybercrime immer einem Restrisiko ausgesetzt werden, den die nicht aus eigenen Mitteln, also vor allem finanziellen Mitteln, abstellen können, werden immer in der Hinsicht schlechter gestellt sein als nen Unternehmen, was zertifizierte Dienstleister einsetzen kann, was ne eigene IT-Abteilung hat."

Und Interviewteilnehmer 2 führt an:

> „Na ja gut, es gibt natürlich Unternehmen, die ich sag mal in Sachen Wirtschaft unterwegs sind, die von daher schon nen ganz anderen Sinn haben, sich um ihre Daten, ihre Informationssicherheit zu kümmern, ne. Es gibt natürlich aber auch trotzdem Unternehmen, handwerkliche Betriebe, kleine Betriebe, die haben diese Affinität schon gar nicht. Die müssen es nutzen, wollen es aber eigentlich überhaupt nicht."

Interviewteilnehmer 7 (B1) äußert bezogen auf „große Unternehmen" wiederum:

> „(…) sollte sich allerdings nehmen wir mal an ne Malware dort verbreiten und einen Rechner nach dem anderen oder Server nach dem anderen wird verschlüsselt, dann stehen die teilweise auch kopflos da und wissen nicht, wie sie darauf reagieren sollen, haben also nicht noch kompetente Partner an der Hand, die sie dann hinzuziehen."

Als weiterer Risikofaktor wurden von den Interviewteilnehmern „unternehmensspezifische Merkmale" angeführt, wobei es sich um Merkmale unabhängig von der Unternehmensgröße handelte (n=12). Das wird zum Beispiel in folgender Aussage aus Interview 4 deutlich:

„Jemand, der Brötchen backt, wird sicherlich nicht so unbedingt im Fokus sein, als wenn jemand irgendein Verfahren entwickelt hat, was sehr viel Geld spart, sehr, sehr innovativ ist."

Auch „Nachlässigkeit" als Risikofaktor spielte für die Interviewteilnehmer eine Rolle (n=7). Interviewteilnehmer 3 betont das beispielsweise in folgender Aussage:

„Aber die Traditionsunternehmen haben halt Altlasten, haben Systeme dabei, die sie nicht mehr patchen können. Sie werden kein neues Unternehmen aufsetzen und haben sie auch ne DOS-Box da drinhängen oder nen Windows 95, 98, es wird nicht passieren. (I: Hmhm) Aber die alten Unternehmen haben es. Und wenn die irgendwas vernetzen, dann sind die damit auf einmal, haben sie andere Angriffsexpositionen, würde ich mal behaupten, ne."

Schutzmaßnahmen

Dieser Kategorie wurden insgesamt 41 Aussagen zugeordnet, wobei sich die Mehrheit der Interview-Aussagen auf den Subcode „direkter Schutz" bezog (n=13). Interviewteilnehmer 7 (B1) war beispielsweise der Meinung, dass es

„(…) so einige grundsätzliche Sachen [gibt], die sind relativ schnell auch umgesetzt und sorgen schon für nen Schutz so. Das fängt schon damit an, dass man vernünftige Passwörter vergibt, ne, oder dass man nicht ja im Internet offen Sachen einstellt oder Daten da ablegt, auf die jedermann Zugriff hat, oder wenn man sich gedankenlos der Cloud bedient, ne. (…). Ne oder beispielsweise solche grundsätzlichen Dinge, dass man auch über Datensicherungen nachdenkt, nen Backup macht."

Einige Interviewteilnehmer führten weiterhin an, dass Unternehmen je nach Größe hinsichtlich ihrer Sicherheitsstandards unterschiedlich aufgestellt sind (n=12). Das wird beispielsweise durch folgende Aussage aus Interview 4 deutlich:

„Bei den Großen nicht so, die kümmern sich sicherlich schon mal so doch deutlich drum, dass sie auch sicher werden, aber bei den Kleinen ist zum Teil überhaupt, aber wie gesagt, kein Gefahrenbewusstsein, insofern wenn mir, wenn ich diese Sensibilität dafür nicht habe, mache ich auch nichts. Wenn ich nicht weiß, dass bei mir zu Hause eingebrochen wird, lasse ich die Türen offen."

Ein weiterer Subcode im Rahmen der Kategorie „Schutzmaßnahmen" war „Resilienz" (n=12). So äußerte beispielsweise Interviewteilnehmer 1, dass

„(…) wir auch positive Ausnahmen [haben], wo eben zum Beispiel der [BSI-]Grundschutz umgesetzt wurde, wo nen IT-Sicherheitsbeauftragter im Unternehmen vorhanden ist oder wo es sogar incident response Teams gibt, (I: Hmhm) ne."

Auch die „Rolle weiterer Akteure" wurde hinsichtlich von „Schutzmaßnahmen" thematisiert, allerdings in eher geringer Anzahl (n=4). Das verdeutlicht beispielsweise folgende Aussage aus Interview 2:

„Aber grundsätzlich habe ich vor kurzem mal gehört, weil wir ja vorhin das Thema Notfallplanung hatten, dass es angeblich auch schone erste Polizeidienststellen gab, die gesagt haben ja und falls sie mal, oder in der Notfallplanung müsste man auch mit aufnehmen oder am besten schon ein Bitcoin-Wallet sich irgendwo anlegen mit Geld drauf, damit man im Falle einer Erpressung schneller zahlen kann. Da kann ich die Hände über dem Kopf zusammenschlagen, da kann ich sagen, so was darf keine Polizeidienststelle rausbringen, unabhängig davon, dass dann auch irgendwie was mit Firma I mit drin stand, dass es nen Wirtschaftsunternehmen dann noch zusammen, da können sie es noch besser machen, wäre keine Sache, die ich nach außen bringen würde, selbst wenn man mir sagen würde, mach das so, würde ich sagen 'Nein, ich mache das definitiv nicht, das kannst Du selber machen', aber das muss jeder selber wissen, Tatsache ist, auf ne Erpressung sollte man niemals eingehen."

5.2.3 Strafverfolgung und Kriminalprävention (Perspektive Behörden)

Strafverfolgung: Probleme/Herausforderungen

In dieser Kategorie befinden sich insgesamt 198 Aussagen, wobei sich die Mehrheit der Interview-Aussagen auf den Subcode „deliktimmanent" (n=37) bezog und damit auf Problematiken und Schwierigkeiten, die sich aus dem Feld ergeben. Interviewteilnehmer 2 war zum Beispiel der Meinung, dass „(…) wenn wir uns nicht irgendwann mal gesellschaftspolitisch, auch international, um diese Anonymität kümmern, wird das nen bodenloses Fass werden. Das ist meine ganz persönliche Prognose." Interviewteilnehmer 1 ergänzte:

„Die Herausforderung, der wir uns konfrontiert sehen ist natürlich, dass dieser Bereich Cybercrime eine Dynamik in sich hat, die ne permanente Fortentwicklung der Organisation, aber auch der Ermittlungsmethoden und eben auch der Technik, die man halt für die Ermittlung braucht, erfordert. Und diese fortlaufende Anpassung, die zum einen Geld kostet, die Ressourcen für Entwicklung, Forschung und Entwicklung kostet, das sind natürlich Herausforderungen, die ich glaub keine Behörde oder keine Polizei immer so in ausreichendem Maße vorhält, ne. Das ist

dann immer quasi am konkreten Projekt die Aufgabe dafür Finanzen und Personal zu akquirieren und das dann voranzubringen."

Auch die „Zuständigkeiten" wurden von den Interviewteilnehmern als Herausforderung bei der Strafverfolgung benannt (n = 33). Ein Beispiel dafür wäre Interview 7 (B2):

„Wir kennen uns, aber die sind halt eben auch vom Ansatz her, immer wenn es vom Ausland kommt, dann sind die dran, die Konkurrentenausspähung der Unternehmer hier mit dem Unternehmer hier, ist schon wieder nicht mehr Verfassungsschutz, das wäre dann schon wieder bei der Wirtschaftskriminalität. Also das ist immer ne Schwierigkeit, nur weil jetzt der Angriff gerade mit ner IP aus Land 3 kommt, wäre es ja auch vermeintlich der Verfassungsschutz, heißt aber nicht, dass es nen Botnetz aus Land 3 ist (…). Also es ist nen sehr schwieriges Feld der Abstimmung dann im Einzelfall." Ein weiteres Beispiel findet sich in Interview 3: „Wir machen uns momentan durchaus Gedanken da drüber mit Informationspflichten gegenüber dem Ministerium D. Eigentlich, ich kann den Firmen gar keine Vertraulichkeit zusagen, das bleibt Amt C intern. Wenn ich einen Erlass vom Ministerium D bekomme, gebt mir den Firmennamen, dann muss ich den Firmennamen rausgeben. (…) Wir machen das Ministerium D, wir machen das denen dann nicht leicht, ja, also, wenn so was mal. Ich weiß gar nicht, ob wir jemals bisher einen genannt haben, ja. Aber de facto sind wir nicht Herr über die Daten."

Weitere Probleme bezogen sich auf die geringe Anzeigebereitschaft von Unternehmen und das damit verbundene große Dunkelfeld (Subcode: „Datenbasis", n = 29). So berichtete beispielsweise Interviewteilnehmer 6 (B1):

„Klassischer Person F-Spruch, müssen vor die Lage kommen und wir hinken tatsächlich weit hinterher, weil wir allenfalls zufällig mal irgendwas mitbekommen, das ist schon auch nen Stück weit frustrierend, dass man uns da so gar nicht einbindet." Interviewteilnehmer 1 ergänzte: „Was jetzt unsere Daten betrifft, (…) ist es halt nicht möglich, eine fundierte Bewertung der Cyberkriminalität zu erstellen. Das ist dieses klassische, also zum einen ist es das Dunkelfeldproblem, dann haben wir natürlich das Problem der Datenqualität und wir haben auch das Problem, dass PKS-mäßig zum Beispiel Auslandsstraftaten noch unsauber erfasst wurden bislang."

