3. Verbreitung von Cyberkriminalität gegen Unternehmen in Deutschland

Arne Dreißigacker, Gina Rosa Wollinger

Inhaltsübersicht

3.1 Einleitung

Nachdem in den beiden vorherigen Kapiteln die Art und Weisen von Bedrohungsformen von Cyberkriminalität sowie die verschiedenen Tätergruppierungen dargestellt wurden, thematisiert der vorliegende Beitrag die Frage der Verbreitung von Cyberangriffen in Deutschland, d. h. in welcher Häufigkeit Straftaten aus dem genannten Bereich vorkommen und wer davon betroffen ist. Leider mangelt es bislang an Untersuchungen, die das Ausmaß von Cyberkriminalität gegen die öffentliche Verwaltung in Deutschland erfassen. Um sich dennoch der Lage in diesem speziellen Bereich anzunähern, werden Daten einer Unternehmensbefragung herangezogen. Dies erscheint insofern ein geeigneter Weg zu sein, als dass Unternehmen gewisse organisatorische Ähnlichkeiten mit Behörden aufweisen und Kommunen auch Träger öffentlicher Unternehmen der Daseinsvorsorge, wie z. B. Versorgungs- und Verkehrsbetriebe, sind.

Die Erfassung von Cyberkriminalität ist einerseits mit der Herausforderung konfrontiert, dass es sich um ein sehr dynamisches Phänomen handelt, bei welchem durch technische Entwicklungen häufig neue Spezifika von Angriffsarten hinzukommen (siehe Kapitel 1 im vorliegenden Band). Andererseits fällt die Erfassung auch dahingehend schwer, dass die betroffenen Nutzer den Angriff nicht notwendigerweise selbst bemerken oder als solchen einordnen können. Die in Kapitel 1 dargestellte Schwierigkeit des fehlenden einheitlichen Begriffsverständnisses von Bedrohungsformen aus dem Bereich der Cyberkriminalität führt u. a. auch zu Problemen der Vergleichbarkeit von verschiedenen empirischen Studien. Differenzen ergeben sich nicht nur hinsichtlich der Frage, welche Bedrohungsform untersucht wird, sondern auch in welchem Stadium überhaupt von einem Angriff gesprochen wird, ob z. B. auch ein versuchter

Angriff gezählt wird. Eine weitere Schwierigkeit in Bezug auf den Forschungsstand stellen die Unterschiede hinsichtlich der wissenschaftlichen Qualität der Untersuchungen dar. So scheint es insbesondere in Bezug auf den Untersuchungsgegenstand Cyberkriminalität gegen Unternehmen einige Untersuchungen zu geben, die Probanden selektiv auswählen, z. B. indem nur der eigene Kundenstamm befragt wird, oder kaum das methodische Vorgehen der Erhebung darlegen (mehr dazu siehe *Dreißigacker et al.*, 2020, S. 24 ff.).

Bisherige Studien weisen dabei auf eine hohe Betroffenheitsrate, auch Viktimisierungs- oder Prävalenzrate genannt, in Bezug auf Unternehmen hin. So ergab eine Untersuchung in den USA aus dem Jahr 2005, dass 67,0 % der 8000 befragten Unternehmen innerhalb eines Jahres von mindestens einem Cyberangriff betroffen war (*Rantala*, 2008). Hierzu zählten Angriffe auf das IT-System, wie sie beispielsweise durch einen Virus ausgelöst werden, Betrugsdelikte und andere Arten von Cyberangriffen. Zu einer ähnlich hohen Rate (66,5 %) kam auch eine Studie bezogen auf belgische Unternehmen aus dem Jahr 2015 (*Paoli et al.*, 2018). Auch der Forschungsstand bezogen auf Unternehmen in Deutschland weist eine hohe Betroffenheitsrate auf. Eine Befragung der Unternehmensberatung PricewaterhouseCoopers (PwC) kam zu dem Ergebnis, dass im Jahr 2015 56,0 % der befragten Unternehmen einen Cyberangriff erlebten (*PwC Strategy&GmbH*, 2016). Innerhalb von 24 Monaten gaben in einer Untersuchung von Bitkom 68,0 % der Unternehmen an, von Vorfällen im Bereich „Digitaler Wirtschaftsschutz" betroffen gewesen zu sein (*Bitkom e.V.*, 2018). Hierzu zählten überwiegend Cyberangriffe wie Diebstahl von IT- und Telekommunikationsgeräten (32,0 %), Diebstahl von sensiblen digitalen Daten (23,0 %), analoger Diebstahl von Daten und Maschinen (21,0 %) sowie digitale Sabotage von Systemen (19,0 %). Andere bekannte Formen von Cyber-Bedrohungen, wie z. B. Social Engineering und das Ausspähen von digitaler Kommunikation, trat mit 11,0 % eher selten in Erscheinung.

Unterschiede der Ergebnisse zur Häufigkeit der Angriffe könnten u. a. daraus resultieren, dass weder einheitlich erfasst wird, welche Delikte und Arten unter den Begriff Cyberkriminalität fallen, noch ab wann ein Angriff vorliegt. So könnten zu den erhobenen Angriffen auch Versuche gezählt werden, die von den Unternehmen in einem mehr oder weniger frühen Stadium erfolgreich abgewehrt wurden, sodass kein oder nur ein sehr geringer Schaden entstand. Demgegenüber könnte ein Angriff aber auch erst dann erfasst werden, wenn er aus Sicht der Angreifer erfolgreich verlief und einen größeren Schaden verursachte. Abgesehen von den Vergleichbarkeitsproblemen und den erkennbaren Unterschieden zeigt sich über alle Studien hinweg, dass relativ viele Unternehmen von Cyberangriffen betroffen sind und das Cyberangriffsrisiko für Unternehmen nicht unterschätzt werden sollte.

Daneben wird in vielen Studien auf den Zusammenhang vom Viktimisierungsrisiko und der Anzahl der Mitarbeiter eines Unternehmens verwiesen, insofern die größeren Unternehmen, gemessen an der Beschäftigtengrößenklasse, mit einer erhöhten Angriffsrate einhergehen. Beispielsweise zeigte eine Studie des Bundesamts für Sicherheit in der Informationstechnik (BSI), dass im Jahr 2018 43,0 % der Unternehmen mit mehr als 250 Beschäftigten und nur 26,0 % der

kleinen und mittleren Unternehmen von einem Cybersicherheitsvorfall[1] betroffen waren (*BSI*, 2019).

Zu den Fragestellungen, die in den bisherigen Studien nur sehr selten adressiert wurden, zählen die nach Angriffsarten differenzierten Auswirkungen auf Technik, Prozesse, Organisation und Beschäftigte von Unternehmen sowie die Art und Höhe entstehender Kosten. Daneben finden sich so gut wie keine Ergebnisse, die über eine beschreibende Darstellung hinausgehen und z. B. Unternehmensmerkmale benennen, die im Zusammenhang mit der Betroffenheit im Sinne von Risiko- und Schutzfaktoren stehen. Da aus solchen Kenntnissen wichtige Ableitungen für die Prävention geschlossen werden könnten, stellt dies eine bedeutende Forschungslücke dar. Hinzu kommt, dass bei der Branchendifferenzierung von Unternehmen kein einheitliches Vorgehen erkennbar ist und diesbezüglich somit auch kaum Vergleichsmöglichkeiten bestehen.

Das Kriminologische Forschungsinstitut Niedersachsen e.V. (KFN) hat aus diesem Grund in Zusammenarbeit mit dem Forschungszentrum L3S der Leibniz-Universität Hannover 2017 ein Forschungsprojekt zum Thema Cyberangriffe gegen Unternehmen begonnen, welches Ende 2020 abgeschlossen sein wird. Das Projekt wird gefördert durch die Initiative „IT-Sicherheit in der Wirtschaft" des Bundesministeriums für Wirtschaft und Energie und erhält eine Zusatzförderung von der Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers GmbH[2] und der VHV-Stiftung[3]. Das Erkenntnisinteresse des Forschungsvorhabens liegt dabei u. a. auf den Fragen, inwiefern insbesondere kleine und mittlere Unternehmen in Deutschland von Cyberkriminalität betroffen sind, welche Folgen und Reaktionen die erlebten Cyberangriffe nach sich ziehen und welche technischen und organisatorischen Präventionsmaßnahmen Unternehmen ergreifen. Mit den erhobenen Daten sollen strukturelle Unternehmensmerkmale und IT-Sicherheitsmaßnahmen herausgearbeitet werden, die im Zusammenhang mit der Betroffenheit stehen und als Risiko- bzw. Schutzfaktoren in Frage kommen. Ein Teilmodul dieses Forschungsprojekts[4] ist eine großangelegte Unternehmensbefragung, die im Folgenden zur näherungsweisen Beantwortung der eingangs aufgeworfenen Frage nach der Verbreitung von Cyberkriminalität in der öffentlichen Verwaltung herangezogen wird.

3.2 Methode

Die Unternehmensbefragung wurde mittels computergestützten Telefoninterviews (so genannte CATI-Befragung) durchgeführt. Dabei kamen professionelle Interviewer zum Einsatz, die Erfahrung in Befragungen aus dem Bereich Informationssicherheit aufwiesen und für die benannte Studie speziell geschult wurden.

---

1 Allerdings wird nicht weiter definiert, was unter Cybersicherheitsvorfällen gefasst wird.

2 www.pwc.de (abgerufen am 15.4.2020).

3 www.vhv-gruppe.de/de/ueber-uns/vhv-stiftung (abgerufen am 15.4.2020).

