Monitor IT-Sicherheit Kritischer Infrastrukturen

Tamara Gurschler · Sebastian Dännart · Ulrike Lechner

Universität der Bundeswehr München
Fakultät für Informatik
{tamara.gurschler | sebastian.daennart | ulrike.lechner}@unibw.de

Zusammenfassung

Mit der Umfrage „Monitor IT-Sicherheit Kritischer Infrastrukturen“ wurden unter anderem Daten zur Selbsteinschätzung der Fähigkeiten in der IT-Sicherheit, zur Bedrohungslage und der Umsetzung des IT-Sicherheitsgesetzes erhoben. Diese Daten wurden hinsichtlich der Unterschiede zwischen KRITIS-Organisationen und Nicht-KRITIS sowie unter besonderer Berücksichtigung kleiner und mittlerer Unternehmen (KMU) analysiert. Darüber hinaus wurde der Bedarf an Technologien, wie sie im Förderschwerpunkt „IT-Sicherheit Kritischer Infrastrukturen“ (ITS|KRITIS) erforscht werden, und die Erwartungen an die Zukunft der IT-Sicherheit erhoben. Die vollständigen Ergebnisse sind auf der ITS|KRITIS-Plattform monitor.itskritis.de zu finden.

1 Einleitung und Motivation

Die Durchdringung von Produktions- und Versorgungsanlagen mit IT und die zunehmende Vernetzung dieser, gemäß der Leitidee von „Industrie 4.0“, birgt Risiken, die unmittelbar auch in, für die Zivilgesellschaft höchst relevanten, *Kritischen Infrastrukturen* spürbar werden. Beispiele sind Krankenhäuser, die nicht mehr auf ihre digitale Patientenverwaltung zugreifen können [Borc16][HoKa17] und Hackerangriffe auf den deutschen Bundestag [MeRe15][Spie17]. Auf diese wachsende Bedrohung reagierte auch die Bundesregierung. Mit dem Inkrafttreten des IT-Sicherheitsgesetzes im Juli 2015 [Bund15] kommen auf KRITIS-Betreiber neue Verpflichtungen zu. Doch wie ist es aktuell um die IT-Sicherheit bei KRITIS bestellt? Wie schätzen diese Organisationen die Bedrohungslage ein?

Diese und andere Fragen haben wir IT-Sicherheitsverantwortlichen in der Umfrage „Monitor IT-Sicherheit Kritischer Infrastrukturen“ gestellt und die Ergebnisse mit Fokus auf Betreiber *Kritischer Infrastrukturen* und von kleineren und mittleren Unternehmen (KMU) ausgewertet.

Die vollständigen Ergebnisse sind über diese Veröffentlichung hinaus grafisch aufbereitet und zu einer Broschüre zusammengefasst auf der Plattform des Förderschwerpunktes ITS|KRITIS unter monitor.itskritis.de zu finden.

1.1 Kritische Infrastrukturen (KRITIS)

Das Bundesministerium des Innern gibt in der „Nationalen Strategie zum Schutz Kritischer Infrastrukturen“ (KRITIS-Strategie) eine offizielle Definition für KRITIS vor. Demnach sind *Kritische Infrastrukturen*: „Organisationen oder Einrichtungen mit wichtiger Bedeutung für das

P. Schartner · A. Baumann (Hrsg.) · D•A•CH Security 2017 · syssec (2017) 170-180.

staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“ [BuMi09]. Das IT-Sicherheitsgesetz [Bund15] ist anwendbar auf die vom BMI definierten KRITIS-Sektoren *Energie*, *Informationstechnik* und *Telekommunikation*, *Transport und Verkehr*, *Gesundheit*, *Wasser*, *Ernährung* sowie *Finanz- und Versicherungswesen*, nicht jedoch *Medien und Kultur* und *Staat und Verwaltung*, die vom BMI ebenfalls zu KRITIS-Sektoren gezählt werden. Das IT-Sicherheitsgesetz [Bund15] trägt den Risiken der IT-Sicherheit in den KRITIS-Sektoren Rechnung.

Die Digitalisierung von Geschäfts- und Produktionsprozessen ist auch bei *Kritischen Infrastrukturen* ein wichtiges Thema. Produktionsanlagen benötigen u. a. zur Auslastungsoptimierung und zur besseren Wartbarkeit Netzwerkverbindung. Die „Industrie 4.0“ ist in vielen Unternehmen bereits Realität. Bei allen Vorteilen, die eine solche Vernetzung mit sich bringt, darf der Schutz dieser Systeme nicht außer Acht gelassen werden. Beispiele für gängige KRITIS-Sicherheitsthemen sind: veraltete Betriebssysteme als Teil von industriellen Steuerungsanlagen; die Architektur der Anlagen ist ursprünglich nicht auf Vernetzung ausgelegt und sieht IT-Sicherheitsmaßnahmen nicht vor; wegen mangelndem Support durch Hersteller und Herstellergewährleistung kann kein wirksamer Schutz vor Bedrohungen realisiert werden; die Kosten für neue Systeme, die bereits für Internet of Things ausgerüstet sind, sind zu hoch oder Umrüstung ist keine Option.

Das Bundesamt für Sicherheit in der Informationstechnik sieht die zunehmende Vernetzung und die daraus resultierenden Abhängigkeiten sowie das parallel steigende potenzielle Schadensausmaß als Grundlage für nötige, umfassende Investitionen [BuSI17]. Dass *Kritische Infrastrukturen* gerade wegen ihrer besonderen Verantwortung lukrative Ziele sein können, zeigen der Ransomware-Angriff auf ein Krankenhaus [Borc16] oder WannaCry [HoKa17].