Auch die „Konkurrenzfähigkeit" der Beschäftigten in den Behörden stellte eine Herausforderung im Rahmen der Strafverfolgung dar (n = 28). So äußerte beispielsweise Interviewteilnehmer 4, dass

„wenn man also wirklich Leute, die das wirklich studiert haben, die das Patent haben entsprechend, die zu kriegen, das kann man sich fast schon abschminken. Wir sind manchmal froh, wenn wir Menschen kriegen, die einfach nur so nen IT-Faible haben. Die haben vielleicht ne ganz andere Ausbildung, der Klassiker ist immer, der ist Polizeibeamter, hat aber sich irgendwo dieses Wissen anderweitig angeeignet und man versucht einfach durch Fortbildung auszubauen." Interviewteilnehmer 2 äußerte dazu, dass „als Einstieg in diesen Beruf ist so ne Arbeitsstelle bei der Polizei und gerade in dem Bereich Cybercrime auch Gold wert. Gerade für die weitere Verwendung, auch nach außen hin, um interessant zu sein für die Wirtschaft. Gerade auch die Lehrgänge, die hier besucht werden, sind natürlich sehr intern und auch sehr gut, auch die Lehrgänge vom Bundeskriminalamt, die dann teilweise auch bestückt werden dann durch Informatiker. Und solche Leute sind natürlich dann in der Wirtschaft besonders begehrt am Ende." Interviewteilnehmer 4 ergänzte: „Sie hatten ja vorhin nachgefragt, das deutsche Beamtenrecht ist insoweit sehr unflexibel als das man, ja, wenn man sieht, wenn man diese Tätigkeiten dann in das Beamtensystem hineingießen will, in der Regel nicht genug bezahlt, um auf dem freien Markt überhaupt konkurrenzfähig zu sein."

Weitere Probleme bezogen sich auf die „Erwartungen an die Behörden" (n = 22). Das wird beispielsweise durch folgende Aussage aus Interview 5 deutlich:

„Na ja, der Anzeigeerstatter möchte natürlich immer, dass man ihm den Täter auf dem Silbertablett serviert und am besten den entstandenen Schaden beim Täter wieder zurückholt, also das sind die Erwartungen, aber die muss man leider, oft können wir denen nicht entsprechen." Interviewteilnehmer 2 äußerte dazu: „(…) wir kennen die Vorurteile, die von früher eigentlich so mehr immer an die Polizei ran getragen wurden oder wo gesagt wurde ‚Mensch, wenn ich jetzt ne Anzeige erstatte, dann kommen die mit grünen Bullis hier vorgefahren oder mittlerweile mit blau-silbernen Bullis und dann nehmen die meine ganze IT-Sicherheit, meine ganze IT hier mit und alles auseinander und alles ist lahmgelegt', das ist natürlich Quatsch. Ne also auch da sagen wir ganz klar, um unsere Ermittlungen zu führen, um überhaupt Ermittlungen zu führen, sagen wir, was wir benötigen und sie stellen uns zur Verfügung. Ne, also das das muss man klarmachen von vornherein, dass da die Angst schon mal nicht da ist."

Weiterhin wurden unzureichende „Ermittlungsmethoden" als Probleme im Rahmen der Strafverfolgung angeführt (n = 19). So äußerte beispielsweise Interviewteilnehmer 7 (B1), dass

„[wir] sind ja auch schon bestrebt, ja ne effektive Strafverfolgung zu betreiben, es ist sehr mühsam. Das muss man klipp und klar unterschreiben. Die Aufklärungsquote ist auch nicht ganz so

hoch in dem Bereich, weil oftmals technische Hürden hier eine Rolle spielen." Interviewteilnehmer 6 (B1) merkte an, dass „(…) ich sie [Instrumentarien vom Gesetzgeber] lieber erst gar nicht [hätte], weil ich ja dann irgendwann erklären muss, dem Geschädigten, ja ich hab doch ne Online-Durchsuchung, ihr dürft doch alles und ich sage ja, aber leider sind in deinem Fall die Voraussetzungen für den Einsatz mal wieder nicht gegeben."

„Sanktionierung" als Herausforderung im Rahmen der Ahndung konnte 19 Aussagen der Interviewteilnehmer entnommen werden. Ein Beispiel dafür wäre Interview 6 (B1):

„Aber ich glaub das [202a StGB] ist nicht das Kernproblem. Ich glaube, das Kernproblem für uns Strafverfolger ist oft nicht das materielle Recht. Das materielle Recht ist oft nur insoweit ein Kernproblem, als es uns nicht erlaubt, dann die Werkzeuge überhaupt anzusetzen, wenn wir denn Werkzeuge haben. Also ich will es ein bisschen präziser ausdrücken. Wenn die Strafrahmen, wie beim 202a fortführend und 303a fortführend [StGB] derart niedrig sind, wie sie sind und es keine schweren Fälle beispielsweise gibt, sind wir viele prozessuale Möglichkeiten, beispielsweise ne Verkehrsdatenerhebung nach 100g [StPO] manchmal schon verschlossen."

Auch die generellen (quantitativen) Möglichkeiten zur Fallbearbeitung wurden als Herausforderung thematisiert (Subcode „Ressourcen", n = 11), was beispielsweise folgende Aussage aus Interview 2 verdeutlicht:

„Das ist natürlich nen Unterschied, ob ich jetzt wie Bundesland A mittlerweile mit ner ganzen Abteilung, die sich mit Cybercrime beschäftigt und auch viel stärker aufgestellt, wir sind da schon relativ gut dabei mit anderen Bundesländern, aber es gibt halt eben, wie schon gesagt, auch Bundesländer, die haben diesen Stellenwert offensichtlich noch nicht so erkannt und haben diese Lücke auch noch nicht so geschlossen wie es unserer Meinung nach sein sollte."

Strafverfolgung: Stärken

Dieser Kategorie wurden insgesamt 109 Aussagen zugeordnet. Die Interviewteilnehmer sahen die Stärken der Strafverfolgung am häufigsten in der personellen Aufstellung (Subcode: „breite Aufstellung: personell", n = 30). Interviewteilnehmer 5 war beispielsweise der Meinung, dass

„es uns schon gelungen [ist], qualifiziertes Personal zu bekommen, weil wir eben doch noch diese ja wie nennt man es, nein Spezialisten, sondern Idealisten zu finden, die eben was für den Dienst in der Gesellschaft tun wollen, und die sich dann für den Polizeiberuf tatsächlich interessieren und weniger auf die finanziellen Aspekte fokussiert sind." Interviewteilnehmer 7 (B2) meinte, dass „(…) das aber sehr unterschiedlich sein [kann]. Also jemand, der nen Abschluss in

> Biologie hat und dann auf dem Streifenwagen sitzt, der ist hier super untergebracht, weil er methodisch-wissenschaftlich arbeiten kann und so was wie Gremiumstrukturen super erkennen kann, da haben wir sehr gute Erfahrungen gemacht, also was immer wir für Chancen brauchen, muss man einfach ausloten."

Aber auch die Möglichkeiten der Schwerpunktsetzung durch Sondereinheiten wurde von den Interviewteilnehmern als Stärke bei der Strafverfolgung genannt (Subcode: „breite Aufstellung: Schwerpunkt, n = 21), was durch folgende Aussagen aus Interview 7 (B1) verdeutlicht wird:

> „Und weiterhin, abgesehen von diesem Zentrum 5 gibt es die Ermittlungskommission, die sich konzentriert auf ja bestimmte Kriminalitätssachverhalte, eben stürzen und die abarbeiten, ne in Form einer Ermittlungskommission." Und Interviewteilnehmer 5 beschrieb dazu: „Das ist eines von drei Sachgebieten hier im Landeskriminalamt aus Bundesland F, der Bereich Cybercrime-Bekämpfung ist im Landeskriminalamt aus Bundelsland F im Dezernat E verortet. Das Dezernat E besteht aus insgesamt drei Sachgebieten. Das ist das Sachgebiet G, das ist die Zentralstelle, die sich mehr dem Bereich Service und Support verschrieben hat. Dann gibt's das Sachgebiet H, das klassische Ermittlungssachgebiet ist das, den Ermittlungsfragen der Bekämpfung der Cybercrime beauftragt ist bzw. ja die wie der Name schon sagt, klassisch ermittelt. Und dann haben wir noch das Sachgebiet I, das ist die sogenannte Netzwerkfahndung, die sich also mit der klassischen Recherche im Internet befasst. Das heißt, die virtuelle Streifenfahrt, sei es soziale Netzwerke, sei es mit Schwerpunkt Kinderpornographie."

Als weitere Stärke wurde die technische Aufstellung der Behörden identifiziert (Subcode: „breite Aufstellung: Technik, n = 16). So äußerte beispielsweise Interviewteilnehmer 2:

> „Natürlich gerade für die Leute, die für solche Leute wie wir, die technisch affin sind, könnte es immer nen bisschen schöner sein und wir hatten auch schon Leute hier gehabt, die gesagt haben ‚Mensch, hier hängen gar keine riesengroßen Monitore an der Wand', habe ich gesagt hätte ich auch gerne, aber nein, aber eigentlich sind wir gut ausgestattet."