4 Zur ausführlichen Darstellung des Forschungsprojekts siehe *Dreißigacker et al.*, 2020, S. 13 ff.

Der dabei eingesetzte standardisierte Fragebogen umfasste insgesamt 40 Fragen und wurde im Vorfeld einem Pretest unterzogen. Neben Merkmalen des Unternehmens und Angaben zur Interviewperson wurden Fragen dazu gestellt, inwiefern Cyberangriffe bereits im Unternehmen vorkamen und welche Folgen dies gegebenenfalls hatte bzw. wie das Unternehmen hierauf reagierte. Ferner wurde erhoben, welche IT-Sicherheitsmaßnahmen in den Unternehmen vor bzw. erst nach dem schwerwiegendsten Cyberangriff vorhanden waren.

3.2.1 Stichprobenziehung

Die Befragung richtete sich an Unternehmen, d. h. rechtliche selbstständige Einheiten (z. B. GmbH, GbR usw.) in Deutschland mit mindestens zehn Mitarbeitern (Grundgesamtheit der Stichprobenziehung), die ca. 11,0 % der insgesamt 3,5 Millionen Unternehmen in Deutschland ausmachen. Kleinstunternehmen mit weniger als zehn Mitarbeitern blieben aus methodischen Gründen unberücksichtigt.

Da die Grundgesamtheit, also Unternehmen ab zehn Mitarbeitern in Deutschland, nicht gleichmäßig nach Beschäftigtengrößen verteilt ist und der Schwerpunkt auf kleinen Unternehmen bis 49 Mitarbeitern liegt, wurde eine disproportional geschichtete Zufallsstichprobe gezogen. Diese hat im Vergleich zu einer einfachen Zufallsstichprobe den Vorteil, dass alle Beschäftigtengrößenklassen in einer für differenzierte Auswertungen ausreichend großen Zahl vorhanden sind und sowohl repräsentative Ergebnisse für alle Unternehmen ab zehn Mitarbeitern in Deutschland als auch differenzierte Auswertungen nach Beschäftigtengrößenklassen und/oder Wirtschaftszweigen möglich sind. Demgegenüber wären in einer einfachen Zufallsstichprobe wahrscheinlich nur sehr wenige große Unternehmen gemäß ihrem kleinen Anteil in der Grundgesamtheit enthalten gewesen.

Weil die gewählte Erhebungsmethode computergestützter Telefoninterviews (CATI-Befragung) telefonische Kontaktdaten der Unternehmen voraussetzt, konnte nicht direkt aus der Grundgesamtheit aller offiziell gelisteten Unternehmen ab zehn Mitarbeitern gezogen werden. Stattdessen erfolgte die Stichprobenziehung aus den kommerziellen Firmendatenbanken von Bisnode (ehemals Hoppenstedt) und Heins & Partner, die die notwendigen Kontaktdaten enthalten, und die zumindest hinsichtlich verschiedener kontrollierter Unternehmensmerkmale weitgehend der Grundgesamtheit entsprechen.[5]

Die Ziehung der disproportional geschichteten Zufallsstichprobe erfolgte nach einem vorher definierten Stratifizierungsplans, der netto jeweils 1000 Unternehmen mit zehn bis 49 Mitarbeitern, 50 bis 99 Mitarbeitern, 100 bis 249 Mitarbeitern und 250 bis 499 Mitarbeitern sowie weitere 500 Unternehmen ab 500 Mitarbeiter vorsah. Unabhängig von der Anzahl der Beschäftigten sollten zusätzlich 500 Unternehmen der Daseinsvorsorge befragt werden. Dazu zählen allgemein Unternehmen folgender Sektoren: Elektrizitätsversorgung, Gasversorgung, Gewerbliche Entsorgung/Kreislaufwirtschaft, Gesundheit (Krankenhäuser, ambulante Versorgung, Vor- und Nachsorge, Pflege), Post, Verkehrs- und

5 Zur Problematik, der nicht in der Auswahlgesamtheit enthaltenen Unternehmen siehe *Dreißigacker et al.*, 2020, S. 51 f.

Beförderungswesen (Schienen, Straßen, Wasserstraßen, Luftverkehr), Geld- und Kreditversorgung (mit dem verbindlichen Auftrag zur Leistungserbringung an die Sparkassen), Telekommunikation/Internet und Wohnungswirtschaft.[6]

Um auf eine Nettostichprobe von 5000 befragten Unternehmen nahezu aller Wirtschaftszweige (WZ08-A bis S) zu kommen, wurden 43219 Unternehmen nach diesem Stratifizierungsplan gezogen (Bruttostichprobe) und kontaktiert. Die Teilnahmequote liegt demnach bei 11,6 %.

3.2.2 Durchführung

Die CATI-Befragung wurde durch das Umfrageinstitut Kantar Emnid zwischen August 2018 und Januar 2019 durchgeführt (Informationen zur Zusammensetzung der Stichprobe siehe unten). Dazu wurden zunächst die ausgewählten Unternehmen telefonisch kontaktiert, über die Studie mit einem Begleitschreiben des BMWi informiert und eine geeignete Interviewperson des jeweiligen Unternehmens identifiziert. Dabei sollte es sich um eine Person handeln, die für die IT- und Informationssicherheit verantwortlich ist. Dies bedeutet, dass es sich bei den ausgewählten Personen sowohl um IT-Beschäftigte als auch um die Geschäftsführung oder andere Mitarbeiter handeln kann (siehe Stichprobenbeschreibung). Im Fall einer Teilnahmebereitschaft wurde im weiteren Verlauf ein Interviewtermin ausgemacht. Die Unternehmen hatten die Möglichkeit, die Befragung zu unterbrechen und zu einem späteren Zeitpunkt fortzusetzen. Ferner konnten sich die Unternehmen über die Befragung auf der Seite des Kriminologischen Forschungsinstituts Niedersachsen e.V. und des Bundesministeriums für Wirtschaft und Energie informieren. Bei Interesse konnte der Fragebogen vorab eingesehen werden.

Nach Erreichung der Nettostrichprobe von 5000 befragten Unternehmen wurde der Datensatz an das Kriminologische Forschungsinstitut Niedersachsen e.V. übermittelt und dort mittels der Statistiksoftware SPSS ausgewertet. Um repräsentative Aussagen für alle Unternehmen ab zehn Mitarbeitern in Deutschland treffen zu können, wurde ein Gewichtungsfaktor genutzt, sodass hinsichtlich der Schichtungsmerkmale Beschäftigtengrößenklasse und Wirtschaftszweig im Vergleich zur Auswahlgesamtheit und damit näherungsweise zur Grundgesamtheit keine Hinweise auf eine Verzerrung erkennbar sind.

3.2.3 Stichprobenbeschreibung

Die meisten befragten Personen waren Mitarbeiter im Bereich der IT- und Informationssicherheit (ungewichtet: 69,8 %). Bei weiteren 23,5 % handelte es sich um Personen aus der Geschäftsführung bzw. dem Vorstand. 6,8 % der Befragten waren Datenschutzbeauftragte. Selten handelte es sich um Mitarbeiter aus den Bereichen Revision und Prüfung (2,1 %) oder Werkssicherheit (1,1 %). 8,1 % der Befragten kamen aus anderen als den genannten Bereichen.

Die Zusammensetzung der ungewichteten und gewichteten Nettostichprobe nach Beschäftigtengrößenklassen sowie nach der Zugehörigkeit zum Bereich

6 Zum Kanon der Daseinsvorsorge siehe *Schäfer*, 2018. Eine detaillierte Auflistung der Wirtschaftszweigklassen (WZ08-Klassen), die in dieser Studie dem Bereich der Daseinsvorsorge zugeordnet wurden, finden sich bei *Dreißigacker et al.*, 2020, S. 171 f.

der Daseinsvorsorge findet sich in Tabelle 1. Bezogen auf die Unternehmensgröße ist zu erkennen, dass die kleinen Unternehmen in der gewichteten Stichprobe wie in der Grundgesamtheit den größten Anteil bilden und dementsprechend stark die Ergebnisse für alle Unternehmen insgesamt beeinflussen. Dies ist bei der Interpretation der Gesamtergebnisse zu beachten.

Tabelle 1: Stichprobe nach Beschäftigtengrößenklassen und dem Merkmal Daseinsvorsorge

	disproportional geschichtete Stichprobe		
	ungewichtet		gewichtet
Beschäftigtengrößenklassen	Anzahl	Prozent	Prozent
10-49 Besch.	1.190	23,8	79,1
50-99 Besch.	1.181	23,6	10,5
100-249 Besch.	1.120	22,4	6,5
250-499 Besch.	1.005	20,1	2,2
ab 500 Besch.	504	10,1	1,8
Gesamt	5.000	100,0	100,0
Unternehmen der Daseinsvorsorge			
ja	847	16,9	11,2
nein	4.153	83,1	88,8
Gesamt	5.000	100,0	100,0

Unternehmen der Daseinsvorsorge sind in der ungewichteten Gesamtstichprobe mit einem Anteil von 16,9 % (n=847) enthalten. Davon gehören die meisten zu den Wirtschaftszweigen Verkehr und Lagerei (31,3 %), Erbringung von Finanz- und Versicherungsdienstleistungen (16,2 %), Gesundheits- und Sozialwesen (14,6 %), Grundstücks- und Wohnungswesen (11,9 %) und Wasserversorgung, Abwasser- und Abfallentsorgung und Beseitigung von Umweltverschmutzungen (10,5 %). Seltener sind die Bereiche Energieversorgung (8,0 %), Erziehung und Unterricht (4,5 %), Öffentliche Verwaltung, Verteidigung, Sozialversicherung (2,2 %) sowie Information und Kommunikation (0,7) vertreten. Ob die Unternehmen der Daseinsvorsorge einen kommunalen Träger haben, wurde nicht erhoben und kann daher nicht differenziert abgebildet werden.