1.2 Kleine und mittlere Unternehmen

Aufgrund der besonderen Bedeutung und dem großen Anteil, den sie innerhalb der *Kritischen Infrastrukturen* ausmachen, wird in dieser Arbeit auch ein Augenmerk auf kleine und mittlere Unternehmen (KMU) gelegt. Beispielhaft bezogen auf den KRITIS-Sektor *Wasser* liegen hierzu konkrete Zahlen vor: 78% von insgesamt 1.658 Unternehmen der Wasserversorgung beschäftigen 20 oder weniger Mitarbeiter [GGK+17]. In der EU-Empfehlung der Europäischen Kommission 2003/361 sind KMU wie folgt definiert: „Die Größenklasse der kleinen und mittleren Unternehmen (KMU) setzt sich aus Unternehmen zusammen, die weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft.“ [KoEG03]. KMU stehen der Herausforderung gegenüber, alle Anforderungen an die IT-Sicherheit trotz knapper Ressourcen umzusetzen.

1.3 Ziele des Beitrags

Obwohl eine Reihe an Studien und Umfragen zur IT-Sicherheit durch Beratungsunternehmen, Behörden und Forschungsinstitutionen existieren, sind *Kritische Infrastrukturen* und die spezifischen Fragestellungen der IT-Sicherheit in *Kritischen Infrastrukturen* unterrepräsentiert. Mit dem Fokus auf die Besonderheiten von KRITIS und dem Vergleich zu Nicht-KRITIS stellen wir in dieser Studie eine bislang kaum betrachtete Perspektive zur Verfügung. Diese Studie adressiert Betreiber *Kritischer Infrastrukturen* und soll Wegweiser für Forschung sein.

1.4 Forschungskontext

Der „Monitor IT-Sicherheit Kritischer Infrastrukturen“ ist eingebettet in den vom Bundesministerium für Bildung und Forschung ausgeschriebenen Förderschwerpunkt „IT-Sicherheit für Kritische Infrastrukturen“. 13 Forschungsprojekte mit ca. 80 Betreibern *Kritischer Infrastrukturen*, Technologieanbietern und Forschungsinstitutionen bilden den Förderschwerpunkt ITS|KRITIS. Der Monitor wurde von der Begleitforschung „Vernetzte IT-Sicherheit Kritischer Infrastrukturen“ (VeSiKi) konzipiert und greift querschnittliche Themen zu Informationssicherheit und *Kritischen Infrastrukturen* auf. Eine Einordung der Forschung des Förderschwerpunktes ITS|KRITIS und des Begleitforschungsprojektes VeSiKi stellt Dr. Steffi Rudel in einem Beitrag zum vorliegenden Konferenzband vor.

2 Studien zu IT-Sicherheit – State of the Art

Das Bundesamt für Sicherheit in der Informationstechnik (BSI), PricewaterhouseCoopers LLP (PWC), Ernst & Young (EY) sowie viele weitere Unternehmen und Organisationen verfassen in regelmäßigen Abständen Untersuchungen zu Informationssicherheit. Dieses Kapitel gibt einen Überblick und untersucht die Themen einiger Studien im Detail. Neben den hier näher betrachteten Studien des BSI [BuSI15], PWC [Pric14] und EY [ErYo15] gibt es u.a. Studien von Kaspersky [Kasp15], HM Government [HMGo15], ISACA [ISAC15] und Dell [Fisc15].

Für eine Kategorisierung der Studien wurden wichtige Aspekte, die in einer Studie behandelt werden, identifiziert und eine entsprechende Analyse durchgeführt. Die Einordnung dreier wichtiger IT-Sicherheitsuntersuchungen aus den Jahren 2015 und 2016 sind in der Analysespinne Abbildung 1 zu finden. Die thematischen Schwerpunkte für die Kategorisierung wurden unter Berücksichtigung der Interessenlage von KRITIS-Organisationen, öffentlichen Institutionen und den Forschungsthemen von VeSiKi gewählt. Die Wertungslinien in der Analysespinne – die mit einem Zahlenwert zwischen 0 („kommt nicht in der Studie vor“) und 9 („Schwerpunkt der Studie“) belegt werden können – erlauben es darüber hinaus Aussagen über die Priorität eines jeden Schwerpunkts in der Studie zu treffen. *Die Lage der IT-Sicherheit in Deutschland* des BSI behandelte sowohl 2015, als auch 2016 vorrangig die Themenschwerpunkte „Bedrohungen“ und „Erkenntnisse“. Der Bezug zur Praxis im Sinne von Fallbeispielen und Umfragen/Statistiken spielte eine untergeordnete Rolle. Der *„Managing cyber risks in an interconnected world“*-Report von PWC setzte genau hier seinen Fokus. In dem Survey „*Creating trust in the digital world“* von EY weisen vier Faktoren – Umfragen/Statistiken, Lösungsvorschläge, Erkenntnisse, Bedrohungen – dieselbe Wertigkeit auf. Der Fokus der drei Studien blieb von 2015 zu 2016 jeweils praktisch identisch. Eine grafische Aufbereitung, mittels Spinnendiagramm nach Georg von Mayr vgl. [Stap13], bestätigt die Vermutung, dass bisherige Studien das Themenfeld IT-Sicherheit in *Kritischen Infrastrukturen* lediglich schwach abdecken.

Die im Frühjahr 2016 konzipierte Untersuchung „Monitor IT-Sicherheit Kritischer Infrastrukturen“ greift genau diese Thematik auf. Der Monitor setzte sich zum Ziel vor allem *Kritische Infrastrukturen* mit ihren spezifischen Themen zu betrachten. Abbildung 2 zeigt die Zielvorstellungen zusammen mit den Mittelwerten der untersuchten Studien aus 2015 und 2016.