Einige Interviewteilnehmer führten weiterhin an, dass der Fokus im Vergleich zur Polizei auf den Interessen des Geschädigten liegt (Subcode: „Fokus auf Geschädigten", n = 15). Das wird beispielsweise durch folgende Aussage aus Interview 4 deutlich:

> „Aber wie gesagt, bei uns haben sie [die Unternehmen] den Vorteil, dass wir das mit denen besprechen, wie der weitere Gang möglicherweise sein könnte, und wenn der nicht in Frage

kommt, weil sie ganz einfach nicht wollen, dass das irgendwie nicht wird, dann machen wir es auch."

Auch die Rolle als zentraler Ansprechpartner wurde von einigen Interviewteilnehmern als Stärke im Rahmen der Strafverfolgung hervorgehoben (Subcode: „zentralisiert", n = 13). So berichtete beispielsweise Interviewteilnehmer 1:

„(…) dann wenn es zu nem Angriff im Unternehmen gekommen ist, wird auch über die zentrale Ansprechstelle Cybercrime dieser erste polizeiliche Angriff koordiniert. Ziel ist es am Ende eine Vertrauensbasis mit den Unternehmen zu finden, um halt, wir nennen es immer am konkreten Fall gemeinsam zu erarbeiten."

Einige Interviewteilnehmer betonten auch die Kooperation und Vernetzung mit anderen Akteuren als Stärke im Rahmen der Strafverfolgung (Subcode: „Kooperationen", n = 10), was beispielsweise durch folgende Aussage aus Interview 4 deutlich wird:

„Also ich weiß in einem konkreten Fall haben wir also einen Hilferuf eines Unternehmens bekommen, die sind reingefallen auf diesen CEO Fraud und wir haben wohl noch feststellen können, dass das Geld nach Land 3 gegangen ist und wir haben über die Organisation(en) C, da gibt es einen Bereich Land 3, mit denen, die haben wiederum Kontakt zu Ansprechpartnern aus Land 3, konnten wir tatsächlich Teile des Geldes wieder zurückholen."

Abschließend wurden auch allgemeine Aussagen zur breiten Aufstellung als Stärke im Rahmen der Strafverfolgung gemacht (n = 3): Interviewteilnehmer 1 äußerte diesbezüglich beispielsweise

„Aber nichtsdestotrotz bleibt es bei der grundsätzlichen Aussage, dass wir recht gut aufgestellt sind."

Kriminalprävention

In dieser Kategorie befinden sich insgesamt 41 Aussagen, wobei sich die Mehrheit der Interview-Aussagen auf den Subcode „durch Behörden: Öffentlichkeitsarbeit" bezog (n=27). Interviewteilnehmer 3 führte beispielsweise an:

„Dann gibt's aber auch ne Organisation D, die wir vor Jahren schon ins Leben gerufen haben, wo es auch drum geht, dass wir so best practices irgendwie rausgeben und da sind dann auch ich weiß nicht keine Ahnung wie viel das jetzt aktuell sind, aber sagen wir mal die machen so zehn Veranstaltungen im Jahr, wo sie auch rumreisen." Interviewteilnehmer 7 (B2) ergänzte: „Wir

versuchen das irgendwie zu bündeln. Wenn ein Unternehmen sagt, wir haben [Interesse], dann versuchen wir das zu gucken, können sie nicht noch jemand anderes dazu holen oder finden wir nen quasi nen Dach, wo man sagt, da kommt ein Unternehmen, lädt ein, aber zehn andere können dazu kommen, so dass wir mit einer Veranstaltung möglichst viele erreichen und nicht, den individuellen Beratungspart kriegen wir nicht abgedeckt, so dass wir versuchen immer irgendwie nen Mehrwert zu kriegen, dass wir sagen, wenn wir irgendwie nen Rahmen finden, wo sich nen paar Leute, nen paar Firmen, Unternehmen zusammen kriegen, ist das für uns eher darstellbar als jedes einzelne aufzusuchen."

Aber auch Empfehlungen hinsichtlich einer notwendigen Sensibilität bezogen auf Cyberangriffe wurden von den Interviewteilnehmern angesprochen (Subcode: „durch Behörden: Awareness", n = 21). Das wird beispielsweise durch folgende Aussagen aus Interview 4 deutlich:

„Das, was nachher der Wirtschaftsschutz macht ist, dass wir lernen oder sehen, was an Arbeitsweisen da sind, wie ist der Modus operandi, um dieses Wissen an die entsprechenden Unternehmen zu bringen und zu sagen ‚Schaut mal, so arbeiten die, jetzt guckt mal bitte in eurem Bereich was ihr dagegen machen könnt. Habt ihr offene Einfallstore, habt ihr offene Scheunentore, wo man reingehen kann, macht sie zu, achtet auf die Dinge, die wichtig sind für euch, für euer Unternehmen', dass die halt nicht zum Beispiel im Netz offen da liegen das sogenannte Tafelsilber." Interviewteilnehmer 7 (B2) betont: „Man braucht im Prinzip beide Ebenen. Zum einen muss die IT-Abteilung natürlich wissen, was gerade so passiert, wo die Angriffsszenarien vielleicht sind, was unsere Täter dann irgendwo ausnutzen, weil das auch Sachen sind, die gar nicht immer so unbedingt offensichtlich sind. Und zum anderen brauchen natürlich die Entscheider, die letztendlich dann auch im Unternehmen die Gelder freigeben, weil am Ende kostet IT-Sicherheit in der Regel Geld, ob das jetzt technisches Geld ist oder personelles Geld, im günstigsten Fall hat es funktioniert, dann weiß ich nicht, wofür habe ich das Geld ausgegeben, im ungünstigsten Fall hat es nicht funktioniert, dann weiß ich auch nicht, wofür habe ich das Geld ausgegeben. Das ist immer die Gratwanderung zwischen ja Security Usability."

Weiterhin wurden Aussagen zusammengefasst, in denen Unternehmen das Angebot bzw. der Leistung der Behörden bewerten (Subcode: „durch Behörden: Bewertung von Unternehmen", n = 17). So äußerte beispielsweise Interviewteilnehmer 2:

„Eigentlich habe ich bis jetzt nur gute Erfahrungen gemacht und auch nur positives Feedback bekommen, was die Arbeit der zentralen Ansprech-, überhaupt das Angebot der zentralen An-

> sprechstelle angeht, was viel gesehen wurde ‚Mensch, das finde ich super, dass so was überhaupt angeboten wird von der Polizei, hätte ich gar nicht gedacht' und eigentlich trifft das genau den Punkt."

Aussagen, die kriminalpräventive Ansätze hinsichtlich einer bestimmten Zielgruppe herausstellen wurden durch den Subcode „durch Behörden: Zielgruppengeleitet" erfasst (n = 13). Interviewteilnehmer 1 führt diesbezüglich beispielsweise an

> „Ja meine ganz persönliche Meinung ist, dass die kleinen Unternehmen und im Bereich der Cybercrime immer einem Restrisiko ausgesetzt werden, den die nicht aus eigenen Mitteln, also vor allem finanziellen Mitteln, abstellen können, werden immer in der Hinsicht schlechter gestellt sein als nen Unternehmen, was zertifizierte Dienstleister einsetzen kann, was ne eigene IT-Abteilung hat. Insofern ist es bei uns ne Zielgruppe, der wir mehr Aufmerksamkeit schenken als den mittleren, großen Unternehmen, in dem wir eben durch Sensibilisierungsveranstaltungen zumindest die Geschäftsführer erreichen."

Auch wurden präventive „Tests/Übungen" durch die Interviewteilnehmer expliziert (Subcode: „durch Behörden: Tests/Übungen", n = 9), was zum Beispiel folgende Aussage aus Interview 2 deutlich macht:

> „Also wir bieten es [Übungszentrum Cyberangriffe] umsonst, wir beschränken uns auf nen paar von diesen Kursen pro Jahr, ne, wir müssen ja kein Geld damit machen. Aber das ist ja ich halte es für notwendig. Ich hab das auch selber, also ich hab 2009 das erste Mal so was mitgemacht gehabt in Land 7 und es war gut, schlicht und einfach mal nen ganzen Tag dann diesen Stress mitzuerleben, da irgendwie Opfer zu sein, ja. Also nen Kollege war Täter, ich war Opfer, also haben es aufgeteilt, (…)."

Zusätzlich wurden auch einige allgemeine Aussagen zur Kriminalprävention durch Behörden gemacht (Subcode: „durch Behörden: allgemein", n = 8): Interviewteilnehmer 2 führt diesbezüglich beispielsweise an, dass

> „wir speziell eigentlich als Ansprechstelle für Wirtschaft, Behörden und Verbände gedacht [sind], im Bereich Cybercrime eben für Angriffe, aber auch im präventiven Bereich. Das haben wir uns ganz oben auf die Fahne geschrieben, sehr präventiv tätig zu sein, um halt eben auch die Mitarbeiter zu sensibilisieren, also in die Unternehmen rauszugehen, dort beratend tätig zu werden, also im Vorfeld von Straftaten, die möglicherweise dort begangen werden, aber natürlich auch im Nachgang."