3.3 Ergebnisse

Im Folgenden werden ausgewählte Ergebnisse der Befragung dargestellt. Dabei wird zunächst auf die Verbreitung von Cyberangriffen eingegangen sowie auf dessen Folgen für die betroffenen Unternehmen. Ferner wird erläutert, inwiefern Unternehmen sich vor Cyberangriffen schützen und wie wirksam verschiedene Präventionsmaßnahmen sind. Abschließend wird auf das Bewusstsein bezüglich des Risikos, von Cyberkriminalität betroffen zu werden eingegangen.

3.3.1 Verbreitung von Cyberkriminalität

Die Unternehmen wurden gefragt, welche der folgenden acht bzw. neun Arten von Cyberangriffen sie jemals bzw. innerhalb der letzten zwölf Monate erlebt haben (Näheres zu den Bedrohungsformen siehe Kapitel 1 im vorliegenden Band):

1. Ransomware-Angriff
   Hierbei handelt es sich um einen Schadsoftware-Angriff, bei dem Daten des betroffenen Unternehmens verschlüsselt werden, sodass diese nicht mehr abgerufen werden können. Häufig wird anschließend für eine in Aussicht gestellte Entschlüsselung der Daten ein Lösegeld (meist in Form einer Kryptowährung, z. B. Bitcoin, siehe dazu auch Kapitel 15 im vorliegenden Handbuch) gefordert.
2. Spyware-Angriff
   Bei dieser Art von Schadsoftware-Angriff versuchen die Täter, möglichst unbemerkt an sensible Unternehmensdaten oder Nutzeraktivitäten zu gelangen. Nach einer erfolgreichen Identifizierung und Ausschleusung der Daten werden häufig die Spuren verwischt. Diese Angriffsart kann z. B. zur Produktspionage oder zur Vorbereitung anderer Cyberangriffe dienen.
3. Sonstiger Schadsoftware-Angriff
   Unter diese Sammelkategorie fallen Schadsoftware-Angriffe mit Viren, Würmern, Trojanern, Rootkits und Scareware (exklusive Ransomware und Spyware), die z. B. zur Manipulation oder Zerstörung von Daten und Informationssysteme dienen.
4. Angriff durch manuelles Hacking
   Manuelles Hacking steht für eine nicht autorisierte Manipulation von Hard- und Softwareeinstellungen von Computern ohne den Einsatz von Schadsoftware. Ziel eines unautorisierten Hackers (z. T. auch als Cracker oder Blackhat bezeichnet) könnte es z. B. sein, illegitime Einsicht in Unternehmensdaten zu erlangen, diese zu entwenden, Unternehmen zu sabotieren oder einen anderen Cyberangriff vorzubereiten.
5. (D)DoS-Angriff
   Ein Denial-of-Service- oder kurz DoS-Angriff zielt auf die mutwillige Überlastung von Web- oder E-Mail-Server von Unternehmen durch massenhafte Anfragen oder E-Mail-Sendungen. Damit stehen diese für den regulären Betrieb nicht mehr zur Verfügung. Wird dieser Angriff durch den Zusammenschluss der Rechenleistung mehrerer verteilter IT-Systeme durchgeführt (Botnetze, siehe dazu Kapitel 1 im vorliegenden Band), um mögliche Schutzmaßnahmen zu überwinden, wird dies als Distributed Denial-of-Service- oder kurz DDoS-Angriff bezeichnet. Solche Angriffe können z. B. auf die Sabotage von Unternehmen durch temporäre Betriebsunterbrechung abzielen und/oder mit einer Erpressung verbunden sein.
6. Defacing-Angriff
   Unter Defacing-Angriffen werden unautorisierte Manipulationen von Inhalten der Webpräsenz oder ganzer Webseiten von Unternehmen gefasst. Diese können der Sabotage dienen oder im Zusammenhang mit anderen Angriffsarten stehen, z. B. zur Einschleusung von Schadprogrammen oder

zur Täuschung der Besucher der Webseite, um an deren persönliche Daten zu gelangen (siehe Phishing-Angriff).

7 CEO-Fraud (Chefbetrug)
Der CEO-Fraud ist eine Form des Betruges, bei der unter Verwendung einer falschen Identität einer weisungsbefugten Person des Unternehmens, z. B. der des CEO (Chief Executive Officer), andere Mitarbeiter meist mit fingierten E-Mails zu bestimmten Handlungen verleitet werden sollen (Social Engineering). Dabei kann es z. B. um eine vermeintlich dringende finanzielle Transaktion zum Abschluss eines geheimen Geschäftes oder die Umleitung einer regulären Transaktion auf ein anderes Konto gehen. Diese Angriffsart ist häufig gut vorbereitet und nutzt interne Informationen des Unternehmens, z. B. über bestimmte Geschäfts- und Kommunikationsabläufe, beteiligte Personen und deren Abwesenheitszeiten, aus, die möglicherweise aus anderen Cyberangriffen stammen.

8. Phishing-Angriff
Phishing-Angriffe gegen Unternehmen zielen insbesondere darauf ab, an sensible Unternehmensdaten, z. B. Zugangsdaten, Passwörter, Daten von Bankkonten oder Kreditkartendaten, zu gelangen. Dazu werden häufig manipulierte Webseiten oder gefälschte E-Mails eingesetzt, um Mitarbeiter *so zu täuschen, dass sie diese preisgeben (Social Engineering). Die Kenntnis solcher Daten eröffnet den Tätern* viele andere Angriffsmöglichkeiten, z. B. Manipulation und Umleitung von Transaktionsvorgängen oder Identitätsdiebstahl zur Täuschung Dritter (siehe CEO-Fraud).

9. Sonstiger Cyberangriff

Ferner wurde gefragt, ob das Unternehmen von anderen als den aufgeführten Angriffsarten betroffen wurde, um der Vielfältigkeit der Bedrohungsformen gerecht zu werden.

Um nicht durch die Angabe von niedrigschwelligen Angriffen, wie beispielsweise einer Spam-Mail, das Gesamtergebnis zu verzerren, wurden die Unternehmen gefragt, inwiefern sie einen solchen der dargestellten Angriffe erlebt haben, auf den reagiert werden musste, um Schaden ganz oder teilweise abzuwenden. Dabei kam es darauf an, dass aktiv reagiert werden musste und nicht nur eine automatische Filterung durch ein Schutzprogramm erfolgte. Bei den so erfassten Angriffen kann es sich jedoch auch um einen Angriffsversuch handeln.

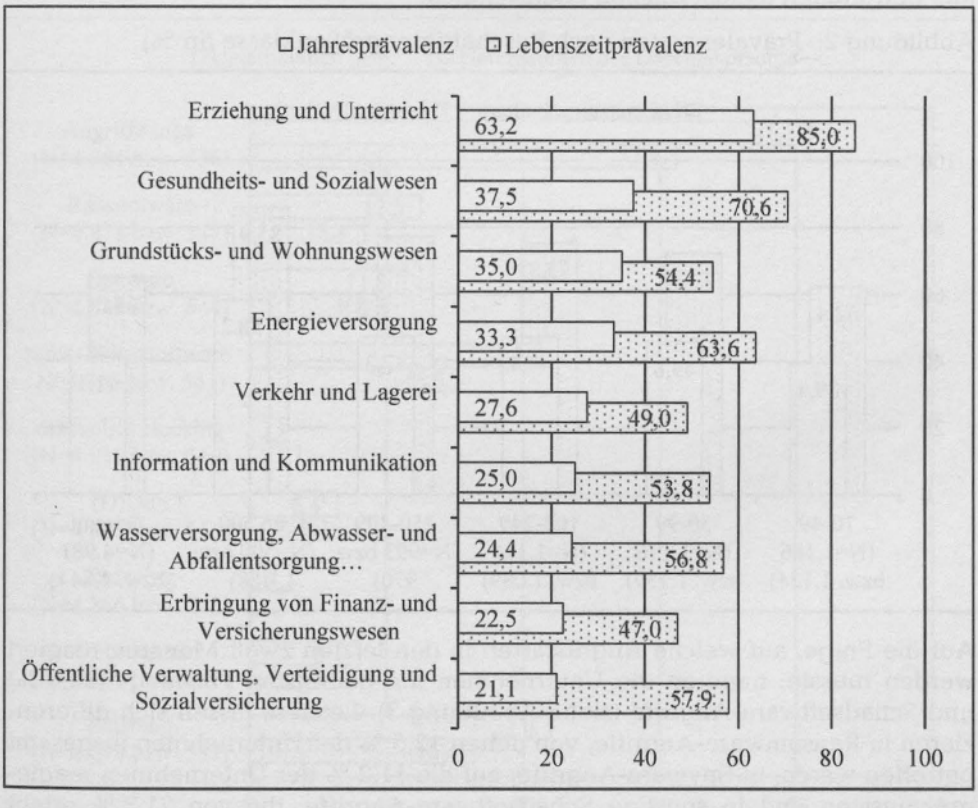
Insgesamt gaben 41,1 % (N=4.981) der befragten Unternehmen an, in den letzten zwölf Monaten mindestens einen der aufgeführten Angriffe erlebt zu haben (so genannte Jahresprävalenz). Von diesen betroffenen Unternehmen berichtete wiederum mehr als die Hälfte (57,2 %) von mehreren erlebten Angriffsarten in den letzten zwölf Monaten. Danach gefragt, ob jemals seit Unternehmensgründung solche Cyberangriffe erfolgten, bejahten dies 65,0 % der Unternehmen (so genannte Lebenszeitprävalenz).

Von den Unternehmen der Daseinsvorsorge gaben 31,1 % an, innerhalb der letzten zwölf Monate mindestens einen Cyberangriff erlebt zu haben (siehe Abbildung 1). Hierunter trafen es besonders Unternehmen der Wirtschaftszweige Erziehung und Unterricht (63,2 %), Gesundheits- und Sozialwesen (37,5 %), Grundstücks- und Wohnungswesen (35,0 %) sowie Energieversor-

gung (33,3 %). Verkehr und Lagerei (27,6 %), Information und Kommunikation (25,0 %), Wasserversorgung, Abwasser- und Abfallentsorgung und Beseitigung von Umweltverschmutzungen (24,4 %) sowie Erbringung von Finanz- und Versicherungswesen (22,5 %), öffentliche Verwaltung, Verteidigung und Sozialversicherung (21,1 %). Allerdings sei bei dieser Differenzierung darauf hingewiesen, dass die Anteile der einzelnen Bereiche der Daseinsvorsorge zum Teil recht klein sind (siehe Stichprobenbeschreibung).