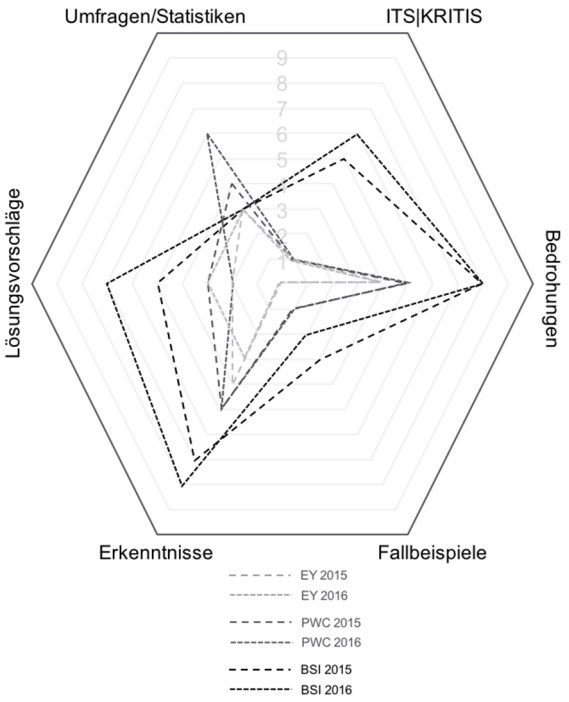

Abb. 1: Einordnung in die Analysespinne

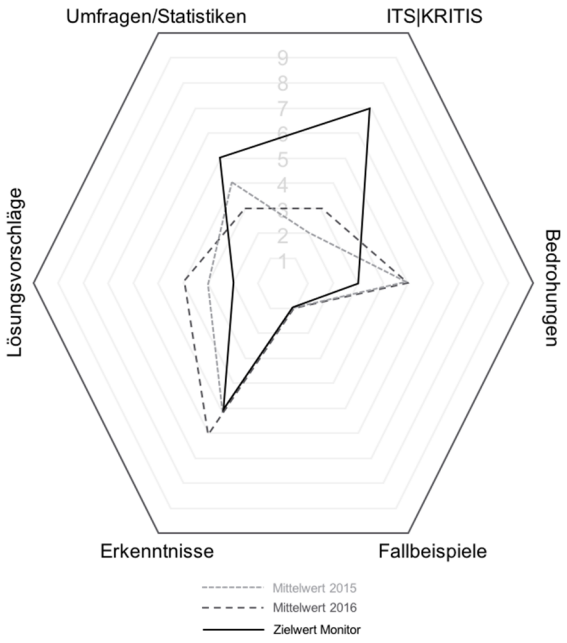

Abb. 2: Mittelwerte der untersuchten Studien aus 2015 und 2016 sowie Zielwert für den Monitor

3 Methodik der Monitor-Studie

Der „Monitor IT-Sicherheit Kritischer Infrastrukturen“ wurde als empirische quantitative Querschnittsanalyse entwickelt. Diese Methodik der Datenerhebung dient besonders dazu objektive Messwerte zu dem zu untersuchenden Forschungsgegenstand zu generieren. Laut Bortz et al. [BoDö05] sind die Ergebnisse von quantitativen Untersuchungen gut auswertbar und bieten die Möglichkeit sie mit anderen Untersuchungen zu vergleichen. Darüber hinaus schaffen quantitative Verfahren eine größere Distanz zum Forscher und eignen sich daher besonders gut bei sensiblen Fragestellungen, wie denen nach IT-Sicherheitsthemen.

Die Feststellung des Wissensbedarfs, also welche Anforderungen bestimmte Personengruppen an die konkreten Inhalte der Untersuchung haben, bildete ein zentrales Element für die Fragenformulierung. Mit der Umfrage soll Politik und Öffentlichkeit adressiert werden und fachliche Fragen werden von Forschungsprojekten von ITS|KRITIS beigesteuert. Als Adressaten der Umfrage wurden IT-Sicherheitsbeauftrage, IT-Sicherheitsverantwortliche oder Personen mit hohen Fachkenntnissen gewählt.

Aus diesen Grundinformationen und mit Hilfe von Hypothesen wurde ein Fragenkatalog entworfen, der in mehreren Workshops und Iterationen verfeinert wurde. 51 Fragen – 3 offene und 48 geschlossene – wurden in einem Online-Fragebogen gestellt. Der Aufbau des Fragebogens entspricht den Grundregeln nach Schnell et al. [ScHE05] und Bortz et al. [BoDö05].

Bei einem so umfangreichen Fragebogen und der Zielgruppe ist es nicht überraschend, dass sich die Akquise der Teilnehmer als aufwändig gestaltet. So halfen Multiplikatoren und ein Partner bei der Rekrutierung von Teilnehmern. Insbesondere wurden als erste Teilnehmer der Umfrage die Betreiber *Kritischer Infrastrukturen* der Projekte des Förderschwerpunkts

ITS|KRITIS eingeladen. Der Fragebogen war über einen Zeitraum von fünf Monaten (Juni – Oktober 2016) online zugänglich – es wurden 1089 Zugriffe verzeichnet. 79 der Webseitenbesucher führten die Umfrage durch. Viele der Besucher verließen die Webseite bereits auf der ersten Seite, die das Informationsschreiben zur Umfrage mit Anzahl der Fragen und Dauer für das Ausfüllen (30 Minuten) beinhaltete.