Aber auch „spezifische Präventionsmaßnahmen“ wurden von einigen Interviewteilnehmern angesprochen (n = 5). So äußerte beispielsweise Interviewteilnehmer 3:

> „Was wir haben, ist für Pentest, also, wenn ne Firma die Sicherheit überprüfen möchte, wir haben zertifizierte Pentester, gibt‘s da und und wir haben zertifizierte Grundschutz-Auditoren, die wir teilweise auch nehmen mangels anderer Listen, wenn ihr jetzt irgendjemand braucht, der euch mal berät hier, damit umgeht, nehmt doch so nen Grundschutz-Auditor, der wird das andere auch kennen, ja.“

Abschließend spielten auch kriminalpräventive Ansätze durch Medien bei einigen Interviewteilnehmern eine Rolle (Subcode: „durch Medien“, n = 3), was beispielsweise durch folgende Aussage aus Interview 5 deutlich wird:

> „So drastisch wie sich das anhört, aber die Vorfälle müssten mehr werden, die in den Medien immer auch publik, mehr publik werden, sage ich jetzt mal so. Fälle, wie jetzt aktuell mit der Bundesregierung, das tage- und wochenlang durch die Medien geistert oder jetzt auch das mit Facebook. Das sind eben Vorfälle, die den Unternehmen vor Augen führt, was eigentlich passieren kann, und dass es in diesem Bereich eben stetig weitergeht.“

Strafverfolgung: Optimierungsvorschläge

Dieser Kategorie wurden insgesamt 30 Aussagen zugeordnet. Die Aussagen der Interviewteilnehmer bezogen sich hier am häufigsten auf Optimierungsvorschläge hinsichtlich der „Strafverfolgung“ (n=14). Interviewteilnehmer 1 war beispielsweise der Meinung, dass

> „(…) je früher nen Unternehmen mit uns in Kontakt tritt, zum Beispiel, wenn nen Angriff noch läuft, desto besser stehen auch die Chancen, dass man zumindest jetzt den Schaden begrenzt mit unserer Hilfe, auch wenn bei uns natürlich der einzige Schwerpunkt auf der Strafverfolgung liegt, aber wenn man einmal vor Ort ist, so sind wir der Meinung, können wir voneinander profitieren.“

Interviewteilnehmer 6 (B2) ergänzt, dass

> „wenn der Gesetzgeber uns nicht die Möglichkeit gibt, Tools am freien Markt einzukaufen, nämlich die Tools, die die Straftäter auch nutzen, wenn die nicht gesagt hätten, ja das, was die Straftäter nutzen, dürft ihr auch nutzen, nur dann wäre es überhaupt theoretisch denkbar, dass das eingesetzt werden wird.“

Weiteren Optimierungsbedarf sahen die Interviewteilnehmer im Bereich von „Spezialisten“ (n = 8), was beispielsweise in folgender Aussage aus Interview 4 deutlich wird:

> „Und insofern wäre es natürlich schön, wenn man außerhalb der Beamtenbesoldung irgendwie noch mal die Möglichkeit hätte, mit Zulagen oder ähnlichen Dingen, Leute [IT-Spezialisten] zu locken, (…)“.

Auch „Schutz“ spielte im Rahmen von Optimierungsvorschlägen eine Rolle (n = 4). So äußerte beispielsweise Interviewteilnehmer 3:

> „Also mittlerweile, also das ist so, jeder baut irgendwo IT in seine Systeme ein, und hat keine Ahnung davon, ja. Also wie gesagt, die Herausforderungen sind furchtbar, ja. Deswegen hat eigentlich auch dieses Problem mit Digitalisierung, ja, wo wir uns alle eigentlich durchaus ein federführendes Ministerium gewünscht hätten, was einfach sagt hier, ich nehme mich dieser Problematik mal an, ja.“

Weiterhin bestand laut Aussagen der Interviewteilnehmer auch im Bereich „Sanktionen“ Optimierungsbedarf (n = 4), was beispielsweise Interviewteilnehmer 6 (B1) deutlich macht:

> „Da hätte ich ganz gerne die Provider nen bisschen mehr in die Haftung eingebunden, auch in die Zusammenarbeit mit Strafverfolgungsbehörden, weil ich glaube, dort ist der sinnvolle Ansatzpunkt, um Informationen zu kriegen, die ist nicht am Endsystem des Bürgers. Das, ich glaube, sie ist eher beim bei dem Provider.“ (Interview 6, B1).

5.3 Zusammenfassung der Ergebnisse

Tabelle 9 (S. 60f.) fasst die vorangegangenen Ausführungen nochmals tabellarisch zusammen. Insgesamt lässt sich auf Basis der Interviews zunächst festhalten, dass sich der Markt rund um Cybersicherheit stetig durch die zunehmende Präsenz des Themas erweitert. Diese Entwicklung wird auch dadurch deutlich, dass von Behörden und Versicherungen Maßnahmen zur Verbesserung sowie zum Schutz angeboten sowie von den Unternehmen in Anspruch genommen werden. Insgesamt ist das Feld für die Behörden allerdings weitestgehend intransparent, was vor allem bedingt ist durch das große Dunkelfeld resultierend aus unentdeckten Angriffen, unzureichender Erfassung von Angriffen aus dem Ausland sowie fehlendem Anzeigeverhalten. Weiterhin beobachten die befragten Experten eine Erweiterung des möglichen Täter- bzw. Täterinnenkreises sowie die anteilige Verlagerung klassischer Delikte in die digitale Welt.

Als größten Risikofaktor für Cyberangriffe betonen die befragten Experten auch die zunehmende Digitalisierung. Die damit einhergehenden technischen Möglichkeiten bieten für Täter bzw. Täterinnen eine größere Angriffsfläche, wodurch die Angriffe spezifizierter werden. Die befragten Experten kritisieren die ausbleibenden Reaktionen auf dieses Risiko und weisen auf fehlende Standards und eine unzureichende Sensibilisierung hin. In diesem Zusammenhang empfehlen einige Interviewteilnehmer sowohl präventive (z.B. ausreichende Passwörter-Standards), aber auch direkte Schutzmaßnahmen (z.B. Datensicherung) sowie Maßnahmen zur Steigerung der Resilienz im Falle eines Angriffes (z.B. durch IT-Sicherheitsbeauftragte). Hinsichtlich Cybersicherheit wird in den Interviews weiterhin deutlich, dass im Vergleich zu großen Unternehmen insbesondere kleinere Unternehmen schlecht aufgestellt sind. Einige Interviewteilnehmer stellen dabei einen Mangel an (finanziellen) Ressourcen heraus, der es kleinen Unternehmen erschwert sich angemessen zu schützen. Folglich sehen die befragten Experten ihre Aufgabe vor allem darin, kleinere Unternehmen hinreichend zu informieren. Dieser Präventionsansatz wird in den Interviews auch als eine Stärke von Behörden wahrgenommen. Es wird weiterhin deutlich, dass unabhängig von der Größe des Unternehmens insbesondere Unternehmen, die innovative und rentable Geschäftsideen oder Daten innehalten, ein erhöhtes Gefährdungspotenzial für Cyberangriffe aufweisen.

Im Hinblick auf die Täter bzw. Täterinnen ist auf Basis der Interviews festzustellen, dass es sich einerseits um zusammengeschlossene Tätergruppierungen handelt. Andererseits gehen Täter bzw. Täterinnen auch allein vor, unter anderem indem sie ihre Fähigkeiten als Dienstleistung zur Verfügung stellen. Tätergruppierungen nehmen nach Aussage der Befragten allerdings einen höheren Stellenwert ein. Aber auch Angriffe von staatlichen Nachrichtendiensten, gefolgt von Angriffen durch konkurrierende Unternehmen werden genannt. Dabei wird berichtet, dass die Angriffe generell sehr unterschiedlich sind (z.B. gezielt, ungezielt). Hinsichtlich der Soziodemografie der Täter bzw. Täterinnen lassen sich nach Aussage einiger befragten Experten Tendenzen erkennen (z.B. finanzielle Situation). Bei den Motiven der Täter bzw. Täterinnen sind jedoch starke Divergenzen zu beobachten. So wird berichtet, dass sowohl ideologische als auch monetäre sowie persönliche Motive der Täter bzw. Täterinnen bei der Tat eine Rolle spielen. Bei der Strafverfolgung liegt der Fokus unabhängig vom Motiv auf dem Täter bzw. der Täterin als solchen bzw. solche und der Art der Straftat.

Probleme bei der Strafverfolgung ergeben sich dabei hauptsächlich aus der Dynamik des Feldes, da sich das Feld rund um die Cyberstraftaten ständig weiterentwickelt und die Strafverfol-

gung folglich einer fortlaufenden Anpassung bedarf. So ist es bezogen auf die Ermittlungsmethoden schwierig, stets auf dem aktuellen technischen Stand zu sein, was wiederum die Aufklärung von Fällen behindert. Eine zweitrangige, aber ebenfalls wichtige Rolle spielt bei einigen Interviewteilnehmern im Rahmen der Strafverfolgung der Mangel an (quantitativen) Ressourcen, wie z.B. Personal. Allerdings wird widersprüchlich zu den angesprochenen Schwierigkeiten hinsichtlich der technischen und personellen Ressourcen auch erwähnt, dass qualifiziertes Personal sowie die technische Ausstattung grundsätzlich eine Stärke der Behörden ist. Durch die qualitativ hochwertige Ausbildung in diesem Bereich sind die Beschäftigten der Behörden jedoch auch für die Wirtschaft von Interesse, wodurch qualifiziertes Personal schwieriger gehalten werden kann. Als weitere Schwierigkeit in der Zusammenarbeit mit Unternehmen beobachten die befragten Experten, dass Unternehmen teilweise mit verzerrten Erwartungen an die Behörden herantreten. Aber auch auf Seite der Behörden sind Schwierigkeiten zu verzeichnen, die sich hier insbesondere auf die Zuständigkeiten im Falle eines Angriffes beziehen. So sind beispielsweise die Verantwortlichkeiten bei einem Angriff aus dem Ausland nicht immer klar abzugrenzen, was wiederkehrende Einzelfallentscheidungen erzwingt.