In Bezug auf die Betroffenheit von Cyberangriffen seit Unternehmensgründung zeigte sich ebenfalls, dass die Wirtschaftszweige Erziehung und Unterricht sowie Gesundheits- und Sozialwesen stärker betroffen sind als andere. Ferner lässt sich erkennen, dass z. B. Energieversorger im Vergleich zur Betroffenheit der letzten zwölf Monate in der weiteren Vergangenheit relativ stark betroffen waren. Möglicherweise wurde hier die IT-Sicherheit in der letzten Zeit erhöht. Dies trifft ebenfalls auf den Bereich der öffentlichen Verwaltung, Verteidigung und Sozialversicherung zu, wobei die zugrundeliegende geringe Fallzahl die Aussagekraft dieser Ergebnisse stark einschränkt.

Abbildung 1: Prävalenzrate der letzten zwölf Monate sowie seit Unternehmensgründung nach Wirtschaftszweigen (WZ08 Ebene 1; in %; nur Unternehmen der Daseinsvorsorge)

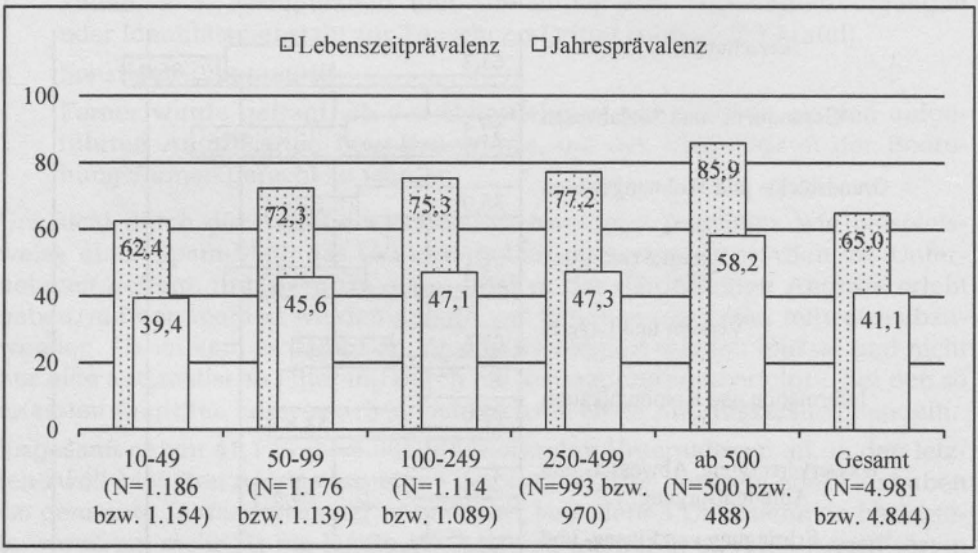


Im Hinblick auf die Beschäftigtengrößenklassen zeigt sich, dass auch kleinere Unternehmen von Cyberkriminalität betroffen sind, wenngleich dies auf größe-

re häufiger zutrifft (siehe Abbildung 2). Sowohl bezogen auf die Jahresprävalenz als auch auf die Lebenszeitprävalenz sind statistisch signifikante Unterschiede zwischen den großen (ab 500 Mitarbeitern) und den mittleren Unternehmen (50 bis 499 Mitarbeiter) sowie zwischen den mittleren und den kleinen Unternehmen (zehn bis 49) zu erkennen. Ähnliche Größenunterschiede auf einem etwas niedrigeren Niveau sind auch bei den Unternehmen der Daseinsvorsorge festzustellen.

Diese Befunde könnten zum einen darauf hinweisen, dass das Cyberangriffsrisiko einer Organisation mit der Anzahl der Mitarbeiter steigt. Gleichzeitig könnte dies mit der damit verbundenen größeren IT-Infrastruktur zusammenhängen. Beide Aspekte erhöhen die Angriffsfläche für unterschiedliche Cyberangriffsarten. Abgesehen von diesen Überlegungen könnten die Unterschiede jedoch auch dadurch zustande kommen, dass größere Unternehmen durch eigene IT-Abteilungen und spezialisierte IT-Mitarbeiter Cyberangriffe häufiger erkennen und somit auch häufiger bei der Befragung angaben. Diese Hypothese lässt sich jedoch nur auf Angriffsarten beziehen, deren Folgen nicht immer erkennbar bzw. auf einen Cyberangriff rückführbar sind wie beispielsweise Spyware-Angriffe oder bestimmte Arten von Schadsoftware-Angriffen, denn die Folgen von Ransomware-Angriffen oder CEO-Fraud (Chefbetrug) sind für alle Betroffenen gleichermaßen offensichtlich.

Abbildung 2: Prävalenzraten nach Beschäftigtengrößenklasse (in %)

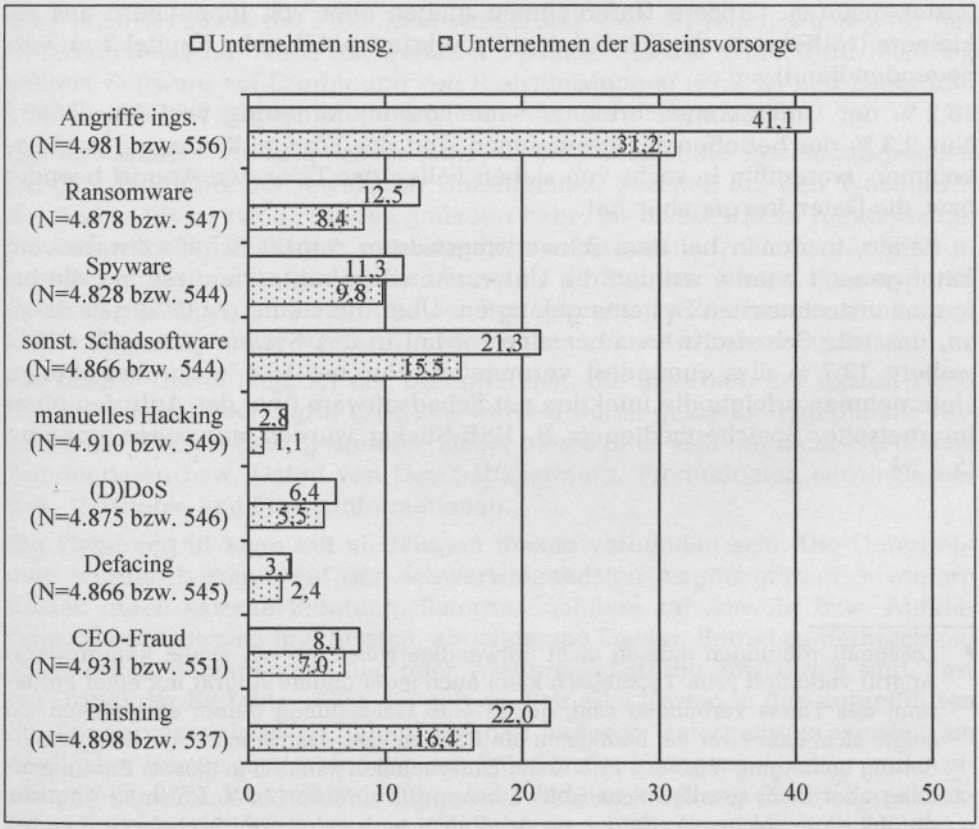


Auf die Frage, auf welche Angriffsarten in den letzten zwölf Monaten reagiert werden musste, nannten die Unternehmen am häufigsten Phishing- (22,0 %) und Schadsoftware-Angriffe (siehe Abbildung 3). Letztere lassen sich differenzieren in Ransomware-Angriffe, von denen 12,5 % der Unternehmen insgesamt betroffen waren, in Spyware-Angriffe, auf die 11,3 % der Unternehmen reagieren mussten und in sonstige Schadsoftware-Angriffe, die von 21,3 % erlebt wurden. Die übrigen Angriffsarten scheinen demgegenüber eine etwas kleine-

re Rolle zu spielen (CEO-Fraud: 8,1 %; (D)DoS: 6,4 %; Defacing: 3,1 %; manuelles Hacking: 2,8 %). Bezogen auf die spezielle Gruppe der Unternehmen der Daseinsvorsorge stellt sich diese Verteilung auf einem etwas niedrigeren Niveau sehr ähnlich dar.

Wenn die eben angeführte Hypothese zuträfe, dass große Unternehmen aufgrund eigener IT-Abteilungen Cyberangriffe häufiger feststellen als kleine Unternehmen ohne spezialisierte IT-Mitarbeiter bzw. Abteilungen, dann müsste sich dies insbesondere bei Spyware- und sonstigen Schadsoftwareangriffen in entsprechenden Größenunterschieden abzeichnen. Interessanterweise waren aber gerade bei diesen Angriffsarten keine statistisch relevanten Unterschiede zwischen den Jahresprävalenzraten der unterschiedlichen Größenklassen erkennbar. Demgegenüber zeigten sich deutliche Größenunterschiede bei Ransomware-Angriffen, beim CEO-Fraud als auch bei Phishing-Angriffen. So berichten z. B. nur 20,6 % der Unternehmen mit zehn bis 49 Mitarbeitern, aber 33,7 % der Unternehmen mit mehr als 500 Mitarbeitern von Phishing-Angriffen. Noch deutlicher ist der Prävalenzunterschied beim CEO-Fraud, den 6,1 % der kleinen, aber 29,2 % der großen Unternehmen mindestens einmal in den letzten zwölf Monaten erlebten.