Die Auswertung der Ergebnisse wurde als deskriptive, beschreibende Statistik vorgenommen.

4 Ergebnisse

Um einen Eindruck der Ergebnisse zu vermitteln, werden in diesem Kapitel je Themenbereich der Umfrage ein kurzer Ausschnitt und ausgewählte Zahlen präsentiert.

4.1 Die Teilnehmer

Um zur IT-Sicherheit im eigenen Unternehmen auskunftsfähig zu sein, wurde als Zielgruppe für die Umfrage Mitarbeiter adressiert, die mit der IT-Sicherheit im Unternehmen betraut ist. Als Rolle im Unternehmen gaben die Teilnehmer zu je etwa 10 % IT-Sicherheitsbeauftragte, CISO bzw. ISO und CEO bzw. Geschäftsführung an. Teilgenommen haben auch IT-Leiter, Leiter F&E, ISMS-Beauftragter, IT-Sicherheitsspezialist, CSO und CTO. 93% der Teilnehmer waren männlich, 7% weiblich.

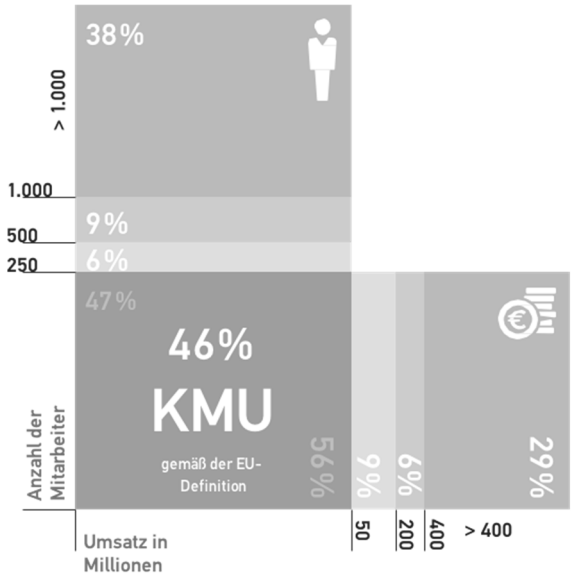

Abb. 3: Einordung der teilnehmenden Unternehmen anhand von Mitarbeiterzahl und Umsatz

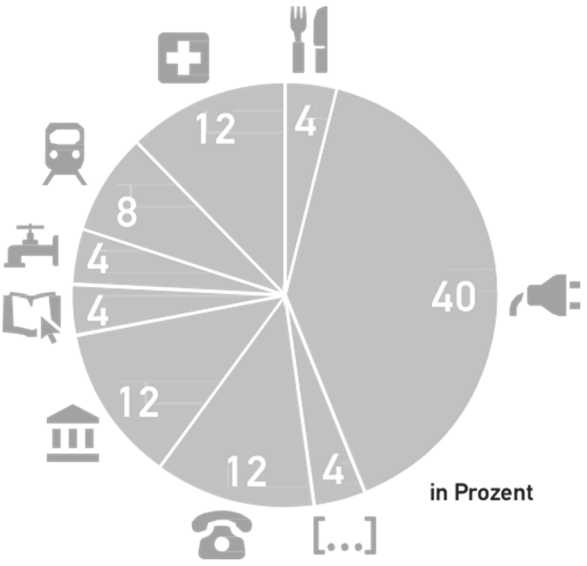

Abb. 4: Einordnung der teilnehmenden Unternehmen anhand des Sektors

Die Teilnehmer sollten in einer offenen Frage definieren, was für Sie KRITIS ausmacht und ihre Organisation als KRITIS einordnen. 37% der Teilnehmer bezeichneten ihre Organisation als KRITIS. Abbildung 3 zeigt die teilnehmenden Unternehmen nach Anzahl der Mitarbeiter und Umsatz in Millionen gegenübergestellt. Demnach sind 46% der teilnehmenden Unternehmen gemäß Definition [KoEG03] KMU.

Eingeteilt in die Sektoren des IT-Sicherheitsgesetzes [Bund15] zeigt Abbildung 4 die Aufteilung der Teilnehmer nach KRITIS Sektoren. Vertreten sind hier alle Sektoren bis auf den des

Finanz- und Versicherungswesens – einen überproportional großen Anteil macht den Sektor Energie aus.

Um sowohl die objektive als auch die subjektiv wahrgenommene Bedrohungslage zu erfassen, stellten wir den Teilnehmern Fragen zu Angriffen und der individuellen Beurteilung der Bedrohungslage. Es stellte sich heraus, dass 85% der KRITIS im letzten Jahr Ziel von Cyber-Attacken waren. Dennoch beurteilen 77% aller Teilnehmer ihre IT-Sicherheit als „gut“ oder „sehr gut“; betrachtet man hier nur KRITIS, sind es sogar 88%.

Abbildung 5 zeigt die Einschätzung der Bedrohungslage für Deutschland, die eigene Branche und das eigene Unternehmen. Die Einschätzungen werden für alle Teilnehmer, für KMU und für KRITIS aufgeschlüsselt. Hier fällt die Tendenz auf, dass alle Teilgruppen die Bedrohung für das eigene Unternehmen niedriger einschätzen, als für die eigene Branche, geschweige denn für Deutschland. Solche Unterschiede in der Risikoeinschätzung sind auch als „Optimism Bias“ bekannt: Individuen schätzen ihr eigenes Risiko geringer als das der Allgemeinheit ein [DeJo89]. Wir fragten außerdem nach der Einschätzung Angriffe abwehren zu können. Die Auswertung der Ergebnisse zeigt ein ähnliches Bild zu jenem der Einschätzung der Bedrohungslage –der Optimism Bias fand auch hier Anwendung, siehe Abbildung 6.