Als Stärke betonen die Interviewteilnehmer wiederum die zentralen Strukturen der Behörden. Behörden stellen eine zentrale Ansprechstelle für Unternehmen rund um das Thema Cybercrime dar. In diesem Zusammenhang wird die Schwerpunktsetzung mittels Spezialeinheiten und die Kooperation sowie Vernetzung der einzelnen Akteure hervorgehoben. Weiterhin ist es den meisten befragten Experten möglich, auf die Interessen der Geschädigten einzugehen, was für die betroffenen Unternehmen von Vorteil ist. Dennoch beschreiben die befragten Experten die Kontaktaufnahme durch die Unternehmen als durchwachsen, da einige Unternehmen Vorbehalte gegenüber den Behörden haben. Diese sind vor allem auf schlechte Erfahrungen bzw. eine verzerrte Berichterstattung zurückzuführen. Grundsätzlich sind die Behörden allerdings durch Mundpropaganda unter den Unternehmen oder durch Fachvorträge zumindest teilweise bekannt. Im Fall einer Kontaktaufnahme seitens der Unternehmen stehen konkrete Handlungsempfehlungen im Mittelpunkt der angebotenen Leistungen der Behörden.

Optimierungspotenzial sehen die befragten Experten in der Zusammenarbeit mit den Unternehmen. Die Chancen auf einen Ermittlungserfolg erhöhen sich, wenn zeitlich schnell auf einen Angriff reagiert wird und zudem geeignete (sowohl technische als auch rechtliche) Möglichkeiten der Strafverfolgung zur Verfügung stehen. Auch sehen einige Interviewteilnehmer die Provider in der Verantwortung, die Behörden bei der Strafverfolgung zu unterstützen. Optimierungspotenzial besteht laut den befragten Experten auch darin, dass sich Unternehmen selbst

präventiv vor Angriffen schützen sollten, beispielsweise durch eine zunehmende Professionalisierung von IT-Systemen. Dieser Aspekt wird in die Kriminalprävention der Behörden aufgenommen und es wird durch Öffentlichkeitsarbeit aktiv auf Unternehmen zugegangen, um derartige Inhalte zu vermitteln. Zur Steigerung der Sensibilität werden zusätzlich vor allem individuelle Beratungen für Unternehmen angeboten, gefolgt von Seminaren, Übungen oder Tests. Diese Angebote seitens der Behörden werden von den Unternehmen laut Aussagen einiger Interviewteilnehmer gut angenommen.

Tabelle 9 Generierte Subcodes und deren Auftretenshäufigkeit

		n	Interview
Trends/Entwicklungen (n = 128)	(unzureichende) Datenerfassung	29	1, 2, 3, 4, 6, 7
	Betroffene_Angebot	20	2, 3, 4, 5
	Täter/Täterinnen_Angriffsfläche	17	2, 3, 4, 5, 6, 7
	Täter/Täterinnen _Angriffstrends	12	1, 2, 3, 6, 7
	Täter/Täterinnen _Verlagerung	10	2, 4, 5, 6, 7
	Betroffene	11	2, 3, 4, 5
	Betroffene_Nachfrage	11	2, 3, 4, 5
	Täter/Täterinnen	9	1, 2, 3, 5, 6
	aktuelle Studien	9	1, 2, 3, 5, 7
Täter/Täterinnen (n = 126)	Täter/Täterinnen_Gruppen	24	1, 2, 3, 5, 6, 7
	Täter/Täterinnen_allgemein	17	1, 2, 3, 4, 6, 7
	Strafverfolgung	16	1, 2, 3, 4, 5, 6
	Täter/Täterinnen_staatlich	14	2, 3, 4, 5, 7
	Motive	14	1, 2, 3, 4, 5, 6, 7
	Täter/Täterinnen_Einzeltäter/-täterinnen	13	1, 2, 3, 5, 6
	Angriffsart	11	1, 3, 7
	Soziodemografie	9	1, 3, 5, 6
	Täter/Täterinnen_Wettbewerber	8	3, 5, 7
Kontaktaufnahme mit Behörden (n = 100)	sich anschließende Leistungen	37	1, 2, 3, 4, 5, 6, 7
	Vorbehalte	24	1, 2, 3, 5, 6
	Art der Kontaktaufnahme	20	1, 2, 3, 4, 6, 7
	Bekanntheit	19	1, 2, 3, 4, 5, 6, 7
Risikofaktoren (n = 99)	Digitalisierung	31	2, 3, 4, 5, 6, 7
	(fehlende) Standards	18	1, 3, 4, 5, 7
	fehlende Sensibilisierung	15	1, 2, 3, 4, 5, 7
	kleine Unternehmen	14	1, 2, 3, 4, 5, 7
	unternehmensspezifische Merkmale	12	1, 3, 4, 5
	Nachlässigkeit	7	1, 2, 3, 4
	große Unternehmen	2	6, 7
Schutzmaßnahmen (n = 41)	direkter Schutz	13	1, 2, 3, 7
	Diskrepanz zwischen kleinen und großen Unternehmen	12	1, 2, 4, 5
	Resilienz	12	1, 2, 3, 4
	Rolle weiterer Akteure	4	1, 2, 3

		n	Interview
Strafverfolgung: Probleme/ Herausforderungen (n = 198)	Deliktimmanent	37	1, 2, 3, 4, 5, 6
	Zuständigkeiten	33	2, 3, 5, 6, 7
	Datenbasis	29	1, 2, 3, 5, 6, 7
	Konkurrenzfähigkeit	28	1, 2, 3, 4, 5, 6, 7
	Erwartungen an die Behörden	22	1, 2, 3, 5, 6
	Ermittlungsmethoden	19	2, 3, 4, 6, 7
	Sanktionierung	19	3, 6
	Ressourcen	11	1, 2, 3, 5, 6, 7
Strafverfolgung: Stärken (n = 109)	breite Aufstellung: personell	30	1, 2, 3, 4, 5, 6, 7
	breite Aufstellung: Schwerpunkt	21	1, 2, 3, 4, 5, 6, 7
	breite Aufstellung: Technik	16	1, 2, 3, 5, 6, 7
	Fokus auf Geschädigten	15	1, 2, 3, 4, 6, 7
	Zentralisiert	13	1, 2, 3, 5
	breite Aufstellung: Kooperationen	10	2, 3, 4, 5, 6, 7
	breite Aufstellung: allgemein	3	1, 4, 7
Kriminalprävention (n = 103)	durch Behörden: Öffentlichkeitsarbeit	27	1, 2, 3, 4, 5, 7
	durch Behörden: Awareness	21	1, 2, 3, 4, 5, 6, 7
	durch Behörden: Bewertung von Unternehmen	17	1, 2, 3, 4, 5, 6, 7
	durch Behörden: Zielgruppengeleitet	13	1, 2, 3, 4, 6, 7
	durch Behörden: Tests/Übungen	9	2, 3, 5, 6
	durch Behörden: allgemein	8	2, 4, 7
	spezifische Präventionsmaßnahmen	5	2, 3
	durch Medien	3	2, 3, 5
Strafverfolgung: Optimierungsvorschläge (n = 30)	Strafverfolgung	14	1, 3, 6
	Spezialisten	8	2, 4, 5, 6, 7
	Schutz	4	3, 6
	Sanktionen	4	6

6 DISKUSSION

In den Interviews wurde deutlich, dass der größte Risikofaktor für Cyberangriffe auf KMU die in fast allen Bereichen zunehmende Digitalisierung darstellt. Zusätzlich fehlt es an entsprechenden Reaktionen (z.B. IT-Sicherheitsbeauftragte, Steigerung der Awareness), wobei vor allem kleinere Unternehmen schlecht aufgestellt sind. Größere Unternehmen verfügen hingegen eher über eigene IT-(Sicherheits-)Abteilungen und sind sowohl technisch als auch organisatorisch besser gegen Cyberangriffe abgesichert. Auch in anderen Untersuchungen wurde dieses Ungleichgewicht zwischen kleinen und größeren Unternehmen festgestellt (siehe u.a. Hillebrand et al., 2017). Der GDV (2018) berichtet in diesem Zusammenhang von einer erhöhten Viktimisierung kleinerer Unternehmen. In zukünftigen Untersuchungen könnte überprüft werden, inwieweit die fehlende Reaktionsbereitschaft kleinerer Unternehmen das Risiko einer Vikitimisierung erhöht.

Einige Experten vorliegender Untersuchung thematisierten allerdings auch, dass es in kleinen Unternehmen an (finanziellen) Ressourcen mangelt, die einem ausreichenden Schutz möglicherweise im Wege stehen. Auch die Untersuchung von Hillebrand et al. (2017) konnte zeigen, dass gerade in kleineren Unternehmen oftmals mehr finanzielle und personelle Ressourcen für eine adäquate Absicherung gegen Cyberangriffe benötigt werden. So wird auch eine fehlende Zielgruppenfokussierung vorhandener Informationsangebote zu Sicherheitslücken kritisiert (Hillebrand et al., 2017). Die Experten vorliegender Untersuchung betonten allerdings als eine Stärke von Behörden, dass sie in ihrer Arbeit vor allem auf kleinere Unternehmen zugehen, um bspw. durch Vorträge, Schulungen und Seminare deren Awareness zu steigern. Laut Aussagen einiger Interviewteilnehmer werden die Angebote seitens der Behörden auch generell gut angenommen. Hier bedarf es weitere Untersuchungen, die sich mit der Bekanntheit vorhandener Angebote und deren Wahrnehmung auseinandersetzen, um einen differenzierten Einblick zu erhalten, inwieweit hier Optimierungsbedarf besteht.