Abbildung 3: Jahresprävalenzraten nach Angriffsart (in %)



Die Unternehmen wurden des Weiteren gefragt, ob ihnen einer der genannten Angriffe angedroht wurde. Dies bestätigte allerdings nur ein sehr kleiner Anteil von 3,9 % (N=4.982), wobei es bei 44,1 % dieser Unternehmen bei der bloßen Drohung blieb.

3.3.2 Schwerwiegendster Angriff

Um weitere detaillierte Angaben zu Cyberangriffen zu erhalten, wurden die befragten betroffenen Unternehmen aufbauend zu den dargestellten Basisangaben ausführlich zu dem Angriff befragt, der für das Unternehmen der schwerwiegendste in den letzten zwölf Monaten war. Hierbei handelte es sich am häufigsten um Phishing- (26,0 %), Schadsoftware- (23,5 %) sowie Ransomware-Angriffe (22,3 %). Zu den schwerwiegendsten Angriffen gehörten selten Spyware- (8,0 %), (D)DoS- (7,4 %) und CEO-Fraud-Vorfälle (7,2 %). Nur vereinzelt wurden manuelles Hacking (3,5 %), Defacing (2,7 %) oder eine sonstige Angriffsform (0,7 %) genannt.

Bezogen auf den Angriff, der für das jeweilige Unternehmen der schwerwiegendste war, hatten nur 30,7 % eine Vermutung dahingehend, wer der Täter sein könnte. Hiervon äußerten 4,4 %, dass es sich bei dem Täter um einen ehemaligen Mitarbeiter handelt. Weitere 6,1 % vermuten Mitbewerber und 1,8 % Geschäftspartner hinter der Tat, wozu z. B. auch Lieferanten und Dienstleister gehören. Größere Unternehmen gingen eher von Innentätern aus als kleinere (Näheres zu den Tätern von Cyberkriminalität siehe Kapitel 2 im vorliegenden Band).

18,2 % der Unternehmen erhielten eine Lösegeldforderung von dem Täter.[7] Nur 2,3 % der betroffenen Unternehmen sind der Lösegeldforderung nachgekommen, woraufhin in sechs von sieben Fällen der Täter den Angriff beendet bzw. die Daten frei gegeben hat.

In Fällen, in denen bei dem schwerwiegendsten Angriff Schadsoftware vom Täter genutzt wurde, wurden die Unternehmen gefragt, wie diese auf die informationstechnischen Systeme gelangten. Über die Hälfte (74,0 %) gab dabei an, dass die Schadsoftware über eine E-Mail in das System gelangte, wobei weitere 13,7 % dies zumindest vermuteten. Nur bei 16,4 % der betroffenen Unternehmen erfolgte die Infektion mit Schadsoftware über das Aufrufen einer Internetseite. Speichermedien (z. B. USB-Sticks) wurden nur selten genannt (5,2 %).

---

7 Lösegeldforderungen müssen nicht notwendigerweise nur mit einem Ransomware-Angriff verknüpft sein. Theoretisch kann auch jeder andere Angriff mit einer Forderung des Täters verbunden sein, gegen eine Geldzahlung diesen einzustellen. So zeigte sich, dass zwar am häufigsten ein Ransomware-Angriff mit einer Lösegeldforderung einherging (68,3 %), 12,5 % der Unternehmen nannten in diesem Zusammenhang aber auch sonstige Schadsoftware-Angriffe und bei 7,5 % Phishing-Angriffe, die mit einer solchen Aufforderung des Täters verbunden war (Mehrfachantworten waren möglich).

3.3.2.1 Folgen

Bezüglich der Folgen des schwerwiegendsten Cyberangriffs der letzten zwölf Monate wurden die betroffenen Unternehmen u. a. gefragt, welche informationstechnischen Systeme infolge nicht bzw. nur noch stark eingeschränkt genutzt werden konnten. Bei 54,5 % der Unternehmen traf dies auf E-Mail- und sonstige Kommunikationssysteme zu. Ein Viertel (25,4 %) waren in der Auftrags- und Kundenverwaltung stark eingeschränkt, wobei bei einem ähnlichen großen Anteil (22,0 %) das Rechnungswesen und Controlling betroffen waren. Seltener wirkte sich der Angriff auf den Webauftritt (14,6 %) und weitere Software zur Erbringung von Dienstleistungen (11,7 %) aus. Zu einem geringen Anteil waren informationstechnische Systeme im Zusammenhang mit Banking und Trading (9,4 %), Lager und Logistik (8,0 %) und Produktionssteuerung (5,3 %) betroffen.

Da verschiedene informationstechnische Systeme unterschiedlich wichtig für ein Unternehmen sein können und somit die Folgen unterschiedlich gravierend, wurden die Unternehmen bezogen auf den schwerwiegendsten Angriff gefragt, wie wichtig das jeweilig betroffene System für das Unternehmen ist. Mit Zustimmungswerten über 90,0 % gaben Unternehmen dabei an, dass E-Mail und Kommunikationssysteme (92,7 %), Auftrags- und Kundenverwaltung (95,3 %), Rechnungswesen und Controlling (93,4 %), Banking und Trading (92,6 %) sowie die Produktionssteuerung (94,1 %) (eher) wichtig für das Unternehmen sind. Auch die weiteren Systeme wie der Webauftritt (68,0 %), weitere Software zur Erbringung von Dienstleistungen (87,7 %) und Lager und Logistik (85,3 %) zeigten sich in großem Anteil als (eher) wichtig.

Gefragt danach, wie lang das als (eher) wichtig eingestufte System ausgefallen ist, gab die Hälfte der jeweiligen Unternehmen bezogen auf den Webauftritt an, dass es bis zu zwölf Stunden gedauert habe, bis dieser wieder funktionierte, die andere Hälfte berichtete von einer höheren Stundenanzahl. Bei der Produktionssteuerung musste die Hälfte länger als 48 Stunden warten. Alle anderen Systeme brauchten bei der Hälfte der Befragten bis zu 24 Stunden, die andere Hälfte länger, bis diese wieder wie vorgesehen genutzt werden konnten.

Bei einem Viertel (25,2 %) der Unternehmen, die innerhalb der letzten zwölf Monate einen Cyberangriff erlebten, wurden Daten gelöscht, manipuliert, verschlüsselt, kopiert bzw. gestohlen. Dabei handelte es sich um nicht-öffentliche Kundendaten bzw. Daten von Geschäftspartnern, Produktdaten sowie Strategie-, Vertriebs- und Finanzinformationen.

Ein Cyberangriff kann mit vielfältigen Kosten verbunden sein. Die Unternehmen wurden bezogen auf den schwerwiegendsten Angriff gefragt, inwiefern Kosten durch externe Beratung, Sofortmaßnahmen zur Abwehr bzw. Aufklärung, Schadensersatz und Strafen, abgeflossene Gelder, Betriebsunterbrechung sowie durch Wiederherstellung oder Wiederbeschaffung entstanden sind. Fast ein Drittel der Befragten (30,0 %) gab an, keinerlei Kosten in den aufgeführten Positionen verzeichnet zu haben. Bei den anderen Unternehmen wurden am häufigsten Kosten in Verbindung mit Sofortmaßnahmen zur Abwehr und Aufklärung (39,9 %), Wiederherstellung und Wiederbeschaffung (33,0 %) sowie externe Beratung (30,3 %) genannt. Für letzteres entstanden vor allem kleineren

Unternehmen deutlich häufiger Kosten als größeren; ebenso verhält es sich bei Kosten durch Betriebsunterbrechungen. Sofortmaßnahmen zur Abwehr und Aufklärung waren v. a. für kleine und große Unternehmen mit Kosten verbunden, weniger jedoch für Unternehmen mit 100 bis 429 bzw. mit 250 bis 499 Mitarbeitern.

Der Forschungsstand zur Höhe der Kosten von Cyberangriffen ist überschaubar und durch wenig verlässliche Daten gekennzeichnet. Dies liegt an verschiedenen Schwierigkeiten. Zum einen können neben direkten Kosten, die unmittelbar infolge des Cyberangriffs entstehen (z. B. abgeflossenen Geldern, Kosten für Sofortmaßnahmen zur Abwehr und Aufklärung, externe Beratung, Kosten durch Betriebsunterbrechung, Wiederherstellung/Wiederbeschaffung, Schadensersatz/Strafen u. a.), auch indirekte Kosten verursacht werden, die möglicherweise erst Monate später erkennbar werden (z. B. Imageverluste, Wettbewerbsnachteile durch Patentdatenverlust u. a.). Neben der teilweise eingeschränkten Bereitschaft von Unternehmen, hierüber Auskunft zu geben, kommt bei deren Erhebung erschwerend hinzu, dass selbst direkte Kosten nicht immer von den Unternehmen erfasst und vorgehalten werden. So konnten 30,9 % der Unternehmen, bei denen direkte Kosten durch den schwerwiegendsten Cyberangriff entstanden sind, keine vollständigen Angaben zur Höhe machen. Andererseits sind die getätigten Angaben eher als Schätzungen zu betrachten und weniger als belastbare Zahlen. Die Gesamtkosten, die nur berechnet wurden, wenn alle Angaben zu den einzelnen Kostenpositionen vorhanden waren, bewegten sich bei den Unternehmen zwischen 10 Euro und 2 Millionen Euro, wobei der Durchschnitt bei 16900 Euro liegt. Da in diesem Kontext Extremwerte die Aussagekraft eines Durchschnittwerts beeinflussen, wurde ferner auch der so genannte Median berechnet. Dieser gibt an, bis zu welcher Höhe sich die Kosten bei der Hälfte der jeweiligen Befragten beliefen. Bei 50 % der Befragten, die Angaben zu den direkten Kosten machten, waren diese bis zu 1000 Euro hoch, bei der anderen Hälfte lagen die direkten Kosten über diesem Wert.