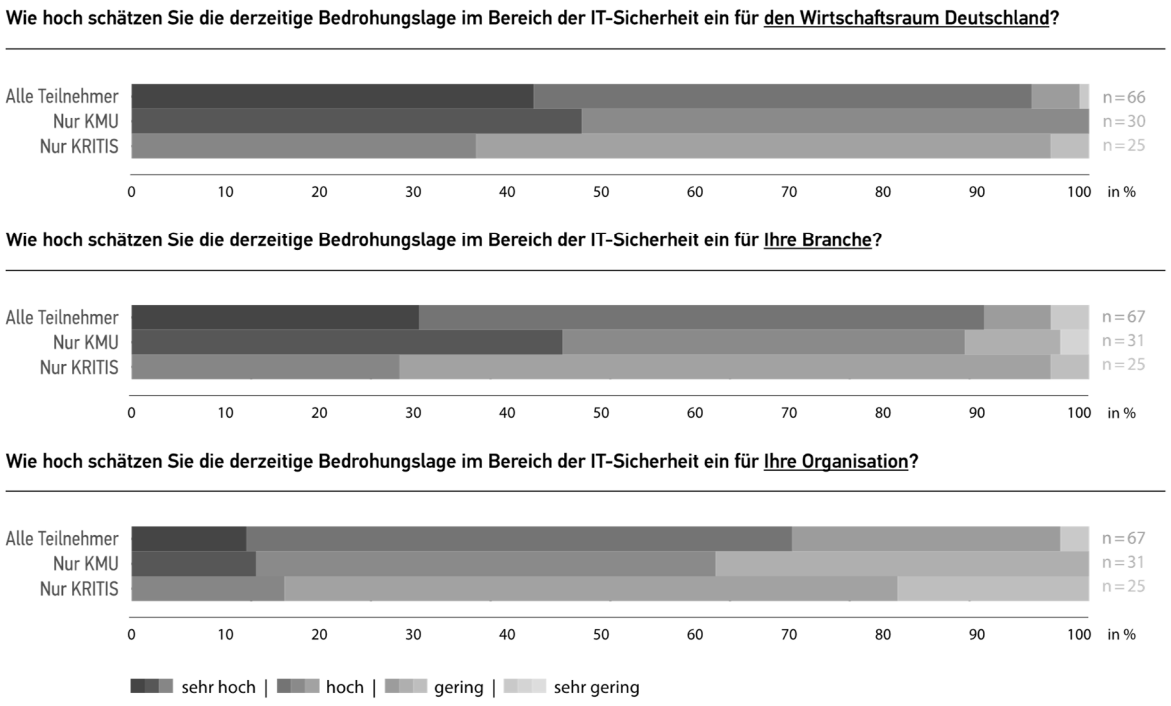

Abb. 5: Einschätzung der Bedrohungslage

Wir fragten nach der Art der Angriffe, die sie auf ihre Systeme feststellen konnten. In Abbildung 7 fällt auf, dass Phishing, Spam und die relativ neuartige bzw. wieder aufkommende Ransomware sehr häufig genannt wurden. Die Balken umfassen sämtliche Angriffsarten, die von allen Teilnehmern der Umfrage gewählt wurden. Die Innenbalken der einzelnen Balken des Diagramms stellen den Anteil der von KRITIS angegebenen Angriffsarten in absoluten Zahlen dar. In Bezug auf die insgesamt angegebenen Angriffsarten wurden für KRITIS verhältnismäßig viele Innentäter, Exploit Kits und Denial of Service genannt. Für 45% der KRITIS

Unternehmen die Cyber-Angriffen verzeichnen konnten waren Serviceausfälle oder Datenverluste die Folge.