Unabhängig von der Unternehmensgröße identifizierten die Experten weitere unternehmensspezifische Merkmale als Risikofaktor; häufig wurde in diesem Zusammenhang auf innovative und rentable Geschäftsideen oder Daten verwiesen, die ein erhöhtes Gefährdungspotenzial für Cyberangriffe darstellen. Auch Bollhöfer und Jäger (2018) stufen „wissensintensive Branchen“ (S. 33) als besonders gefährdet ein. Unternehmen sollten sich darüber bewusst sein, welche

„schützenswerten Assets“ für Angreifer von Interesse sein könnten (Hillebrand et al., 2017, S. 80). Zu besonders schützenswerten Assets zählen vor allem Kunden- und Bank- oder Finanzdaten sowie Informationen über Konditionen und „Patente, Produktinformationen und Konstruktionszeichnungen“ (KPMG, 2017, S. 16). So scheint es im Rahmen eines zielgruppenspezifischen Vorgehens neben der Unternehmensgröße zusätzlich wichtig zu sein, als Behörde auch auf Unternehmen aus besonders gefährdeten Branchen zuzugehen. In diesem Zusammenhang sollte das Thema IT-Sicherheit gemäß Bollhöfer und Jäger (2018) auch stärker in den Fokus von Vorgesetzten rücken. Werden IT-Sicherheitsrichtlinien von der Geschäftsführung nicht beachtet, wird es schwierig, anderen Beschäftigten deren Notwendigkeit zu vermitteln.

In diesem Zusammenhang weisen einige Experten vorliegender Untersuchung darauf hin, dass es neben den klassischen, direkten Sicherheitsmaßnahmen (wie bspw. aktuelle Antivirensoftware und Firewalls, regelmäßiges Anlegen von (verschlüsselten) Datensicherungen) auch wichtig ist, die Resilienz im Falle eines Angriffs zu steigern (bspw. IT-Sicherheitsbeauftragte, Incident-Response-Teams). Hier ist von Bedeutung, dass direkte Sicherheitsmaßnahmen eher kurzfristig und kostengünstig sind, wobei Maßnahmen zur Steigerung der Resilienz eher langfristig ausgelegt sind und damit ein höheres Maß an Ressourcen erfordern. Möglicherweise sind kleinere Unternehmen hier wiederum aufgrund ihres Ressourcenmangels benachteiligt. So sollte ein weiterer Schwerpunkt zukünftiger Forschung auf der Entwicklung differenzierter Lösungen gegen Cyberangriffe liegen, um hier ein breites Spektrum zielgruppenspezifischer Sicherheitsvorkehrungen anbieten zu können.

Ein weiteres Kernproblem, das sich in den Interviews gezeigt hat, ist das große Dunkelfeld resultierend aus unentdeckten Angriffen, unzureichender Erfassung von Angriffen aus dem Ausland sowie aus geringen Anzeigequoten. Auch in anderen Untersuchungen wird das Problem geringer Anzeigenerstattung deutlich (Bitkom e.V., 2017; Bollhöfer & Jäger, 2018). Wird angezeigt, so zeigt vorliegende Untersuchung wiederum, dass das teilweise mit größeren zeitlichen Verzögerungen verbunden ist. Insofern Anzeigen nicht direkt bei den Zentralen Ansprechstellen Cybercrime für die Wirtschaft (ZAC) erstattet werden, bedarf es einer Verbesserung der Weiterleitung entsprechender Anzeigen an diese Spezialdienststellen (zumal die Kooperations- und Vernetzungsarbeit der einzelnen behördlichen Akteure in den Interviews vereinzelt als Stärke betont wurde). Das würde den Anzeigeprozess und die notwendigen Ermittlungen beschleunigen und damit die Chance auf einen Ermittlungserfolg erhöhen. So könnte das Image der Behörden verbessert sowie ggf. einem gestörtem Vertrauensverhältnis zwischen

KMU und staatlichen Behörden entgegengewirkt werden, worauf sich in der vorliegenden Untersuchung und der Untersuchung von Bollhöfer und Jäger (2018) Hinweise finden ließen. Zudem wurde in der vorliegenden Untersuchung deutlich, dass die Bekanntheit der ZAC der Landeskriminalämter unter KMU weiter gesteigert werden kann und KMU zukünftig noch häufiger den direkten Weg der Anzeigenerstattung bei den ZAC als Option in Erwägung ziehen.[10] Damit könnte die häufig ausschließlich interne Regelung von Schadensfällen (vgl. dazu Bitkom e.V., 2017) verringert und das Dunkelfeld erhellt werden.

Der Bitkom e.V. (2017) konnte aufzeigen, dass vor allem die Angst vor Imageschäden zu einem geringen Anzeigeverhalten führt. Diesbezüglich betonten einige Interviewteilnehmer in vorliegender Untersuchung, dass es in den meisten Fällen durchaus möglich ist, auf die Interessen der anzeigenden Unternehmen einzugehen. Die Interviewpartner waren sich darin einig, dass die Ermittlungsbehörden bemüht sind, die Behinderungen im Betriebsablauf während der Strafermittlungen so gering wie möglich zu halten; Konfiszierungen von Servern und Endgeräten bei Betroffenen seien zudem nicht üblich, die Beweissicherung erfolge meist vor Ort im laufenden Betrieb. Im Falle der Ergreifung von Tatverdächtigen lassen sich öffentliche Gerichtsverhandlungen jedoch entgegen der Erwartungen einiger KMU nicht vermeiden. In zukünftigen Studien könnte diesbezüglich untersucht werden, wie hoch das Risiko oder das Ausmaß eines Imageschadens aufgrund einer öffentlichen Bekanntmachung eines Cyberangriffs ist. Resultierende Ergebnisse könnten in die Aufklärungsarbeit einfließen und so möglicherweise Ängste von KMU abbauen bzw. relativieren.

Bezogen auf den möglichen Täter- bzw. Täterinnenkreis beobachten die befragten Experten vorliegender Untersuchung, dass sich klassische Delikte weiter in den digitalen Raum verlagern (z.B. Erpressung in der Form von Ransomware). Das wiederum erweitert das Spektrum möglicher Täter bzw. Täterinnen (Täter- bzw. Täterinnengruppierungen, EinzeltäterInnen, konkurrierende Unternehmen, [ehemalige] Beschäftigte, Nachrichtendienste), wodurch sich die Tatmotive auch sehr stark unterscheiden (ideologisch, monetär, persönlich). Auch das BKA (2018) kam in seiner Untersuchung zu ähnlichen Ergebnissen. Die von KPMG (2017) befragten Unternehmen vermuten darüber hinaus vor allem „unbekannte“ oder „sonstige Externe“ (S. 23) als Täter bzw. Täterinnen. Hinsichtlich der Strafverfolgung macht vorliegende Untersuchung deutlich, dass die Dynamik des Feldes (u.a. Möglichkeiten der Anonymisierung, Vielzahl der

10 Ein Factsheet zur Anzeige von Cyberangriffen gegen Unternehmen und den aktuellen telefonischen Kontaktdaten der Zentralen Ansprechstellen Cybercrime der LKÄ findet sich im Anhang 3 sowie unter: https://www.cybercrime-forschung.de/cybercrime/fact-sheet/

Angriffsvektoren) und der damit verbundene fortlaufend geforderte Anpassungszwang ein großes Problem darstellt, insbesondere bezogen auf die Aktualität der Ermittlungsmethoden sowie auf die Kontinuität qualifizierten Personals. Hier besteht Handlungsbedarf. So fordern einige befragte Experten vor allem geeignete technische und rechtliche Möglichkeiten der Strafverfolgung sowie mehr Aus- und Weiterbildungen im Bereich IT-Sicherheit. Weiterhin sollten neben einer Beamtenbesoldung zusätzliche Anreize für IT-Spezialisten geschaffen werden (z.B. Zulagen). In diesem Zusammenhang würden sich z.B. Kooperationen mit Hochschulen anbieten, um kurzfristig qualifiziertes Personal zu rekrutieren. Mit längerfristiger Perspektive ist zu diskutieren, ob und wie die eigene Ausbildung von MitarbeiterInnen im IT-Bereich z.B. innerhalb der Fachhochschulen für die Polizei und Verwaltung möglich ist.

Vorliegende Untersuchung hat gezeigt, dass im Bereich Cyberangriffe gegen Unternehmen weiterhin dringender Forschungsbedarf besteht. Neben der Erhellung des Dunkelfeldes bestehen nach wie vor offene Fragen hinsichtlich der Folgen von Cyberangriffen für die Unternehmen sowie in Hinblick auf spezifische Risikofaktoren und geeignete Schutzmaßnahmen. Diese Forschungsfragen sind bei der Konzeption der CATI-Befragung von 5.000 Unternehmen (AP 3) eingeflossen. Die Ergebnisse der Unternehmensbefragung werden in einem gesonderten Forschungsbericht veröffentlicht.[11] Daneben wurden in der Ergebnisdiskussion verschiedene Ansatzpunkte für eine Verbesserung der Ermittlungsarbeit erkennbar. Dazu gehören vor allem die Steigerung der Bekanntheit der Zentralen Ansprechstellen Cybercrime (ZAC) mit deren Möglichkeiten und Grenzen bei der Ermittlung, die regelmäßige Überprüfung technischer und rechtlicher Mittel der Strafverfolgungsbehörden im Zusammenhang mit möglicherweise neuen Anforderungen im Bereich der Cyberkriminalität als auch die Diskussion neuer Wege zur Gewinnung, Bindung und Weiterbildung von Personal mit der benötigten IT-Kompetenz.