3.3.2.2 Anzeigeverhalten

Ferner wurden die Unternehmen gefragt, ob sie den für sie schwerwiegendsten Angriff der Polizei bzw. den Strafverfolgungsbehörden angezeigt haben. Lediglich 11,9 % der Unternehmen insgesamt zeigten den schwerwiegendsten Cyberangriff der letzten zwölf Monate polizeilich an. Zwar erstatten Unternehmen der Daseinsvorsorge mit 21,0 % häufiger Anzeige als Unternehmen der übrigen Wirtschaftszweige mit 11,1 %, aber von der überwiegenden Mehrheit der Cyberangriffe erlangen die Strafverfolgungsbehörden demnach keine Kenntnis. Zu den am häufigsten angezeigten Angriffsarten zählen CEO-Fraud (24,6 %), Spyware (19,7 %) und manuelles Hacking (19,4 %). Demgegenüber zeigen Unternehmen Angriffe mit sonstiger Schadsoftware und Defacing am seltensten an (4,4 % bzw. 6,4 %).

Als Grund für die Nichtanzeige nannten die Unternehmen am häufigsten die fehlende Aussicht auf einen Ermittlungserfolg (72,0 %). Zwar ist diese Einschätzung nicht verkehrt, denn lediglich in 7,7 % der berichteten angezeigten Cyberangriffe konnte die Polizei nach Kenntnis der Unternehmen tatverdächtige Personen ermitteln. Dennoch ist die Anzeige von Cyberangriffen sinnvoll,

denn ohne diese Kenntnis können die Strafverfolgungsbehörden kaum fundierte Lageeinschätzungen treffen, Veränderungen erkennen und das Problembewusstsein in Politik und Gesellschaft erhöhen. Ähnlich scheint dies ein Großteil der Unternehmen zu sehen, die eine Anzeige erstattet hat. Auch wenn nur etwa die Hälfte dieser Unternehmen mit der Arbeit der Polizei insgesamt (eher) zufrieden ist (52,2 %), würden fast alle (93,7 %) anderen Unternehmen die Anzeige (eher) empfehlen. Hinzu kommt das anzeigeermutigende Ergebnis, dass die Ermittlungsarbeit der Polizei lediglich bei einem kleinen Anteil von 9,6 % der angezeigten Fälle den Betriebsablauf der anzeigenden Unternehmen (eher) gestört hat.

Ein weiterer von 20,7 % und damit relativ häufig genannter Nichtanzeigegrund ist die Unsicherheit von Unternehmen, an wen genau sie sich für eine Anzeige wenden müssen. Dies weist auf einen zusätzlichen Informationsbedarf und gleichzeitig auf eine Möglichkeit hin, die Anzeigequote zu erhöhen.

3.3.3 Verbreitung und Wirksamkeit von Schutzmaßnahmen

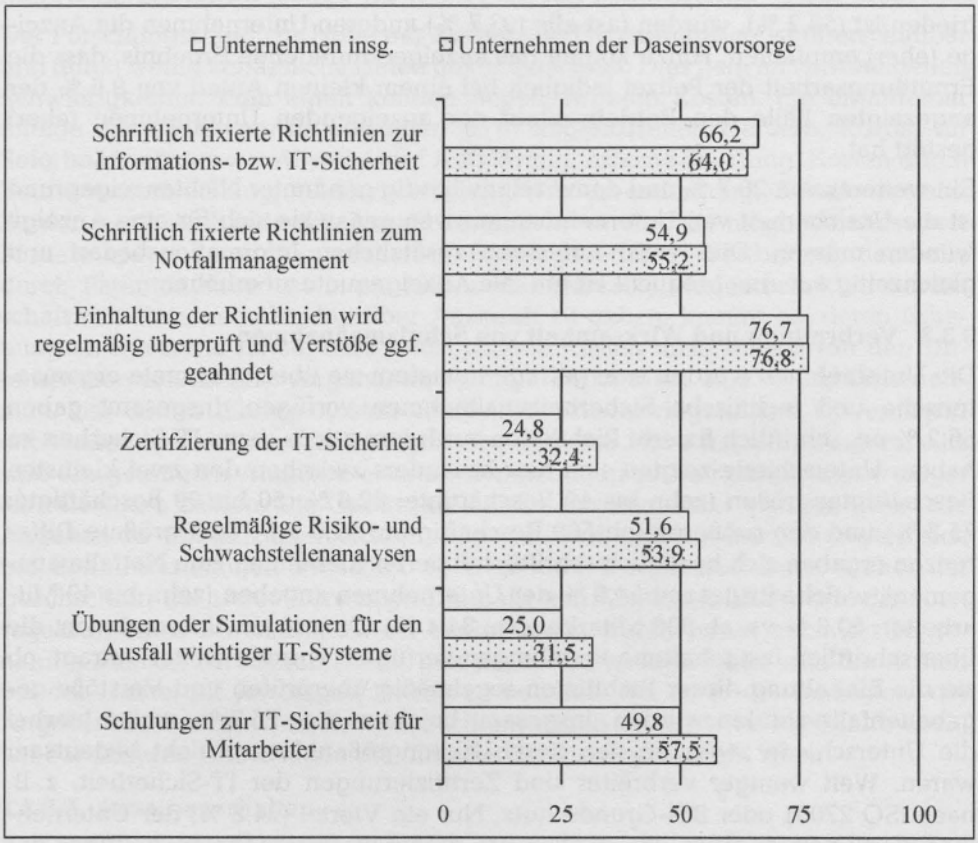
Die Unternehmen wurden u. a. gefragt, inwiefern sie über bestimmte organisatorische und technische Sicherheitsmaßnahmen verfügen. Insgesamt gaben 66,2 % an, schriftlich fixierte Richtlinien zur Informations- bzw. IT-Sicherheit zu haben. Unterschiede zeigten sich hier besonders zwischen den zwei kleinsten Beschäftigtengrößen (zehn bis 49 Beschäftigte: 62,6 %; 50 bis 99 Beschäftigte: 75,3 %) und den größeren (ab 500 Beschäftigten: 92,0 %). Noch größere Differenzen ergaben sich bezüglich schriftlich fixierter Richtlinien zum Notfallmanagement, welche insgesamt 54,9 % der Unternehmen angaben (zehn bis 49 Mitarbeiter: 50,6 % vs. ab 500 Mitarbeitern: 84,4 %). Diejenigen Unternehmen, die über schriftlich festgehaltene Regelungen verfügen, wurden weiter gefragt, ob sie die Einhaltung dieser Richtlinien regelmäßig überprüfen und Verstöße gegebenenfalls ahnden würden. Insgesamt bejahten dies 76,7 %, wobei hierbei die Unterschiede zwischen den Beschäftigtengrößenklassen nicht bedeutsam waren. Weit weniger verbreitet sind Zertifizierungen der IT-Sicherheit, z. B. nach ISO 27001 oder BSI-Grundschutz. Nur ein Viertel (24,8 %) der Unternehmen verfügten darüber, wobei dies bei größeren Unternehmen häufiger der Fall war.

Regelmäßige Risiko- und Schwachstellenanalysen führt die Hälfte der Unternehmen (51,6 %) durch, wobei hier die drei größten Beschäftigtengrößenklassen dies häufiger angaben als die zwei kleineren Gruppierungen. Ein Viertel der befragten Unternehmen (25,0 %) führen Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme durch. Hierbei zeigt sich ein großer Unterschied an Unternehmensgröße: Unternehmen mit mehr als 500 Mitarbeitern gaben dies in über der Hälfte der Fälle (56,6 %) an, kleinere Unternehmen mit zehn bis 49 Mitarbeitern hingegen nur zu 21,5 % und solche mit 50 bis 99 Mitarbeitern zu 30,4 % an. Schulungen für Mitarbeiter zum Thema IT-Sicherheit waren demgegenüber verbreiteter mit insgesamt 49,8 %, wobei sich auch hier eine höhere Verbreitung nach Anzahl der Mitarbeiter zeigte.

Mit Blick auf die Unternehmen der Daseinsvorsorge (siehe Abbildung 4) ist vor allem erkennbar, dass diese anteilig häufiger eine zertifizierte IT-Sicherheit haben, häufiger Übungen oder Simulationen für den Ausfall wichtiger IT-Sys-

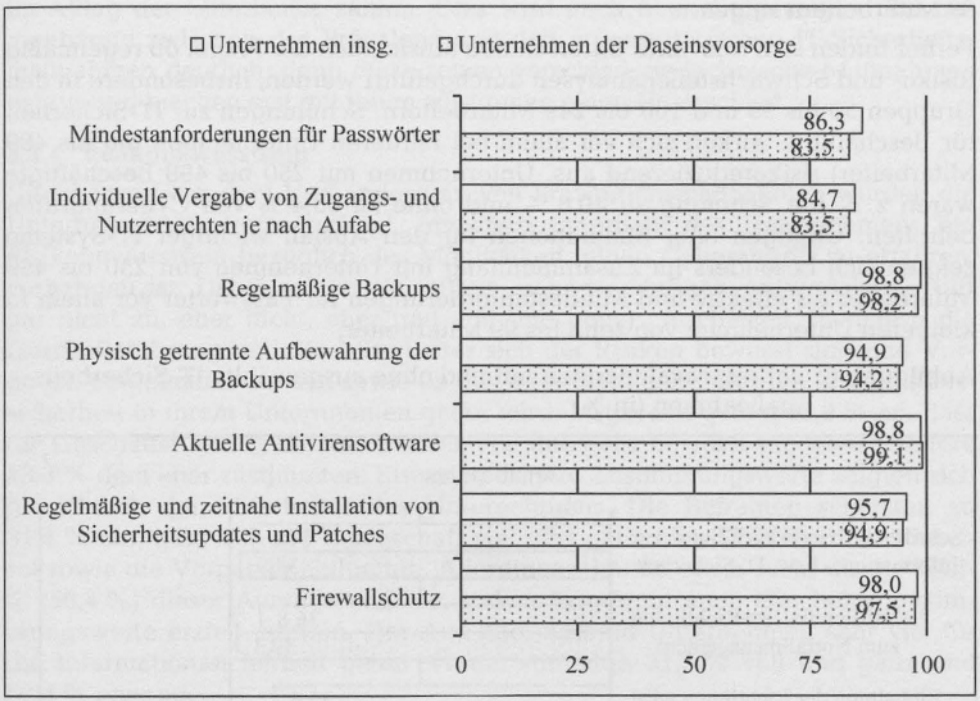
teme sowie Schulungen zur IT-Sicherheit für die Mitarbeiter durchführen. Dies könnte ein Grund für die vergleichsweise geringe Prävalenzrate im Vergleich zu Unternehmen der übrigen Wirtschaftszweige sein.