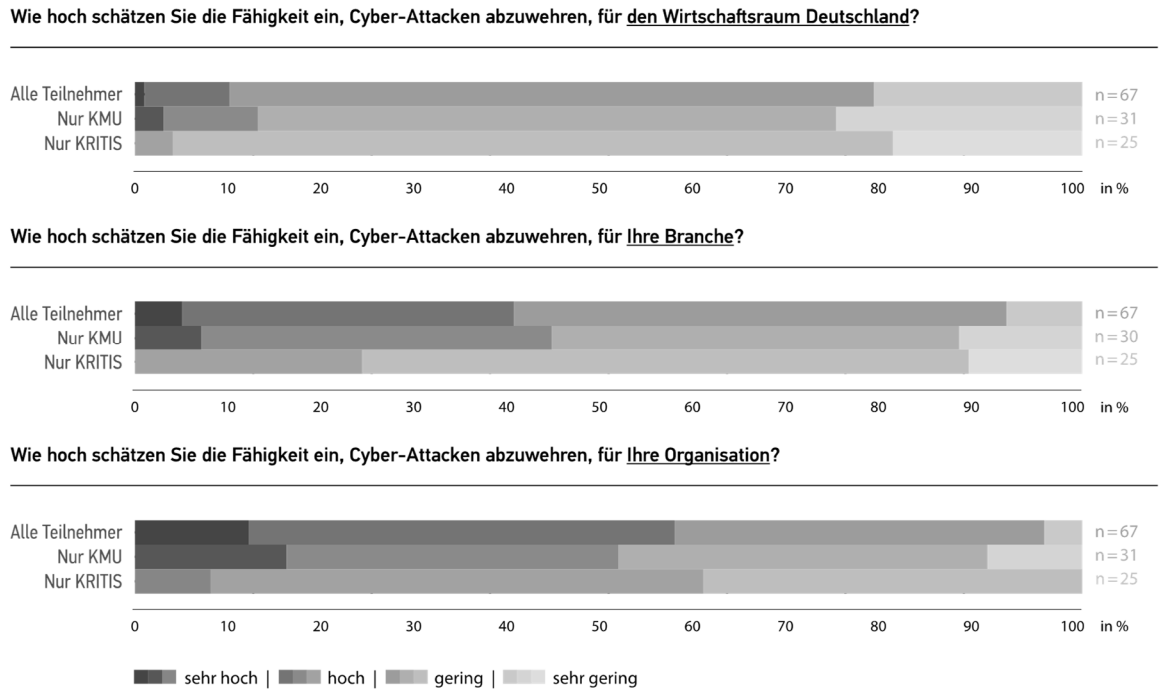

Abb. 6: Einschätzung der Abwehrfähigkeiten

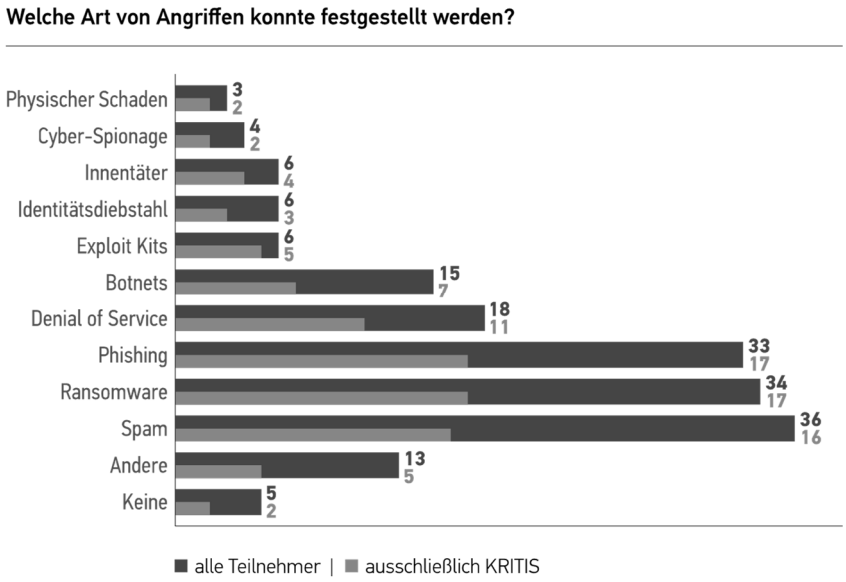

Abb. 7: Arten von Angriffen (absolute Zahlen, Mehrfachauswahl möglich)

Das Budget für IT-Sicherheit ist ein Indikator, wie wichtig das Thema in Organisationen ist. Abbildung 8 zeigt die finanzielle Ausstattung für IT-Sicherheit gemessen am IT-Budget der Organisation. Überraschend ist, dass 60% der KRITIS das Budget für nicht ausreichend halten. Beachtenswert ist die Tendenz, dass das Budget bei 64% der KRITIS im nächsten Jahr steigen

soll; kein einziges KRITIS-Unternehmen erwartet eine Reduzierung des Budgets für IT-Sicherheit.

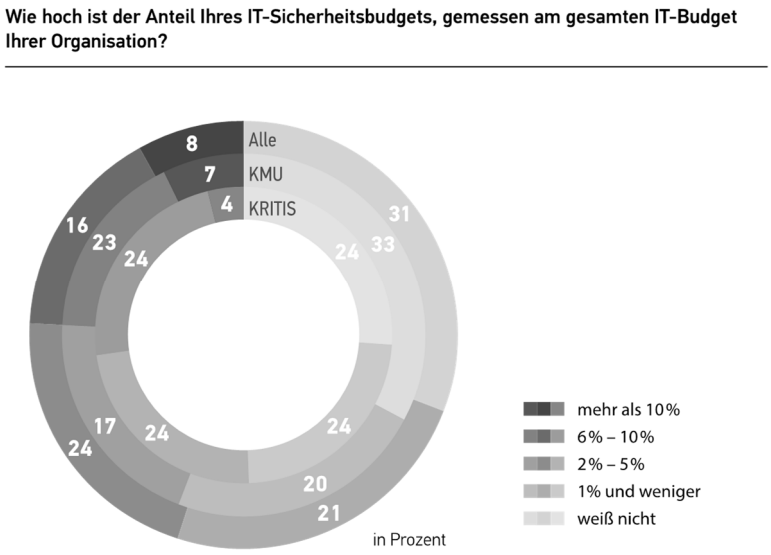

Abb. 8: Budget für IT-Sicherheit

4.2 Die Realisierung von IT-Sicherheit

Dieser Bereich der Umfrage beschäftigt sich mit der konkreten Umsetzung der IT-Sicherheit in den befragten Unternehmen. Unter anderem werden hier gängige Rahmenwerke und Standards sowie Zertifizierungen nach ISO/IEC 27001 aufgegriffen – letztere streben rund 28% der KRITIS an, 12% haben sie bereits. Weiterhin werden Zusammenarbeit mit Behörden und Verbänden sowie die Weiterbildung der Mitarbeiter thematisiert.