[11] Siehe Dreißigacker, Skarczinski und Wollinger (2020).

ANHANG 1 – INTERVIEWLEITFADEN

Abbildung 3 Interviewleitfaden

KRIMINOLOGISCHES FORSCHUNGSINSTITUT NIEDERSACHSEN E.V.

Interview-Leitfaden für das Forschungsprojekt Cyberangriffe gegen Unternehmen

Einstieg:

Herzlichen Dank, dass Sie sich die Zeit für das Interview nehmen und bereit sind, mit uns über Ihre Erfahrungen und Ansichten zu sprechen. Bevor wir mit dem Interview beginnen, möchte ich Ihnen noch einmal kurz erläutern, worum es in unserer Studie geht und worauf es uns ankommt.

Wir machen eine Befragung zum Thema „Cyberangriffe gegen Unternehmen" und zielen dabei im Besonderen auf kleine und mittlere Unternehmen ab, d.h. auf Unternehmen mit höchstens 249 Mitarbeitern.

Wir sind heute im Gespräch an Ihren beruflichen Expertise zu diesem Thema interessiert, d.h. an Ihren Erfahrungen und Sichtweisen, die Sie in Ihre Arbeit gewonnen haben und die Sie in Ihre Arbeit einbringen.

(Haben Sie dazu Fragen?)

Im Verlauf unseres Gesprächs werden wir Ihnen verschiedene offene Fragen stellen, bei denen ich Sie grundsätzlich bitte, einfach all das zu erzählen, was Sie für relevant und bedeutsam halten. Beim Zuhören werde ich mir hin und wieder Notizen machen, um später nachfragen zu können, lassen Sie sich davon bitte nicht stören. In diesem Interview gibt es für uns kein „richtig" oder „falsch". Wir prüfen kein Faktenwissen, sondern sind an Ihrer Perspektive interessiert. Zudem haben wir ausreichend Zeit: Das Interview wird schätzungsweise 1,5 Stunden dauern.

Noch zu ein paar formellen Angelegenheiten:

Wie wir Ihnen ja auch schon angekündigt haben, möchten wir das Interview für die spätere Auswertung auf Band aufnehmen und es anschließend verschriftlichen. Dadurch können wir Ihnen im Gespräch auch besser folgen. Selbstverständlich verwenden wir das Interviewmaterial in der Studie streng vertraulich und anonym. D.h., alle persönlichen Daten, die Rückschlüsse auf Sie erlauben, werden gelöscht oder anonymisiert.

→ Informationsblatt und Einverständniserklärung erläutern

(Haben Sie noch Fragen oder Einwände?)

→ Tonband anschalten

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages
IT-Sicherheit IN DER WIRTSCHAFT
VHV STIFTUNG
pwc

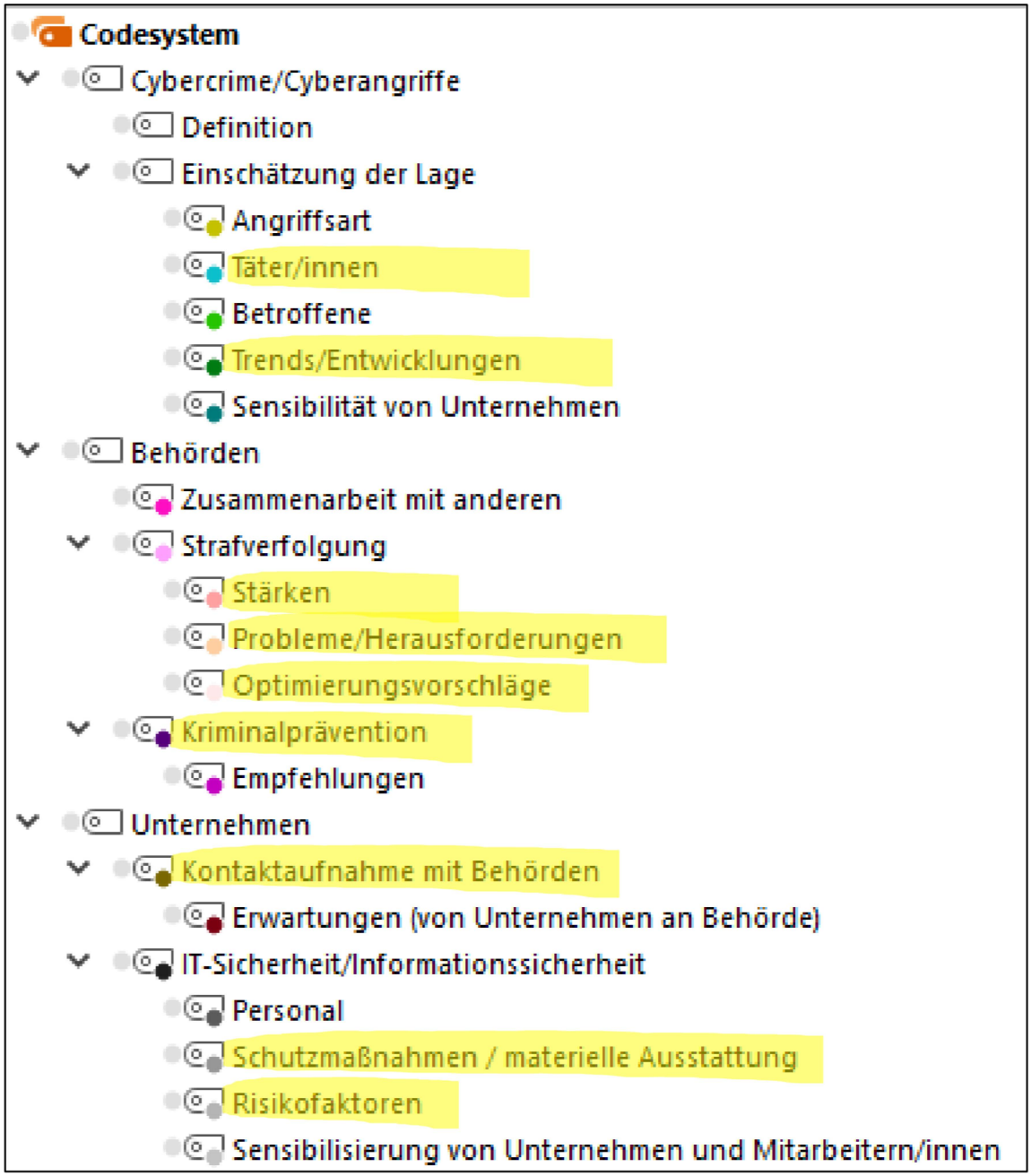
Leitfrage	Stichwörter	Nachfragen
BLOCK I: BERUFLICHER HINTERGRUND		
Wie würden Sie Ihre Aufgaben und Tätigkeiten in dieser Behörde beschreiben?	Position	Welche Position haben Sie innerhalb der Behörde/Abteilung?
	Schwerpunkt	Haben Sie einen thematischen Schwerpunkt in Ihrer Arbeit?
	Beschäftigungsdauer	Seit wann eschäftigen Sie sich mit dem Thema Cybercrime?
	Stellenwert Cybercrime	Welchen Stellenwert nimmt das Thema Cybercrime gegen Unternhemen in Ihrer Arbeit ein?
BLOCK II: AUFGBAEN UND MÖGLICHKEITEN DER BEHÖRDE/ABTEILUNG		
Wie würden Sie die Aufgaben und Möglichkeiten Ihrer Behörde/Abteilung in Bezug auf Cyberangriffe gegen Unternehmen beschreiben?	Zusammenarbeit	Arbeiten Sie mit anderen Behörden zusammen? Wie gestaltet sich die Zusammenarbeit (Informationsaustausch, Arbeitsteilung, Unterstützung)?
	Strafverfolgung	Wie schätzen Sie die Chancen für eine erfolgreiche Strafverfolgung ein? Wovon ist diese Abhängig?
	Herausforderungen	Finden auch Ermittlungen statt, ohne dass eine Anzeige eines Unternehmens vorliegt? Vor welchen Herausforderungen steht Ihre Behörde/Abteilung?
	Veränderung	Lassen sich diese derzeit bewältigen (Präventionsarbeit/ Strafverfolgung)? Hat sich in Hinblick auf diese Herausforderungen in den letzten Jahren etwas zum positiven oder negativen verändert?
	Ausstattung	Wie würden Sie die materielle und personelle Ausstattung Ihrer Behörde/Abteilung einschätzen? Besteht ein besonderer Mangel, der die Arbeit Ihrer Behörde/Abteilung erschwert? >IT-Spezialisten, >gesetzliche Grundlage
BLOCK III: DEFINITION/DIFFERENZIERUNG VON CYBERANGRIFFEN		
Cybercrime bzw. Cyberangriff ist ein weiter Begriff. Was zählen Sie alles zu Cyberangriffen gegen Unternehmen und was nicht?	Abgrenzung	Was gehört aus Ihrer Sicht nicht zum Bereich Cyberangriff gegen Unternehmen?
	Differenzierung	Lassen sich Cyberangriffe gegen Unternehmen differenzieren >Voraussetzungen, technische Umsetzung, Konsequenzen? Sind Ihrer Einschätzung nach bestimmte Angriffs- bzw. Deliktformen zentral oder spielen eine besondere Rolle (Warum)?