Abbildung 4: Verbreitung organisatorischer IT-Sicherheitsmaßnahmen (in %)



Bezüglich der Nutzung von technischen Sicherheitsmaßnahmen deuten die Ergebnisse auf einen sehr hohen Verbreitungsgrad hin (siehe Abbildung 5). Dies gilt sowohl für Unternehmen insgesamt als auch für Unternehmen der Daseinsvorsorge im Speziellen. Während regelmäßige Backups von allen Beschäftigtengrößenklassen gleichermaßen zu einem sehr hohen Anteil durchgeführt werden, zeigen sich kleinere, aber signifikante Unterschiede bei der Mindestanforderung für Passwörter, welche bei größeren Unternehmen häufiger vorliegen. Die individuelle Vergabe von Zugangs- und Nutzerrechten je nach Aufgabe wird nur von den kleinen Unternehmen mit zehn bis 49 Mitarbeitern mit 82,0 % etwas weniger durchgeführt als bei den anderen, welche alle Werte über 90,0 % aufweisen. Bezüglich der Frage, ob die Aufbewahrung der Backups physisch getrennt werden, zeigen sich nur kleinere signifikante Utnerschiede zwischen den Unternehmensgrößen, letztendlich sind die Werte jedoch bei allen über 90,0 % und damit stark verbreitet.

Abbildung 5: Verbreitung technischer IT-Sicherheitsmaßnahmen (in %)



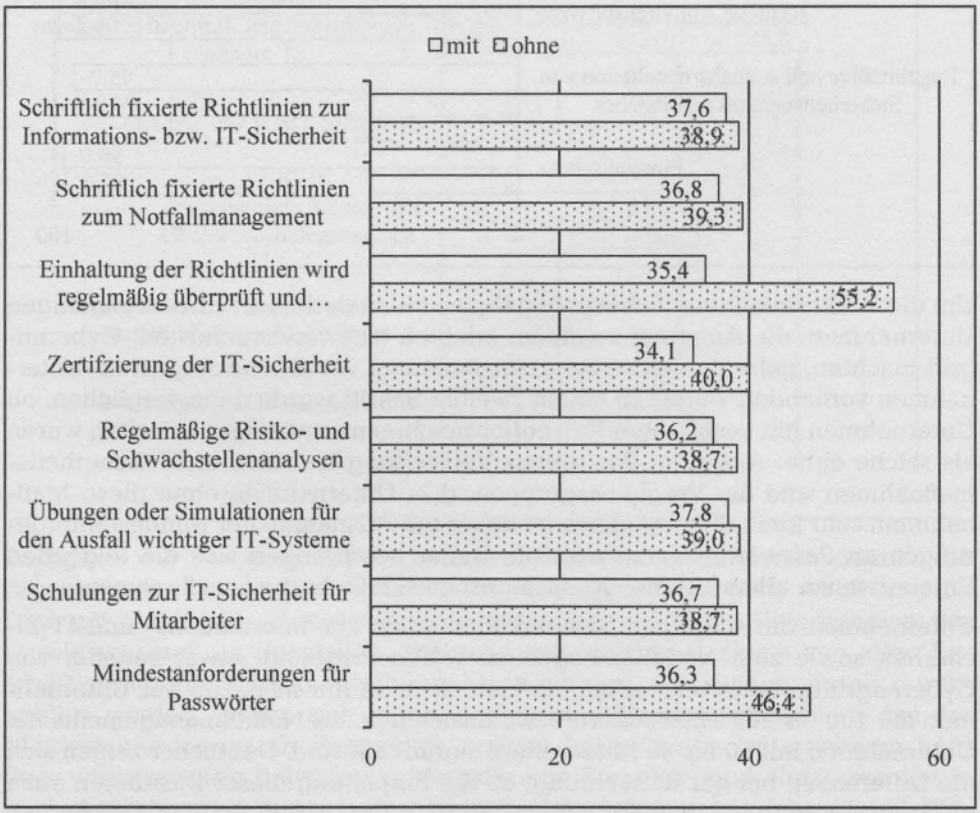
Um die Wirksamkeit von Schutzmaßnahmen zu analysieren, wurden diejenigen Unternehmen, die Angaben zu einem erlebten (schwerwiegendsten) Cyberangriff machten, gefragt, welche Schutzmaßnahmen vor diesem Angriff im Unternehmen vorhanden waren. In einem zweiten Schritt wurde dann verglichen, ob Unternehmen mit bestimmten Präventionsmaßnahmen weniger betroffen waren als solche ohne. Aufgrund der weiten Verbreitung technischer IT-Sicherheitsmaßnahmen sind die Vergleichsgruppen, d. h. Unternehmen ohne diese Maßnahmen, sehr klein. Ein Vergleich ist daher mit Ausnahme der Mindestanforderungen an Passwörter wenig sinnvoll. Daher beschränken sich die folgenden Ergebnisse vor allem auf die organisatorischen IT-Sicherheitsmaßnahmen.

Unternehmen mit schriftlich fixierten Richtlinien zur Informations- und IT-Sicherheit sowie zum Notfallmanagement waren insgesamt etwas seltener von Cyberangriffen betroffen, wobei die Unterschiede nur in Bezug auf Unternehmen mit 100 bis 249 Mitarbeitern bzw. hinsichtlich des Notfallmanagements bei Unternehmen mit 50 bis 99 Mitarbeitern signifikant sind. Deutlicher zeigen sich die Differenzen bei der Betrachtung, ob die Einhaltung dieser Richtlinien auch überprüft wird und Verstöße gegebenenfalls geahndet werden. Besonders deutlich zeigt sich die Wichtigkeit der Überprüfung der Einhaltung der Regeln: 35,4 % der Unternehmen waren betroffen, wenn Richtlinien überprüft wurden, wohingegen 55,2 % Opfer wurden, wenn keine derartige Überprüfung stattfindet. Dies gilt insbesondere für kleine Unternehmen mit zehn bis 49 Beschäftigten. Das Vorhandensein einer Zertifizierung der IT-Sicherheit mindert ebenfalls statistisch bedeutsam das Risiko, einen Cyberangriff zu erleben, wobei sich die

Unterschiede besonders bei kleinen Unternehmen mit zehn bis 48 bzw. 50 bis 99 Mitarbeitern zeigen.

Ferner finden sich relevante Unterschiede hinsichtlich der Frage, ob regelmäßig Risiko- und Schwachstellenanalysen durchgeführt werden, insbesondere in den Gruppen 50 bis 99 und 100 bis 249 Mitarbeitern. Schulungen zur IT-Sicherheit für Beschäftigte wirken sich vor allem bei mittleren Unternehmen (50 bis 499 Mitarbeiter) risikoreduzierend aus. Unternehmen mit 250 bis 499 Beschäftigte waren z. B. mit Schulung zu 40,8 % und ohne zu 53,4 % von Cyberangriffen betroffen. Übungen oder Simulationen für den Ausfall wichtiger IT-Systeme zeigten sich besonders im Zusammenhang mit Unternehmen von 250 bis 499 Mitarbeiter als effektiv und Mindestanforderungen für Passwörter vor allem in kleineren Unternehmen von zehn bis 99 Mitarbeiter.

Abbildung 6: Jahresprävalenzraten mit und ohne ausgewählte IT-Sicherheitsmaßnahmen (in %)



Der Umstand, dass die meisten der technischen IT-Sicherheitsmaßnahmen bereits weit verbreitet sind und viele Unternehmen trotzdem von Cyberangriffen betroffen sind, sollte nicht zu dem Trugschluss führen, dass diese Maßnahmen keine präventive Wirkung entfalten. Vielmehr weist dies auf weitere Faktoren hin, die mit deren Wirksamkeit zusammenhängen. Neben der Qualität, dem Reifegrad sowie der sachgemäßen Konfiguration und Wartung der technischen

Maßnahmen dürften dazu ebenso die Frage des Designs und der Nutzbarkeit im Alltag der Mitarbeiter zählen. Dies wird auch über die gezeigten Zusammenhänge zwischen der Prävalenz und den organisatorischen IT-Sicherheitsmaßnahmen deutlich, denn diese setzen verschiedene technische Maßnahmen voraus und machen erst mit ihnen zusammen einen Unterschied.