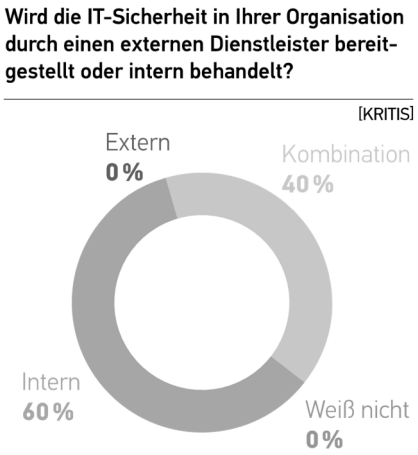

Abb. 9: Externe Dienstleister für IT-Sicherheit

Risiko ist im Bereich der IT-Sicherheit höchst individuell und mit zeitlichem Bezug zu bewerten. Es überrascht daher, dass lediglich 54,5% aller teilnehmenden Unternehmen regelmäßig eine IT-Risikobewertung durchführen; bei den KRITIS Unternehmen sind dies bereits 68%. Die Sensibilität, die das Thema IT-Sicherheit mitbringt, ist den Unternehmen jedoch durchaus bewusst, da, wie Abbildung 9. zeigt, keines der teilnehmenden Unternehmen die IT-Sicherheit

vollständig an einen externen Dienstleister übertragen hat und 60% diese vollständig intern abbilden.

Das IT-Sicherheitsgesetz ist ein Thema, das Organisationen bewegt. Es fordert von KRITIS Mindeststandards und verpflichtende Meldungen über Cyber-Angriffe. Für über 50% der KRITIS hat dies signifikante Auswirkungen auf die IT-Sicherheit im Unternehmen. Fast die Hälfte aller Teilnehmer der Umfrage halten die neuen gesetzlichen Regelungen für KMU nicht für überdimensioniert.

4.3 Der Bedarf nach Forschungsergebnissen

Der Förderschwerpunkt ITS|KRITIS beschäftigt sich in seinen 13 Forschungsprojekten mit verschiedenen Dimensionen und Perspektiven der IT Sicherheit für KRITIS. Die Umfrage greift die Kernthemen der einzelnen Forschungsprojekte auf und fragt nach der Relevanz für Organisationen. Diese Fragen wurden von den Forschungsprojekten von ITS|KRITIS beigetragen. Es fällt auf, dass bereits einige Organisationen – als Vorreiter – bestimmte Themen umgesetzt haben und das Interesse an Lösungen groß ist.

So fänden es 71% der Unternehmen interessant, die externe Erreichbarkeit ihrer Industrieanlagen analysieren zu können; erst 27% können dies bereits. Die Erkenntnisse daraus in eine Risikoabschätzung einfließen zu lassen, wäre sogar für 83% von Interesse. Ein anderes Projekt beschäftigt sich mit der automatisierten Maßnahmenzuordnung bei Sicherheitsvorfällen. Hier wären 94% daran interessiert, ein Hilfsmittel zu haben, das Sicherheitsvorfälle aufdeckt und Gegenmaßnahmen vorschlägt; nur 9% nutzen ein solches System bislang.

Ein weiteres Forschungsprojekt beschäftigt sich mit der Bewertung von Sicherheitsbewusstsein der Mitarbeiter im Unternehmen. Laut den Zahlen der Monitor-Umfrage können 59% dieses Bewusstsein noch nicht messen. So eine Messung ist jedoch für eine valide Risikoanalyse von großer Bedeutung.

Insgesamt zeigt dieser Bereich einen hohen Bedarf an Unterstützung und Automatisierung im Rahmen der IT-Sicherheit für KRITIS.

5 Diskussion, Konklusion und Ausblick

Der Fokus auf Themen der *IT-Sicherheit Kritischer Infrastrukturen* und der Ansatz, Ergebnisse nach KRITIS und Nicht-KRITIS zu untergliedern, gibt es in dieser Form im Themenfeld der *IT-Sicherheit Kritischer Infrastrukturen*. Die interessanten Ergebnisse entstehen aus dem Vergleich KRITIS zu Nicht-KRITIS Organisationen, von Unternehmen zu KMU und aus dem Vergleich zwischen Einschätzungen zum eigenen Unternehmen, zur eigenen Branche und zu Deutschland. Die vorliegende Umfrage kann nicht den Anspruch der Repräsentativität erheben.

Die Umfrage „Monitor IT-Sicherheit Kritischer Infrastrukturen“ fasst mit dem Bereich Informationssicherheit in Verknüpfung mit *Kritischen Infrastrukturen* ein Themenfeld auf, das bislang noch sehr wenig in Umfragen betrachtet wurde.

Diese Umfrage zeigt, dass KRITIS ihre eigene Situation im Vergleich zur Branche und zum Wirtschaftsraum weniger optimistisch sehen, als es die Gesamtheit der Teilnehmer tut. Ob dies ein Zeichen für das Bewusstsein der eigenen Verantwortung und der Auswirkung eines potenziellen Ausfalls der Leistung des eigenen Unternehmens wäre bleibt zwar offen, in Kombina-

tion mit der überdurchschnittlichen Beteiligung in Verbänden (83%) und der insgesamt positiveren Einschätzung des eigenen Standes bezüglich der IT-Sicherheit (88% „gut“ oder „sehr gut“; Gesamtteilnehmer 77% „gut“ oder „sehr gut“) zeigt es ein positives Bild.

Eine häufig getätigte Aussage, dass das IT-Sicherheitsgesetz [Bund15] Auswirkungen auf KRITIS hat, bestätigte sich hingegen. 52% der befragten KRITIS sehen signifikante Auswirkungen auf die IT-Sicherheit im Unternehmen. Auch dies spricht für ein Bewusstsein für IT-Sicherheit und auch, dass diese Organisationen bereits weit in der Umsetzung der Anforderungen des IT-Sicherheitsgesetzes sind.

Weitere interessante Themen der Monitor-Umfrage sind die strategische Ausrichtung im Unternehmen, der Einsatz neuer Informations- und Kommunikationstechnologie, der Umgang mit dem IT-Sicherheitsgesetz, die Einschätzung der eigenen Fähigkeiten.