Leitfrage	Stichwörter	Nachfragen
BLOCK IV: KOOPERATION MIT KMU		
Welche Rolle spielen kleine und mittelständische Unternehmen in der Arbeit Ihrer Behörde/Abteilung?	Beispiele	Können Sie typische, besonders gute oder weniger gute Beispiele der Zusammenarbeit schildern?
	Erwartungen	Welche Erwartungen haben betroffene Unternehmen von Ihrer Behörde/Abteilung? Gibt es dabei Unterschiede zwischen den KMU?
	Kontakt	Wie entsteht üblicherweise der Kontakt zu Unternehmen? Gehen Sie proaktiv auf Unternehmen zu und wenn ja, in welcher Form (z.B. informierend, beratend)?
	Kooperation	Wie schätzen Sie die allgemeine Kooperationsbereitschaft von betroffenen Unternehmen ein Gibt es dabei Unterschiede zwischen den KMU (Größe, Branche, etc.)? Welche Hürden und Verbesserungspotenziale sehen Sie bei der Zusammenarbeit? Sind die Unternehmen zufrieden mit der Kooperation?
	Anzeige	Welche Vorfälle werden typischerweise angezeigt, welche eher nicht? Was sind die wichtigsten Anzeige-/Nichtanzeigegründe der Unternehmen?
BLOCK V: LAGE UND ENTWICKLUNG		
Wie schätzen Sie die derzeitige Lage und Entwicklung bezüglich Cyberangriffe auf Unternehmen ein?	Digitalisierung	Wie schätzen Sie den Digitalisierungsgrad und die digitale Vernetzung deutscher Unternehmen ein? Gibt es Unterschiede: Region, Größe, Branche; Umsatz, etc.?
	Betroffenheit	Gibt es stark und weniger stark betroffene Unternehmen (Unterscheidungsmerkmale)?
	Angriffsziele	Gibt es aus Ihrer Sicht derzeit besonders häufige Formen und -ziele von Cyberangriffen?
	Täter/innen	Welche Erkenntnisse zu Tätern/-gruppen gibt es?
	Belastung	Gibt es Hinweise auf regionale oder internationale Belastungsunterschiede?
	Trends	Nehmen Sie bestimmte Trends/Verschiebungen bei Cyberangriffen wahr?
BLOCK VI: SICHERHEITSSTANDARDS UND NOTFALLMANAGEMENT		
Wenn Sie an Risiken und Sicherungsmöglichkeiten gegen Cyberangriffe denken, wie sind deutsche Unternehmen derzeit aufgestellt?	Risikofaktoren	Was zählen Sie zu den wichtigsten Risikofaktoren für Cyberangriffe gegen Unternehmen?
	Schutzmaßnahmen	Welche Maßnahmen wären aus Ihrer Sicht am geeignetsten um sich nachhaltig vor Cyberangriffen zu schützen?
	Sensibilität	Wie schätzen Sie die Sensibilität deutscher Unternehmen in Bezug auf Cybercrime ein? Wie viele Cyberangriffe werden überhaupt entdeckt (doppeltes Dunkelfeld)?

Leitfrage	Stichwörter	Nachfragen
	Technische IT-Sicherheit	Wie schätzen sie die technische IT-Sicherheit von KMU derzeit ein? Sind Unterschiede erkennbar (Unterscheidungsmerkmale)?
	Personelle IT-Sicherheit	Wie beurteilen Sie die Kompetenz des IT-Sicherheitspersonals von Unternehmen? Wie verbreitet sind Mitarbeiterschulungen?
	Organisatorische IT-Sicherheit	Wie verbreitet sind Ablaufplänen bei erfolgreichen Cyberangriffen? Sind KMU i.d.R. gegen Cyberangriffe versichert? Sehen Sie einen Versicherungsbedarf?
	Hürden	Nehmen Sie besondere Hürden für die Verbesserung der IT-Sicherheit in Unternehmen war? Was müsste sich aus Ihrer Sicht ändern, um diese zu verbessern?
BLOCK VII: ABSCHLUSS		
Gibt es aus Ihrer Sicht einen relevanten Punkt, den wir noch nicht angesprochen haben?		
> Dank für Aufwand und Konzentration > positives Feedback hinsichtlich des persönlichen und wissenschaftlichen Nutzens des Gespräches **Tonband ausschalten!** **→ Code auf Informationsblatt; Einverständniserklärung unterschreiben**		

ANHANG 2 – CODESYSTEM

Abbildung 4 Codesystem MAXQDA mit Markierungen



ANHANG 3 – FACTSHEET ANZEIGE

Abbildung 5 Factsheet zur Anzeige von Cyberangriffen gegen Unternehmen

TABELLEN

ABBILDUNGEN

LITERATURVERZEICHNIS

Bitkom e.V. (2017). *Wirtschaftsschutz in der digitalen Welt*. Zugriff am 28.08.2018. Verfügbar unter https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf

BKA. (2015). *Bundeslagebild Cybercrime 2014*. Wiesbaden: Bundeskriminalamt. Zugriff am 04.06.2019. Verfügbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html

BKA. (2016). *Bundeslagebild Cybercrime 2015*. Wiesbaden: Bundeskriminalamt. Zugriff am 04.06.2019. Verfügbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html

BKA. (2017). *Cybercrime Bundeslagebild 2016*. Wiesbaden: Bundeskriminalamt. Zugriff am 04.06.2019. Verfügbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html

BKA. (2018). *Cybercrime Bundeslagebild 2017*. Wiesbaden: Bundeskriminalamt. Zugriff am 04.06.2019. Verfügbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html

BKA. (2019). *Polizeiliche Kriminalstatistik 2018*. Wiesbaden: Bundeskriminalamt. Zugriff am 04.06.2019. Verfügbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2018/pks2018_node.html

Bogner, A., Littig, B. & Menz, W. (2014). *Interviews mit Experten. Eine praxisorientierte Einführung*. Wiesbaden: Springer VS.

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

BSI. (2018). *Cyber-Sicherheits-Umfrage 2017*. Bonn: Bundesamt für Sicherheit in der Informationstechnik. Zugriff am 12.04.2019. Verfügbar unter https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Cyber-Sicherheits-Umfrage/Cyber-Sicherheits-Umfrage_node.html

BSI. (2019). *Cyber-Sicherheits-Umfrage 2018*. Bonn: Bundesamt für Sicherheit in der Informationstechnik. Zugriff am 04.06.2019. Verfügbar unter https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2018.pdf?__blob=publicationFile&v=9

Dreißigacker, A., Skarczinski, B. von & Wollinger, G. R. (2020). *Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer repräsentativen Unternehmensbefragung*

2018/2019 (Kriminologisches Forschungsinstitut Niedersachsen e. V., Hrsg.) (KFN-Forschungsbericht Nr. 152). Hannover.

GDV. (2018). *Cyberrisiken im Mittelstand. Ergebnisse einer Forsa-Befragung Frühjahr 2018* (Gesamtverband der Deutschen Versicherungswirtschaft e. V., Hrsg.). Zugriff am 12.04.2019. Verfügbar unter https://www.gdv.de/resource/blob/32708/d3d1509dbb080d899fbfb7162ae4f9f6/cyberrisiken-im-mittelstand-pdf-data.pdf

GDV. (2019). *Cyberrisiken im Mittelstand. Ergebnisse einer Forsa-Befragung Frühjahr 2019* (Gesamtverband der Deutschen Versicherungswirtschaft e. V., Hrsg.). Zugriff am 21.10.2019. Verfügbar unter https://www.gdv.de/resource/blob/48506/a1193bc12647d526f75da3376517ad06/cyberrisiken-im-mittelstand-2019-pdf-data.pdf

Hillebrand, A., Niederprüm, A., Schäfer, S., Thiele, S. & Henseler-Ungar, I. (2017). *Aktuelle Lage der IT-Sicherheit in KMU*. Bad Honnef: Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste (WIK). Zugriff am 18.09.2018. Verfügbar unter https://www.wik.org/fileadmin/Sonstige_Dateien/IT-Sicherheit_in_KMU/WIK-Studie_Aktuelle_Lage_der_IT-Sicherheit_in_KMU_Langfassung__2_.pdf

KPMG. (2017). *e-Crime in der deutschen Wirtschaft 2017* (KPMG AG, Hrsg.). Zugriff am 30.01.2018. Verfügbar unter https://home.kpmg.com/de/de/home/themen/2017/04/ecrime-studie.html

Mayring, P. (2010). *Qualitative Inhaltsanalyse. Grundlagen und Techniken* (11., aktual., überarb. Aufl.). Weinheim: Beltz. Verfügbar unter http://www.content-select.com/index.php?id=bib_view&ean=9783407291424

Schreier, M. (2010). Fallauswahl. In G. Mey & K. Mruck (Hrsg.), *Handbuch qualitative Forschung in der Psychologie* (1. Aufl., S. 238–251). Wiesbaden: Springer VS.

Viera, A. J. & Garrett, J. M. (2005). Understanding Interobserver Agreement: The Kappa Statistic. *Family Medicine*, *37*(5), 360–363.

Wassermann, S. (2015). Das qualitative Experteninterview. In M. Niederberger & S. Wassermann (Hrsg.), *Methoden der Experten- und Stakeholdereinbindung in der sozialwissenschaftlichen Forschung* (S. 51–67). Wiesbaden: Springer VS.