3.3.4 Risikobewusstsein

Unabhängig von dem Vorhandensein von Präventionsmaßnahmen wurden die Unternehmensvertreter gefragt, inwiefern innerhalb des Unternehmens ein Risikobewusstsein bezüglich der Möglichkeit, einen Cyberangriff zu erfahren, vorhanden ist. Dabei sollten sie mittels einer vierstufigen Antwortskala (trifft gar nicht zu, eher nicht, eher und voll und ganz) einschätzen, inwiefern die Geschäftsführung und die Mitarbeiter sich der Risiken bewusst sind und Vorgaben eingehalten werden sowie ob aus ihrer Sicht genug für die Informationssicherheit in ihrem Unternehmen getan wird. Insgesamt gaben 48,8 % an, dass die Geschäftsführung sich der Risiken voll und ganz bewusst sei, wobei weitere 43,3 % dem eher zustimmten. Etwas niedrigere Zustimmungswerte zeigten sich hinsichtlich der Mitarbeiter des Unternehmens. Die Befragten schätzten zu 31,4 % ein, dass sich die Belegschaft voll und ganz über IT-Risiken im Klaren sei sowie die Vorgaben einhielten. Allerdings stimmte etwas mehr als die Hälfte (56,4 %) dieser Aussage eher zu, sodass insgesamt auch hier hohe Zustimmungswerte erzielt wurden. Der Aussage, dass im Unternehmen sehr viel für die Informationssicherheit getan würde, stimmten 31,5 % voll und ganz und 53,4 % eher zu.

Im Vergleich zwischen Unternehmen der Daseinsvorsorge und allen anderen sind diesbezüglich keine statistisch relevanten Unterschiede feststellbar. Allerdings steht das Antwortverhalten mit der Position der Personen im Zusammenhang, die für die Interviewstudie als Vertreter des Unternehmens befragt wurden. Handelte es sich dabei um Mitarbeiter aus dem Bereich IT und Informationssicherheit, schätzten sie das Risikobewusstsein der Geschäftsführung niedriger ein als es Befragte aus der Geschäftsführung selbst taten. Bezüglich der Frage, ob genug im Unternehmen insgesamt für die Informationssicherheit getan wird, schätzten wiederum Personen aus der Geschäftsführung dies kritischer ein als Mitarbeiter aus der IT- und Informationssicherheitsabteilung. Ferner zeigen sich auch Unterschiede hinsichtlich der Unternehmensgröße. Das Risikobewusstsein der Mitarbeiter wird von Vertretern größerer Unternehmen geringer eingeschätzt als von kleineren. Dass im Unternehmen genug für die IT-Sicherheit getan wird, wird hingegen von kleineren Unternehmen eher verneint als von größeren.

Des Weiteren wurden die Unternehmen gefragt, für wie wahrscheinlich sie es halten, dass in den nächsten zwölf Monaten das Unternehmen einen gezielten bzw. ungezielten Cyberangriff erlebt. Insgesamt wurde dieses Risiko eher gering eingeschätzt. Bezüglich eines ungezielten Angriffs schätzten nur 6,0 % das Risiko als sehr hoch und weitere 25,5 % als hoch ein. Die Gefahr, einen gezielten Angriff zu erleben, schätzten sogar nur 1,3 % als hoch und 5,7 % als eher hoch ein. Auch hierbei sind keine Besonderheiten für Unternehmen der Daseinsvorsorge festzustellen. Hingegen zeigt sich wiederum, dass Befragte aus dem Bereich der IT- und Informationssicherheit die Risiken höher einschätzten

als andere Befragte. Größere Unternehmen schätzten die Wahrscheinlichkeit höher ein, einen Cyberangriff in den kommenden zwölf Monaten zu erleben, als kleinere.

3.4 Fazit und Ausblick

Die Ergebnisse der Befragung weisen auf ein hohes Risiko von Unternehmen hin, Opfer eines Cyberangriffs zu werden, der eine Reaktion notwendig macht und in der Regel Kosten verursacht. Auch wenn dabei die Betroffenheitsrate bei großen Unternehmen höher ist als bei kleineren, weisen alle Beschäftigtengrößenklassen eine relevante Anzahl bereits erfahrener Straftaten gegen ihre IT-Systeme auf. Vor diesem Hintergrund – und in Anbetracht möglicher Folgen und Kosten – wird deutlich, dass Cyberkriminalität eine Gefahr für alle Unternehmen darstellt, unabhängig davon, inwiefern sie ein vermeintlich lohnendes Ziel für Täter sein könnten oder in welchem Umfang die Arbeitsabläufe digitalisiert sind. Auch wenn hierbei Behörden bzw. Unternehmen der öffentlichen Verwaltung nicht explizit untersucht wurden, liegt nahe, dass diese ebenso durch Cyberangriffe gefährdet sind. In der vorliegenden Untersuchung konnten Hinweise hierfür u. a. in Bezug auf Unternehmen der Daseinsvorsorge gefunden werden, welche teilweise in öffentlicher Hand sind. Auch diese weisen eine relevante, wenn auch im Vergleich mit anderen Unternehmen geringere Anzahl bereits erfahrener Cyberangriffe auf.

Eine Ursache für die geringere Betroffenheit von Unternehmen der Daseinsvorsorge könnte sein, dass diese umfangreichere IT-Sicherheitsmaßnahmen anwenden als andere. Die Bedeutung von Präventionsmaßnahmen gehört damit zu einem weiteren Kernergebnis der Studie. Hierbei zeigt sich, dass IT-Sicherheitsmaßnahmen wirksam sind. Differenziert nach Art der Maßnahme wird dabei deutlich, dass neben den technischen Präventionsmöglichkeiten auch organisatorische Maßnahmen effektiv sind. Während technische Maßnahmen weit verbreitet sind, zeigen die Befragungsergebnisse, dass dies bei organisatorischen Präventionsmöglichkeiten noch nicht der Fall ist. Die Anwender der jeweiligen IT-Systeme, d. h. in diesem Fall die Mitarbeiter und Vorgesetzten, müssen noch stärker beim Aufbau sowie bei der regelmäßigen Überprüfung und Anpassung von Cybersecurity mit einbezogen werden. Dazu gehört zunächst, dass sie ein Problembewusstsein entwickeln und für das Phänomen sensibilisiert sind. Unterschiede in Bezug auf die Einschätzung des Risikos je nach Position im Unternehmen zeigten sich auch schon in dieser Befragung. Dabei ist davon auszugehen, dass die jeweilige Einschätzung sich auch auf das Verhalten auswirkt. In den alltäglichen Arbeitsroutinen, beispielsweise beim Öffnen von Links und E-Mail-Anhängen und der Sicherung von Daten sowie dem Vergeben von Passwörtern, kommt es auf das Sicherheitsverhalten des einzelnen an. Auch in den prominenten Fällen von Cyberangriffen auf öffentliche Verwaltungsbehörden der Stadt Neustadt und des Kammergerichts Berlin, die in Kapitel 1 und 4 im vorliegenden Band ausgeführt sind, lag es nicht am technischen Versagen, dass der Betrieb über Wochen nicht mehr funktionierte. Vielmehr waren es die jeweiligen Mitarbeiter, die durch das Anklicken eines Links oder das Öffnen eines E-Mail-Anhangs die Verbreitung des Virus ermöglicht haben.

Technische und organisatorische IT-Sicherheitsmaßnahmen sind sowohl für Unternehmen als auch für die öffentliche Verwaltung relevant, um Cyberangriffe zu verhindern oder deren Folgen zu begrenzen. Dennoch liegt die Vermutung nahe, dass es auch aufgrund einiger Besonderheiten Unterschiede zwischen Unternehmen und Behörden in Bezug auf Cyberkriminalität geben könnte. So könnte es sein, dass die IT-Struktur und das Vorhandensein von IT-Sicherheitsmaßnahmen bei Behörden der öffentlichen Verwaltung schlechter sind, als dies bei privatwirtschaftlichen Unternehmen bzw. Unternehmen der Daseinsvorsorge der Fall ist. Hierzu könnte auch beitragen, dass die Rekrutierung von IT-Fachkräften für Behörden schwerer ist als für die Privatwirtschaft, die u. a. höhere Löhne zahlen kann (in Bezug auf die Polizei siehe *Stiller et al.*, 2020; siehe dazu auch Kapitel 4 und 7 im vorliegenden Band). Behörden könnten für bestimmte Täter durch die Vielzahl an vertrauensvollen personenbezogenen und anderen sensiblen Daten auch besonders interessant sein und deren Angriff möglicherweise vielversprechender als bei privatwirtschaftlichen Unternehmen. Vor dem Hintergrund dieser Überlegungen wird deutlich, dass hinsichtlich des Phänomens von Cyberangriffen gegen die öffentliche Verwaltung eine Forschungslücke vorliegt, die nur ansatzweise durch die berichteten unternehmensbezogenen Erkenntnisse geschlossen werden kann.

3.5 Literatur

Bitkom e.V., Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie, Studienbericht, 2018. Abrufbar unter: https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf (abgerufen am 23.3.2020).

BSI, Cyber-Sicherheits-Umfrage. Cyber-Risiken & Schutzmaßnahmen in Unternehmen. Betrachtungszeitraum 2018. Version 1.0 vom 10.4.2019, Bonn 2019.

Dreißigacker, Arne/von Skarczinski, Bennet/Wollinger, Gina R., Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019, Forschungsbericht Nr. 152, Kriminologisches Forschungsinstitut Niedersachsen e.V., Hannover 2020.

Paoli, Letizia/Visschers, Jonas/Verstraete, Cedric, The impact of cybercrime on businesses: a novel framework and its application to Belgium, Crime, Law and Social Change, 70(4), 2018, S. 397-420.

PwC Strategy&GmbH, Cybersicherheitsstrategie. Ergebnisse einer Online-Erhebung, Düsseldorf 2016.

Rantala, Ramona R., Cybercrime against Businesses, Bureau of Justice Statistics, Special Report, Washington DC 2008.

Schäfer, Michael, Daseinsvorsorge, in Gabler Wirtschaftslexikon, Wiesbaden 2018.

Stiller, Anja/Boll, Lukas/Kretschmer, Saskia/Wollinger, Gina R./Dreißigacker, Arne, Cyberangriffe in Deutschland. Ergebnisse einer qualitativen Expertenbefragung, KFN-Forschungsbericht Nr. 155, Hannover 2020 (in press).