Zu den interessantesten Ergebnissen gehören die Bedrohungslage von KRITIS, der Optimism Bias in der Einschätzung der Bedrohung und den eigenen Fähigkeiten sowie die Implikationen des IT-Sicherheitsgesetzes auf die Organisationen.

Im Zuge der Auswertung konnte festgestellt werden, dass der Bedarf nach Forschung im Bereich IT-Sicherheit für *Kritische Infrastrukturen* noch lange nicht gesättigt ist. Viele der teilnehmenden IT-Sicherheitsverantwortlichen würden die verschiedenen Projektergebnisse, die im Rahmen des Förderschwerpunkts ITS|KRITIS entstehen, gerne einsetzen. Hier werden mehr und bessere Methoden sowie Werkzeuge benötigt – der Forschungsbedarf ist sichtbar.

Die Erforschung der IT-Sicherheit in *Kritischen Infrastrukturen* wird auch zukünftig von Relevanz sein, weshalb die Absicht besteht die Studie erneut durchzuführen.

Danksagung

Das Begleitforschungsprojekt „Vernetzte IT-Sicherheit Kritischer Infrastrukturen“, VeSiKi, dankt dem BMBF für die Förderung (FKZ 16KIS0213). Des Weiteren danken wir Christian Voß, der einen wesentlichen Beitrag zur Entstehung des Fragebogens und der Durchführung der Umfragen eingebracht hat, Toni Kehr, der die Entwicklung und Einordnung in die Analysespinne vorangetrieben hat, Nuno de Mendoça, Oliver Götzenberger sowie den Multiplikatoren der Umfrage und vor allem den Teilnehmern der Umfrage, die uns die Informationsgewinnung erst ermöglichten.

Literatur

[BoDö05] J. Bortz, N. Döring: Forschungsmethoden und Evaluation : für Human- und Sozialwissenschaftler. Springer (2005) 3. Auflage.

[Borc16] D. Borchers: Ransomware-Virus legt Krankenhaus lahm. heise online (2016). Online verfügbar unter https://www.heise.de/newsticker/meldung/Ransomware-Virus-legt-Krankenhaus-lahm-3100418.html, zuletzt geprüft am 31.05.2017.

[BuMI09] Bundesministerium des Innern (BMI): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). (2009).

[Bund15] Bundestag: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015, Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31, Seite 8 ausgegeben zu Bonn am 24. Juli 2015.

[BuSI15] Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland 2015. (2015).

[BuSI17] Bundesamt für Sicherheit in der Informationstechnik (BSI): Schutz Kritischer Infrastrukturen durch Sicherheitsgesetz und UP KRITIS. (2017).

[DeJo89] D. M. DeJoy: The optimism bias and traffic accident risk perception. In: Accident Analysis & Prevention, (1989) 21. Jg., Nr. 4, S. 333–340.

[ErYo15] Ernst & Young (EY): Creating trust in the digital world: EY's Global Information Security Survey 2015. (2015).

[Fisc15] T. Fischer: Dell Security Survey 2015: Aktuelle IT-Sicherheitsstudie für deutsche Unternehmen. (2015).

[GGK+17] T. Gurschler, J. Großmann, D. Kotarski, C. Teichmann, C. Thim, J. Eichler, J. Göllner, N. Gronau, and U. Lechner: Risikobeurteilung in der IT-Sicherheit Kritischer Infrastrukturen – Eine Analyse der Risikobeurteilung im Förderschwerpunkt ITS|KRITIS. In: BSI (Hrsg.): Digitale Gesellschaft zwischen Risikobereitschaft und Sicherheitsbedürfnisse (Tagungsband zum 15. Deutschen IT-Sicherheitskongress, 16.-18.5.2017 in Bonn). SecuMedia (2017) S. 395-410.

[HMGo15] HM Government: 2015 Information Security breaches Survey. (2015).

[HoKa17] M. Holland, A. Kannenberg: WannaCry: Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm. heise online (2017). Online verfügbar unter https://www.heise.de/newsticker/meldung/WannaCry-Angriff-mit-Ransomware-legt-weltweit-Zehntausende-Rechner-lahm-3713235.html, Stand 31.05.2017.

[ISAC15] ISACA: State of Cybersecurity: Implications for 2015. (2015).

[Kasp15] Kaspersky: Global IT Security Risk Survey 2015. (2015).

[KoEG03] Die Kommission der europäischen Gemeinschaften: Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen. Amtsblatt der Europäischen Union, ABl. L 124 vom 20. Mai 2003.

[MeRe15] A. Meiritz, F. Reinbold: Hackerangriff auf den Bundestag: Das entblößte Parlament. Spiegel Online (2015). Online verfügbar unter http://www.spiegel.de/politik/deutschland/deutscher-bundestag-nach-hacker-angriff-das-entbloesste-parlament-a-1038290.html, zuletzt geprüft am 31.05.2017.

[Pric14] PricewaterhouseCoopers International (PWC): Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security Survey 2015. (2014).

[ScHE05] R. Schnell, P. B. Hill, E. Esser: *Methoden der empirischen Sozialforschung.* (2005) 7. Auflage.

[Spie17] Spiegel: Hacker greifen Bundestag an. Spiegel Online (2017). Online verfügbar unter http://www.spiegel.de/netzwelt/netzpolitik/berlin-hacker-greifen-bundestag-an-a-1140883.html, zuletzt geprüft am 31.05.2017.

[Stap13] T. Stapelkamp: Informationsvisualisierung : Web - Print - Signaletik. Springer, (2013).